М. Я. Кельберт, Ю. М. Сухов

ВЕРОЯТНОСТЬ И СТАТИСТИКА В ПРИМЕРАХ И ЗАДАЧАХ

Том 3

Теория информации и кодирования

Москва
Издательство МЦНМО
2013

УДК 519.21
ББК 22.171
К34

Издание осуществлено при поддержке РФФИ (издательский проект № 11-??-?????).

РФФИ

Кельберт М. Я., Сухов Ю. М.

К34 Вероятность и статистика в примерах и задачах. Т. 3: Теория информации и кодирования. М.: МЦНМО, 2013. — ??? с.: ил.

ISBN 978-5-94057-513-9

Для освоения таких разделов прикладной математики, как теория вероятностей, математическая статистика, теория информации и кодирование, тренировка в решении задач и выработка интуиции важны не меньше, чем изучение доказательств теорем; большое разнообразие задач по этому предмету затрудняет студентам переход от лекций к экзаменационным задачам, а от них — к практике.

Этот том включает стандартный пакет информационно-теоретического материала, обычно читаемого на факультетах информатики и электроники, а также прикладной математики ведущих университетов. При этом излагаются как вероятностные, так и алгебраические аспекты теории информации и кодирования, включая как основы теории, так и некоторые ее современные аспекты. Предмет этой книги критически важен для современных приложений (телекоммуникации, обработка сигналов, информатика, криптография).

Авторы собрали большое количество упражнений, снабженных полными решениями. Эти решения адаптированы к нуждам и умениям учащихся. Необходимые теоретические сведения приводятся по ходу изложения; кроме того, текст снабжен историческими отступлениями.

ББК 22.171

Перевод с английского С. Кулешова

ISBN 978-5-94057-???-? (т. 3)
ISBN 978-5-94057-513-9

Оглавление

Предисловие

Эта книга частично основывается на нескольких математических курсах Кембриджа: теория информации для 3-го года обучения (который читался, постоянно развиваясь, на протяжении последних четырех десятилетий под разными названиями), кодирование и криптография (более молодой и упрощённый курс, исключающий сложные технические вопросы) и более сложные курсы из части III (представляющей собой кембриджский эквивалент математической магистратуры). Содержание книги построено, по существу, вокруг следующих понятий:

а) энтропия распределения вероятностей как мера «недостоверности» и энтропия на случайный символ как мера «изменчивости» типичных траекторий случайного процесса,

б) кодирование как средство для измерения и использования избыточности информации, генерируемой процессом.

Таким образом, содержание данной книги включает более или менее стандартный пакет информационно-теоретического материала, который можно найти в наше время в учебных курсах по всему миру, в основном, читаемых на факультетах информатики и электроники и иногда теории вероятностей и математической статистики. Что отличает эту книгу от остальных, так это, прежде всего, широкий спектр примеров (отличительная черта всей нашей серии учебников «*Вероятность и статистика, в примерах*», опубликованной в издательстве Кембриджского университета). Большинство из этих примеров соответствуют уровню, принятому на экзаменах математических курсов в Кембридже. Таким образом, наши читатели могут сами понять, какого уровня они достигли или собираются достичь.

Второе отличие этой книги от большинства других книг по теории информации или теории кодирования заключается в том, что она охватывает оба возможных направления: вероятностное и алгебраическое. Как правило, эти направления исследований представлены в *разных* монографиях, учебниках и курсах, зачастую написанных людьми, работающими на разных факультетах. Подготовке этой книги способствовало то, что её авторы имели давние связи с Институтом проблем передачи информации Российской академии наук (ИППИ), в котором традиционно изучается широкий спектр проблем. Достаточно упомянуть, среди прочих, такие имена, как Роланд Добрушин, Рафаил Хасьминский, Марк Пинскер, Владимир Блиновский, Вячеслав Прелов, Борис Цыбаков, Камиль Зигангиров

(теория вероятностей и математическая статистика), Валентин Афанасьев, Сергей Гельфанд, Валерий Гоппа, Инна Грушко, Григорий Кабатянский, Григорий Маргулис, Юрий Сагалович, Алексей Скоробогатов, Михаил Цфасман, Леонид Бассалыго, Виктор Зиновьев, Виктор Зяблов (алгебра, комбинаторика, геометрия и теория чисел), которые работали или продолжают работать в ИППИ (было время, когда все они размещались в пяти комнатах в центре Москвы). Традиции преподавания математических тем в теории информации и кодирования в Кембридже восходят первоначально к Питеру Уиттлу (теория вероятностей и оптимизация) и позднее к Чарльзу Голди (теория вероятностей), Ричарду Пинчу (алгебра и геометрия), Тому Кёрнеру и Кейту Карну (анализ) и Тому Фишеру (теория чисел).

Мы также хотели бы добавить, что книга написана авторами, имеющими математическое образование (и остающимися до сих пор математиками), которые, тем не менее, имеют сильную тягу к приложениям, невзирая на все сопутствующие проблемы, возникающие в процессе прикладной работы: неопределённость, неточность, дискуссионность (включая, разумеется, личностный фактор) и последнее, но отнюдь не менее важное — необходимость эффективно применять на практике математические идеи. Авторы твердо считают, что математизация является основным путём к выживанию и совершенствованию в современном конкурентном мире и, следовательно, математику необходимо воспринимать всерьёз и изучать добросовестно.

Обе вышеупомянутые концепции (энтропия и коды), формирующие основу информационно-теоретического подхода к случайным процессам, были введены Шенноном в 1940-х гг., в довольно завершённой форме в публикациях [S, SW]. Конечно, понятие энтропии уже существовало в термодинамике, и его очень хорошо осознавали Больцман и Гиббс на стыке XIX и XX столетий. Коды также эффективно применялись на практике со времен античного мира. Но именно Шеннон полностью оценил роль этих понятий и положил их в основу современного информационно-теоретического подхода к случайным процессам. Не будучи профессиональным математиком, он не всегда давал полные доказательства своих конструкций. (Может быть, он и не задумывался о них.) В соответствующих разделах мы прокомментируем некоторые довольно деликатные моменты в отношениях Шеннона с математическим сообществом. К счастью, похоже, это его сильно не тревожило. (В отличие от Больцмана, который был особенно чувствителен к внешним отзывам и принимал их, пожалуй, слишком близко к сердцу.) Шеннон несомненно понимал всю ценность своих открытий, и, по нашему мнению, они ставят его в один ряд с такими выдающимися математиками, как Винер и фон Нейман.

Будет справедливо отметить, что имя Шеннона по-прежнему доминирует как в вероятностном, так и в алгебраическом направлениях в современной теории информации и кодирования. Это довольно необычно, учитывая, что мы говорим о вкладе человека, который работал в этой области более чем 40 лет назад. (Хотя в отношении нескольких сложных вопросов Шеннон, вероятно, мог бы повторить слова Эйнштейна, переформулировав их так: «С тех пор как математики вторглись в теорию связи, я перестал что-либо понимать в ней».)

За годы, что прошли после работ Шеннона, в математике и электротехнике произошли большие изменения, не говоря уже о компьютерных науках. Кто бы мог предвидеть в 1940–1950-х гг., что соперничество между подходами Шеннона в теории информации и Винера в кибернетике получит такое завершение? Действительно, кибернетика обещала огромные (даже фантастические) выгоды для всего человечества, в то время как теория информации только утверждала, что в определенных пределах можно достичь скромной цели исправления ошибок при передаче.

Книга Винера [W] в 1950–1960-х гг. пленила умы мыслителей практически во всех областях интеллектуальной деятельности. В частности, кибернетика стала серьезной политической проблемой в Советском Союзе и его странах-сателлитах: сначала она была объявлена «буржуазной антинаучной теорией», а затем ей придали неоправданно большое значение. (Цитата из критического обзора кибернетики в ведущем в советской идеологии журнале «*Вопросы философии*» 1953 г. гласит: «Империалистам не удаётся разрешить противоречия умирающего капиталистического общества. Они не могут предотвратить неизбежный экономический кризис. И поэтому они пытаются найти решение не только в бешеной гонке вооружений, но и в идеологической войне. В глубоком отчаянии они прибегают к помощи псевдонауки, которая даёт им некоторые проблески надежды продлить их существование». Советский «*Краткий словарь по философии*» (1954 г.), имевший тираж в сотни тысяч экземпляров, определял кибернетику как «реакционную псевдонауку, которая появилась в США после первой мировой войны и позднее распространилась в других капиталистических странах: вид современного механицизма». Однако под давлением ведущих советских физиков, завоевавших авторитет после успехов советской ядерной программы, тот же самый журнал «*Вопросы философии*» в 1955 г. опубликовал позитивный отзыв о кибернетике. Среди авторов этой статьи были Алексей Ляпунов и Сергей Соболев, выдающиеся советские математики.)

Любопытно, что в недавно опубликованной биографии Винера [CS] указывается, что существуют «тайные правительственные документы (США), которые показывают, как ФБР и ЦРУ следили за Винером

в разгар холодной войны, чтобы помешать его социальной активности и растущему влиянию кибернетики в стране и за рубежом». Интересные сравнения можно найти в работе [Hei].

Однако история пошла своим путём. Фримен Дайсон написал в своём обзоре [Dy]: «(Теория Шеннона) была математически элегантной, понятной и легко применимой на практике к проблемам связи. Она была намного более удобной для пользователя, чем кибернетика. Теория стала основой новой дисциплины под названием теория информации... (В настоящее время) в базовый курс подготовки инженеров по электронике входит теория информации, основанная на теории Шеннона, а кибернетика оказалась забытой».

Однако не совсем так: только на территории бывшего Советского Союза до сих пор работают институты и отделы, в название которых входит слово «кибернетика»: два в Москве, два в Минске, и по одному в Таллине, Тбилиси, Ташкенте и Киеве (последний являлся известнейшим центром компьютерной науки в целом в бывшем СССР). И в Великобритании существуют по крайней мере четыре факультета, в университетах Болтона, Брэдфорда, Халла и Рединга, не считая различных ассоциаций и обществ. Во всём мире общества, связанные с кибернетикой, кажется, процветают, что видно из перечисления названий: от Института метода (Швейцария) или Академии кибернетики (Италия) до аргентинской Ассоциации общей теории систем и кибернетики, Буэнос-Айрес. И мы были рады узнать о существовании Кембриджского кибернетического общества (Бельмонт, Калифорния, США). Напротив, теория информации фигурирует в названиях лишь нескольких организаций. Видимо, давний спор между Шенноном и Винером еще не вполне закончен.

В любом случае репутация Винера в области математики остаётся несокрушимой. Достаточно назвать несколько жемчужин его творчества, таких как теорема Пэли—Винера (которая была доказана во время многочисленных посещений Винером Кембриджа), метод Винера—Хопфа и, конечно, особенно близкий нашему сердцу винеровский процесс, чтобы понять его истинную роль в научных исследованиях и приложениях.

Существующие воспоминания об этом гиганте науки изображают Винера сложной и противоречивой личностью. (Название биографии [CS] в этом смысле весьма показательно, хотя такие взгляды оспариваются; см., например, обзор [Mar]. В этой книге мы пытаемся принять более мягкий тон, как, например, в главе о Винере в книге [Ja], с. 386–391). С другой стороны, имеющиеся документальные записи о жизни Шеннона (так же как и других отцов теории информации и кодирования, в частности Ричарда Хэмминга) дают целостную картину спокойного, умного человека, не лишённого чувства юмора. Мы надеемся, что такое впечатление не будет

мешать написанию биографии Шеннона и что в будущем мы увидим столь же много книг о Шенноне, сколько их написано о Винере.

Как было сказано ранее, цель этой книги двояка: обеспечить синтетическое введение в вероятностные и алгебраические аспекты теории, поддерживаемое значительным количеством задач и примеров, и обсудить ряд вопросов, редко представленных в большинстве книг. Главы 1–3 дают введение в основы теории информации и кодирования и обсуждают некоторые современные ответвления этих тем. Мы концентрируемся в этих главах на типичных задачах и примерах (многие из которых возникли в кембриджских курсах) больше, чем на подробном изложении теории, стоящей за ними. Глава 4 даёт краткое введение в более специализированные разделы теории информации. Здесь изложение более сжато и некоторые важные результаты приводятся без доказательств.

В связи с тем, что большая часть текста основана на конспектах лекций и решений различных задач для аудиторных занятий и экзаменов, в книге встречаются неизбежные повторы, многие обозначения и примеры даются на упрощённом языке. Часто мы делали это сознательно, чтобы передать живую атмосферу процесса преподавания и изучения.

Три прекрасные книги [GP], [M] и [CT] оказали особенно сильное влияние на наш учебник. Здесь сыграла свою роль наша долгая дружба с Чарльзом Голди, так же как и знакомство с Томом Ковером. Кроме того, на наш текст оказали влияние такие книги, как [Bl, MWS, R1] и [vL] (мы даже кое-что заимствовали из них). Мы благодарим за гостеприимство Институт Исаака Ньютона Университета Кембриджа (2002–2010 гг.), особенно программу стохастических процессов в коммуникационных науках (январь–июль 2010 г.). Различные части книги обсуждались со многими коллегами из разных учреждений, в первую очередь из Института проблем передачи информации и Института математической геофизики и прогноза землетрясений, Москва. Мы хотели бы поблагодарить Джеймса Лоуренса (статистическая лаборатория Университета Кембриджа) за его помощь с рисунками.

В ходе заключительного этапа работы над книгой значительную роль сыграла поддержка агентства FAPESP (штат Сан-Пауло, Бразилия), в рамках грантов 2010/17835-0, 2011.20133-0 и 2012.04372-7, а также Ректории Университета Сан-Пауло в рамках гранта 2011.5.764.45.0. Перевод книги на русский язык и техническая сторона её подготовки к печати были выполнены при поддержке РФФИ. Работа переводчика С. Кулешова и редактора О. Широковой заслуживает самой высокой оценки и глубокой благодарности.

Ссылки на том 1 и том 2 относятся к переводам наших книг «Вероятность и статистика в примерах», том 1 и 2 (Probability and Statistics

by Example, Cambridge University Press); страницы даются по русскому изданию. Мы используем стиль этих книг, подавая бóльшую часть материала как «примеры с решениями». Много материала дается в виде задач, взятых из экзаменационных работ (Cambridge Tripos Exam papers), которые сохраняют свой оригинальный стиль.

На протяжении всей книги мы старались развлечь читателя. Когда нашей собственной фантазии не хватало, мы привлекали идеи других авторов, в основном из различных интернет-источников. (К счастью, поток юмора кажется неиссякаемым, и иногда в интернете появляются блестящие высказывания.)

Символ □ указывает на конец отдельной части книги, чтобы отделить её от последующего текста: это относится к примерам, задачам (решениям), определениям, замечаниям и доказательствам.

Глава 1

Основные понятия теории информации

На протяжении всей книги символ P обозначает различные распределения вероятностей. В частности, в гл. 1 этот символ преимущественно обозначает распределение вероятностей последовательности случайных величин (с. в.), характеризующей источники информации. Как правило, это будут последовательности независимых одинаково распределенных случайных величин (н. о. р. с. в.) или цепи Маркова с дискретным временем (ц. м. д. в.); $\mathsf{P}(U_1 = u_1, \ldots, U_n = u_n)$ — *совместная вероятность* события, при котором с. в. $U_1, \ldots, U_n$ принимают значения $u_1, \ldots, u_n$, а $\mathsf{P}(V = v \,|\, U = u,\ W = w)$ — *условная вероятность*, т. е. вероятность того, что с. в. V принимает значение v при условии, что с. в. U и W равны u и w соответственно. Символ E закреплён за *математическим ожиданием* с. в. с распределением P.

Символы p и P используются для обозначения различных вероятностей (и связанных с ними объектов, таких как переходная функция ц. м. д. в.). Символ $\#A$ обозначает мощность конечного множества A. Символом $\mathbf{1}$ обозначается *индикаторная* (характеристическая) функция множества. Для логарифмов будем использовать следующие обозначения и правила действия: $\log = \log_2$ и $\forall\, b > 1$: $0 \cdot \log_b 0 = 0 \cdot \log_b \infty = 0$. Далее, при $x > 0$ через $\lfloor x \rfloor$ и $\lceil x \rceil$ мы обозначим максимальное целое число, не превосходящее x, и минимальное целое число, не меньшее x, соответственно. Таким образом, $\lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil$; неравенство превращается в равенство при целых x ($\lfloor x \rfloor$ называется *целой частью* числа x).

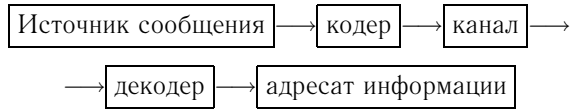
Аббревиатуры л. ч. и п. ч. обозначают соответственно левую и правую части уравнения или неравенства.

§ 1.1. Основные понятия. Неравенство Крафта. Кодирование Хаффмана

Жить эффективно — жить с адекватной информацией.

Норберт Винер (1894–1964),
американский математик

Типичная схема, применяемая при передаче информации, выглядит следующим образом:



Пример 1.1.1. 1. Источник сообщения: хор Кембриджского колледжа.

2. Кодер: блок записи Би-Би-Си. Он переводит звук в двоичный массив и записывает его на дорожку компакт-диска. Затем компакт-диск размножают и передают в магазин.

3. Канал: оптовый покупатель компакт-дисков в Англии, переправляющий их в Австралию. На канал воздействует «шум»: возможный ущерб (от механических, электрических, химических и др. воздействий), полученный во время передачи (транспортировки).

4. Декодер: проигрыватель компакт-дисков в Австралии.

5. Адресат информации: аудитории в Австралии.

6. Цель: обеспечение высокого качества звука, несмотря на повреждения.

В самом деле, компакт-диск может повредиться от иглы, если в нём проделать аккуратную дырку, или от крошечной капли кислоты и все еще давать высокое качество звучания при проигрывании (мы категорически не рекомендуем проводить такой эксперимент!). Это наглядно иллюстрирует способности корректирующих кодов. С технической точки зрения типичные цели передачи информации следующие: 1) быстрое кодирование информации, 2) удобная передача закодированных данных, 3) эффективное использование доступного канала (т. е. максимальная передача информации в единицу времени), 4) быстрое декодирование, 5) исправление ошибок (как можно большего количества), внесенных шумом в канале. □

Как правило, эти цели противоречат друг другу, и необходимо найти оптимальное решение. Как раз об этом и говорит данная глава. К сожалению, не приходится ожидать идеального решения: теория, которая будет изложена, в основном нацелена на изложение основных принципов. Окончательное решение всегда ложится на плечи ответственного лица (или

группы). Большая часть этого параграфа (и вся глава 1) будет посвящена проблемам кодирования. Целями кодирования являются:

1) сжатие данных для уменьшения избыточной информации, содержащейся в сообщении;

2) защита текста от несанкционированного пользователя;

3) исправление допущенных ошибок.

Мы начинаем с изучения *источников* и *кодеров*. Источник генерирует последовательность букв (или символов)

$$u_1 u_2 \dots u_n \dots, \tag{1.1.1}$$

где $u_j \in I$ $(= I_m)$ — m-элементное множество, часто отождествляемое с $\{1, \dots, m\}$ (*алфавит источника*). В случае литературного английского языка $m = 26 + 7$, 26 букв плюс 7 символов пунктуации: . , : ; – ( ). (Иногда добавляют знаки: ? ! ’ ‘ и "). В случае английского телеграфа $m = 27$.

Как правило, последовательность (1.1.1) рассматривают как *выборку* из случайного источника, т. е. последовательности с. в.

$$U_1, U_2, \dots, U_n, \dots, \tag{1.1.2}$$

и пытаются разработать теорию для разумного класса таких последовательностей.

Пример 1.1.2. 1. Простейший пример случайного источника — это последовательность н. о. р. с. в.:

$$\mathsf{P}(U_1 = u_1, U_2 = u_2, \dots, U_k = u_k) = \prod_{j=1}^{k} p(u_j), \tag{1.1.3а}$$

где $p(u) = \mathsf{P}(U_j = u)$, $u \in I$, — распределение одной с. в. Случайный источник с независимыми одинаково распределёнными символами часто называют *источником Бернулли*.

Частный случай, когда вероятность $p(u)$ не зависит от $u \in I$ (и поэтому равна $1/m$), соответствует *равновероятному источнику Бернулли*.

2. Более общим примером служит *источник Маркова*, где последовательность символов представляет собой дискретную цепь Маркова:

$$\mathsf{P}(U_1 = u_1, U_2 = u_2, \dots, U_k = u_k) = \lambda(u_1) \prod_{j=1}^{k-1} P(u_j, u_{j+1}), \tag{1.1.3б}$$

где $\lambda(u) = \mathsf{P}(U_1 = u)$, $u \in I$, — начальное распределение и $P(u, u') = \mathsf{P}(U_{j+1} = u' \,|\, U_j = u)$, $u, u' \in I$, — вероятность перехода. Источник Маркова называется *стационарным*, если $\mathsf{P}(U_j = u) = \lambda(u)$, $j \geqslant 1$, т. е.

$\lambda = \{\lambda(u),\ u = 1, \ldots, m\}$ — инвариантная вектор-строка матрицы $P = \{P(u, v)\} : \sum\limits_{u \in I} \lambda(u) P(u, v) = \lambda(v),\ v \in I$, или, короче, $\lambda P = \lambda$.

«Вырожденным» примером источника Маркова является источник, генерирующий повторяющиеся символы. В этой ситуации

$$\begin{aligned} \mathsf{P}(U_1 = U_2 = \ldots = U_k = u) &= p(u), \quad u \in I, \\ \mathsf{P}(U_k \neq U_{k'}) &= 0, \quad 1 \leqslant k < k', \end{aligned} \tag{1.1.3в}$$

где $0 \leqslant p(u) \leqslant 1$ и $\sum\limits_{u \in I} p(u) = 1$. □

Начальный участок последовательности (1.1.1)

$$\mathbf{u}(n) = (u_1, u_2, \ldots, u_n), \quad \text{или} \quad \mathbf{u}(n) = u_1 u_2 \ldots u_n,$$

называется выборочной (из источника) *n-строкой* или *n-словом* (или, короче, строкой или словом), Соответственно рассматриваются случайные n-строки (случайные сообщения):

$$\mathbf{U}^{(n)} = (U_1, U_2, \ldots, U_n), \quad \text{или, иначе} \quad \mathbf{U}^{(n)} = U_1 U_2 \ldots U_n.$$

Кодер использует *алфавит* $J (= J_q)$, который мы обычно будем записывать как $0, 1, \ldots, q-1$; как правило, число кодирующих символов q меньше m (или даже $q \ll m$); во многих случаях $q = 2$ и $J = \{0, 1\}$ (двоичный кодер). *Код* (также кодировка) — это отображение f, переводящее символ $u \in I$ в конечное слово $f(u) = x_1 \ldots x_s$, знаки которого выбираются из J. Иначе говоря, f отображает I в множество J^* всех возможных строк:

$$f\colon I \to J^* = \bigcup_{s \geqslant 1} \underbrace{J \times J \times \ldots \times J}_{s \text{ раз}}.$$

Строка $f(u)$, являющаяся образом при отображении f символов $u \in I$, называется *кодовым словом* (в коде f). Говорят, что код имеет (постоянную) длину N, если величина s (длина кодового слова) равна N для всех кодовых слов. Сообщение $\mathbf{u}(n) = u_1 u_2 \ldots u_n$ представляется как сцепление кодовых слов:

$$f(\mathbf{u}^{(n)}) = f(u_1) f(u_2) \ldots f(u_n),$$

т. е. снова как строка из J^*.

Определение 1.1.3. Мы говорим, что данный код является *кодом без потерь*, если из предположения $u \neq u'$ следует, что $f(u) \neq f(u')$ (т. е. отображение $f\colon I \to J^*$ — вложение[1]). Код допускает декодирование (или декодируемый), если любая строка из J^* изображает не более одного

[1] В оригинале использован термин «one-to-one map», т. е. «взаимно однозначное отображение», но мы следуем здесь российской математической традиции. — *Прим. перев.*

сообщения. Строка x служит *префиксом* в другой строке y, если $y = xz$, т. е. строка y может быть представлена как результат сцепления x и z. Код называют *свободным от префиксов* или *беспрефиксным*, если ни одно из кодовых слов не является префиксом другого (например, код постоянной длины беспрефиксный). □

Беспрефиксный код допускает декодирование, однако обратное утверждение неверно.

Пример 1.1.4. Код с трехсимвольным алфавитом источника $I = \{1, 2, 3\}$ и двоичным алфавитом кодера $J = \{0, 1\}$, заданный соотношениями

$$f(1) = 0, \quad f(2) = 01, \quad f(3) = 011,$$

декодируемый, но не свободен от префиксов. □

Теорема 1.1.5 (неравенство Крафта). *Для данных натуральных чисел $s_1, \ldots, s_m$ декодируемый код $f\colon I \to J^*$ с кодовыми словами длин $s_1, \ldots, s_m$ существует тогда и только тогда, когда*

$$\sum_{i=1}^{m} q^{-s_i} \leqslant 1. \tag{1.1.4}$$

Более того, если выполнено неравенство (1.1.4), *то существует беспрефиксный код с кодовыми словами длин $s_1, \ldots, s_m$.*

Доказательство. 1. Достаточность. Пусть неравенство (1.1.4) выполнено. Нам нужно построить беспрефиксный код с кодовыми словами длин $s_1, \ldots, s_m$. Перепишем неравенство (1.1.4) как

$$\sum_{l=1}^{s} n_l q^{-l} \leqslant 1, \tag{1.1.5}$$

или

$$n_s q^{-s} \leqslant 1 - \sum_{l=1}^{s-1} n_l q^{-l},$$

где n_l — количество слов длины l и $s = \max[s_i]$. Распишем последнее неравенство подробнее:

$$n_s \leqslant q^s - n_1 q^{s-1} - \ldots - n_{s-1} q. \tag{1.1.6.1}$$

Поскольку $n_s \geqslant 0$, получаем

$$n_{s-1} q \leqslant q^s - n_1 q^{s-1} - \ldots - n_{s-2} q^2,$$

или

$$n_{s-1} \leqslant q^{s-1} - n_1 q^{s-2} - \ldots - n_{s-2} q. \tag{1.1.6.2}$$

Продолжая рассуждения, последовательно приходим к неравенствам

$$n_{s-2} \leqslant q^{s-2} - n_1 q^{s-3} - \ldots - n_{s-3} q,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$n_2 \leqslant q^2 - n_1 q, \qquad (1.1.6.s{-}1)$$
$$n_1 \leqslant q. \qquad (1.1.6.s)$$

Отметим, что на самом деле или $n_{i+1} = 0$, или n_i меньше п. ч. неравенства $\forall\, i = 1, \ldots, s-1$ (по определению $n_s \geqslant 1$, так что для $i = s-1$ имеет место вторая возможность). Проделаем следующее. Сначала выпишем n_1 слов длины 1, используя различные символы из J (это возможно в силу неравенства (1.6.s)). Осталось $q - n_1$ неиспользованных символов; далее, сформируем $(q - n_1)q$ слов длины 2, дописывая к каждому неиспользованному символу ещё по одному. Выберем n_2 таких слов (что можно сделать ввиду неравенства (1.6.s-1). У нас все еще остаётся $q^2 - n_1 q - n_2$ неиспользованных слова длины 2. Строим n_3 слов длины 3 и т. д. По построению ни одно из новых слов не будет содержать предыдущих в качестве префикса. Следовательно, построенный код свободен от префиксов.

2. Необходимость. Предположим, что существует декодируемый код с алфавитом J с кодовыми словами длин $s_1, \ldots, s_m$. Вновь положим $s = \max\{s_i\}$ и заметим, что для любого натурального r выполняется равенство

$$(q^{-s_1} + \ldots + q^{-s_m})^r = \sum_{l=1}^{rs} b_l q^{-l},$$

где b_l — количество способов получения из r слов строки длины l.

Ввиду декодируемости эти строки должны быть различными. Значит, $b_l \leqslant q^l$, поскольку q^l — число всех строк длины l. Следовательно,

$$(q^{-s_1} + \ldots + q^{-s_m})^r \leqslant rs,$$

и

$$q^{-s_1} + \ldots + q^{-s_m} \leqslant r^{1/r} s^{1/r} = \exp\left(\frac{1}{r}(\log r + \log s)\right).$$

Так как это верно при любом r, переходя к пределу при $r \to \infty$, мы увидим, что правая часть неравенства стремится к 1. □

Замечание 1.1.6. Код, подчиняющийся неравенству (1.1.4), не обязательно допускает декодирование. □

Леон Г. Крафт вывел неравенство (1.1.4) в своей диссертации на звание доктора философии в Массачусетском технологическом институте в 1949 г.

Одна из основных целей теории состоит в том, чтобы найти «лучший» (т. е. кратчайший) декодируемый (или беспрефиксный) код. Встанем сейчас

на вероятностную точку зрения и предположим, что символ $u \in I$ генерируется источником с вероятностью $p(u)$:

$$\mathsf{P}(U_k = u) = p(u).$$

(На данный момент нет необходимости указывать совместную вероятность более чем одного сгенерированного символа.)

Напомним, что данным кодом $f\colon I \to J^*$ мы кодируем букву $i \in I$, предписывая ей кодовое слово $f(i) = x_1 \dots x_{s(i)}$ длины $s(i)$. Для произвольного символа сгенерированное кодовое слово становится случайной строкой из J^*. Пусть f — код без потерь, тогда вероятность получения данной строки как кодового слова для символа в точности равна $p(i)$, если эта строка совпадает с $f(i)$, и 0, если нет такой буквы $i \in I$, для которой это так.

Если f не вложение, то вероятность строки равна сумме членов $p(i)$, для которых кодовое слово $f(i)$ равно данной строке. Таким образом, длина кодового слова тоже случайная величина S с распределением вероятностей

$$\mathsf{P}(S = s) = \sum_{1 \leqslant i \leqslant m} \mathbf{1}(s(i) = s) p(i).$$

Мы ищем такой декодируемый код, чтобы минимизировать *математическое ожидание длины слова*

$$\mathsf{E}S = \sum_{s \geqslant 1} s\,\mathsf{P}(S = s) = \sum_{i=1}^{m} s(i) p(i).$$

Таким образом, возникает следующая задача:

$$\begin{gathered}\text{минимизировать } g(s(1) \dots s(m)) = \mathsf{E}S \text{ при условии} \\ \sum_i q^{-s(i)} \leqslant 1 \text{ (Крафт), где } s(i) \text{ — натуральные числа.}\end{gathered} \tag{1.1.7}$$

Теорема 1.1.7. *Оптимальное решение задачи* (1.1.7) *удовлетворяет неравенству*

$$\min \mathsf{E}S \geqslant h_q(p(1), \dots, p(m)), \tag{1.1.8}$$

где

$$h_q(p(1), \dots, p(m)) = -\sum_i p(i) \log_q p(i). \tag{1.1.9a}$$

Доказательство. Задача (1.1.7) — это целочисленная задача оптимизации. Если заменить условие $s(1), \dots, s(m) \in \{1, 2, \dots\}$ более слабым: $s(i) > 0,\ \ 1 \leqslant i \leqslant m$, то можно использовать теорему Лагранжа об

условном минимуме. Функция Лагранжа в этом случае выглядит так:

$$\mathcal{L}(s(1), \ldots, s(m), z; \lambda) = \sum_i s(i)p(i) + \lambda\Big(1 - \sum_i q^{-s(i)} - z\Big)$$

(здесь $z \geqslant 0$ — резервная переменная). Минимизируя $\mathcal{L}$ по $s(1), \ldots, s(m)$ и z, получаем

$$\lambda < 0, \;\; z = 0 \;\; \text{и} \;\; \frac{\partial \mathcal{L}}{\partial s(i)} = p(i) + q^{-s(i)}\lambda \ln q = 0,$$

откуда следует, что

$$-\frac{p(i)}{\lambda \ln q} = q^{-s(i)}, \quad \text{т. е.} \;\; s(i) = -\log_q p(i) + \log_q(-\lambda \ln q), \quad 1 \leqslant i \leqslant m.$$

Учитывая ограничение $\sum\limits_i q^{-s(i)} = 1$ (резервная переменная $z = 0$), получаем

$$\sum_i p(i)/(-\lambda \ln q) = 1, \quad \text{т. е.} \quad -\lambda \ln q = 1.$$

Следовательно, набор

$$s(i) = -\log_q p(i), \quad 1 \leqslant i \leqslant m,$$

является (единственным) решением задачи минимизации, определяющим значение h_q из формулы (1.1.9а). Мы нашли решение задачи минимизации на бóльшем множестве, чем требовалось, поэтому минимальное значение не больше, чем п. ч. формулы (1.1.8). □

Замечание 1.1.8. Величина h_q, определенная формулой (1.1.9а), играет центральную роль в теории информации. Она называется *q-ичной энтропией* распределения вероятностей $(p(x),\ x \in I)$ и будет появляться во многих ситуациях. Отметим, что справедлива формула

$$h_q(p(1), \ldots, p(m)) = \frac{1}{\log q} h_2(p(1), \ldots, p(m)),$$

где h_2 — двоичная энтропия,

$$h_2(p(1), \ldots, p(m)) = -\sum_i p(i) \log p(i). \qquad (1.1.9б)$$

□

Пример 1.1.9. 1. Приведите пример кода без потерь с алфавитом J_q, не удовлетворяющего неравенству Крафта. Приведите пример кода без потерь, в котором математическое ожидание длины кодового слова строго меньше чем $h_q(X)$.

2. Покажите, что «сумма Крафта» $\sum_i q^{-s(i)}$, выписанная по коду без потерь, может быть сколь угодно большой (при достаточно большом алфавите источника).

Решение. 1. Рассмотрим алфавит $I = \{0, 1, 2\}$ и код без потерь f с $f(0) = 0$, $f(1) = 1$, $f(2) = 00$. Тогда длины кодовых слов таковы: $s(0) = s(1) = 1$, $s(2) = 2$. Очевидно, что $\sum_{x \in I} 2^{-s(x)} = 5/4$, что противоречит неравенству Крафта. Для с. в. X с $p(0) = p(1) = p(2) = 1/3$ математическое ожидание длины кодового слова равно $\mathsf{E}S(X) = 4/3 < h(X) = \log 3 \approx 1{,}585$.

2. Предположим, что размер алфавита m равен $\#I = 2(2^L - 1)$ для некоторого натурального числа L. Рассмотрим код без потерь, сопоставляющий буквам $x \in I$ кодовые слова 0, 1, 00, 01, 10, 11, 000, ..., достигающие максимальной длины L. Суммой Крафта будет

$$\sum_{x \in I} 2^{-s(x)} = \sum_{l \leqslant L} \sum_{x:\, s(x) = l} 2^{-s(x)} = \sum_{l \leqslant L} 2^l \times 2^{-l} = L,$$

что может быть сколь угодно большим. □

Теорема 1.1.7 получает дальнейшее развитие в теореме 1.1.10.

Теорема 1.1.10 (теорема Шеннона для канала без шума). *Для случайного источника, генерирующего символы с вероятностью $p(i) > 0$, минимальное математическое ожидание длины кодового слова в декодируемом кодере с алфавитом J_q подчиняется неравенству*

$$h_q \leqslant \min \mathsf{E}S < h_q + 1, \tag{1.1.10}$$

где $h_q = -\sum_i p(i) \log_q p(i)$ — q-ичная энтропия источника (ср. с формулой (1.1.9а)).

Доказательство. Л. ч. неравенства следует из теоремы 1.1.7. Для доказательства п. ч. выберем такое натуральное число $s(i)$, что

$$q^{-s(i)} \leqslant p(i) < q^{-s(i)+1}.$$

Отсюда следует нестрогая оценка $\sum_i q^{-s(i)} \leqslant \sum_i p(i) = 1$, т. е. неравенство Крафта. Значит, найдется декодируемый код с кодовыми словами длин $s(1), \ldots, s(m)$. Из п. ч. неравенства вытекает, что

$$s(i) < -\frac{\log p(i)}{\log q} + 1,$$

и поэтому

$$\mathsf{E}S < -\frac{\sum_i p(i) \log p(i)}{\log q} + \sum_i p(i) = \frac{h}{\log q} + 1. \qquad \square$$

Остерегайтесь найти то, что вы ищете.

Ричард Хэмминг (1915–1998),
американский математик и программист

Пример 1.1.11. Поучительное приложение теоремы Шеннона 1.1.10 заключается в следующем. Пусть размер m алфавита источника равен 2^k, и предположим, что буквы $i = 1, \ldots, m$ генерируются равновероятно: $p(i) = 2^{-k}$. Допустим, алфавит кодера — это $J_2 = \{0, 1\}$ (двоичный кодер). Так как двоичная энтропия равна $h_2 = -\log 2^{-k} \sum\limits_{1 \leqslant i \leqslant 2^k} 2^{-k} = k$, нам потребуется (в среднем) по крайней мере k двоичных знаков для декодируемого кодера. Используя термин «бит» для единицы энтропии, мы говорим, что в среднем кодирование требует по крайней мере k битов. Кроме того, теорема 1.1.10 приводит к процедуре кодирования Шеннона—Фано: мы фиксируем в качестве длин кодовых слов такие натуральные числа $s(1), \ldots, s(m)$, что $q^{-s(i)} \leqslant p(i) < q^{-s(i)+1}$, или, что эквивалентно,

$$-\log p(i) \leqslant s(i) < -\log p(i) + 1, \quad \text{т. е.} \quad s(i) = \lceil -\log p(i) \rceil. \tag{1.1.11}$$

Затем мы строим беспрефиксный код, начиная со слова наименьшей длины $s(i)$, постепенно увеличивая длину слов следя за тем, чтобы предыдущие кодовые слова не являлись префиксами. Неравенство Крафта гарантирует, что нам это удастся. Полученный код может не быть оптимальным, но средняя длина его кодового слова удовлетворяет неравенству (1.1.11), как в оптимальном коде. □

Оптимальность достигается при *кодировании Хаффмана* $f_m^{\mathrm{H}}\colon I_m \to J_q^*$. Сначала мы обсудим случай двоичной кодировки, т. е. $q = 2$ и $J = \{0, 1\}$. Алгоритм построения бинарного дерева выглядит следующим образом.

1. Во-первых, упорядочим буквы $i \in I$ так, что

$$p(1) \geqslant p(2) \geqslant \ldots \geqslant p(m).$$

2. Припишем символ 0 букве $m - 1$ и символ 1 букве m.

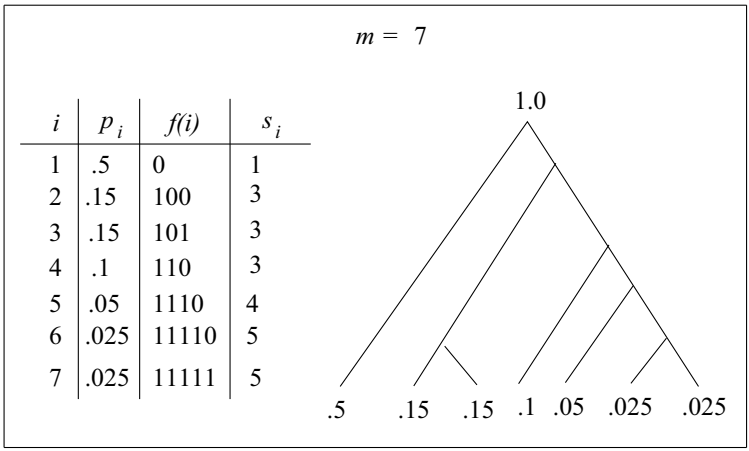
3. Построим редуцированный алфавит

$$I_{m-1} = \{1, \ldots, m-2, (m-1, m)\}$$

с вероятностями $p(1), \ldots, p(m-2), p(m-1) + p(m)$.

Повторим шаги 1 и 2 с редуцированным алфавитом, и т. д. Мы получаем двоичное дерево, листья которого соответствуют буквам алфавита источника, а вершины — группам объединенных символов. Пример кодирования Хаффмана для $m = 7$ приведён на рис. 1.1.

Количество ветвей, которое мы должны пройти, от листа i до корня, равно $s(i)$. Структура дерева, листья которого отождествляются с буквами



i	p_i	$f(i)$	s_i
1	.5	0	1
2	.15	100	3
3	.15	101	3
4	.1	110	3
5	.05	1110	4
6	.025	11110	5
7	.025	11111	5

Рис. 1.1

алфавита, гарантирует, что код будет свободен от префиксов. Оптимальность двоичного кодирования Хаффмана вытекает из следующих двух простых лемм.

Лемма 1.1.12. *У любого оптимального беспрефиксного двоичного кода длины кодовых слов упорядочены противоположно вероятностям*:

$$p(i) \geqslant p(i') \quad \Rightarrow \quad s(i) \leqslant s(i'). \tag{1.1.12}$$

Доказательство. Если это не так, то можно модифицировать код, поменяв местами кодовые слова для i и i'. Это уменьшит математическое ожидание длины кодового слова, сохранив свободу от префиксов. □

Лемма 1.1.13. *В любом оптимальном свободном от префиксов двоичном коде среди кодовых слов максимальной длины существуют ровно два совпадающих всюду, кроме последнего знака.*

Доказательство. Если это не так, то либо 1) существует единственное слово максимальной длины, либо 2) найдутся два или больше слов максимальной длины, но отличаться друг от друга они будут ранее последнего знака. В обоих случаях последний знак из некоторого слова максимальной длины можно выбросить, не влияя на свободу от префиксов. □

Теорема 1.1.14. *Код Хаффмана — оптимальный среди всех беспрефиксных двоичных кодов.*

Доказательство. Доказательство проведём индукцией по m. При $m = 2$ код Хаффмана f_2^{H} определяется так: $f_2^{\mathrm{H}}(1) = 0$, $f_2^{\mathrm{H}}(2) = 1$ или наобо-

рот, и он является оптимальным. Предположим, что код Хаффмана f^{H}_{m-1} оптимален для I_{m-1} при любом распределении вероятностей. Допустим, далее, что код Хаффмана f^{H}_m не оптимален для I_m при некотором распределении вероятностей. Иначе говоря, существует другой беспрефиксный код f^*_m, для I_m с меньшим математическим ожиданием длины кодового слова:

$$\mathsf{E}S^*_m < \mathsf{E}S^{\mathrm{H}}_m. \tag{1.1.13}$$

Без ограничения общности можно считать, что распределение вероятностей удовлетворяет неравенствам

$$p(1) \geqslant \ldots \geqslant p(m).$$

По леммам 1.1.12 и 1.1.13 можно перенумеровать кодовые слова в обоих кодах так, что слова, соответствующие $m-1$ и m, будут иметь максимальную длину и отличаться друг от друга лишь в последнем знаке. Это позволяет свести оба кода к I_{m-1}. Действительно, в коде Хаффмана f^{H}_m мы удалим последний знак из $f^{\mathrm{H}}_m(m)$ и $f^{\mathrm{H}}_m(m-1)$, «склеив» эти слова. Эта процедура приведёт нас к коду Хаффмана f^{H}_{m-1}. С кодом f^*_m поступим аналогично, и получим новый беспрефиксный код f^*_{m-1}.

Заметим, что в коде Хаффмана f^{H}_m вклад в $\mathsf{E}S^{\mathrm{H}}_m$ из $f^{\mathrm{H}}_m(m-1)$ и $f^{\mathrm{H}}_m(m)$ равен $s^{\mathrm{H}}(m)(p(m-1)+p(m))$, и после редуцирования он становится равен $(s^{\mathrm{H}}(m)-1)(p(m-1)+p(m))$, т. е. $\mathsf{E}S$ уменьшается на $p(m-1)+p(m)$. В коде f^*_m аналогичный вклад уменьшается с $s^*(m)(p(m-1)+p(m))$ до $(s^*(m)-1)(p(m-1)+p(m))$. Значит, и здесь разница составит $p(m-1)+p(m)$. Все остальные вклады в $\mathsf{E}S^{\mathrm{H}}_{m-1}$ и $\mathsf{E}S^*_{m-1}$ совпадают с соответствующими вкладами в $\mathsf{E}S^{\mathrm{H}}_m$ и $\mathsf{E}S^*_m$. Следовательно, код f^*_{m-1} предпочтительнее, чем f^{H}_{m-1}: $\mathsf{E}S^*_{m-1} < \mathsf{E}S^{\mathrm{H}}_{m-1}$, что противоречит предположению индукции. □

С учетом теоремы 1.1.14 мы получаем следующий результат.

Следствие 1.1.15. *Кодирование Хаффмана является оптимальным среди всех декодируемых двоичных кодов.*

Обобщение конструкции Хаффмана на q-ичные коды (с кодовым алфавитом $J_q = \{0, 1, \ldots, q-1\}$) проводится следующим образом: вместо объединения двух символов $m-1$, $m \in I_m$, имеющих наименьшую вероятность, мы объединяем q из них (тоже с наименьшей вероятностью), повторяя предыдущие рассуждения. Фактически оригинальная работа Хаффмана (1952 г.) была посвящена общему алфавиту кодера. Существуют многочисленные модификации кода Хаффмана, учитывающие разную стоимость кодирования (где некоторые символы $j \in J_q$ более дорогостоящие, чем другие) и другие факторы. Мы не будем обсуждать их в этой книге.

Дэвид Хаффман умер 7 октября 1999 г. в городе Санта-Круз, Калифорния, в возрасте 74 лет. Он был не только блестящим ученым, но и яркой

личностью. Легенда говорит, что он изобрёл свой метод кодирования в 1951 г. при написании курсовой работы (часть экзамена в Массачусетском технологическом институте), поставленной перед ним его руководителем, профессором Робертом Фано (который в то время был ближайшим соратником Шеннона). Фано (род. в 1917 г.) тоже оставил заметный след в теории информации. Его имя не однажды появится на страницах нашей книги (неравенство Фано и обобщённое неравенство Фано). Он родился в известной математической семье: его отец Джино Фано был выдающимся членом итальянской школы алгебраической геометрии (ведущая группа в мире в этой области в первой половине XX века), а его старший брат Уго Фано внёс основополагающий вклад в теоретическую физику.

Пример 1.1.16. Недостаток кодера Хаффмана состоит в том, что длина кодового слова является довольно сложной функцией вероятностей символов $p(1), \ldots, p(m)$. Однако нетрудно получить некоторые оценки. Предположим, что $p(1) \geqslant p(2) \geqslant \ldots \geqslant p(m)$. Докажите, что в любом двоичном коде Хаффмана

1) если $p(1) < 1/3$, то при $m > 2$ буква 1 должна быть закодирована кодовым словом, длины не меньше 2,

2) если $p(1) > 2/5$, то длина кодового слова, соответствующего 1, должна равняться 1.

Решение. 1. Возможны два случая: буква 1 а) объединилась с другими буквами раньше последнего шага при построении кода Хаффмана и б) не объединялась. В случае а) $s(1) \geqslant 2$. В случае б) у нас на третьем с конца шаге алгоритма есть символы 1, b и b' и верхняя часть дерева Хаффмана устроена, как на рис. 1.2 а, с $0 \leqslant p(b)$, $p(b') \leqslant 1 - p(1)$ и $p(b) + p(b') = 1 - p(1)$. Но тогда $\max[p(b), p(b')] > 1/3$, и поэтому $p(1)$ должна быть объединена с $\min[p(b), p(b')]$. Значит, рис. 1.2 а невозможен, и длина кодового слова буквы 1 не меньше 2.

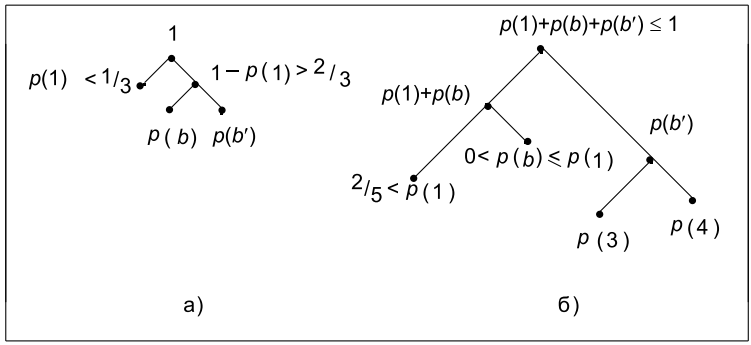


Рис. 1.2

Эта граница является точной, поскольку оба кода

$$\{0,\ 01,\ 110,\ 111\} \quad \text{и} \quad \{00,\ 01,\ 10,\ 11\}$$

являются двоичными кодами Хаффмана для распределения вероятностей 1/3, 1/3, 1/4, 1/12.

2. Пусть теперь $p(1) > 2/5$, а длина кодового слова в коде Хаффмана, соответствующего 1, не меньше 2. Тогда при построении двоичного дерева буква 1 объединялась на каком-то шаге, кроме последнего, с другими буквами. Значит, на каком-то подходящем шаге у нас были символы 1, b и b' с возможным распределением вероятностей

$$\text{А)}\ p(b') \geqslant p(1) > 2/5, \quad \text{Б)}\ p(b') \geqslant p(b),$$
$$\text{В)}\ p(1) + p(b) + p(b') \leqslant 1 \quad \text{и} \quad \text{Г)}\ p(1),\ p(b) \geqslant \frac{1}{2}p(b').$$

Действительно, если, скажем, $p(b) < p(b')/2$, то b должно быть отобрано для объединения вместо $p(3)$ или $p(4)$, объединение которых давало $p(b')$. Ввиду неравенства Г) имеем $p(b) > 1/5$, что делает случай одновременного выполнения А, Б и В невозможным.

Тогда часть дерева Хаффмана над $p(1)$ устроена, как на рис. 1.2 б, причем $p(3) + p(4) = p(b')$ и $p(1) + p(b') + p(b) \leqslant 1$. Запишем

$$p(1) = 2/5 + \varepsilon, \quad p(b') = 2/5 + \varepsilon + \delta, \quad p(b) = 2/5 + \varepsilon + \delta - \eta,$$

с $\varepsilon > 0$, $\delta,\ \eta \geqslant 0$. Итак,

$$p(1) + p(b') + p(b) = 6/5 + 3\varepsilon + 2\delta - \eta \leqslant 1, \quad \text{и} \quad \eta \geqslant 1/5 + 3\varepsilon + 2\delta.$$

Отсюда получаем

$$p(b) \leqslant 1/5 - 2\varepsilon - \delta < 1/5.$$

Однако так как

$$\max\{p(3),\ p(4)\} \geqslant p(b')/2 \geqslant p(1)/2 > 1/5,$$

вероятность $p(b)$ должна быть объединена с $\min[p(3),\ p(4)]$, т. е. диаграмма, изображённая на рис. 1.2 б, невозможна. Следовательно, длина кодового слова, соответствующего 1, $s(1) = 1$. □

Пример 1.1.17. Предположим, что буквы $i_1, \ldots, i_5$ генерируются с вероятностями 0,45, 0,25, 0,2, 0,05, 0,05. Вычислите математическое ожидание длины кодового слова для кодов Шеннона—Фано и Хаффмана. Проиллюстрируйте оба метода выписыванием декодируемых двоичных кодировок в каждом случае.

Решение. В обоих случаях $q = 2$, и для кода Шеннона—Фано имеем

$p(i)$	$-\lceil \log_2 p(i) \rceil$	кодовое слово
0,45	2	00
0,25	2	01
0,2	3	100
0,05	5	11100
0,05	5	11111

$\mathsf{E}S = 0{,}9 + 0{,}5 + 0{,}6 + 0{,}25 + 0{,}25 = 2{,}5$, а для кода Хаффмана

$p(i)$	кодовое слово
0,45	1
0,25	01
0,2	000
0,05	0010
0,05	0011

$\mathsf{E}S = 0{,}45 + 0{,}5 + 0{,}6 + 0{,}2 + 0{,}2 = 1{,}95$. □

Пример 1.1.18. Вообще говоря, код Шеннона—Фано не оптимален. Однако он «не намного» хуже, чем код Хаффмана. Пусть S_{SF} — длина кодового слова в коде Шеннона—Фано. Докажите, что для любого $r = 1, 2, \ldots$ и любого декодируемого кода f^* с длиной кодового слова S^* выполняется неравенство

$$\mathsf{P}(S^* \leqslant S_{\mathrm{SF}} - r) \leqslant q^{1-r}.$$

Решение. Запишем $\mathsf{P}(S^* \leqslant S_{\mathrm{SF}} - r) = \sum\limits_{\substack{i \in I: \\ S^*(i) \leqslant S_{\mathrm{SF}}(i) - r}} p(i)$. Заметим, что $S_{\mathrm{SF}}(i) < -\log_q p(i) + 1$, поэтому последняя сумма не превосходит $\sum\limits_{\substack{i \in I: \\ S^*(i) \leqslant -\log_q p(i) + 1 - r}} p(i)$, что, в свою очередь, равно $\sum\limits_{\substack{i \in I: \\ S^*(i) - 1 + r \leqslant -\log_q p(i)}} p(i) = \sum\limits_{\substack{i \in I: \\ p(i) \leqslant q^{-S^*(i)+1-r}}} p(i) \leqslant \sum\limits_{i \in I} q^{-S^*(i)+1-r} = q^{1-r} \sum\limits_{i \in I} q^{-S^*(i)} \leqslant q^{1-r}$. Последний переход осуществлён по неравенству Крафта. □

В современной практике принято вместо кодирования каждой отдельной буквы $u \in I$ разбивать исходное сообщение источника на «сегменты», или «блоки», фиксированной длины n и кодировать их как буквы. Это, очевидно, увеличивает количество букв в алфавите источника: все возможные блоки образуют прямое произведение $I^{\times n} = \underbrace{I \times \ldots \times I}_{n}$. Но нам важна только энтропия распределения вероятностей блоков в типичном

сообщении:

$$h_q^{(n)} = -\sum_{i_1,\dots,i_n} \mathsf{P}(U_1 = i_1, \dots, U_n = i_n) \log_q \mathsf{P}(U_1 = i_1, \dots, U_n = i_n). \quad (1.1.14)$$

(Очевидно, нам нужно знать совместное распределение последовательно генерируемых букв.) Обозначим через $S(n)$ случайную длину кодового слова в блочном коде. Минимальная средняя длина кодового слова на букву источника определяется как $e_n := \min \frac{1}{n} \mathsf{E}S(n)$; по теореме Шеннона 1.1.10 имеем

$$\frac{h_q^{(n)}}{n} \leqslant e_n \leqslant \frac{h_q^{(n)}}{n} + \frac{1}{n}. \quad (1.1.15)$$

Отсюда при больших n получаем $e_n \sim h_q^{(n)}/n$.

Пример 1.1.19. Для источника Бернулли, генерирующего букву i с вероятностью $p(i)$ (ср. пример 1.1.2), из формулы (1.1.14) получаем

$$h_q^{(n)} = -\sum_{i_1,\dots,i_n} p(i_1)\dots p(i_n) \log_q p(i_1)\dots p(i_n) = \\ = -\sum_{j=1}^{n} \sum_{i_1,\dots,i_n} p(i_1)\dots p(i_n) \log_q p(i_j) = nh_q, \quad (1.1.16)$$

где $h_q = -\sum\limits_i p(i) \log_q p(i)$. Здесь $e_n \sim h_q$. Таким образом, при больших n минимальная средняя длина кодового слова на букву источника в блочном коде в конце концов достигает нижней границы из неравенства (1.1.11) и, следовательно, не превышает $\min \mathsf{E}S$ — минимальной средней длины кодового слова для побуквенного кодирования. Эффект блочного кодирования может быть значительно бóльшим в ситуации, когда последовательные буквы источника зависимы. Во многих случаях $h_q^{(n)} \ll nh_q$, т. е. $e_n \ll h_q$. В этом и заключается сжатие данных. □

Следовательно, статистика длинных строк становится важным свойством источника.

Вообще говоря, строки $\mathbf{u}^{(n)} = u_1 \dots u_n$ длины n «замащивают» декартову степень $I^{\times n}$; общее число таких строк составляет m^n, и для кодирования возможных строк нам потребуется $m^n = 2^{n \log m}$ разных кодовых слов. Если кодовые слова имеют фиксированную длину (что гарантирует свободу от префиксов), то эта длина лежит между $\lfloor n \log m \rfloor$, и $\lceil n \log m \rceil$, а скорость кодирования (для больших n) примерно равна $\log m$ бит/буква источника. Но если некоторые строки редко встречаются, мы можем игнорировать их, уменьшая количество используемых слов. Это приводит к следующим определениям.

Определение 1.1.20. Говорят, что источник надёжно кодируется со скоростью $R > 0$, если для любого n можно найти такое подмножество $A_n \subset I^{\times n}$, что

$$\#A_n \leqslant 2^{nR} \quad \text{и} \quad \lim_{n\to\infty} \mathsf{P}(\mathbf{U}^{(n)} \in A_n) = 1. \tag{1.1.17}$$

Иначе говоря, можно кодировать сообщения со скоростью R с незначительными ошибками на длинных строках источника. □

Определение 1.1.21. *Скоростью передачи информации* H данного источника называется точная нижняя граница его надёжных скоростей кодирования

$$H = \inf\{R\colon R \text{ — надёжная скорость кодирования}\}. \tag{1.1.18}$$

□

Теорема 1.1.22. *Скорость передачи информации источника с алфавитом* I_m *удовлетворяет неравенству*

$$0 \leqslant H \leqslant \log m. \tag{1.1.19}$$

Обе границы достижимы.

Доказательство. Л. ч. неравенства тривиальна. Она достигается на вырожденном источнике (см. пример 1.1.2); здесь A_n содержит не более m постоянных строчек, мощность которых в итоге ограничивается числом 2^{nR} для любого $R > 0$. С другой стороны, $\#I^{\times n} = m^n = 2^{n\log m}$, что даёт п. ч. неравенства. Она достигается на источнике, буквы которого — н. о. р. с. в. с $p(u) = 1/m$: в этом случае $\mathsf{P}(A_n) = (1/m^n)\#A_n$, что стремится к нулю, когда $\#A_n \leqslant 2^{nR}$ и $R < \log m$. □

Пример 1.1.23. а) Для английского телеграфа $m = 27 \simeq 2^{4{,}76}$, т. е. $H \leqslant 4{,}76$. К счастью, $H \ll 4{,}76$, что делает возможным: (i) сжатие данных, (ii) корректировку ошибок, (iii) декодирование сообщений, (iv) кроссворды.

Точного значения H для английского телеграфа (не говоря уже о литературном английском языке) никто не знает: точное вычисление этого параметра — сложная задача. Тем не менее, современные теоретические инструменты и вычислительные мощности позволяют оценить скорость передачи информации определённого (длинного) текста в предположении, что он происходит из источника, который обладает изрядным количеством случайности и однородности (см. раздел 6.3 в книге [CT].) □

Некоторые результаты численного анализа можно найти в работе [SG], анализирующей три документа: а) собрание сочинений Шекспира, б) смешанный текст из различных газет и в) библию короля Джеймса I, считающуюся эталоном в англоязычных странах. Тексты были освобождены от знаков препинания и пробелов между словами. Тексты а) и б) дают значения 1,7 и 1,25 соответственно (что является весьма лестным для

современной журналистики). В случае в) результаты были неубедительными; по-видимому, вышеуказанные предположения не подходят в данном случае. (Например, генеалогическое перечисления Книги Бытия трудно сравнить с философскими дискуссиями посланий Апостола Павла, поэтому очевидно, до однородности источнику далеко.)

Ещё более сложной задачей является сравнение различных языков: какой из них может быть более подходящим для международной связи? Кроме того, было бы интересно повторить описанный выше эксперимент с сочинениями Толстого или Достоевского.

В качестве иллюстрации мы приводим оригинальную таблицу Сэмюэля Морзе (1791–1872), создателя азбуки Морзе, дающую представление о частоте встречаемости различных букв в телеграфном английском языке, в котором доминирует относительно небольшое число общих слов.

$$\begin{pmatrix} E & T & A & I & N & O & S & H & R \\ 12000 & 9000 & 8000 & 8000 & 8000 & 8000 & 8000 & 6400 & 6200 \\ D & L & U & C & M & F & W & Y & G \\ 4400 & 4000 & 3400 & 3000 & 3000 & 2500 & 2000 & 2000 & 1700 \\ P & B & V & K & Q & J & X & Z & \\ 1700 & 1600 & 1200 & 800 & 500 & 400 & 400 & 200 & \end{pmatrix}.$$

б) Подобная идея была применена к десятичной и двоичной записям данного числа. Возьмём, например, число π. Если скорость передачи информации для двоичной его записи приближается к 1 (что является скоростью передачи информации случайной последовательности), мы можем подумать, что π ведёт себя как совершенно случайное число; в противном случае мы могли бы вообразить, что π было специально подобранным числом. Аналогичный вопрос можно задать и о числах e, $\sqrt{2}$ или константе Эйлера—Маскерони $\gamma = \lim\limits_{N\to\infty}\left(\sum\limits_{1\leqslant n\leqslant N}\frac{1}{n} - \ln N\right)$. (Открытая часть одной из проблем Гильберта — доказать или опровергнуть трансцендентность числа γ; нетрудно доказать, что трансцендентные числа получаются с вероятностью 1 при последовательном генерировании символов источником Бернулли.) Как показывают результаты численных экспериментов, для количества цифр $N \sim 500\,000$ все упомянутые выше числа демонстрируют тот же шаблон поведения, что и совершенно случайные числа, см. [BS]. В § 1.3 мы вычислим скорость передачи информации для источников Бернулли и Маркова. Мы заканчиваем этот параграф следующим простым, но фундаментальным фактом.

Теорема 1.1.24 (неравенство Гиббса (ср. том 2, с. 480)). *Пусть* $\{p(i)\}$ *и* $\{p'(i)\}$ *— два распределения вероятностей* (*на конечном или счёт-*

ном множестве I). Тогда для любого $b > 1$ выполняется неравенство

$$\sum_i p(i) \log_b \frac{p'(i)}{p(i)} \leqslant 0, \quad \textit{т. е.} \quad -\sum_i p(i) \log_b p(i) \leqslant -\sum_i p(i) \log_b p'(i), \tag{1.1.20}$$

и равенство достигается тогда и только тогда, когда $p(i) = p'(i)$, $1 \leqslant i \leqslant m$.

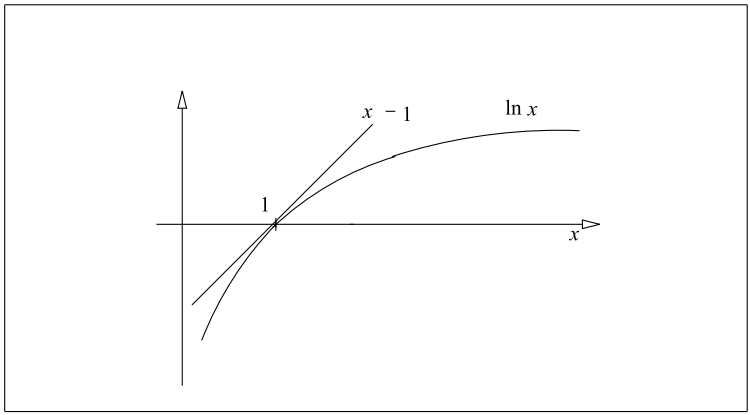


Рис. 1.3

Доказательство. Неравенство

$$\log_b x \leqslant \frac{x-1}{\ln b}$$

справедливо при каждом $x > 0$ и становится равенством тогда и только тогда, когда $x = 1$. Положив $I' = \Big(i\colon p(i) > 0\Big)$, получим

$$\sum_i p(i) \log_b \frac{p'(i)}{p(i)} = \sum_{i \in I'} p(i) \log_b \frac{p'(i)}{p(i)} \leqslant \frac{1}{\ln b} \sum_{i \in I'} p(i) \Big(\frac{p'(i)}{p(i)} - 1 \Big) =$$

$$= \frac{1}{\ln b} \left(\sum_{i \in I'} p'(i) - \sum_{i \in I'} p(i) \right) = \frac{1}{\ln b} \left(\sum_{i \in I'} p'(i) - 1 \right) \leqslant 0.$$

Для равенства нам нужно, чтобы выполнялись условия а) $\sum\limits_{i \in I'} p'(i) = 1$, т. е. $p'(i) = 0$, когда $p(i) = 0$ и б) $p'(i)/p(i) = 1$ при $i \in I'$. □

§ 1.2. Понятие энтропии

Только энтропия приходит легко.

Антон Чехов (1860–1904),
русский писатель и драматург

Этот параграф полностью посвящён свойствам энтропии. Для простоты, мы работаем с двоичной энтропией, где логарифмы берутся по основанию 2 и опускаем индекс 2 в обозначении h_2. Мы начнём с формального повторения основных определений, расставив несколько другие акценты.

Определение 1.2.1. Для данного события A с вероятностью $p(A)$, информация, полученная в результате того, что A произошло, определяется как

$$i(A) = -\log p(A).$$

Далее, пусть X — с. в., принимающая конечное число различных значений $\{x_1, \ldots, x_m\}$ с вероятностями $p_i = p_X(x_i) = \mathsf{P}(X = x_i)$. *Двоичная энтропия* $h(X)$ определяется как математическое ожидание количества информации, полученного из наблюдений X:

$$h(X) = -\sum_{x_i} p_X(x_i) \log_X p_X(x_i) = -\sum_i p_i \log p_i = \mathsf{E}[-\log p_X(X)]. \quad (1.2.1)$$

(Ввиду соглашения $0 \cdot \log 0 = 0$, сумму можно ограничить теми x_i, для которых $p_X(x_i) > 0$.) □

Иногда полезен альтернативный взгляд: $i(A)$ представляет собой количество информации, необходимое для идентификации события A, и $h(X)$ означает среднее количество информации, необходимой для идентификации с. в. X. Ясно, что энтропия $h(X)$ зависит от распределения вероятностей, но не от значений $x_1, \ldots, x_m$: $h(X) = h(p_1, \ldots, p_m)$. При $m = 2$ (двухточечное распределение вероятностей) энтропию удобно рассматривать как функцию $\eta(p) (= \eta_2(p))$ одной переменной $p \in [0, 1]$:

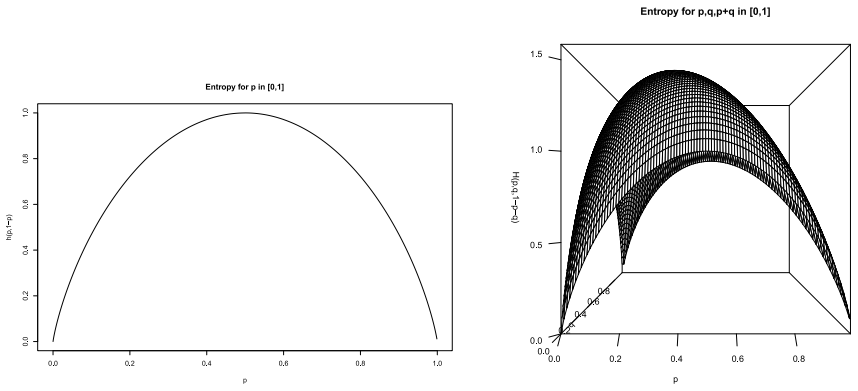
$$\eta(p) = -p \log p - (1 - p) \log(1 - p). \quad (1.2.2а)$$

График функции $\eta(p)$ изображён на рис. 1.4а. Заметим, что эта функция выпукла вверх, так как

$$\frac{\mathrm{d}^2}{\mathrm{d}p^2}\eta(p) = -\log e/[p(1 - p)] < 0. \quad (1.2.2б)$$

График энтропии трёхточечного распределения вероятностей

$$\eta_3(p, q) = -p \log p - q \log q - (1 - p - q) \log(1 - p - q)$$



а б

Рис. 1.4

как функции переменных p, $q \in [0,\ 1]$, $p + q \leqslant 1$, представлен на рис 1.4 б. На нём отчётливо видно, что имеет место свойство выпуклости.

Из определения 1.2.1 вытекает, что для независимых событий A_1 и A_2

$$i(A_1 \cap A_2) = i(A_1) + i(A_2). \tag{1.2.2в}$$

и $i(A) = 1$ для такого события A, что $p(A) = 1/2$.

Мотивировка определения 1.2.1 состоит в том, что любая функция $i^*(A)$, которая зависит от вероятности $p(A)$ (т. е. $i^*(A) = i^*(A')$, если $p(A) = p(A')$), непрерывна относительно $p(A)$ и удовлетворяет условию (1.2.2в), совпадает с $i(A)$ (аксиоматическое определение энтропии см. в примере 1.2.25 ниже).

Определение 1.2.2. *Совместная энтропия* $h(X,\ Y)$ пары с. в. X и Y со значениями x_i и y_j определяется по формуле

$$h(X,\ Y) = -\sum_{x_i, y_j} p_{X,Y}(x_i,\ y_j) \log p_{X,Y}(x_i,\ y_j) = \mathsf{E}[-\log p_{X,Y}(X,\ Y)], \tag{1.2.3}$$

где $p_{X,Y}(x_i,\ y_j) = \mathsf{P}(X = x_i,\ Y = y_j)$ — совместное распределение вероятностей. Иначе говоря, $h(X,\ Y)$ — энтропия случайного вектора $(X,\ Y)$ со значениями $(x_i,\ y_j)$.

Условная энтропия $h(X \,|\, Y)$ с. в. X при данном Y определяется как ожидаемое количество информации от наблюдения X при условии, что значение Y известно:

$$h(X \,|\, Y) = -\sum_{x_i, y_j} p_{X,Y}(x_i,\ y_j) \log p_{X \,|\, Y}(x_i \,|\, y_j) = \mathsf{E}[-\log p_{X \,|\, Y}(X \,|\, Y)]. \tag{1.2.4}$$

Здесь $p_{X,Y}(x_i,\, y_j)$ — совместная вероятность $\mathsf{P}(X = x_i,\, Y = y_j)$ и $p_{X\,|\,Y}(x_i\,|\,y_j)$ — условная вероятность $\mathsf{P}(X = x_i\,|\,Y = y_j)$. Ясно, что из формул (1.2.3) и (1.2.4) следует равенство

$$h(X\,|\,Y) = h(X,\, Y) - h(Y). \tag{1.2.5}$$

Заметим, что в общем случае $h(X\,|\,Y) \neq h(Y\,|\,X)$.

Пусть X и Y — с. в. со значениями из I, причём $p_Y(x) > 0$ для всех $x \in I$. *Относительная энтропия* $h(X\,||\,Y)$ (или энтропия X относительно Y, или расстояние Кульбака—Лейблера $D(p(X)\,||\,p(Y))$) определяется как

$$h(X\,||\,Y) = \sum_x p_X(x) \log \frac{p_X(x)}{p_Y(x)} = \mathsf{E}_X\Big[-\log \frac{p_Y(x)}{p_X(x)}\Big], \tag{1.2.6}$$

где $p_X(x) = \mathsf{P}(X = x)$ и $p_Y(x) = \mathsf{P}(Y = x)$, $x \in I$. □

Вытекающие из определения свойства энтропии перечислены ниже:

Теорема 1.2.3. *а) Если с. в. X принимает не более чем m значений, то*

$$0 \leqslant h(X) \leqslant \log m. \tag{1.2.7}$$

Левое неравенство превращается в равенство тогда и только тогда, когда X принимает единственное значение, а правое неравенство становится равенством тогда и только тогда, когда X принимает m значений с равными вероятностями.

б) Совместная энтропия удовлетворяет неравенству:

$$h(X,\, Y) \leqslant h(X) + h(Y), \tag{1.2.8}$$

которое становится равенством тогда и только тогда, когда X и Y независимы, т. е. $\mathsf{P}(X = x,\, Y = y) = \mathsf{P}(X = x)\,\mathsf{P}(Y = y)\ \forall\, x,\, y \in I$.

в) Относительная энтропия всегда неотрицательна:

$$h(X\,||\,Y) \geqslant 0 \tag{1.2.9}$$

и равна нулю тогда и только тогда, когда X и Y одинаково распределены: $p_X(x) \equiv p_Y(x)\ \forall\, x \in I$.

Доказательство. Утверждение в) эквивалентно неравенству Гиббса из теоремы 1.1.24. Далее, а) следует из в), в котором $\{p(i)\}$ — распределение с. в. X и $p'(i) \equiv 1/m$, $1 \leqslant i \leqslant m$. Аналогично б) следует из в), в котором i обозначает пару $(i_1,\, i_2)$ значений X и Y, $p(i) = p_{X,Y}(i_1,\, i_2)$ — совместное распределение с. в. X и Y, $p'(i) = p_X(i_1)p_Y(i_2)$ обозначает

произведение маргинальных распределений. С формальной точки зрения

$$\text{а)}\quad h(X) = -\sum_i p(i)\log p(i) \leqslant -\sum_i p(i)\log m = \log m,$$

$$\text{б)}\quad h(X,\,Y) = -\sum_{i_1,i_2} p_{X,Y}(i_1,\,i_2)\log p_{X,Y}(i_1,\,i_2) \leqslant$$

$$\leqslant -\sum_{i_1,i_2} p_{X,Y}(i_1,\,i_2)\times\log(p_X(i_1)p_Y(i_2)) =$$

$$= -\sum_{i_1} p_X(i_1)\log p_X(i_1) - \sum_{i_2} p_Y(i_2)\log p_Y(i_2) = h(X) + h(Y).$$

Мы здесь воспользовались тождествами $\sum_{i_2} p_{X,Y}(i_1,\,i_2) = p_X(i_1)$, $\sum_{i_1} p_{X,Y}(i_1,\,i_2) = p_Y(i_2)$. □

Пример 1.2.4. а) Покажите, что геометрическая с. в. Y с $p_j = \mathsf{P}(Y = j) = (1-p)p^j$, $j = 0,\,1,\,2,\,\ldots$, обладает максимальной энтропией среди всех с. в., принимающих значения в $\mathbb{Z}_+ = \{0,\,1,\,2,\,\ldots\}$ с тем же самым средним.

б) Пусть Z — с. в., принимающая значения в конечном множестве K и f — вещественнозначная функция $f\colon K \to \mathbb{R}$ с $f_* = \min[f(k)\colon k \in K]$ и $f^* = \max\{f(k)\colon k \in K\}$. Положим $E(f) = \sum_{k\in K} f(k)/(\#K)$ и рассмотрим задачу максимизации энтропии $h(Z)$ с. в. Z, подчинённой условию

$$\mathsf{E}f(Z) \leqslant \alpha. \tag{1.2.10}$$

Покажите, что (bi) если $f^* \geqslant \alpha \geqslant E(f)$, то решение задачи максимизации даёт равномерное на K распределение $P(Z = k) = 1/(\#K)$, $k \in K$, и (bii) если $f^* \leqslant \alpha < E(f)$ и f отлична от константы, то распределение вероятностей, дающее решение задачи максимизации, задаётся формулой:

$$\mathsf{P}(Z = k) = p_k = e^{\lambda f(k)}\Big/\sum_i e^{\lambda f(i)}, \quad k \in K, \tag{1.2.11}$$

где $\lambda = \lambda(\alpha) < 0$ выбирается так, что

$$\sum_k p_k f(k) = \alpha. \tag{1.2.12}$$

Более того, допустим, что Z принимает счётное число значений, но $f \geqslant 0$ и для данного такое α найдётся $\lambda < 0$, что $\sum_i e^{\lambda f(i)} < \infty$ и $\sum_k p_k f(k) = \alpha$, где p_k определены формулой (1.2.11). Тогда (biii) распределение из формулы (1.2.11) обладает максимальной энтропией $h(Z)$ при условии (1.2.10). Выведите утверждение а) из (biii).

в) Докажите, что $h_Y(X) \geqslant 0$, причём равенство достигается тогда и только тогда, когда $\mathsf{P}(X = x) = \mathsf{P}(Y = x)$ для всех x. Рассматривая геометрическую с. в. Y, распределённую на $\mathbb{Z}_+$ с подходящим образом выбранным параметром, покажите, что если среднее $\mathsf{E}X = \mu$ конечно, то

$$h(X) \leqslant (\mu + 1)\log(\mu + 1) - \mu \log \mu, \tag{1.2.13}$$

а равенство достигается тогда и только тогда, когда X — геометрическая с. в.

Решение. а) Согласно неравенству Гиббса для любого распределения вероятностей $(q_0, q_1, \ldots)$ со средним $\sum_{i \geqslant 0} i q_i \leqslant \mu$ имеем

$$\begin{aligned} h(q) &= -\sum_i q_i \log q_i \leqslant -\sum_i q_i \log p_i = \\ &= -\sum_i q_i (\log(1-p) + i \log p) \leqslant -\log(1-p) - \mu \log p = h(Y), \end{aligned}$$

где $\mu = p/(1-p)$. Равенство достигается тогда и только тогда, когда q — геометрическое распределение со средним μ.

б) Прежде всего заметим, что равномерное распределение с $p_k = 1/(\#K)$, которое даёт «глобальный» максимум $h(Z)$, получается из формулы (1.2.11) при $\lambda = 0$. В части (bi), это распределение удовлетворяет условию (1.2.10) и, следовательно, максимизирует $h(Z)$ при таком ограничении. Переходя к (bii), положим $p_k^* = e^{\lambda f(k)} \Big/ \sum_i e^{\lambda f(i)}$, $k \in K$, где λ выбирается так, что $\mathsf{E}^* f(Z) = \sum_k p_k^* f(k) = \alpha$. Пусть $q = \{q_k\}$ — произвольное распределение вероятностей, подчиняющееся условию $\mathsf{E}_q f = \sum_k q_k f(k) \leqslant \alpha$. Далее заметим, что среднее значение (1.2.12), вычисленное для распределения (1.2.11), представляет собой неубывающую функцию переменной λ. Действительно, производная

$$\frac{\mathrm{d}\alpha}{\mathrm{d}\lambda} = \frac{\sum_k (f(k))^2 e^{\lambda f(k)}}{\sum_i e^{\lambda f(i)}} - \frac{\left(\sum_k f(k) e^{\lambda f(k)}\right)^2}{\left(\sum_i e^{\lambda f(i)}\right)^2} = \mathsf{E}(f(Z)^2) - (\mathsf{E}f(Z))^2$$

положительна (это выражение дает дисперсию с. в. $f(Z)$); следовательно, если $f \not\equiv 0$, п. ч. больше 0. Итак, если $f \not\equiv \mathrm{const}$ (т. е. $f_* < E(f) < f^*$), для любого $\alpha \in [f_*, f^*]$ найдётся ровно одно распределение вероятностей вида (1.2.11), удовлетворяющее (1.2.12), и для $f_* \leqslant \alpha < E(f)$ соответствующее $\lambda(\alpha) < 0$.

Далее воспользуемся тем фактом, что расстояние Кульбака—Лейблера $D(q\,||\,p^*) = \sum\limits_k q_k \log(q_k/p_k^*) \geqslant 0$ (неравенство Гиббса) с учётом неравенств: $\sum\limits_k q_k f(k) \leqslant \alpha$ и $\lambda < 0$ и получим

$$\begin{aligned} h(q) &= -\sum_k q_k \log q_k = -D(q\,||\,p^*) - \sum_k q_k \log p_k^* \leqslant \\ &\leqslant -\sum_k q_k \log p_k^* = -\sum_k q_k \Big(-\log \sum_i e^{\lambda f(i)} + \lambda f(k) \Big) \leqslant \\ &\leqslant -\sum_k q_k \Big(-\log \sum_i e^{\lambda f(i)} \Big) - \lambda\alpha = \\ &= -\sum_k p_k^* \Big(-\log \sum_i e^{\lambda f(i)} + \lambda f(k) \Big) = -\sum_k p_k^* \log p_k^* = h(p^*). \end{aligned}$$

Для доказательства части (biii) заметим, что предыдущие аргументы остаются в силе и для счётного множества K при том условии, что значение $\lambda(\alpha)$, определённое формулой (1.2.12), меньше 0.

в) По неравенству Гиббса $h_Y(X) \geqslant 0$. Далее, опираясь на часть б), положим $f(k) = k$, $\alpha = \mu$ и $\lambda = \ln q$. Распределение с максимальной энтропией можно записать как $p_j^* = (1-p)p^j$, $j = 0, 1, 2, \ldots$, где $\sum\limits_k k p_k^* = \mu$, или $\mu = p/(1-p)$. Энтропия такого распределения равна

$$\begin{aligned} h(p^*) &= -\sum_j (1-p)p^j \log((1-p)p^j) = \\ &= -\frac{p}{1-p}\log p - \log(1-p) = (\mu+1)\log(\mu+1) - \mu\log\mu, \end{aligned}$$

где $\mu = p/(1-p)$.

В качестве альтернативы

$$\begin{aligned} 0 \leqslant h_Y(X) &= \sum_i p(i) \log \frac{p(i)}{(1-p)p^i} = \\ &= -h(X) - \log(1-p)\sum_i p(i) - (\log p)\Big(\sum_i i p(i)\Big) = \\ &= -h(X) - \log(1-p) - \mu\log p. \end{aligned}$$

Оптимальный выбор p будет $p = \mu/(\mu+1)$. Тогда

$$h(X) \leqslant -\log\frac{1}{\mu+1} - \mu\log\frac{\mu}{\mu+1} = (\mu+1)\log(\mu+1) - \mu\log\mu.$$

П. ч. неравенства — это энтропия $h(Y)$ геометрической с. в. Y. Неравенство становится равенством, если и только если $X \sim Y$, т. е. X тоже геометрическая с. в. □

Приведём простое, но полезное следствие.

Лемма 1.2.5 (неравенства группировки данных[2]). *Для любых* $q_1, q_2 \geqslant 0$, *удовлетворяющих условию* $q_1 + q_2 > 0$ *выполнены неравенства*:

$$-(q_1+q_2)\log(q_1+q_2) \leqslant -q_1\log q_1 - q_2\log q_2 \leqslant -(q_1+q_2)\log\frac{q_1+q_2}{2}. \tag{1.2.14}$$

Нижняя граница неравенства достигается тогда и только тогда, когда $q_1 q_2 = 0$ (*т. е. одно из* q_i *равно* 0). *Верхняя граница достигается тогда и только тогда, когда* $q_1 = q_2$.

Доказательство. Действительно, неравенство (1.2.14) равносильно такому:

$$0 \leqslant \eta\Big(\frac{q_1}{q_1+q_2}\Big) \leqslant \log 2 (= 1). \qquad \square$$

По лемме 1.2.4 «склеивание» значений с. в. может уменьшить соответствующий вклад в энтропию. С другой стороны, «перераспределение» вероятностей, делающее с. в. равновероятными, увеличивает этот вклад. Непосредственное следствие из леммы 1.2.4 — следующая теорема.

Теорема 1.2.6. *Предположим, что дискретная случайная величина* X *является функцией от дискретной случайной величины* Y: $X = \varphi(Y)$. *Тогда*

$$h(X) \leqslant h(Y), \tag{1.2.15}$$

причём равенство достигается тогда и только тогда, когда функция φ *обратима*.

Доказательство. В самом деле, если функция $\varphi(X)$ обратима, то распределения с. в. X и Y отличаются лишь порядком вероятностей, что не меняет энтропию. Если φ «склеивает» некоторые значения y_i, то нужно несколько раз воспользоваться л. ч. неравенства группировки данных. □

Информация — оборотная сторона вероятности.

Клод Шеннон (1916–2001),
американский электротехник и математик

Пример 1.2.7. Пусть $p_1, \ldots, p_n$ — распределение вероятностей с $p^* = \max\{p_i\}$. Выведите следующие оценки для энтропии $h = -\sum_i p_i \log p_i$:

(i) $h \geqslant -p^*\log p^* - (1-p^*)\log(1-p^*) = \eta(p^*)$;

[2] The pooling inequalities.

(ii) $h \geqslant -\log p^*$;

(iii) $h \geqslant 2(1-p^*)$.

Решение. (i) следует из неравенств группировки данных, а (ii) верно ввиду того, что

$$h \geqslant -\sum_i p_i \log p^* = -\log p^*.$$

Для проверки (iii), предположим сначала, что $p^* \geqslant 1/2$. Поскольку функция $p \mapsto \eta(p)$, $0 \leqslant p \leqslant 1$, выпукла вверх (см. формулу (1.2.2б)), её график на отрезке $[1/2,\ 1]$ расположен выше прямой $x \mapsto 2(1-p)$. Значит, по (i)

$$h \geqslant \eta(p^*) \geqslant 2(1-p^*). \tag{1.2.16}$$

С другой стороны, если $p^* \leqslant 1/2$, надо воспользоваться (ii):

$$h \geqslant -\log p^*$$

и применить неравенство $-\log p \geqslant 2(1-p)$ при $0 \leqslant p \leqslant 1/2$. □

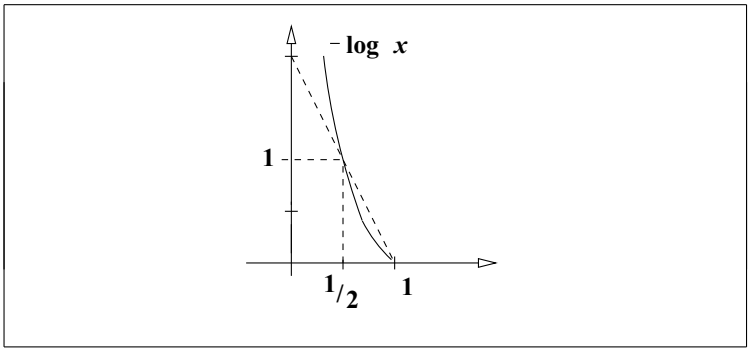


Рис. 1.5

Теорема 1.2.8 (неравенство Фано). *Предположим, что случайная величина X принимает $m > 1$ значений и одно из них с вероятностью $1-\varepsilon$. Тогда*

$$h(X) \leqslant \eta(\varepsilon) + \varepsilon \log(m-1), \tag{1.2.17}$$

где η — функция, определённая формулой (1.2.2а).

Доказательство. Предположим, что $p_1 = p(x_1) = 1 - \varepsilon$. Тогда

$$h(X) = h(p_1, \ldots, p_m) = -\sum_{i=1}^{m} p_i \log p_i =$$
$$= -p_1 \log p_1 - (1-p_1)\log(1-p_1) + (1-p_1)\log(1-p_1) -$$
$$- \sum_{2 \leqslant i \leqslant m} p_i \log p_i = \eta(p_1) + (1-p_1) h\Big(\frac{p_2}{1-p_1}, \ldots, \frac{p_m}{1-p_1}\Big) \quad (1.2.18)$$

Первое слагаемое в п. ч. — это $\eta(\varepsilon)$, а второе не превышает $\varepsilon \log(m-1)$. □

Определение 1.2.9. Пусть X, Y, Z — с. в.. Будем называть с. в. X и Y *условно независимыми* при данной с. в. Z, если для любых x и y и любого z, $\mathsf{P}(Z = z) > 0$, имеет место равенство

$$\mathsf{P}(X = x,\ Y = y \,|\, Z = z) = \mathsf{P}(X = x \,|\, Z = z)\, \mathsf{P}(Y = y \,|\, Z = z). \quad (1.2.19)$$

□

Для условной энтропии немедленно получается следующий результат.

Теорема 1.2.10. *а) Для любых с. в. X, Y*

$$0 \leqslant h(X \,|\, Y) \leqslant h(X), \quad (1.2.20)$$

причём левое неравенство становится равенством тогда и только тогда, когда X является функцией от Y, а правое неравенство становится равенством тогда и только тогда, когда X и Y независимы.

б) Для любых с. в. X, Y, Z выполнены неравенства

$$h(X \,|\, Y,\ Z) \leqslant h(X \,|\, Y) \leqslant h(X \,|\, \varphi(Y)); \quad (1.2.21)$$

причём левое неравенство становится равенством тогда и только тогда, когда X и Z условно независимы при данной с. в. Y, а правое неравенство становится равенством тогда и только тогда, когда X и Y условно независимы при данной с. в. $\varphi(Y)$.

Доказательство. а) Левое неравенство из (1.2.20) следует из соотношений (1.2.4), а правое слагаемое — из (1.2.5) и (1.2.10). Равенство в л. ч. (1.2.20) равносильно тому, что $h(X,\ Y) = h(Y)$; а это верно тогда и только тогда, когда отображение $(X,\ Y) \mapsto Y$ обратимо с вероятностью 1, т. е. X является функцией от Y. Равенство в п. ч. (1.2.20) равносильно тому, что $h(X,\ Y) = h(X) + h(Y)$, т. е. X и Y независимы.

б) Для левой части неравенства используем формулу, аналогичную (1.2.5)

$$h(X \,|\, Y,\ Z) = h(X,\ Z \,|\, Y) - h(Z \,|\, Y), \quad (1.2.22)$$

и неравенство, подобное (1.2.10):

$$h(X,\, Z\,|\,Y) \leqslant h(X\,|\,Y) + h(Z\,|\,Y), \tag{1.2.23}$$

которое становится равенством тогда и только тогда, когда X и Z условно независимы при данной с. в. Y. Для п. ч. воспользуемся (i) формулой, являющейся частным случаем (1.2.22): $h(X\,|\,Y,\, \varphi(Y)) = h(X,\, Y\,|\,\varphi(Y)) - h(Y\,|\,\varphi(Y))$, с учётом того, что $h(X\,|\,Y,\, \varphi(Y)) = h(X\,|\,Y)$ и (ii) неравенством, являющимся частным случаем (1.2.23): $h(X,\, Y\,|\,\varphi(Y)) \leqslant h(X\,|\,\varphi(Y)) + h(Y\,|\,\varphi(Y))$, которое становится равенством тогда и только тогда, когда X и Y условно независимы при данной с. в. $\varphi(Y)$. □

Теоремы 1.2.8 (см. выше) и 1.2.11 (ниже) показывают, как энтропия $h(X)$ и условная энтропия $h(X\,|\,Y)$ контролируют, когда X является «почти» константой (соответственно «почти» функция от Y).

Теорема 1.2.11 (обобщённое неравенство Фано). *Пусть X и Y — с. в., принимающие значения $x_1, \ldots, x_m$ и $y_1, \ldots, y_m$. Если*

$$\sum_{j=1}^{m} \mathsf{P}(X = x_j,\, Y = y_j) = 1 - \varepsilon, \tag{1.2.24}$$

то

$$h(X\,|\,Y) \leqslant \eta(\varepsilon) + \varepsilon \log(m-1), \tag{1.2.25}$$

где $\eta(\varepsilon)$ определяется формулой (1.2.2a).

Доказательство. Обозначая $\varepsilon_j = \mathsf{P}(X \neq x_j\,|\,Y = y_j)$, можно записать

$$\sum_j p_Y(y_j)\varepsilon_j = \sum_j \mathsf{P}(X \neq x_j,\, Y = y_j) = \varepsilon.$$

По определению условной энтропии и неравенству Фано, учитывая выпуклости функции $\eta(\cdot)$, получаем

$$h(X\,|\,Y) \leqslant \sum_j p_Y(y_j)(\eta(\varepsilon_j) + \varepsilon_j \log(m-1)) \leqslant$$

$$\leqslant \sum_j p_Y(y_j)\eta(\varepsilon_j) + \varepsilon \log(m-1) \leqslant \eta(\varepsilon) + \varepsilon \log(m-1). \quad \square$$

Предыдущие определения можно переформулировать и для с. в. X, принимающей счётное число значений $\{x_1, x_2, \ldots\}$, за исключением формул (1.2.7), (1.2.17) и (1.2.25).

Многие свойства энтропии, перечисленные до этого момента, распространяются и на случайные строки.

Теорема 1.2.12. *Для пары случайных строчек* $\mathbf{X}^{(n)} = X_1 \dots X_n$ *и* $\mathbf{Y}^{(n)} = Y_1 \dots Y_n$ *выполнено следующее*:

а) *совместная энтропия* $h(\mathbf{X}^{(n)}) = -\sum\limits_{\mathbf{x}^{(n)}} \mathsf{P}(\mathbf{X}^{(n)} = \mathbf{x}^{(n)}) \log \mathsf{P}(\mathbf{X}^{(n)} = \mathbf{x}^{(n)})$ *удовлетворяет неравенству*

$$h(\mathbf{X}^{(n)}) = \sum_{i=1}^{n} h(X_i \,|\, \mathbf{X}^{(i-1)}) \leqslant \sum_{i=1}^{n} h(X_i), \tag{1.2.26}$$

причём равенство достигается тогда и только тогда, когда компоненты $X_1, \dots, X_n$ *независимы*;

б) *условная энтропия* $h(\mathbf{X}^{(n)} \,|\, \mathbf{Y}^{(n)}) = -\sum\limits_{\mathbf{x}^{(n)}, \mathbf{y}^{(n)}} \mathsf{P}(\mathbf{X}^{(n)} = \mathbf{x}^{(n)}, \mathbf{Y}^{(n)} = \mathbf{y}^{(n)}) \log \mathsf{P}(\mathbf{X}^{(n)} = \mathbf{x}^{(n)} \,|\, \mathbf{Y}^{(n)} = \mathbf{y}^{(n)})$ *удовлетворяет неравенствам*

$$h(\mathbf{X}^{(n)} \,|\, \mathbf{Y}^{(n)}) \leqslant \sum_{i=1}^{n} h(X_i \,|\, \mathbf{Y}^{(n)}) \leqslant \sum_{i=1}^{n} h(X_i \,|\, Y_i), \tag{1.2.27}$$

где левое неравенство становится равенством тогда и только тогда, когда $X_1, \dots, X_n$ *условно независимы при данной с.в.* $\mathbf{Y}^{(n)}$, *а правое — тогда и только тогда, когда для каждого* $i = 1, \dots, n$, X_i *и* $\{Y_r \colon 1 \leqslant r \leqslant n,\ r \neq i\}$ *условно независимы при данной с.в.* Y_i.

Доказательство. Доказательство полностью повторяет рассуждения, использованные ранее в скалярном случае. □

Определение 1.2.13. *Взаимная информация*, или *взаимная энтропия* $I(X : Y)$, между X и Y определяется как

$$I(X : Y) := \sum_{x,y} p_{X,Y}(x, y) \log \frac{p_{X,Y}(X, Y)}{p_X(x) p_Y(y)} = \mathsf{E} \log \frac{p_{X,Y}(X, Y)}{p_X(X) p_Y(Y)} =$$
$$= h(X) + h(Y) - h(X, Y) = h(X) - h(X \,|\, Y) = h(Y) - h(Y \,|\, X). \tag{1.2.28}$$

Как можно видеть из этого определения, $I(X : Y) = I(Y : X)$. □

Интуитивно, $I(X : Y)$ измеряет количество информации о X, передаваемое Y (и наоборот). Из теоремы 1.2.10b вытекает следующий результат.

Теорема 1.2.14. *Если с.в.* $\varphi(Y)$ *— функция с.в.* Y, *то*

$$0 \leqslant I(X : \varphi(Y)) \leqslant I(X : Y); \tag{1.2.29}$$

левое неравенство становится равенством тогда и только тогда, когда X *и* $\varphi(Y)$ *независимы, а правое — тогда и только тогда, когда* X *и* Y *условно независимы при данной с.в.* $\varphi(Y)$.

Пример 1.2.15. Предположим, что две неотрицательные с.в. X и Y связаны соотношением $Y = X + N$, где N — геометрическая с.в., принимающая значения на $\mathbb{Z}_+$ и не зависящая от X. Найдите распределение

Y, максимизирующее взаимную энтропию между X и Y при условии, что $\mathsf{E}X \leqslant K$, и покажите, что это распределение можно реализовать, присваивая X нулевое значение с подходящей вероятностью и присваивая X геометрическое распределение с дополнительной вероятностью.

Решение. Поскольку $Y = X + N$ с независимыми X и N, имеем

$$I(X:Y) = h(Y) - h(Y\,|\,X) = h(Y) - h(N).$$

Кроме того, $\mathsf{E}(Y) = \mathsf{E}(X) + \mathsf{E}(N) \leqslant K + \mathsf{E}(N)$. Следовательно, если можно гарантировать, что с. в. Y имеет геометрическое распределение со средним $K + \mathsf{E}(N)$, то она даёт максимальное значение $I(X:Y)$. Чтобы проверить этот факт, выпишем уравнение на производящие функции вероятности:

$$\mathsf{E}(z^Y) = \mathsf{E}(z^X)\,\mathsf{E}(z^N), \quad z > 0,$$

где $\mathsf{E}(z^N) = (1-p)/(1-zp)$, $0 < z < 1/p$, и

$$\mathsf{E}(z^Y) = \frac{1-p^*}{1-zp^*}, \quad 0 < z < \frac{1}{p^*}.$$

Значение p^* можно найти из уравнения

$$\mu_Y = \frac{p^*}{1-p^*} = K + \frac{p}{1-p} = \frac{K(1-p)+p}{1-p}.$$

Отсюда

$$p^* = \frac{K(1-zp)+p}{1+K(1-p)}, \quad \mathsf{E}(z^Y) = \frac{1-p}{1+K(1-p)-z(p+K(1-p))},$$

и

$$\mathsf{E}(z^X) = \frac{1-zp}{1+K(1-p)-z(p+K(1-p))}. \tag{1.2.30}$$

Вид распределения X, предложенного в формулировке примера, приводит к равенству

$$\mathsf{E}(z^X) = \varkappa_0 + (1-\varkappa_0)\frac{1-p_X}{1-zp_X}, \tag{1.2.31}$$

где $\varkappa_0 + (1-\varkappa_0)(1-p_X) = \mathsf{P}(X=0)$. Собирая вместе равенства

$$p_X = \frac{p+K(1-p)}{1+K(1-p)}, \quad \varkappa_0 = \frac{p}{p+K(1-p)},$$

убеждаемся, что формулы (1.2.30) и (1.2.31) совпадают. □

Я лишь прошу информации...

Чарльз Диккенс (1812–1870),
английский писатель;
«Дэвид Копперфилд»

В определении 1.2.13 и теореме 1.2.14 с. в. X и Y можно заменить случайными строками. Кроме того, повторяя предыдущие рассуждения для строк $\mathbf{X}^{(n)}$ и $\mathbf{Y}^{(n)}$, мы получим следующий результат.

Теорема 1.2.16. *а*) *Взаимная энтропия между случайными строками удовлетворяет неравенству*

$$I(\mathbf{X}^{(n)} : \mathbf{Y}^{(n)}) \geqslant h(\mathbf{X}^{(n)}) - \sum_{i=1}^{n} h(X_i \,|\, \mathbf{Y}^{(n)}) \geqslant h(\mathbf{X}^{(n)}) - \sum_{i=1}^{n} h(X_i \,|\, Y_i). \quad (1.2.32)$$

б) *Если* $X_1, \ldots, X_n$ *независимы, то*

$$I(\mathbf{X}^{(n)} : \mathbf{Y}^{(n)}) \geqslant \sum_{i=1}^{n} I(X_i : \mathbf{Y}^{(n)}). \quad (1.2.33)$$

Заметим, что п. ч. неравенства (1.2.33) *всегда удовлетворяется оценка*

$$\sum_{i=1}^{n} I(X_i : \mathbf{Y}^{(n)}) \geqslant \sum_{i=1}^{n} I(X_i : Y_i). \quad (1.2.34)$$

Пример 1.2.17. Пусть X, Z — с. в. и $\mathbf{Y}^{(n)} = Y_1 \ldots Y_n$ — случайная строка.

а) Докажите неравенство

$$0 \leqslant I(X : Z) \leqslant \min[h(X),\, h(Z)].$$

б) Докажите или опровергните контрпримером неравенство

$$I(X : \mathbf{Y}^{(n)}) \leqslant \sum_{j=1}^{n} I(X : Y_j), \quad (1.2.35)$$

сначала в предположении, что $Y_1, \ldots, Y_n$ независимые с. в., а затем в предположении, что $Y_1, \ldots, Y_n$ условно независимы при данном X.

в) Докажите или опровергните контрпримером неравенство:

$$I(X : \mathbf{Y}^{(n)}) \geqslant \sum_{j=1}^{n} I(X : Y_j), \quad (1.2.36)$$

сначала в предположении, что $Y_1, \ldots, Y_n$ — независимые с. в., а затем в предположении, что $Y_1, \ldots, Y_n$ условно независимы при данном X.

Решение. а) Согласно неравенству Гиббса $I(X:Z) \geqslant 0$ и

$$I(X:Z) := -\sum_{x,z} \mathsf{P}(X=x,\ Z=z) \log \frac{\mathsf{P}(X=x,\ Z=z)}{\mathsf{P}(X=x)\,\mathsf{P}(Z=z)} =$$

$$= h(X) - h(X\,|\,Z) = h(Z) - h(Z\,|\,X).$$

Здесь $h(X\,|\,Z) \geqslant 0$ и $h(Z\,|\,X) \geqslant 0$. Следовательно, $I(X:Z) \leqslant h(X)$ и $I(X:Z) \leqslant h(Z)$, так что $I(X:Z) \leqslant \min[h(X),\ h(Z)]$.

б) Запишем

$$I(X:\mathbf{Y}^{(n)}) = h(\mathbf{Y}^{(n)}) - h(\mathbf{Y}^{(n)}\,|\,X). \tag{1.2.37}$$

Тогда если $Y_1, \ldots, Y_n$ условно независимы при данном X, то п. ч. формулы (1.2.37) равна

$$h(\mathbf{Y}^{(n)}) - \sum_{j=1}^{n} h(Y_j\,|\,X) \leqslant \sum_{j=1}^{n} [h(Y_j) - h(Y_j\,|\,X)] = \sum_{j=1}^{n} I(X:Y_j),$$

что доказывает оценку (1.2.35). Далее, если $Y_1, \ldots, Y_n$ независимы, то п. ч. формулы (1.2.37) равна

$$\sum_{j=1}^{n} h(Y_j) - h(\mathbf{Y}^{(n)}\,|\,X) \geqslant \sum_{j=1}^{n} [h(Y_j) - h(Y_j\,|\,X)] = \sum_{j=1}^{n} I(X:Y_j)$$

и совпадает с п. ч. формулы (1.2.36).

С другой стороны, свойство б) нарушается, если нет условной независимости. Действительно, положим $n=2$ и $\mathbf{Y}^{(2)} = (Y_1,\ Y_2)$, где с. в. Y_1 и Y_2 принимают значения 0 или 1 с вероятностью $1/2$ независимо друг от друга. Положим $X = (Y_1 + Y_2) \bmod 2$. Тогда

$$h(X) = h(X\,|\,Y_j) = 1, \quad \text{так что} \quad I(X:Yj) \equiv 0, \quad j = 1,\ 2,$$

но

$$h(X\,|\,\mathbf{Y}^{(2)}) = 0, \quad \text{так что} \quad I(X:\mathbf{Y}^{(2)}) = 1.$$

Свойство в) ложно в предположении условной независимости. Действительно, возьмём дискретную марковскую цепь $(U_1,\ U_2,\ \ldots)$ с состояниями ± 1, начальным распределением вероятностей $\{1/2,\ 1/2\}$ и переходной матрицей $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Положим

$$Y_1 = U_1, \quad X = U_2, \quad Y_2 = U_3.$$

Тогда Y_1, Y_2 условно независимы при данном X: $Y_1 = Y_2 = -X$. С другой стороны,

$$1 = I(X : \mathbf{Y}^{(2)}) = h(\mathbf{Y}^{(2)}) = h(Y_1) = h(Y_2) < \\ < h(Y_1) + h(Y_2) = I(X : Y_1) + I(X : Y_2) = 2. \quad \square$$

Напомним, что вещественная функция $f(y)$, определённая на выпуклом множестве $\mathbb{V} \subset \mathbb{R}^m$, называется *выпуклой вверх*, если $f(\lambda_0 \mathbf{y}^{(0)} + \lambda_1 \mathbf{y}^{(1)}) \geqslant \geqslant \lambda_0 f(\mathbf{y}^{(0)}) + \lambda_1 f(\mathbf{y}^{(1)})$ для любых таких $\mathbf{y}(0)$, $\mathbf{y}(1) \in \mathbb{V}$ и λ_0, $\lambda_1 \in [0, 1]$, что $\lambda_0 + \lambda_1 = 1$. Она называется *строго выпуклой*, если равенство достигается только в случае $\mathbf{y}^{(0)} = \mathbf{y}^{(1)}$ или $\lambda_0 \lambda_1 = 0$. Будем рассматривать $h(X)$ как функцию от переменной $\mathbf{p} = (p_1, \ldots, p_m)$; в этом случае определим $\mathbb{V}$ как

$$\mathbb{V} = \{\mathbf{y} = (y_1, \ldots, y_m) \subset \mathbb{R}^m : y_i \geqslant 0, \ \ 1 \leqslant i \leqslant m, \ \ y_1 + \ldots + y_m = 1\}.$$

Теорема 1.2.18. *Энтропия — строго выпуклая функция от распределения вероятностей.*

Доказательство. Пусть с. в. $X^{(i)}$ имеют распределение вероятностей $p^{(i)}$, $i = 0, 1$, а с. в. Λ принимает значения 0 и 1 с вероятностями λ_0 и λ_1 соответственно, причём Λ не зависит от $X^{(0)}$, $X^{(1)}$. Положим $X = X^{(\Lambda)}$, тогда неравенство $h(\lambda_0 \mathbf{p}^{(0)} + \lambda_1 \mathbf{p}^{(1)}) \geqslant \lambda_0 h(\mathbf{p}^{(0)}) + \lambda_1 h(\mathbf{p}^{(1)})$ будет равносильно неравенству

$$h(X) \geqslant h(X \,|\, \Lambda), \tag{1.2.38}$$

которое следует из оценки (1.2.20). Если в формуле (1.2.38) достигается равенство, то X и Λ должны быть независимыми. Предположим, кроме того, что $\lambda_0 > 0$ и выпишем, пользуясь независимостью,

$$\mathsf{P}(X = i, \ \Lambda = 0) = \mathsf{P}(X = i) P(\Lambda = 0) = \lambda_0 \, \mathsf{P}(X = i).$$

Л. ч. равна $\lambda_0 \, \mathsf{P}(X = i \,|\, \Lambda = 0) = \lambda_0 p_i^{(0)}$, а п. ч. равна $\lambda_0 (\lambda_0 p_i^{(0)} + \lambda_1 p_i^{(1)})$. Сокращая на λ_0, получаем

$$(1 - \lambda_0) p_i^{(0)} = \lambda_1 p_i^{(1)},$$

т. е. распределения вероятностей $\mathbf{p}^{(0)}$ и $\mathbf{p}^{(1)}$ пропорциональны. Тогда либо они совпадают, либо $\lambda_1 = 0$, $\lambda_0 = 1$. Предположение $\lambda_1 > 0$ приводит к аналогичному выводу. $\square$

Пример 1.2.19. Покажите, что сумма

$$\rho(X, \ Y) = h(X \,|\, Y) + h(Y \,|\, X)$$

подчиняется равенству

$$\rho(X,\,Y) = h(X) + h(Y) + 2I(X:Y) = \\ = h(X,\,Y) - I(X:Y) = 2h(X,\,Y) - h(X) - h(Y).$$

Докажите, что функция ρ симметрична, т. е. $\rho(X,\,Y) = \rho(Y,\,X)$, и удовлетворяет неравенству треугольника: $\rho(X,\,Y) + \rho(Y,\,Z) \geqslant \rho(X,\,Z)$. Проверьте, что $\rho(X,\,Y) = 0$ тогда и только тогда, когда с. в. X и Y функционально зависят одна от другой. Кроме того, покажите, что если X' и X функционально зависят друг от друга, то $\rho(X,\,Y) = \rho(X',\,Y)$. Следовательно, ρ можно рассматривать как метрику на множестве с. в. X с точностью до эквивалентности: $X \sim X'$ тогда и только тогда, когда X и X' функционально зависят друг от друга.

Решение. Проверим неравенство треугольника

$$h(X\,|\,Z) + h(Z\,|\,X) \leqslant h(X\,|\,Y) + h(Y\,|\,X) + h(Y\,|\,Z) + h(Z\,|\,Y)$$

или

$$h(X,\,Z) \leqslant h(X,\,Y) + h(Y,\,Z) - h(Y).$$

Чтобы закончить доказательство, запишем $h(X,\,Y) \leqslant h(X,\,Y,\,Z)$ и заметим, что $h(X,\,Y,\,Z)$ равно

$$h(X,\,Z\,|\,Y) + h(Y) \leqslant h(X\,|\,Y) + h(Z\,|\,Y) + h(Y) = h(X,\,Y) + h(Y,\,Z) - h(Y).$$

Равенство достигается тогда и только тогда, когда (i) $Y = \varphi(X,\,Z)$ и (ii) X и Z условно независимы при данной с. в. Y. □

Замечание 1.2.20. Равенство $\rho(X,\,Z) = \rho(X,\,Y) + \rho(Y,\,Z)$ означает, что «точка» Y лежит на «прямой», проходящей через X и Z; иначе говоря, все три точки X, Y, Z лежат на одной прямой. Условную независимость X и Z при данной с. в. Y можно переформулировать другим (элегантным) способом: тройка $X \to Y \to Z$ обладает марковским свойством, т. е. $\rho(X,\,Z) = \\ = \rho(X,\,Y) + \rho(Y,\,Z)$ (короче говоря, является *марковской*). Предположим теперь, что у нас есть четыре с. в. X_1, X_2, X_3, X_4 причём $\forall\ 1 \leqslant i_1 < i_2 < \\ < i_3 \leqslant 4$, с. в. X_{i_1} и X_{i_3} условно независимы при данном X_{i_2}. Это свойство означает, что четвёрка $X_1 \to X_2 \to X_3 \to X_4$ является марковской, или, с геометрической точки зрения, все четыре точки лежат на одной прямой. Имеет место следующий факт: если $X_1 \to X_2 \to X_3 \to X_4$ — марковская четвёрка, то взаимные энтропии обладают свойством

$$I(X_1 : X_3) + I(X_2 : X_4) = I(X_1 : X_4) + I(X_2 : X_3). \tag{1.2.39}$$

Аналогичное свойство выполнено и для совместных энтропий:

$$h(X_1,\,X_3) + h(X_2,\,X_4) = h(X_1,\,X_4) + h(X_2,\,X_3). \tag{1.2.40}$$

Фактически для любой тройки X_{i_1}, X_{i_2}, X_{i_3} из четвёрки Маркова в метрике ρ мы имеем

$$\rho(X_{i_1}, X_{i_3}) = \rho(X_{i_1}, X_{i_2}) + \rho(X_{i_2}, X_{i_3}),$$

что в терминах совместной энтропии переписывается как

$$h(X_{i_1}, X_{i_3}) = h(X_{i_1}, X_{i_2}) + h(X_{i_2}, X_{i_3}) - h(X_{i_2}).$$

В результате соотношение (1.2.39) становится тождеством

$$\begin{aligned} h(X_1, X_2) + h(X_2, X_3) - h(X_2) + h(X_2, X_3) + h(X_3, X_4) - h(X_3) = \\ = h(X_1, X_2) + h(X_2, X_3) - h(X_2) + h(X_3, X_4) + h(X_2, X_3) - h(X_3). \end{aligned}$$

В книге [CT, с. 687, задача 17.3] это свойство записывается как более слабая версия приведённых выше оценок. □

Пример 1.2.21. Рассмотрим следующее неравенство (см. [CT], с. 687, (17.159)). Пусть дана тройка Маркова $X \to Y \to \mathbf{Z}$, где $\mathbf{Z}$ — случайная строка $Z_1 \dots Z_n$. Тогда

$$\sum_{1 \leqslant i \leqslant n} I(X : Z_i) \leqslant I(X, Y) + I(\mathbf{Z}), \quad \text{где} \quad I(\mathbf{Z}) := \sum_{1 \leqslant i \leqslant n} h(Z_i) - h(\mathbf{Z}).$$

Решение. Марковское свойство тройки $X \to Y \to \mathbf{Z}$ приводит к неравенству:

$$I(X : \mathbf{Z}) \leqslant I(X : Y).$$

Следовательно, достаточно проверить, что

$$\sum_{1 \leqslant i \leqslant n} I(X : Z_i) - I(\mathbf{Z}) \leqslant I(X : \mathbf{Z}). \tag{1.2.41}$$

Как мы покажем ниже, неравенство (1.2.41) выполнено для любых X и Y (вне зависимости от свойства Маркова). Действительно, оно равносильно такому неравенству

$$nh(X) \leqslant \sum_{1 \leqslant i \leqslant n} h(X, Z_i) + h(\mathbf{Z}) \leqslant h(X) + h(\mathbf{Z}) - h(X, \mathbf{Z}),$$

или

$$h(X, \mathbf{Z}) - h(X) \leqslant \sum_{1 \leqslant i \leqslant n} h(X, Z_i) - nh(X),$$

что, очевидно, совпадает с неравенством $h(\mathbf{Z} \,|\, X) \leqslant \sum\limits_{1 \leqslant i \leqslant n} h(Z_i \,|\, X)$. □

Пример 1.2.22. Выпишем $h(\mathbf{p}) := -\sum_1^m p_j \log p_j$ для «вектора» вероятностей $\mathbf{p} = \begin{pmatrix} p_1 \\ \vdots \\ p_m \end{pmatrix}$ с компонентами $p_j \geqslant 0$ и $p_1 + \ldots + p_m = 1$.

а) Покажите, что $h(P\mathbf{p}) \geqslant h(\mathbf{p})$, если $P = (P_{ij})$ — дважды стохастическая матрица (т. е. квадратная матрица с элементами $P_{ij} \geqslant 0$, сумма элементов которой в каждой строке и столбце равна единице). Более того, $h(P\mathbf{p}) \equiv h(\mathbf{p})$, если и только если P является матрицей перестановки. Напомним, что матрица оператора, переставляющего базисные векторы, — это матрица, полученная из единичной матрицы $\mathbf{1}$ перестановкой строк.

б) Покажите, что $h(\mathbf{p}) \geqslant -\sum_{j=1}^m \sum_{k=1}^m p_j P_{jk} \log P_{jk}$, если P — стохастическая матрица, а $\mathbf{p}$ — её собственный вектор: $P\mathbf{p} = \mathbf{p}$.

Решение. а) Ввиду выпуклости логарифма $x \mapsto \log x$ для любых таких λ_i, $c_i \geqslant 0$, что $\sum_1^m \lambda_i = 1$, выполнено неравенство

$$\log(\lambda_1 c_1 + \ldots + \lambda_m c_m) \geqslant \sum_1^m \lambda_i \log c_i.$$

Применим его к

$$h(P\mathbf{p}) = -\sum_{ij} P_{i,j} p_j \log\Big(\sum_k P_{ik} p_k\Big) \geqslant$$
$$\geqslant -\sum_j p_j \log\Big(\sum_{i,k} P_{ij} P_{ik} p_k\Big) = -\sum_j p_j \log\Big(\Big(P^{\mathrm{T}} P\mathbf{p}\Big)_j\Big).$$

По неравенству Гиббса п. ч. не меньше $h(\mathbf{p})$. Равенство имеет место тогда и только тогда, когда $P^{\mathrm{T}} P\mathbf{p} = \mathbf{p}$, т. е. $P^{\mathrm{T}} P\mathbf{p} = \mathbf{1}$ (единичная матрица). Такое получается если и только если P — матрица перестановки.

б) Л. ч. неравенства равна $h(U_n)$ для стационарного источника Маркова $(U_1, U_2, \ldots)$ с инвариантным распределением $\mathbf{p}$, тогда как п. ч. равна $h(U_n \,|\, U_{n-1})$. Поэтому общее неравенство $h(U_n \,|\, U_{n-1}) \leqslant h(U_n)$ даёт искомый результат. □

Пример 1.2.23. Последовательность с. в. $\{X_j : j = 1, 2, \ldots\}$ представляет собой ц. м. д. в. с конечным пространством состояний.

а) Используя стандартные свойства условной энтропии, покажите, что $h(X_j \,|\, X_{j-1}) \leqslant h(X_j \,|\, X_{j-2})$, и в случае стационарной ц. м. д. в. докажите неравенство $h(X_j \,|\, X_{j-2}) \leqslant 2h(X_j \,|\, X_{j-1})$.

б) Покажите, что взаимная информация $I(X_m : X_n)$ не убывает по m и не возрастает по n, $1 \leqslant m \leqslant n$.

Решение. а) По свойству Маркова и благодаря стационарности можно записать:

$$h(X_j \,|\, X_{j-1}) = h(X_j \,|\, X_{j-1},\, X_{j-2}) \leqslant h(X_j \,|\, X_{j-2}) \leqslant h(X_j,\, X_{j-1} \,|\, X_{j-2}) = \\ = h(X_j \,|\, X_{j-1},\, X_{j-2}) + h(X_{j-1} \,|\, X_{j-2}) = 2h(X_j \,|\, X_{j-1}).$$

б) Запишем

$$I(X_m : X_n) - I(X_m : X_{n+1}) = h(X_m \,|\, X_{n+1}) - h(X_m \,|\, X_n) = \\ = h(X_m \,|\, X_{n+1}) - h(X_m \,|\, X_n,\, X_{n+1}) \geqslant 0$$

(так как X_m и X_{n+1} условно независимы при данном X_n). Поэтому $I(X_m : X_n)$ не возрастает по n.

Аналогично

$$I(X_{m-1} : X_n) - I(X_m : X_n) = h(X_n \,|\, X_{m-1}) - h(X_n \,|\, X_m,\, X_{m-1}) \geqslant 0.$$

Значит, $I(X_m : X_n)$ не убывает по m.

Здесь мы не использовали предположение о стационарности. Ц. м. д. в. может быть даже не однородной по времени (т. е. вероятности перехода могут зависеть не только от i и j, но и от времени перехода). □

Пример 1.2.24. Для с. в. Y_1, Y_2, Y_3 определим

$$I(Y_1 : Y_2 \,|\, Y_3) = h(Y_1 \,|\, Y_3) + h(Y_2 \,|\, Y_3) - h(Y_1,\, Y_2 \,|\, Y_3).$$

Пусть теперь последовательность X_n, $n = 0,\, 1,\, \ldots,$ является ц. м. д. в. Покажите, что

$$I(X_{n-1} : X_{n+1} \,|\, X_n) = 0 \quad \text{и, следовательно,} \quad I(X_{n-1} : X_{n+1}) \leqslant I(X_n : X_{n+1}).$$

Покажите также, что $I(X_n : X_{n+m})$ не возрастает по m, при $m = 0,\, 1,\, 2,\, \ldots$.

Решение. По свойству Маркова X_{n-1} и X_{n+1} условно независимы при данном X_n. Следовательно,

$$h(X_{n-1},\, X_{n+1} \,|\, X_n) = h(X_{n+1} \,|\, X_n) + h(X_{n-1} \,|\, X_n)$$

и $I(X_{n-1} : X_{n+1} \,|\, X_n) = 0$. Кроме того,

$$\begin{aligned} I(X_n : X_{n+m}) - I(X_n : X_{n+m+1}) &= \\ = h(X_{n+m}) - h(X_{n+m+1}) + h(X_n,\, X_{n+m+1}) - h(X_n,\, X_{n+m}) &= \\ = h(X_n \,|\, X_{n+m+1}) - h(X_n \,|\, X_{n+m}) &= \\ = h(X_n \,|\, X_{n+m+1}) - h(X_n \,|\, X_{n+m},\, X_{n+m+1}) &\geqslant 0; \end{aligned}$$

последнее равенство выполнено ввиду условной независимости, а последнее неравенство следует из оценки (1.2.21). □

Информация — это разрешение неопределенности.

Клод Шеннон (1916–2001),
американский электротехник и математик

Пример 1.2.25 (аксиоматическое определение энтропии). а) Рассмотрим распределение вероятностей $(p_1,\, \ldots,\, p_m)$ и соответствующую меру неопределенности (энтропию), удовлетворяющую условию

$$h(p_1q_1,\, p_1q_2,\, \ldots,\, p_1q_n,\, p_2,\, p_3,\, \ldots,\, p_m) = h(p_1,\, \ldots,\, p_m) + p_1 h(q_1,\, \ldots,\, q_n), \tag{1.2.42}$$

где $(q_1,\, \ldots,\, q_n)$ — какое-то другое распределение. Можно сказать, что если одно из событий A_1 (вероятности p_1) разделяется на подсобытия $B_{11},\, \ldots,\, B_{1n}$ условных вероятностей $q_1,\, \ldots,\, q_n$, то вся неопределённость распадается в сумму, как показано в формуле. Предполагается, что функционал h симметричен относительно своих аргументов, так что если события $A_2,\, A_3,\, \ldots$ разделяются на подсобытия $B_{21},\, \ldots,\, B_{2n}$ и т. д., то будет выполнено аналогичное равенство.

Предположим, что $F(m) := h(1/m, \ldots, 1/m)$ монотонно возрастает по m. Покажите, что из условия (1.2.42) вытекает равенство $F(m^k) = kF(m)$, и, следовательно, $F(m) = c\log m$ для некоторой константы c. Выведите отсюда, что

$$h(p_1, \ldots, p_m) = -c\sum_j p_j \log p_j, \tag{1.2.43}$$

если p_j рациональны. Справедливость (1.2.43) для произвольных $\{p_j\}$ тогда будет следовать из предположения о непрерывности h.

б) Существует и альтернативная аксиоматическая характеризация энтропии: если симметричная функция h для всех $k < m$ подчиняется условию

$$h(p_1, \ldots, p_m) = h(p_1 + \ldots + p_k, p_{k+1}, \ldots, p_m) + \\ + (p_1 + \ldots + p_k)h\Big(\frac{p_1}{p_1 + \ldots + p_k}, \ldots, \frac{p_k}{p_1 + \ldots + p_k}\Big), \tag{1.2.44}$$

$h(1/2, 1/2) = 1$ и функция $h(p, 1-p)$ непрерывна при $p \in [0, 1]$, то

$$h(p_1, \ldots, p_m) = -\sum_j p_j \log p_j.$$

Решение. а) Опираясь на формулу (1.2.42), мы получим для функции $F(m) = h(1/m, \ldots, 1/m)$ следующее тождество:

$$\begin{aligned} F(m^2) &= h\Big(\frac{1}{m}\times\frac{1}{m}, \ldots, \frac{1}{m}\times\frac{1}{m}, \frac{1}{m^2}, \ldots, \frac{1}{m^2}\Big) = \\ &= h\Big(\frac{1}{m}, \frac{1}{m^2}, \ldots, \frac{1}{m^2}\Big) + \frac{1}{m}F(m) = \\ &= \ldots = h\Big(\frac{1}{m}, \ldots, \frac{1}{m}\Big) + \frac{m}{m}F(m) = 2F(m). \end{aligned}$$

Если индуктивно предположить, что $F(m^{k-1}) = (k-1)F(m)$, то

$$\begin{aligned} F(m^k) &= h\Big(\frac{1}{m}\times\frac{1}{m^{k-1}}, \ldots, \frac{1}{m}\times\frac{1}{m^{k-1}}, \frac{1}{m^k}, \ldots, \frac{1}{m^k}\Big) = \\ &= h\Big(\frac{1}{m^{k-1}}, \frac{1}{m^k}, \ldots, \frac{1}{m^k}\Big) + \frac{1}{m}F(m) = \\ &= \ldots = h\Big(\frac{1}{m^{k-1}}, \ldots, \frac{1}{m^{k-1}}\Big) + \frac{m}{m}F(m) = \\ &= (k-1)F(m) + F(m) = kF(m). \end{aligned}$$

Далее, при данном натуральном $b > 2$ и данном m можно найти такое натуральное n, что $2^n \leqslant b^m \leqslant 2^{n+1}$, т. е.

$$\frac{n}{m} \leqslant \log_2 b \leqslant \frac{n}{m} + \frac{1}{m}.$$

Ввиду монотонности $F(m)$ получаем $nF(2) \leqslant mF(b) \leqslant (n+1)F(2)$, или

$$\frac{n}{m} \leqslant \frac{F(b)}{F(2)} \leqslant \frac{n}{m} + \frac{1}{m}.$$

Можно заключить, что $\left|\log_2 b - \dfrac{F(b)}{F(2)}\right| \leqslant \dfrac{1}{m}$. Переходя к пределу при $m \to \infty$, находим, что $F(b) = c \log b$, где $c = F(2)$.

Возьмём теперь рациональные числа $p_1 = \dfrac{r_1}{r}, \ldots, p_m = \dfrac{r_m}{r}$ и получим

$$\begin{aligned} h\Big(\frac{r_1}{r}, \ldots, \frac{r_m}{r}\Big) &= h\Big(\frac{r_1}{r_1} \times \frac{1}{r_1}, \ldots, \frac{r_1}{r_1} \times \frac{1}{r}, \frac{r_2}{r}, \ldots, \frac{r_m}{r}\Big) - \frac{r_1}{r} F(r_1) = \ldots = \\ &= h\Big(\frac{1}{r}, \ldots, \frac{1}{r}\Big) - c \sum_{1 \leqslant i \leqslant m} \frac{r_i}{r} \log r_i = \\ &= c \log r - c \sum_{1 \leqslant i \leqslant m} \frac{r_i}{r} \log r_i = -c \sum_{1 \leqslant i \leqslant m} \frac{r_i}{r} \log \frac{r_i}{r}. \end{aligned}$$

б) Во втором определении особенность в том, что мы не предполагаем монотонности по m у функции $F(m) = h(1/m, \ldots, 1/m)$. Однако опираясь на (1.2.44), легко проверить следующее свойство аддитивности

$$F(mn) = F(m) + F(n)$$

для всех натуральных m и n. Следовательно, разложив m на простые множители $m = q_1^{\alpha_1} \ldots q_s^{\alpha_s}$, получим

$$F(m) = \alpha_1 F(q_1) + \ldots + \alpha_s F(q_s).$$

Далее покажем, что

$$\frac{F(m)}{m} \to 0, \quad F(m) - F(m-1) \to 0 \quad \text{при } m \to \infty. \tag{1.2.45}$$

Действительно,

$$\begin{aligned} F(m) &= h\Big(\frac{1}{m}, \ldots, \frac{1}{m}\Big) = \\ &= h\Big(\frac{1}{m}, \frac{m-1}{m}\Big) + \frac{m-1}{m} h\Big(\frac{1}{m-1}, \ldots, \frac{1}{m-1}\Big), \end{aligned}$$

т. е.

$$h\Big(\frac{1}{m}, \frac{m-1}{m}\Big) = F(m) - \frac{m-1}{m} F(m-1).$$

По непрерывности и симметричности функции $h(p, 1-p)$ имеем

$$\lim_{m \to \infty} h\Big(\frac{1}{m}, \frac{m-1}{m}\Big) = h(0, 1) = h(1, 0)$$

Но из представления

$$h\Big(\frac{1}{2},\,\frac{1}{2},\,0\Big)=h\Big(\frac{1}{2},\,\frac{1}{2}\Big)+\frac{1}{2}h\Big(1,\,0\Big)$$

и симметрии

$$h\Big(\frac{1}{2},\,\frac{1}{2},\,0\Big)=h\Big(0,\,\frac{1}{2},\,\frac{1}{2}\Big)=h\Big(1,\,0\Big)+h\Big(\frac{1}{2},\,\frac{1}{2}\Big)$$

находим, что $h(1,\,0)=0$. Следовательно,

$$\lim_{m\to\infty}\Big(F(m)-\frac{m-1}{m}F(m-1)\Big)=0. \tag{1.2.46}$$

Далее запишем

$$mF(m)=\sum_{k=1}^{m}k\Big(F(k)-\frac{k-1}{k}F(k-1)\Big),$$

или, что равносильно,

$$\frac{F(m)}{m}=\frac{m+1}{2m}\left[\frac{2}{m(m+1)}\sum_{k=1}^{m}k\Big(F(k)-\frac{k-1}{k}F(k-1)\Big)\right].$$

Выражение в квадратных скобках — это среднее арифметическое $m(m+1)/2$ членов последовательности

$$F(1),\;\; F(2)-F(1),\;\; F(2)-F(1),\;\; F(3)-\frac{2}{3}F(2),\;\; F(3)-\frac{2}{3}F(2),$$
$$F(3)-\frac{2}{3}F(2),\;\;\ldots,\;\; F(k)-\frac{k-1}{k}F(k-1),\;\;\ldots,$$
$$F(k)-\frac{k-1}{k}F(k-1),\;\;\ldots,$$

стремящейся к 0. Поэтому среднее арифметическое тоже стремится к нулю. Следовательно, $F(m)/m\to 0$. Более того,

$$F(m)-F(m-1)=\Big(F(m)-\frac{m-1}{m}F(m-1)\Big)-\frac{1}{m}F(m-1)\to 0,$$

и свойство (1.2.45) доказано. Теперь определим

$$c(m)=\frac{F(m)}{\log m}$$

и покажем, что $c(m)=\mathrm{const}$. Достаточно доказать, что $c(p)=\mathrm{const}$ для всех простых чисел p. Сначала докажем ограниченность последовательности $(c(p))$. Если это не так и последовательность $(c(p))$ не ограничена сверху, то найдётся бесконечная последовательность простых чисел $p_1,\,p_2,\,\ldots,\,p_n,\,\ldots$ с минимальным p_n, для которого $c(p_n)>c(p_{n-1})$ при

$p_n > p_{n-1}$. Тогда по построению, если q — простое число, $q < p_n$, то $c(q) < c(p_n)$.

Разложим число $p_n - 1$ на простые сомножители: $p_n - 1 = q_1^{\alpha_1} \dots q_s^{\alpha_s}$, причём $q_1 = 2$. Тогда разность $F(p_n) - F(p_n - 1)$ запишется как

$$F(p_n) - \frac{F(p_n)}{\log p_n} \log(p_n - 1) + c(p_n) \log(p_n - 1) - F(p_n - 1) = \\ = \frac{F(p_n)}{p_n} \frac{p_n}{\log p_n} \log \frac{p_n}{p_n - 1} + \sum_{j=1}^{s} \alpha_j (c(p_n) - c(q_j)) \log q_j.$$

Из предыдущего замечания следует, что

$$\sum_{j=1}^{s} \alpha_j (c(p_n) - c(q_j)) \log q_j \geqslant (c(p_n) - c(2)) \log 2 = c(p_n) - c(2). \qquad (1.2.47)$$

Более того, так как $\lim\limits_{p \to \infty} \dfrac{p}{\log p} \log \dfrac{p}{p-1} = 0$, то из формул (1.2.46) и (1.2.47) вытекает неравенство $c(p) - c(2) \leqslant 0$, что противоречит построению последовательности $c(p)$. Следовательно, последовательность $c(p)$ ограничена сверху. Аналогично проверяется ограниченность этой последовательности снизу. Более того, предыдущие рассуждения показывают, что $\inf_p c(p)$ и $\sup_p c(p)$ достигаются.

Допустим, что $c(\hat{p}) = \sup_p c(p) > c(2)$. Возьмём натуральное m и разложим число $\hat{p}^m - 1$ на простые сомножители: $\hat{p}^m - 1 = q_1^{\alpha_1} \dots q_s^{\alpha_s}$. Повторяя проведённые выше рассуждения, получаем

$$F(\hat{p}^m) - \frac{\hat{p}^m}{\log \hat{p}^m} \log(\hat{p}^m - 1) + c(\hat{p}) \log(\hat{p}^m - 1) - F(\hat{p}^m - 1) = \\ = \frac{F(\hat{p}^m)}{\hat{p}^m} \frac{\hat{p}^m}{\log \hat{p}^m} \log \frac{\hat{p}^m}{\hat{p}^m - 1} + \sum_{j=1}^{s} \alpha_j (c(\hat{p}) - c(q_j)) \log q_j \geqslant \\ \geqslant \frac{c(\hat{p}^m)}{\hat{p}^m} \frac{\hat{p}^m}{\log \hat{p}^m} \log \frac{\hat{p}^m}{\hat{p}^m - 1} + (c(\hat{p}) - c(2)).$$

Вновь переходя к пределу при $m \to \infty$, получим неравенство $c(\hat{p}) - c(2) \leqslant 0$, что даёт противоречие. Аналогично можно показать, что $\inf_p c(p) = c(2)$. Следовательно, $c(p) = c$ — константа и $F(m) = c \log m$. Из равенства $F(2) = h\left(\frac{1}{2}, \frac{1}{2}\right) = 1$ получаем, что $c = 1$. Наконец, как и в п. а) получаем

$$h(p_1, \dots, p_m) = -\sum_{i=1}^{m} p_i \log p_i \qquad (1.2.48)$$

для любых рациональных чисел $p_1, \ldots, p_m$ с $\sum\limits_{i=1}^{m} p_i = 1$. В силу непрерывности равенство (1.2.48) выполняется для любого распределения вероятностей. □

Пример 1.2.26. Покажите, что «более однородное» распределение обладает большей энтропией. Если $\mathbf{p} = (p_1, \ldots, p_n)$ и $\mathbf{q} = (q_1, \ldots, q_n)$ — распределения вероятностей на множестве $\{1, \ldots, n\}$, то говорят, что $\mathbf{p}$ более однородное, чем $\mathbf{q}$ ($\mathbf{p} \preceq \mathbf{q}$, см. [МО]), если после переупорядочивания $(p_1, \ldots, p_n)$ и $(q_1, \ldots, q_n)$ по убыванию:

$$p_1 \geqslant \ldots \geqslant p_n, \quad q_1 \geqslant \ldots \geqslant q_n,$$

выполняются неравенства

$$\sum_{i=1}^{k} p_i \leqslant \sum_{i=1}^{k} q_i \quad \forall\, k = 1, \ldots, n.$$

Итак, покажите, что

$$h(\mathbf{p}) \geqslant h(\mathbf{q}), \quad \text{если } \mathbf{p} \preceq \mathbf{q}.$$

Решение. Запишем распределения вероятностей $\mathbf{p}$ и $\mathbf{q}$ как неубывающие функции дискретного аргумента

$$\mathbf{p} \sim p^{(1)} \geqslant \ldots \geqslant p^{(n)} \geqslant 0, \quad \mathbf{q} \sim q^{(1)} \geqslant \ldots \geqslant q^{(n)} \geqslant 0,$$
$$\sum_i p^{(i)} = 1, \quad \sum_i q^{(i)} = 1.$$

Условие $\mathbf{p} \preceq \mathbf{q}$ означает, что если $\mathbf{p} \neq \mathbf{q}$, то найдутся такие i_1 и i_2, что а) $1 \leqslant i_1 \leqslant i_2 \leqslant n$, б) $q^{(i_1)} > p^{(i_1)} \geqslant p^{(i_2)} > q^{(i_2)}$, в) $q^{(i)} \geqslant p^{(i)}$ при $1 \leqslant i \leqslant i_1$, $q(i) \leqslant p(i)$ при $i \geqslant i_2$.

Теперь применим индукцию по s — числу индексов $i = 1, \ldots, n$, для которых $q^{(i)} \neq p^{(i)}$. Если $s = 0$, то $\mathbf{p} = \mathbf{q}$ и энтропии совпадают. Сделаем индуктивное предположение и увеличим s на 1. Выберем пару i_1, i_2 как и раньше. Будем увеличивать $q^{(i_2)}$ и уменьшать $q^{(i_1)}$ с сохранением суммы $q(i_1) + q(i_2)$, до тех пор пока $q^{(i_1)}$ не достигнет $p^{(i_1)}$ или $q^{(i_2)}$ не достигнет $p^{(i_2)}$. Свойство в) гарантирует, что и модифицированные распределения будут подчиняться неравенству $\mathbf{p} \preceq \mathbf{q}$.

Так как функция $x \mapsto \eta(x) = -x \log x - (1 - x) \log(1 - x)$ строго возрастает на отрезке $[0,\ 1/2]$, тоже энтропия модифицированного распределения будет строго возрастать. Для завершения доказательства уменьшим s и воспользуемся предположением индукции. □

Завершая тему энтропии, мы хотели бы упомянуть имена ученых, которые внесли большой вклад в ее изучение: С. Карно (Франция, 1796–1832),

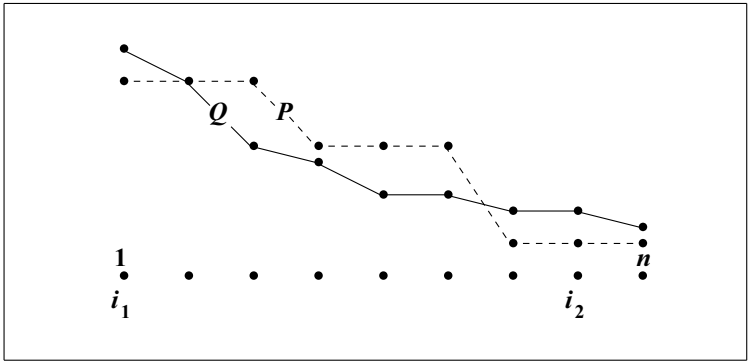


Рис. 1.6

Р. Клаузиус (Германия, 1822–1888), У. Т. Кельвин (Великобритания, 1824–1907), Дж. К. Максвелл (Великобритания, 1831–1879), Дж. У. Гиббс (США, 1839–1903), Л. Больцман (Австрия, 1844–1906), А. Я. Хинчин (Россия, 1894–1959), А. Н. Колмогоров (Россия, 1903–1987) и К. Шеннон (США, 1916–2001). Но даже сегодня мы все еще далеки от полного понимание значения их фундаментального вклада.

Мне... было интересно, как это называть (мера неопределенности). Когда я обсуждал этот вопрос с Джоном фон Нейманом, он... сказал мне: «... назовите это энтропией. Во-первых, ... [она] была использована в статистической механике под этим именем.... Во-вторых, и что более важно, никто не знает, что такое энтропия, поэтому в дискуссии у вас всегда будет преимущество».

Клод Шеннон (1916–2001),
американский электротехник и математик

Пользуйтесь словом «кибернетика», Норберт, никто не знает, что... оно означает. Это... даст вам преимущество в спорах.

Клод Шеннон (1916–2001),
американский электротехник и математик;
из письма к Н. Винеру

§ 1.3. Первая теорема Шеннона о кодировании. Энтропийная скорость марковского источника

Современная наука знает, что блокировка информации ведёт к энтропии и всеобщему уничтожению.

Александр Солженицын (1918–2008), русский писатель, лауреат Нобелевской премии по литературе; из нобелевской лекции

Полезный смысл скорости передачи информации источника заключается в том, что она указывает на минимальную скорость роста размера множества строк, асимптотически несущих полную вероятность.

Лемма 1.3.1. *Пусть H — скорость передачи информации источника* (*см.* (1.1.18)). *Определим*

$$D_n(R) := \max\left[\mathsf{P}(\mathbf{U}^{(n)} \in A)\colon A \subset I^{\times n},\ \ \#A \leqslant 2^{nR}\right]. \tag{1.3.1}$$

Тогда для любого $\varepsilon > 0$ при $n \to \infty$

$$\lim D_n(H+\varepsilon) = 1 \quad \textit{и если} \quad H > 0,\ \textit{то}\ D_n(H-\varepsilon) \not\to 1. \tag{1.3.2}$$

Доказательство. По определению $R := H + \varepsilon$ — надёжная скорость кодирования. Следовательно, существует такая последовательность подмножеств $A_n \subset I^{\times n}$ с количеством элементов $\#A_n \leqslant 2^{nR}$, что $\mathsf{P}(U^{(n)} \in A_n) \to 1$, при $n \to \infty$. Поскольку $D_n(R) \geqslant \mathsf{P}(U^{(n)} \in A_n)$, то $D_n(R) \to 1$.

Пусть теперь $H > 0$, и выберем $R := H - \varepsilon$; при достаточно малом ε получим $R > 0$. Однако R не является надёжной скоростью передачи. Поэтому не существует последовательности A_n, обладающей описанным выше свойством. Возьмём множество C_n, на котором достигается максимум из формулы (1.3.1). Тогда $\#C_n \leqslant 2^{nR}$, но $\mathsf{P}(C_n) \not\to 1$. □

Рассмотрим значение «логарифма правдоподобия» на букву источника для данной строки $\mathbf{u}^{(n)} = u_1 \dots u_n$:

$$\xi_n(\mathbf{u}^{(n)}) = -\frac{1}{n}\log_+ p_n(\mathbf{u}^{(n)}), \qquad \mathbf{u}^{(n)} \in I^{\times n}, \tag{1.3.3а}$$

где $p_n(\mathbf{u}^{(n)}) := \mathsf{P}(\mathbf{U}^{(n)} = \mathbf{u}^{(n)})$ — вероятность, приписанная строке $\mathbf{u}^{(n)}$. Здесь и далее $\log_+ x = \log x$, если $x > 0$ и $\log_+ x = 0$, если $x = 0$. Для случайной строки $\mathbf{U}^{(n)} = u_1 \dots u_n$ определим с. в.

$$\xi_n(\mathbf{U}^{(n)}) = -\frac{1}{n}\log_+ p_n(\mathbf{U}^{(n)}). \tag{1.3.3б}$$

□

Лемма 1.3.2. *Для любых R, $\varepsilon > 0$ справедлива оценка*

$$\mathsf{P}(\xi_n \leqslant R) \leqslant D_n(R) \leqslant \mathsf{P}(\xi_n \leqslant R + \varepsilon) + 2^{-n\varepsilon}. \tag{1.3.4}$$

Доказательство. Опустим для краткости верхний индекс (n) в обозначении $\mathbf{u}^{(n)}$ и $\mathbf{U}^{(n)}$. Положим

$$B_n := (\mathbf{u} \in I^{\times n} \colon p_n(u) \geqslant 2^{-nR}) = \\ = (\mathbf{u} \in I^{\times n} \colon -\log p_n(u) \leqslant nR) = (\mathbf{u} \in I^{\times n} \colon \xi_n(\mathbf{u}) \leqslant R).$$

Тогда

$$1 \geqslant \mathsf{P}(\mathbf{U} \in B_n) = \sum_{\mathbf{u} \in B_n} p_n(\mathbf{u}) \geqslant 2^{-nR} \# B_n, \quad \text{где } \# B_n < 2^{nR}.$$

Отсюда

$$D_n(R) = \max\left[\mathsf{P}(\mathbf{U} \in A_n) \colon A_n \subset I^{\times n}, \ \# A_n \leqslant 2^{nR}\right] \geqslant \mathsf{P}(\mathbf{U} \in B_n) = \mathsf{P}(\xi_n \leqslant R),$$

что доказывает л. ч. формулы (1.3.4).

С другой стороны, существует множество $C_n \subset I^{\times n}$, на котором достигается максимум в формуле (1.3.1). Для такого множества $D_n(R) = \mathsf{P}(\mathbf{U} \in C_n)$ раскладывается следующим образом:

$$D_n(R) = \mathsf{P}(\mathbf{U} \in C_n, \, \xi_n \leqslant R + \varepsilon) + \mathsf{P}(\mathbf{U} \in C_n, \, \xi_n > R + \varepsilon) \leqslant \\ \leqslant \mathsf{P}(\xi_n \leqslant R + \varepsilon) + \sum_{\mathbf{u} \in C_n} p_n(\mathbf{u}) \mathbf{1}(p_n(\mathbf{u}) < 2^{-n(R+\varepsilon)}) \leqslant \\ \leqslant \mathsf{P}(\xi_n \leqslant R + \varepsilon) + 2^{-n(R+\varepsilon)} \# C_n = \\ = \mathsf{P}(\xi_n \leqslant R + \varepsilon) + 2^{-n(R+\varepsilon)} 2^{nR} = \mathsf{P}(\xi_n \leqslant R + \varepsilon) + 2^{-n\varepsilon}. \quad \square$$

Определение 1.3.3 (см. т. 2, с. 424). Последовательность с. в. $\{\eta_n\}$ сходится по вероятности к с. в. η, если $\forall\, \varepsilon > 0$

$$\lim_{n \to \infty} \mathsf{P}(|\eta_n - \eta| \geqslant \varepsilon) = 0. \tag{1.3.5}$$

В дальнейшем сходимость по вероятности будем обозначать как $\eta_n \xrightarrow{\mathsf{P}} \eta$.

Замечание 1.3.4. Напомним, что сходимость по вероятности (к среднему значению) фигурирует в так называемом законе больших чисел (см. (1.3.8) ниже и т. 1, с. 106). $\square$

Теорема 1.3.5 (первая теорема Шеннона о кодировании (ПТШК)). *Если последовательность ξ_n сходится по вероятности к γ, то эта константа γ равна H — скорости передачи информации источника.*

Доказательство. Пусть $\xi_n \xrightarrow{\mathsf{P}} \gamma$. Так как $\xi_n \geqslant 0$, получаем, что $\gamma \geqslant 0$. По лемме 1.3.2 для любого $\varepsilon > 0$ имеем, что

$$D_n(\gamma+\varepsilon) \geqslant \mathsf{P}(\xi_n \leqslant \gamma+\varepsilon) \geqslant \mathsf{P}(\gamma-\varepsilon \leqslant \xi_n \leqslant \gamma+\varepsilon) = \\ = \mathsf{P}(|\xi_n-\gamma| \leqslant \varepsilon) = 1-\mathsf{P}(|\xi_n-\gamma| \geqslant \varepsilon) \to 1 \ (n\to\infty).$$

Следовательно, $H \leqslant \gamma$. В частности, если $\gamma = 0$, то и $H = 0$. Если $\gamma > 0$, то снова по лемме 1.3.2 получаем, что $D_n(\gamma-\varepsilon)$ не превосходит

$$\mathsf{P}(\xi_n \leqslant \gamma-\varepsilon/2) + 2^{-n\varepsilon/2} \leqslant \mathsf{P}(|\xi_n-\gamma| \geqslant \varepsilon/2) + 2^{-n\varepsilon/2} \to 0.$$

Ввиду леммы 1.3.1 имеем, что $H \geqslant \gamma$. Значит, $H = \gamma$. □

Замечание 1.3.6. а) Сходимость $\xi_n \xrightarrow{\mathsf{P}} \gamma = H$ эквивалентна следующему асимптотическому свойству равнораспределённости (а. с. р.): для любого $\varepsilon > 0$ выполняется равенство

$$\lim_{n\to\infty} \mathsf{P}(2^{-n(H+\varepsilon)} \leqslant p_n(\mathbf{U}^{(n)}) \leqslant 2^{-n(H-\varepsilon)}) = 1. \tag{1.3.6}$$

Действительно,

$$\mathsf{P}(2^{-n(H+\varepsilon)} \leqslant p_n(\mathbf{U}^{(n)}) \leqslant 2^{-n(H-\varepsilon)}) = \mathsf{P}(H-\varepsilon \leqslant -\frac{1}{n}\log p_n(\mathbf{U}^{(n)}) \leqslant H+\varepsilon) = \\ = \mathsf{P}(|\xi_n - H| \leqslant \varepsilon) = 1-\mathsf{P}(|\xi_n-H| > \varepsilon).$$

Иначе говоря, $\forall\, \varepsilon > 0$ существует такое $n_0 = n_0(\varepsilon)$, что для всех $n > n_0$ множество $I^{\times n}$ распадается в объединение непересекающихся подмножеств Π_n и T_n, причём

(i) $\mathsf{P}(\mathbf{U}^{(n)} \in \Pi_n) < \varepsilon$,

(ii) $2^{-n(H+\varepsilon)} \leqslant \mathsf{P}(\mathbf{U}^{(n)} = \mathbf{u}^{(n)}) \leqslant 2^{-n(H-\varepsilon)}\ \forall\, \mathbf{u}^{(n)} \in T_n$.

Образно говоря, T_n — множество «типичных» строчек, а Π_n — дополнительное множество.

Можно сделать вывод, что для источника с а. с. р. можно кодировать типичные строки кодовыми словами одной длины, а остальные — как получится. Тогда эффективная скорость кодирования составит $H + o(1)$ бит на букву источника, хотя источник выдаёт информацию со скоростью $\log m$ бит на букву источника.

б) Заметим, что

$$\mathsf{E}\xi_n = -\frac{1}{n}\sum_{\mathbf{u}^{(n)}\in I^{\times n}} p_n(\mathbf{u}^{(n)})\log p_n(\mathbf{u}^{(n)}) = \frac{1}{n}h^{(n)}. \tag{1.3.7}$$

Простейшим примером источника информации (и одним из наиболее поучительных) служит *источник Бернулли*.

Теорема 1.3.7. *Для источника Бернулли* $U_1, U_2, \ldots,$ *с* $\mathsf{P}(U_i = x) = p(x)$ *выполнено равенство*

$$H = -\sum_x p(x)\log p(x).$$

Доказательство. Для последовательности н. о. р. с. в. $U_1, U_2, \ldots,$ вероятность строки вычисляется по формуле

$$p_n(\mathbf{u}^{(n)}) = \prod_{i=1}^n p(u_i), \qquad \mathbf{u}^{(n)} = u_1 \ldots u_n.$$

Следовательно, $-\log p_n(u) = \sum\limits_i -\log p(u_i)$. Обозначая $\sigma_i = -\log p(U_i)$, $i = 1, 2, \ldots,$ мы видим, что $\sigma_1, \sigma_2, \ldots$ образуют последовательность н. о. р. с. в. Для случайной строки $\mathbf{U}^{(n)} = U_1 \ldots U_n$ имеем $-\log p_n(\mathbf{U}^{(n)}) = \sum\limits_{i=1}^n \sigma_i$, где $\sigma_i = -\log p(U_i)$ — н. о. р. с. в.

Далее запишем $\xi_n = \dfrac{1}{n}\sum\limits_{i=1}^n \sigma_i$. Заметим, что $\mathsf{E}\sigma_i = -\sum\limits_j p(j)\log p(j) = h$ и

$$\mathsf{E}\xi_n = \mathsf{E}\left(\frac{1}{n}\sum_{i=1}^n \sigma_i\right) = \frac{1}{n}\sum_{i=1}^n \mathsf{E}\sigma_i = \frac{1}{n}\sum_{i=1}^n h = h.$$

Последнее равенство получено в соответствии с формулой (1.3.7), так как, для источника Бернулли $h^{(n)} = nh$ (см. формулу (1.1.16)) и, следовательно, $\mathsf{E}\xi_n = h$. Мы сразу же видим, что по закону больших чисел $\xi_n \xrightarrow{\mathsf{P}} h$, так что $H = h$ по теореме 1.3.5 (ПТШК). □

Теорема 1.3.8 (закон больших чисел для н. о. р. с. в.). *Для любой последовательности н. о. р. с. в.* $\eta_1, \eta_2, \ldots,$ $\mathsf{E}\eta_i = r$, *и любого* $\varepsilon > 0$ *имеет место равенство*

$$\lim_{n\to\infty} \mathsf{P}\left(\left|\frac{1}{n}\sum_{i=1}^n \eta_i - r\right| \geqslant \varepsilon\right) = 0. \tag{1.3.8}$$

Доказательство. Результат следует из неравенства Чебышёва (см. т. 1, с. 103). Ниже мы напомним неравенство Маркова, обобщающее неравенство Чебышёва. □

Лемма 1.3.9. *Для любой с. в.* η *и любого* $\varepsilon > 0$ *выполнено неравенство*

$$\mathsf{P}(\eta \geqslant \varepsilon) \leqslant \frac{1}{\varepsilon^2}\,\mathsf{E}\eta^2.$$

Далее рассмотрим марковский источник $U_1\,U_2\,\ldots$ с буквами из алфавита $I_m = (1,\ldots,m)$ и предположим, что матрица переходных вероятностей $(P(u,v))$ (или, точнее, её степени) обладает свойством

$$\min_{u,v} P^{(r)}(u,v) = \rho > 0 \quad \text{для некоторого } r \geqslant 1. \tag{1.3.9}$$

Это условие означает, что ц. м. д. в. неприводима и апериодична. Тогда ц. м. д. в. обладает единственным инвариантным (равновесным) распределением $\pi(1),\ldots,\pi(m)$:

$$0 \leqslant \pi(u) \leqslant 1, \quad \sum_{u=1}^{m} \pi(u) = 1, \quad \pi(v) = \sum_{u=1}^{m} \pi(u) P(u,v) \tag{1.3.10}$$

и n-шаговая матрица переходных вероятностей $P^{(n)}(u,v)$ стремится к $\pi(v)$ так же, как вероятности $(\lambda P^{n-1})(v) = \mathsf{P}(U_n = v)$:

$$\lim_{n\to\infty} P^{(n)}(u,v) = \lim_{n\to\infty} \mathsf{P}(U_n = v) = \lim_{n\to\infty} \sum_{u} \lambda(u) P^{(n)}(u,v) = \pi(v) \tag{1.3.11}$$

для любого начального распределения $(\lambda(u),\ u \in I)$. Более того, сходимость в формуле (1.3.11) имеет экспоненциальную (геометрическую) скорость.

Теорема 1.3.10. *Предположим, что условие* (1.3.9) *выполнено с константой* $r = 1$. *Тогда ц. м. д. в.* $U_1, U_2, \ldots$ *обладает единственным инвариантным распределением* (1.3.10) *и для любых* $u, v \in I$ *и произвольного начального распределения* λ *на* I *выполнены неравенства*

$$|P^{(n)}(u,v) - \pi(v)| \leqslant (1-\rho)^n \quad и \quad |\mathsf{P}(U_n = v) - \pi(v)| \leqslant (1-\rho)^{n-1}. \tag{1.3.12}$$

В случае общего $r \geqslant 1$ *надо поменять в п. ч. неравенств* (1.3.12) $(1-\rho)^n$ *на* $(1-\rho)^{[n/r]}$ *и* $(1-\rho)^{n-1}$ *на* $(1-\rho)^{[(n-1)/r]}$.

Доказательство теоремы 1.3.10 дается в примере 1.3.13. □

Теперь введём скорость передачи информации H марковского источника.

Теорема 1.3.11. *Если источник Маркова удовлетворяет условию* (1.3.9), *то*

$$H = -\sum_{1\leqslant u,v\leqslant m} \pi(u) P(u,v) \log P(u,v) = \lim_{n\to\infty} h(U_{n+1} \,|\, U_n); \tag{1.3.13}$$

если источник стационарен, то $H = h(U_{n+1} \,|\, U_n)$.

Доказательство. Вновь воспользуемся теоремой Шеннона (ПТШК) для проверки сходимости $\xi_n \xrightarrow{\mathsf{P}} H$, где H задаётся формулой

(1.3.13) и $\xi_n = -\frac{1}{n}\log p_n(\mathbf{U}^{(n)})$ (см. формулу (1.3.3б)). Другими словами, из условия (1.3.9) следует а. с. р. для марковского источника.

Тот факт, что источник марковский, означает, что для любой строки $\mathbf{u}^{(n)} = u_1 \dots u_n$ выполняется равенство

$$p_n(\mathbf{u}^{(n)}) = \lambda(u_1)P(u_1, u_2)\dots P(u_{n-1}, u_n) \tag{1.3.14а}$$

и $-\log p_n(\mathbf{u}^{(n)})$ представляется в виде суммы

$$-\log\lambda(u_1) - \log P(u_1, u_2) - \dots - \log P(u_{n-1}, u_n). \tag{1.3.14б}$$

Для случайной строки $\mathbf{U}^{(n)} = U_1 \dots U_n$ с. в. $-\log p_n(\mathbf{U}_n)$ имеет аналогичный вид:

$$-\log\lambda(U_1) - \log P(U_1, U_2) - \dots - \log P(U_{n-1}, U_n). \tag{1.3.15}$$

Как и в случае источника Бернулли, обозначим

$$\sigma_1(U_1) := -\log\lambda(U_1), \quad \sigma_i(U_1) := -\log(U_{i-1}, U_i), \ \ i \geqslant 2, \tag{1.3.16}$$

и запишем

$$\xi_n = \frac{1}{n}\left(\sigma_1 + \sum_{i=1}^{n-1}\sigma_{i+1}\right). \tag{1.3.17}$$

Математическое ожидание с. в. σ приведено ниже:

$$\mathsf{E}\sigma_1 = -\sum_u \lambda(u)\log\lambda(u) \tag{1.3.18а}$$

и, так как $\mathsf{P}(U_i = v) = \lambda P^{i-1}(v) = \sum\limits_u \lambda(u)P^{(i-1)}(u, v)$,

$$\mathsf{E}\sigma_{i+1} = -\sum_{u,u'}\mathsf{P}(U_i = u, U_{i+1} = u')\log P(u, u') =$$

$$= -\sum_{u,u'}(\lambda P^{i-1})(u)P(u, u')\log P(u, u'), \ \ i \geqslant 1. \tag{1.3.18б}$$

Из теоремы 1.3.10 вытекает, что $\lim\limits_{i\to\infty}\mathsf{E}\sigma_i = H$. Следовательно,

$$\lim_{n\to\infty}\mathsf{E}\xi_n = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\mathsf{E}\sigma_i = H,$$

и сходимость $\xi_n \xrightarrow{\mathsf{P}} H$ есть не что иное, как закон больших чисел для последовательности (σ_i):

$$\lim_{n\to\infty}\mathsf{P}\left(\left|\frac{1}{n}\sum_{i=1}^{n}\sigma_i - H\right| \geqslant \varepsilon\right) = 0. \tag{1.3.19}$$

Однако ситуация тут не такая простая, как в случае источника Бернулли. Существуют две трудности: (i) $\mathsf{E}\sigma_i$ равняется H только в пределе при $i \to \infty$, (ii) $\sigma_1, \sigma_2, \ldots$ теперь не являются независимыми. Более того, эта последовательность даже не является ц. м. д. в. или марковской цепью более высокого порядка. Говорят, что последовательность $\xi_1, \xi_2, \ldots$ образует дискретную марковскую цепь порядка k (ц. м. д. в. (k)), если $\forall\, n \geqslant 1$

$$\mathsf{P}(U_{n+k+1} = u' \,|\, U_{n+k} = u_k, \ldots, U_{n+1} = u_1, \ldots) = \\ = \mathsf{P}(U_{n+k+1} = u' \,|\, U_{n+k} = u_k, \ldots, U_{n+1} = u_1).$$

Очевидно, что для ц. м. д. в. (k) последовательность векторов $\bar{U}_n = (U_n, U_{n+1}, \ldots, U_{n+k-1})$ при $n \geqslant 1$ является обычной дискретной марковской цепью. Можно сказать, что «память» в последовательности $\sigma_1, \sigma_2, \ldots$ является бесконечной. Однако она убывает в геометрической прогрессии: точный смысл этого высказывания раскрывается в примере 1.3.14.

В любом случае, используя неравенство Чебышёва, получаем

$$\mathsf{P}\left(\left|\frac{1}{n}\sum_{i=1}^{n}\sigma_i - H\right| \geqslant \varepsilon\right) \leqslant \frac{1}{n^2\varepsilon^2}\,\mathsf{E}\left(\sum_{i=1}^{n}(\sigma_i - H)\right)^2. \tag{1.3.20}$$

Теорема 1.3.11 немедленно следует из леммы.

Лемма 1.3.12. *Справедлива оценка*

$$\mathsf{E}\left(\sum_{i=1}^{n}(\sigma_i - H)\right)^2 \leqslant Cn, \tag{1.3.21}$$

где положительная константа C не зависит от n.

По формуле (1.3.21) п. ч. неравенства (1.3.20) не превосходит $\dfrac{C}{n\varepsilon^2}$ и стремится к 0 при $n \to \infty$.

Доказательство леммы 1.3.12 дано в примере 1.3.14.

Пример 1.3.13. Докажите следующее неравенство (см. неравенство (1.3.12)):

$$|P^{(n)}(u, v) - \pi(v)| \leqslant (1 - \rho)^n. \tag{1.3.22}$$

Решение (ср. т. 2, с. 86). Прежде всего заметим, что из неравенства (1.3.22) следует первое неравенство теоремы 1.3.10, так же как и формула (1.3.10). Действительно,

$$\pi(v) = \lim_{n\to\infty} P^{(n)}(u, v) = \lim_{n\to\infty} \sum_{\tilde{u}} P^{(n-1)}(u, \tilde{u})P(\tilde{u}, v) = \sum_{\tilde{u}} \pi(\tilde{u})P(\tilde{u}, v), \tag{1.3.23}$$

что даёт формулу (1.3.10). Если $\pi'(1), \pi'(2), \dots, \pi'(m)$ — ещё один инвариантный вектор вероятностей, т. е.

$$0 \leqslant \pi'(u) \leqslant 1, \quad \sum_{u=1}^{m} \pi'(u) = 1, \quad \pi'(v) = \sum_{u} \pi'(u) P(u, v),$$

то $\pi'(v) = \sum\limits_{u} \pi'(u) P(u, v)\ \forall\, n \geqslant 1$. Переходя к пределу при $n \to \infty$, получаем

$$\pi'(v) = \sum_{u} \pi'(u) \lim_{n\to\infty} P^{(n)}(u, v) = \sum_{u} \pi'(u)\pi'(v) = \pi(v),$$

что означает единственность инвариантного вектора.

Для доказательства неравенства (1.3.22) обозначим

$$m_n(v) = \min_{u} P^{(n)}(u, v), \quad M_n(v) = \max_{u} P^{(n)}(u, v). \tag{1.3.24}$$

Тогда

$$m_{n+1}(v) = \min_{u} P^{(n+1)}(u, v) = \min_{u} \sum_{\tilde{u}} P(u, \tilde{u}) P^{(n)}(\tilde{u}, u) \geqslant$$
$$\geqslant \min_{u} P^{(n)}(u, v) \sum_{\tilde{u}} P(u, \tilde{u}) = m_n(v).$$

Аналогично

$$M_{n+1}(v) = \max_{u} P^{(n+1)}(u, v) = \max_{u} \sum_{\tilde{u}} P(u, \tilde{u}) P^{(n)}(\tilde{u}, v) \leqslant$$
$$\leqslant \max_{u} P^{(n)}(u, v) \sum_{\tilde{u}} P(u, \tilde{u}) = M_n(v).$$

Из неравенств $0 \leqslant m_n(v) \leqslant M_n(v) \leqslant 1$ следует, что как $m_n(v)$, так и $M_n(v)$ имеют пределы, причём

$$m(v) = \lim_{n\to\infty} m_n(v) \leqslant \lim_{n\to\infty} M_n(v) = M(v).$$

Более того, разность $M(v) - m(v)$ вычисляется как предел

$$\lim_{n\to\infty} (M_n(v) - m_n(v)) = \lim_{n\to\infty} \max_{u,u'} (P^{(n)}(u, v) - P^{(n)}(u', v)).$$

Так что, если нам удастся доказать неравенство

$$\max_{u,u'} |P^{(n)}(u, v) - P^{(n)}(u', v)| \leqslant (1 - \rho)^n, \tag{1.3.25}$$

мы придём к равенству $M(v) = m(v)$ при каждом v. Более того, переобозначив общее значение $M(v) = m(v)$ через $\pi(v)$, получим неравенство (1.3.22):

$$|P^{(n)}(u, v) - \pi(v)| \leqslant M_n(v) - m_n(v) \leqslant (1 - \rho)^n.$$

Для доказательства неравенства (1.3.25) рассмотрим ц. м. д. в. на $I \times I$ с состояниями (u_1, u_2) и вероятностями переходов

$$\mathbf{P}((u_1, u_2), (v_1, v_2)) = \\ = \begin{cases} P(u_1, v_1)P(u_2, v_2), & \text{если } u_1 \neq u_2, \\ P(u, v), & \text{если } u_1 = u_2 = u, \ v_1 = v_2 = v, \\ 0, & \text{если } u_1 = u_2, \ v_1 \neq v_2. \end{cases} \quad (1.3.26)$$

Легко проверить, что $\mathbf{P}((u_1, u_2), (v_1, v_2))$ действительно является матрицей переходных вероятностей (размера $m^2 \times m^2$): если $u_1 = u_2 = u$, то

$$\sum_{v_1, v_2} \mathbf{P}((u_1, u_2), (v_1, v_2)) = \sum_{v} P(u, v) = 1,$$

тогда как при $u_1 \neq u_2$ имеем

$$\sum_{v_1, v_2} \mathbf{P}((u_1, u_2), (v_1, v_2)) = \sum_{v_1} P(u_1, v_1) \sum_{v_2} P(u_2, v_2) = 1$$

(неравенство $0 \leqslant \mathbf{P}((u_1, u_2), (v_1, v_2)) \leqslant 1$ непосредственно вытекает из определения (1.3.26)).

Это так называемая *склеенная ц. м. д. в.* на $I \times I$, будем обозначать её через (V_n, W_n), $n \geqslant 1$. Заметим, что обе компоненты V_n и W_n — ц. м. д. в. с вероятностями переходов $P(u, v)$. Более точно, компоненты V_n и W_n меняются независимо друг от друга до первого (случайного) момента τ, когда они совпадут. Будем называть этот момент моментом склеивания. После этого момента компоненты V_n и W_n «слипаются» вместе и меняются синхронно с вероятностями переходов $P(u, v)$.

Предположим, что склеенная цепь начинается с состояния (u, u'). Тогда

$$|P^{(n)}(u, v) - P^{(n)}(u', v)| = \\ = |\mathsf{P}(V_n = v \,|\, V_1 = u, \ W_1 = u') - \mathsf{P}(W_n = v \,|\, V_1 = u, \ W_1 = u')| = \\ \text{(так как каждая компонента пары } (V_n, W_n) \text{ меняется} \\ \text{с одинаковыми вероятностями переходов)} \\ = \big|\, \mathsf{P}(V_n = v, \ W_n \neq v \,|\, V_1 = u, \ W_1 = u') - \\ - \mathsf{P}(V_n \neq v, \ W_n = v \,|\, V_1 = u, \ W_1 = u')\big| \leqslant \\ \leqslant \mathsf{P}(V_n \neq W_n \,|\, V_1 = u, \ W_1 = u') = \mathsf{P}(\tau > n \,|\, V_1 = u, \ W_1 = u'). \quad (1.3.27)$$

Далее, вероятность $\mathsf{P}(\tau = 1 \,|\, V_1 = u, \ W_1 = u')$ оценивается как

$$\geqslant \sum_{v} P(u, v)P(u', v) \geqslant \rho \sum_{v} P(u', v) = \rho,$$

т. е. для дополнительной вероятности получаем

$$\mathsf{P}(\tau > 1 \,|\, V_1 = u,\ W_1 = u') \leqslant 1 - \rho.$$

Строгое свойство Маркова (склеенной цепи) дает оценку

$$\mathsf{P}(\tau > n \,|\, V_1 = u,\ W_1 = u') \leqslant (1 - \rho)^n. \tag{1.3.28}$$

Теперь неравенства (1.3.28) и (1.3.27) доказывают оценку (1.3.25). □

Пример 1.3.14. В предположении (1.3.9) с $r = 1$ докажите следующее неравенство:

$$|\,\mathsf{E}[(\sigma_i - H)(\sigma_{i+k} - H)]| \leqslant (H + |\log\rho|)^2(1 - \rho)^{k-1}. \tag{1.3.29}$$

Решение. Для краткости будем считать, что $i > 1$, случай $i = 1$ требует незначительных изменений. Возвращаясь к определению с. в. σ_i, $i > 1$, запишем

$$\begin{aligned}
&\mathsf{E}[(\sigma_i - H)(\sigma_{i+k} - H)] = \\
&= \sum_{u,u'} \sum_{v,v'} \mathsf{P}(U_i = u,\ U_{i+1} = u';\ U_{i+k} = v,\ U_{i+k+1} = v') \times \\
&\qquad \times (-\log P(u,\ u') - H)(-\log P(v,\ v') - H).
\end{aligned} \tag{1.3.30}$$

Наша цель — сравнить это выражение со следующим:

$$\begin{aligned}
&\sum_{u,u'} \sum_{v,v'} (\lambda P^{i-1})(u) P(u,\ u')(-\log P(u,\ u') - H) \times \\
&\qquad \times \pi(v) P(v,\ v')(-\log P(v,\ v') - H).
\end{aligned} \tag{1.3.31}$$

Заметим, что (1.3.31) равно нулю, так как $\sum\limits_{v,v'}$ равна нулю по определению H (см. формулу (1.3.13)).

Разница в суммах (1.3.30) и (1.3.31) проистекает из того факта, что вероятности

$$\begin{aligned}
&\mathsf{P}(U_i = u,\ U_{i+1} = u';\ U_{i+k} = v,\ U_{i+k+1} = v') = \\
&\qquad = (\lambda P^{i-1})(u) P(u,\ u') P^{(k-1)}(u',\ u) P(v,\ v')
\end{aligned}$$

и

$$(\lambda P^{i-1})(u) P(u,\ u') \pi(v) P(v,\ v')$$

не совпадают. Оценим разность этих вероятностей по модулю:

$$|\,P^{(k-1)}(u',\ v) - \pi(v)\,| \leqslant (1 - \rho)^{k-1}$$

и, так как $|\,-\log P(\cdot\,,\cdot) - H\,| \leqslant H + |\,\log\rho\,|$, получим неравенство (1.3.29). □

Доказательство теоремы 1.3.11 теперь легко завершить. Для доказательства оценки (1.3.21) раскроем квадрат и воспользуемся аддитивностью математического ожидания:

$$\mathsf{E}\left[\sum_{i=1}^{n}(\sigma_i - H)\right]^2 = \sum_{1\leqslant i\leqslant n}\mathsf{E}[(\sigma_i - H)^2] + 2\sum_{1\leqslant i<j\leqslant n}\mathsf{E}[(\sigma_i - H)(\sigma_j - H)]. \tag{1.3.32}$$

С первой суммой в формуле (1.3.32) всё хорошо: она состоит из n слагаемых $\mathsf{E}(\sigma_i - H)^2$, каждое из которых ограничено константой (можно взять, например, $C' = (H + |\log\rho|)^2$). Поэтому первая сумма не превосходит $C'n$. А вот со второй суммой возникает проблема: она состоит из $n(n-1)/2$ членов. Оценим её следующим образом:

$$\left|\sum_{1\leqslant i<j\leqslant n}\mathsf{E}[(\sigma_i - H)(\sigma_j - H)]\right| \leqslant \sum_{i=1}^{n}\left(\sum_{k=1}^{\infty}|\mathsf{E}[(\sigma_i - H)(\sigma_{i+k} - H)]|\right). \tag{1.3.33}$$

Теперь для завершения доказательства воспользуемся формулой (1.3.29). □

Следующая теорема говорит о роли (относительной) энтропии в локальной центральной предельной теореме (ср. т. 1, с. 111).

Теорема 1.3.15. *Пусть $\xi_1, \xi_2, \ldots$ — последовательность н. о. р. с. в. со значениями 0 и 1 и вероятностями $1-p$ и p соответственно, $0 < p < 1$. Тогда для любой последовательности натуральных чисел k_n, удовлетворяющей условиям $k_n \to \infty$ и $n - k_n \to \infty$ при $n \to \infty$, справедлива следующая асимптотика*:

$$\mathsf{P}\left(\sum_{i=1}^{n}\xi_i = k_n\right) \sim (2\pi np^*(1-p^*))^{-1/2}\exp(-nD(p\,\|\,p^*)). \tag{1.3.34}$$

Знак «$\sim$» здесь означает, что отношение левой и правой частей стремится к 1 при $n \to \infty$, $p^*(= p_n^*)$ обозначает отношение k_n/n и символ $D(p\,\|\,p^*)$ обозначает относительную энтропию $h(X\,|\,Y)$, где X — распределено как ξ_i, т. е. принимает значения 0 и 1 с вероятностями $1-p$ и p, а Y принимает те же значения с вероятностями $1-p^*$ и p^*.

Доказательство. Воспользуемся формулой Стирлинга (см. т. 1, с. 112):

$$n! \sim \sqrt{2\pi n}\, n^n e^{-n}. \tag{1.3.35}$$

(Справедлива более точная формула: $n! = \sqrt{2\pi n}\, n^n e^{-n+\theta(n)}$, где $\dfrac{1}{12n+1} < \theta(n) < \dfrac{1}{12n}$, но для наших целей достаточно оценки (1.3.35).) Тогда

вероятность в л. ч. формулы (1.3.34) равна (для краткости опускаем нижний индекс у k_n)

$$C_n^k p^k (1-p)^{n-k} \sim \Big(\frac{n}{2\pi k(n-k)}\Big)^{1/2} \frac{n^n}{k^k (n-k)^{n-k}} p^k (1-p)^{n-k} =$$
$$= (2\pi n p^*(1-p^*))^{-1/2} \times$$
$$\times \exp\Big(- \frac{k \ln k}{n} - \frac{(n-k)\ln(n-k)}{n} + k \ln p + (n-k)\ln(1-p)\Big).$$

П. ч. последней формулы совпадает с п. ч. формулы (1.3.34), что завершает доказательство. □

Если p^* близко к p, то можно записать

$$D(p \,\|\, p^*) = \frac{1}{2}\Big(\frac{1}{p} + \frac{1}{1-p}\Big)(p^* - p)^2 + O(|p^* - p|^3), \tag{1.3.36}$$

где $D(p \,\|\, p^*)\Big|_{p^*=p} = \Big(\frac{\mathrm{d}}{\mathrm{d}p^*} D(p \,\|\, p^*)\Big)\Big|_{p^*=p} = 0$, и немедленно получить следующий результат.

Следствие 1.3.16 (локальная теорема Муавра—Лапласа; см. т. 1, с. 111). *Если* $n(p^* - p) = k_n - np = o(n^{2/3})$, *то*

$$\mathsf{P}\Big(\sum_{i=1}^n \xi_i = k_n\Big) \sim \frac{1}{\sqrt{2\pi n p(1-p)}} \exp\Big(- \frac{n}{2p(1-p)}(p^* - p)^2\Big). \tag{1.3.37}$$

Пример 1.3.17. В каждый момент времени прибор считывает текущую версию строки из N двоичных символов. Затем он передаёт количество символов, равных 1. В промежуток между считываниями строка меняется случайным образом в одном символе (0 на 1 или наоборот, причём вероятность быть изменённым не зависит от символа). Найдите формулу для скорости передачи данного источника.

Решение. Это марковский источник с пространством состояний $\{0, 1, \ldots, N\}$ и матрицей переходных вероятностей

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 1/N & 0 & (N-1)/N & 0 & \ldots & 0 & 0 \\ 0 & 2/N & 0 & (N-2)/N & \ldots & 0 & 0 \\ & & \ldots & \ldots & & & \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1/N \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

Ц. м. д. в. неприводима и периодична. Она обладает единственным инвариантным распределением

$$\pi_i = 2^{-N} C_N^i, \quad 0 \leqslant i \leqslant N.$$

По теореме 1.3.11 имеем

$$H = -\sum_{i,j} \pi_i P(i,\, j) \log P(i,\, j) = 2^{1-N} \frac{1}{N} \sum_{j=1}^{N-1} j C_N^j \log \frac{N}{j}. \qquad \square$$

Пример 1.3.18. Стационарный источник генерирует символы 0, 1, ..., m ($m \geqslant 4$ — чётное число) в соответствии с ц. м. д. в. со следующими вероятностями переходов $p_{jk} = P(U_{n+1} = k \,|\, U_n = j)$:

$$p_{jj+2} = 1/3, \;\; 0 \leqslant j \leqslant m-2, \quad p_{jj-2} = 1/3, \;\; 2 \leqslant j \leqslant m,$$
$$p_{jj} = 1/3, \;\; 2 \leqslant j \leqslant m-2, \quad p_{00} = p_{11} = p_{m-1m-1} = p_{mm} = 2/3.$$

Первый символ имеет равномерное распределение. Найдите скорость передачи информации источника. Противоречит ли полученный результат первой теореме Шеннона о кодировании 1.3.5 (ПТШК)? Как изменится ответ при нечётном m? Как можно использовать ПТШК при нечётном m для вычисления скорости передачи информации описанного выше источника?

Решение. При чётном m ц. м. д. в. приводима: пространство состояний разбивается на два класса: $I_1 = \{0, 2, \ldots, m\}$ с $m/2 + 1$ состояниями и $I_2 = \{1, 3, \ldots, m-1\}$ с $m/2$ состояниями. Соответственно для любого множества A_n n-строчек

$$\mathsf{P}(A_n) = q\, \mathsf{P}_1(A_{n1}) + (1-q)\, \mathsf{P}_2(A_{n2}), \tag{1.3.38}$$

где $A_{n1} = A_n \cap I_1$ и $A_{n2} = A_n \cap I_2$; P_i относится к цепочке из класса I_i, $i = 1, 2$, и $q = \mathsf{P}(U_1 \in I_1)$. С. в. из формулы (1.3.3б) — это $\xi_n = -\frac{1}{n} \log p_n(\mathbf{U}^{(n)})$, что сообразуясь с равенством (1.3.38), можно переписать как

$$\xi_n = \begin{cases} -\frac{1}{n} \log p_{n1}(\mathbf{U}^{(n)}) & \text{с вероятностью } q, \\ -\frac{1}{n} \log p_{n2}(\mathbf{U}^{(n)}) & \text{с вероятностью } 1-q. \end{cases} \tag{1.3.39}$$

Обе получившиеся ц. м. д. в. неприводимы и апериодичны на своих классах состояний. Их инвариантные распределения равномерны:

$$\pi_i^{(1)} = \frac{2}{m+2}, \quad i \in I_1, \qquad \pi_i^{(2)} = \frac{2}{m}, \quad i \in I_2. \tag{1.3.40}$$

Скорости передачи информации соответственно равны

$$H^{(1)} = \log 3 - \frac{8}{3(m+2)} \quad \text{и} \quad H^{(2)} = \log 3 - \frac{8}{3m}. \tag{1.3.41}$$

Как вытекает из равенства (1.3.38), скорость передачи информации всей исходной ц. м. д. в. равна

$$H_{\text{even}} = \begin{cases} H^{(1)} = \max[H^{(1)}, H^{(2)}], & \text{если } 0 < q \leqslant 1, \\ H^{(2)}, & \text{если } q = 0. \end{cases} \tag{1.3.42}$$

При $0 < q < 1$ ПТШК неприменима:

$$-\frac{1}{n}\log p_{n1}(\mathbf{U}^{(n)}) \xrightarrow{\mathsf{P}_1} H^{(1)}, \quad \text{в то время как } -\frac{1}{n}\log p_{n2}(\mathbf{U}^{(n)}) \xrightarrow{\mathsf{P}_2} H^{(2)},$$

т. е. ξ_n сходится не к константе. Однако если $q(1-q) = 0$, то выражение (1.3.42) сводится к единственному пределу и ПТШК применима: ξ_n сходится к соответствующей константе $H^{(i)}$.

Если m нечётно, то опять возникает два сообщающихся класса $I_1 = \{0, 2, \ldots, m-1\}$ и $I_2 = \{1, 3, \ldots, m\}$, каждый из которых теперь имеет $(m+1)/2$ состояний. Как и ранее, ц. м. д. в. P_1 и P_2 неприводимы и апериодичны и обладают равномерным инвариантным распределением:

$$\pi_i^{(1)} = \frac{2}{m+1}, \ \ i \in I_1, \quad \pi_i^{(2)} = \frac{2}{m+1}, \ \ i \in I_2.$$

Их общая скорость передачи информации равна

$$H_{\text{odd}} = \log 3 - \frac{8}{3(m+1)}, \tag{1.3.43}$$

что также совпадает со скоростью передачи информации всего источника. Это согласуется с ПТШК, так как теперь

$$\xi_n = -\frac{1}{n}\log p_n(U^{(n)}) \xrightarrow{\mathsf{P}} H_{\text{odd}}. \tag{1.3.44}$$

Пример 1.3.19. Пусть a — размер A и b — размер алфавита B. Рассмотрим источник с алфавитом $A + B$ с тем ограничением, что никакие две буквы из A не могут быть соседними в строке.

а) Предположим, что сообщение генерируется ц. м. д. в., в которой в данном месте может равновероятно появиться любой разрешенный символ. Покажите, что скорость передачи информации этого источника равна

$$H = \frac{a\log b + (a+b)\log(a+b)}{2a+b}. \tag{1.3.45}$$

б) Найдите количество строк длины n из алфавита $A + B$, удовлетворяющих ограничению: никакая пара соседних букв не принадлежит множеству A. Рассмотрим источник, равновероятно выбирающий и передающий одну из этих строк. Покажите, что предельная скорость передачи информации при $n \to \infty$ равна

$$H = \log\left(\frac{b + \sqrt{b^2 + 4ab}}{2}\right).$$

Почему получились разные ответы?

Решение. а) Вероятности переходов ц. м. д. в. выглядят следующим образом:

$$P(x, y) = \begin{cases} 0, & \text{если } x, y \in \{1, \ldots, a\}, \\ 1/b, & \text{если } x \in \{1, \ldots, a\},\ y \in \{a+1, \ldots, a+b\}, \\ 1/(a+b), & \text{если } x \in \{a+1, \ldots, a+b\},\ y \in \{1, \ldots, a+b\} \end{cases}$$

Эта ц. м. д. в. неприводима и апериодична. Более того, $\min P^{(2)}(x, y) > 0$, следовательно, она обладает единственным инвариантным распределением $\pi = (\pi(x),\ x \in \{1, \ldots, a+b\})$, которое можно найти из уравнений детального баланса $\pi(x)P(x, y) = \pi(y)P(y, x)$ (у. д. б., см. т. 2, с. 95). Получаем

$$\pi(x) = \begin{cases} 1/(2a+b), & x \in \{1, \ldots, a\}, \\ (a+b)/[b(2a+b)], & x \in \{a+1, \ldots, a+b\}. \end{cases}$$

Напомним, что из у. д. б. вытекает, что π — инвариантное распределение: $\pi(y) = \sum\limits_x \pi(x)P(x, y)$, но обратное, вообще говоря, неверно. Таким образом, мы получаем формулу (1.3.45).

б) Пусть M_n — число допустимых n-строчек, A_n — число допустимых n-строчек, заканчивающихся буквой из A, и B_n — число допустимых n-строчек, заканчивающихся буквой из B. Тогда

$$M_n = A_n + B_n, \quad A_{n+1} = aB_n \ \text{ и } \ B_{n+1} = b(A_n + B_n),$$

следовательно,

$$B_{n+1} = bB_n + abB_{n-1}.$$

Решение этого рекуррентного соотношения имеет вид

$$B_n = c_+\lambda_+^n + c_-\lambda_-^n,$$

где $\lambda_\pm$ — собственные числа матрицы

$$\begin{pmatrix} 0 & ab \\ 1 & b \end{pmatrix},$$

т. е.

$$\lambda_\pm = \frac{b \pm \sqrt{b^2 + 4ab}}{2},$$

а $c_\pm$ — константы, $c_+ > 0$. Следовательно,

$$M_n = a(c_+\lambda_+^{n-1} + c_-\lambda_-^{n-1}) + (c_+\lambda_+^n + c_+\lambda_-^n) =$$
$$= \lambda_+^n \left(c_- \left(a\frac{\lambda_-^{n-1}}{\lambda_+^n} + \frac{\lambda_-^n}{\lambda_+^n} \right) + c_+ \left(a\frac{1}{\lambda_+} + 1 \right) \right),$$

и $\frac{1}{n}\log M_n$ представляется суммой

$$\log\lambda_+ + \frac{1}{n}\log\left(c_-\left(a\frac{\lambda_-^{n-1}}{\lambda_+^n}+\frac{\lambda_-^n}{\lambda_+^n}\right)+c_+\left(a\frac{1}{\lambda_+}+1\right)\right).$$

Заметим, что $\left|\frac{\lambda_-}{\lambda_+}\right|<1$. Поэтому предельная скорость передачи информации равна

$$\lim_{n\to\infty}\frac{1}{n}\log M_n=\log\lambda_+.$$

Ответы отличаются по той причине, что условие равной вероятности допустимых цепочек приводит к сложной зависимости между соседними символами, в связи с чем последовательность букв не образует ц. м. д. в. □

Пример 1.3.20. Пусть $\{U_j\colon j=1,2,\ldots\}$ — неприводимая апериодичная ц. м. д. в. с конечным пространством состояний. При данных $n\geqslant 1$ и $\alpha\in(0,1)$ упорядочим строки $\mathbf{u}^{(n)}$ по убыванию вероятности: $\{\mathsf{P}(\mathbf{U}^{(n)}=\mathbf{u}_1^{(n)})\geqslant\mathsf{P}(\mathbf{U}^{(n)}=\mathbf{u}_2^{(n)})\geqslant\ldots\}$ и разделим их на две группы в том месте, где вероятность остатка не будет превосходить $1-\alpha$. Пусть $\mathcal{M}_n(\alpha)$ обозначает число строк первой группы. Докажите, что $\lim\limits_{n\to\infty}\frac{1}{n}\log M_n(\alpha)=H$ — скорость передачи информации источника в следующих случаях:

а) строки матрицы переходных вероятностей P равны между собой (т. е. $\{U_j\}$ — последовательность Бернулли),

б) строки матрицы переходных вероятностей P являются перестановками друг друга и в общем случае.

Прокомментируйте значения полученного результата для теории кодирования.

Решение. а) Обозначим через P распределение вероятности н. о. р. последовательности (U_n) и положим $H=-\sum\limits_{j=1}^{m}p_j\log p_j$ (двоичная энтропия источника). Фиксируем $\varepsilon>0$ и разобьём множество $I^{\times n}$ всех n-строчек на три непересекающихся подмножества:

$$K_+=(\mathbf{u}^{(n)}\colon p(\mathbf{u}^{(n)})\geqslant 2^{-n(H-\varepsilon)}),\quad K_-=(\mathbf{u}^{(n)}\colon p(\mathbf{u}^{(n)})\leqslant 2^{-n(H+\varepsilon)})$$

и

$$K=(\mathbf{u}^{(n)}\colon 2^{-n(H+\varepsilon)}<p(\mathbf{u}^{(n)})<2^{-n(H-\varepsilon)}).$$

По закону больших чисел (или а. с. р.) $-\frac{1}{n}\log\mathsf{P}(\mathbf{U}^{(n)})$ сходится к $H(=h)$, т. е. $\lim\limits_{n\to\infty}\mathsf{P}(K_+\cup K_-)=0$ и $\lim\limits_{n\to\infty}\mathsf{P}(K)=1$. Значит, чтобы при достаточно больших n получить вероятность не меньше α, мы (i) не можем ограничится множеством K_+, а должны брать строки из K, (ii) не должны трогать строчки из K_-, т. е. последняя отобранная строка будет из K. Обозначим через

$\mathcal{M}_n(\alpha)$ множество строк, отобранных в первую группу, и пусть $\#\mathcal{M}_n(\alpha) = M_n(\alpha)$. У нас возникают неравенства

$$\alpha \leqslant \mathsf{P}(\mathcal{M}_n(\alpha)) \leqslant \alpha + 2^{-n(H-\varepsilon)}$$

и

$$2^{-n(H+\varepsilon)} M_n(\alpha) \leqslant \mathsf{P}(\mathcal{M}_n(\alpha)) \leqslant \mathsf{P}(K_+) + 2^{-n(H-\varepsilon)} M_n(\alpha).$$

Исключая $\mathsf{P}(\mathcal{M}_n(\alpha))$, получаем

$$2^{-n(H+\varepsilon)} M_n(\alpha) \leqslant \alpha + 2^{-n(H-\varepsilon)} \quad \text{и} \quad 2^{-n(H-\varepsilon)} M_n(\alpha) \geqslant \alpha - \mathsf{P}(K_+),$$

откуда

$$\limsup_{n\to\infty} \frac{1}{n} \log M_n(\alpha) \leqslant H + \varepsilon \quad \text{и} \quad \liminf_{n\to\infty} \frac{1}{n} \log M_n(\alpha) \geqslant H - \varepsilon,$$

а так как ε сколь угодно мало, предел в точности равен H.

б) Рассуждения без изменений можно повторить и в случае перестановок, поскольку упорядочение по убыванию вероятностей даёт то же множество, что и в случае а), а в общем случае нужно применить закон больших чисел к последовательности $\frac{1}{n}\xi_n$ (см. формулы (1.3.3б) и (1.3.19)). Говоря о значении для теории кодирования, отметим, что если мы хотим работать с вероятностью ошибки не больше α, то не нужно кодировать все m^n строчек $\mathbf{u}^{(n)}$, а достаточно закодировать только примерно 2^{nH} из них. Поскольку $H \leqslant \log m$ (а во многих случаях $H \ll \log m$), это даёт значительную экономию машинной памяти (сжатие данных). □

Пример 1.3.21. Двоичный источник генерирует знаки 0 и 1 по следующему правилу:

$$P(X_n = k \,|\, X_{n-1} = j,\, X_{n-2} = i) = q_r,$$

где k, i, j и r принимают значения 0 или 1, причём $r = k - j - i (\mathrm{mod} 2)$ и $q_0 + q_1 = 1$. Найдите скорость передачи информации источника.

Сравните ее со скоростью передачи информации источника Бернулли, генерирующего знаки 0 и 1 с вероятностями q_0 и q_1.

Решение. Источник представляет собой ц. м. д. в. (2) (2-го порядка), т. е. пары составляют ц. м. д. в. с четырьмя состояниями и вероятностями

$$P(00,\,00) = q_0,\ \ P(00,\,01) = q_1,\ \ P(01,\,10) = q_0,\ \ P(01,\,11) = q_1,$$
$$P(10,\,00) = q_0,\ \ P(10,\,01) = q_1,\ \ P(11,\,10) = q_0,\ \ P(11,\,11) = q_1;$$

оставшиеся 8 ячеек матрицы переходных вероятностей равны 0. Откуда следует, что

$$H = -q_0 \log q_0 - q_1 \log q_1.$$

Для источника Бернулли ответ тот же самый. □

Пример 1.3.22. Найдите энтропийную скорость ц. м. д. в., ассоциированной со случайным блужданием по шахматной доске размера 3×3

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}. \tag{1.3.46}$$

Найдите энтропийные скорости ладьи, слона (обоих типов), ферзя и короля.

Решение. Рассмотрим только ц. м. д. в. короля, остальные случаи исследуются аналогично. Матрица переходных вероятностей имеет вид:

$$\begin{pmatrix} 0 & 1/3 & 0 & 1/3 & 1/3 & 0 & 0 & 0 & 0 \\ 1/5 & 0 & 1/5 & 1/5 & 1/5 & 1/5 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 & 1/3 & 1/3 & 0 & 0 & 0 \\ 1/5 & 1/5 & 0 & 0 & 1/5 & 0 & 1/5 & 1/5 & 0 \\ 1/8 & 1/8 & 1/8 & 1/8 & 0 & 1/8 & 1/8 & 1/8 & 1/8 \\ 0 & 1/5 & 1/5 & 0 & 1/5 & 0 & 0 & 1/5 & 1/5 \\ 0 & 0 & 0 & 1/3 & 1/3 & 0 & 0 & 0 & 1/3 \\ 0 & 0 & 0 & 1/5 & 1/5 & 1/5 & 1/5 & 0 & 1/5 \\ 0 & 0 & 0 & 0 & 1/3 & 1/3 & 0 & 1/3 & 0 \end{pmatrix}.$$

Из соображений симметрии находим, что инвариантное распределение должно выглядеть так: $\pi_1 = \pi_3 = \pi_9 = \pi_7 = \lambda$, $\pi_4 = \pi_2 = \pi_6 = \pi_8 = \mu$, $\pi_5 = \nu$, и по уравнениям детального баланса (см. с. 70)

$$\lambda/3 = \mu/5, \quad \lambda/3 = \nu/8, \quad 4\lambda + 4\mu + \nu = 1,$$

откуда $\lambda = 3/40$, $\mu = 1/8$, $\nu = 1/5$. Теперь

$$H = -4\lambda\frac{1}{3}\log\frac{1}{3} - 4\mu\frac{1}{5}\log\frac{1}{5} - \nu\frac{1}{8}\log\frac{1}{8} = \frac{1}{10}\log 15 + \frac{3}{40}. \qquad \square$$

§ 1.4. Каналы передачи информации. Правила декодирования. Вторая теорема

Шеннона о кодировании

> The discussion is suggestive throughout, rather than mathematical, and it is not always clear that the author's mathematical intentions are honorable.
>
> На протяжении всего текста философским рассуждениям уделяется больше времени, чем математике, и не всегда ясна добросовестность автора в том, что касается математики.
>
> *Джозеф Л. Дуб* (1910–2004), американский математик (о некоторых разделах статьи Шеннона)

В этом параграфе мы докажем основные утверждения теории Шеннона: вторую теорему о кодировании для канала с шумами[3] (ВТШК). Шеннон сформулировал свои теоремы и набросал их доказательства в статьях и книге в 1940-х годах. Его аргументы стали предметом (не совсем неоправданной) критики со стороны профессиональных математиков, в частности Дуба (см. эпиграф). Около десяти лет потребовалось математическому сообществу для того, чтобы найти тщательное и полное доказательство ВТШК. Однако с позиций сегодняшнего дня нельзя не восхищаться интуицией Шеннона и его ясным пониманием основных понятий, таких как энтропия и кодирование, и их связью со статистикой длинных случайных строк. Останавливаясь на различных аспектах этой темы, невозможно избежать личностных черт, присущих работам основных специалистов в этой области.

Итак, мы рассмотрели источник, генерирующий случайный текст $U_1U_2\ldots$, и кодирование сообщения $\mathbf{u}^{(n)}$ двоичным кодовым словом $\mathbf{x}^{(N)}$ с помощью кода $f_n\colon I^{\times n}\to J^{\times N}$, $J=\{0,1\}$. Теперь мы сосредоточимся на связи между длиной сообщения n и длиной кодового слова N, что определяется свойствами *канала*, по которому передаётся информация. Важно помнить, что код f_n должен быть известен получателю. Как правило, на канал воздействует «шум», который искажает передаваемые сообщения: сообщение на выходе, вообще говоря, отличается от сообщения на входе. Формально канал характеризуется условным распределением

$$\mathbf{P}_{\rm ch}(\text{получено слово } \mathbf{y}^{(N)}\,|\,\text{передано кодовое слово } \mathbf{x}^{(N)}); \tag{1.4.1}$$

мы вновь предполагаем, что это условное распределение известно как отправителю, так и получателю. (Символ $\mathbf{P}_{\rm ch}(\,\cdot\,|\,\text{передано кодовое слово } \mathbf{x}^{(N)})$, или, короче, $\mathbf{P}_{\rm ch}(\,\cdot\,|\,\mathbf{x}^{(N)})$, используется для того, чтобы подчеркнуть, что это распределение вероятностей зависит от канала.) Говоря далее о каналах,

[3] Noisy Coding theorem.

мы имеем в виду условную вероятность (1.4.1) (или, скорее, семейство распределений, зависящих от N), поэтому используем символ $\mathbf{Y}^{(N)}$ для обозначения случайной строки на выходе канала при условии посланного слова $\mathbf{x}^{(N)}$:

$$\mathbf{P}_{\mathrm{ch}}(\mathbf{Y}^{(N)} = \mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}) = \mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}).$$

Важным примером служат так называемые *двоичные каналы без памяти* (д. к. б. п.):

$$\mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}) = \prod_{i=1}^{N} P(y_i \,|\, x_i), \tag{1.4.2}$$

где $\mathbf{y}^{(N)} = y_1 \ldots y_N$, $\mathbf{x}^{(N)} = x_1 \ldots x_N$. Здесь $P(y\,|\,x)$, $x, y = 0, 1$, является вероятностью канала символ на символ (т. е. условной вероятностью получения символа y на выходе канала при условии посланного символа x). Очевидно, $(P(y|x))$ — это (2×2)-стохастическая матрица (часто называемая *матрицей канала*). В частности, если $P(1\,|\,0) = P(0\,|\,1) = p$, то матрица канала является *симметричной*

$$\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix},$$

а p называют вероятностью ошибочной строки (или вероятностью ошибочного символа).

Пример 1.4.1. Рассмотрим канал без памяти $Y = X + Z$, где аддитивный шум Z принимает значения 0 и a с вероятностью $1/2$, a — данное вещественное число. Пусть $\{0, 1\}$ — входной алфавит и Z не зависит от X.

Свойства такого канала зависят от значения a. Действительно, если $a \neq \pm 1$, то канал поддаётся однозначному декодированию. Другими словами, если нам предстоит использовать канал для передачи сообщений (строк) длины n (их общее количество — 2^n), то любое сообщение можно отправить без кодировки и получатель сможет легко восстановить его. Но если $a = \pm 1$, то возможны ошибки. Поэтому нам придётся кодировать сообщение, чтобы гарантировать, что получатель сможет восстановить его. Это приводит к увеличению длины передаваемой строки от n до, скажем, N. □

Иначе говоря, строки длины N, посылаемые через канал, — это результат кодирования более коротких строк исходного сообщения длины n. Максимальное отношение n/N, при котором ещё остаётся возможность восстановления исходного сообщения, — важная характеристика канала, называемая *пропускной способностью*. Как мы увидим, переход от $a \neq \pm 1$ к $a = \pm 1$ уменьшает пропускную способность с 1 (кодирование не

требуется) до $1/2$ (когда длина кодовых слов в два раза больше длины исходного сообщения). □

Итак, нам нужно использовать такое правило декодирования $\hat{f}_N : J^{\times N} \to \to I^{\times n}$, при котором совокупная вероятность ошибки $\varepsilon = \varepsilon(f_n, \hat{f}_N, \mathsf{P})$, определяемая как

$$\varepsilon = \sum_{\mathbf{u}^{(n)}} \mathsf{P}(\hat{f}_N(\mathbf{Y}^{(N)}) \neq \mathbf{u}^{(n)},\ \mathbf{u}^{(n)} \text{ сгенерировано}) =$$

$$= \sum_{\mathbf{u}^{(n)}} \mathsf{P}(\mathbf{U}^{(n)} = \mathbf{u}^{(n)}) \mathbf{P}_{\mathrm{ch}}(\hat{f}_N(\mathbf{Y}^{(N)}) \neq \mathbf{u}^{(n)} \,|\, f_n(\mathbf{u}^{(n)}) \text{ послано}), \quad (1.4.3)$$

мала. Мы будем пытаться (и при некоторых условиях добьёмся успеха) получить вероятность ошибки (1.4.3), стремящуюся к нулю при $n \to \infty$.

Идея, которая стоит за нашими попытками, основывается на следующих фактах.

1) Для источника с а. с. р. количество различных сгенерированных n-строк равно $2^{n(H+o(1))}$, где $H \leqslant \log m$ — скорость передачи информации источника. Поэтому мы должны кодировать не $m^n = 2^{n \log m}$ сообщений, а только $2^{n(H+o(1))}$, что может оказаться значительно меньше. Тем самым, код f_n может быть определён только на подмножестве $I^{\times n}$ мощности, отвечающей словам длины $N = \lceil nH \rceil$.

2) Можно использовать еще большее N: $N = \lceil \bar{R}^{-1} nH \rceil$, где $\bar{R}$ — константа из интервала (0, 1). Другими словами, увеличение длины кодовых слов с $\lceil nH \rceil$ до $\lceil \bar{R}^{-1} nH \rceil$ позволит ввести избыточность в код f_n, и можно надеяться, что полученная избыточность дает возможность уменьшить общую вероятность ошибки (1.4.3) (при условии «хороших» правил декодирования). При этом естественно минимизировать константу $\bar{R}^{-1}$, т. е. увеличить $\bar{R}$: это даст нам код с оптимальными параметрами. Вопрос о том, насколько большое $\bar{R}$ допустимо, конечно, зависит от канала.

Введем удобные обозначения. Поскольку длина кодового слова является ключевым параметром, мы пишем N вместо $\bar{R}^{-1} Hn$ и $\bar{R}N$ вместо Hn: количество различных строк, генерируемых источником, становится равным $2^{N(\bar{R}+o(1))}$. В дальнейшем индекс $n \sim \dfrac{N\bar{R}}{H}$ будет по возможности опускаться (или иногда заменяться на N). Удобно рассмотреть «типичное» множество $\mathcal{U}_N$ различных строк, генерируемых источником, с $\#\mathcal{U}_N = 2^{N(\bar{R}+o(1))}$. Формально $\mathcal{U}_N$ может включать в себя строки различной длины; нас интересует лишь логарифмическая асимптотика $\#\mathcal{U}_N$. Соответственно будем опускать индекс (n) в обозначении $\mathbf{u}^{(n)}$.

Определение 1.4.2. Величина $\bar{R} \in (0, 1)$ называется *надёжной скоростью передачи* (для данного канала), если в предположении о том, что строки, генерируемые источником, равномерно распределены по мно-

жеству $\mathcal{U}_N$, найдутся правило кодирования $f_N\colon \mathcal{U}_N \to \mathcal{X}_N \subseteq J^{\times N}$ и правило декодирования $\hat{f}_N\colon J^{\times N} \to \mathcal{U}_N$ с вероятностью ошибки

$$\sum_{\mathbf{u}\in\mathcal{U}_N} \frac{1}{\#\mathcal{U}_N} \mathbf{P}_{\mathrm{ch}}(\hat{f}(\mathbf{Y}^{(N)}) \neq \mathbf{u} \,|\, f_N(\mathbf{u}) \text{ послано}), \tag{1.4.4}$$

стремящейся к нулю при $N \to \infty$, т. е. для каждой последовательности $\mathcal{U}_N$ с $\lim\limits_{N\to\infty} \frac{1}{N} \log \#\mathcal{U}_N = \bar{R}$ найдётся такая последовательность правил кодирования $f_N\colon \mathcal{U}_N \to \mathcal{X}_N$, $\mathcal{X}_N \subseteq J^{\times N}$ и такая последовательность правил декодирования $\hat{f}\colon J^{\times N} \to \mathcal{U}_N$, что

$$\lim_{N\to\infty} \frac{1}{\#\mathcal{U}_N} \sum_{\mathbf{u}\in\mathcal{U}_N} \sum_{\mathbf{y}^{(N)}} \mathbf{1}(\hat{f}_N(\mathbf{y}^{(N)}) \neq \mathbf{u}) \mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)} \,|\, f_N(\mathbf{u})) = 0. \tag{1.4.5}$$

Определение 1.4.3. *Пропускная способность канала* определяется как точная верхняя граница

$$C = \sup\left[\bar{R} \in (0,\, 1)\colon \bar{R} \text{ — надёжная скорость передачи}\right]. \tag{1.4.6}$$

□

Замечание 1.4.4. а) С физической точки зрения пропускную способность канала можно представлять себе как предел $\lim\limits_{N\to\infty} \frac{1}{N} \log n(N)$, где $n(N)$ — число строк длины N, которое можно переслать через канал с пренебрежимо малой вероятностью ошибки при декодировании.

б) Причина, по которой на $\mathcal{U}_N$ выбирается равномерное распределение, заключается в том, что это наихудший случай из всех распределений (см. теорему 1.4.6 ниже).

в) Если использовался код f_N без потерь (т. е. f_N — вложение), то для правила декодирования достаточно брать отображение $J^{\times N} \to \mathcal{X}_N$, а не $J^{\times N} \to \mathcal{U}_N$: если мы правильно угадали посланное слово $\mathbf{x}^{(N)}$, то просто положим $\mathbf{u} = f_N^{-1}(\mathbf{x}^{(N)})$. Если, кроме того, распределение источника равномерно на $\mathcal{U}$, то вероятность ошибки ε можно представить как среднее по всем кодовым словам $\mathcal{X}_N$:

$$\varepsilon = \frac{1}{\#\mathcal{X}} \sum_{\mathbf{x}\in\mathcal{X}_N} \mathbf{P}_{\mathrm{ch}}(\hat{f}_N(\mathbf{x}) \neq \mathbf{x} \,|\, \mathbf{x} \text{ послано}).$$

Таким образом, имеет смысл записать $\varepsilon = \varepsilon^{\mathrm{ave}}$ и говорить о средней вероятности ошибки. Другой случай — максимальная вероятность ошибки

$$\varepsilon^{\max} = \max[\mathbf{P}_{\mathrm{ch}}(\hat{f}_N(\mathbf{x}) \neq \mathbf{x} \,|\, \mathbf{x} \text{ послано})\colon \mathbf{x} \in \mathcal{X}_N].$$

Очевидно, $\varepsilon^{\mathrm{ave}} \leqslant \varepsilon^{\max}$. В этом параграфе мы рассматриваем предел при $\varepsilon^{\mathrm{ave}} \to 0$, не останавливаясь на вопросе о пределе при $\varepsilon^{\max} \to 0$. Однако

в § 2.2 мы свяжем задачу оценки $\varepsilon^{\max}$ с аналогичной проблемой для ε^{ave}, и, как следствие, формулы для пропускной способности канала, выведенные в этом параграфе, будут оставаться в силе даже при замене ε^{ave} на $\varepsilon^{\max}$.

Замечание 1.4.5. а) По теореме 1.4.17, сформулированной ниже, пропускная способность двоичного канала без памяти равна

$$C = \sup_{p_X} I(X_k : Y_k). \tag{1.4.7}$$

Здесь $I(X_k : Y_k)$ — взаимная информация между отдельными входными и выходными буквами X_k и Y_k (индекс k может быть опущен), с совместным распределением

$$\mathsf{P}(X = x,\, Y = y) = p_X(x)P(y\,|\,x), \quad x,\, y = 0,\, 1, \tag{1.4.8}$$

где $p_X(x) = \mathsf{P}(X = x)$. Точная верхняя граница в формуле (1.4.7) берётся по всем возможным распределениям $p_X = (p_X(0),\, p_X(1))$. Есть полезная формула: $I(X : Y) = h(Y) - h(Y\,|\,X)$ (см. формулу (1.2.28)). Фактически для двоичного симметричного канала без памяти (д. с. к. б. п.) имеет место формула

$$h(Y\,|\,X) = -\sum_{x=0,1} p_X(x) \sum_{y=0,1} P(y\,|\,x)\log P(y\,|\,x) - \\ - \sum_{y=0,1} P(y\,|\,x)\log P(y\,|\,x) = h_2(p,\,1-p) = \eta_2(p); \tag{1.4.9}$$

для краткости нижний индекс 2 будет опускаться. Следовательно, $h(Y\,|\,X) = \eta(p)$ не зависит от входного распределения p_X, и для д. с. к. б. п. получаем

$$C = \sup_{p_X} h(Y) - \eta(p). \tag{1.4.10}$$

Но $\sup\limits_{p_X} h(Y)$ равен $\log 2 = 1$: он достигается при $p_X(0) = p_X(1) = 1/2$, и для д. с. к. б. п. с вероятностью ошибочной строки p имеем

$$C = 1 - \eta(p). \tag{1.4.11}$$

б) Предположим, что источник $U_1U_2\ldots$ имеет а. с. р. и скорость передачи информации H. Для пересылки текста, сгенерированного этим источником, через канал с пропускной способностью C нам нужно закодировать сообщения длины n кодовыми словами длины $\dfrac{n(H+\varepsilon)}{C}$, чтобы предел суммарной ошибки был равен 0 при $n \to \infty$. Значение ε можно выбирать сколь угодно маленьким. Значит, если $H/C < 1$, то текст можно кодировать с большей скоростью, чем он генерируется: в этом случае

канал надёжно передаёт информацию от данного источника. С другой стороны, если $H/C > 1$, то текст генерируется быстрее, чем мы можем его закодировать и надёжно переслать его по каналу. В такой ситуации надёжная передача невозможна. Для источников Бернулли или стационарного марковского и д. с. к. б. п. условие $H/C < 1$ равносильно тому, что $h(U) + \eta(p) < 1$ или $h(U_{n+1}\,|\,U_n) + \eta(p) < 1$ соответственно. □

Как видно из эпиграфа к этому параграфу, идеи Шеннона ведущими математиками того времени воспринимались с большим трудом. Интересно посмотреть на мнение ведущих учёных, которые могли бы считаться «создателями» теории информации.

> Professor Doob... took the strict view of proofs and... doubted, in his Math Review, Shannon's mathematical integrity!
> Профессор Дуб... продемонстрировал строгий подход к доказательствам и... указывал в обзоре в «Математическом обозрении», что добросовестность Шеннона как математика вызывает сомнения!
>
> *Ричард Хэмминг* (1915–1998),
> американский математик и программист

Теорема 1.4.6. *Фиксируем канал* (*т. е. условную вероятность* $\mathbf{P}_{\mathrm{ch}}$ *в формуле* (1.4.1)) *и множество* $\mathcal{U}$ *строк источника и обозначим через* $\varepsilon(\mathsf{P})$ *общую вероятность ошибки* (1.4.3) *для* $\mathbf{U}^{(n)}$ *с распределением вероятностей* P *на* $\mathcal{U}$, *минимальную среди всех правил кодирования и декодирования. Тогда*

$$\varepsilon(\mathsf{P}) \leqslant \varepsilon(\mathsf{P}^0), \tag{1.4.12}$$

где $\varepsilon(\mathsf{P}^0)$ *— равномерное распределение на* $\mathcal{U}$.

Доказательство. Зафиксируем правила кодирования и декодирования f и $\hat{f}$ и предположим, что вероятность строки $\mathbf{u} \in \mathcal{U}$ равна $\mathsf{P}(\mathbf{u})$. Определим вероятность ошибки для сгенерированной строки $\mathbf{u}$ как

$$\beta(\mathbf{u}) := \sum_{\mathbf{y}:\ \hat{f}(\mathbf{y}) \neq \mathbf{u}} \mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,f(\mathbf{u})).$$

Общая вероятность ошибки тогда равна

$$\varepsilon(= \varepsilon(\mathsf{P}, f, \hat{f})) = \sum_{\mathbf{u} \in \mathcal{U}} \mathsf{P}(\mathbf{u})\beta(\mathbf{u}).$$

Если переставить кодовые слова (т. е. закодировать $\mathbf{u}$ как $f(\mathbf{u}')$, где $\mathbf{u}' = \lambda(\mathbf{u})$ и λ — перестановка степени $\#\mathcal{U}$), то общая вероятность ошибки запишется как $\varepsilon(\lambda) = \sum\limits_{\mathbf{u} \in \mathcal{U}} \mathsf{P}(\mathbf{u})\beta(\lambda(\mathbf{u}))$. В случае $\mathsf{P}(\mathbf{u}) = (\#\mathcal{U})^{-1}$ (равномер-

ное распределение) $\varepsilon(\lambda)$ не будет зависеть от λ и не будет равна

$$\bar{\varepsilon} = \frac{1}{\#\mathcal{U}} \sum_{\mathbf{u}\in\mathcal{U}} \beta(\mathbf{u}) \ (= \varepsilon(\mathsf{P}^0, f, \hat{f})).$$

Ясно, что для каждого распределения вероятностей $(\mathsf{P}(\mathbf{u}),\ \mathbf{u}\in\mathcal{U})$ найдётся такая перестановка λ, что $\varepsilon(\lambda) \leqslant \bar{\varepsilon}$. Действительно, можно взять *случайную* перестановку Λ, равномерно распределённую среди всех перестановок степени $\#\mathcal{U}$. Тогда

$$\min_{\lambda} \varepsilon(\lambda) \leqslant \mathsf{E}\varepsilon(\Lambda) = \mathsf{E} \sum_{\mathbf{u}\in\mathcal{U}} \mathsf{P}(\mathbf{u})\beta(\Lambda\mathbf{u}) =$$
$$= \sum_{\mathbf{u}\in\mathcal{U}} \mathsf{P}(\mathbf{u})\, \mathsf{E}\beta(\Lambda\mathbf{u}) = \sum_{\mathbf{u}\in\mathcal{U}} \mathsf{P}(\mathbf{u}) \frac{1}{\#\mathcal{U}} \sum_{\mathbf{u}\in\mathcal{U}} \beta(\bar{u}) = \bar{\varepsilon}.$$

Итак, для любой пары f и $\hat{f}$ можно найти новые правила кодирования и декодирования с общей вероятностью ошибки не превосходит $\varepsilon(\mathsf{P}^0, f, \hat{f})$. Поэтому минимизация ошибки по всем f и $\hat{f}$ приводит к неравенству (1.4.12). □

Пример 1.4.7. Пусть с. в. X и Y, принимающие значения в конечных алфавитах I и J, представляют соответственно вход и выход канала передач с условной вероятностью $P(x\,|\,y) = \mathsf{P}(X = x\,|\,Y = y)$. Пусть $h(P(\cdot\,|\,y))$ обозначает энтропию условного распределения $P(\cdot\,|\,y)$, $y \in J$:

$$h(P(\cdot\,|\,y)) = -\sum_{x} P(x\,|\,y) \log P(x\,|\,y).$$

Пусть $h(X\,|\,Y)$ обозначает условную энтропию с. в. X при данной с. в. Y. Определим правило декодирования *идеального наблюдателя* как такое отображение $f^{\mathrm{IO}}: J \to I$, при котором $P(f(y)\,|\,y) = \max\limits_{x\in I} P(x\,|\,y)$ для всех $y \in J$. Покажите, что а) при таком правиле вероятность ошибки

$$\pi_{\mathrm{er}}^{\mathrm{IO}}(y) = \sum_{x\in I} \mathbf{1}(x \neq f(y)) P(x\,|\,y)$$

удовлетворяет неравенству $\pi_{\mathrm{er}}^{\mathrm{IO}}(y) \leqslant \frac{1}{2} h(P(\cdot\,|\,y))$ и б) математическое ожидание вероятности ошибки подчиняется неравенству $\mathsf{E}\pi_{\mathrm{er}}^{\mathrm{IO}}(y) \leqslant \frac{1}{2} h(X\,|\,Y)$.

Решение. Действительно, а) следует из п. (iii) примера 1.2.7, так как

$$\pi_{\mathrm{er}}^{\mathrm{IO}} = 1 - P(f(y)\,|\,y) = 1 - P_{\max}(\cdot\,|\,y) \leqslant \frac{1}{2} h(P(\cdot\,|\,y)).$$

Наконец, б) вытекает из а), если среднее вычислять как $h(X\,|\,Y) = \mathsf{E}h(P(\cdot\,|\,Y))$. □

Как было отмечено ранее, общее *правило декодирования* (или *декодер*) — это отображение $\hat{f}_N\colon J^{\times N}\to\mathcal{U}_N$; для кода f_N без потерь $\hat{f}_N$ — это отображение $J^{\times N}\to\mathcal{X}_N$. Здесь $\mathcal{X}$ — множество кодовых слов. Иногда удобно правило декодирования для каждого кодового слова $\mathbf{x}^{(N)}$ отождествлять с таким множеством $A(\mathbf{x}^{(N)})\subset J^{\times N}$, что $A(\mathbf{x}_1^{(N)})$ и $A(\mathbf{x}_2^{(N)})$ не пересекаются при $\mathbf{x}_1^{(N)}\neq\mathbf{x}_2^{(N)}$, а объединение $\bigcup\limits_{\mathbf{x}^{(N)}\in\mathcal{X}_N} A(\mathbf{x}^{(N)})$ даёт всё $J^{\times N}$. Тогда, получив $\mathbf{y}^{(N)}\in A(\mathbf{x}^{(N)})$, мы декодируем его как $\hat{f}_N(\mathbf{y}^{(N)})=\mathbf{x}^{(N)}$.

Хотя в определении пропускной способности канала мы предполагаем равномерное распределение сообщений источника (как отмечалось, это наихудший случай в смысле теоремы 1.4.6), в реальности, конечно, источник не всегда обладает этим свойством. В этой связи мы проанализируем два случая: (i) получатель знает вероятности

$$p(\mathbf{u})=\mathsf{P}(\mathbf{U}=\mathbf{u}) \tag{1.4.13}$$

строк источника (и, следовательно, распределение вероятностей $p_N(\mathbf{x}^{(N)})$ кодовых слов $\mathbf{x}^{(N)}\in\mathcal{X}_N$) и (ii) получатель не знает $p_N(\mathbf{x}^{(N)})$. В зависимости от ситуации возникают два естественных правила декодирования:

(i) правило декодирования «*идеальный наблюдатель*»(и. н.) декодирует полученное слово $\mathbf{y}^{(N)}$ как кодовое слово $\mathbf{x}^{(N)*}$, максимизирующее апостериорную вероятность

$$\mathsf{P}(\mathbf{x}^{(N)}\text{ послано }|\,\mathbf{y}^{(N)}\text{ получено})=\frac{p_N(\mathbf{x}^{(N)})\mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)}\,|\,\mathbf{x}^{(N)})}{p_{\mathbf{Y}^{(N)}}(\mathbf{y}^{(N)})}, \tag{1.4.14}$$

где

$$p_{\mathbf{Y}^{(N)}}(\mathbf{y}^{(N)})=\sum_{\tilde{\mathbf{x}}^{(N)}\in\mathcal{X}_N} p_N(\tilde{x}^{(N)})\mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)}\,|\,\mathbf{x}^{(N)});$$

(ii) правило декодирования «*максимальное правдоподобие*» (м. п.) декодирует полученное слово $\mathbf{y}^{(N)}$ кодовым словом $\mathbf{x}_*^{(N)}$, которое максимизирует априорную вероятность

$$\mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)}\,|\,\mathbf{x}^{(N)}). \tag{1.4.15}$$

Теорема 1.4.8. *Предположим, что правило кодирования f определено для всех сообщений, которые генерируются с положительной вероятностью, причём f — вложение. Тогда*

а) для любого правила кодирования правило декодирования и. н. минимизирует общую вероятность ошибки по всем правилам декодирования;

б) если сообщение U получено из источника с равномерным распределением на множестве $\mathcal{U}$, то для любого правила кодирования

$f\colon \mathcal{U} \to \mathcal{X}_N$ случайное слово $\mathbf{X}^{(N)} = f(\mathbf{U})$ равномерно распределено на $\mathcal{X}_N$; при этом правила декодирования и. н. и м. п. совпадают.

Доказательство. Вновь будем опускать верхний индекс (N).

а) Заметим, что, получив слово $\mathbf{y}$, правило и. н., очевидно, максимизирует совместную вероятность $p(\mathbf{x})\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\mathbf{x})$ (знаменатель в формуле (1.4.14) фиксирован при фиксированном слове $\mathbf{y}$). При использовании правил кодирования f и декодирования $\hat{f}$ общая вероятность ошибки (см. формулу (1.4.3)) составит

$$\sum_{\mathbf{u}} \mathsf{P}(\mathbf{U}=\mathbf{u})\mathbf{P}_{\mathrm{ch}}(\hat{f}(\mathbf{y}) \neq \mathbf{u}\,|\,f(\mathbf{u}) \text{ послано}) =$$

$$= \sum_{\mathbf{x}} p(\mathbf{x}) \sum_{\mathbf{y}} \mathbf{1}(\hat{f}(\mathbf{y}) \neq \mathbf{x})\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\mathbf{x}) = \sum_{\mathbf{y}}\sum_{\mathbf{x}} \mathbf{1}(\mathbf{x} \neq \hat{f}(\mathbf{y}))p(\mathbf{x})\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\mathbf{x}) =$$

$$= \sum_{\mathbf{y}}\sum_{\mathbf{x}} p(\mathbf{x})\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\mathbf{x}) - \sum_{\mathbf{y}} p(\hat{f}(\mathbf{y}))\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\hat{f}(\mathbf{y})) = 1 - \sum_{\mathbf{y}} p(\hat{f}(\mathbf{y}))\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\hat{f}(\mathbf{y})).$$

Остаётся заметить, что каждое слагаемое суммы $\sum_{\mathbf{y}} p(\hat{f}(\mathbf{y}))\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\hat{f}(\mathbf{y}))$ максимально, если $\hat{f}$ совпадает с правилом и. н. Следовательно, и вся сумма максимальна, а общая вероятность ошибки минимальна.

б) Первое утверждение очевидно, как, несомненно, и второе. □

Предположив в определении пропускной способности канала равномерное распределение сообщений источника, естественно далее использовать правило декодирования м. п. При этом ошибки могут возникать либо потому, что декодер выбрал неправильное кодовое слово $\mathbf{x}$, либо из-за того, что применяемый код f не был вложением. Вероятность этих событий оценивается в лемме 1.4.9. Для простоты далее мы будем писать $\mathbf{P}$ вместо $\mathbf{P}_{\mathrm{ch}}$, а символом P будем обозначать совместное входное/выходное распределение.

Лемма 1.4.9. *Если сообщения источника равномерно распределены по $\mathcal{U}$, то при использовании декодера м. п. и правила кодирования f общая вероятность ошибки удовлетворяет неравенству*

$$\varepsilon(f) \leqslant \frac{1}{\#\mathcal{U}} \sum_{\mathbf{u}\in\mathcal{U}} \sum_{\mathbf{u}'\in\mathcal{U}:\mathbf{u}'\neq\mathbf{u}} \mathsf{P}(\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}')) \geqslant \mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u})\,|\,\mathbf{U}=\mathbf{u}). \tag{1.4.16}$$

Доказательство. Если источник генерирует $\mathbf{u}$ и используется декодер м. п., мы получаем а) ошибку, когда $\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}')) > \mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}))$ для некоторого $\mathbf{u}' \neq \mathbf{u}$, б) возможно, ошибку, когда $\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}')) = \mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}))$ для некоторого $\mathbf{u}' \neq \mathbf{u}$ (сюда входит случай, когда $f(\mathbf{u}) = f(\mathbf{u}')$), и, наконец, в) отсутствие ошибок, когда $\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}')) < \mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}))$ для любых $\mathbf{u}' \neq \mathbf{u}$. Таким

образом, вероятность $\mathsf{P}(\text{ошибка}\,|\,\mathbf{U}=\mathbf{u})$ не превосходит

$$\mathsf{P}\big(\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}'))\geqslant\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}))\text{ для некоторого }\mathbf{u}'\neq\mathbf{u}\,|\,\mathbf{U}=\mathbf{u}\big)\leqslant$$
$$\leqslant\sum_{\mathbf{u}'\in\mathcal{U}}\mathbf{1}(\mathbf{u}'\neq\mathbf{u})\,\mathsf{P}\big(\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}'))\geqslant\mathbf{P}(\mathbf{Y}\,|\,f(\mathbf{u}))\;\big|\;\mathbf{U}=\mathbf{u}\big).$$

Умножив это неравенство на $\dfrac{1}{\#\mathcal{U}}$ и просуммировав по $\mathbf{u}$, получим требуемый результат. □

Замечание 1.4.10. Ограничение (1.4.16), конечно, сохранится при любом распределении $p(\mathbf{u})=\mathsf{P}(\mathbf{U}=\mathbf{u})$, если заменить $\dfrac{1}{\#\mathcal{U}}$ на $p(\mathbf{u})$.

Как отмечалось, случайное кодирование — полезный инструмент наряду с детерминированным кодированием. Детерминированное правило кодирования — это отображение $f\colon\mathcal{U}\to J^{\times N}$; если $\#\mathcal{U}=r$, то f можно интерпретировать как набор кодовых слов $(f(\mathbf{u}_1),\ldots,f(\mathbf{u}_r))$, или, что то же самое, мегастрочку (или кодовую книгу)

$$f(\mathbf{u}_1)\ldots f(\mathbf{u}_r)\in(J^{\times N})^{\times r}=\{0,\,1\}^{\times Nr}.$$

Здесь $\mathbf{u}_1,\ldots,\mathbf{u}_r$ — строки источника (не буквы!), составляющие множество $\mathcal{U}$. Если f — код без потерь, то $f(\mathbf{u}_i)\neq f(\mathbf{u}_j)$ при $i\neq j$. Случайное правило кодирования — это случайный элемент F из $(J^{\times N})^r$ с вероятностью $\mathsf{P}(F=f)$, $f\in(J^{\times N})^r$. С другой стороны, F можно рассматривать как набор случайных кодовых слов $F(\mathbf{u}_i)$, $i=1,\ldots,r$, или, что то же самое, как случайную кодовую книгу

$$F(\mathbf{u}_1)F(\mathbf{u}_2)\ldots F(\mathbf{u}_r)\in\{0,\,1\}^{Nr}.$$

Типичный пример — это независимые кодовые слова $F(\mathbf{u}_1)$, $F(\mathbf{u}_2)$, $\ldots$, $F(\mathbf{u}_r)$, для которых случайные символы $W_{i1},\ldots,W_{iN}$, составляющие слово $F(\mathbf{u}_i)$, тоже независимы.

Вот причины, по которым рассматривается случайное кодирование:

1^0 существование «хорошего» детерминированного кода часто следует из существования хорошего случайного кода;

2^0 вычисления для случайного кода, как правило, легче, чем для оптимального детерминированного, поскольку дискретная оптимизация заменяется оптимизацией по распределениям вероятностей.

Идея случайного кодирования восходит к Шеннону. Как это часто случается в истории математики, блестящие идеи, решая одну задачу, открывают ящик Пандоры других вопросов.

В нашем случае специфическая проблема, возникшая после привлечения случайного кодирования, состояла в поиске «хорошего» не случайного

кода. Бóльшая часть современных теорий информации и кодирования вращается вокруг этой проблемы, но до сих пор не было найдено общего удовлетворительного решения. Однако был достигнут ряд замечательных результатов, некоторые из них обсуждаются в этой книге.

Проводя вычисления со случайным кодом, выпишем математическое ожидание вероятности ошибки для случайного правила кодирования F:

$$E := \mathcal{E}\varepsilon(F) = \sum_f \varepsilon(f)\mathcal{P}(F = f). \tag{1.4.17}$$

Теорема 1.4.11. (*i*) *Существует такое детерминированное правило кодирования* f, *что* $\varepsilon(f) \leqslant E$.

(*ii*) *Для любого* $\rho \in (0, 1)$ *справедливо неравенство* $\mathcal{P}\left(\varepsilon(F) < \right.$ $\left. < \dfrac{E}{1-\rho}\right) \geqslant \rho$.

Доказательство. (i) очевидно. Для доказательства (ii) используем неравенство Чебышёва (см. т. 1, с. 103): $\mathcal{P}\left(\varepsilon(F) \geqslant \dfrac{E}{1-\rho}\right) \leqslant \dfrac{1-\rho}{E}E = 1 - \rho$. □

Определение 1.4.12. Для случайных слов $\mathbf{X}^{(N)} = X_1 \dots X_N$ и $\mathbf{Y}^{(N)} = Y_1 \dots Y_N$ определим

$$C_N := \sup\left[\frac{1}{N} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \text{ по всем входным распределениям вероятностей } P_{\mathbf{X}^{(N)}}\right]. \tag{1.4.18}$$

Напомним, что $I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})$ — взаимная энтропия, задаваемая формулой

$$h(\mathbf{X}^{(N)}) - h(\mathbf{X}^{(N)} \,|\, \mathbf{Y}^{(N)}) = h(\mathbf{Y}^{(N)}) - h(\mathbf{Y}^{(N)} \,|\, \mathbf{X}^{(N)}). \qquad \square$$

Замечание 1.4.13. Простое эвристическое рассуждение (которое будет строго обосновано в § 2.2) показывает, что пропускная способность канала не может превышать взаимную информацию между входом и выходом канала. Действительно, для каждой типичной входной N-последовательности существуют приблизительно $2^{h(\mathbf{Y}^{(N)} \,|\, \mathbf{X}^{(N)})}$ возможных последовательностей $\mathbf{Y}^{(N)}$, которые равновероятны. Мы не сможем определить, какая последовательность $\mathbf{X}$ была послана, если найдутся две последовательности $\mathbf{X}^{(N)}$ и $\mathbf{X}'^{(N)}$, при которых получается тот же самый выход $\mathbf{Y}^{(N)}$. Всего типичных последовательностей $\mathbf{Y}^{(N)}$ насчитывается $2^{h(\mathbf{Y}^{(N)})}$. Это множество должно быть разбито на подмножества размера $2^{h(\mathbf{Y}^{(N)} \,|\, \mathbf{X}^{(N)})}$, соответствующие различным входным последовательностям $\mathbf{X}^{(N)}$. Общее число непересекающихся подмножеств не превосходит

$$2^{h(\mathbf{Y}^{(N)}) - h(\mathbf{Y}^{(N)} \,|\, \mathbf{X}^{(N)})} = 2^{I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})}.$$

Следовательно, общее число отличающихся друг от друга сигналов длины N не может превышать $2^{I(\mathbf{X}^{(N)}:\mathbf{Y}^{(N)})}$.

Если несколько изменить те же рассуждения, то можно сказать, что количество типичных последовательностей $\mathbf{X}^{(N)}$ — $2^{h(\mathbf{X}^{(N)})}$. Однако есть только $2^{h(\mathbf{Y}^{(N)}\,|\,\mathbf{X}^{(N)})}$ *совместно типичных* последовательностей $(\mathbf{X}^{(N)}, \mathbf{Y}^{(N)})$. Таким образом, вероятность того, что любая произвольно выбранная пара совместно типична, приблизительно равна $2^{-I(\mathbf{X}^{(N)}:\mathbf{Y}^{(N)})}$. Поэтому число отличающихся друг от друга сигналов ограничено величиной $2^{h(\mathbf{Y}^{(N)})-h(\mathbf{Y}^{(N)}\,|\,\mathbf{X}^{(N)})}$. □

Теорема 1.4.14 (вторая теорема Шеннона о кодировании: обратная часть). *Пропускная способность канала C удовлетворяет неравенству*

$$C \leqslant \limsup_{N\to\infty} C_N. \tag{1.4.19}$$

Доказательство. Рассмотрим код $f(=f_N)\colon \mathcal{U}_N \to \mathcal{X}_N \subseteq J^{\times N}$, где $\#\mathcal{U}_N = 2^{N(\bar{R}+o(1))}$, $\bar{R} \in (0,\,1)$. Мы хотим доказать, что для любого правила декодирования справедливо неравенство

$$\varepsilon(f) \geqslant 1 - \frac{C_N + o(1)}{\bar{R} + o(1)}. \tag{1.4.20}$$

Утверждение теоремы немедленно следует из неравенства (1.4.20) и определения пропускной способности канала, поскольку

$$\liminf_{N\to\infty} \varepsilon(f) \geqslant 1 - \frac{1}{\bar{R}} \limsup_{N\to\infty} C_N,$$

а эта величина положительна, когда $\bar{R} > \limsup\limits_{N\to\infty} C_N$.

Проверим неравенство (1.4.20) для вложения f (для общего кода $\varepsilon(f)$ даже больше). В этом случае кодовые слова $\mathbf{X}^{(N)} = f(\mathbf{U})$ равномерно распределены, если так распределены строки $\mathbf{U}$. Если $\hat{f}\colon J^{\times N} \to \mathcal{X}$ — правило декодирования, то для достаточно больших N получаем

$$\begin{aligned} NC_N \geqslant I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \geqslant I(\mathbf{X}^{(N)} : \hat{f}(\mathbf{Y}^{(N)})) \quad &\text{(см. теорему 1.2.6)} \ = \\ = h(\mathbf{X}^{(N)}) - h(\mathbf{X}^{(N)}\,|\,\hat{f}(\mathbf{Y}^{(N)})) &= \log r - h(\mathbf{X}^{(N)}\,|\,\hat{f}(\mathbf{Y}^{(N)})) \\ \text{из-за равномерной распределённости} &\geqslant \log r - \varepsilon(f)\log(r-1) - 1. \end{aligned}$$

Здесь и далее $r = \#\mathcal{U}$. Последнее ограничение следует из обобщённого неравенства Фано (1.2.25). Действительно, заметим, что (случайное) кодовое слово $\mathbf{X}^{(N)} = f(\mathbf{U})$ принимает r значений $\mathbf{x}_1^{(N)}, \ldots, \mathbf{x}_r^{(N)}$ из множества кодовых слов $\mathcal{X}(=\mathcal{X}_N)$, и вероятность ошибки равна

$$\varepsilon(f) = \sum_{i=1}^{r} \mathsf{P}\left(\mathbf{X}^{(N)} = x_i^{(N)},\, \hat{f}(\mathbf{Y}^{(N)}) \neq x_i^{(N)}\right).$$

Итак, из неравенства (1.2.25) следует, что

$$h\big(\mathbf{X}^{(N)} \,|\, \hat{f}(\mathbf{Y}^{(N)})\big) \leqslant \eta(\varepsilon) + \varepsilon \log(r-1) \leqslant 1 + \varepsilon(f) \log(r-1),$$

и мы получаем неравенство $NC_N \geqslant \log r - \varepsilon(f)\log(r-1) - 1$. Наконец, $r = 2^{N(\bar{R}+o(1))}$, и

$$NC_N \geqslant N(\bar{R} + o(1)) - \varepsilon(f) \log(2^{N(\bar{R}+o(1))} - 1),$$

т. е.

$$\varepsilon(f) \geqslant \frac{N(\bar{R} + o(1)) - NC_N}{\log(2^{N(\bar{R}+o(1))} - 1)} = 1 - \frac{C_N + o(1)}{\bar{R} + o(1)}. \qquad \square$$

Пусть $\mathbf{X}^{(N)}$ и $\mathbf{Y}^{(N)}$ — случайные слова на входе и выходе канала, $p_N(\mathbf{X}^{(N)})$ и $p_N(\mathbf{Y}^{(N)})$ — их вероятности, а $p(\mathbf{X}^{(N)}, \mathbf{Y}^{(N)})$ — совместная вероятность пары $(\mathbf{X}^{(N)}, \mathbf{Y}^{(N)})$.

Теорема 1.4.15 (вторая теорема Шеннона о кодировании: прямая часть). *Пусть можно найти такую константу $c \in (0, 1)$, что для любых $\bar{R} \in (0, c)$ и $N \geqslant 1$ существует кодирование $F(\mathbf{u}_1), \ldots, F(\mathbf{u}_r)$, где $r = 2^{N(\bar{R}+o(1))}$, с н.о.р. кодовыми словами $F(\mathbf{u}_i) \in J^{\times N}$, для которой взаимная информация между случайными входом и выходом*

$$\Theta_N := \frac{1}{N} \log \frac{p(\mathbf{X}^{(N)}, \mathbf{Y}^{(N)})}{p_X(\mathbf{X}^{(N)}) p_Y(\mathbf{Y}^{(N)})} \tag{1.4.21}$$

сходится по вероятности к c при $N \to \infty$. Тогда пропускная способность канала удовлетворяет оценке $C \geqslant c$.

Доказательство теоремы 1.4.15 приведено после примеров 1.4.24 и 1.4.25 (последний скорее технический, нежели сложный). Для начала мы объясним стратегию доказательства, набросок которого Шеннон дал в своей статье 1948 года. (Понадобилось около 10 лет на то, чтобы его идея трансформировалась в строгое рассуждение.)

Прежде всего генерируем случайную кодовую книгу $\mathcal{X}$, состоящую из $r = 2^{\lceil NR \rceil}$ слов $\mathbf{X}^{(N)}(1), \ldots, \mathbf{X}^{(N)}(r)$. Предполагается, что кодовые слова $\mathbf{X}^{(N)}(1), \ldots, \mathbf{X}^{(N)}(r)$ известны как отправителю, так и получателю, так же как и матрица переходов канала $\mathbf{P}_{\mathrm{ch}}(\mathbf{y}\,|\,\mathbf{x})$. Затем выбирается сообщение в соответствии с равномерным распределением и соответствующее кодовое слово пересылается по каналу. Получатель использует декодер максимального правдоподобия, т. е. выбирает апостериорно наиболее вероятное сообщение. Но эта процедура сложна для анализа. Вместо этого используется субоптимальный, но простой декодер, основанный на совместной типичности сообщений. Получатель заявляет, что было послано сообщение w, если есть только один такой вход, что кодовое слово для w и выход канала будут совместно типичны. Если такого слова нет или

оно не единственное, то объявляется об ошибке. Удивительно, что эта процедура является асимптотически оптимальной. Наконец, из существования хорошей случайной кодовой книги следует существование хорошего неслучайного кодирования.

Другими словами, пропускная способность канала C — это в точности точная верхняя граница значений c, для которых имеет место сходимость по вероятности (1.4.21) для подходящего случайного кодирования.

Следствие 1.4.16. *Если c — константа из теоремы* 1.4.13, *то имеет место неравенство*

$$\sup c \leqslant C \leqslant \limsup_{N\to\infty} C_N. \tag{1.4.22}$$

Таким образом, при совпадении л. ч. и п. ч. неравенства (1.4.22) *их общее значение даст пропускную способность канала.*

Далее, опираясь на вторую теорему Шеннона о кодировании, вычислим пропускную способность двоичного канала без памяти. Напомним (см. формулу (1.4.2)), что для этого канала

$$\mathbf{P}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}) = \prod_{i=1}^{N} P(y_i \,|\, x_i). \tag{1.4.23}$$

Теорема 1.4.17. *Для двоичного канала без памяти*

$$I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \leqslant \sum_{j=1}^{N} I(X_j : Y_j), \tag{1.4.24}$$

где равенство достигается, если входные символы $X_1, \ldots, X_N$ независимы.

Доказательство. Ввиду равенства $\mathbf{P}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}) = \prod_{j=1}^{N} P(y_j \,|\, x_j)$ условная энтропия $h(\mathbf{Y}^{(N)} \,|\, \mathbf{X}^{(N)})$ вычисляется как сумма $\sum\limits_{j=1}^{N} h(Y_j \,|\, X_j)$. Следовательно, взаимная информация подчиняется неравенству

$$I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) = h(\mathbf{Y}^{(N)}) - h(\mathbf{Y}^{(N)} \,|\, \mathbf{X}^{(N)}) = h(\mathbf{Y}^{(N)}) - \sum_{1\leqslant j\leqslant N} h(Y_j \,|\, X_j) \leqslant$$

$$\leqslant \sum_{j} (h(Y_j) - h(Y_j \,|\, X_j)) = \sum_{j} I(X_j : Y_j).$$

Равенство достигается тогда и только тогда, когда $Y_1, \ldots, Y_N$ независимы. Но они независимы, если независимы с. в. $X_1, \ldots, X_N$. □

Замечание 1.4.18. Ср. неравенства (1.4.24) и (1.2.27). В силу неравенства (1.2.27) имеем $h(\mathbf{X}^{(N)}\,|\,\mathbf{Y}^{(N)}) \leqslant \sum\limits_{j=1}^{N} h(Y_j\,|\,X_j)$, но для д. к. б. п. имеет место равенство, а $h(\mathbf{X}^{(N)}) \leqslant \sum\limits_{j=1}^{N} h(X_j)$. □

> Значение работ Шеннона для ... математики не было сразу понято... На Международном Математическом конгрессе (1954 г.) мои американские коллеги, специалисты по теории вероятностей, считали мой интерес к его работам ... преувеличенным, поскольку в них было больше техники, чем математики. В настоящее время такую точку зрения не стоит и опровергать. Это верно... в каждом сложном случае Шеннон оставил задачу «строгого» обоснования его идеи для последователей. Однако его математическая интуиция удивительно точна.
>
> *Андрей Колмогоров* (1903–1987),
> советский математик

Многие работы Шеннона были переведены на различные иностранные языки. Пожалуй, наиболее исчерпывающая работа выполнена русскими учеными, которые уже давно заинтересовались теорией информации и компьютерами и внесли большой вклад в эти области. В 1963 г. Шеннон получил три копии 830-страничных переводов его научных работ на русский язык. В 1964 г. во время его визита в Россию ему сообщили о том, что авторский гонорар его книги составил несколько тысяч рублей, которые обменивались на примерно такое же количество долларов. К сожалению, там была ловушка — деньги нельзя было вывезти из страны, их нужно было тратить в России. Любопытно, что ничего из того, что Шеннон мог бы купить, не казалось ему подходящим. Книги были на русском языке, у его жены Бетти уже была шуба, мебель трудно было транспортировать. Они наконец остановились на восьми музыкальных инструментах, начиная от фагота и заканчивая балалайкой. На обратном пути Шеннонов многие принимали за путешествующий оркестр. Шеннон играл на кларнете и очень любил музыку, особенно диксиленд, популярный во времена его молодости. Он также любил поэзию, особенно Т. С. Элиота, Рубаи и Огдена Нэша, и было известно, что Шеннон время от времени сам писал (не очень серьезные) стихи.

В свободное время Шеннон, в дополнение к упомянутым выше увлечениям, занимался и своим здоровьем. Он предпринимал ежедневные прогулки длиной в милю или две, и увлекался таким видом спорта, как жонглирование, требующим хорошей координации. Как-то на Рождество Бетти, зная его пристрастия, подарила ему одноколесный велосипед. В течение нескольких дней он ездил вокруг квартала; а уже через несколько недель смог при движении на этом велосипеде жонглировать тремя шарами. В течение нескольких месяцев он сконструировал необычные велосипеды, такие как, например, с эксцентричным колесом (велосипедист при движении велосипеда вперёд перемещается вверх и вниз). Он с удовольствием отвечал на любой новой интеллектуальный вызов, например разработал машину для решения головоломки «кубик Рубика».

Теорема 1.4.19. *Пропускная способность двоичного канала без памяти составляет*

$$C = \sup_{p_{X_1}} I(X_1 : Y_1). \tag{1.4.25}$$

Точная верхняя граница берётся по всем возможным распределениям p_{X_1} символа X_1.

Доказательство. По определению C_N величина NC_N не превышает границы

$$\sup_{p_X} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \leqslant \sum_j \sup_{p_{X_1}} I(X_j : Y_j) = N \sup_{p_{X_j}} I(X_1 : Y_1).$$

Таким образом, по второй теореме Шеннона (обратная часть) имеем

$$C \leqslant \limsup_{N\to\infty} C_N \leqslant \sup_{p_{X_1}} I(X_1 : Y_1).$$

С другой стороны, возьмём случайное кодирование F с кодовыми словами $F(\mathbf{u}_l) = V_{l_1} \dots V_{l_N}$, $1 \leqslant l \leqslant r$, содержащими н. о. р. символы V_{l_j} с распределением p^*, максимизирующим взаимную информацию $I(X_1 : Y_1)$. (Такое случайное кодирование определяется *для любого* r, т. е. для любого $\bar{R}$ (даже для $\bar{R} > 1$!).) Для этого случайного кодирования (случайная) взаимная энтропия Θ_N равна

$$\frac{1}{N} \log \frac{p(\mathbf{X}^{(N)}, \mathbf{Y}^{(N)})}{p_{\mathbf{X}}(\mathbf{X}^{(N)}) p_{\mathbf{Y}}(\mathbf{Y}^{(N)})} = \frac{1}{N} \sum_j \log \frac{p(X_j, Y_j)}{p^*(X_j) p_Y(Y_j)} = \frac{1}{N} \sum_{j=1}^N \xi_j,$$

где $\xi_j = \log \dfrac{p(X_j, Y_j)}{p^*(X_j) p_Y(Y_j)}$. С. в. ξ_j независимы, одинаково распределены, и

$$\mathsf{E}\xi_j = \mathsf{E} \log \frac{p(X_j, Y_j)}{p^*(X_j) p_Y(Y_j)} = I_{p^*}(X_1 : Y_1).$$

Применим закон больших чисел для н. о. р. с. в. (ср. теорему 1.3.5), который для случайного кодирования утверждает, что

$$\Theta_N \xrightarrow{\mathsf{P}} I_{p^*}(X_1 : Y_1) = \sup_{p_{X_1}} I(X_1 : Y_1).$$

По второй теореме Шеннона о кодировании (прямая часть) имеем

$$C \geqslant \sup_{p_{X_1}} I(X_1 : Y_1).$$

Следовательно, $C = \sup_{p_{X_1}} I(X_1 : Y_1)$. □

Замечание 1.4.20. 1. Пару (X_1, Y_1) можно заменить любой парой (X_j, Y_j), $j \geqslant 1$.

2. Напомним, что совместное распределение с. в. X_1 и Y_1 определяется как $\mathsf{P}(X_1 = x, Y_1 = y) = p_{X_1}(x) P(y\,|\,x)$, где $(P(y\,|\,x))$ — матрица канала.

3. Хотя, как было отмечено, конструкция остаётся в силе при каждом r, т. е. при каждом $\bar{R} \geqslant 0$, только $\bar{R} \leqslant C$ отвечают надёжным скоростям передачи. □

Пример 1.4.21. Статистик проводит предварительную обработку выхода д. к. б. п. с переходными вероятностями $P(y\,|\,x)$ и пропускной способностью $C = \max\limits_{p_X} I(X:Y)$ путём формирования $Y' = g(Y)$ и утверждает, что эта процедура повысит пропускную способность. Верно ли это?

Конечно же нет, предварительная обработка (или отбор) не увеличивает пропускную способность. Действительно,

$$I(X:Y) = h(X) - h(X\,|\,Y) \geqslant h(X) - h(X\,|\,g(Y)) = I(X:g(Y)). \qquad (1.4.26)$$

При каких условиях можно утверждать, что пропускная способность не уменьшается? Равенство в формуле (1.4.26) имеет место тогда и только тогда, когда распределение p_X максимизирует взаимную информацию $I(X:Y)$, т. е. с. в. X и Y условно независимы при данном $g(Y)$. (Например, $g(y_1) = g(y_2)$, если и только если для любых x имеет место равенство $P_{X\,|\,Y}(x\,|\,y_1) = P_{X\,|\,Y}(x\,|\,y_2)$, т. е., g склеивает вместе только те значения y, при которых условная вероятность $P_{X\,|\,Y}(\cdot\,|\,y_2)$ имеет одинаковые значения.) В случае двоичного канала без памяти равенство достигается тогда и только тогда, когда g — вложение или $p = P(1\,|\,0) = P(0\,|\,1) = 1/2$. □

В случае д. с. к. б. п. (т. е. $P(1\,|\,0) = P(0\,|\,1) = p$) формулу (1.4.25) можно ещё упростить.

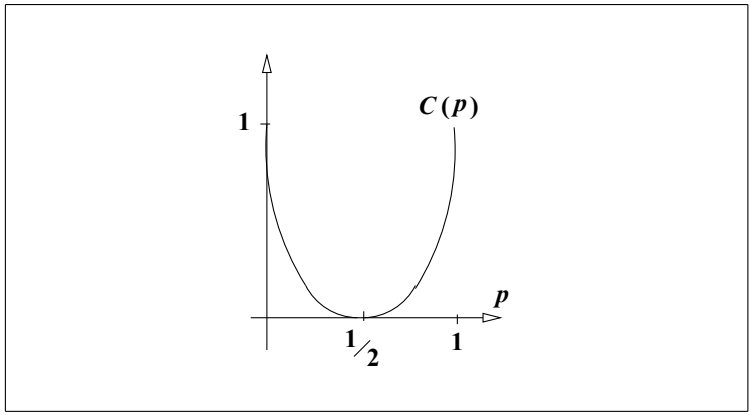


Рис. 1.7

Теорема 1.4.22. *Пропускная способность симметричного двоичного канала без памяти с вероятностью ошибки p записывается в виде*

$$C = 1 - h(p,\,1-p) = 1 - \eta(p) \qquad (1.4.27)$$

(*см. формулу* (1.4.11)). *Пропускная способность канала реализуется случайным кодированием с н.о.р. символами* V_{l_j}, *принимающими значения* 0 *и* 1 *с вероятностью* 1/2.

Доказательство. Вид максимизирующего распределения вероятностей тот же, что и в равенстве (1.4.27), что установлено в формуле (1.4.11). □

Пример 1.4.23. 1. Рассмотрим канал без памяти с двумя входными символами A и B, и тремя выходными символами A, B, $*$. Предположим, что с вероятностью 1/2 каждый входной символ остаётся нетронутым и с вероятностью 1/2 трансформируется в $*$ независимо от других символов. Запишите матрицу канала и вычислите его пропускную способность.

2. Рассчитайте пропускную способность канала при условии, что выходные данные подвергаются обработке, которая не может различать символы A и $*$, так что матрица приобретает вид

$$\begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \end{pmatrix}.$$

Решение. 1. Канал обладает симметричной матрицей

$$\begin{pmatrix} 1/2 & 0 & 1/2 \\ 0 & 1/2 & 1/2 \end{pmatrix}$$

(строки получаются друг из друга перестановкой). Таким образом, $h(Y|X = x) = -2 \times \frac{1}{2}\log\frac{1}{2} = 1$ не зависит от значения $x = A,\ B$. Поэтому $h(Y|X) = 1$ и

$$I(X:Y) = h(Y) - 1. \tag{1.4.28}$$

Если $\mathsf{P}(X = A) = \alpha$, то выходное распределение Y имеет вид

$$\left(\frac{1}{2}\alpha,\ \frac{1}{2}(1-\alpha),\ \frac{1}{2}\right)$$

и $h(Y|X)$ максимальна при $\alpha = 1/2$. Следовательно, пропускная способность канала равна

$$h(1/4,\ 1/4,\ 1/2) - 1 = \frac{1}{2}. \tag{1.4.29}$$

2. В этом случае канал не симметричен. Если $\mathsf{P}(X = A) = \alpha$, то условная энтропия раскладывается в сумму

$$h(Y|X) = \alpha h(Y|X = A) + (1-\alpha)h(Y|X = B) = \alpha \times 0 + (1-\alpha) \times 1 = 1 - \alpha.$$

Следовательно,

$$h(Y) = -\frac{1+\alpha}{2}\log\frac{1+\alpha}{2} - \frac{1-\alpha}{2}\log\frac{1-\alpha}{2}$$

и

$$I(X:Y) = -\frac{1+\alpha}{2}\log\frac{1+\alpha}{2} - \frac{1-\alpha}{2}\log\frac{1-\alpha}{2} - 1 + \alpha,$$

а эта величина достигает максимума при $\alpha = 3/5$. Значит, пропускная способность канала составляет

$$\log 5 - 2 \approx 0{,}321928. \qquad \square$$

Наша следующая цель — доказать прямую часть второй теоремы Шеннона о кодировании (теорема 1.4.15). Технические детали доказательства представлены в двух следующих примерах.

Пример 1.4.24. Пусть F — случайное кодирование, не зависящее от строки источника $\mathbf{U}$ такое, что кодовые слова $F(\mathbf{u}_1), \ldots, F(\mathbf{u}_r)$ независимы и имеют одинаковое распределение вероятностей p_F

$$p_F(\mathbf{v}) = \mathsf{P}(F(\mathbf{u}) = \mathbf{v}), \quad \mathbf{v}(= \mathbf{v}^{(N)}) \in J^{\times N}.$$

Здесь $\mathbf{u}_j$, $j = 1, \ldots, r$, обозначают строки источника, а $r = 2^{N(\bar{R}+o(1))}$. Определим случайные кодовые слова $\mathbf{V}_1, \ldots, \mathbf{V}_{r-1}$ по следующему правилу. Если $\mathbf{U} = \mathbf{u}_j$, то

$$\mathbf{V}_i := \begin{cases} F(\mathbf{u}_i) & \text{для } i < j, \\ F(\mathbf{u}_{i+1}) & \text{для } i \geqslant j, \\ & 1 \leqslant j \leqslant r, \quad 1 \leqslant i \leqslant r-1. \end{cases} \tag{1.4.30}$$

Тогда $\mathbf{U}$ (строка сообщения), $\mathbf{X} = F(\mathbf{U})$ (случайное кодовое слово) и $\mathbf{V}_1, \ldots, \mathbf{V}_{r-1}$ — независимые слова, причём каждое из слов $\mathbf{X}, \mathbf{V}_1, \ldots, \mathbf{V}_{r-1}$ обладает распределением p_F.

Решение непосредственно следует из формулы совместной вероятности

$$\mathsf{P}(\mathbf{U} = \mathbf{u}_j, \mathbf{X} = \mathbf{x}, \mathbf{V}_1 = \mathbf{v}_1, \ldots, \mathbf{V}_{r-1} = \mathbf{v}_{r-1}) = \\ = \mathsf{P}(\mathbf{U} = \mathbf{u}_j) p_F(\mathbf{x}) p_F(\mathbf{v}_1) \ldots p_F(\mathbf{v}_{r-1}). \tag{1.4.31}$$

$\square$

Пример 1.4.25. Проверьте, что для случайного кодирования, описанного в примере 1.4.24, для любого $\varkappa > 0$ выполнено неравенство

$$E = \mathsf{E}\varepsilon(F) \leqslant \mathsf{P}(\Theta_N \leqslant \varkappa) + r2^{-N\varkappa}. \tag{1.4.32}$$

Здесь с. в. Θ_N определяется формулой (1.4.21) и $\mathsf{E}\Theta_N = \dfrac{1}{N} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})$.

Решение. Для данных слов $\mathbf{x}(= \mathbf{x}^{(N)})$ и $\mathbf{y}(= \mathbf{y}^{(N)}) \in J^{\times N}$ обозначим

$$S_{\mathbf{y}}(\mathbf{x}) := \big(\mathbf{x}' \in J^{\times N} \colon \mathbf{P}(\mathbf{y}\,|\,\mathbf{x}') \geqslant \mathbf{P}(\mathbf{y}\,|\,\mathbf{x})\big). \tag{1.4.33}$$

Иначе говоря, множество $S_{\mathbf{y}}(\mathbf{x})$ включает в себя все слова, которые декодер м. п. может выдать в ситуации, когда было послано слово $\mathbf{x}$, а получено $\mathbf{y}$. Пусть заданы неслучайное правило кодирования f и строка источника $\mathbf{u}$, положим $\delta(f, \mathbf{u}, \mathbf{y}) = 1$, если $f(\mathbf{u}') \in S_{\mathbf{y}}(f(\mathbf{u}))$ при некотором $\mathbf{u}' \neq \mathbf{u}$, и $\delta(f, \mathbf{u}, \mathbf{y}) = 0$ в противном случае. Ясно, что $\delta(f, \mathbf{u}, \mathbf{y})$ равняется

$$1 - \prod_{\mathbf{u}' :\, \mathbf{u}' \neq \mathbf{u}} \mathbf{1}\big(f(\mathbf{u}') \notin S_{\mathbf{y}}(f(\mathbf{u}))\big) = 1 - \prod_{\mathbf{u}' :\, \mathbf{u}' \neq \mathbf{u}} \big[1 - \mathbf{1}\big(f(\mathbf{u}') \in S_{\mathbf{y}}(f(\mathbf{u}))\big)\big].$$

Очевидно, что для любого неслучайного кодирования f имеет место оценка $\varepsilon(f) \leqslant \mathsf{E}\delta(f, \mathbf{U}, \mathbf{Y})$, а для любого случайного кодирования F выполнено неравенство $E = \mathsf{E}\delta(F) \leqslant \mathsf{E}\delta(F, \mathbf{U}, \mathbf{Y})$. Более того, для случайного кодирования, описанного в примере 1.4.24, среднее значение $\mathsf{E}\delta(F, \mathbf{U}, \mathbf{Y})$ не превосходит

$$\mathsf{E}\left(1 - \prod_{i=1}^{r-1}[1 - \mathbf{1}(\mathbf{V}_i \in S_{\mathbf{Y}}(\mathbf{X}))]\right) =$$

$$= \sum_{\mathbf{x}} p_X(\mathbf{x}) \sum_{\mathbf{y}} \mathbf{P}(\mathbf{y}\,|\,\mathbf{x}) \cdot \mathsf{E}\left[\left(1 - \prod_{i=1}^{r-1}[1 - \mathbf{1}(\mathbf{V}_i \in S_{\mathbf{Y}}(\mathbf{X}))]\,|\,\mathbf{X} = \mathbf{x},\, \mathbf{Y} = \mathbf{y}\right)\right],$$

что благодаря независимости равно

$$\sum_{\mathbf{x}} p_{\mathbf{X}}(\mathbf{x}) \sum_{\mathbf{y}} \mathbf{P}(\mathbf{y}\,|\,\mathbf{x}) \left(1 - \prod_{i=1}^{r-1} \mathsf{E}(1 - \mathbf{1}(\mathbf{V}_i \in S_{\mathbf{y}}(\mathbf{x}))\right).$$

Более того, ввиду независимости и одинаковой распределённости (что объяснено в примере 1.4.24) имеет место равенство

$$\prod_{i=1}^{r-1} \mathsf{E}(1 - \mathbf{1}(\mathbf{V}_i \in S_{\mathbf{y}}(\mathbf{x})) = (1 - Q_{\mathbf{y}}(\mathbf{x}))^{r-1},$$

где

$$Q_{\mathbf{y}}(\mathbf{x}) := \sum_{\mathbf{x}'} \mathbf{1}(\mathbf{x}' \in S_{\mathbf{y}}(\mathbf{x}))p_X(\mathbf{x}').$$

Следовательно, средняя вероятность ошибки подчиняется неравенству $E \leqslant 1 - \mathsf{E}(1 - Q_{\mathbf{Y}}(\mathbf{X}))^{r-1}$.

Обозначим через $\mathbb{T} = \mathbb{T}(\varkappa)$ множество пар слов $\mathbf{x}$, $\mathbf{y}$, для которых

$$\Theta_N = \frac{1}{N} \log \frac{p(\mathbf{x}, \mathbf{y})}{p_{\mathbf{X}}(\mathbf{x}) p_{\mathbf{Y}}(\mathbf{y})} > \varkappa,$$

и воспользуемся тождеством

$$1-(1-Q_{\mathbf{y}}(\mathbf{x}))^{r-1}=\sum_{j=0}^{r-2}(1-Q_{\mathbf{y}}(\mathbf{x}))^{j}Q_{\mathbf{y}}(\mathbf{x}). \tag{1.4.34}$$

Далее заметим, что

$$1-(1-Q_{\mathbf{y}}(\mathbf{x}))^{r-1}\leqslant 1, \quad \text{когда } (\mathbf{x},\,\mathbf{y})\notin\mathbb{T}. \tag{1.4.35}$$

При $(\mathbf{x},\,\mathbf{y})\in\mathbb{T}$ имеет место соотношение

$$(1-(1-Q_{\mathbf{y}}(\mathbf{x}))^{r})=\sum_{j=1}^{r-1}\Bigl(1-Q_{\mathbf{y}}(\mathbf{x}))^{j}\Bigr)Q_{\mathbf{y}}(\mathbf{x})\leqslant(r-1)Q_{\mathbf{y}}(\mathbf{x}),$$

откуда следует неравенство

$$E\leqslant\mathsf{P}((\mathbf{x},\,\mathbf{y})\notin\mathbb{T})+(r-1)\sum_{(\mathbf{x},\mathbf{y})\in\mathbb{T}}p_X(\mathbf{x})\mathbf{P}(\mathbf{y}\,|\,\mathbf{x})Q_{\mathbf{y}}(\mathbf{x}). \tag{1.4.36}$$

Теперь заметим, что

$$\mathsf{P}((\mathbf{x},\,\mathbf{y})\notin\mathbb{T})=\mathsf{P}(\Theta_N\leqslant\varkappa). \tag{1.4.37}$$

Наконец, для $(\mathbf{x},\,\mathbf{y})\in\mathbb{T}$ и $\mathbf{x}'\in S_{\mathbf{y}}(\mathbf{x})$ имеем

$$\mathbf{P}(\mathbf{y}\,|\,\mathbf{x}')\geqslant\mathbf{P}(\mathbf{y}\,|\,\mathbf{x})\geqslant p_{\mathbf{Y}}(\mathbf{y})2^{N\varkappa}.$$

Умножая это неравенство на $\dfrac{p_X(\mathbf{x}')}{p_{\mathbf{Y}}(\mathbf{y})}$, получаем $\mathsf{P}(X=\mathbf{x}'\,|\,Y=\mathbf{y})\geqslant p_X(\mathbf{x}')2^{N\varkappa}$. Тогда, суммируя по $\mathbf{x}'\in S_{\mathbf{y}}(\mathbf{x})$, приходим к неравенству

$$1\geqslant\mathsf{P}(S_{\mathbf{y}}(\mathbf{x})\,|\,\mathbf{Y}=\mathbf{y})\geqslant Q_{\mathbf{y}}(\mathbf{x})2^{N\varkappa}, \quad \text{или} \quad Q_{\mathbf{y}}(\mathbf{x})\leqslant 2^{-N\varkappa}. \tag{1.4.38}$$

Подставляя формулы (1.4.37) и (1.4.38) в неравенство (1.4.36), получаем соотношение (1.4.32). □

Доказательство теоремы 1.4.15. Для завершения доказательства теоремы 1.4.15 положим $\bar{R}=c-2\varepsilon$ и $\varkappa=c-\varepsilon$. Тогда, поскольку $r=2^{N(\bar{R}+o(1))}$, мы видим, что E не превышает

$$\mathsf{P}(\Theta_N\leqslant c-\varepsilon)+2^{N(c-2\varepsilon-c+\varepsilon+o(1))}=\mathsf{P}(\Theta_N\leqslant c-\varepsilon)+2^{-N\varepsilon}.$$

Эта величина стремится к нулю при $N\to\infty$, так как $\mathsf{P}(\Theta_N\leqslant c-\varepsilon)\to 0$ из-за условия $\Theta_N\xrightarrow{\mathbb{R}}c$. Следовательно, при случайном кодировании F средняя вероятность ошибки стремится к нулю при $N\to\infty$.

По п. 1 теоремы 1.4.10 для любого $N\geqslant 1$ найдётся такое детерминированное кодирование $f=f_N$, что при $\bar{R}=c-2\varepsilon$ верно равенство $\lim\limits_{N\to\infty}\varepsilon(f)=0$. Значит, $\bar{R}$ — надёжная скорость передачи. Поскольку это верно при всех $\varepsilon>0$, получаем, что $C\geqslant c$. □

Приведенное выше доказательство было предложено П. Уиттлом и излагалось в его лекциях в Кембриджском университете, оно опубликовано в книге [GP], с. 114–117. Мы благодарны Ч. Голди за эту информацию. Альтернативный подход основывается на концепции совместной типичности; этот подход используется в § 2.2, где обсуждается канал с непрерывно распределенным шумом.

Теоремы 1.4.17 и 1.4.19 можно обобщить на случай канала без памяти с любым (конечным) выходным алфавитом $J_q = \{0, \dots, q-1\}$. Иначе говоря, на выходе канала появляется слово $\mathbf{Y}^{(N)} = Y_1 \dots Y_N$, в котором каждый символ Y_j (случайно) принимает значение из алфавита J_q. Свойство «отсутствия памяти» означает, как и ранее, что

$$\mathbf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}) = \prod_{i=1}^{N} P(y_i \,|\, x_i), \tag{1.4.39}$$

и посимвольные переходные вероятности канала $P(y\,|\,x)$ образуют стохастическую матрицу размера $2 \times q$ (матрица канала). Канал без памяти называется симметричным, если строки матрицы канала получаются друг из друга перестановкой элементов. Он называется дважды симметричным, если к тому же столбцы матрицы канала получаются друг из друга перестановками. Определения надёжной скорости передачи и пропускной способности переносятся на этот случай без изменения.

Теорема 1.4.26. *Пропускная способность канала без памяти с выходным алфавитом J_q оценивается как*

$$C \leqslant \log q - h(p_0, \dots, p_{q-1}), \tag{1.4.40}$$

где $(p_0, \dots, p_{q-1})$ — строка матрицы канала. Равенство реализуется на дважды симметричном канале, а максимизирующее случайное кодирование имеет н.о.р. символы V_i, принимающие значения из J_q с вероятностью $1/q$.

Доказательство. Доказательство переносится с двоичного случая с учётом того факта, что $h(X_1 : Y_1) = h(Y_1) - h(Y_1\,|\,X_1) \leqslant \log q - h(Y_1\,|\,X_1)$. Но в симметричном случае

$$h(X_1\,|\,Y_1) = -\sum_{x,y} \mathsf{P}(X_1 = x) P(y\,|\,x) \log P(y\,|\,x) =$$

$$= -\sum_{x} \mathsf{P}(X_1 = x) \sum_{k} p_k \log p_k = h(p_0, \dots, p_{q-1}). \tag{1.4.41}$$

Кроме того, столбцы матрицы канала получаются друг из друга перестановками, поэтому $h(Y_1)$ достигает $\log q$. Действительно, выберем случайное кодирование, как предлагалось. Тогда $\mathsf{P}(Y = y) = \sum_{x=0}^{q-1} \mathsf{P}(X_1 = x) P(y\,|\,x) =$

$= \frac{1}{q}\sum_x P(y\,|\,x)$. Сумма $\sum_x P(y\,|\,x)$ берётся по столбцам матрицы канала и не зависит от y. Следовательно, $\mathsf{P}(Y = y)$ не зависит от $y \in J_q$, что свидетельствует о равномерном распределении. □

Замечание 1.4.27. При случайном кодировании F, использованном в примерах 1.4.22 и 1.4.23 и теоремах 1.4.7, 1.4.13 и 1.4.17, предел средней вероятности ошибки E при $N \to \infty$ равен нулю. Это гарантирует не только существование «хорошего» не случайного кодирования, при котором средняя вероятность ошибки стремится к нулю при $N \to \infty$ (см. п. 2 теоремы 1.4.11), но и то, что «почти все» кодирования асимптотически хорошие. Фактически по теореме 1.4.11 с $\rho = 1 - \sqrt{E}$ имеет место следующее утверждение: $\mathsf{P}(\varepsilon(F) < \sqrt{E}) \geqslant 1 - \sqrt{E} \to 1$ при $N \to \infty$. Однако это не помогает найти хотя бы один хороший код: построение хорошего кода — это сложная задача теории информации. Мы вернёмся к ней позже.

Пример 1.4.28. По каналу связи передаются биты. Бит может быть заменён на противоположный с вероятностью λ, и с вероятностью μ его не удается распознать при получении. Исходы передач бит не зависят друг от друга. Найдите пропускную способность этого канала.

Решение. Матрица канала имеет вид

$$\begin{pmatrix} 1-\lambda-\mu & \lambda & \mu \\ \lambda & 1-\lambda-\mu & \mu \end{pmatrix},$$

ее строки получаются друг из друга перестановкой элементов и поэтому обладают одинаковой энтропией. Следовательно, условная энтропия

$$h(Y\,|\,X) = -(1-\lambda-\mu)\log(1-\lambda-\mu) - \lambda\log\lambda - \mu\log\mu$$

не зависит от распределения входного символа X.

Таким образом, $I(X:Y)$ достигает максимума одновременно с $h(Y)$. Если $p_Y(0) = p$ и $p_Y(1) = q$, то Y принимает значение 0 с вероятностью $p(1-\lambda-\mu) + q\lambda$, 1 с вероятностью $q(1-\lambda-\mu) + p\lambda$ и не читается с вероятностью μ. Энтропия $h(Y)$ достигает максимума при $p = q = (1-\mu)/2$ (по неравенству группировки данных), т. е. $p_X(0) = p_X(1) = 1/2$. Это даёт следующее выражение для пропускной способности:

$$-(1-\mu)\log\frac{1-\mu}{2} + (1-\lambda-\mu)\log(1-\lambda-\mu) + \lambda\log\lambda = \\ = (1-\mu)\Big(1 - \eta\Big(\frac{\lambda}{1-\mu}\Big)\Big). \quad \square$$

Пример 1.4.29. 1. Рассмотрим два независимых канала, подключенных последовательно. Случайный сигнал X посылается через канал 1, и на его выходе получается Y. Затем этот сигнал посылается по каналу 2,

и на его выходе получается Z. Докажите, что выполняется *неравенство обработки данных*[4]

$$I(X : Z) \leqslant I(X : Y),$$

так что дальнейшая обработка второго канала может лишь уменьшить взаимную информацию.

Независимость каналов означает, что при данной с. в. Y с. в. X и Z условно независимы. Выведите, что

$$h(X,\, Y \,|\, Z) = h(X \,|\, Y) + h(Z \,|\, Y)$$

и

$$h(X,\, Y,\, Z) + h(Z) = h(X,\, Z) + h(Y,\, Z).$$

Определим $I(X : Z \,|\, Y)$ как $h(X \,|\, Y) + h(Z \,|\, Y) - h(X,\, Z \,|\, Y)$. Покажите, что

$$I(X : Z \,|\, Y) = I(X : Y) - I(X : Z).$$

Может ли в неравенстве обработки данных достигаться равенство

$$I(X : Z) = I(X : Y)?$$

2. Входные и выходные данные дискретного по времени канала записываются через алфавит, состоящий из остатков от деления натуральных чисел на фиксированное натуральное число r. Переданная буква $[x]$ получается на выходе канала как $[j + x]$ с вероятностью p_j, где x и j целые, а $[c]$ обозначает остаток от деления c на r. Вычислите пропускную способность канала.

Решение. 1. При данной с. в. Y с. в. X и Z условно независимы. Следовательно,

$$h(X \,|\, Y) = h(X \,|\, Y,\, Z) \leqslant h(X \,|\, Z),$$

и

$$I(X : Y) = h(X) - h(X \,|\, Y) \geqslant h(X) - h(X \,|\, Z) = I(X : Z).$$

Равенство достигается тогда и только тогда, когда X и Y условно независимы при данной с. в. Z, например если второй канал свободен от ошибок: отображение $(Y,\, Z) \mapsto Z$ является вложением, или первый канал полностью зашумлён, т. е. X и Y независимы.

2. Строки матрицы канала получаются друг из друга перестановкой. Значит, $h(Y \,|\, X) = h(p_0,\, \ldots,\, p_{r-1})$ не зависит от p_X. Величина $h(Y)$ достигает максимума при $p_X(i) = 1/r$, следовательно,

$$C = \log r - h(p_0,\, \ldots,\, p_{r-1}). \qquad \square$$

[4] Data processing inequality

Пример 1.4.30. Найдите вероятность ошибки каскада из n одинаковых независимых симметричных двоичных каналов без памяти (д. с. к. б. п., рис. 1.8), если вероятность ошибки каждого канала равна p, $0 < p < 1$. Проверьте, что пропускная способность каскада стремится к нулю при $n \to \infty$.

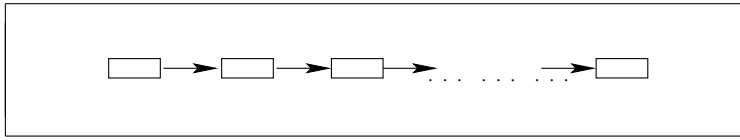


Рис. 1.8

Решение. Матрица комбинированного канала, состоящего из каскада n каналов, равна Π^n, где

$$\Pi = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

Найдя собственные числа и векторы, можно вычислить нужную степень матрицы:

$$\Pi^n = \frac{1}{2}\begin{pmatrix} 1+(1-2p)^n & 1-(1-2p)^n \\ 1-(1-2p)^n & 1+(1-2p)^n \end{pmatrix},$$

что даёт вероятность ошибки $1/2(1-(1-2p)^n)$. Если $0 < p < 1$, то матрица Π^n сходится к

$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

и пропускная способность канала стремится к

$$1 - h(1/2,\, 1/2) = 1 - 1 = 0.$$

Если $p = 0$ или 1, то канал свободен от ошибок и $C \equiv 1$. □

Пример 1.4.31. Рассмотрим два двоичных канала без памяти с пропускными способностями C_1 и C_2 бит/с. Докажите или опровергните контрпримером каждое из перечисленных ниже утверждений относительно пропускной способности C комбинированного канала в каждом из следующих случаев.

1. Если каналы подключены последовательно и выход одного поступает на вход другого без дополнительного кодирования, то $C = \min[C_1,\, C_2]$.

2. Пусть каналы используются параллельно в том смысле, что в каждую секунду символ (из его входного алфавита) передаётся через канал 1, а следующий через канал 2; каждый канал, таким образом, передаёт по одному символу в каждую секунду. Тогда $C = C_1 + C_2$.

3. Если каналы используют один алфавит и в каждую секунду выбирается символ и передаётся по обоим каналам одновременно, то $C = \max[C_1, C_2]$.

4. Если матрица i-го канала равна Π_i, а матрица комбинированного канала равна

$$\begin{pmatrix} \Pi_1 & 0 \\ 0 & \Pi_2 \end{pmatrix},$$

то C вычисляется по формуле $2^C = 2^{C_1} + 2^{C_2}$. Какому способу подключения это соответствует?

Решение. 1. $\xrightarrow{X}$ [канал 1] $\xrightarrow{Y}$ [канал 2] $\xrightarrow{Z}$

Как было доказано в п. 1 примера 1.4.29,

$$I(X:Z) \leqslant I(X:Y), \quad I(X:Z) \leqslant I(Y:Z).$$

Следовательно,

$$C = \sup_{p_X} I(X:Z) \leqslant \sup_{p_X} I(X:Y) = C_1,$$

и аналогично

$$C \leqslant \sup_{p_Y} I(Y:Z) = C_2,$$

т. е. $C \leqslant \min[C_1, C_2]$. Чтобы привести пример, когда $C < \min[C_1, C_2]$, выберем $\delta \in (0, 1/2)$ и следующие матрицы каналов:

$$\text{ch } 1 \sim \begin{pmatrix} 1-\delta & \delta \\ \delta & 1-\delta \end{pmatrix}, \quad \text{ch } 2 \sim \begin{pmatrix} 1-\delta & \delta \\ \delta & 1-\delta \end{pmatrix},$$

$$\text{ch}[1+2] \sim \frac{1}{2}\begin{pmatrix} (1-\delta)^2+\delta^2 & 2\delta(1-\delta) \\ 2\delta(1-\delta) & (1-\delta)^2+\delta^2 \end{pmatrix}.$$

Здесь $1/2 > 2\delta(1-\delta) > \delta$,

$$C_1 = C_2 = 1 - \eta(\delta)$$

и

$$C = 1 - \eta(2\delta(1-\delta)) < C_i,$$

так как $\eta(\varepsilon)$ строго возрастает по $\varepsilon \in [0, 1/2]$.

2. $X_1 \longrightarrow$ [канал 1] $\longrightarrow Y_1$

$X_2 \longrightarrow$ [канал 2] $\longrightarrow Y_2$.

Пропускная способность комбинированного канала равна

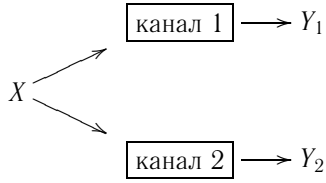
$$C = \sup_{p(X_1, X_2)} I((X_1, X_2) : (Y_1, Y_2)).$$

Но

$$I((X_1,\,X_2):(Y_1,\,Y_2)) = h(Y_1,\,Y_2) - h(Y_1,\,Y_2\,|\,X_1,\,X_2) \leqslant$$
$$\leqslant h(Y_1) + h(Y_2) - h(Y_1\,|\,X_1) - h(Y_2\,|\,X_2) = I(X_1 : Y_1) + I(X_2 : Y_2);$$

равенство достигается тогда и только тогда, когда X_1 и X_2 независимы. Таким образом, $C = C_1 + C_2$, и максимизирующее распределение $p(X_1,\,X_2)$ совпадает с $p_{X_1} \times p_{X_2}$, где распределения p_{X_1} и p_{X_2} максимизируют $I(X_1 : Y_1)$ и $I(X_2 : Y_2)$.

3.



Здесь

$$C = \sup_{p_X} I(X : (Y_1 : Y_2))$$

и

$$I((Y_1 : Y_2) : X) = h(X) - h(X\,|\,Y_1,\,Y_2) \geqslant h(X) - \min_{j=1,2} h(X\,|\,Y_j) = \min_{j=1,2} I(X : Y_j).$$

Таким образом, $C \geqslant \max[C_1,\,C_2]$. Чтобы привести пример, когда $C > \max[C_1,\,C_2]$, вновь рассмотрим матрицы каналов из п. 1. Здесь $C_i = 1 - \eta(\delta)$. Кроме того,

$$I((Y_1,\,Y_2) : X) = h(Y_1,\,Y_2) - h(Y_1,\,Y_2\,|\,X) =$$
$$= h(Y_1,\,Y_2) - h(Y_1\,|\,X) - h(Y_2\,|\,X) = h(Y_1,\,Y_2) - 2\eta(\delta).$$

Если положить $p_X(0) = p_X(1) = 1/2$, то получим

$$(Y_1,\,Y_2) = (0,\,0) \text{ с вероятностью } ((1-\delta)^2 + \delta^2)/2,$$
$$(Y_1,\,Y_2) = (1,\,1) \text{ с вероятностью } ((1-\delta)^2 + \delta^2)/2,$$
$$(Y_1,\,Y_2) = (1,\,0) \text{ с вероятностью } \delta(1-\delta),$$
$$(Y_1,\,Y_2) = (0,\,1) \text{ с вероятностью } \delta(1-\delta).$$

При этом

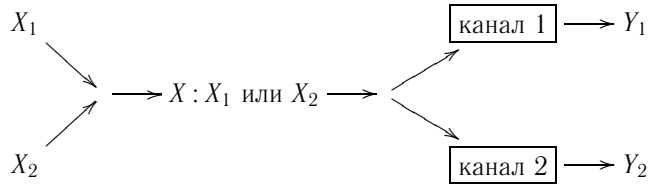
$$h(Y_1,\,Y_2) = 1 + \eta(2\delta(1-\delta))$$

и

$$I((Y_1,\,Y_2) : X) = 1 + \eta(2\delta(1-\delta)) - 2\eta(\delta) > 1 - \eta(\delta) = C_i.$$

Следовательно, $C > C_i$, $i = 1,\,2$.

4. Рассмотрим следующую схему подключения каналов:



Отличие от предыдущей ситуации состоит в том, что каждую секунду посылается только один символ либо по каналу 1, либо по каналу 2. Если мы обозначим вероятность того, что символ посылается по первому каналу, через α, а по второму — через $1-\alpha$, то можно записать, что

$$I(X:Y) = \eta(\alpha) + \alpha I(X_1 : Y_1) + (1-\alpha) I(X_2 : Y_2). \tag{1.4.42}$$

Действительно, $I(X:Y) = h(Y) - h(Y\,|\,X)$, где

$$h(Y) = -\sum_y \alpha p_{Y_1}(y) \log \alpha p_{Y_1}(y) - \sum_y (1-\alpha) p_{Y_2}(y) \log (1-\alpha) p_{Y_2}(y) = \\ = \eta(\alpha) + \alpha h(Y_1) + (1-\alpha) h(Y_2)$$

и

$$h(Y\,|\,X) = -\sum_{x,y} \alpha p_{X_1,Y_1}(x,\,y) \log \alpha p_{Y_1\,|\,X_1}(y\,|\,x) - \\ - \sum_{x,y} (1-\alpha) p_{X_2,Y_2}(y\,|\,x) \log p_{X_2,Y_2}(y\,|\,x) = \alpha h(Y_1\,|\,X_1) + (1-\alpha) h(Y_2\,|\,X_2),$$

что доказывает равенство (1.4.42). Отсюда следует, что

$$C = \max_{0 \leqslant \alpha \leqslant 1} [h(\alpha,\, 1-\alpha) + \alpha C_1 + (1-\alpha) C_2].$$

Максимум достигается при

$$\alpha = 2^{C_1}/(2^{C_1} + 2^{C_2}), \quad 1-\alpha = 2^{C_2}/(2^{C_1} + 2^{C_2})$$

и $C = \log(2^{C_1} + 2^{C_2})$. □

Пример 1.4.32. Шпионская программа посылает сообщения в центр слежения следующим образом. Каждый час она либо звонит по телефону и позволяет прозвучать звонкам определённое число раз (не более N из-за опасения быть обнаруженной), либо не звонит вовсе. Центр слежения не отвечает, а просто подсчитывает число звонков (0, если их не было). Из-за недостатков в системе телефонной связи телефон не всегда подключается должным образом; правильное подключение имеет вероятность p, где $0 < p < 1$, и независимо от остальных попыток подключения, но

шпионская программа не имеет возможности узнать, какие попытки связи прошли корректно. Если соединение установлено, то число звонков передаётся правильно. Вероятностью соединения от иного пользователя в те часы, когда шпионская программа не звонила по телефону, можно пренебречь. Выпишите матрицу этого канала и явно рассчитайте его пропускную способность. При каком соотношении между N и p при оптимальном кодировании шпионская программа будет всегда звонить по телефону?

Решение. Алфавит канала — это множество $\{0, 1, \ldots, N\}$ (0 — это отсутствие соединения в данный час). Выпишем элементы матрицы канала: $P(0\,|\,0) = 1$, $P(0\,|\,j) = 1 - p$ и $P(j\,|\,j) = p$, $1 \leqslant j \leqslant N$. При этом $h(Y\,|\,X) = q\eta(p)$, где $q = p_X(X \geqslant 1)$. Более того, при данном q величина $h(Y)$ достигает максимума при

$$p_Y(0) = 1 - pq, \quad p_Y(k) = \frac{pq}{N}, \quad 1 \leqslant k \leqslant N.$$

Максимизируя $I(X : Y) = h(Y) - h(Y\,|\,X)$ по q, получаем $p(1-p)^{(1-p)/p}(1-pq) = pq/N$, или

$$q = \min\left[\left(p + \frac{1}{N}\left(\frac{1}{1-p}\right)^{(1-p)/p}\right)^{-1}, 1\right].$$

Условие $q = 1$ равносильно тому, что $\log N \geqslant -\dfrac{1}{p}\log(1-p)$, т. е. $N \geqslant \dfrac{1}{(1-p)^{1/p}}$. □

Чтобы сбалансировать наше щедрое цитирование Шеннона и Хэмминга, мы закончим этот параграф рассказами о Норберте Винере (1894–1964), одном из выдающихся математиков, который повлиял на развитие теории информации, по крайней мере на начальной её стадии (см. предисловие к этой книге). Как это бывает с выдающимися личностями, ходит множество анекдотов и историй о нём (его противники намекали на то, что он сам часто использовал этот вид «рекламы»; некоторые связывали эту особенность с его отцом, который настойчиво продвигал молодого Норберта как чрезвычайно одарённого человека).

Винер славился своей рассеянностью. Согласно легенде, когда его семья переезжала, жена Винера дала ему листок с новым адресом. По дороге на работу Винер начал громоздкий расчёт на этой бумаге, ошибся и в отчаянии кинул его в мусорную корзину. По возвращении он понял, что не может найти новое место жительства. Винер решил пойти к прежнему дому и поспрашивать старых соседей. К счастью, возле своего старого дома он встретил девочку, и спросил её, не знает ли она случайно, куда переехала семья Винера. Девочка ответила: «О'кей, папа. Я отведу тебя домой».

The idea that information can be stored... without an overwhelming depreciation of its value is false. It is scarcely less false that the more plausible claim that after a war we may take our existing weapons and fill their barrels with information

Идея, что информацию можно хранить... без подавляющего ущерба её значимости, неверна. Она едва ли менее ошибочна, чем выглядящее более правдоподобным рассуждение, что после войны мы возьмем существующее оружие и заполним информацией его стволы.

Норберт Винер (1894–1964),
американский математик

Как математик, Винер продемонстрировал значительный спектр интересов. В частности, он был одним из создателей знаменитого метода Винера—Хопфа, основанного на комплексном анализе и используемого в различных приложениях, от теории массового обслуживания (важное направление в прикладной теории вероятностей) до квантовой теории твердого тела (в аномальном скин-эффекте в металлах). В начале 1960-х гг. Винер посетил Москву, где он встретился с корифеями советской науки, в том числе с математиком Андреем Колмогоровым и физиком Львом Ландау. Последний восхищался элегантностью и эффективностью метода Винера—Хопфа и превозносил его в своём выступлении на семинаре по теоретической физике в Институте физических проблем, где директором был П. Капица, центре академической жизни в Москве того периода. Во время визита Винер обедал вместе с Ландау и подробно рассказывал о теории информации и кибернетике. Согласно мнению современников, он был плохой слушатель и его беседы были смесью помпезности и экстравагантности (см. книгу [Ja]). Предмет рассказа Винера за обедом был не интересен Ландау, который сказал потом с видимым раздражением, что он «никогда не встречал более неинтересного человека, чем Винер», добавив: «Он никак не мог придумать метод Винера—Хопфа. Очевидно, это изобретение Хопфа». (Цитата из [Хал], в соответствии с этим источником на самом деле Ландау использовал гораздо более сильные выражения на русском языке.)

В заключение этих заметок ещё одна история о Винере. В 1960-е годы в одной из своих поездок в Индию (где кибернетика была не менее популярна, чем в СССР) Винер встретился с Сергеем Соболевым, замечательным советским математиком, много сделавшим для пропаганды кибернетических идей и знаний. По предложению Винера они отправились вместе пообедать. За столом говорил исключительно Винер, в основном, о себе и главным образом в превосходной степени. По завершению обеда Винер был в прекрасном настроении. На прощание он с чувством пожал руку собеседника и сказал, что он был чрезвычайно счастлив узнать мнение уважаемого профессора Соболева по ряду важных вопросов и рад, что это мнение совпало с его собственным. (Мы благодарны Л. Сабининой, рассказавшей нам этот эпизод со слов её деда.)

Прогресс создаёт не только новые возможности для будущего, но и новые ограничения.

Норберт Винер (1894–1964),
американский математик

§ 1.5. Дифференциальная энтропия и её свойства

> Случайность разделяет с... пространством и временем то свойство, что чем больше человек знает о них, тем меньше это знание становится.
>
> *Брайан Р. Гейнс* (род. в 1938 г.), канадский ученый и инженер, выходец из Британии

Этот параграф содержит довольно сложный материал, и читатель может пропустить его при первом прочтении (в частности, если он ещё не до конца освоил энтропию).

Определение 1.5.1. Предположим, что с. в. X обладает плотностью распределения (п. р.) $p(\mathbf{x})$, $\mathbf{x} \in \mathbb{R}^d$:

$$\mathsf{P}(X \in A) = \int\limits_A p(\mathbf{x})d\mathbf{x}$$

для любого (измеримого) множества $A \subseteq \mathbb{R}^d$, где $p(\mathbf{x}) \geqslant 0$, $\mathbf{x} \in \mathbb{R}^d$ и $\int\limits_{\mathbb{R}^d} p(\mathbf{x})d\mathbf{x} = 1$. *Дифференциальная энтропия* $h_{\text{diff}}(X)$ определяется как

$$h_{\text{diff}}(X) = -\int p(\mathbf{x}) \log p(\mathbf{x})d\mathbf{x} \tag{1.5.1}$$

при условии, что интеграл абсолютно сходится. Как и в дискретном случае $h_{\text{diff}}(X)$ можно представлять себе как функционал от плотности $p(\mathbf{x})$, $\mathbf{x} \in \mathbb{R}$. Отличие, однако, состоит в том, что $h_{\text{diff}}(X)$ может принимать отрицательные значения, например для равномерного распределения на отрезке $[0,\, a]$ $h_{\text{diff}}(X) = -\int\limits_0^a (1/a)\log(1/a)dx = \log a < 0$ при $a < 1$. (Мы пишем x вместо $\mathbf{x}$, когда $x \in \mathbb{R}$.) Относительная, совместная и условная дифференциальная энтропия определяются так же, как и в дискретном случае:

$$h_{\text{diff}}(X \parallel X') = -\int p(\mathbf{x}) \log \frac{p'(\mathbf{x})}{p(\mathbf{x})}d\mathbf{x}, \tag{1.5.2}$$

$$h_{\text{diff}}(X,\, Y) = -\int p_{X,Y}(\mathbf{x},\, \mathbf{y}) \log p_{X,Y}(\mathbf{x},\, \mathbf{y})d\mathbf{x}d\mathbf{y}, \tag{1.5.3}$$

$$h_{\text{diff}}(X \,|\, Y) = -\int p_{X,Y}(\mathbf{x},\, \mathbf{y}) \log p_{X \,|\, Y}(\mathbf{x} \,|\, \mathbf{y})d\mathbf{x}d\mathbf{y} = h_{\text{diff}}(X,\, Y) - h_{\text{diff}}(Y) \tag{1.5.4}$$

при условии, что все интегралы абсолютно сходятся. Здесь $p_{X,Y}$ — п. р. совместной вероятности, $p_{X \,|\, Y}$ — п. р. условной вероятности (п. р. условного распределения). В дальнейшем мы будем опускать индекс diff, если понятно, о какой энтропии идёт речь. Формулировки теорем 1.2.14 и 1.2.18 можно перенести на случай дифференциальной энтропии: доказательства переносятся без изменений, и мы их повторять не будем.

Замечание 1.5.2. Любое число $x \in [0, 1]$ можно записать как сумму $\sum\limits_{n\geqslant 1} \alpha_n 2^{-n}$, где $\alpha_n (= \alpha_n(x))$ равно 0 или 1. Для «почти всех» чисел x ряд не сведётся к конечной сумме (т. е. найдётся бесконечно много α_n, равных 1); формальное утверждение заключается в том, что мера (Лебега) множества чисел $x \in (0, 1)$ с бесконечным числом $\alpha_n(x) = 1$ равна 1. Таким образом, если «кодировать» x двоичными знаками, мы, как правило, получим бесконечное кодовое слово. Другими словами, типичное значение равномерно распределённой с. в. X, где $0 \leqslant X \leqslant 1$ нуждается в бесконечном числе битов для её «точного» описания. Это замечание легко обобщается на общий случай, когда п. р. X имеет вид $f_X(x)$.

Однако если мы хотим представить значение с. в. X с точностью до n двоичных знаков, то в среднем нам потребуется $n + h(X)$ бит, где $h(X)$ — дифференциальная энтропия с. в. X. Дифференциальная энтропия может принимать как положительные, так и отрицательные значения, она даже может быть равной $-\infty$. Так как $h(X)$ может иметь разные знаки, число $n + h(X)$ бывает больше или меньше n. В дискретном случае энтропия инвариантна как относительно сдвигов, так и относительно масштабирования, поскольку зависит только от вероятностей $p_1, \ldots, p_m$, а не от значений с. в. Хотя дифференциальная энтропия не инвариантна относительно масштабирования, она инвариантна относительно сдвигов, о чём свидетельствует тождество (см. теорему 1.5.7)

$$h(aX + b) = h(X) + \log |a|.$$

Пример 1.5.3. Рассмотрим п. р.

$$f_r(x) = C_r \frac{1}{x(-\ln x)^{r+1}}, \quad 0 < r < 1,$$

на множестве $0 \leqslant x \leqslant e^{-1}$. Тогда дифференциальная энтропия равна $h(X) = -\infty$.

Решение. Подставив $y = -\ln x$, получим

$$\int\limits_0^{e^{-1}} \frac{1}{x(-\ln x)^{r+1}} dx = \int\limits_1^{\infty} \frac{1}{y^{r+1}} dy = \frac{1}{r}.$$

Значит, $C_r = r$. Более того, применив подстановку $z = \ln(-\ln x)$, получим

$$\int\limits_0^{e^{-1}} \frac{\ln(-\ln x)}{x(-\ln x)^{r+1}} dx = \int\limits_0^{\infty} z e^{-rz} dz = \frac{1}{r^2}.$$

Следовательно,

$$h(X) = -\int f_r(x)\ln f_r(x)dx = \int f_r(x)(-\ln r + \ln x + (r+1)\ln(-\ln x))dx =$$
$$= -\ln r - \int_0^{e^{-1}} \Big[\frac{r}{x(-\ln x)^r} - r(r+1)\frac{\ln(-\ln x)}{x(-\ln x)^{r+1}}\Big]dx,$$

так что при $0 < r < 1$ второй член бесконечен, а два других конечны. □

Теорема 1.5.4. *Пусть* $\mathbf{X} = (X_1, \ldots, X_d) \sim N(\mu, C)$ — *случайный вектор с многомерным нормальным распределением, со средним* $\mu = (\mu_1, \ldots, \mu_d)$ *и матрицей ковариации* $C = (C_{ij})$, *т.е.* $\mathsf{E}X_i = \mu_i$, $\mathsf{E}(X_i - \mu_i)(X_j - \mu_j) = C_{ij} = C_{ji}$, $1 \leqslant i, j \leqslant d$. *Тогда*

$$h(X) = \frac{1}{2}\log((2\pi e)^d \det C). \tag{1.5.5}$$

Доказательство. Плотность распределения $p_{\mathbf{X}}(\mathbf{x})$ равна

$$p(\mathbf{x}) = \frac{1}{((2\pi)^d \det C)^{1/2}} \exp\Big(-\frac{1}{2}(\mathbf{x}-\mu,\, C^{-1}(\mathbf{x}-\mu)\Big), \quad \mathbf{x} \in \mathbb{R}^d.$$

Поэтому $h(X)$ принимает вид

$$-\int_{\mathbb{R}^d} p(\mathbf{x})\Big[-\frac{1}{2}\log((2\pi)^d \det C) - \frac{\log e}{2}(\mathbf{x}-\mu,\, C^{-1}(x-\mu))\Big]d\mathbf{x} =$$
$$= \frac{\log e}{2}\mathsf{E}\Big[\sum_{i,j}(x_i-\mu_i)(x_j-\mu_j)(C^{-1})_{ij}\Big] + \frac{1}{2}\log((2\pi)^d \det C) =$$
$$= \frac{\log e}{2}\sum_{i,j}(C^{-1})_{ij}\,\mathsf{E}(x_i-\mu_i)(x_j-\mu_j) + \frac{1}{2}\log((2\pi)^d \det C) =$$
$$= \frac{\log e}{2}\sum_{i,j}(C^{-1})_{ij}C_{ji} + \frac{1}{2}\log((2\pi)^d \det C) =$$
$$= \frac{d\log e}{2} + \frac{1}{2}\log((2\pi)^d \det C) = \frac{1}{2}\log((2\pi e)^d \det C). \quad \square$$

Теорема 1.5.5. *Для случайного вектора* $\mathbf{X} = (X_1, \ldots, X_d)$ *со средним* μ *и матрицей ковариации* $C = (C_{ij})$ (*т.е.* $C_{ij} = \mathsf{E}(X_i - \mu_i)(X_j - \mu_j) = C_{ji}$) *имеет место неравенство*

$$h(\mathbf{X}) \leqslant \frac{1}{2}\log((2\pi e)^d \det C), \tag{1.5.6}$$

равенство в котором достигается тогда и только тогда, когда вектор $\mathbf{X}$ *распределён по многомерному нормальному закону.*

Доказательство. Пусть $p(\mathbf{x})$ — п. р. случайного вектора $\mathbf{X}$ и $p^0(\mathbf{x})$ — плотность нормального распределения со средним μ и матрицей ковариации C. Без ограничения общности предположим, что $\mu = 0$. Заметим, что $\log p^0(\mathbf{x})$ — квадратичная форма относительно переменных x_k (с точностью до аддитивной константы). Более того, для каждого монома $x_i x_j$ имеет место равенство $\int p^0(\mathbf{x}) x_i x_j d\mathbf{x} = \int p(\mathbf{x}) x_i x_j d\mathbf{x} = C_{ij} = C_{ji}$, и средние значения квадратичных форм $\ln p^0(\mathbf{x})$ и $\ln p(\mathbf{x})$ равны. Получаем

$$0 \leqslant D(p \,\|\, p^0) \text{ (по неравенству Гиббса) } = \int p(\mathbf{x}) \log \frac{p(\mathbf{x})}{p^0(\mathbf{x})} d\mathbf{x} =$$
$$= -\eta(p) - \int p(\mathbf{x}) \log p^0(\mathbf{x}) d\mathbf{x} = -\eta(p) - \int p^0(\mathbf{x}) \log p^0(\mathbf{x}) d\mathbf{x} =$$
$$= \text{ (по предыдущему замечанию) } - \eta(p) + \eta(p^0).$$

Равенство достигается тогда и только тогда, когда $p = p^0$. □

Пример 1.5.6. 1. Покажите, что экспоненциальная плотность максимизирует дифференциальную энтропию по всем п. р. на $\mathbb{R}_+ = [0, \infty)$ с данным средним, а нормальная плотность максимизирует дифференциальную энтропию по всем п. р. на $\mathbb{R}$ с данной дисперсией.

Более того, пусть $\mathbf{X} = (X_1, \ldots, X_d)^{\mathrm{T}}$ — случайный вектор, $\mathsf{E}\mathbf{X} = \mathbf{0}$ и $\mathsf{E}X_i X_j = C_{ij}$, $1 \leqslant i, j \leqslant d$. Тогда $h_{\text{diff}}(\mathbf{X}) \leqslant \frac{1}{2} \log((2\pi e)^d \det(C_{ij}))$, где равенство достигается тогда и только тогда, когда $\mathbf{X} \sim N(\mathbf{0}, C)$.

2. Докажите, что неравенство $h(X) \leqslant \log m$ (см. формулу (1.2.7)) для с. в. X, принимающей не более чем m значений, допускает следующее обобщение на случай дискретной с. в., принимающей бесконечное число значений на $\mathbb{Z}_+$:

$$h(X) \leqslant \frac{1}{2} \log \left(2\pi e \left(\mathrm{Var}[X] + \frac{1}{12} \right) \right),$$

где $\mathrm{Var}[X]$ — дисперсия с. в. X.

Решение. 1. В случае гауссовского распределения см. теорему 1.5.5. В случае экспоненциального распределения по неравенству Гиббса для любой с. в. Y с п. р. $f(y)$ имеем

$$\int f(y) \log(f(y) e^{\lambda y} / \lambda) dy \geqslant 0, \quad \text{или} \quad h(y) \leqslant (\lambda \mathsf{E}Y \log e - \log \lambda) = h(\mathrm{Exp}(\lambda)),$$

где равенство достигается тогда и только тогда, когда $Y \sim \mathrm{Exp}(\lambda)$, $\lambda = (\mathsf{E}Y)^{-1}$.

2. Пусть X_0 — дискретная с. в., $\mathsf{P}(X_0 = i) = p_i$, $i = 1, 2, \ldots$, и равномерно распределённая на отрезке $[0, 1]$ с. в. U не зависит от X_0. Положим $X = X_0 + U$. Для с. в. Y, распределённой по нормальному закону с диспер-

сией $\mathrm{Var}[Y] = \mathrm{Var}[X]$, энтропия не меньше чем для с. в. X:

$$h_{\mathrm{diff}}(X) \leqslant h_{\mathrm{diff}}(Y) = \frac{1}{2}\log(2\pi e \mathrm{Var}[Y] = \frac{1}{2}\log\left(2\pi e\left(\mathrm{Var}[X] + \frac{1}{12}\right)\right). \qquad \square$$

Теорема 1.5.7. 1. *Дифференциальная энтропия не меняется при сдвигах*: $\forall \mathbf{y} \in \mathbb{R}^d$ *выполнено равенство*

$$h(\mathbf{X} + \mathbf{y}) = h(\mathbf{X}).$$

2. *При умножении с. в. на константу, к дифференциальной энтропии добавляется слагаемое*:

$$h(a\mathbf{X}) = h(\mathbf{X}) + \log|a| \quad \forall a \in \mathbb{R}.$$

Более того, для любой невырожденной матрицы A размера $d \times d$ при аффинном преобразовании $\mathbf{x} \in \mathbb{R}^d \mapsto A\mathbf{x} + \mathbf{y} \in \mathbb{R}^d$ выполняется равенство

$$h(A\mathbf{X} + \mathbf{y}) = h(\mathbf{X}) + \log|\det A|. \tag{1.5.7}$$

Доказательство заключается в простом вычислении и оставляется читателю в качестве упражнения. Отметим, что значение $\mathsf{E}\mathbf{X}$ не существенно для $h(\mathbf{X})$. $\square$

Пример 1.5.8 (неравенство обработки данных для относительной энтропии). Пусть S — конечное множество и $\mathbf{\Pi} = (\Pi(x, y),\ x, y \in S)$ — стохастическое ядро (т. е. $\Pi(x, y) \geqslant 0$ и $\sum\limits_{y \in S} \Pi(x, y) = 1\ \ \forall x, y \in S$; другими словами, $\Pi(x, y)$ — вероятности переходов в цепи Маркова). Докажите, что $D(p_1\mathbf{\Pi} \parallel p_2\mathbf{\Pi}) \leqslant D(p_1 \parallel p_2)$, где $p_i\mathbf{\Pi}(y) = \sum\limits_{x \in S} p_i(x)\Pi(x, y)$, $y \in S$. Иначе говоря, применение марковской матрицы переходов к обоим распределениям не может увеличить относительную энтропию.

Обобщите этот факт на дифференциальную энтропию.

Решение. В дискретном случае Π определяется стохастической матрицей $(\Pi(x, y))$. По сумматорно-логарифмическому неравенству (см. т. 2, с. 484, или задачу 1.6.6) для любого y имеем

$$\sum_x p_1(x)\Pi(x, y)\log\frac{\sum\limits_w p_1(w)\Pi(w, y)}{\sum\limits_z p_2(z)\Pi(z, y)} \leqslant$$

$$\leqslant \sum_x p_1(x)\Pi(x, y)\log\frac{p_1(x)\Pi(x, y)}{p_2(x)\Pi(x, y)} = \sum_x p_1(x)\Pi(x, y)\log\frac{p_1(x)}{p_2(x)}.$$

Суммируя по y, получаем

$$D(p_1\boldsymbol{\Pi} \parallel p_2\boldsymbol{\Pi}) = \sum_x \sum_y p_1(x)\Pi(x,\, y) \log \frac{\sum\limits_w p_1(w)\Pi(w,\, y)}{\sum\limits_z p_2(z)\Pi(z,\, y)} \leqslant$$

$$\leqslant \sum_x \sum_y p_1(x)\Pi(x,\, y) \log \frac{p_1(x)}{p_2(x)} = D(p_1 \parallel p_2).$$

В непрерывном случае выполняется аналогичное неравенство, нужно лишь суммирование заменить интегрированием. □

Дифференциальная энтропия оказывается полезной в большом разнообразии ситуаций, зачастую совершенно неожиданных. Мы рассмотрим здесь неравенства для детерминантов и отношений детерминантов положительно определённых симметричных матриц. Напомним, что ковариационная матрица $C = (C_{ij})$ случайного вектора $\mathbf{X} = (X_1, \ldots, X_d)$ является положительно определённой, поскольку для любого комплексного вектора $\mathbf{y} = (y_1, \ldots, y_d)$ скалярное произведение $(\mathbf{y},\, C\mathbf{y}) = \sum\limits_{i,j} C_{ij} y_i \bar{y}_j$ имеет вид:

$$\sum_{i,j} \mathsf{E}(X_i - \mu_i)(X_j - \mu_j) y_i \bar{y}_j = \mathsf{E}\left| \sum_i (X_i - \mu_i) y_i \right|^2 \geqslant 0.$$

Следовательно, для любой положительно определённой матрицы C найдётся п. р., при которой C будет матрицей ковариации, например плотность многомерного нормального распределения (если матрица C не является строго положительно определённой, распределение будет вырожденным).

Пример 1.5.9. Если C — положительно определённая симметричная матрица, то $\log(\det C)$ вогнута как функция от матрицы C.

Решение. Возьмём две положительно определённые матрицы $C^{(0)}$ и $C^{(1)}$ и число $\lambda \in (0,\, 1)$. Пусть $\mathbf{X}^{(0)}$ и $\mathbf{X}^{(1)}$ — два вектора, распределённых по многомерному нормальному закону $(\mathbf{X}^{(i)} \sim N(\mathbf{0},\, C^{(i)}))$. Положим, как в теореме 1.2.18, $\mathbf{X} = \mathbf{X}^{(\Lambda)}$, где с. в. Λ принимает два значения 0 и 1 с вероятностями λ и $1 - \lambda$ соответственно и независимо от $\mathbf{X}^{(0)}$ и $\mathbf{X}^{(1)}$. Тогда с. в. $\mathbf{X}$ имеет ковариацию $C = \lambda C^{(0)} + (1 - \lambda) C^{(1)}$, хотя $\mathbf{X}$ уже не

распределено по нормальному закону. Таким образом,

$$\begin{aligned}\frac{1}{2}\log(2\pi e)^d + \frac{1}{2}\log[\det(\lambda C^{(0)} + (1-\lambda)C^{(1)})] = \\ = \frac{1}{2}\log((2\pi e)^d \det C) \geqslant h(X) \text{ (по теореме 1.5.5)} \geqslant \\ \geqslant h(\mathbf{X}|\,\Lambda) \text{ (по теореме 1.2.11)} \geqslant \\ \geqslant \frac{\lambda}{2}\log((2\pi e)^d \det C^{(0)}) + \frac{1-\lambda}{2}\log((2\pi e)^d \det C^{(1)}) = \\ = \frac{1}{2}[\log(2\pi e)^d + \lambda\log(\det C^{(0)}) + (1-\lambda)\log(\det C^{(1)})]. \quad \square\end{aligned}$$

Это свойство часто называют *неравенством Ки Фана*. Впервые оно было доказано в 1950 г. с привлечением гораздо более продвинутых методов. Другое знаменитое неравенство принадлежит Адамару.

Пример 1.5.10. Для положительно определённой симметричной матрицы $C = (C_{ij})$ выполнено неравенство

$$\det C \leqslant \prod_i C_{ii}, \tag{1.5.8}$$

где равенство достигается тогда и только тогда, когда C — диагональная матрица.

Решение. Если $\mathbf{X} = (X_1, \ldots, X_n) \sim N(\mathbf{0}, C)$, то

$$\frac{1}{2}\log[(2\pi e)^d \det C] = h(\mathbf{X}) \leqslant \sum_i h(X_i) = \sum_i \frac{1}{2}\log(2\pi e C_{ii}), \tag{1.5.9}$$

причём равенство достигается тогда и только тогда, когда $X_1, \ldots, X_n$ независимы, т. е. матрица C диагональна. $\square$

Далее мы обсудим так называемое неравенство на экспоненты от энтропии[5] (н. э. э.). Ситуация с н. э. э. довольно интригующая: оно считается одним из «таинственных» фактов теории информации, поскольку не имеет прямой интерпретации. Неравенство было предложено Шенноном; в книге [SW] есть набросок рассуждений в поддержку этого неравенства. Однако первое строгое доказательство н. э. э. появилось только 20 лет спустя, при некоторых довольно жестких условиях, которые до сих пор пытаются ослабить. Шеннон использовал н. э. э. для оценки пропускной способности аддитивного канала с непрерывным шумом пропускной способностью гауссовского канала (см. гл. 4). Н. э. э. также связана с важным свойством монотонности энтропии; примером является теорема 1.5.15, приведённая ниже. Существующие доказательства н. э. э. не совсем элементарны; одна из более коротких версий представлена ниже.

[5] Entropy power inequality.

Теорема 1.5.11 (неравенство Шеннона на экспоненты от энтропии). *Для двух независимых с. в. X и Y с п. р. $f_X(x)$ и $f_Y(x)$, $x \in \mathbb{R}$, выполнено неравенство*

$$h(X+Y) \geqslant h(X'+Y'), \tag{1.5.11}$$

где X' и Y' — независимые с. в., распределённые по нормальному закону, причём $h(X) = h(X')$ и $h(Y) = h(Y')$.

В d-мерном случае неравенство на экспоненты от энтропии выглядит следующим образом: для двух независимых с. в. $\mathbf{X}$ и $\mathbf{Y}$ с п. р. $f_{\mathbf{X}}(\mathbf{x})$ и $f_{\mathbf{Y}}(\mathbf{x})$, $\mathbf{x} \in \mathbb{R}^d$, имеет место неравенство

$$e^{2h(\mathbf{X}+\mathbf{Y})/d} \geqslant e^{2h(\mathbf{X})/d} + e^{2h(\mathbf{Y})/d}. \tag{1.5.12}$$

Легко видеть, что при $d = 1$ формулы (1.5.11) и (1.5.12) эквивалентны. В общем случае из формулы (1.5.11) следует (1.5.12) с учётом формулы (1.5.15), выписанной далее, которую можно вывести независимо. Заметим, что для дискретных с. в. неравенство (1.5.12) может быть как верным, так и ложным. Рассмотрим следующий пример: пусть $X \sim Y$ независимы и $P_X(0) = 1/6$, $P_X(1) = 2/3$, $P_X(2) = 1/6$. Тогда

$$h(X) = h(Y) = \ln 6 - \frac{2}{3}\ln 4, \quad h(X+Y) = \ln 36 - \frac{16}{36}\ln 8 - \frac{18}{36}\ln 18.$$

Прямая проверка показывает, что $e^{2h(\mathbf{X}+\mathbf{Y})/d} = e^{2h(\mathbf{X})/d} + e^{2h(\mathbf{Y})/d}$. Если X и Y — неслучайные константы, то $h(X) = h(Y) = h(X+Y) = 0$ и н. э. э., очевидно, нарушается. Значит, можно сделать вывод, что наличие п. р. является существенным условием, которым нельзя пренебречь. В случае дискретных с. в. н. э. э. может быть переписана в несколько ином виде, но здесь мы не будем обсуждать эту теорию.

Иногда дифференциальная энтропия определяется как $h(X) = -\mathsf{E}\log_2 p(X)$; тогда оценка (1.5.12) принимает вид $2^{h(X+Y)/d} \geqslant 2^{h(X)/d} + 2^{h(Y)/d}$.

Н. э. э. играет весьма важную роль не только в теории информации и теории вероятностей, но также в геометрии и анализе. Для иллюстрации приведём неравенство Брунна—Минковского, частного случая н. э. э. Определим сумму двух множеств как

$$A_1 + A_2 = \{x_1 + x_2 \colon x_1 \in A_1,\ \ x_2 \in A_2\}.$$

По определению $A + \varnothing = A$.

Теорема 1.5.12 (Брунна—Минковского). 1. *Пусть A_1 и A_2 — измеримые множества. Тогда для объёма множеств справедливо неравенство*

$$V(A_1 + A_2)^{1/d} \geqslant V(A_1)^{1/d} + V(A_2)^{1/d}. \tag{1.5.13}$$

2. *Объём суммы двух множеств A_1 и A_2 больше, чем объём суммы двух шаров B_1 и B_2, каждый из которых имеет тот же объём, что и соответствующее множество A_i:*

$$V(A_1 + A_2) \geqslant V(B_1 + B_2), \tag{1.5.14}$$

где B_i — шар и $V(B_i) = V(A_i)$, $i = 1, 2$.

Пример 1.5.13. Пусть C_1 и C_2 — положительно определённые симметричные матрицы размера $d \times d$. Тогда

$$[\det(C_1 + C_2)]^{1/d} \geqslant [\det C_1]^{1/d} + [\det C_2]^{1/d}. \tag{1.5.15}$$

Решение. Пусть $X_1 \sim N(\mathbf{0}, C_1)$, $X_2 \sim N(\mathbf{0}, C_2)$ тогда $X_1 + X_2 \sim \sim N(\mathbf{0}, C_1 + C_2)$. Из неравенства на экспоненты от энтропии следует, что

$$(2\pi e)[\det(C_1 + C_2)]^{1/d} = e^{2h(X_1+X_2)/d} \geqslant$$
$$\geqslant e^{2h(X_1)/d} + e^{2h(X_2)/d} = (2\pi e)[\det C_1]^{1/d} + (2\pi e)[\det C_2]^{1/d}. \quad \square$$

Пример 1.5.14. Тёплицева матрица C размера $n \times n$ характеризуется тем свойством, что $C_{ij} = C_{rs}$, если $|i - j| = |r - s|$. Пусть $C_k = = C(1, 2, \ldots, k)$ — главные миноры положительно определённой тёплицевой матрицы, построенные на строках и столбцах с номерами $1, \ldots, k$. Докажите, что выполнены неравенства

$$|C_1| \geqslant |C_2|^{1/2} \geqslant \ldots \geqslant |C_n|^{1/n}, \tag{1.5.16}$$

где $|C| = \det C$, отношения $|C_n|/|C_{n-1}|$ убывают по n и

$$\lim_{n\to\infty} \frac{|C_n|}{|C_{n-1}|} = \lim_{n\to\infty} |C_n|^{1/n}. \tag{1.5.17}$$

Решение. Пусть $(X_1, X_2, \ldots, X_n) \sim N(\mathbf{0}, C_n)$. Тогда величина $h(X_k | X_{k-1}, \ldots, X_1)$ убывает по k, так как

$$h(X_k | X_{k-1}, \ldots, X_1) = h(X_{k+1} | X_k, \ldots, X_2) \geqslant h(X_{k+1} | X_k, \ldots, X_1),$$

где равенство следует из предположений о тёплицевости, а неравенство — из того факта, что дополнительное условие уменьшает энтропию. Затем мы используем результат задачи 1.6.7, п. 2 (из § 1.6), по которому среднее арифметическое

$$\frac{1}{k} h(X_1, \ldots, X_k) = \frac{1}{k} \sum_{i=1}^{k} h(X_i | X_{i-1}, \ldots, X_1)$$

убывает по k. Теперь неравенства (1.5.16) следуют из соотношения

$$h(X_1, \ldots, X_k) = \frac{1}{2} \log[(2\pi e)^k |C_k|].$$

Так как $h(X_n\,|\,X_{n-1},\,\ldots,\,X_1)$ представляет собой убывающую последовательность, она имеет предел. Следовательно, по теореме о чезаровских средних

$$\lim_{n\to\infty}\frac{h(X_1,\,X_2,\,\ldots,\,X_n)}{n}=\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}h(X_k\,|\,X_{k-1},\,\ldots,\,X_1)=$$

$$=\lim_{n\to\infty}h(X_n\,|\,X_{n-1},\,\ldots,\,X_1).$$

Переформулировав этот факт в терминах определителей, получим соотношение (1.5.17). □

Неравенство на экспоненты от энтропии можно обобщить на случай нескольких слагаемых:

$$e^{2h(X_1+\ldots+X_n)/d}\geqslant\sum_{i=1}^{n}e^{2h(X_i)/d}.$$

Но более интересно то, что имеет место промежуточное неравенство. Пусть $X_1,\,X_2,\,\ldots,\,X_{n+1}$ — последовательность независимых одинаково распределённых с. в. с интегрируемым квадратом. Тогда

$$e^{2h(X_1+\ldots+X_{n+1})/d}\geqslant\frac{1}{n}\sum_{j=1}^{n+1}e^{2h\left(\sum\limits_{i\neq j}X_i\right)/d}. \tag{1.5.18}$$

Как было установлено, дифференциальная энтропия достигает максимума на распределении Гаусса при условии, что дисперсии рассматриваемых с. в. ограничены сверху. Сформулируем без доказательства следующий важный результат, показывающий, что энтропия возрастает с каждым шагом в центральной предельной теореме.

Теорема 1.5.15. *Пусть* $X_1,\,X_2,\,\ldots$ — *последовательность н. о. р. с. в. с интегрируемым квадратом, причём* $\mathsf{E}X_i=0$, $\mathrm{Var}[X_i]=1$. *Тогда*

$$h\left(\frac{X_1+\ldots+X_n}{\sqrt{n}}\right)\leqslant h\left(\frac{X_1+\ldots+X_{n+1}}{\sqrt{n+1}}\right). \tag{1.5.19}$$

В остальной части данного параграфа размещён более сложный материал и он может быть пропущен при первом чтении. Мы приводим здесь доказательство неравенства Шеннона на экспоненты от энтропии (н. э. э.). Как было сказано ранее, впервые оно было сформулировано Шенноном и использовалось для анализа гауссовских каналов передачи сигнала без памяти. В доказательстве мы придерживаемся линии, предложенной в работе [VG]. Нам необходимо углубить понимание свойств непрерывности дифференциальной энтропии.

Здесь мы изучаем только непрерывные с. в. с п. р., принимающие значения в $\mathbb{R}^d$ (т. е. d-мерные вещественные случайные векторы). Как обычно символ $f_{\mathbf{X},\mathbf{Y}}(\mathbf{x}, \mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$, обозначает совместную п. р. двух с. в. $\mathbf{X}$, $\mathbf{Y}$. Соответственно $h(\mathbf{X}, \mathbf{Y})$ — совместная энтропия с. в. $\mathbf{X}$ и $\mathbf{Y}$ и $I(\mathbf{X} : \mathbf{Y})$ — их взаимная энтропия:

$$h(\mathbf{X}, \mathbf{Y}) = -\int f_{\mathbf{X},\mathbf{Y}}(\mathbf{x}, \mathbf{y}) \ln f_{\mathbf{X},\mathbf{Y}}(\mathbf{x}, \mathbf{y})\, d\mathbf{x}\, d\mathbf{y},$$

и $I(\mathbf{X} : \mathbf{Y}) = h(\mathbf{X}) + h(\mathbf{Y}) - h(\mathbf{X}, \mathbf{Y})$. Далее мы используем знакомые соотношения:

$$I(\mathbf{X} : \mathbf{Y}) = h(\mathbf{X}) - h(\mathbf{X} \,|\, \mathbf{Y}) = h(\mathbf{Y}) - h(\mathbf{Y} \,|\, \mathbf{X}), \tag{1.5.20}$$

где

$$h(\mathbf{X} \,|\, \mathbf{Y}) = h(\mathbf{X}, \mathbf{Y}) - h(\mathbf{Y}), \quad h(\mathbf{Y} \,|\, \mathbf{X}) = h(\mathbf{X}, \mathbf{Y}) - h(\mathbf{X}). \tag{1.5.21}$$

Нас интересуют различные свойства непрерывности энтропии, относящиеся к так называемому аддитивному каналу, где с. в. X (сигнал) преобразуется в сумму $X + U$, со с. в. U, представляющей собой «шум» в канале. На самом деле мы рассмотрим несколько более общую схему, в которой X сравнивается с $X\sqrt{\gamma} + U$, где $\gamma > 0$ — параметр (называемый иногда «отношением сигнал–шум»), и исследуем пределы при $\gamma \to +\infty$ или $\gamma \to +0$. Будем предполагать, что с. в. X и U независимы (хотя это предположение может быть ослаблено), и пусть п. р. «шума» равна $f_U(x)$, $\int f_U(x)dx = 1$. Однако сигнал X может иметь более общее распределение, включающее дискретную и абсолютно непрерывную компоненты. Сначала мы проанализируем поведение взаимной энтропии $I(X : X\sqrt{\gamma} + U)$ при $\gamma \to +\infty$. Здесь и далее мы используем (стандартные) обозначения $(b)_+ = \max[0, b]$ и $(b)_- = \min[0, b]$, $d \in \mathbb{R}$.

Лемма 1.5.16. *Пусть X, U — независимые с. в. с п. р. f_X и f_U, где $\int f_X(x)dx = \int f_U(x)dx = 1$. Предположим, что*

1) $\int f_X(x)|\ln f_X(x)|dx < \infty$,

2) *для любого $\varepsilon > 0$ существует такая область $\mathbf{D}_\varepsilon \subseteq \mathbb{R}^d \times \mathbb{R}^d$, что для всех $\gamma > \gamma_0(\varepsilon)$ имеет место неравенство*

$$-\int\limits_{(\mathbb{R}^d \times \mathbb{R}^d)/\mathbf{D}_\varepsilon} \mathbf{1}(f_X(x) > 0) f_X(x) f_U(y) \times \times \left(\ln\left[\int f_X\left(x + \frac{y - v}{\sqrt{\gamma}}\right) f_U(v)dv\right]\right)_- dydx < \varepsilon. \tag{1.5.22}$$

Более того, для всех $(x, y) \in \mathbf{D}_\varepsilon$ равномерно по всем $\gamma > \gamma_0(\varepsilon)$ выполнено следующее неравенство:

$$-\left(\ln\left[\int f_X\left(x + \frac{y - v}{\sqrt{\gamma}}\right) f_U(v)dv\right]\right)_- \leqslant \Psi_\varepsilon(x, y), \tag{1.5.23}$$

где $\Psi_\varepsilon(x, y)$ *— функция, не зависящая от* γ *и удовлетворяющая оценке*

$$\int dx \int dy f_X(x) f_U(y) \Psi_\varepsilon(x, y) < \infty.$$

Кроме того, предположим, что

3) *п. р.* f_X *кусочно непрерывна, т. е.* f_X *непрерывна на каждом открытом подмножестве из* $\mathbf{C}_1, \ldots, \mathbf{C}_N \subseteq \mathbb{R}^d$ (*эти подмножества могут пересекаться лишь по границе*) *с кусочно гладкими границами* $\partial\mathbf{C}_1, \ldots, \partial\mathbf{C}_N$, $\dim \partial\mathbf{C}_i < d$, *и* $f_X = 0$ *на дополнении* $\mathbb{R}^d \setminus \bigcup\limits_{1 \leqslant j \leqslant N} (\mathbf{C}_j \cup \partial\mathbf{C}_j)$.

Более того, будем считать, что функция f_X *ограничена*: $\sup\limits_{x \in \mathbb{R}^d} |f_X(x)| = b < +\infty$.

Тогда

$$h(X) = \lim_{\gamma \to \infty} \big[I(X : X\sqrt{\gamma} + U) + h(U/\sqrt{\gamma}) \big]. \tag{1.5.24}$$

Доказательство. Положив $Y := X\sqrt{\gamma} + U$, можно выписать эквивалентную задачу:

$$[h(X \,|\, Y) - h(U/\sqrt{\gamma})] \to 0.$$

Вспомнив равенство $h(U/\sqrt{\gamma}) = -\ln\sqrt{\gamma} - \int f_U(u) \ln f_U(u) du$, мы увидим, что разность $h(X \,|\, Y) - h(U/\sqrt{\gamma})$ равна

$$\begin{aligned}
&- \int dx \mathbf{1}(f_X(x) > 0) f_X(x) \int f_U(y - x\sqrt{\gamma}) \ln \frac{f_X(x) f_U(y - x\sqrt{\gamma})}{\int du f_X(u) f_U(y - u\sqrt{\gamma})} dy + \\
&\qquad + \ln\sqrt{\gamma} + \int f_U(u) \ln f_U(u) du = \\
&= \int dx \mathbf{1}(f_X(x) > 0) f_X(x) \int f_U(y) \ln \left(\frac{\sqrt{\gamma} \int du f_X(u) f_U(y + (x - u)\sqrt{\gamma})}{f_X(x)} \right) dy = \\
&= \int dx \mathbf{1}(f_X(x) > 0) f_X(x) \int f_U(y) \ln \left(\frac{\int f_X\Big(x + \dfrac{y - v}{\sqrt{\gamma}}\Big) f_U(v) dv}{f_X(x)} \right) dy.
\end{aligned} \tag{1.5.25}$$

Обозначив последний интеграл через $I_\pm(\gamma)$, придём к разложению

$$I(\gamma) = I_+(\gamma) + I_-(\gamma), \tag{1.5.26}$$

где слагаемые $I_\pm(\gamma)$ задаются как положительная и отрицательная части интеграла

$$I_\pm(\gamma) = \int dx \mathbf{1}(f_X > 0) f_X(x) \int f_U(y) \left(\ln \left(\frac{\int f_X\Big(x + \dfrac{y - v}{\sqrt{\gamma}}\Big) f_U(v) dv}{f_X(x)} \right) \right)_\pm dy. \tag{1.5.27}$$

Слагаемое $I_+(\gamma)$ исследуется с помощью теоремы Лебега о мажорируемой сходимости. Действительно, для почти всех x, $y \in \mathbb{R}^d$ имеем

$$\lim_{\gamma\to+\infty} \mathbf{1}(f_X(x) > 0)\left(\ln\left(\frac{\int f_X\left(x + \frac{y-v}{\sqrt{\gamma}}\right) f_U(v)dv}{f_X(x)}\right)\right)_+ = 0, \tag{1.5.28}$$

поскольку

1) $f_X\left(x + \frac{y-v}{\sqrt{\gamma}}\right) \to f_X(x)$ для всех x, y, $v \in \mathbb{R}^d$ из-за непрерывности f_X,

2) $\int f_X\left(x + \frac{y-v}{\sqrt{\gamma}}\right) f_U(v)dv \to f_X(x)$ для всех x, y, так как f_X ограничена.

Далее из формулы (1.5.28) заключаем, что $I_+(\gamma) \to 0$. Здесь мы пишем

$$\left[\ln \int f_X\left(x + \frac{y-v}{\sqrt{\gamma}}\right) f_U(v)dv - \ln f_X(x)\right]_+ \leqslant |\ln b| + |\ln f_X(x)|$$

и вновь прибегаем к теореме Лебега вместе с предположением о неравенстве: $\int f_X(x)\,|\ln f_X(x)|\,dx < +\infty$.

Со слагаемым $I_-(\gamma)$ нужно разбираться иначе. Представим его как $I_-(\gamma) = I_-(\gamma, \mathbf{D}_\varepsilon) + I_-(\gamma, \bar{\mathbf{D}}_\varepsilon)$, ограничив интегрирование по $dxdy$ на $\mathbf{D}_\varepsilon$ и $\bar{\mathbf{D}}_\varepsilon = (\mathbb{R}^d \times \mathbb{R}^d) \setminus \mathbf{D}_\varepsilon$ соответственно. Тот факт, что $I_-(\gamma, \mathbf{D}_\varepsilon) \to 0$, доказывается примерно так же, как и в формуле (1.5.28) (т. е. через теорему Лебега). Для $I_-(\gamma, \bar{\mathbf{D}}_\varepsilon)$ мы имеем $\limsup\limits_{\gamma\to+\infty} -I_-(\gamma, \bar{\mathbf{D}}_\varepsilon) \leqslant \varepsilon$. Так как ε можно выбрать сколь угодно малым, лемма 1.5.16 доказана. □

Ниже мы проверим условия леммы 1.5.16 для некоторых важных случаев.

В дискретной ситуации, когда сигнал X принимает конечное или счётное число значений, имеет место следующее утверждение.

Лемма 1.5.17. *Пусть X и U — независимые с. в. Предположим, что X принимает дискретные значения x_1, x_2, ... с вероятностями $p_X(x_1)$, $p_X(x_2)$, ... и $h(X) = -\sum\limits_{x_i} p_X(x_i)\ln p_X(x_i) < +\infty$. Далее предположим, что п. р. $f_U(x)$ с. в. U ограничена, т. е. $\sup(f_U(x)\colon x \in \mathbb{R}^d) = a < +\infty$, $\int f_U(x)dx = 1$ и*

$$\lim_{\alpha\to\pm\infty} f_U(x + \alpha x_0) = 0 \quad \forall x,\, x_0 \in \mathbb{R}^d \;\; c\; x_0 \neq 0.$$

Допустим, наконец, что $\int f_U(x)\,|\ln f_U(x)|\,dx < +\infty$. Тогда

$$h(X) = \lim_{\gamma\to\infty} I(X : X\sqrt{\gamma} + U). \tag{1.5.29}$$

Доказательство. Как и ранее, обозначив $Y = X\sqrt{\gamma} + U$, вновь сведём доказательство к проверке сходимости $h(X\,|\,Y) \to 0$. Теперь запишем $h(X\,|\,Y)$ в следующем виде:

$$
\begin{aligned}
&-\sum_{i\geqslant j} p_X(x_i) \int f_U(y - x_i\sqrt{\gamma}) \ln \frac{p_X(x_i) f_U(y - x_i\sqrt{\gamma})}{\sum\limits_{j\geqslant 1} p_X(x_j) f_U(y - x_j\sqrt{\gamma})}\, dy = \\
&= -\sum_{i\geqslant j} p_X(x_i) \int dy f_U(y) \ln \Biggl(1 + \sum_{j:\, j\neq i} p_X(x_j) p_X(x_i)^{-1} \times \\
&\qquad\qquad \times f_U(y + (x_j - x_i)\sqrt{\gamma}) f_U(y)^{-1}\Biggr). \qquad (1.5.30)
\end{aligned}
$$

Аргумент логарифма, очевидно, сходится к 1 при $\gamma \to +\infty$ $\forall i \geqslant 1$ и $y \in \mathbb{R}^d$. Поэтому $\forall i \geqslant 1$ и $y \in \mathbb{R}^d$ всё подынтегральное выражение

$$
f_U(y) \ln \Biggl(1 + \sum_{j:\, j\neq i} p_X(x_j) p_X(x_i)^{-1} f_U(y + (x_j - x_i)\sqrt{\gamma}) f_U(y)^{-1}\Biggr)
$$

стремится к 0.

Чтобы гарантировать сходимость интеграла, мы положим

$$
q_i = \sum_{j:\, j\neq i} p_X(x_j) p_X(x_i)^{-1} = 1 - p_X(x_i)^{-1}
$$

и $\psi(y) = \ln f_U(y)$, после чего воспользуемся ограничением

$$
\begin{aligned}
\ln \Biggl(1 + \sum_{j:\, j\neq i} p_X(x_j) p_X(x_i)^{-1} f_U(y - x_j\sqrt{\gamma}) f_U(y)^{-1}\Biggr) &\leqslant \ln\bigl(1 + a q_i e^{-\psi(y)}\bigr) \leqslant \\
&\leqslant \mathbf{1}\bigl(a q_i e^{-\psi(y)} > 1\bigr) \ln\bigl(2 a q_i e^{-\psi(y)}\bigr) + \mathbf{1}\bigl(a q_i e^{-\psi(y)} \leqslant 1\bigr) \ln 2 \leqslant \\
&\leqslant 2\ln 2 + \ln a + \ln(q_i + 1) + |\psi(y)|.
\end{aligned}
$$

Затем мы снова применяем теорему Лебега о мажорируемой сходимости и заключаем, что $\lim\limits_{\gamma\to+\infty} h(X\,|\,Y) = 0$. □

Для доказательства н. э. э. нам ещё нужен анализ поведения $I(X : X\sqrt{\gamma} + U)$ при $\gamma \to 0$.

Лемма 1.5.18. *Пусть X и U — независимые с. в. Предположим, что U обладает ограниченной непрерывной п. р. $f_U \in C^0(\mathbb{R}^d)$, $\int f_U(x)dx = 1$ и $\sup(f_U(x),\ \ x \in \mathbb{R}^d) = a < +\infty$. Предположим, так же как и в лемме* 1.5.16, *что*

$$
\int g_X(u)\,|\ln g_X(u)|\,du + \int f_U(u)\,|\ln f_U(u)|\,du < +\infty.
$$

Тогда

$$\lim_{\gamma\to 0} I(X : X\sqrt{\gamma} + U) = 0. \tag{1.5.31}$$

Доказательство. Вновь обозначим $Y = X\sqrt{\gamma} + U$ и сведём доказательство к проверке того факта, что $h(X\,|\,Y) \to h(X)$. Здесь мы имеем

$$h(X\,|\,Y) = -\int dx g_X(x) \int dy f_U(y - x\sqrt{\gamma}) \ln \frac{g_X(x) f_U(y - x\sqrt{\gamma})}{\int g_X(u) f_U(y - u\sqrt{\gamma}) m_X(du)} =$$

$$= \int dx g_X(x) \int f_U(y) \ln \left(\frac{\int dy g_X(u) f_U(y + (x-u)\sqrt{\gamma}) m_X(du)}{g_X(x) f_U(y)} \right). \tag{1.5.32}$$

В силу непрерывности f_U отношение, стоящее под знаком логарифма, сходится к $\big(g_X(x)\big)^{-1}$ при $\gamma \to 0$ для любых x, $y \in \mathbb{R}^d$. Следовательно, интеграл в формуле (1.5.32) при $\gamma \to 0$ сходится к $h(X)$. Доказательство завершается с помощью теоремы Лебега о мажорируемой сходимости. □

Далее мы рассмотрим несколько случаев, где проверяются предположения леммы 1.5.16. Начнём со случая, в котором п. р. f_X ограничена снизу функцией, пропорциональной гауссовской п. р. Пусть символ φ_Σ (или, короче, σ) закреплён за стандартной d-мерной нормальной п. р. с нулевым средним и строго положительно определённой матрицей ковариации Σ размера $d \times d$:

$$\varphi_\Sigma = \frac{1}{(2\pi)^{d/2} (\det \Sigma)^{1/2}} \exp\Big[-\frac{1}{2} \langle x,\, \Sigma^{-1} x \rangle \Big], \quad x \in \mathbb{R}^d. \tag{1.5.33}$$

Здесь и далее $\langle \cdot\,, \cdot \rangle$ обозначает евклидово скалярное произведение в $\mathbb{R}^d$.

Предложение 1.5.19. *Предположим, что* $f_X(x) \geqslant \alpha \varphi_\Sigma(x)$, $x \in \mathbb{R}^d$, *где* $\alpha \in (0,\, 1]$, *и*

$$\int f_X(x) (|\ln f_X(x)| + \langle x,\, \Sigma^{-1} x \rangle) dx,\ \int f_U(y) \langle y,\, \Sigma^{-1} y \rangle dy < +\infty. \tag{1.5.34}$$

Тогда предположения 1 *и* 2 *леммы* 1.5.16 *выполнены, как и неравенство* (1.5.22) *с функцией* $\gamma_0(\varepsilon) = 1$ *и областью* $\mathbf{D}_\varepsilon \equiv \mathbb{R}^d \times \mathbb{R}^d$, *и*

$$\Psi(x,\, y) = \frac{1}{2} (\langle x,\, \Sigma^{-1} x \rangle + \langle y,\, \Sigma^{-1} y \rangle) +$$

$$+ \left| \ln \int \exp[-\langle v,\, \Sigma^{-1} v \rangle] f_U(v) dv \right| + \rho, \tag{1.5.35}$$

где $\rho = \left| \ln \dfrac{\alpha}{(2\pi)^{d/2} \det(\Sigma)^{1/2}} \right|$.

Доказательство. Имеем

$$\int f_X\Big(x+\frac{y-v}{\sqrt{\gamma}}\Big)f_U(v)dv \geqslant \alpha\int \varphi_\Sigma\Big(x+\frac{y-v}{\sqrt{\gamma}}\Big)f_U(v)dv \geqslant$$
$$\geqslant \frac{\alpha}{(2\pi)^{d/2}(\det\Sigma)^{1/2}}\int \exp\Big[-\frac{1}{2}\Big\langle x+\frac{y-v}{\sqrt{\gamma}},\,\Sigma^{-1}\Big(x+\frac{y-v}{\sqrt{\gamma}}\Big)\Big\rangle\Big]f_U(v)dv \geqslant$$
$$\geqslant \frac{\alpha}{(2\pi)^{d/2}(\det\Sigma)^{1/2}}\exp\Big[-\frac{1}{2}\langle x,\,\Sigma^{-1}x\rangle\Big]\exp\Big[-\frac{1}{\gamma}\langle y,\,\Sigma^{-1}y\rangle\Big]\times$$
$$\times\int \exp\Big[-\frac{1}{\gamma}\langle v,\,\Sigma^{-1}v\rangle\Big]f_U(v)dv.$$

Отсюда получаем, что для всех $x,\ y\in\mathbb{R}^d$ выполнено неравенство

$$-\Big(\ln\int f_X\Big(x+\frac{y-v}{\sqrt{\gamma}}\Big)f_U(v)dv-\ln f_X(x)\Big)_- \leqslant \frac{1}{2}\langle x,\,\Sigma^{-1}x\rangle+\frac{1}{\gamma}\langle y,\,\Sigma^{-1}y\rangle+$$
$$+\Big|\ln\int\exp\Big[-\frac{1}{\gamma}\langle v,\,\Sigma^{-1}v\rangle\Big]f_U(v)dv\Big|+|\ln f_X(x)|+\Big|\ln\frac{\alpha}{(2\pi)^{d/2}(\det\Sigma^{1/2}}\Big|,$$

причём п. ч. этого неравенства убывает по γ. При $\gamma=1$ оно даёт оценку (1.5.23). □

Доказательство предложения 1.5.19 нетрудно обобщить на случай более общей оценки снизу:

$$f_X(x)\geqslant\exp(-P(x)),\qquad x\in\mathbb{R}^d,$$

где $P(x)$ — многочлен от $x\in\mathbb{R}^d$, ограниченный снизу. Конечно, нужно предполагать существование конечных полиномиальных моментов для обеих п. р. f_X и f_U. Более того, нижние границы для f_X можно заменить нижними границами для f_U; в частности, это включает в себя случай, когда $f_U(y)\geqslant\alpha\varphi(y)$, $y\in\mathbb{R}^d$, $\alpha\in(0,\,1]$, и выполнено условие (1.5.34).

Противоположный случай, также представляющий значительный интерес, связан с ситуацией, когда п. р. f_X и f_U имеют компактные носители. В этой книге мы не будем изучать его в полной общности. Тем не менее мы обсудим пару примеров, чтобы показать, какие механизмы лежат в основе сходимости. Для $A,\ B\in\mathbb{R}^d$ обозначим

$$[[A,\,B]]=\prod_{1\leqslant j\leqslant d}[A_j,\,B_j]$$

(предполагая, что $A_i<B_i\ \forall i$).

Пример 1.5.20. Пусть п. р. f_X принимает конечное множество значений. Предположим, что п. р. f_U, имеющая компактный носитель $[[A,\,B]]$, удовлетворяет неравенству

$$f_U(y)\geqslant\frac{\alpha}{\prod\limits_{1\leqslant i\leqslant d}(B_i-A_i)}\mathbf{1}(A_i<y<B_i,\ \ i=1,\,\ldots,\,d),\tag{1.5.36}$$

где $0 < \alpha < 1$ и $A = (A_1, \ldots, A_d)$, $B = (B_1, \ldots, B_d) \in \mathbb{R}^d$, $-\infty < A_i < B_i < +\infty$. Тогда выполнено предположение 1 леммы 1.5.16 с функцией $\Psi_\varepsilon(x, y) \equiv 0$ и областью $\mathbf{D}_\varepsilon = \prod_{1 \leqslant j \leqslant d} \mathbf{D}_\varepsilon^{(i)}$, где множества $\mathbf{D}_\varepsilon^{(i)}$ определены формулами (1.5.40). Более того, $\gamma_0 = C\varepsilon^{-2/d}$.

Решение. Рассмотрим сначала скалярный случай, когда $f_X(x) = \frac{1}{b-a}\mathbf{1}(a < x < b)$, $-\infty < a < b < +\infty$, в то время как f_U имеет носитель $[A, B]$ и удовлетворяет условию $f_U(y) \geqslant \frac{\alpha}{B-A}\mathbf{1}(A < y < B)$, $0 < \alpha < 1$ и $-\infty < A < B < +\infty$. Выберем $\gamma > 4(B-A)^2/(b-a)^2$. Тогда можно записать

$$I := -\int dx 1(f_X(x) > 0) f_X(x) \int dy f_U(y) \left(\ln \left[\int f_X\left(x + \frac{y-v}{\sqrt{\gamma}}\right) f_u(v) dv \Big/ f_X(x) \right] \right)_- =$$

$$= -\frac{1}{b-a} \int_a^b dx \int_A^B dy f_U(y) \left(\ln \left[\int_{A \vee (y+(x-b)\sqrt{\gamma})}^{B \wedge (y+(x-a)\sqrt{\gamma})} f_U(v) dv \right] \right)_- := I(0) + I(1). \tag{1.5.37}$$

Разложение $I = I(0) + I(1)$ правой части формулы (1.5.37) выделяет «внутренний» член $I(0)$, который вырождается, и «граничный» член $I(1)$, который предстоит еще оценивать. Более точно, $I(0) = I_-(0) + I_0(0) + I_+(0)$, где все слагаемые $I_-(0)$, $I_0(0)$ и $I_+(0)$ равны нулю. Формально $I_-(0)(b-a)$ равно

$$-\int_a^{a+(B-A)/\sqrt{\gamma}} dx \int_{B-(x-a)\sqrt{\gamma}}^B dy f_U(y) \left(\ln \left[\int_A^B dv f_U(v) \right] \right)_-, \tag{1.5.38}$$

$I_0(0)(b-a)$ равно

$$\int_{a+(B-A)/\sqrt{\gamma}}^{b-(B-A)/\sqrt{\gamma}} dx \int_A^B dy f_U(y) \left(\ln \left[\int_A^B dv f_U(v) \right] \right)_- \tag{1.5.39а}$$

и $I_+(0)(b-a)$ равно

$$-\int_{b-(B-A)/\sqrt{\gamma}}^b dx \int_A^{A+(b-x)\sqrt{\gamma}} dy f_U(y) \left(\ln \left[\int_A^B dv f_U(v) \right] \right)_-. \tag{1.5.39б}$$

Соответственно множество $\mathbf{D}_\varepsilon$ в рассматриваемом случае является объединением трёх подмножеств $\mathbf{D}_\varepsilon = \mathbf{D}_{\varepsilon,-} \cup \mathbf{D}_{\varepsilon,0} \cup \mathbf{D}_{\varepsilon,+}$, где

$$\begin{aligned}
&\mathbf{D}_{\varepsilon,-} = \{(x,\, y)\colon a < x < a + (B-A)\sqrt{\varepsilon},\ \ B - (x-a)/\sqrt{\varepsilon} < y < B\},\\
&\mathbf{D}_{\varepsilon,0} = (a + (B-A)\sqrt{\varepsilon},\, b - (B-A)\sqrt{\varepsilon}\,) \times (A,\, B),\\
&\mathbf{D}_{\varepsilon,+} = \{(x,\, y)\colon b - (B-A)\sqrt{\varepsilon} < x < b,\, A < y < A + (b-x)/\sqrt{\varepsilon}\,\}.
\end{aligned} \tag{1.5.40}$$

Заметим, что до сих пор нам не было нужды использовать верхнюю границу п. р. f_U; см. рис. 1.9.

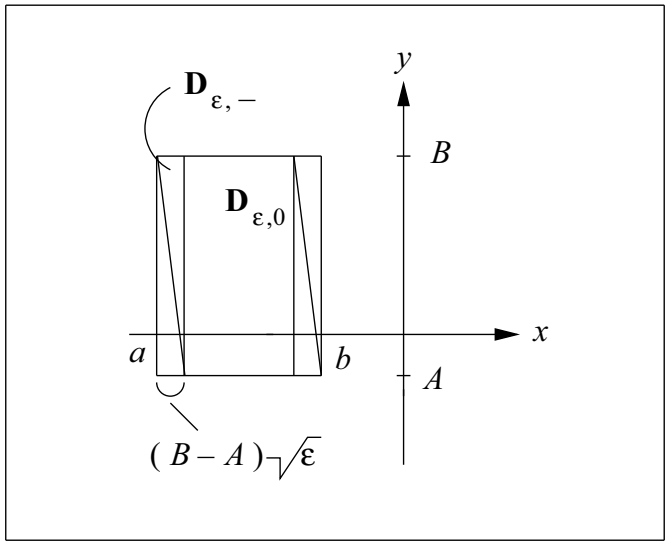


Рис. 1.9

Далее, $I(1) = I_-(1) + I_+(1)$, где $I_-(1)(b-a)$ и $I_+(1)(b-a)$ совпадают с интегралами

$$-\int\limits_a^{a+(B-A)/\sqrt{\Upsilon}} dx \int\limits_A^{B-(x-a)\sqrt{\Upsilon}} dy f_U(y) \left(\ln \left[\int\limits_A^{y+(x-a)\sqrt{\Upsilon}} dv f_U(v) \right] \right)_-, \tag{1.5.41}$$

$$-\int\limits_{b-(B-A)/\sqrt{\Upsilon}}^{b} dx \int\limits_{A+(b-x)\sqrt{\Upsilon}}^{B} dy f_U(y) \left(\ln \left[\int\limits_{y+(x-b)\sqrt{\Upsilon}}^{B} dv f_U(v) \right] \right)_- \tag{1.5.42}$$

соответственно.

Нам нужно оценить сверху интегралы $I_-(1)$ и $I_+(1)$. Для определённости мы сосредоточимся на $I_-(1)$; изменения для $I_+(1)$ очевидны. Член

$I_-(1)(b-a)$ ограничивается сверху величиной

$$\leqslant -\int\limits_a^{a+(B-A)/\sqrt{\gamma}} dx \int\limits_A^{B-(x-a)\sqrt{\gamma}} dy f_U(y) \ln\left[\frac{\alpha}{B-A}(y+(x-a)\sqrt{\gamma}-A)\right] =$$

$$= -\int\limits_0^{(B-A)/\sqrt{\gamma}} dx \int\limits_0^{B-A-x\sqrt{\gamma}} dy f_U(y+A) \ln\left[\frac{\alpha}{B-A}(y+x\sqrt{\gamma})\right] =$$

$$= -(B-A)\int\limits_0^{1/\sqrt{\gamma}} dx \int\limits_0^{1-x\sqrt{\gamma}} dy f_U(y(B-A)+A) \ln[\alpha(y+x\sqrt{\gamma})] =$$

$$= -(B-A)\frac{1}{\sqrt{\gamma}}\int\limits_0^1 dx \int\limits_0^{1-x} dy f_U(y(B-A)+A) \ln[\alpha(y+x)]. \quad (1.5.43)$$

Остаётся проверить, что интеграл в п. ч. формулы (1.5.43) конечен.

Но подынтегральное выражение в п. ч. формулы (1.5.43) имеет особенность только в точке $x=y=0$ и интегрируемо. Аналогичные вычисления можно проделать и для $I_+(1)$. Таким образом, в упрощённой ситуации, которую мы рассматриваем, член I в формуле (1.5.37) подчиняется неравенству $I \leqslant C/\sqrt{\gamma}$. В многомерной ситуации после предположения о том, что $X \sim \mathbf{U}([[A, B]])$, аналогичные рассуждения дадут оценку $I \leqslant C\gamma^{-d/2}$. Обобщение наших рассуждений на общий скалярный случай, когда f_X принимает конечное число значений, проводится напрямую. В многомерной ситуации, когда $X \sim U \sim \mathrm{U}([0, 1]^d)$, похожие вычисления показывают, что $I = C\gamma^{-d/2}$. Наконец, когда X принимает конечное число значений, справедливы аналогичные оценки. □

Пример 1.5.21. Пусть как f_X, так и f_U имеют пирамидальный вид:

$$f_X(x) = \prod_{i=1}^d (1-|x_i|)_+, \quad f_U(y) = \prod_{i=1}^d \frac{1}{a_i}\Big(1-\frac{1}{a_i}|y_i-b_i|\Big)_+, \quad x, y \in \mathbb{R}, \quad (1.5.44)$$

где $a_1, \ldots, a_d > 0$ и $-\infty < b_i < +\infty$, $i = 1, \ldots, d$. Тогда выполнено предположение 2 леммы 1.5.16 с областью

$$\mathbf{D}_\varepsilon = ([[-1+\underline{\varepsilon}, -\underline{\varepsilon}]]) \times [[b-a, b+a]], \quad (1.5.45)$$

где $a = (a_1, \ldots, a_d)$, $(b_1 \ldots, b_d)$, $\underline{\varepsilon} = (\varepsilon, \ldots, \varepsilon) \in \mathbb{R}^d$ и $\varepsilon \in (0, 1/2)$. Далее, $\gamma_0(\varepsilon) = 1/(4\varepsilon^2)$, и функция $\Psi_\varepsilon(x, y)$ задаётся формулой

$$\Psi_\varepsilon(x, y, \gamma) = \prod_{i=1}^d \Big|1 - 2\varepsilon\frac{a_i + b_i + y_i(\mathrm{sgn}x_i)}{1-|x_i|}\Big|. \quad (1.5.46)$$

Решение. Рассмотрим сначала скалярный случай (где обе п. р. имеют треугольный вид) и предположим без потери общности, что $b = 0$. Прямоугольник $(-1, 1) \times (-a, 0)$ на (x, y)-плоскости удобно обозначить через $\mathcal{R}$. Для $(x, y) \in \mathcal{R}$ положим

$$J(= J(x, y)) = \int dv f_U(v) f_X\Big(x + \frac{y - v}{\sqrt{\gamma}}\Big) = \\ = \sqrt{\gamma} \int du f_X(u) f_U((x - u)\sqrt{\gamma} + y). \quad (1.5.47)$$

Тогда для $\sqrt{\gamma} > a$ на параллелограмме

$$\mathcal{P}_+(= \mathcal{P}_+(\gamma)) = \{(x, y) \in \mathcal{R}\colon a - x\sqrt{\gamma} < y < \sqrt{\gamma}(1 - x) - a\}$$

будем иметь

$$J = \frac{\sqrt{\gamma}}{a}\left(\int\limits_{x + \frac{y}{\sqrt{\gamma}}}^{x + \frac{y+a}{\sqrt{\gamma}}} (1 - u)\Big(1 - \frac{1}{a}(\sqrt{\gamma}(x - u) + y)\Big) du + \right. \\ \left. + \int\limits_{x + \frac{y+a}{\sqrt{\gamma}}}^{x + \frac{y}{\sqrt{\gamma}}} (1 - u)\Big(\frac{1}{a}(\sqrt{\gamma}(x - u) + y) - 1\Big) du\right).$$

Прямым вычислением находим, что

$$J = 1 - x - \frac{1}{\sqrt{\gamma}}(a + y).$$

Так что при $\sqrt{\gamma} > a$ в параллелограмме $\mathcal{P}_+$ имеем

$$J(x, y) = 1 - x - \frac{1}{\sqrt{\gamma}}(a + y) \quad \text{и} \quad \ln \frac{J(x, y)}{f_X(x)} = \ln\Big(1 - \frac{y + a}{\sqrt{\gamma}(1 - x)}\Big). \quad (1.5.48)$$

Следовательно, параллелограмм $\mathcal{P}_+$ соответствует тому случаю, в котором носитель скалярной п. р. полностью лежит в интервале $(0, 1)$; правая часть носителя f_X изображена на рис. 1.10.

Аналогично на симметричном параллелограмме

$$\mathcal{P}_-(= \mathcal{P}_-(\gamma)) = \{(x, y) \in \mathcal{R}\colon -(1 + x)\sqrt{\gamma} + a < y < -\sqrt{\gamma}x - a\}$$

имеем

$$J(x, y) = 1 - x\frac{1}{\sqrt{\gamma}}(a - y) \quad \text{и} \quad \ln \frac{J(x, y)}{f_X(x)} = \ln\Big(1 - \frac{a - y}{\sqrt{\gamma}(1 + x)}\Big). \quad (1.5.49)$$

Этот параллелограмм соответствует случаю, в котором носитель п. р. из формулы (1.5.37) лежит в интервале $(-1, 0)$. На объединении $\mathcal{P} = \mathcal{P}_+ \cup \mathcal{P}_-$

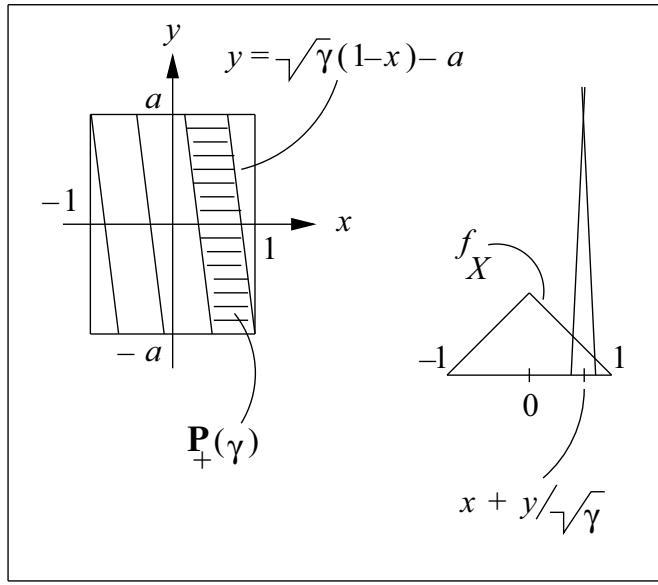


Рис. 1.10

получаем

$$H(x,\, y,\, \gamma) := \ln \frac{J(x,\, y)}{f_X(x)} = \ln \left(1 - \frac{a + y(\mathrm{sgn} x)}{\sqrt{\gamma}(1 - |x|)}\right).$$

Если положить $H(x,\, y,\, \gamma) = 0$ на множестве $\mathcal{R} \setminus \mathcal{P}$, то функция $H(x,\, y,\, \gamma)$ будет поточечно сходиться к 0 на всём $\mathcal{R}$. Зафиксировав $\varepsilon \in (0,\, 1/2)$, выберем $\gamma > 1/(4\varepsilon^2)$. На множестве $\mathbf{D}_\varepsilon$ будет выполнено неравенство

$$|H(x,\, y,\, \gamma)| \leqslant |H(x,\, y,\, 1/(4\varepsilon^2))| := \Psi_\varepsilon(x,\, y).$$

Дополнение $\mathcal{R} \setminus \mathcal{P}$ разбивается на шесть областей (правильный треугольник с вершиной в точке $(-1,\, -a)$, плюс смежная трапеция, расположенная слева от правильного треугольника, с вершиной в точке $(1,\, a)$, плюс смежная трапеция справа от треугольника и два смежных параллелограмма в середине). Эти области соответствуют различным положениям «центра» и концам носителя п. р. $x \mapsto \sqrt{\gamma} f_U((x - u)\sqrt{\gamma} + y)$ относительно $(-1,\, 1)$ (исключая случаи, покрытые множеством $\mathcal{P}$). На каждой из этих областей функция $J(x,\, y)$ является полиномом степени не выше 3. На правой части

треугольника $\{(x, y) \in \mathcal{R}\colon \sqrt{\gamma}(1-x) < y\}$ выполнено равенство

$$J(x, y) = \frac{\sqrt{\gamma}}{a} \int\limits_{x+\frac{y-a}{\sqrt{\gamma}}}^{1} (1-u)\Big(\frac{1}{a}(\sqrt{\gamma}(x-u)+y) - 1\Big)du.$$

Далее, на правой части трапеции $\{(x, y) \in \mathcal{R}\colon \sqrt{\gamma}(1-x) - a < y < \sqrt{\gamma}(1-x)\}$ выполнено равенство

$$J(x, y) = \frac{\sqrt{\gamma}}{a}\Bigg[\int\limits_{x+\frac{y}{\sqrt{\gamma}}}^{1} (1-u)\Big(1 - \frac{1}{a}(\sqrt{\gamma}(x-u)+y)\Big)du + \int\limits_{x+\frac{y-a}{\sqrt{\gamma}}}^{x+\frac{y}{\sqrt{\gamma}}} (1-u)\Big(\frac{1}{a}(\sqrt{\gamma}(x-u)+y) - 1\Big)du\Bigg].$$

Наконец, на правой части параллелограмма $\{(x, y) \in \mathcal{R}\colon -x\sqrt{\gamma} < y < a - x\sqrt{\gamma}\}$ имеет место такое соотношение:

$$J(x, y) = \frac{\sqrt{\gamma}}{a}\Bigg[\int\limits_{x+\frac{y-a}{\sqrt{\gamma}}}^{0} (-1+u)\Big(1 - \frac{1}{a}(\sqrt{\gamma}(x-u)+y)\Big)du + \int\limits_{0}^{x+\frac{y}{\sqrt{\gamma}}} (1-u)\Big(1 - \frac{1}{a}(\sqrt{\gamma}(x-u)+y)\Big)du + \int\limits_{x+\frac{y}{\sqrt{\gamma}}}^{(x+\frac{y+a}{\sqrt{\gamma}}\wedge 1)} (1-u)\Big(\frac{1}{a}(\sqrt{\gamma}(x-u)+y) - 1\Big)du\Bigg].$$

Аналогичные формулы справедливы для левых частей многоугольников. Интегралы

$$\iint f_X(x) f_U(y) |\ln[J(x, y)/f_X(x)]| dxdy \tag{1.5.50}$$

над каждой из этих областей оцениваются прямым вычислением. Они ведут себя как $O(1/\sqrt{\gamma})$. Кроме того, чтобы разобраться с дополнением $\mathcal{R} \setminus \mathbf{D}_\varepsilon$, нам следует рассмотреть множество $\mathcal{P} \setminus \mathbf{D}_\varepsilon$ и проинтегрировать функцию $J(x, y)$ из формул (1.5.46) и (1.5.48). Это тоже можно сделать прямым вычислением; соответствующие интегралы оцениваются как $O(\varepsilon)$. Следовательно, интеграл (1.5.50) по всей компоненте $\mathcal{R} \setminus \mathbf{D}_\varepsilon$ не превосходит $C\varepsilon$ при правильно выбранной константе $C > 0$.

Приведённое рассуждение легко обобщается на d-мерный случай, так как мы там будем иметь дело с произведением интегралов. □

Нам также потребуется удобное представление взаимной энтропии $I(X : X\sqrt{\gamma} + U)$ для случая, когда U — d-мерная гауссовская с. в.

Лемма 1.5.22. *Пусть X и N — независимые с. в., где с. в. $N \sim N(\mathbf{0}, \Sigma)$, а п. р. с. в. X равна $g_X(x)$. Предположим, что $\int g_X(x)\,|x|^2 dx < +\infty$. При данном $\gamma > 0$ запишем взаимную энтропию $I(X : X\sqrt{\gamma} + N)$ между X и $X\sqrt{\gamma} + N$ как*

$$-\int g_X(x)\varphi(u - x\sqrt{\gamma})\ln[g_X(x)\varphi(u - x\sqrt{\gamma})]du dx + \\ + \int g_X(x)\ln g_X(x)dx + \int f_{X\sqrt{\gamma}+N}(u)\ln f_{X\sqrt{\gamma}+N}(u)du,$$

где

$$f_{X\sqrt{\gamma}+N}(u) = \int g_X(x)\varphi(u - x\sqrt{\gamma})dx. \tag{1.5.51}$$

Тогда

$$\frac{d}{d\gamma}[I(X : X\sqrt{\gamma} + N) + h(N/\sqrt{\gamma})] = \frac{1}{2}M(X;\,\gamma) - \frac{1}{2\gamma}, \tag{1.5.52}$$

где

$$M(X;\,\gamma) = \mathsf{E}[|X - \mathsf{E}(X\,|\,X\sqrt{\gamma} + N)|^2].$$

Доказательство. Продифференцировав выражение для $I(X : X\sqrt{\gamma} + N)$ в формуле (1.5.51), заметим, что производная совместной энтропии $h(X,\, X\sqrt{\gamma} + N)$ равна нулю, так как $h(X,\, X\sqrt{\gamma} + N)$ не зависит от $\gamma > 0$:

$$h(X,\, X\sqrt{\gamma} + N) = \\ = -\int g_X(x)\varphi(u - x\sqrt{\gamma})\big[\ln g_X(x) + \ln\varphi(u - x\sqrt{\gamma})\big]dx du = h(X) + h(N).$$

Производная обычной энтропии $h(X\sqrt{\gamma} + N)$ требует некоторых вычислений

$$\frac{d}{d\gamma}h(X\sqrt{\gamma}+N) = -\frac{d}{d\gamma}\int f_{X\sqrt{\gamma}+N}(u)\ln f_{X\sqrt{\gamma}+N}(u)du = \\ = \int \frac{1}{2\sqrt{\gamma}}\int g_X(y)\varphi(u - \sqrt{\gamma}y)\langle(u - \sqrt{\gamma}y), \Sigma^{-1}y\rangle dy \ln\int g_X(z)\varphi(u - \sqrt{\gamma}z)dz du + \\ + \int \frac{1}{2\sqrt{\gamma}}\int g_X(y)\varphi(u - \sqrt{\gamma}y)dy + \frac{\int g_X(w)\varphi(u - \sqrt{\gamma}w)\langle(u - \sqrt{\gamma}w), \Sigma^{-1}w\rangle dw}{\int g_X(z)\varphi(u - \sqrt{\gamma}z)dz}. \tag{1.5.53}$$

Второе слагаемое равно 0, так как

1) интегралы

$$\int g_X(y)\varphi(u-\sqrt{\gamma}y)dy \quad \text{и} \quad \int g_X(z)\varphi(u-\sqrt{\gamma}z)dz$$

взаимно уничтожаются и 2) оставшееся интегрирование можно сначала проводить по du, что даёт 0 при любом w.

Первый интеграл надо брать по частям. Всё это приводит к представлению

$$\frac{d}{d\gamma}I(X : X\sqrt{\gamma}+N) = \frac{1}{2\sqrt{\gamma}}\iint g_X(y)\varphi(u-\sqrt{\gamma}y)\times$$
$$\times\frac{\int g_X(x)\varphi(u-\sqrt{\gamma}x)\langle(u-\sqrt{\gamma}x),\,\Sigma^{-1}x\rangle dx}{\int g_X(z)\varphi(u-\sqrt{\gamma}z)dz}dydu =$$
$$= \frac{1}{2\sqrt{\gamma}}\iint dydu g_X(y)\varphi(u-\sqrt{\gamma}y)\frac{1}{\int g_X(z)\varphi(u-\sqrt{\gamma}z)dz}\times$$
$$\times\int g_X(x)\varphi(u-\sqrt{\gamma}x)\big[\langle(u-\sqrt{\gamma}y),\,\Sigma^{-1}y\rangle+\sqrt{\gamma}\langle(y-x),\,\Sigma^{-1}y\rangle\big]dx. \tag{1.5.54}$$

Интеграл, возникающий из слагаемого $\langle(u-\sqrt{\gamma}y),\,\Sigma^{-1}y\rangle$ равен нулю, поскольку средний вектор п. р. φ нулевой. Остаток, получающийся из вклада разности $\langle y,\,\Sigma^{-1}y\rangle - \langle x,\,\Sigma^{-1}y\rangle$, равен

$$\frac{1}{2}\,\mathsf{E}\big[|X-\mathsf{E}(X\,|\,X\sqrt{\gamma}+N|^2\big].$$

С другой стороны, первый член правой части формулы (1.5.54) равен

$$\int\Big|x-\frac{\int g_X(y)\varphi(u-\sqrt{\gamma}y)\Sigma y m_X(dy)}{\int g_X(z)\varphi(u-\sqrt{\gamma}z)m_X(dz)}\Big|^2\times g_X(x)\varphi(u-\sqrt{\gamma}x)m_X(dx)\,du =$$
$$= \mathsf{E}\big[|X-\mathsf{E}(X\sqrt{\gamma}+N)|^2\big] \equiv M(X;\,\gamma). \quad \square$$

Теперь мы собираемся вывести н. э. э. (1.5.11), (1.5.12) для с. в. X с п. р. f_X, где $\int f_X(x)dx = 1$. Предположим, что f_X удовлетворяет предположениям лемм 1.5.16 и 1.5.19, и применим эти леммы с $U\sim N(\mathbf{0},\,\Sigma)$. Следовательно, для любого $\varepsilon>0$ выполнено соотношение

$$h(X) = \lim_{\gamma\to\infty}\big[I(X : X\sqrt{\gamma}+N)+h(N/\sqrt{\gamma})\big] =$$
$$= \int_{\varepsilon}^{+\infty}\frac{d}{d\gamma}\big[I(X : X\sqrt{\gamma}+N)+h(N/\sqrt{\gamma})\big]d\gamma + I(X : X\sqrt{\gamma}+N)+h(N/\sqrt{\varepsilon}) =$$
$$= \frac{1}{2}\int_{\varepsilon}^{+\infty}\Big[M(X;\,\gamma)-\frac{1}{\gamma}\mathbf{1}(\gamma>1)\Big]d\gamma + h(N) + I(X : X\sqrt{\varepsilon}+N). \tag{1.5.55}$$

Здесь мы пользуемся тождеством $\int_{\varepsilon}^{1}(1/\gamma)d\gamma = -\ln\varepsilon$. По лемме 1.5.19 последний член в соотношении (1.5.55) стремится к 0 при $\varepsilon \to 0$. Следовательно, для с. в. X с п. р. $f_X \in C^0$ получаем

$$h(X) = h(N) + \frac{1}{2}\int_0^\infty \Big[M(X;\,\gamma) - \mathbf{1}(\gamma > 1)\frac{1}{\gamma}\Big]d\gamma. \tag{1.5.56}$$

В том случае, когда X принимает дискретные значения в $\mathbb{R}^d$, (1.5.56) меняется на такую формулу:

$$h(X) = h(N) + \frac{1}{2}\int_0^\infty M(X;\,\gamma)d\gamma, \tag{1.5.57}$$

которая выводится в простом предположении о том, что $h(X) < +\infty$, ввиду лемм 1.5.2 и 1.5.4. Однако равенство (1.5.52) не имеет места.

Доказательство н. э. э. при $d = 1$ основывается на соотношении (1.5.36) и следующем факте из работы [L].

Лемма 1.5.23. *Пусть $\mathcal{X}$ — фиксированный класс распределений вероятностей на $\mathbb{R}$. Неравенство*

$$h(X_1\cos\theta + X_2\sin\theta) \geqslant h(X_1)\cos^2\theta + h(X_2)\sin^2\theta \tag{1.5.58}$$

справедливо для произвольного $\theta \in [0,\, 2\pi]$ и любой пары независимых с. в. X_1, X_2 с распределениями из $\mathcal{X}$ тогда и только тогда, когда н. э. э. выполняется для всякой пары с. в. X_1, X_2 с распределениями из $\mathcal{X}$.

Доказательство. Выберем произвольные независимые с. в. X и Y и положим

$$\operatorname{tg}\theta = e^{h(Y)-h(X)}, \quad X_1 = X/\cos\theta, \quad Y_1 = Y/\sin\theta. \tag{1.5.59}$$

Тогда

$$\cos^2\theta = \frac{e^{2h(X)}}{e^{2h(X)} + e^{2h(Y)}}, \quad \sin^2\theta = \frac{e^{2h(Y)}}{e^{2h(X)} + e^{2h(Y)}}.$$

В силу формулы (1.5.7) неравенство (1.5.58) принимает вид

$$h(X+Y) \geqslant (h(X) - \log(\cos\theta))\cos^2(\theta) + (h(Y) - \log(\sin\theta))\sin^2(\theta) =$$
$$= \frac{1}{2}\log(e^{2h(X)} + e^{2h(Y)}),$$

т. е. совпадает с (1.5.12). Для доказательства в противоположную сторону выберем X и Y при фиксированных произвольном θ и независимых X_1, X_2 так, чтобы выполнялось условие (1.5.59). Затем, прологарифмировав неравенство (1.5.12), получим требуемое в силу выпуклости логарифмической функции. □

Теорема 1.5.24. *Пусть X_1, X_2 — с. в. со значениями в $\mathbb{R}$ и непрерывными ограниченными п. р. $f_{X_1}(x)$, $f_{X_2}(x)$, $x \in \mathbb{R}$, удовлетворяющими условию* 2) *леммы* 1.5.16. *Предположим, что дифференциальные энтропии $h(X_1)$ и $h(X_2)$ подчиняются неравенству $-\infty < h(X_1)$, $h(X_2) < +\infty$. Тогда выполнено н. э. э.* (*см. неравенство* (1.5.12)).

Доказательство. Учитывая лемму 1.5.23, достаточно проверить неравенство (1.5.58) для любого $\theta \in (0, 2\pi)$ и любой пары с. в. X_1, X_2 с непрерывными ограниченными п. р. $f_{X_i}(x)$, $i = 1, 2$. Возьмём произвольную такую пару и выберем с. в. $N \sim \mathrm{N}(0, 1)$. Для доказательства мы применяем формулу (1.5.56) к с. в. $X = X_1 \cos\theta + X_2 \sin\theta$:

$$h(X_1\cos\theta + X_2\sin\theta) = h(N) + \frac{1}{2}\int\limits_0^\infty \Big(M(X_1\cos\theta + X_2\sin\theta;\,\gamma) - \mathbf{1}(\gamma > 1)\frac{1}{\gamma}\Big)\,d\gamma.$$

Для доказательства неравенства (1.5.58) нам нужно проверить, что

$$M(X_1\cos\theta + X_2\sin\theta;\,\gamma) \geqslant M(X_1;\,\gamma)\cos^2\theta + M(X_2;\,\gamma)\sin^2\theta. \qquad (1.5.60)$$

Чтобы завершить доказательство, возьмём две независимые с. в. N_1, $N_2 \sim \mathrm{N}(0, 1)$ и положим

$$Z_1 = X_1\sqrt{\gamma} + N_1, \quad Z_2 = X_2\sqrt{\gamma} + N_2 \ \text{ и } \ Z = Z_1\cos\theta + Z_2\sin\theta.$$

Тогда неравенство (1.5.58) будет выполнено, так как

$$\begin{aligned}\mathsf{E}\big[|X - \mathsf{E}(X\,|\,Z)|^2\big] &\geqslant \mathsf{E}\big[|X - \mathsf{E}(X\,|\,Z_1,\,Z_2)|^2\big] = \\ &= \mathsf{E}\big[|X_1 - \mathsf{E}(X_1\,|\,Z_1)|^2\big]\cos^2\theta + \mathsf{E}\big[|X_2 - \mathsf{E}(X_2\,|\,Z_2)|^2\big]\sin^2\theta. \quad \square\end{aligned}$$

Только неодушевлённые механизмы движутся по... прямым линиям и... кругам. В искусстве самый надёжный способ разрушения заключается в канонизации одной формы и одной философии: то, что канонизировано, быстро умирает от ожирения, или энтропии.

Евгений Замятин (1884–1937),
русский писатель; «Новая русская проза»

§ 1.6. Дополнительные задачи к главе 1

В идеале, теория информации должна предшествовать теории вероятностей, а не наоборот.

Андрей Колмогоров (1903–1987), советский математик (о преподавании математики в вузах)

Задача 1.6.1. Пусть Σ_1 и Σ_2 — алфавиты размеров m и q. Рассмотрим $\Sigma^* = \bigcup\limits_{n\geqslant 0} \Sigma^n$ — множество всех строк, составленных из знаков алфавита Σ. Что означает высказывание $f\colon \Sigma_1 \to \Sigma_2^*$ — декодируемый код?

Выведите из неравенств Крафта и Гиббса, что если буквы из алфавита Σ_1 выбираются с вероятностями $p_1, \ldots, p_m$, то средняя длина слова не менее чем $h(p_1, \ldots, p_m)/\log q$.

Найдите декодируемый двоичный код с кодовыми словами 011, 0111, 01111, 11111 и тремя дополнительными кодовыми словами длины 2. Как проверить, что предложенный вами код декодируемый?

Решение. Будем кодировать сообщение $x_1x_2\ldots x_n \in \Sigma_1^*$ как сцепление $f(x_1)f(x_2)\ldots f(x_n) \in \Sigma_2^*$, т. е. продолжим f до функции $f^*\colon \Sigma_1^* \to \Sigma_2^*$. Будем называть код декодируемым, если f^* — вложение.

Согласно неравенству Крафта свободный от префиксов код $f\colon \Sigma_1 \to \Sigma_2^*$ с длинами кодовых слов $s_1, \ldots, s_m$ существует тогда и только тогда, когда

$$\sum_{i=1}^{m} q^{-s_i} \leqslant 1. \tag{1.6.1}$$

Более того, любой декодируемый код удовлетворяет этому неравенству.

В силу неравенства Гиббса для двух распределений вероятностей $p_1, \ldots, p_n$ и $\hat{p}_1, \ldots, \hat{p}_n$ имеем

$$h(p_1, \ldots, p_n) = -\sum_{i=1}^{n} p_i \log p_i \leqslant -\sum_{i=1}^{n} p_i \log \hat{p}_i,$$

а равенство достигается тогда и только тогда, когда $p_i = \hat{p}_i$.

Предположим, что код f поддаётся декодированию и длины его кодовых слов равны $s_1, \ldots, s_m$. Положим $\hat{p}_i = q^{-s_i}/c$, где $c = \sum\limits_{i=1}^{m} q^{-s_i}$. Тогда по

неравенству Гиббса получаем оценку

$$h(p_1, \ldots, p_n) \leqslant -\sum_{i=1}^{n} p_i \log \hat{p}_i = -\sum_{i=1}^{n} p_i(-s_i \log q - \log c) =$$
$$= \Big(\sum_i p_i s_i\Big) \log q + \Big(\sum_i p_i\Big) \log c.$$

Так как по неравенству Крафта $c \leqslant 1$, т. е. $\log c \leqslant 0$, поэтому

$$\text{средняя длина кодового слова } \sum_i p_i s_i \geqslant h(p_1, \ldots, p_n)/\log q.$$

Переходя к примеру, выберем три дополнительных кодовых слова 00, 01, 10 (11 взять нельзя, так как тогда последовательность десяти первых единиц не будет декодируемой). Обращение порядка в каждом кодовом слове приводит к коду без префиксов, а свободный от префиксов код является декодируемым. Следовательно, наш код декодируемый.

В заключение представим альтернативное доказательство необходимости в неравенстве Крафта. Обозначим $s = \max s_i$. Договоримся увеличить длину всех кодовых слов из $\mathcal{X}$ до s, добавляя, например, некоторый фиксированный символ. Если $x = x_1 x_2 \ldots x_{s_i} \in \mathcal{X}$, то любое слово $x_1 x_2 \ldots x_{s_i} y_{s_i+1} \ldots y_s \notin \mathcal{X}$, поскольку x тогда будет префиксом. Но существует не более чем q^{s-s_i} таких слов. Суммируя по i, мы получим, что общее количество исключённых слов составляет $\sum\limits_{i=1}^{m} q^{s-s_i}$, что не может превысить числа всех слов q^s. Поэтому $q^s \sum\limits_{i=1}^{m} q^{-s_i} \leqslant q^s$, что эквивалентно неравенству (1.6.1). □

The Forbidden Fruit of Huffman's Tree of Desire
Запретный плод дерева желаний Хаффмана[6]
(Из серии «Фильмы, которые не вышли на большой экран».)

Задача 1.6.2. Рассмотрим алфавит из m символов, которые используются с равной вероятностью $1/m$. Для кодирования применяем двоичный код Хаффмана, чтобы минимизировать среднюю длину кодового слова $(s_1 + \ldots + s_m)/m$, где s_i — длина слова, приписанного букве i. Положим $s^* = \max[s_i\colon 1 \leqslant i \leqslant m]$, $s_* = \min[s_i\colon 1 \leqslant i \leqslant m]$ и обозначим через n_l количество кодовых слов длины l.

[6]Ср. с названиями фильмов «Fruits of Desire» (1916 г., по повести Генри Миллера) и «Forbidden Fruit» (1921 г.).

1. Покажите, что $2 \leqslant n_{s^*} \leqslant m$.

2. При каких значениях m выполнено равенство $n_s^* = m$?

3. Выразите s^* через m.

4. Докажите, что $n_{s^*-1} + n_{s^*} = m$, т. е. любые две длины кодовых слов отличаются не больше чем на 1

5. Найдите n_{s^*-1} и n_{s^*}.

6. Найдите длины кодовых слов для идеализированного английского языка ($m = 27$), в котором все символы равновероятны.

7. Пусть теперь двоичным кодом Хаффмана кодируются символы $1, \ldots, m$, появляющиеся с вероятностями $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_m > 0$, где $\sum\limits_{1 \leqslant i \leqslant m} p_i = 1$. Определите максимальное и минимальное значения s^* и s_* и найдите двоичные деревья, в которых они появляются.

Решение. 1. Ограничение $n_s \geqslant 2$ следует из древовидной структуры кода Хаффмана. Более точно, допустим, что $n_{s^*} = 1$, т. е. найдётся единственное кодовое слово максимальной длины, соответствующее, скажем, букве i. Тогда можно отсечь последний символ из ветви длины s^*, ведущей к i, не нарушая беспрефиксного свойства. Но это противоречит минимальности. Ограничение $n_{s^*} \leqslant m$ очевидно. (Ниже мы увидим, что n_{s^*} всегда чётно.)

2. Равенство $n_{s^*} = m$ означает, что все кодовые слова имеют одинаковую длину. Это происходит тогда и только тогда, когда $m = 2^k$, т. е. $s^* = k$ (совершенное двоичное дерево $\mathbb{T}_k$ с 2^k листьями).

3. В общем случае

$$s^* = \begin{cases} \log m, & \text{если } m = 2^k, \\ \lceil \log m \rceil, & \text{если } m \neq 2^k. \end{cases}$$

Случай $m = 2^k$ уже разобран, поэтому предположим, что $m \neq 2^k$. Тогда $2^k < m < 2^{k+1}$, где $k = \lfloor \log m \rfloor$. Этот факт вытекает из наблюдения, что двоичное дерево для вероятностей $1/m$ содержит совершенное двоичное дерево $\mathbb{T}_k$, но содержится в дереве $\mathbb{T}_{k+1}$, откуда получаем $s^* = \lceil \log m \rceil$.

4. В случае равномерного распределения $1/m, \ldots, 1/m$ существование ветви дерева, длина которой отличается на 2 или более от максимального значения s^*, невозможно. Действительно, предположим, что существует такая ветвь B_i, ведущая к вершине i, и выберем ветвь M_j максимальной длины, ведущую к вершине j. Тогда буква j участвовала в s^* объединениях, а i — в $t \leqslant s^* - 2$. В конечном счёте ветви B_i и M_j должны слиться, что создаёт противоречие. Например, картина, изображенная на рис. 1.11, невозможна по следующей причине. Здесь вершина i, имеющая вероятность $1/m$, должны быть объединена с вершинами a или b, каждая

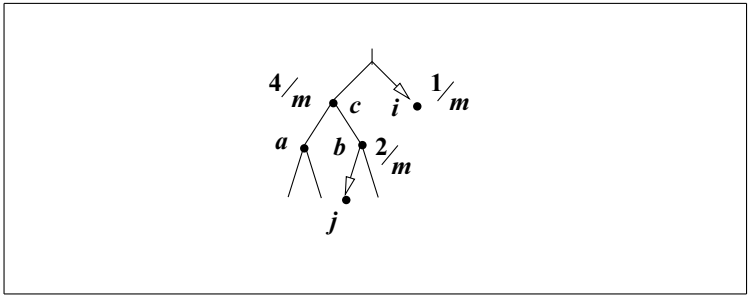


Рис. 1.11

из которых имеет вероятность $2/m$, вместо объединения a и b (как на рисунке), так как это создаёт вершину с общей вероятностью $4/m$.

5. Итак, 1) для $m = 2^k$ m-дерево $\mathbb{B}_m$ совпадает с $\mathbb{T}_k$, 2) при $m \neq 2^k$ мы получаем $\mathbb{B}_m$ следующим образом. Сначала возьмём двоичное дерево $\mathbb{T}_k$ с $k = \lfloor \log m \rfloor$, так, чтобы выполнялось условие $1 \leqslant m - 2^k < 2^k$. Тогда $m - 2^k$ листьев дерева $\mathbb{T}_k$ позволяют ветвям пройти на один шаг дальше, что генерирует $2(m - 2^k) = 2m - 2^{k+1}$ листьев дерева $\mathbb{T}_{r+1}$. Остальные $2^k - (m - 2^k) = 2^{k+1} - m$ листьев остаются нетронутыми (см. рис. 1.12). Таким образом,

$$n_{s^*-1} = 2^{k+1} - m, \quad n_{s^*} = 2m - 2^{k+1}, \quad \text{где } k = \lfloor \log m \rfloor.$$

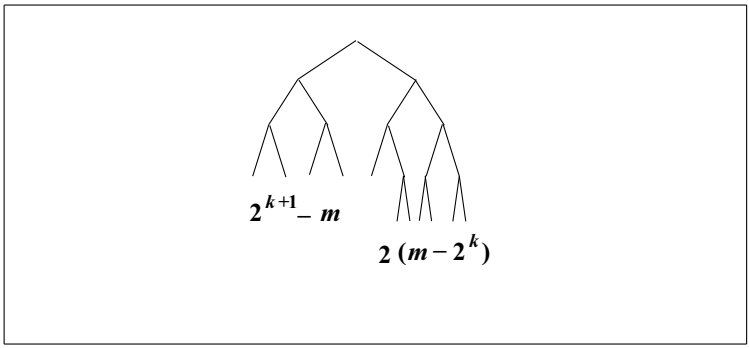


Рис. 1.12

6. В примере с английским языком с равномерно распределёнными $m = 27 = 16 + 11$ символами мы имеем 5 кодовых слов длины 4 и 22 слова

длины 5. Средняя длина кодового слова составит

$$\frac{5\times 4+22\times 5}{27}=\frac{130}{27}\approx 4{,}8.$$

7. Минимальное значение для s_* равно 1 (очевидно). Максимальное значение равно $\lceil \log m \rceil$, т. е. такому натуральному числа l, что $2^{l-1} < m \leqslant 2^l$.

Дерево с $s_* = 1$ и $s^* = m-1$ показано на рис. 1.13.

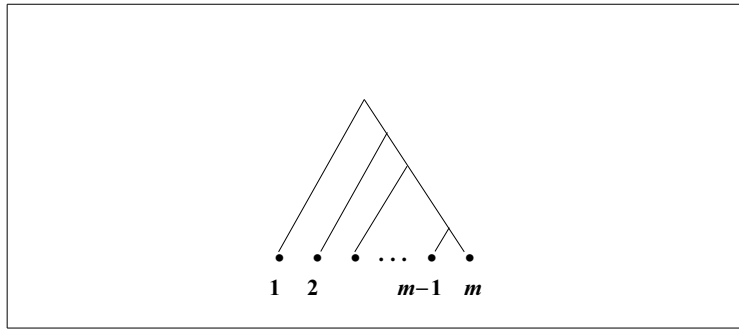


Рис. 1.13

Для него получаем код

i	$f(i)$	s_i
1	0	1
2	10	2
⋮	⋮	⋮
$m-1$	$11\ldots10$	$m-1$
m	$11\ldots11$	$m-1$

и получается, когда

$$p_1 > p_2 + \ldots + p_m > 2(p_3 + \ldots + p_m) > \ldots > 2^{m-1}p_m.$$

Дерево, максимизирующее s_1 и минимизирующее s_m, соответствует равномерному распределению, т. е. $p_1 = \ldots = p_m = 1/m$. Когда $m = 2^k$, ветви дерева имеют одинаковую длину $k = \log_2 m$ (совершенное двоичное дерево, см. рис. 1.14).

Если $2^k < m < 2^{k+1}$, то дерево насчитывает $2^{k+1} - m$ листьев на уровне k и $2(m-2^k)$ листьев на уровне $k+1$ (1.15).

В силу конструкции Хаффмана кратчайшая ветвь не может быть длиннее, чем $\lceil \log_2 m \rceil$, а наиболее длинная ветвь короче чем $\lfloor \log_2 m \rfloor$, так как дерево всегда является поддеревом совершенного двоичного дерева. □

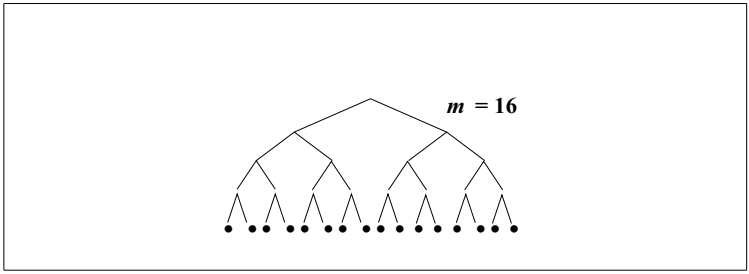


Рис. 1.14

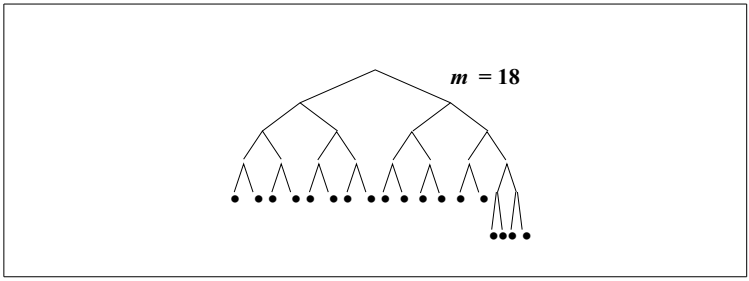


Рис. 1.15

Только некоторые из людей могут понимать английский язык, но каждый может понимать глупца.

Клод Шеннон (1916–2001),
американский электротехник и математик

Задача 1.6.3. Сформулируйте вторую теорему Шеннона о кодировании (ВТШК) и вычислите пропускную способность двоичного канала с вероятностью стирания p, т. е. д. к. б. п. с матрицей канала

$$\begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix}.$$

Решение. ВТШК утверждает, что для двоичного канала без памяти

пропускная способность = максимум передачи информации на букву.

Здесь пропускная способность $C = \max_X I(X : Y)$, где с. в. X и Y представляют собой вход и соответствующий выход.

Двоичный стирающий канал хранит входные символы 0 или 1 неповреждёнными с вероятностью $1 - p$ и заменяет их символом $*$ с вероятностью p. Входная с. в. X принимает значение 0 с вероятностью α и 1

с вероятностью $1-\alpha$. Тогда выходная с. в. принимает три значения:

$$\begin{aligned}
&\mathsf{P}(Y=0)=(1-p)\alpha,\\
&\mathsf{P}(Y=1)=(1-p)(1-\alpha),\\
&\mathsf{P}(Y=*)=p.
\end{aligned}$$

Условная энтропия равна

$$\left.\begin{aligned}
&h(X\,|\,Y=0)=0,\\
&h(X\,|\,Y=1)=0,\\
&h(X\,|\,Y=*)=\eta(\alpha)
\end{aligned}\right\} \implies h(X\,|\,Y)=p\eta(\alpha).$$

Таким образом,

$$\begin{aligned}
\text{пропускная способность} &= \max_{\alpha} I(X:Y)=\max_{\alpha}(h(X)-h(X\,|\,Y))=\\
&=\max_{\alpha}(\eta(\alpha)-p\eta(\alpha))=(1-p)\max_{\alpha}\eta(\alpha)=1-p,
\end{aligned}$$

так как $\eta(\alpha)$ достигает своего максимального значения 1 при $\alpha=1/2$. $\square$

Задача 1.6.4. Пусть X и Y — дискретные с. в. с распределениями P_X и P_Y.

1. Определите условную энтропию $h(X\,|\,Y)$ и покажите, что она удовлетворяет неравенству

$$h(X\,|\,Y)\leqslant h(X).$$

Сформулируйте необходимые и достаточные условия для равенства.

2. Для каждого $\alpha\in[0,\,1]$ п. р. смеси с. в. $W(\alpha)$ имеет вид

$$\mathsf{P}_{W(\alpha)}(x)=\alpha\,\mathsf{P}_X(x)+(1-\alpha)\,\mathsf{P}_Y(x).$$

Докажите, что при всех α энтропия с. в. $W(\alpha)$ подчиняется неравенству:

$$h(W(\alpha))\geqslant\alpha h(X)+(1-\alpha)h(Y).$$

3. Пусть $h_{\mathbf{Po}}(\lambda)$ — энтропия пуассоновой с. в. $\mathbf{Po}(\lambda)$. Покажите, что $h_{\mathbf{Po}}(\lambda)$ — неубывающая функция от $\lambda>0$.

Решение. 1. По определению

$$\begin{aligned}
h(X\,|\,Y)&=h(X,\,Y)-h(Y)=\\
&=-\sum_{x,y}\mathsf{P}(X=x,\,Y=y)\log\mathsf{P}(X=x,\,Y=y)+\sum_{y}\mathsf{P}(Y=y)\log\mathsf{P}(Y=y).
\end{aligned}$$

Неравенство $h(X\,|\,Y)\leqslant h(X)$ эквивалентно такому:

$$h(X,\,Y)\leqslant h(X)+h(Y)$$

и следует из неравенства Гиббса $\sum_i p_i \log \frac{p_i}{q_i} \geqslant 0$. Действительно, возьмём

$$p_i = \mathsf{P}(X = x,\ Y = y), \quad q_i = \mathsf{P}(X = x)\,\mathsf{P}(Y = y), \quad i = (x,\ y).$$

Тогда

$$0 \leqslant \sum_{x,y} \mathsf{P}(X = x,\ Y = y) \log \frac{\mathsf{P}(X = x,\ Y = y)}{\mathsf{P}(X = x)\,\mathsf{P}(Y = y)} =$$

$$= \sum_{x,y} \mathsf{P}(X = x,\ Y = y) \log \mathsf{P}(X = x,\ Y = y) -$$

$$- \sum_{x,y} \mathsf{P}(X = x,\ Y = y)[\log \mathsf{P}(X = x) + \log \mathsf{P}(Y = y)] =$$

$$= -h(X,\ Y) + h(X) + h(Y).$$

Равенство здесь возникает тогда и только тогда, когда X и Y независимы.

2. Определим с. в. T, равную 0 с вероятностью α и 1 с вероятностью $1 - \alpha$. Тогда с. в. Z имеет то же распределение, что и $W(\alpha)$:

$$Z = \begin{cases} X, & \text{если } T = 0, \\ Y, & \text{если } T = 1. \end{cases}$$

По пункту 1 имеем

$$h(Z \,|\, T) \leqslant h(Z),$$

где л. ч. равна $\alpha h(X) + (1 - \alpha)h(Y)$, а п. ч. равна $h(W(\alpha))$.

3. Заметим, что для независимых с. в. X и Y выполнено равенство $h(X + Y \,|\, X) = h(Y \,|\, X) = h(Y)$. Следовательно, применяя пункт 1, получаем

$$h(X + Y) \geqslant h(X + Y \,|\, X) = h(Y).$$

Используя этот факт, возьмём независимые с. в. $Y \sim \mathbf{Po}(\lambda_1)$, $X \sim \mathbf{Po}(\lambda_2 - \lambda_1)$ при любых $\lambda_1 < \lambda_2$. Тогда

$$h(X + Y) \geqslant h(Y) \implies h_{\mathbf{Po}}(\lambda_2) \geqslant h_{\mathbf{Po}}(\lambda_1). \qquad \square$$

> Специалисты по теории информации делают это с максимальной пропускной способностью.
>
> Они также делают это, обеспечивая максимальную взаимную информацию.
>
> (Из серии «Как они делают это».)

Задача 1.6.5. Что означает надёжная передача со скоростью R по двоичному симметричному каналу без памяти (д. с. к. б. п.) с вероятностью

ошибки p? Опираясь на вторую теорему Шеннона о кодировании, вычислите точную верхнюю границу всех скоростей надёжных передач по такому каналу. Что получится, если

1) p очень мало,

2) $p = 1/2$,

3) $p > 1/2$?

Решение. Д. с. к. б. п. может надёжно передавать со скоростью R, если существует такая последовательность кодов $\mathcal{X}_N$, $N = 1, 2, \ldots$ с $\lfloor 2^{NR} \rfloor$ кодовыми словами, что

$$\hat{e}(\mathcal{X}_N) = \max_{x \in \mathcal{X}_N} \mathsf{P}(\text{ошибка} \,|\, x \text{ послано}) \to 0 \quad \text{при } N \to \infty. \tag{1.6.2}$$

По ВТШК так называемая оперативная пропускная способность канала — это $\sup R = \max\limits_{\alpha} I(X : Y)$, т. е. максимум информации, переданной на один входной символ. Здесь X — с. в. Бернулли, принимающая значения 0 и 1 с вероятностями $\alpha \in [0, 1]$ и $1 - \alpha$, а Y — выходная с. в. при данной входной с. в. X. Далее, $I(X : Y)$ — взаимная энтропия (информация):

$$I(X : Y) = h(X) - h(X \,|\, Y) = h(Y) - h(Y \,|\, X).$$

Заметим, что функция двоичной энтропии удовлетворяет неравенству $\eta(x) \leqslant 1$, в котором равенство достигается при $x = 1/2$. Выбрав $\alpha = 1/2$, заключаем, что пропускная способность д. с. к. б. п. с вероятностью ошибки p равна

$$\max_{\alpha} I(X : Y) = \max_{\alpha} [h(Y) - h(Y \,|\, X)] =$$
$$= \max_{\alpha} [\eta(\alpha p + (1 - \alpha)(1 - p)) - \eta(p)] = 1 - \eta(p).$$

1) Если p мало, то пропускная способность тоже незначительно меньше 1 (пропускная способность незашумлённого канала).

2) Если $p = 1/2$, пропускная способность равна нулю (бесполезный канал).

3) Если $p > 1/2$, то заменив p на $1 - p$, т. е. переставив метки в выходном алфавите, получим, что пропускная способность $C > 0$. □

Задача 1.6.6. 1. Что больше: π^e или e^π?

2. Пусть $a_1, a_2, \ldots, a_n \geqslant 0$ и $b_1, b_2, \ldots, b_n \geqslant 0$. Докажите сумматорно-логарифмическое неравенство

$$\sum_i a_i \log \frac{a_i}{b_i} \geqslant \Big(\sum_i a_i \Big) \log \left(\frac{\sum\limits_i a_i}{\sum\limits_i b_i} \right), \tag{1.6.3}$$

в котором равенство достигается тогда и только тогда, когда $a_i / b_i = \text{const}$.

3. Рассмотрим два дискретных распределения вероятностей $p = (p(x))$ и $q = (q(x))$. Определите относительную энтропию (или расстояние Кульбака—Лейблера) и докажите неравенство Гиббса

$$D(p \parallel q) = \sum_x p(x) \log \left(\frac{p(x)}{q(x)} \right) \geqslant 0, \tag{1.6.4}$$

в котором равенство достигается тогда и только тогда, когда $p(x) = q(x)$ для всех x.

Опираясь на оценку (1.6.3), докажите неравенство

$$\sum_{x \in A} f(x) \log \left(\frac{f(x)}{g(x)} \right) \geqslant \left(\sum_{x \in A} f(x) \right) \log \left(\frac{\sum\limits_{x \in A} f(x)}{\sum\limits_{x \in A} g(x)} \right)$$

для любых положительных функций $f(x)$ и $g(x)$ и конечного множества A.

Проверьте, что для всех p, q, $0 \leqslant p$, $q \leqslant 1$ имеет место неравенство

$$p \log \left(\frac{p}{q} \right) + (1 - p) \log \left(\frac{1 - p}{1 - q} \right) \geqslant (2 \log_2 e)(p - q)^2 \tag{1.6.5}$$

и покажите, что для всех распределений вероятностей p и q выполняется неравенство:

$$D(p \parallel q) \geqslant \frac{\log_2 e}{2} \Big(\sum_x |p(x) - q(x)| \Big)^2. \tag{1.6.6}$$

Решение. 1. Обозначим $x = \ln \pi$. Взяв логарифм дважды, получим неравенство $x - 1 > \ln x$. Это верно, поскольку $x > 1$, следовательно, $e^\pi > \pi^e$.

2. Без ограничения общности предположим, что $a_i > 0$ и $b_i > 0$. По неравенству Йенсена, примененному к строго выпуклой функции $g(x) = x \log x$, при любых коэффициентах $c_i \geqslant 0$, $\sum c_i = 1$, имеем

$$\sum c_i g(x_i) \geqslant g\Big(\sum c_i x_i \Big).$$

Выбирая $c_i = b_i \Big(\sum\limits_j b_j \Big)^{-1}$ и $x_i = a_i / b_i$, получим сумматорно-логарифмическое неравенство

$$\sum_i \frac{a_i}{\sum b_j} \log \frac{a_i}{b_i} \geqslant \Big(\sum_i \frac{a_i}{\sum b_j} \Big) \log \left(\frac{\sum\limits_i a_i}{\sum\limits_i b_i} \right).$$

3. Существует такая константа $c > 0$, что выполнено неравенство

$$\log y \geqslant c \Big(1 - \frac{1}{y} \Big),$$

в котором равенство достигается тогда и только тогда, когда $y = 1$. Обозначив $B := \{x\colon p(x) > 0\}$, запишем

$$D(p \parallel q) = \sum_{x\in B} p(x) \log \frac{p(x)}{q(x)} \geqslant c \sum_{x\in B} p(x)\Big(1 - \frac{p(x)}{q(x)}\Big) = c[1 - q(B)] \geqslant 0.$$

Равенство достигается тогда и только тогда, когда $q(x) \equiv p(x)$. Положим

$$f(A) = \sum_{x\in A} f(x), \qquad p(x) = \frac{f(x)}{f(A)}\mathbf{1}(x \in A),$$
$$g(A) = \sum_{x\in A} g(x), \qquad q(x) = \frac{g(x)}{g(A)}\mathbf{1}(x \in A).$$

Тогда

$$\sum_{x\in A} f(x) \log \frac{f(x)}{g(x)} = f(A) \sum_{x\in A} p(x) \log \frac{f(A)p(x)}{g(A)q(x)} =$$
$$= f(A) \underbrace{\sum_{x\in A} p(x) \log \frac{p(x)}{q(x)}}_{\geqslant 0 \text{ по предыдущему пункту}} + f(A) \log \frac{f(A)}{g(A)} \geqslant f(A) \log \frac{f(A)}{g(A)}.$$

Неравенство (1.6.5) доказывается простой проверкой. Наконец, рассмотрим $A = \{x\colon p(x) \leqslant q(x)\}$. Так как

$$\sum_x |p(x) - q(x)| = 2[q(A) - p(A)] = 2[p(A^{\mathrm{c}}) - q(A^{\mathrm{c}})],$$

получаем, что

$$D(p \parallel q) = \sum_{x\in A} p(x) \log \frac{p(x)}{q(x)} + \sum_{x\in A^{\mathrm{c}}} p(x) \log \frac{p(x)}{q(x)} \geqslant$$
$$\geqslant p(A) \log \frac{p(A)}{q(A)} + p(A^{\mathrm{c}}) \log \frac{p(A^{\mathrm{c}})}{q(A^{\mathrm{c}})} \geqslant$$
$$\geqslant (2 \log_2 e)[p(A) - q(A)]^2 = \frac{\log_2 e}{2}\left[\sum_x |p(x) - q(x)|\right]^2. \quad \square$$

Задача 1.6.7. 1. Сформулируйте определение условной энтропии и покажите, что совместная энтропия с. в. U и V удовлетворяет равенству

$$h(U, V) = h(V \,|\, U) + h(U).$$

Для с. в. $X_1, \ldots, X_n$ индукцией по n докажите правило цепи

$$h(X_1, \ldots, X_n) = \sum_{i=1}^{n} h(X_i \,|\, X_1, \ldots, X_{i-1}). \tag{1.6.7}$$

2. Определим среднюю по подмножествам размера k энтропию по формуле

$$h_k^{(n)} = \sum_{S:\ |S|=k} \frac{h(X_S)}{k} \Big/ C_n^k,$$

где $h(X_S) = h(X_{s_1}, \ldots, X_{s_k})$ для $S = \{s_1, \ldots, s_k\}$. Покажите, что для любого i имеет место неравенство $h(X_i \,|\, X_S) \leqslant h(X_i \,|\, X_T)$ при $T \subseteq S$ и $i \notin S$.

Рассматривая члены вида

$$h(X_1, \ldots, X_n) - h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n),$$

покажите, что $h_n^{(n)} \leqslant h_{n-1}^{(n)}$.

Учитывая неравенство $h_k^{(k)} \leqslant h_{k-1}^{(k)}$, покажите, что $h_k^{(n)} \leqslant h_{k-1}^{(n)}$ при $k = 2, \ldots, n$.

3. Для $\beta > 0$ положим

$$t_k^{(n)} = \sum_{S:\ |S|=k} e^{\beta h(X_S)/k} \Big/ C_n^k.$$

Докажите, что

$$t_1^{(n)} \geqslant t_2^{(n)} \geqslant \ldots \geqslant t_n^{(n)}.$$

Решение. 1. По определению условной энтропии

$$h(U \,|\, V) = h(U, V) - h(U) = \sum_u \mathsf{P}(U = u) h(V \,|\, U = u),$$

где $h(V \,|\, U = u)$ — энтропия условного распределения:

$$h(V \,|\, U = u) = -\sum_v \mathsf{P}(V = v \,|\, U = u) \log \mathsf{P}(V = v \,|\, U = u).$$

Правило цепи (1.6.7) доказывается индукцией по n.

2. По правилу цепи

$$h(X_1, \ldots, X_n) = h(X_1, \ldots, X_{n-1}) + h(X_n \,|\, X_1, \ldots, X_{n-1}) \tag{1.6.8}$$

и в общем случае

$$\begin{aligned} h(X_1, \ldots, X_n) &= h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) + \\ &\quad + h(X_i \,|\, X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) \leqslant \\ &\leqslant h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) + h(X_i \,|\, X_1, \ldots, X_{i-1}), \end{aligned} \tag{1.6.9}$$

потому что

$$h(X_i \,|\, X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) \leqslant h(X_i \,|\, X_1, \ldots, X_{i-1}).$$

Теперь, суммируя формулу (1.6.9) по i от 1 до n, получим

$$nh(X_1, \ldots, X_n) \leqslant \sum_{i=1}^{n} h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) + \sum_{i=1}^{n} h(X_i \,|\, X_1, \ldots, X_{i-1}).$$

Вторая сумма в п. ч. неравенства равна $h(X_1, \ldots, X_n)$ по правилу цепи (1.6.7), так что

$$(n-1)h(X_1, \ldots, X_n) \leqslant \sum_{i=1}^{n} h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n).$$

Отсюда следует, что $h_n^{(n)} \leqslant h_{n-1}^{(n)}$, так как

$$\frac{1}{n} h(X_1, \ldots, X_n) \leqslant \frac{1}{n} \sum_{i=1}^{n} \frac{h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)}{n-1}. \tag{1.6.10}$$

В общей ситуации фиксируем подмножество S размера k в $\{1, \ldots, n\}$. Обозначим через $S(i)$ подмножество $S \setminus \{i\}$ и получим

$$\frac{1}{k}[h(X(S)] \leqslant \frac{1}{k} \sum_{i \in S} \frac{h(X[S(i)])}{k-1}$$

по предыдущим рассуждениям. Следовательно,

$$C_n^k h_k^{(n)} = \sum_{S \subset \{1,\ldots,n\}:\ |S|=k} \frac{h[X(S)]}{k} \leqslant \sum_{S \subset \{1,\ldots,n\}:\ |S|=k} \sum_{i \in S} \frac{h(X[S(i)])}{k(k-1)}. \tag{1.6.11}$$

Наконец, каждое подмножество $S(i)$ размера $k-1$ в сумме (1.6.11) появляется $[n-(k-1)]$ раз. Поэтому $h_k^{(n)}$ можно оценить сверху как

$$\left[\sum_{T \subset \{1,\ldots,n\}:\ |T|=k-1} \frac{h[X(T)]}{k-1} \right] \frac{n-(k-1)}{k} \Big/ C_n^k =$$

$$= \sum_{T \subset \{1,\ldots,n\}:\ |T|=k-1} \frac{h[X(T)]}{k-1} \Big/ C_n^{k-1} = h_{k-1}^{(n)}.$$

3. Потенцируя формулу (1.6.11) и применяя затем неравенство между средним арифметическим и средним геометрическим, для $S_0 = \{1, \ldots, n\}$ получим следующее неравенство:

$$e^{\beta h(X(S_0))/n} \leqslant e^{\beta[h(S_0(1))+\ldots+h(S_0(n))]/(n(n-1)} \leqslant \frac{1}{n} \sum_{i=1}^{n} e^{\beta h(S_0(i))/(n-1)},$$

что эквивалентно неравенству $t_n^{(n)} \leqslant t_{n-1}^{(n)}$. Теперь используем те же рассуждения, что и в п. 2, взяв среднее по всем подмножествам, для доказательства неравенства $t_k^{(n)} \leqslant t_{k-1}^{(n)}$ для всех $k \leqslant n$. □

Задача 1.6.8. Пусть $p_1, \ldots, p_n$ — распределение вероятностей и $p^* = \max\limits_i [p_i]$. Докажите следующие неравенства:

1) $-\sum\limits_i p_i \log_2 p_i \geqslant -p^* \log_2 p^* - (1-p^*)\log_2(1-p^*)$;

2) $-\sum\limits_i p_i \log_2 p_i \geqslant \log_2(1/p^*)$;

3) $-\sum\limits_i p_i \log_2 p_i \geqslant 2(1-p^*)$.

С. в. X и Y со значениями x и y из «алфавитов» I и J представляют вход и выход канала передач с условной вероятностью $P(x\,|\,y) = \mathsf{P}(X = x\,|\,Y = y)$. Пусть $h(P(\cdot\,|\,y))$ обозначает условную энтропию X при заданном Y. Определим правило декодирования идеального наблюдателя (и. н.) как такое отображение $f\colon J \to I$, при котором $P(f(y)\,|\,y) = \max\limits_{x\in I} P(x\,|\,y)$ для всех $y \in J$. Покажите, что при декодировании и. н. вероятность ошибки

$$\pi_{\mathrm{er}}(y) = \sum_{x\in I:\ x\neq f(y)} P(x\,|\,y)$$

удовлетворяет неравенству $\pi_{\mathrm{er}}(y) \leqslant \frac{1}{2} h(P(\cdot\,|\,y))$, а средняя ошибка ограничена сверху:

$$\mathsf{E}\pi_{\mathrm{er}}(Y) \leqslant \frac{1}{2} h(X\,|\,Y).$$

Решение. Неравенство 1 следует из леммы 1.2.5 (неравенства группировки данных). Неравенство 2 верно, так как

$$-\sum_i p_i \log p_i \geqslant \sum_i p_i \log \frac{1}{p^*} = \log \frac{1}{p^*}.$$

Для проверки последнего неравенства удобно воспользоваться неравенством 1 для $p^* \geqslant 1/2$ и неравенством 2 для $p^* \leqslant 1/2$. Функция $x \in (0,\,1) \mapsto \eta(x)$ вогнута, и её график на интервале $(1/2,\,1)$ находится строго выше прямой $x \mapsto 2(1-x)$. Используя неравенство 1 и вогнутость функции $\eta(x)$, получаем

$$h(p_1, \ldots, p_n) \geqslant \eta(p^*) \geqslant 2(1-p^*).$$

Далее для $0 \leqslant x \leqslant 1/2$ верно неравенство:

$$\log \frac{1}{x} \geqslant 2(1-x) \quad \Big(\text{равенство} \Leftrightarrow x = \frac{1}{2}\Big).$$

Поэтому при $p^* \leqslant 1/2$ в силу неравенства 2:

$$h(p_1, \ldots, p_n) \geqslant \log \frac{1}{p^*} \geqslant 2(1 - p^*).$$

Для оценки среднего $\mathsf{E}\pi_{\mathbf{er}}$ воспользуемся неравенством 3 и запишем

$$\pi_{\mathrm{er}} = 1 - \mathsf{P}_{\mathbf{ch}}(f(y)\,|\,y) = 1 - p_{\mathbf{max}}(\cdot\,|\,y),$$

что не превосходит $h(P(\cdot\,|\,y))/2$. Оценка для $\mathsf{E}\pi_{\mathbf{er}}$ немедленно получается, если взять среднее от обеих частей, так как $h(X\,|\,Y) = \mathsf{E}h(P(\cdot\,|\,Y))$. □

Хотя мы не можем изменить прошлое, мы можем его узнать.
Мы в состоянии изменить будущее, но мы не можем его знать.

Эдвард Теллер (1908–2003), американский физик,
родившийся в Венгрии

Задача 1.6.9. Дайте определение скорости передачи информации H и асимптотического свойства равнораспределённости (а. с. р.) источника. Вычислите скорость передачи информации источника Бернулли. Определите пропускную способность C двоичного канала без памяти (д. к. б. п.). Опираясь на вторую теорему Шеннона о кодировании (ВТШК), докажите, что $C = \sup\limits_{p_X} I(X : Y)$.

Стирающий канал передает символ неповреждённым с вероятностью $1 - p$ и заменяет его на что-то нечитаемое с вероятностью p. Найдите пропускную способность стирающего канала.

Решение. Скорость передачи информации H источника $U_1, U_2, \ldots$ с конечным алфавитом I — это точная верхняя граница всех значений $R > 0$, для которых существует такая последовательность множеств $A_N \in I^{\times N}$, что $|A_N| \leqslant 2^{NR}$ и $\lim\limits_{N\to\infty} \mathsf{P}(U_1^N \in A_N) = 1$.

А. с. р. означает, что

$$-\frac{1}{N}\log p_N(U_1^N) \to H \quad \text{при } N \to \infty$$

в том или ином смысле (здесь имеется ввиду сходимость по вероятности). Здесь $U_1^N = U_1 \ldots U_N$ и $p_N(u_1^N) = \mathsf{P}(U_1^N = u_1^N)$. ВТШК утверждает, что с. в. $-\log p_N(U_1^N)/N$ сходится к конечному пределу H.

Двоичный канал без памяти задается условной вероятностью

$$\mathsf{P}_{\mathrm{ch}}(\mathbf{Y}^{(N)}\,|\,\mathbf{X}^{(N)} \text{ послано}) = \prod_{1\leqslant i\leqslant N} P(y_i\,|\,x_i)$$

и допускает ошибку с вероятностью

$$\varepsilon^{(N)} = \sum_u \mathsf{P}_{\mathrm{source}}(U = u)\,\mathsf{P}_{\mathrm{ch}}(\hat{f}_N(\mathbf{Y}^{(N)}) \neq u\,|\,f_N(u) \text{ послано}),$$

где $\mathsf{P}_{\text{source}}$ обозначает распределение вероятностей источника, используются правила кодирования f_N и декодирования $\hat{f}_N$. Значение $\bar{R} \in (0, 1)$ называют надёжной скоростью передачи, если при равномерном распределении $\mathsf{P}_{\text{source}}$ на множестве $\mathcal{U}_N$ строк источника u с $\#\mathcal{U}_N = 2^{N[\bar{R}+o(1)]}$ существуют такие f_N и $\hat{f}_N$, что

$$\lim_{N\to\infty} \frac{1}{\#\mathcal{U}_N} \sum_{u\in\mathcal{U}_N} \mathsf{P}_{\text{ch}}(\hat{f}_N(\mathbf{Y}^{(N)}) \neq u \,|\, f_N(u) \text{ послано}) = 0.$$

Пропускной способностью канала называют точную верхнюю границу всех надёжных скоростей передачи.

Матрица стирающего канала имеет вид

$$\begin{matrix} 0 \\ 1 \end{matrix}\begin{pmatrix} 1-p & 0 & p \\ 0 & 1-p & p \\ 0 & 1 & * \end{pmatrix}$$

Условная энтропия $h(Y\,|\,X) = \eta(p)$ не зависит от p_X. Поэтому

$$C = \sup_{p_X} I(X : Y) = \sup_{p_X} h(Y) - h(Y\,|\,X)$$

достигается при $p_X(0) = p_X(1) = 1/2$ с энтропией

$$h(Y) = -(1-p)\log[(1-p)/2] - p\log p = \eta(p) + (1-p).$$

Следовательно, пропускная способность $C = 1 - p$. □

Задача 1.6.10. Дайте определение кода Хаффмана и докажите его оптимальность по сравнению с другими декодируемыми кодами. Вычислите длину кодового слова для вероятностей символов $\frac{1}{5}, \frac{1}{5}, \frac{1}{6}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{30}$.

Докажите или опровергните контрпримером высказывание: если длина кодового слова кода Хаффмана равна l, то в том же коде найдётся кодовое слово длины l', для которого $|\,l - l'\,| \leqslant 1$.

Решение. Ответом к первой части задачи служит таблица:

вероятность	кодовое слово	длина
1/5	00	2
1/5	100	3
1/6	101	3
1/10	110	3
1/10	010	3
1/10	011	3
1/10	1110	4
1/30	1111	4

Контрпример ко второй части:

вероятность	кодовое слово	длина
1/2	0	1
1/8	100	3
1/8	101	3
1/8	110	3
1/8	111	3

□

Задача 1.6.11. Д. с. к. б. п. с входным алфавитом $\{0, 1\}$ корректно воспроизводит символы с вероятностью $(n-1)/n^2$ и обращает их с вероятностью $1/n^2$, т. е. для $n = 1$ канал является незашумлённым. При $n \geqslant 2$ он также производит $2(n-1)$ видов ошибочных символов, обозначаемых α_i и β_i, $i = 1, \ldots, n-1$, с вероятностями $P(\alpha_i \,|\, 0) = (n-1)/n^2$, $P(\beta_i \,|\, 0) = 1/n^2$, $P(\beta_i \,|\, 1) = (n-1)/n^2$, $P(\alpha_i \,|\, 1) = 1/n^2$. Докажите, что пропускная способность C_n канала монотонно растёт с ростом n и $\lim\limits_{n\to\infty} C_n = \infty$. Как повлияет на пропускную способность замена α_i на 0 и β_i на 1?

Решение. Матрица канала имеет вид

$$\begin{array}{c} 0 \\ 1 \end{array}\!\!\begin{pmatrix} \dfrac{n-1}{n^2} & \dfrac{1}{n^2} & \dfrac{n-1}{n^2} & \dfrac{1}{n^2} & \ldots & \dfrac{n-1}{n^2} & \dfrac{1}{n^2} \\ \dfrac{1}{n^2} & \dfrac{n-1}{n^2} & \dfrac{1}{n^2} & \dfrac{n-1}{n^2} & \ldots & \dfrac{1}{n^2} & \dfrac{n-1}{n^2} \\ 0 & 1 & \alpha_1 & \beta_1 & \ldots & \alpha_{n-1} & \beta_{n-1} \end{pmatrix}.$$

Канал дважды симметричен (строки и столбцы получаются перестановками), следовательно, распределение на входе, обеспечивающее наилучшую пропускную способность, равномерное

$$p_X(0) = p_X(1) = \frac{1}{2},$$

а пропускная способность C_n задаётся формулой

$$C_n = \log(2n) + n\frac{1}{n^2}\log(n^2) + n\frac{n-1}{n^2}\log\frac{n^2}{n-1} = \\ = 1 + 3\log n - \frac{n-1}{n}\log(n-1) \to +\infty \text{ при } n \to \infty.$$

Далее, экстраполируя:

$$C(x) = 1 + 3\log x - \left(1 - \frac{1}{x}\right)\log(x-1), \quad x \geqslant 1,$$

находим, что

$$\frac{dC(x)}{dx} = \frac{3}{x} - \frac{1}{x-1} + \frac{1}{x(x-1)} - \frac{1}{x^2}\log(x-1) =$$
$$= \frac{2}{x} - \frac{1}{x^2}\log(x-1) = \frac{1}{x^2}[2x - \log(x-1)] > 0, \quad x > 1.$$

Таким образом, пропускная способность возрастает по n. Когда α_i, β_i трактуются как 0 или 1, пропускная способность не меняется. □

Задача 1.6.12. Пусть н. о. р. с. в. X_i, $i = 1, 2, \ldots$, принимают значения 0 и 1 с вероятностями p и $1-p$. Докажите локальную теорему Муавра—Лапласа с остаточным членом

$$\mathsf{P}(S_n = k) = \frac{1}{\sqrt{2\pi y(1-y)n}} \exp[-nh_p(y) + \theta_n(k)], \quad k = 1, \ldots, n-1. \tag{1.6.12}$$

Здесь $S_n = \sum\limits_{1 \leqslant i \leqslant n} X_i$, $y = k/n$, $h_p(y) = y\ln\left(\frac{y}{p}\right) + (1-y)\ln\left(\frac{1-y}{1-p}\right)$ и остаток $\theta_n(k)$ подчиняется неравенству

$$|\theta_n(k)| < \frac{1}{6ny(1-y)}, \quad y = k/n.$$

Указание. Используйте формулу Стирлинга с остаточным членом:

$$n! = \sqrt{2\pi n}\, n^n e^{-n+\theta(n)}, \quad \text{где } \frac{1}{12n+1} < \theta(n) < \frac{1}{12n}.$$

Найдите такие значения $k^{\pm}$, $0 \leqslant k^+, k^- \leqslant n$ (зависящие от n), что $\mathsf{P}(S_n = k^+)$ асимптотически максимально, а $\mathsf{P}(S_n = k^-)$ асимптотически минимально при $n \to \infty$, и выпишите соответствующие асимптотики.

Решение. Запишем

$$\mathsf{P}(S_n = k) = \frac{n!}{k!(n-k)!}(1-p)^{n-k}p^k =$$
$$= \sqrt{\frac{n}{2\pi k(n-k)}}\,\frac{n}{k^k(n-k)^{n-k}}(1-p)^{n-k}p^k \exp[\theta(n) - \theta(k) - \theta(n-k)] =$$
$$= \frac{1}{\sqrt{2\pi ny(1-y)}} \exp[-k\ln y - (n-k)\ln(1-y) +$$
$$+ k\ln p + (n-k)\ln(1-p)] \exp[\theta(n) - \theta(k) - \theta(n-k)] =$$
$$= \frac{1}{\sqrt{2\pi ny(1-y)}} \exp[-nh_p(y)] \exp[\theta(n) - \theta(k) - \theta(n-k)].$$

Далее, из неравенств

$$|\theta(n) - \theta(k) - \theta(n-k)| < \frac{1}{12n} + \frac{1}{12k} + \frac{1}{12(n-k)} < \frac{2n^2}{12nk(n-k)}$$

следует формула (1.6.12) с $\theta_n(k) = \theta(n) - \theta(k) - \theta(n-k)$.

По неравенству Гиббса $h_p(y) \geqslant 0$ и $h_p(y) = 0$ тогда и только тогда, когда $y = p$. Более того,

$$\frac{dh_p(y)}{dy} = \ln\frac{y}{p} - \ln\frac{1-y}{1-p} \quad \text{и} \quad \frac{d^2h_p(y)}{dy^2} = \frac{1}{y} + \frac{1}{1-y} > 0,$$

а значит,

$$\frac{dh_p(y)}{dy}\Big|_{y=p} = 0, \quad \frac{dh_p(y)}{dy} < 0, \ \ 0 < y < p \quad \text{и} \quad \frac{dh_p(y)}{dy} > 0, \ \ p < y < 1.$$

Следовательно,

$\underline{h}_p = \min h_p(y) = 0$ достигается при $y = p$,

$\overline{h}_p = \max h_p(y)$ достигается при $y = 0$ или $y = 1$.

Таким образом, при $n \gg 1$ максимальная вероятность достигается при $y^* = p$, т. е. $k^+ = \lfloor np \rfloor$:

$$\mathsf{P}(S_n = \lfloor np \rfloor) \simeq \frac{1}{\sqrt{2\pi np(1-p)}} \exp(\theta_n(\lfloor np \rfloor)),$$

где

$$|\theta_n(\lfloor np \rfloor)| \leqslant \frac{1}{6np(1-p)}.$$

Аналогично минимальная вероятность равна

$$\begin{aligned} &\mathsf{P}(S_n = 0) = p^n, && \text{если } 0 < p \leqslant 1/2, \\ &\mathsf{P}(S_n = n) = (1-p)^n, && \text{если } 1/2 \leqslant p \leqslant 1. \end{aligned}$$ □

Задача 1.6.13. 1. Докажите, что энтропия $h(X) = -\sum\limits_{i=1}^{n} p(i)\log p(i)$ дискретной с. в. X с распределением вероятностей $\mathbf{p} = (p(1), \ldots, p(n))$ является выпуклой функцией от вектора $\mathbf{p}$.

Докажите, что взаимная энтропия $I(X:Y) = h(Y) - h(Y\,|\,X)$ между такими с. в. X и Y, что $\mathsf{P}(X = i,\ Y = k) = p_X(i)P_{Y\,|\,X}(k\,|\,i)$, $i,\ k = 1, \ldots, n$ является выпуклой функцией вектора $p_X = (p_X(1), \ldots, p_X(n))$ при фиксированных условных вероятностях $(P_{Y\,|\,X}(k\,|\,i))$.

2. Покажите, что $h(X) \geqslant \eta(p^*)$, где $p^* = \max\limits_x \mathsf{P}(X = x)$, и при $p^* \geqslant 1/2$ докажите неравенство

$$h(X) \geqslant 2(1 - p^*). \tag{1.6.13а}$$

Покажите также, что неравенство (1.6.13а) остаётся верным даже при $p^* < 1/2$.

Решение. 1. Выпуклость функции $h(\mathbf{p})$ означает, что

$$h(\lambda_1\mathbf{p}_1 + \lambda_2\mathbf{p}_2) \geqslant \lambda_1 h(\mathbf{p}_1) + \lambda_2 h(\mathbf{p}_2) \tag{1.6.13б}$$

для любых векторов вероятностей $\mathbf{p}_j = (p_j(1), \ldots, p_j(n))$, $j = 1, 2$, и λ_1, $\lambda_2 \in (0, 1)$, $\lambda_1 + \lambda_2 = 1$. Пусть X_1 имеет распределение $\mathbf{p}_1$, а X_2 — распределение $\mathbf{p}_2$. Положим $Y = X_Z$, где

$$Z = 1 \text{ с вероятностью } \lambda_1 \text{ или } 2 \text{ с вероятностью } \lambda_2.$$

Тогда распределением с. в. Y служит вектор $\lambda_1 \mathbf{p}_1 + \lambda_2 \mathbf{p}_2$. По п. 1 теоремы 1.2.10 имеем

$$h(Y) \geqslant h(Y \,|\, Z),$$

и по определению условной энтропии

$$h(Y \,|\, Z) = \lambda_1 h(X_1) + \lambda_2 h(X_2).$$

Это даёт неравенство (1.6.13б). Теперь

$$I(X : Y) = h(Y) - h(Y \,|\, X) = h(Y) - \sum p_X(i) h(P_{Y \,|\, X}(\cdot \,|\, i)). \tag{1.6.14}$$

При фиксированном распределении $P_{Y \,|\, X}(\cdot \,|\, \cdot)$ второй член линеен по p_X и поэтому является выпуклой функцией. Первый член $h(Y)$ — выпуклая функция от p_Y и линейная по p_X. Таким образом, $h(Y)$ является выпуклой функцией от p_X, а значит таким свойством обладает и $I(X : Y)$.

2. Рассмотрим два случая: 1) $p^* \geqslant 1/2$ и 2) $p^* \leqslant 1/2$. В первом случае по неравенству группировки данных (1.2.14) имеем

$$h(X) \geqslant \eta(p^*) \geqslant (1 - p^*) \log \frac{1}{p^*(1 - p^*)} \geqslant (1 - p^*) \log \frac{1}{4} = 2(1 - p^*),$$

поскольку $p^* \geqslant \dfrac{1}{2}$. В случае 2 применяем индукцию по n, числу значений, принимаемых с. в. X.

База индукции при $n = 3$: без ограничения общности предположим, что $p^* = p_1 \geqslant p_2 \geqslant p_3$. Тогда $1/3 \leqslant p_1 < 1/2$ и $(1 - p_1)/2 \leqslant p_2 \leqslant p_1$. Запишем

$$h(p_1, p_2, p_3) = \eta(p_1) + (1 - p_1)\eta(q),$$

где $q = \dfrac{p_2}{1 - p_1}$. Так как $1/2 \leqslant q \leqslant p_1/(1 - p_1) \leqslant 1$, имеем

$$\eta(q) \geqslant \eta(p_1/(1 - p_1)),$$

т. е.

$$h(p_1, p_2, p_3) \geqslant h(p_1, p_1, 1 - 2p_1) = 2p_1 + \eta(2p_1).$$

Неравенство $2p_1 + \eta(2p_1) \geqslant 2(1 - p_1)$ равносильно тому, что

$$\eta(2p_1) > 2 - 4p_1, \quad 1/3 \leqslant p_1 < 1/2,$$

или неравенству

$$\eta(p) > 2 - 2p, \quad 2/3 \leqslant p < 1,$$

которое следует из п. 1. Таким образом, при $n = 3$ выполнено неравенство $h(p_1, p_2, p_3) \geqslant 2(1 - p^*)$ вне зависимости от значения p^*.

Предположим теперь, что для всех с. в. X с числом значений, меньшим чем n, верно неравенство $h(X) \geqslant \eta(p^*) \geqslant 2(1 - p^*)$. Возьмём $\mathbf{p} = (p_1, \ldots, p_n)$ и предположим без ограничения общности, что $p^* = p_1 \geqslant \ldots \geqslant p_n$. Запишем $\mathbf{q} = (p_2/(1 - p_1), \ldots, p_n/(1 - p_1))$ и

$$h(\mathbf{p}) = \eta(p_1) + (1 - p_1)h(\mathbf{q}) \geqslant \eta(p_1) + (1 - p_1)2(1 - q_1). \tag{1.6.15}$$

Неравенство $h(\mathbf{p}) \geqslant 2(1 - p^*)$ будет следовать из неравенства

$$\eta(p_1) + (1 - p_1)(2 - 2q_1) \geqslant (2 - 2p_1),$$

которое эквивалентно следующему:

$$\eta(p_1) \geqslant 2(1 - p_1)(1 - 1 + q_1) = 2(1 - p_1)q_1 = 2p_2$$

для $1/n \leqslant p_1 < 1/2$, $(1 - p_1)/(n - 1) \leqslant p_2 < p_1$. Но, очевидно,

$$\eta(p_1) \geqslant 2(1 - p_1) \geqslant 2p_2$$

(где равенство достигается при $p_1 = 0, 1/2$). Неравенство (1.6.15) следует из индуктивного предположения. □

Задача 1.6.14. Пусть распределение вероятностей p_i, $i \in I = \{1, 2, \ldots, n\}$, обладает таким свойством, что $\log_2(1/p_i)$ — целые числа для всех i, при которых $p_i > 0$. Будем рассматривать I как алфавит, буквы которого кодируются двоичными словами. Код Шеннона—Фано сопоставляет букве i кодовое слово длины $l_i = \lceil \log_2(1/p_i) \rceil$. По неравенству Крафта этот код может быть построен как однозначно декодируемый. Докажите *конкурентоспособную оптимальность* этого кода: если l'_i, $i \in I$, — длины кодовых слов любого однозначно декодируемого кода, то

$$\mathsf{P}(l_i < l'_i) \geqslant \mathsf{P}(l'_i < l_i), \tag{1.6.16}$$

где равенство достигается тогда и только тогда, когда $l_i \equiv l'_i$.

Указание. Воспользуйтесь неравенством $\operatorname{sign}(l - l') \leqslant 2^{l-l'} - 1$, l, $l' = 1, \ldots, n$.

Решение. Запишем

$$\mathsf{P}(l'_i < l_i) - \mathsf{P}(l'_i > l_i) = \sum_{i:\, l'_i < l_i} p_i - \sum_{i:\, l'_i > l_i} p_i = \sum_i p_i \operatorname{sign}(l_i - l'_i) =$$

$$= \mathsf{E} \operatorname{sign}(l - l') \leqslant \mathsf{E}(2^{l-l'} - 1),$$

так как $\operatorname{sign} x \leqslant 2^x - 1$ для целых x. Далее,

$$\mathsf{E}(2^{l-l'} - 1) = \sum_i p_i(2^{l_i - l'_i} - 1) = \sum_i 2^{-l_i}(2^{l_i - l'_i} - 1) =$$
$$= \sum_i 2^{-l'_i} - \sum_i 2^{-l_i} \leqslant 1 - \sum_i 2^{-l_i} = 1 - 1 = 0$$

по неравенству Крафта. Отсюда следует неравенство

$$\mathsf{P}(l_i < l'_i) \geqslant \mathsf{P}(l'_i < l_i).$$

Случай равенства возможен только при 1) $2^{l_i - l'_i} - 1 = 0$ или 1, $i \in I$ (потому что $\operatorname{sign} x = 2^x - 1$ только при $x = 0$ или 1); 2) $\sum_i 2^{-l'_i} = 1$ (так как $\sum_i 2^{-l_i} = 1$, что возможно только при $2^{l_i - l'_i} \equiv 1$, т. е. $l_i = l'_i$). □

The Grafter Kraft, the Shining Shannon and the Funny Fano
Жуликоватый Крафт, блистательный Шеннон и забавный Фано
(Из серии «Фильмы, которые не вышли на большой экран».)

Задача 1.6.15. Дайте определение пропускной способности C двоичного канала. Пусть $C_N = (1/N) \sup I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})$, где символ $I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})$ обозначает взаимную энтропию между случайным словом $\mathbf{X}^{(N)}$ длины N, посланным по каналу, и принятым словом $\mathbf{Y}^{(N)}$, и где точная верхняя граница берётся по всем распределениям вероятностей с. в. $\mathbf{X}^{(N)}$. Докажите, что $C \leqslant \limsup_{N \to \infty} C_N$.

Решение. Двоичный канал определяется как последовательность распределений условных вероятностей

$$\mathsf{P}_{\mathrm{ch}}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}), \quad N = 1, 2, \ldots,$$

где $\mathbf{x}^{(N)} = x_1 \ldots x_N$ — двоичное слово (строка) на входе и $\mathbf{y}^{(N)} = y_1 \ldots y_N$ — двоичное слово (строка) на выходе канала. Пропускная способность канала C является асимптотическим параметром семейства $\{\mathsf{P}^{(N)}_{\mathrm{ch}}(\cdot \,|\, \cdot)\}$, определяемым как

$$C = \sup[\bar{R} \in (0, 1) \colon \bar{R} \text{— надёжная скорость передачи}]. \tag{1.6.17}$$

Здесь число $\bar{R} \in (0, 1)$ называется надёжной скоростью передачи (для данного канала), если дано, что случайные строки источника равномерно распределены на множестве $\mathcal{U}^{(N)}$ с $\#\mathcal{U}^{(N)} = 2^{N[\bar{R} + o(1)]}$, и существуют правило кодирования $f^{(N)} \colon \mathcal{U}^{(N)} \to \mathcal{X}_N \subseteq \{0, 1\}^N$ и правило декодирования $\hat{f}^{(N)} \colon \{0, 1\}^N \to \mathcal{U}^{(N)}$, для которых средняя вероятность ошибки $e^{(N)} \to 0$ при

$N \to \infty$:

$$e^{(N)}(= e^{(N)}(f^{(N)}, \hat{f}^{(N)})) := \\ := \frac{1}{\#\mathcal{U}^{(N)}} \sum_{u \in \mathcal{U}^{(N)}} \mathsf{P}_{\mathrm{ch}}^{(N)}\big(\{\mathbf{y}^{(N)} : \hat{f}^{(N)}(\mathbf{y}^{(N)}) \neq u\} \,|\, f^{(N)}(u)\big). \quad (1.6.18)$$

Обратная часть ВТШК говорит, что

$$C \leqslant \lim_{N\to\infty} \frac{1}{N} \sup_{\mathsf{P}_{\mathbf{X}^{(N)}}} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}), \quad (1.6.19)$$

где $I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})$ — взаимная информация между случайными входной и выходной строками $\mathbf{X}^{(N)}$ и $\mathbf{Y}^{(N)}$, а $\mathsf{P}_{\mathbf{X}^{(N)}}$ — распределение с. в. $\mathbf{X}^{(N)}$.

Для доказательства достаточно проверить, что если $\#\mathcal{U}^{(N)} = 2^{N[\bar{R}+o(1)]}$, то для всех $f^{(N)}$ и $\hat{f}^{(N)}$ выполнено неравенство

$$e^{(N)} \geqslant 1 - \frac{C_N + o(1)}{\bar{R} + o(1)}, \quad (1.6.20)$$

где

$$C_N = \frac{1}{N} \sup_{\mathsf{P}_{\mathbf{X}^{(N)}}} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}).$$

Действительно, если $\bar{R} > \limsup_{N\to\infty} C_N$, то согласно формуле (1.6.20) имеем $\lim_{N\to\infty} \inf_{f^{(N)}, \hat{f}^{(N)}} e^{(N)} > 0$ и $\bar{R}$ не является надёжной скоростью передачи.

Для доказательства неравенства (1.6.20) предположим без ограничения общности, что $f^{(N)}$ кодирует без потерь. Тогда входное слово $\mathbf{x}^{(N)}$ равномерно распределено с вероятностью $1/(\#\mathcal{U})$. Для всех правил декодирования $\hat{f}^{(N)}$ и любого достаточно большого N имеем

$$NC_N \geqslant I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \geqslant I(\mathbf{X}^{(N)} : \hat{f}(\mathbf{Y}^{(N)})) = h(\mathbf{X}^{(N)}) - h(\mathbf{X}^{(N)} \,|\, \hat{f}(\mathbf{Y}^{(N)})) = \\ = \log(\#\mathcal{U}^{(N)}) - h(\mathbf{X}^{(N)} \,|\, \hat{f}(\mathbf{Y}^{(N)})) \geqslant \\ \geqslant \log(\#\mathcal{U}^{(N)}) - 1 - \varepsilon^{(N)} \log(\#\mathcal{U}^{(N)} - 1). \quad (1.6.21)$$

Последнее неравенство здесь следует из обобщённого неравенства Фано (1.2.11)

$$h(\mathbf{X}^{(N)} \,|\, \hat{f}(\mathbf{Y}^{(N)})) \leqslant \eta(\varepsilon^{(N)}) + \varepsilon^{(N)} \log(\#\mathcal{U}^{(N)} - 1) \leqslant 1 + \varepsilon^{(N)} \log(\#\mathcal{U}^{(N)} - 1).$$

Теперь из неравенства (1.6.21) следует оценка (1.6.20):

$$NC_N \geqslant N[\bar{R} + o(1)] - 1 - \varepsilon^{(N)} \log\Big(2^{N[\bar{R}+o(1)]} - 1\Big),$$

т. е.

$$e^{(N)} \geqslant \frac{N[\bar{R}+o(1)]-NC_N-1}{\log(2^{N[\bar{R}+o(1)]}-1)} = 1-\frac{C_N+o(1)}{\bar{R}+o(1)}. \qquad \square$$

Задача 1.6.16. На вход д. с. к. б. п. подаются нули и единицы, а на выходе, кроме них, появляется ещё и $*$ (как трудно читаемый символ). Матрица канала состоит из элементов

$$\mathbf{P}(0\,|\,0)=1,\ \ \mathbf{P}(0\,|\,1)=\mathbf{P}(1\,|\,1)=\mathbf{P}(*\,|\,1)=1/3.$$

Вычислите пропускную способность канала и входные вероятности $p_X(0)$ и $p_X(1)$, при которых пропускная способность достигается.

Поскольку символ $*$ принимается только при посланной единице, то предлагается воспринимать его как 1: такое соглашение позволит извлечь больше информации из выходной последовательности и улучшит пропускную способность канала. Согласны ли вы с этим? Обоснуйте свой ответ.

Решение. Воспользуемся формулой

$$C=\sup_{p_X} I(X:Y)=\sup_{p_X}[h(Y)-h(Y\,|\,X)],$$

где p_X — распределение входных символов:

$$p_X(0)=p,\quad p_X(1)=1-p,\quad 0\leqslant p\leqslant 1.$$

Вычислим $I(X:Y)$ как функцию от p:

$$h(Y)=-p_Y(0)\log p_Y(0)-p_Y(1)\log p_Y(1)-p_Y(*)\log p_Y(*).$$

Здесь

$$\begin{aligned} p_Y(0)&=p+(1-p)/3=(1+2p)/3,\\ p_Y(1)&=p_Y(*)=(1-p)/3 \end{aligned}$$

и

$$h(Y)=-\frac{1+2p}{3}\log\frac{1+2p}{3}-\frac{2(1-p)}{3}\log\frac{1-p}{3}.$$

Кроме того,

$$h(Y\,|\,X)=-\sum_{x=0,1}p_X(x)\sum_y P(y\,|\,x)\log P(y\,|\,x)=-p_X(1)\log 1/3=(1-p)\log 3.$$

Таким образом,

$$I(X:Y)=-\frac{1+2p}{3}\log\frac{1+2p}{3}-\frac{2(1-p)}{3}\log\frac{1-p}{3}-(1-p)\log 3.$$

Дифференцируя последнее равенство, получаем

$$\frac{d}{dp}I(X:Y)=-\frac{2}{3}\log\left(\frac{1}{3}+\frac{2p}{3}\right)+\frac{2}{3}\log\left(\frac{1}{3}-\frac{p}{3}\right)+\log 3.$$

Для точки максимума функции $I(X:Y)$ получаем уравнение

$$\frac{2}{3}\log\frac{1-p}{1+2p}+\log 3=0.$$

Используя обозначение $b:=-\frac{3}{2}\log 3$, получаем

$$p=\frac{1-2^b}{1+2^{b+1}}.$$

Для последней части задачи воспользуемся неравенством обработки данных:

$$I(X:Y)=h(X)-h(X\,|\,Y)\leqslant h(X)-h(X\,|\,Y')=I(X:Y')$$

для любой функции Y' от Y. Равенство достигается тогда и только тогда, когда Y и X условно независимы при данной с. в. Y'. Это как раз наш случай, поэтому пропускная способность останется без изменений. □

Задача 1.6.17. 1. Определите совместную $h(X,\,Y)$ и условную $h(X\,|\,Y)$ энтропии для дискретных с. в.

2. Докажите, что $h(X,\,Y)\geqslant h(X\,|\,Y)$ и объясните, когда достигается равенство.

3. Пусть $0<\delta<1$. Докажите, что

$$h(X\,|\,Y)\geqslant(\log(\delta^{-1}))\,\mathsf{P}(q(X,\,Y)\leqslant\delta),$$

где $q(X,\,Y)=\mathsf{P}(X=x\,|\,Y=y)$. При каких δ и с. в. X и Y здесь получается равенство?

Решение. 1. Условная энтропия определяется по формуле:

$$h(X\,|\,Y)=-\,\mathsf{E}\log q(x,\,y)=-\sum_{x,y}\mathsf{P}(X=x,\,Y=y)\log q(x,\,y).$$

Совместная энтропия определяется как

$$h(X,\,Y)=-\sum_{x,y}\mathsf{P}(X=x,\,Y=y)\log\mathsf{P}(X=x,\,Y=y).$$

2. По определению

$$h(X,\,Y)=h(X\,|\,Y)-\sum_{y}\mathsf{P}(Y=y)\log\mathsf{P}(Y=y)\geqslant h(X\,|\,Y).$$

Равенство здесь достигается, только если $h(Y)=0$, т. е. Y является константой.

3. По неравенству Чебышёва имеем

$$\mathsf{P}(q(X,\,Y)\leqslant\delta)=\mathsf{P}(-\log q(X,\,Y)\geqslant\log(\delta^{-1}))\leqslant$$
$$\leqslant\frac{1}{\log(\delta^{-1})}\,\mathsf{E}[-\log q(X,\,Y)]=\frac{1}{\log(\delta^{-1})}h(X\,|\,Y).$$

Равенство здесь достигается тогда и только тогда, когда

$$\mathsf{P}(q(X,\,Y)=\delta)=1.$$

Для этого нужно, чтобы 1) выполнялось условие $\delta = 1/m$, где m — натуральное число, и 2) для всех y из носителя с. в. Y нашлось бы такое множество A_y, состоящее из m элементов, что

$$\mathsf{P}(X=x\,|\,Y=y)=\frac{1}{m},\quad \forall x\in A_y. \qquad \square$$

Задача 1.6.18. Источник Бернулли с алфавитом $1, 2, \ldots, m$ и вероятностями $p_1, \ldots, p_m$ генерирует текст. Нужно надёжно переслать этот текст по д. с. к. б. п. с вероятностью ошибки на символ p^*. Покажите, что пропускная способность канала вычисляется по формуле

$$C = 1 - \eta(p^*).$$

Объясните, почему возможна надёжная передача, если

$$h(p_1,\,\ldots,\,p_m)+\eta(p^*)<1,$$

где $h(p_1, \ldots, p_m) = -\sum\limits_{i=1}^{m} p_i \log p_i$.

Решение. Асимптотическое свойство равнораспределённости (а. с. р.) утверждает, что число различных слов (строк) длины n, сгенерированных источником Бернулли, «типично» равно $2^{nH+o(n)}$, причём слова имеют «почти равные» вероятности $2^{-nH+o(n)}$:

$$\lim_{n\to\infty}\mathsf{P}\left(2^{-n(H+\varepsilon)}\leqslant \mathsf{P}_n(\mathbf{U}^{(n)})\leqslant 2^{-n(H-\varepsilon)}\right)=1.$$

Здесь $H = h(p_1, \ldots, p_n)$.

Обозначим

$$T_n(=T_n(\varepsilon))=\{\mathbf{u}^{(n)}\colon 2^{-n(H+\varepsilon)}\leqslant \mathsf{P}_n(\mathbf{u}^{(n)})\leqslant 2^{-n(H-\varepsilon)}\}$$

и заметим, что

$$\lim_{n\to\infty}\frac{1}{n}\log\#T_n=H,\quad \text{т. е. } \limsup_{n\to\infty}\frac{1}{n}\log\#T_n<H+\varepsilon.$$

По определению пропускной способности д. с. к. б. п. слово $\mathbf{u}^{(n)}\in T_n(\varepsilon)$ можно закодировать двоичным кодовым словом длины $\bar{R}^{-1}(H+\varepsilon)n$ и надёжно передать по д. с. к. б. п. с матрицей

$$\begin{pmatrix} 1-p^* & p^* \\ p^* & 1-p^* \end{pmatrix}$$

при любом $\bar{R} < C$, где

$$C = \sup_{p_X} I(X:Y) = \sup_{p_X}[h(Y) - h(Y|X)].$$

Точная верхняя граница здесь берётся по всем распределениям $p_X = (p_X(0), p_X(1))$ входного двоичного символа X; условное распределение выходного символа Y дано следующей формулой:

$$\mathsf{P}(Y = y|X = x) = \begin{cases} 1 - p^*, & y = x, \\ p^*, & y \neq x. \end{cases}$$

Мы видим, что

$$h(Y|X) = -p_X(0)\eta(p^*) + p_X(1)\eta(p^*) = \eta(p^*),$$

не зависит от p_X. Следовательно,

$$C = \sup_{p_X} h(Y) - \eta(p^*) = 1 - \eta(p^*),$$

так как $h(Y)$ достигает единицы при $p_Y(0) = p_Y(1) = 1/2$ (что бывает при $p_X(0) = p_X(1) = 1/2$). Следовательно, если

$$H < C \iff h(p_1, \ldots, p_n) + \eta(p^*) < 1, \tag{1.6.22}$$

то $\bar{R}^{-1}(H + \varepsilon)$ можно сделать меньше 1 при достаточно малом $\varepsilon > 0$ и $\bar{R} < C$, близком к C. Это означает, что существует последовательность кодов f_n длины n, такая что вероятность ошибки (при использовании кода f_n и м. п. декодирования) ограничена сверху:

$$\mathsf{P}(\mathbf{u}^{(n)} \notin T_n) + \\ + \mathsf{P}\big(\mathbf{u}^{(n)} \in T_n;\ \text{ошибки при использовании } f_n(\mathbf{u}^{(n)}) \text{ и м. п. декодера}\big) \to 0, \\ \text{при } n \to \infty,$$

поскольку обе вероятности стремятся к нулю.

С другой стороны, если $H > C$, то $\bar{R}^{-1}H > 1\ \forall \bar{R} < C$ и невозможно закодировать слово $\mathbf{u}^{(n)} \in T_n$ кодовым словом длины n так, чтобы вероятность ошибки стремилась к нулю, т. е. надёжная передача невозможна. □

Задача 1.6.19. Рассмотрим марковский источник с алфавитом из m символов и матрицей переходов P_m вида

$$P_m = \begin{pmatrix} 2/3 & 1/3 & 0 & 0 & \ldots & 0 \\ 1/3 & 1/3 & 1/3 & 0 & \ldots & 0 \\ 0 & 1/3 & 1/3 & 1/3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 2/3 \end{pmatrix}.$$

Найдите скорость передачи информации этого источника.

Теперь рассмотрим источник с алфавитом $m+n$ и матрицей переходов вида $\begin{pmatrix} P_m & 0 \\ 0 & P_n \end{pmatrix}$, где нули изображают нулевые матрицы подходящего размера. Считаем, что начальный символ равномерно распределён по алфавиту. Какова скорость передачи у этого источника?

Решение. Матрица P_m симметрична, и ц. м. д. в. имеет равномерное инвариантное распределение $\pi = (\pi_i)$, где $\pi_i = 1/m$, $1 \leqslant i \leqslant m$. Скорость передачи информации равна

$$H_m = -\sum_{j,k} \pi_j p_{jk} \log p_{jk} =$$

$$= -\frac{1}{m}\left[2\left(\frac{2}{3}\log\frac{2}{3} + \frac{1}{3}\log\frac{1}{3}\right) + 3(m-2)\frac{1}{3}\log\frac{1}{3}\right] = \log 3 - \frac{4}{3m}.$$

Источник с матрицей переходов $\begin{pmatrix} P_m & 0 \\ 0 & P_n \end{pmatrix}$ не является эргодическим, и его скорость передачи информации равна максимальной из скоростей:

$$\max[H_m,\, H_n] = H_{\max[m,n]}. \qquad \square$$

Задача 1.6.20. Рассмотрим источник с конечным алфавитом. Определим $J_n = n^{-1}h(\mathbf{U}^{(n)})$ и $K_n = h(U_{n+1}\,|\,\mathbf{U}^{(n)})$ для $n = 1, 2, \ldots$. Здесь U_n — n-й символ в последовательности и $\mathbf{U}^{(n)}$ — строка, составленная из первых n символов, $h(\mathbf{U}^{(n)})$ — энтропия и $h(U_{n+1}\,|\,\mathbf{U}^{(n)})$ — условная энтропия. Покажите, что для стационарного источника J_n и K_n — невозрастающие функции, имеющие общий предел.

Предположите, что источник марковский, но не обязательно стационарный, и покажите, что взаимная информация между U_1 и U_2 не меньше, чем между U_1 и U_3.

Решение. Для доказательства второй части заметим, что из свойства Маркова следует равенство

$$\mathsf{P}(U_1 = u_1\,|\,U_2 = u_2,\, U_3 = u_3) = \mathsf{P}(U_1 = u_1\,|\,U_2 = u_2).$$

Таким образом,

$$I(U_1 : (U_2,\, U_3)) = \mathsf{E}\left[-\log\frac{\mathsf{P}(U_1 = u_1\,|\,U_2 = u_2,\, U_3 = u_3)}{\mathsf{P}(U_1 = u_1)}\right] =$$

$$= \mathsf{E}\left[-\log\frac{\mathsf{P}(U_1 = u_1\,|\,U_2 = u_2)}{\mathsf{P}(U_1 = u_1)}\right] = I(U_1 : U_2).$$

Результат непосредственно вытекает из неравенства

$$I(U_1 : (U_2,\, U_3)) \geqslant I(U_1 : U_3). \qquad \square$$

Задача 1.6.21. Постройте код Хаффмана для множества из пяти сообщений, если их вероятности представлены в следующей таблице:

Сообщение	1	2	3	4	5
Вероятность	0,1	0,15	0,2	0,26	0,29

Решение.

Сообщение	1	2	3	4	5
Вероятность	0,1	0,15	0,2	0,26	0,29
Кодовое слово	101	100	11	01	00

Средняя длина кодового слова составляет 2,4. □

Задача 1.6.22. Сформулируйте первую теорему Шеннона о кодировании для канала с шумом (ПТШК) и дайте ее интерпретацию с точки зрения свойства а. с. р. Что такое скорость передачи информации для источника Бернулли?

Пусть $\mathbf{U}^{(n)}$ — строка, составленная из первых n символов, сгенерированных источником Бернулли, который порождает символы 0, 1 с вероятностями $1-p$ и p соответственно, $0<p<1$. Докажите, что найдётся такое множество T_n возможных значений строки $\mathbf{U}^{(n)}$, что

$$\mathsf{P}(\mathbf{U}^{(n)}\in T_n)\geqslant 1-\left(\log\frac{p}{1-p}\right)^2\frac{p(1-p)}{n\varepsilon^2}, \tag{1.6.23}$$

и что для каждого $\mathbf{u}^n\in T_n$ вероятность $\mathsf{P}(\mathbf{U}^{(n)}=\mathbf{u}^{(n)})$ лежит между $2^{-n(\eta(p)+\varepsilon)}$ и $2^{-n(\eta(p)-\varepsilon)}$ для любого $\varepsilon>0$.

Решение. Для источника Бернулли имеем

$$-\frac{1}{n}\log P_n(\mathbf{U}^{(n)})=-\frac{1}{n}\sum_{1\leqslant j\leqslant n}\log P(U_j)\to\eta(p),$$

в том смысле, что для любого $\varepsilon>0$ выполняется неравенство

$$\mathsf{P}\left(\left|-\frac{1}{n}\log P_n(\mathbf{U}^{(n)})-\eta(p)\right|>\varepsilon\right)\leqslant$$
$$\leqslant\frac{1}{\varepsilon^2n^2}\mathrm{Var}\left(\sum_{1\leqslant j\leqslant n}\log P(U_j)\right)=\frac{1}{\varepsilon^2n}\mathrm{Var}[\log P(U_1)]. \tag{1.6.24}$$

Здесь

$$P(U_j)=\begin{cases}1-p, & \text{если } U_j=0,\\ p, & \text{если } U_j=1,\end{cases}\qquad P_n(\mathbf{U}^{(n)})=\prod_{1\leqslant j\leqslant n}p(U_j)$$

и

$$\mathrm{Var}\left(\sum_{i\leqslant j\leqslant n}\log P(U_j)\right)=\sum_{i\leqslant j\leqslant n}\mathrm{Var}(\log P(U_j)),$$

где

$$\operatorname{Var}(\log P(U_j)) = \mathsf{E}[\log P(U_j)]^2 - [\mathsf{E}\log P(U_j)]^2 =$$
$$= p(\log p)^2 + (1-p)(\log(1-p))^2 - (\eta(p))^2 = p(1-p)\Big(\log\frac{p}{1-p}\Big)^2.$$

Таким образом, из неравенства (1.6.24) следует, что

$$\mathsf{P}(2^{-n(\eta(p)+\varepsilon)} \leqslant P_n(\mathbf{U}^{(n)}) \leqslant 2^{-n(\eta(p)-\varepsilon)}) \geqslant 1 - \frac{1}{n\varepsilon^2}p(1-p)\Big(\log\frac{p}{1-p}\Big)^2.$$

Неравенство (1.6.23) выполняется, если положить

$$T_n = (\mathbf{u}^{(n)} = u_1 \ldots u_n \colon 2^{-n(\eta(p)+\varepsilon)} \leqslant P_n(\mathbf{U}^{(n)} = \mathbf{u}^{(n)}) \leqslant 2^{-n(\eta(p)-\varepsilon)}). \qquad \square$$

Задача 1.6.23. Сформулируйте неравенство Крафта для длин кодовых слов $s_1, \ldots, s_m$ декодируемого кода. Предположим, что источник генерирует буквы алфавита из q символов с известными вероятностями $p_i > 0$ появления букв i. Пусть S — случайная длина кодового слова, получающегося из побуквенного кодирования выхода источника. Хотелось бы найти декодируемый код, минимизирующий $\mathsf{E}(q^S)$. Докажите оценку $\mathsf{E}(q^S) \geqslant \Big(\sum\limits_{1\leqslant i\leqslant m}\sqrt{p_i}\Big)^2$ и укажите, когда достигается равенство.

Докажите также, что при оптимальном кодировании по критерию, сформулированному выше, должно выполняться неравенство

$$\mathsf{E}(q^S) < q\Big(\sum_{1\leqslant i\leqslant m}\sqrt{p_i}\Big)^2. \tag{1.6.25}$$

Указание. Воспользуйтесь неравенством Коши—Шварца

$$\sum_{1\leqslant i\leqslant m} x_i y_i \leqslant \Big(\sum_{1\leqslant i\leqslant m} x_i^2\Big)^{1/2}\Big(\sum_{1\leqslant i\leqslant m} y_i^2\Big)^{1/2}$$

для всех положительных x_i, y_i, где равенство достигается тогда и только тогда, когда $x_i = cy_i$ для всех i.

Решение. По неравенству Коши—Шварца имеем

$$\sum_{1\leqslant i\leqslant m} p_i^{1/2} = \sum_{1\leqslant i\leqslant m} p_i^{1/2} q^{s_i/2} q^{-s_i/2} \leqslant$$
$$\leqslant \Big(\sum_{1\leqslant i\leqslant m} p_i q^{s_i}\Big)^{1/2}\Big(\sum_{1\leqslant i\leqslant m} q^{-s_i}\Big)^{1/2} \leqslant \Big(\sum_{1\leqslant i\leqslant m} p_i q^{s_i}\Big)^{1/2};$$

по неравенству Крафта $\sum_{1\leqslant i\leqslant m} q^{-s_i} < 1$. Следовательно,

$$\mathsf{E}(q^S) = \sum_{1\leqslant i\leqslant m} p_i q^{s_i} \geqslant \Bigg(\sum_{1\leqslant i\leqslant m} p_i^{1/2} \Bigg)^2.$$

Теперь выберем вероятности следующим образом:

$$p_i = (cq^{-x_i})^2 \quad \text{при некоторых} \quad x_i > 0,$$

где $\sum_{1\leqslant i\leqslant m} q^{-x_i} = 1$, так что $\sum_{1\leqslant i\leqslant m} p_i^{1/2} = c$, и $c = \Big(\sum_j q^{-2x_j} \Big)^{-1/2}$. В качестве s_i возьмём наименьшие целые числа не меньше x_i. Тогда $\sum_{1\leqslant i\leqslant m} q^{-s_i} \leqslant 1$ и, вновь по неравенству Крафта, существует декодируемый код с длинами кодовых слов s_i. Для этого кода $q^{s_i-1} < q^{x_i} = c/(p_i^{1/2})$, поэтому

$$\mathsf{E}(q^S) = \sum_{1\leqslant i\leqslant m} p_i q^{s_i} = q \sum_{1\leqslant i\leqslant m} p_i q^{s_i-1} <$$

$$< q \sum_{1\leqslant i\leqslant m} p_i q^{x_i} = qc \sum_{1\leqslant i\leqslant m} p_i^{1/2} = q \Bigg(\sum_{1\leqslant i\leqslant m} p_i^{1/2} \Bigg)^2,$$

тем более неравенство (1.6.25) выполнено для оптимального кода. □

Задача 1.6.24. Источник Бернулли со скоростью передачи информации H последовательно подает символы на линию передач, которая может как функционировать, так и перестать работать. Если линия функционирует во время передачи символа, то он принимается на выходе неискажённым. Если линия перестаёт работать, то получатель понимает только то, что она действительно не работает. Переходы между этими двумя состояниями линии описываются ц. м. д. в. с постоянными вероятностями переходов, независимыми от передающегося текста.

Покажите, что скорость передачи информации источника, под которым понимается полученный сигнал, равна $H_{RS} = H_L + \pi_L^1 H_S$ где $H_S = -\sum_j p_j \log p_j$ — энтропия сигнала, H_L — скорость передачи информации ц. м. д. в., регулирующей работу линии, и π_L^1 — стационарная вероятность того, что линия работает.

Решение. Скорость генерирования информации источником Бернулли $H = -\sum_j p_j \log p_j$, где p_j — вероятность появления символа $j = 1, 2, \ldots$ Состояние линии описывается ц. м. д. в. с матрицей переходных вероятностей вида

$$\begin{array}{r} \text{не работает} \\ \text{работает} \end{array} \begin{pmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{pmatrix}$$

и инвариантным распределением

$$\pi_L^0(\text{не работает}) = \frac{\beta}{\alpha+\beta}, \quad \pi_L^1(\text{работает}) = \frac{\alpha}{\alpha+\beta}$$

(предполагается, что $\alpha+\beta>0$). Последовательность полученных сигналов представляет собой ц. м. д. в. с состояниями 0 (не работает), 1, 2, ... и следующими вероятностями переходов:

$$q_{00} = 1-\alpha, \quad q_{0j} = \alpha p_j, \quad q_{j0} = \beta, \quad q_{jk} = (1-\beta)p_k, \quad j,\, k \geqslant 1.$$

Ц. м. д. в., описывающая полученный сигнал, имеет единственное инвариантное распределение

$$\pi_{RS}(0) = \frac{\beta}{\alpha+\beta}, \quad \pi_{RS}(j) = \frac{\alpha}{\alpha+\beta}p_j, \quad j \geqslant 1.$$

Тогда скорость передачи информации полученного сигнала равна

$$H_{\mathrm{RS}} = -\sum_{j,k\geqslant 0} \pi_{\mathrm{RS}}(j) q_{jk} \log q_{jk} =$$

$$= -\frac{\beta}{\alpha+\beta}\left[(1-\alpha)\log(1-\alpha) + \sum_{j\geqslant 1}\alpha p_j \log(\alpha p_j)\right] -$$

$$-\frac{\alpha}{\alpha+\beta}\left(\sum_{j\geqslant 1} p_j\left[\beta\log\beta + (1-\beta)\sum_{k\geqslant 1} p_k \log((1-\beta)p_k)\right]\right) = H_L + \frac{\alpha}{\alpha+\beta}H_S.$$

Здесь H_L — энтропийная скорость ц. м. д. в., описывающей состояние линии:

$$H_L = \frac{\beta}{\alpha+\beta}\eta(\alpha) + \frac{\alpha}{\alpha+\beta}\eta(\beta). \qquad \square$$

Задача 1.6.25. Рассмотрим источник Бернулли, генерирующий символы $i = 1, \ldots, m$ с вероятностями p_i. Пусть n_i — число появлений символа i в последовательности $\mathbf{u}^{(n)} = u_1 u_2 \ldots u_n$ длины n. Пусть A_n — минимальный набор последовательностей $\mathbf{u}^{(n)}$, вероятность которого оценивается снизу $1-\varepsilon$. Покажите, что каждая последовательность из A_n удовлетворяет неравенству

$$-\sum n_i \log p_i \leqslant nh + (nv/\varepsilon)^{1/2}, \tag{1.6.26}$$

где v — константа, не зависящая от n и ε. Сформулируйте аналогичное утверждение для марковского источника.

Решение. Для источника Бернулли с m символами вероятность данной строки $\mathbf{u}^{(n)} = u_1 \ldots u_n$ равна

$$\mathsf{P}(\mathbf{U}^{(n)} = \mathbf{u}^{(n)}) = \prod_{1\leqslant i\leqslant m} p_i^{n_i}.$$

Множество A_n состоит из строк максимальной вероятности (отобранных по убыванию вероятности), т. е. имеющих максимальное значение $\log \mathsf{P}(\mathbf{U}^{(n)} = \mathbf{u}^{(n)}) = \sum\limits_{1 \leqslant i \leqslant m} n_i \log p_i$. Следовательно,

$$A_n = \left\{ \mathbf{u}^{(n)} : \ -\sum_i n_i \log p_i \leqslant c \right\}$$

для некоторой (вещественной) константы c, которую ещё нужно найти. Для этого воспользуемся неравенством

$$\mathsf{P}(A_n) \geqslant 1 - \varepsilon.$$

Значит, c — это такое число, для которого

$$\mathsf{P}\left(\mathbf{u}^{(n)} : \ -\sum_i n_i \log p_i \geqslant c \right) < \varepsilon.$$

Теперь для случайной строки $\mathbf{U}^{(n)} = U_1 \ldots U_n$ обозначим через N_i число появлений символа i. Тогда

$$-\sum_{1 \leqslant i \leqslant m} N_i \log p_i = \sum_{j=1}^{n} \theta_j, \quad \text{где } \theta_j = -\log p_i, \ \text{ если } U_j = i.$$

Поскольку U_j — н. о. р. с. в., такими же будут и с. в. θ_j. Далее,

$$\mathsf{E}\theta_j = -\sum_{1 \leqslant i \leqslant m} p_i \log p_i := h$$

и

$$\mathrm{Var}[\theta_j] = \mathsf{E}(\theta_j)^2 - (\mathsf{E}\theta_j)^2 = \sum_{1 \leqslant i \leqslant m} p_i (\log p_i)^2 - \left(\sum_{1 \leqslant i \leqslant m} p_i \log p_i \right)^2 := v.$$

Таким образом,

$$\mathsf{E}\left[\sum_{j=1}^{n} \theta_j \right] = nh \quad \text{и} \quad \mathrm{Var}\left[\sum_{j=1}^{n} \theta_j \right] = nv.$$

Напомним, что $h = H$ — скорость передачи информации источника.

По неравенству Чебышёва для любого $b > 0$ имеем

$$\mathsf{P}\left(\left| -\sum_{1 \leqslant i \leqslant m} N_i \log p_i - nh \right| > b \right) \leqslant \frac{nv}{b^2},$$

а при $b = \sqrt{nv/\varepsilon}$ мы получаем

$$\mathsf{P}\left(\left| - \sum_{1 \leqslant i \leqslant m} N_i \log p_i - nh \right| > \sqrt{\frac{nv}{\varepsilon}}\right) \leqslant \varepsilon.$$

Следовательно, $\forall \mathbf{u}^{(n)} \in A_n$ имеет место неравенство

$$- \sum_{1 \leqslant i \leqslant m} n_i \log p_i \leqslant nh + \sqrt{\frac{nv}{\varepsilon}} := c.$$

Для неприводимого и апериодичного марковского источника неравенство (1.6.26) выполняется при

$$h = - \sum_{1 \leqslant i,j \leqslant m} \pi_i p_{ij} \log p_{ij} \quad \text{и} \quad v = \limsup_{n \to \infty} \frac{1}{n} \operatorname{Var}\left[\sum_{j=1}^{n} \theta_j\right]. \qquad \square$$

Задача 1.6.26. Продемонстрируйте, что эффективная декодируемая процедура кодирования в канале с шумом приводит к энтропии как мере наилучшей достижимой скорости передачи.

Выбираются слова длин s_i, $i = 1, \ldots, n$, из алфавита $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$, минимизирующие среднюю длину кодового слова $\sum\limits_{i=1}^{n} p_i s_i$ так, чтобы код допускал декодирование, но выполнялось дополнительное условие $\sum\limits_{i=1}^{n} \hat{p}_i s_i \leqslant b$. Здесь $\hat{p}_i$ — некоторое альтернативное распределение вероятностей символов исходного алфавита, которое сравнивается с априорным распределением $\{p_i\}$.

Найдите нижнюю границу суммы $\sum\limits_{i=1}^{n} p_i s_i$.

Решение. Сформулируем задачу минимизации, отбросив требование, что s_i — натуральные числа:

$$\begin{aligned} &\text{минимизировать } \sum_{i=1}^{n} p_i s_i \text{ при условиях } s_i \geqslant 0 \\ &\text{и } \sum_i q^{-s_i} \leqslant 1 \text{ (неравенство Крафта).} \end{aligned} \tag{1.6.27}$$

Её можно решить методом Лагранжа с лагранжианом

$$\mathcal{L}(s_1, \ldots, s_n; \lambda) = \sum_{1 \leqslant i \leqslant n} s_i p_i - \lambda\left(1 - \sum_{1 \leqslant i \leqslant n} q^{-s_i}\right).$$

Решение такой ослабленной задачи единственно:

$$s_i = -\log_q p_i, \quad 1 \leqslant i \leqslant n, \tag{1.6.28}$$

и оптимальное значение v_{rel} равно

$$v_{\text{rel}} = -\sum_{1 \leqslant i \leqslant n} p_i \log_q p_i = h,$$

что даёт нижнюю границу оптимальной средней длины кодового слова:

$$\sum_i s_i^* p_i \geqslant h.$$

Теперь рассмотрим дополнительное ограничение

$$\sum_{1 \leqslant i \leqslant n} \hat{p}_i s_i \leqslant b. \tag{1.6.29}$$

Ослабленная задача (1.6.27) с дополнительным ограничением (1.6.29) вновь может быть решена методом Лагранжа. Здесь если

$$-\sum_i \hat{p}_i \log_q p_i \leqslant b,$$

то дополнительное ограничение не влияет на задачу минимизации (1.6.27), т. е. оптимальные положительные $s_1, \ldots, s_n$ совпадут с теми, что приведены в формуле (1.6.28), и оптимальным значением будет h. Заметим, что при $-\sum_i \hat{p}_i \log_q p_i > b$ новые минимизирующие значения $\tilde{s}_1, \ldots, \tilde{s}_n$ всё ещё будут единственными (так как задача останется строго лагранжевой) и оба ограничения принимают форму равенств:

$$\sum_i q^{-\tilde{s}_i} = 1, \quad \sum_i \hat{p}_i \tilde{s}_i = b.$$

В обоих случаях $h \leqslant \tilde{v}_{\text{rel}}$, где $\tilde{v}_{\text{rel}}$ — оптимальное значение для новой ослабленной задачи.

Наконец, решение $\tilde{s}_1^*, \ldots, \tilde{s}_n^*$ задачи с целочисленной длиной слова

$$\begin{aligned} &\text{минимизировать } \sum_{i=1}^n p_i s_i \\ &\text{при условиях } s_i \geqslant 1,\ \ s_i \in \mathbb{N} \ \text{ и } \ \sum_i q^{-s_i} \leqslant 1,\ \ \sum_i \hat{p}_i s_i \leqslant b \end{aligned} \tag{1.6.30}$$

удовлетворяет неравенствам $h \leqslant \tilde{v}_{\text{rel}} \leqslant \sum_i \tilde{s}_i^* p_i$, $\sum_i \tilde{s}_i^* \hat{p}_i \leqslant b$. □

Задача 1.6.27. Пусть ц. м. д. в. (X_t) имеет переходные вероятности вида

$$p_{jk} = \mathsf{P}(X_{t+1} = k \,|\, X_t = j), \quad t = 1, 2, \ldots,$$

с инвариантным распределением (π_j). Предположим, что буквы могут искажаться из-за шума (в этом случае отмечается лишь то, что символ невозможно прочесть) с вероятностью $\beta = 1 - \alpha$ независимо от текущей или предыдущей буквы или предыдущего шума. Покажите, что скорость передачи информации зашумлённого источника вычисляется по формуле

$$H = -\alpha \log \alpha - \beta \log \beta - \alpha^2 \sum_j \sum_k \sum_{s \geqslant 1} \pi_j \beta^{s-1} p_{jk}^{(s)} \log p_{jk}^{(s)},$$

где $p_{jk}^{(s)}$ — вероятность s-шагового перехода исходной ц. м. д. в.

Решение. Обозначим последовательность символов зашумлённого источника через $\{\tilde{X}_t\}$, где $\tilde{X}_t = *$ для каждого нечитаемого символа. При этом строка $\tilde{x}_1^n$ из зашумлённого источника получается из строки x_1^n исходного марковского источника заменой непрочитанных символов звёздочкой. Вероятность $p_n(\tilde{x}) = \mathsf{P}(\tilde{X}_i^n = \tilde{x}_i^n)$ такой строки равна

$$\sum_{x_1^n \text{ согласуется с } \tilde{x}_1^n} \mathsf{P}(X_1^n = x_1^n)\, \mathsf{P}(\tilde{X}_1^n \,|\, X_1^n = x_1^n) \tag{1.6.31}$$

и вычисляется как произведение, где вероятность первого неискаженного символа в $\tilde{x}_1^n$ равна

$$\pi_{x_1}\alpha \quad \text{или} \quad \sum_y \pi_y p_{yx}^{(s)} \beta^{s-1}\alpha, \quad \text{где } 1 < s \leqslant n, \quad \text{или } 1$$

в зависимости от того, где он появляется (если он вообще есть). Следующий множитель, вносящий вклад в формулу (1.6.31), имеет схожую структуру

$$p_{x_{t-1},x_t}\beta \quad \text{или} \quad p_{x_{t-1},x_t}^{(s)}\beta^{s-1}\alpha, \quad \text{или } 1.$$

Вычислим количество информации $-\log p_n(\tilde{x}_1^n)$, отвечающее строке $\tilde{x}_1^n$:

$$\begin{aligned} -\log \mathsf{P}(X_{s_1} = x_{s_1}) - (s_1 - 1)\log\beta - \log\alpha - \\ - \log p_{x_{s_1}x_{s_2}}^{(s_2 - s_1)} - (s_2 - s_1 - 1)\log\beta - \log\alpha - \ldots \\ \ldots - \log p_{x_{s_{N-1}}x_{s_N}}^{(s_N - s_{N-1})} - (s_N - s_{N-1} - 1)\log\beta - \log\alpha, \end{aligned}$$

где $1 \leqslant s_1 < \ldots < s_N \leqslant n$ — последовательные позиции неискажённых символов в строке $\tilde{x}_1^n$.

Теперь подсчитаем скорость передачи информации H, заданную случайной строкой $\tilde{X}_1^n$. Игнорируя начальный бит, запишем

$$-\frac{1}{n}\log p_n(\tilde{X}_1^n) = -\frac{N(\beta)}{n}\log\beta - \frac{N(\alpha)}{n}\log\alpha - \sum_i \frac{N(i,\, j;\, s)}{n}\log p_{ij}^{(s)}.$$

При $n \to \infty$ по усиленному закону больших чисел (у. з. б. ч.)

$$\frac{N(\alpha)}{n} \to \alpha, \quad \frac{N(\beta)}{n} \to \beta, \quad \frac{N(i,\, j;\, s)}{n} \to \alpha\beta^{s-1}\pi_i p_{ij}^{(s)}\alpha,$$

где

$N(\alpha)$ — число неискажённых символов в $\tilde{X}_1^n$,

$N(\beta)$ — число искажённых символов в $\tilde{X}_1^n$,

$N(i,\, j;\, s)$ — число серий символов $i * \ldots * j$ в $\tilde{X}_1^n$ длины $s+1$.

Отсюда следует, что

$$-\frac{1}{n}\log p_n(\tilde{X}_1^n) \to -\alpha\log\alpha - \beta\log\beta - \alpha^2\sum_{i,j}\pi_i\sum_{s\geqslant 1}\beta^{s-1}p_{ij}^{(s)}\log p_{ij}^{(s)},$$

что и требовалось. Согласно ВТШК предельное значение совпадает со скоростью передачи информации зашумлённого источника. □

Задача 1.6.28. Двоичный источник генерирует символы 0 или 1 по следующему правилу:

$$\mathsf{P}(X_t = k \,|\, X_{t-1} = j,\, X_{t-2} = i) = q_r,$$

где k, i, j и r принимают значения 0 или 1, $r = k - i - j \bmod 2$ и $q_0 + q_1 = 1$. Найдите скорость передачи информации этого источника.

Кроме того, выведите скорость передачи информации источника Бернулли, генерирующего символы 0 и 1 с вероятностями q_0 и q_1. Объясните связь между ответами к этим задачам.

Решение. Распишем условные вероятности:

$$\mathsf{P}(X_t = 0 \,|\, X_{t-1} = j,\, X_{t-2} = i) = \begin{cases} q_0, & i = j, \\ q_1, & i \neq j, \end{cases}$$

$$\mathsf{P}(X_t = 1 \,|\, X_{t-1} = j,\, X_{t-2} = i) = \begin{cases} q_1, & i = j, \\ q_0, & i \neq j. \end{cases}$$

Источник является ц. м. д. в. (2) на множестве $\{0,\, 1\}$, т. е. ц. м. д. в. с четырьмя состояниями: $\{00,\, 01,\, 10,\, 11\}$. Матрица переходных вероятностей имеет вид

$$\begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix}\begin{pmatrix} q_0 & q_1 & 0 & 0 \\ 0 & 0 & q_1 & q_0 \\ q_1 & q_0 & 0 & 0 \\ 0 & 0 & q_0 & q_1 \end{pmatrix}.$$

Инвариантное распределение является равномерным:

$$\pi_{00} = \pi_{01} = \pi_{10} = \pi_{11} = \frac{1}{4}.$$

Скорость передачи информации вычисляется стандартным способом:

$$H = -\sum_{\alpha,\beta=0,1} \pi_{\alpha\beta} \sum_{\gamma=0,1} \pi_{\alpha\beta} p_{\alpha\beta,\beta\gamma} \log p_{\alpha\beta,\beta\gamma} =$$
$$= \frac{1}{4} \sum_{\alpha,\beta=0,1} h(q_0, q_1) = -q_0 \log q_0 - q_1 \log q_1. \quad \square$$

Задача 1.6.29. На вход д. к. б. п. подаются буквы 1, 2 и 3. Буква j на выходе принимается как $j-1$ с вероятностью p, как $j+1$ с вероятностью p, и как j с вероятностью $1-2p$. Выходные символы образуют алфавит из цифр от 0 до 4. Найдите вид оптимального входного распределения как функцию p настолько явно, насколько возможно. Вычислите пропускную способность канала в трёх случаях: $p = 0$, $p = 1/3$ и $p = 1/2$.

Решение. Матрица канала имеет вид

$$\begin{matrix} 1 \\ 2 \\ 3 \end{matrix} \begin{pmatrix} p & (1-2p) & p & 0 & 0 \\ 0 & p & (1-2p) & p & 0 \\ 0 & 0 & p & (1-2p) & p \end{pmatrix}$$

Её строки получаются друг из друга перестановками, так что пропускная способность равна

$$C = \max_{P_X} [h(Y) - h(Y|X)] = \bigl(\max_{P_X} h(Y)\bigr) + [2p \log p + (1-2p)\log(1-2p)],$$

где максимум по всем распределениям P_X входных букв применяется только к энтропии выходных символов $h(Y)$.

Далее,

$$h(Y) = -\sum_{y=0}^{4} P_Y(y) \log P_Y(y),$$

где

$$\begin{aligned} P_Y(0) &= P_X(1)p, \\ P_Y(1) &= P_X(1)(1-2p) + P_X(2)p, \\ P_Y(2) &= P_X(1)p + P_X(2)(1-2p) + P_X(3)p, \\ P_Y(3) &= P_X(3)(1-2p) + P_X(2)p, \\ P_Y(4) &= P_X(3)p. \end{aligned} \tag{1.6.32}$$

Симметричный вид формул (1.6.32) подсказывает, что $h(Y)$ будет максимальной, когда $P_X(0) = P_X(2) = q$ и $P_X(1) = 1 - 2q$. Таким образом,

$$\max_{P_X} h(Y) =$$
$$= \max_q [-2qp \log(qp) - 2[q(1-2p) + (1-2q)p] \log[q(1-2q) + (1-2q)p] -$$
$$- [2qp + (1-2q)(1-2p)] \log[2qp + (1-2q)(1-2p)].$$

Оптимальное q находится из уравнения

$$\frac{d}{dq} h(Y) = -2p \log(qp) - 2p - 2(1-4p) \log[q(1-2p) + (1-2q)p] -$$
$$- 2(1-4p) - (2p-2) \log[2qp + (1-2q)(1-2p)] - (2p-2) =$$
$$= 4p - 2p \log(qp) - 2(1-4p) \log[q(1-2p) + (1-2q)p] -$$
$$- 2(1-4p) - 2(p-1) \log[2qp + (1-2q)(1-2p)] = 0.$$

Пропускная способность совершенного канала, свободного от ошибок ($p = 0$), $C = \log 3$ достигается при $P_X(1) = P_X(2) = P_X(3) = 1/3$ (т. е. $q = 1/3$) и $P_Y(1) = P_Y(2) = P_Y(3) = 1/3$, $P_Y(0) = P_Y(4) = 0$.

Вычислим вероятности выходных сигналов при $p = 1/3$:

$$p_Y(0) = p_Y(4) = q/3, \quad p_Y(1) = (1-q)/3, \quad p_Y(2) = 1/3.$$

Здесь

$$h(Y) = -2\frac{q}{3} \log \frac{q}{3} - 2\frac{1-q}{3} \log \frac{1-q}{3} - \frac{1}{3} \log \frac{1}{3},$$

и $q = 1/2$ — это решение уравнения

$$\frac{dh(Y)}{dq} = -\frac{2}{3} \log \frac{q}{3} - \frac{2}{3} + \frac{2}{3} \log \frac{1-q}{3} + \frac{2}{3} = 0$$

т. е.

$$P_X(1) = P_X(3) = 1/2, \quad P_X(2) = 0,$$
$$P_Y(0) = P_Y(1) = P_Y(3) = P_Y(4) = 1/6, \quad P_Y(2) = 1/3.$$

Условная энтропия имеет вид $h(Y|X) = \log 3$. Отсюда находим пропускную способность

$$C = -\frac{2}{3} \log \frac{1}{6} - \frac{1}{3} \log \frac{1}{3} - \log 3 = \frac{2}{3}.$$

Наконец, при $p = 1/2$ имеем $h(Y|X) = 1$ и

$$P_Y(0) = P_Y(4) = \frac{q}{3}, \quad P_Y(1) = P_Y(3) = \frac{1-2q}{2}, \quad P_Y(2) = q.$$

Энтропия выходных символов равна

$$h(Y) = -q\log\frac{q}{2} - \frac{1-2q}{2}\log\frac{1-2q}{2} - q\log q = q - 2q\log q - \frac{1-2q}{2}\log\frac{1-2q}{2}$$

и достигает максимального значения при $q = 1/6$, т. е.

$$P_X(1) = P_X(2) = \frac{1}{6}, \quad P_X(2) = \frac{2}{3},$$
$$P_Y(0) = P_Y(4) = \frac{1}{12}, \quad P_Y(1) = P_Y(3) = \frac{1}{3}, \quad P_Y(2) = \frac{1}{6}.$$

В этом случае пропускная способность имеет вид $C = \log 3 - \frac{1}{2}$. □

Задача 1.6.30. Д. к. б. п. производит на выходе с. в. Y из неотрицательной целочисленной с. в. X на входе по правилу

$$Y = \varepsilon X,$$

где ε не зависит от X, $\mathsf{P}(\varepsilon = 1) = p$, $\mathsf{P}(\varepsilon = 0) = 1 - p$ и входная с. в. подчиняется условию $\mathsf{E}X \leqslant 1$.

Рассматривая входные распределения $\{a_i,\, i = 0,\, 1,\, \ldots\}$ вида $a_i = cd^i$, $i = 1,\, 2\ldots$, найдите оптимальное распределение входной с. в. и выпишите выражение для пропускной способности канала.

Решение. Матрица канала имеет вид

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1-p & p & 0 & \ldots & 0 \\ 1-p & 0 & p & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}.$$

Для входного распределения $q_i = \mathsf{P}(X = i)$ имеем

$$\mathsf{P}(Y = 0) = q_0 + (1-p)(1-q_0) = 1 - p + pq_0,$$
$$\mathsf{P}(Y = i) = pq_i, \quad i \geqslant 1,$$

откуда

$$h(Y) = -(1 - p + pq_0)\log(1 - p + pq_0) - \sum_{i\geqslant 1} pq_i \log(pq_i).$$

Выпишем условную энтропию и взаимную энтропию:

$$h(Y\,|\,X) = (1 - q_0)\eta(p),$$
$$I(Y : X) = -(1 - p + pq_0)\log(1 - p + pq_0) - \sum_{i\geqslant 1} pq_i \log(pq_i) - (1 - q_0)\eta(p).$$

Нам нужно максимизировать взаимную энтропию $I(Y:X)$ по $q_0, q_1, \ldots$ при следующих условиях: $q_i \geqslant 0$, $\sum\limits_i q_i = 1$, $\sum\limits_i i q_i \leqslant 1$. Прежде всего зафиксируем q_0 и максимизируем сумму $-\sum\limits_{i\geqslant 1} pq_i \log(pq_i)$ по q_i, $i \geqslant 1$. По неравенству Гиббса (1.1.24) для всех неотрицательных $a_1, a_2, \ldots$, удовлетворяющих условию $\sum\limits_{i\geqslant 1} a_i = 1 - q_0$, выполняется неравенство

$$-\sum_{i\geqslant 1} q_i \log q_i \leqslant -\sum_{i\geqslant 1} q_i \log a_i, \tag{1.6.33}$$

где равенство достигается только при $q_i \equiv a_i$. Для $a_i = cd^i$, удовлетворяющих условию $\sum\limits_{i\geqslant 1} i a_i = 1$, п. ч. неравенства (1.6.33) равна

$$-(1-q_0)\log c - (\log d)\sum_{i\geqslant 1} i a_i = -(1-q_0)\log c - \log d,$$

так как $\sum\limits_i icd^i = 1$, $cd/(1-d) = 1 - a_0$ и $d = a_0$, $c = (1-a_0)^2/a_0$.

Теперь мы ищем максимум функции

$$f(a_0) = -(1-p+pa_0)\log(1-p+pa_0) - p(1-a_0)\log\frac{(1-a_0)^2}{a_0} - \\ - \log a_0 + (1-a_0)[(1-p)\log(1-p) + p\log p]$$

по $a_0 \in [0, 1]$. Необходимо выполнение двух условий:

$$f'(a_0) = 0 \tag{1.6.34а}$$

и

$$f''(a_0) = \frac{-p^2}{q+pa_0} - \frac{2p}{1-a_0} - \frac{p}{a_0} \leqslant 0. \tag{1.6.34б}$$

Решим уравнение (1.6.34а) численно. Обозначим его корень, для которого выполнено неравенство (1.6.34б), через a_0^-. Тогда для оптимального распределения на входе мы получим следующий ответ:

$$a_i = \begin{cases} a_0^-, & i = 0, \\ (1-a_0^-)^2 (a_0^-)^{i-1}, & i \geqslant 1, \end{cases}$$

а пропускная способность равна $C = f(a_0^-)$. □

Задача 1.6.31. Как известно, двоичный код десятичных цифр кодирует 0 как 0000, 1 как 0001 и т. д. до 9 с кодом 1001, а другие 4-разрядные двоичные строки отброшены. Покажите, что, применяя блочное кодирование, можно снизить длину кодового слова на десятичную цифру с 4 до $1 + \varepsilon$ при любом $\varepsilon > 0$.

Указание. Предположите, что все целые числа равновероятны.

Решение. Код, о котором идёт речь, очевидно, декодируемый (и даже беспрефиксный, как и любой декодируемый код с фиксированной длиной кодового слова). Стандартная процедура блочного кодирования работает со строками из n символов оригинального источника (U_n), оперируя алфавитом $\mathcal{A}$ как буквой из $\mathcal{A}^n$. При данной совместной вероятности $p_n(u_1^{(n)}) = \mathsf{P}(U_1 = i_1, \ldots, U_n = i_n)$ блока в типичном сообщении мы смотрим на двоичную энтропию

$$h^{(n)} = -\sum_{i_1,\ldots,i_n} \mathsf{P}(U_1 = i_1, \ldots, U_n = i_n) \log \mathsf{P}(U_1 = i_1, \ldots, U_n = i_n).$$

Обозначим через $S^{(n)}$ случайную длину слова при блочном кодировании. Минимальная средняя длина кодового слова на букву источника равна $e_n := \dfrac{1}{n}\mathsf{E}S^{(n)}$. По теореме Шеннона для канала без шума 1.1.10 выполнено неравенство

$$\frac{h^{(n)}}{n \log q} \leqslant e_n \leqslant \frac{h^{(n)}}{n \log q} + \frac{1}{n},$$

где q — размер исходного алфавита $\mathcal{A}$. Видно, что $e_n \sim \dfrac{h^{(n)}}{n \log q}$ для больших n. По условию $q = 10$ и

$$h^{(n)} = hn, \quad \text{где } h = \log 10 \text{ (равновероятность)}.$$

Следовательно, минимальную среднюю длину кодового слово можно сделать сколь угодно близкой к 1. □

Задача 1.6.32. Пусть $\{U_t\}$ — процесс, дискретный по времени, со значениями u_t и $\mathsf{P}(\mathbf{u}^{(n)})$ — вероятность появления строки $\mathbf{u}^{(n)} = u_1 \ldots u_n$. Покажите, что если $-\log \mathsf{P}(\mathbf{U}^{(n)})/n$ по вероятности сходится к константе H, то H — скорость передачи информации процесса.

Выпишите формулу для скорости передачи информации H в ц. м. д. в. с m состояниями и вычислите эту скорость для случая, когда матрица переходных вероятностей имеет элементы p_{jk}, где

$$p_{jj} = p, \quad p_{jj+1} = 1 - p, \quad j = 1, \ldots, m-1, \quad p_{m1} = 1 - p.$$

Перенесите результат на ц. м. д. в. с двумя состояниями, в котором переходные вероятности равны p и $1 - p$.

Решение. Для ц. м. д. в. с m состояниями с матрицей переходных вероятностей $P = (p_{ij})$ и инвариантным распределением $\pi = (\pi_i)$ имеем

$$H = -\sum_{i,j} \pi_i p_{ij} \log p_{ij}.$$

Если матрица P неприводима (т. е. имеет единственный сообщающийся класс), то это утверждение верно при любом начальном распределении λ (в этом случае инвариантное распределение единственно).

В качестве примера рассмотрим матрицу переходных вероятностей

$$\begin{pmatrix} p & 1-p & 0 & \dots & 0 \\ 0 & p & 1-p & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1-p & 0 & 0 & \dots & p \end{pmatrix}.$$

Строки матрицы получаются друг из друга перестановками, и каждая из них обладает энтропией $\eta(p)$. Инвариантное распределение единственно и равно $\pi = (1/m, \dots, 1/m)$:

$$\sum_{1 \leqslant i \leqslant m} \frac{1}{m} p_{ij} = \frac{1}{m}(p + 1 - p) = \frac{1}{m}.$$

Поскольку ц. м. д. в. имеет единственный сообщающийся класс,

$$H = \frac{1}{m} \sum_{1 \leqslant i \leqslant m} \eta(p) = \eta(p).$$

При $m = 2$ получаем матрицу $\begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$, инвариантное распределение $\pi = (1/2, 1/2)$, и вновь $H = \eta(p)$. □

Задача 1.6.33. Дайте определение д. с. к. б. п. и найдите его пропускную способность.

Индейский воин посылает дымовые сигналы. Сигнал кодируется клубами дыма различных длин: короткий, средний и длинный. За единицу времени посылается один сигнал. Предполагается, что сигнал правильно воспринимается с вероятностью p, а с вероятностью $1 - p$

1) короткий сигнал воспринимается наблюдателем как средний,

2) средний кажется длинным,

3) длинный сигнал кажется коротким.

Какова максимальная скорость, с которой индеец может надёжно передавать информацию, при условии, что получатель знает используемую систему кодирования?

Разумнее предполагать, что короткий сигнал может быть полностью незамеченным, но вряд ли покажется средним. Какое влияние окажет это предположение на вывод формулы пропускной способности канала?

Решение. Пусть входной алфавит I состоит из m букв, сообщения передаются по д. к. б. п. и на выходе получаются строки, состоящие из

символов алфавита J размера n (включая трудночитаемые). Канал описывается матрицей размера $m \times n$ с элементами p_{ij}, дающими вероятность того, что символ $i \in I$ трансформируется в символ $j \in J$. Строки матрицы представляют собой стохастические n-векторы (распределение вероятностей над J):

$$\begin{pmatrix} p_{11} & \dots & p_{1j} & \dots & p_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{i1} & \dots & p_{ij} & \dots & p_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ p_{m1} & \dots & p_{mj} & \dots & p_{mn} \end{pmatrix}.$$

Канал называется симметричным, если строки матрицы получаются друг из друга перестановками элементов (или, более общим образом, обладают одинаковой энтропией $E = h(p_{i1}, \dots p_{in})\ \forall i \in I$). Канал называется дважды симметричным, если он симметричен и его столбцы получаются друг из друга перестановками (или, более общим образом, имеют одинаковые суммы $\sum\limits_{1 \leqslant i \leqslant m} p_{ij} = m/n\ \forall j \in J$).

Пропускная способность д. с. к. б. п. (точная верхняя граница надёжных скоростей передач) равна

$$C = \max_{P_X} I(X : Y).$$

Здесь максимум ищется по всем распределениям вероятностей $P_X = (P_X(i),\ i \in I)$ входных букв и $I(X : Y)$ — взаимная энтропия между входной и выходной случайными буквами X и Y, связанная с матрицей канала:

$$I(X : Y) = h(Y) - h(Y \,|\, X) = h(X) - h(X \,|\, Y).$$

Для симметричного канала условная энтропия выражается как

$$h(Y \,|\, X) = -\sum_{i,j} P_X(i) p_{ij} \log p_{ij} \equiv E$$

вне зависимости от входного распределения вероятностей $p_X(i)$. Следовательно,

$$C = \bigl(\max_{P_X} h(Y)\bigr) - h(Y \,|\, X),$$

и максимизацию нужно провести только для энтропии выходных символов

$$h(Y) = -\sum_j P_Y(j) \log P_Y(j), \quad \text{где } P_Y(j) = \sum_i P_X(i) p_{ij}.$$

Для дважды симметричного канала задача упрощается: $h(Y)$ достигает максимума на равномерно распределённом входе $P_X^{\mathrm{eq}} = 1/m$, так как в этом

случае P_Y тоже равномерное распределение:

$$P_Y(j) = \frac{1}{m}\sum_i p_{ij} = \frac{1}{n}$$

и $P_Y(j)$ не зависит от $j \in J$. Таким образом, для дважды симметричного канала

$$C = \log n - h(Y\,|\,X).$$

Для примера из условия матрица канала, равная

$$\begin{matrix} 1 \sim \text{короткий} \\ 1 \sim \text{средний} \\ 1 \sim \text{длинный} \end{matrix}\begin{pmatrix} p & 1-p & 0 \\ 0 & p & 1-p \\ 1-p & 0 & p \end{pmatrix},$$

является дважды симметричной. Отсюда следует, что

$$C = \log 3 - \eta(p).$$

В модифицированном примере размер матрицы равен 3×4:

$$\begin{pmatrix} p & 0 & 0 & 1-p \\ 0 & p & 1-p & 0 \\ 1-p & 0 & p & 0 \end{pmatrix};$$

четвёртый столбец соответствует состоянию на выходе «сигнала нет» (ошибка). Матрица не является дважды симметричной. Теперь задача максимизации имеет вид

$$\max\left[-\sum_{j=1}^{4}\left(\sum_{i=1}^{3}P_X(i)p_{ij}\right)\log\left(\sum_{i=1}^{3}P_X(i)p_{ij}\right) - \sum_{i=1}^{3}P_X(i)\sum_{j=1}^{4}p_{ij}\log p_{ij}\right],$$

где $P_X(1)$, $P_X(2)$, $P_X(3) \geqslant 0$ и $\sum\limits_{i=1}^{3} P_X(i) = 1$. Она нуждается в полномасштабном анализе. □

Задача 1.6.34. Неравенство Шеннона (н. э. э., см. формулу (1.5.12)) утверждает, для независимых d-мерных случайных векторов $\mathbf{X}$ и $\mathbf{Y}$ выполнена оценка

$$2^{2h(\mathbf{X}+\mathbf{Y})/d} \geqslant 2^{2h(\mathbf{X})/d} + 2^{2h(\mathbf{Y})/d} \tag{1.6.35}$$

и равенство достигается тогда и только тогда, когда $\mathbf{X}$ и $\mathbf{Y}$ — гауссовы с. в. с пропорциональными матрицами ковариации.

Пусть X — вещественнозначная с. в. с п. р. f_X и конечной дифференциальной энтропией $h(X)$. Предположим, что функция $g\colon \mathbb{R} \to \mathbb{R}$ имеет строго положительную производную на всём $\mathbb{R}$. Покажите, что с. в. $g(X)$ обладает дифференциальной энтропией, удовлетворяющей равенству

$$h(g(X)) = h(X) + \mathsf{E}\log_2 g'(X),$$

в предположении, что $\mathsf{E}\log_2 g'(X)$ конечно.

Пусть Y_1 и Y_2 — независимые, строго положительные с. в. с плотностями. Покажите, что дифференциальная энтропия произведения Y_1Y_2 подчиняется неравенству

$$2^{2h(Y_1Y_2)} \geqslant \alpha_1 2^{2h(Y_1)} + \alpha_2 2^{2h(Y_2)},$$

где $\log_2(\alpha_1) = 2\,\mathsf{E}\log_2 Y_2$ и $\log_2(\alpha_2) = 2\,\mathsf{E}\log_2 Y_1$.

Решение. П. р. с. в. $g(X)$ обладает свойством

$$F_{g(X)}(y) = \mathsf{P}(g(X) \leqslant y) = \mathsf{P}(X \leqslant g^{-1}(y)) = F_X(g^{-1}(y)),$$

т. е. п. р. $f_{g(X)}(y) = \dfrac{dF_{g(X)}(y)}{dy}$ принимает вид

$$f_{g(X)}(y) = f_X\big(g^{-1}(y)\big)\big(g^{-1}(y)\big)' = \frac{f_X\big(g^{-1}(y)\big)}{g'\big(g^{-1}(y)\big)}$$

Таким образом,

$$\begin{aligned} h(g(X)) = -\int f_{g(X)}(y)\log_2 f_{g(X)}(y)dy = \\ = -\int \frac{f_X(g^{-1}(y))}{g'(g^{-1}(y))}\log_2 \frac{f_X(g^{-1}(y))}{g'(g^{-1}(y))}dy = \\ = -\int \frac{f_X(x)}{g'(x)}[\log_2 f_X(x) - \log_2 g'(x)]g'(x)dx = \\ = h(X) + \mathsf{E}[\log_2 g'(X)]. \quad (1.6.36) \end{aligned}$$

При $g(t) = e^t$ получаем

$$\log_2 g'(t) = \log_2 e^t = t\log_2 e.$$

Так что при $Y_i = e^{X_i} = g(X_i)$ из формулы (1.6.36) следует равенство

$$h(e^{X_i}) = h(g(X_i)) = h(X_i) + \mathsf{E}X_i \log_2 e, \quad i = 1, 2, 3,$$

где $X_3 = X_1 + X_2$. Тогда

$$h(Y_1Y_2) = h(e^{X_1+X_2}) = h(X_1 + X_2) + (\mathsf{E}X_1 + \mathsf{E}X_2)\log_2 e.$$

Согласно н. э. э. получаем

$$\begin{aligned} 2^{2h(Y_1Y_2)} = 2^{2h(X_1+X_2)+2(\mathsf{E}X_1+\mathsf{E}X_2)\log_2 e} \geqslant 2^{2(\mathsf{E}X_1+\mathsf{E}X_2)\log_2 e}\big(2^{2h(X_1)} + 2^{2h(X_2)}\big) = \\ = 2^{2\,\mathsf{E}X_2\log_2 e}\big(2^{2[h(X_1)+\mathsf{E}X_1\log_2 e]}\big) + 2^{2\,\mathsf{E}X_1\log_2 e}\big(2^{2[h(X_2)+\mathsf{E}X_2\log_2 e]}\big) = \\ = \alpha_1 2^{2h(Y_1)} + \alpha_2 2^{2h(Y_2)}. \end{aligned}$$

Здесь

$$\log_2 \alpha_1 = 2\,\mathsf{E}X_2\log_2 e = 2\,\mathsf{E}\ln Y_2 \log_2 e = 2\,\mathsf{E}\log_2 Y_2,$$

а $\log_2 \alpha_2 = 2\,\mathsf{E}\log_2 Y_1$. □

Задача 1.6.35. В этом примере мы работаем со следующими функциями, определёнными на $0 < a < b$:

$$G(a,\, b) = \sqrt{ab}, \quad L(a,\, b) = \frac{b-a}{\ln(b/a)}, \quad I(a,\, b) = (b^b/a^a)^{1/(b-a)}.$$

Проверьте, что

$$0 < a < G(a,\, b) < L(a,\, b) < I(a,\, b) < A(a,\, b) = \frac{a+b}{2} < b. \tag{1.6.37}$$

Далее, для $0 < a < b$ определим

$$\Lambda(a,\, b) = L(a,\, b)I(a,\, b)/G^2(a,\, b).$$

Пусть $\mathbf{p} = (p_i)$ и $\mathbf{q} = (q_i)$ — распределения вероятностей с. в. X и Y:

$$\mathsf{P}(X = i) = p_i > 0, \quad \mathsf{P}(Y = i) = q_i,\ i = 1,\, \ldots,\, r, \quad \sum p_i = \sum q_i = 1.$$

Введём обозначения: $m = \min[q_i/p_i]$, $M = \max[q_i/p_i]$, $\mu = \min[p_i]$, $\nu = \max[p_i]$. Докажите следующие неравенства для энтропии $h(X)$ и расстояния Кульбака—Лейблера $D(\mathbf{p} \parallel \mathbf{q})$ (см. т. 2, с. 478):

$$0 \leqslant \log_2 r - h(X) \leqslant \log_2 \Lambda(\mu,\, \nu), \tag{1.6.38}$$

$$0 \leqslant D(\mathbf{p} \parallel \mathbf{q}) \leqslant \log_2 \Lambda(m,\, M). \tag{1.6.39}$$

Решение. Неравенства (1.6.37) остаются в качестве упражнения. При $a \leqslant x_i \leqslant b$ положим $\mathcal{A}(\mathbf{p},\, \mathbf{x}) = \sum p_i x_i$, $\mathcal{G}(\mathbf{p},\, \mathbf{x}) = \prod x_i^{p_i}$. Имеют место следующие неравенства между арифметическим и геометрическим средними:

$$1 \leqslant \frac{\mathcal{A}(\mathbf{p},\, \mathbf{x})}{\mathcal{G}(\mathbf{p},\, \mathbf{x})} \leqslant \Lambda(a,\, b). \tag{1.6.40}$$

Из них следует, что

$$0 \leqslant \ln\Big(\sum p_i x_i\Big) - \sum p_i \ln x_i \leqslant \ln \Lambda(a,\, b).$$

Выбирая $x_i = q_i/p_i$, мы сразу получаем неравенство (1.6.39). Взяв в качестве $\mathbf{q}$ равномерное распределение, получаем неравенство (1.6.38) из формулы (1.6.39), так как

$$\Lambda\Big(\frac{1}{r\nu},\, \frac{1}{r\mu}\Big) = \Lambda\Big(\frac{1}{\nu},\, \frac{1}{\mu}\Big) = \Lambda(\mu,\, \nu).$$

Теперь приведём набросок доказательства неравенств (1.6.40) (подробности можно посмотреть в работе [Si, GK]). Пусть f — выпуклая функция, $p,\, q \geqslant 0$, $p + q = 1$. Тогда для $x_i \in [a,\, b]$ мы имеем

$$0 \leqslant \sum_i p_i f(x_i) - f\Big(\sum p_i x_i\Big) \leqslant \max_p [pf(a) + qf(b) - f(pa + qb)]. \tag{1.6.41}$$

Применяя неравенство (1.6.41) к выпуклой функции $f(x) = -\ln x$, после некоторых вычислений получим, что максимум в формуле (1.6.41) достигается в точке $p_0 = (b - L(a, b))/(b - a)$, $p_0 a + (1 - p_0)b = L(a, b)$ и

$$0 \leqslant \ln \frac{\mathcal{A}(\mathbf{p}, \mathbf{x})}{\mathcal{G}(\mathbf{q}, \mathbf{x})} \leqslant \ln\left(\frac{b-a}{\ln(b/a)}\right) - \ln(ab) + \frac{\ln(b^b/a^a)}{b-a} - 1,$$

что равносильно неравенствам (1.6.40). Наконец, мы докажем неравенство (1.6.41). Запишем $x_i = \lambda_i a + (1 - \lambda_i)b$ для некоторого $\lambda_i \in [0, 1]$. Тогда благодаря выпуклости получаем

$$0 \leqslant \sum p_i f(x_i) - f\Big(\sum p_i x_i\Big) \leqslant$$
$$\leqslant \sum p_i(\lambda_i f(a) + (1 - \lambda_i)f(b)) - f\Big(a\sum p_i\lambda_i + b\sum p_i(1 - \lambda_i)\Big).$$

Обозначая $\sum p_i\lambda_i = p$ и $1 - \sum p_i\lambda_i = q$ и найдя максимум по p, мы получим оценку (1.6.41). □

> В сегодняшнем правовой среде практически невозможно нарушить [код] правил; ... т. е. невозможно нарушить и остаться незамеченным, конечно, на значительное время.
>
> *Бернард Мэдофф* (род. в 1938 г.), американский финансист, осуждённый в 2009 г. на 150 лет по обвинению в мошенничес на сумму в 50 млрд. долл.; из выступлении 20.10.2007 г. на панели «Будущее фондового рынка»

Задача 1.6.36. Пусть f — строго положительная п. р. на $\mathbb{R}$. Определите расстояние Кульбака—Лейблера и докажите, что $D(g \parallel f) \geqslant 0$.

Далее, предположим, что $\int e^x f(x)dx < \infty$ и $\int |x|e^x f(x)dx < \infty$. Докажите, что минимум выражения

$$-\int xg(x)dx + D(g \parallel f) \tag{1.6.42}$$

по всем таким плотностям g, что $\int |x|g(x)dx < \infty$, достигается на единственной плотности $g^* \propto e^x f(x)$, и вычислите этот минимум.

Решение. Расстояние Кульбака—Лейблера $D(g \parallel f)$ определяется соотношением

$$D(g \parallel f) = \int g(x) \ln \frac{g(x)}{f(x)}dx, \quad \text{если} \quad \int g(x)\left|\ln \frac{g(x)}{f(x)}\right|dx < \infty,$$

и

$$D(g \parallel f) = \infty, \quad \text{если} \quad \int g(x)\left|\ln \frac{g(x)}{f(x)}\right|dx = \infty.$$

Оценка $D(g \parallel f) \geqslant 0$ следует из неравенства Гиббса.

Выберем плотность вида $g^*(x) = e^x f(x)/Z$, где $Z = \int e^z f(z)dz$. Положим $W = \int xe^x f(x)dx$, тогда $W/Z = \int xg^*(x)dx$. Далее, запишем

$$D(g^* \parallel f) = \frac{1}{Z}\int e^x f(x)\ln(e^x/Z)dx =$$
$$= \frac{1}{Z}\int e^x f(x)(x - \ln Z)dx = Z^{-1}(W - Z\ln Z) = WZ^{-1} - \ln Z$$

и получим, что

$$-\int xg^*(x)dx + D(g^* \parallel f) = -\ln Z.$$

Это и есть минимум, требуемый в последней части вопроса.

Действительно, для любой такой плотности g, что $\int |x|g(x)dx < \infty$, положим $q(x) = g(x)/f(x)$ и запишем:

$$D(g \parallel g^*) = \int g(x)\ln\frac{g(x)}{g^*(x)}dx = \int g(x)\ln[q(x)e^{-x}Z] =$$
$$= -\int xf(x)q(x)dx + \int f(x)q(x)\ln q(x)dx + \ln Z =$$
$$= -\int xg(x)dx + D(g \parallel f) + \ln Z,$$

следовательно,

$$-\int xg(x)dx + D(g \parallel f) = -\int xg^*(x)dx + D(g^* \parallel f) + D(g \parallel g^*).$$

Поскольку $D(g \parallel g^*) > 0$ за исключением случая $g = g^*$, утверждение доказано. □

Замечание 1.6.37. Свойство минимальности (1.6.42) имеет важные следствия в различных областях, включая статистическую физику, эргодическую теорию и финансовую математику. Мы отсылаем читателя к статье [MCh] за подробностями.

Глава 2

Введение в теорию кодирования

§ 2.1. Пространства Хэмминга. Геометрия кодов. Основные ограничения на размер кода

Лучше решать правильную задачу ошибочным способом, чем ошибочную задачу верным способом.

Ричард Хэмминг (1915–1998), американский математик и программист

Для лучшего понимания при первом чтении этого параграфа, целесообразно представлять себе двоичный случай, когда символы, пересылаемые по каналу, исчерпываются 0 и 1.

Как было отмечено ранее, в случае двоичного симметричного канала без памяти (д. с. к. б. п.) с вероятностью ошибочной передачи символа $p \in (0, 1/2)$ наблюдатель м. п. ищет кодовое слово $\mathbf{x}_*^{(N)}$, имеющее максимальное число знаков, совпадающих с полученным двоичным словом $\mathbf{y}^{(N)}$. Фактически, если получено слово $\mathbf{y}^{(N)}$, декодер м. п. сравнивает вероятности

$$\mathbf{P}(\mathbf{y}^{(N)} \,|\, \mathbf{x}^{(N)}) = p^{\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)})}(1-p)^{N-\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)})} = (1-p)^N \left(\frac{p}{1-p}\right)^{\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)})}$$

для различных двоичных слов $\mathbf{x}^{(N)}$. Здесь

$$\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) = \text{число индексов } i, \text{ при которых } x_i \neq y_i \qquad (2.1.1a)$$

называют *расстоянием Хэмминга* между словами $\mathbf{x}^{(N)} = x_1 \dots x_N$ и $\mathbf{y}^{(N)} = y_1 \dots y_N$. Так как первый множитель $(1-p)^N$ не зависит от $\mathbf{x}^{(N)}$, декодер ищет максимум второго сомножителя, т. е. минимизирует расстояние $\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)})$ (так как $0 < p/(1-p) < 1$ при $p \in (0, 1/2)$). Определение (2.1.1a) можно обобщить на q-ичные строки. Пространство q-ичных строк $\mathcal{H}_{N,q} = \{0, 1, \dots, q-1\}^{\times N}$ (N-я декартова степень множества $J_q = \{0, 1, \dots, q-1\}$) с расстоянием (2.1.1a) называется *q-ичным про-*

странством Хэмминга длины N. Оно состоит из q^N элементов. В двоичном случае $\mathcal{H}_{N,2} = \{0, 1\}^N$.

Важную роль играет расстояние $\delta(\mathbf{x}^{(N)}, \mathbf{0}^{(N)})$ между словами $\mathbf{x}^{(N)} = x_1 \dots x_N$ и $\mathbf{0}^{(N)} = 0 \dots 0$; оно называется *весом слова* $\mathbf{x}^{(N)}$ и обозначается символом $w(\mathbf{x}^{(N)})$:

$$w(\mathbf{x}^{(N)}) = \text{число ненулевых символов в слове } \mathbf{x}^{(N)}. \qquad (2.1.1б)$$

Лемма 2.1.1. *Функция* $\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)})$ *является расстоянием на* $\mathcal{H}_{N,q}$, *т. е.*

1) $0 \leqslant \delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) \leqslant N$ *и* $\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) = 0$ *тогда и только тогда, когда* $\mathbf{x}^{(N)} = \mathbf{y}^{(N)}$,
2) $\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) = \delta(\mathbf{y}^{(N)}, \mathbf{x}^{(N)})$,
3) $\delta(\mathbf{x}^{(N)}, \mathbf{z}^{(N)}) \leqslant \delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) + \delta(\mathbf{y}^{(N)}, \mathbf{z}^{(N)})$ (*неравенство треугольника*).

Доказательство. Первые два утверждения очевидны. Для проверки последнего заметим, что для индекса i, при котором $z_i \neq x_i$, будет выполнено одно из условий: $y_i \neq x_i$, и индекс даёт вклад в $\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)})$, или $z_i \neq y_i$, и индекс даёт вклад в $\delta(\mathbf{y}^{(N)}, \mathbf{z}^{(N)})$. □

С геометрической точки зрения двоичное пространство Хэмминга $\mathcal{H}_{N,2}$ можно представлять себе в виде вершин N-мерного куба. Расстояние Хэмминга здесь интерпретируется как наименьшее число рёбер, по которым нужно пройти для достижения одной вершины из другой. Очень полезно нарисовать соответствующие картинки для относительно небольших значений N (см. рис. 2.1).

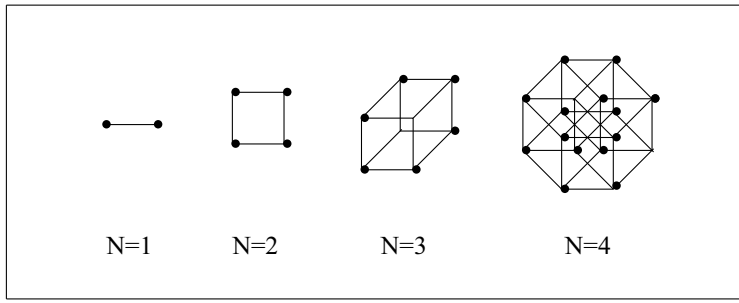


Рис. 2.1

В дальнейшем важную роль будут играть геометрические и алгебраические свойства пространства Хэмминга. Как и в любом метрическом

пространстве, мы можем рассмотреть шар заданного радиуса R с центром в данном слове $\mathbf{x}^{(N)}$

$$\mathcal{B}_{N,q}(\mathbf{x}^{(N)}, R) = \{\mathbf{y}^{(N)} \in \mathcal{H}_{N,q} \colon \delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) \leqslant R\}. \tag{2.1.2}$$

Задача о подсчёте максимального числа непересекающихся шаров, которые можно разместить в данном пространстве Хэмминга, является важной и трудной.

Заметим, что слова можно складывать по модулю q:

$$\mathbf{x}^{(N)} + \mathbf{y}^{(N)} = (x_1 + y_1) \bmod q \ldots (x_N + y_N) \bmod q. \tag{2.1.3а}$$

Это наделяет пространство Хэмминга $\mathcal{H}_{N,q}$ структурой коммутативной группы с нулевым кодовым словом $\mathbf{0}^{(N)} = 0 \ldots 0$ в качестве нуля группы. (Слова можно также и перемножать, что создаёт довольно мощный аппарат; см. ниже.)

При $q = 2$ мы имеем дело с двухточечным кодовым алфавитом $\{0, 1\}$, который является двухэлементным полем $\mathbb{F}_2$ со следующей арифметикой: $0 + 0 = 1 + 1 = 0 \cdot 1 = 1 \cdot 0 = 0$, $0 + 1 = 1 + 0 = 1 \cdot 1 = 1$. (Напомним, что поле — это множество с двумя коммутативными операциями: сложением и умножением, удовлетворяющими стандартным аксиомам ассоциативности и дистрибутивности.) Таким образом, каждая точка в двоичном пространстве Хэмминга $\mathcal{H}_{N,2}$ противоположна сама себе: $\mathbf{x}^{(N)} + \mathbf{y}^{(N)} = \mathbf{0}^{(N)}$ тогда и только тогда, когда $\mathbf{x}^{(N)} = \mathbf{y}^{(N)}$. Иными словами, $\mathcal{H}_{N,2}$ — линейное пространство над полем коэффициентов $\mathbb{F}_2$ с умножением: $1 \cdot \mathbf{x}^{(N)} = \mathbf{x}^{(N)}$ и $0 \cdot \mathbf{x}^{(N)} = \mathbf{0}^{(N)}$.

Рассмотрим также q-ичные слова, которые складываются посимвольно по модулю q.

Лемма 2.1.2. *Расстояние Хэмминга на пространстве $\mathcal{H}_{N,q}$ инвариантно относительно сдвигов по группе*:

$$\delta(\mathbf{x}^{(N)} + \mathbf{z}^{(N)}, \mathbf{y}^{(N)} + \mathbf{z}^{(N)}) = \delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}). \tag{2.1.3б}$$

Доказательство. Для любых $i = 1, \ldots, N$ и $x_i, y_i, z_i \in \{0, 1, \ldots, q-1\}$ цифры $x_i + z_i \bmod q$ и $y_i + z_i \bmod q$ находятся в том же отношении ($=$ или $\neq$), что и цифры x_i и y_i. □

Код отождествляется с множеством кодовых слов $\mathcal{X}_N \subset \mathcal{H}_{N,q}$. Это означает, что мы игнорируем порядок кодовых слов (что соответствует предположению о равномерной распределённости сообщений источника). Остаётся предположение о том, что код известен как отправителю, так и получателю. Теоремы Шеннона о кодировании гарантируют, что при подходящих условиях существуют асимптотически хорошие коды, достигающие предела, установленного скоростью передачи информации источника и пропускной способностью канала. Более того, вторая теорема Шеннона

показывает, что почти все коды асимптотически хорошие. Практическая ценность этих фактов ограничена: хотелось бы не просто знать о существовании хорошего кода, но и иметь его в явном виде. Кроме того, хочется обладать кодом, позволяющим быстрое кодирование и декодирование и максимизирующим скорость передачи информации.

Итак, предположим, что источник генерирует двоичные строки $\mathbf{u}^{(n)} = u_1 \dots u_n$, $u_i = 0, 1$. Чтобы получить вероятность ошибки, стремящуюся к нулю при $n \to \infty$, следует кодировать слова $\mathbf{u}^{(n)}$ бóльшими кодовыми словами $\mathbf{x}^{(N)} \in \mathcal{H}_{N,2}$, где $N \sim R^{-1}n$ и $0 < R < 1$. Слово $\mathbf{x}^{(N)}$ затем посылается по каналу и трансформируется в другое слово $\mathbf{y}^{(N)} \in \mathcal{H}_{N,2}$. Возникающую ошибку удобно представлять разностью двух слов: $\mathbf{e}^{(N)} = \mathbf{y}^{(N)} - \mathbf{x}^{(N)} = \mathbf{y}^{(N)} + \mathbf{x}^{(N)}$, или в эквивалентной записи $\mathbf{y}^{(N)} = \mathbf{x}^{(N)} + \mathbf{e}^{(N)}$ в смысле формулы (2.1.3а). Таким образом, чем больше цифр 1 появится в слове $\mathbf{e}^{(N)}$, тем больше символов искажено в канале. Правило декодирования м. п. производит «гипотетическое» кодовое слово $\mathbf{x}_*^{(N)}$, которое может совпадать или не совпадать со словом $\mathbf{x}^{(N)}$, после чего восстанавливается строка $\mathbf{u}_*^{(n)}$. Когда правило кодирования является вложением, последняя операция (теоретически) простая: мы просто обращаем отображение $\mathbf{u}^{(n)} \to \mathbf{x}^{(N)}$. Интуитивно код можно назвать «хорошим», если он позволяет получателю исправить ошибочную строку $\mathbf{e}^{(N)}$, по крайней мере когда слово $\mathbf{e}^{(N)}$ содержит «не слишком много» ненулевых символов.

В случае двоичного симметричного канала без памяти (д. с. к. б. п.) с вероятностью ошибки $p < 1/2$ декодер м. п. выбирает кодовое слово, $\mathbf{x}_*^{(N)}$, приводящее к слову $\mathbf{e}^{(N)}$ с минимальным количеством единичных цифр. В геометрических терминах

$$\mathbf{x}_*^{(N)} \in \mathcal{X}_N \text{— кодовое слово, ближайшее к } \mathbf{y}^{(N)} \text{ по расстоянию Хэмминга.} \tag{2.1.4}$$

Такое же правило применимо и в q-ичном случае: мы ищем кодовое слово, ближайшее к полученной строке. Проблема возникает в случае, когда на минимальном расстоянии от полученной строки лежат несколько кодовых слов. В этом случае мы либо выбираем одно из таких слов произвольно (или случайно, или в связи со смыслом сообщения; это приводит к так называемому списку декодирования), либо, когда требуется высокое качество передачи, отказываемся декодировать полученное слово и просим повторить передачу.

Определение 2.1.3. Число N называется *длиной* двоичного кода $\mathcal{X}_N$, $M := \#\mathcal{X}_N$ — *размером* и $\rho := \dfrac{\log_2 M}{N}$ — *скоростью передачи информации*. Говорят, что *код* $\mathcal{X}_N$ *обнаруживает* D *ошибок*, если, совершив до D изменений в любом кодовом слове, мы не получим другого кодового

слова. Код называется *исправляющим E ошибок*, если, произведя до E изменений в любом кодовом слове $\mathbf{x}^{(N)}$, мы получим слово, остающееся всё ещё (строго) ближе к $\mathbf{x}^{(N)}$, чем к любому другому кодовому слову (т. е. $\mathbf{x}^{(N)}$ — верно угаданное слово по полученному искажённому в соответствии с правилом (2.1.4)). Код имеет *минимальное расстояние* (или просто расстояние) d, если

$$d = \min\bigl[\delta(\mathbf{x}^{(N)}, \mathbf{x}'^{(N)})\colon \mathbf{x}^{(N)}, \mathbf{x}'^{(N)} \in \mathcal{X}_N,\ \mathbf{x}^{(N)} \neq \mathbf{x}'^{(N)}\bigr]. \tag{2.1.5}$$

Минимальное расстояние и скорость передачи информации кода $\mathcal{X}_N$ будут иногда обозначаться символами $d(\mathcal{X}_N)$ и $\rho(\mathcal{X}_N)$ соответственно.

Определение почти дословно переносится на общий случай q-ичного кода $\mathcal{X}_N \subset \mathcal{H}_{N,q}$ со скоростью передачи информации $\rho = \dfrac{\log_q M}{N}$. А именно, код $\mathcal{X}_N$ называют исправляющим E ошибок, если для любых $r = 1, \ldots, E$, $\mathbf{x}^{(N)} \in \mathcal{X}_N$ и $\mathbf{y}^{(N)} \in \mathcal{H}_{N,q}$, удовлетворяющих условию $\delta(\mathbf{x}^{(N)}, \mathbf{y}^{(N)}) = r$ расстояние $\delta(\mathbf{x}'^{(N)}, \mathbf{y}^{(N)}) > r$ для всех таких $\mathbf{x}'^{(N)} \in \mathcal{X}_N$, что $\mathbf{x}'^{(N)} \neq \mathbf{x}^{(N)}$. Иначе говоря, если внести до E ошибок в кодовое слово, то полученная последовательность будет всё ещё ближе к исходному слову, чем к любому другому кодовому слову. С геометрической точки зрения это означает, что шары радиуса E с центрами в кодовых словах не пересекаются:

$$\mathcal{B}_{N,q}(\mathbf{x}^{(N)}, E) \cap \mathcal{B}_{N,q}(\mathbf{x}'^{(N)}, E) = \varnothing\ \forall \mathbf{x}^{(N)}, \mathbf{x}'^{(N)} \in \mathcal{X}_N$$

(см. формулу (2.1.2)). Далее, код $\mathcal{X}_N$ обнаруживает D ошибок, если шар радиуса D с центром в кодовом слове не содержит других кодовых слов. Это равносильно тому, что пересечение $\mathcal{B}_{N,q}(\mathbf{x}^{(N)}, D) \cap \mathcal{X}_N$ состоит из единственной точки $\mathbf{x}^{(N)} \in \mathcal{X}_N$.

Код длины N, размера M и с минимальным расстоянием d называют $[N, M, d]$-кодом. Говоря о $[N, M]$-коде или о $[N, d]$-коде, мы имеем в виду произвольный код длины N и размера M (в первом случае) или длины N и с расстоянием d (во втором). □

Чтобы убедиться, что мы действительно поняли определение, докажем сформулированную выше эквивалентность определений кода, исправляющего E ошибок. Предположим сначала, что шары радиуса E не пересекаются. Тогда, внеся до E изменений в кодовое слово, мы получим слово, которое ещё остаётся в соответствующем шаре и, следовательно, лежит на бóльшем расстоянии от других кодовых слов. Обратно, предположим, что наш код обладает тем свойством, что, сделав до E изменений в кодовом слове, мы не получим слово, которое лежит на том же расстоянии или ближе от других кодовых слов. Тогда каждое слово, полученное изменениями ровно в E цифрах кодового слова, не может попасть в любой другой шар радиуса E. Если число изменений меньше, мы опять не сможем попасть

в другой шар, в противном случае, двигаясь в направлении второго центра, мы рано или поздно создадим слово, расположенное на расстоянии E от исходного кодового слова и на расстоянии, меньшем чем E, от второго, что невозможно. □

Для кода, обнаруживающего D ошибок, минимальное расстояние $d \geqslant D+1$. Более того, код с расстоянием d обнаруживает $d-1$ и исправляет $\left\lfloor \dfrac{d-1}{2} \right\rfloor$ ошибок.

Замечание 2.1.4. Формально определение 2.1.3 означает, что код обнаруживает *по крайней мере* D и исправляет *по крайней мере* E ошибок, и некоторые авторы уточняют этот факт, определяя D и E как максимальные числа с этим свойством. Мы следуем оригинальной традиции, когда способность кодов к обнаружению и исправлению определяется в терминах неравенств, в отличие от равенств, хотя в некоторых конструкциях и примерах будет утверждаться, что в кодах, обнаруживающих D и/или исправляющих E ошибок, эти значения максимальны. □

Определение 2.1.5. В § 2.3 мы систематически изучаем так называемые линейные коды. Линейная структура возникает в пространстве $\mathcal{H}_{N,q}$, когда размер алфавита $q = p^s$, где p — простое, а s — натуральное число. В этом случае алфавит $\{0, 1, \dots, q-1\}$ можно интерпретировать как поле $\mathbb{F}_q$, введя две подходящие операции: сложение и умножение (как мы говорили ранее, сложение — это стандартное сложение по модулю q, см. § 3.1). Когда $s = 1$, т. е. q — простое число, обе операции понимаются как стандартные операции по модулю q. Когда $\mathbb{F}_q$ — поле со сложением $+$ и умножением $\cdot$, множество $\mathcal{H}_{N,q} = \mathbb{F}_q^{\times N}$ наделяется структурой линейного пространства над $\mathbb{F}_q$ с покомпонентным сложением и умножением на «скаляры», порождёнными соответствующими операциями в $\mathbb{F}_q$. А именно, для $\mathbf{x}^{(N)} = x_1 \dots x_N$, $\mathbf{y}^{(N)} = y_1 \dots y_N$ и $\gamma \in \mathbb{F}_q$ имеем

$$\mathbf{x}^{(N)} + \mathbf{y}^{(N)} = (x_1 + y_1) \dots (x_N + y_N), \qquad \gamma \cdot \mathbf{x}^{(N)} = (\gamma \cdot x_1) \dots (\gamma \cdot x_N). \quad (2.1.6a)$$

При $q = p^s$ q-ичный $[N, M, d]$-код $\mathcal{X}_N$ называется *линейным*, если он является линейным подпространством в $\mathcal{H}_{N,q}$, т. е. множество $\mathcal{X}_N$ обладает тем свойством, что с любыми словами $\mathbf{x}^{(N)}, \mathbf{y}^{(N)} \in \mathcal{X}_N$ их сумма $\mathbf{x}^{(N)} + \mathbf{y}^{(N)} \in \mathcal{X}_N$ и $\forall \gamma \in \mathbb{F}_q$ произведение $\gamma \cdot \mathbf{x}_N \in \mathcal{X}_N$. Размер M линейного кода $\mathcal{X}$ выражается как $M = q^k$, где $k = 1, \dots, N$ и задаёт *размерность* кода, т. е. максимальное число линейно независимых кодовых слов. Обозначают размерность так: $k = \dim \mathcal{X}$. Как и в обычной геометрии, если $k = \dim \mathcal{X}$, то в $\mathcal{X}$ существует *базис* размера k, т. е. такой линейно независимый набор кодовых слов $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(k)}$, что любое кодовое слово может быть (однозначно) записано как линейная комбинация $\sum\limits_{1 \leqslant j \leqslant k} a_j \mathbf{x}^{(j)}$,

где $a_j \in \mathbb{F}_q$. (На самом деле если $k = \dim \mathcal{X}$, то любой линейно независимый набор k кодовых слов является базисом в $\mathcal{X}$.) В линейном случае мы говорим о $[N, k, d]$- или $[N, k]$-кодах.

Как следует из определения, линейный $[N, k, d]$-код всегда содержит нулевую строку $\mathbf{0}^{(N)} = 0 \ldots 0$. Более того, благодаря свойству (2.1.3б) минимальное расстояние $d(\mathcal{X}_N)$ в линейном коде $\mathcal{X}$ равно минимальному весу $w(\mathbf{x}^{(N)})$ ненулевого кодового слова $\mathbf{x}^{(N)} \in \mathcal{X}_N$ (см. формулу (2.1.1б)).

Наконец, определим так называемую конъюнкцию (wedge-product) кодовых слов $\mathbf{x}$ и $\mathbf{y}$ как слово $\mathbf{w} = \mathbf{x} \wedge \mathbf{y}$ с компонентами

$$w_i = \min[x_i, y_i], \quad i = 1, \ldots, N. \tag{2.1.6б}$$

□

Простым примером линейного кода служит *код повторений* $\mathcal{R}_N \subset \mathcal{H}_{N,q}$ вида

$$\{\mathbf{x}^{(N)} = x \ldots x \colon x = 0, 1, \ldots, q-1\},$$

обнаруживающий $N-1$ и исправляющий $\left\lfloor \dfrac{N-1}{2} \right\rfloor$ ошибок. Линейный код *проверки на чётность* (parity-check)

$$\{\mathbf{x}^{(N)} = x_1 \ldots x_N \colon x_1 + \ldots + x_N = 0\}$$

обнаруживает единственную ошибку, но не исправляет её.

> Достаточно сложно найти ошибку в коде, когда вы её ищете; это окажется ещё сложнее, если вы предположили, что ваш код свободен от них.
>
> *С. Макконнелл.* Совершенный код, 2-е издание. Майкрософт Пресс, 2004 г.

Заметим, что «объём» шара радиуса R в пространстве Хэмминга $\mathcal{H}_{N,q}$ с центром в точке $\mathbf{z}^{(N)}$ равен

$$v_{N,q}(R) = \#\mathcal{B}_{N,q}(\mathbf{z}^{(N)}, R) = \sum_{k=0}^{R} C_N^k (q-1)^k; \tag{2.1.7}$$

он не зависит от выбора центра $\mathbf{z}^{(N)} \in \mathcal{H}_{N,q}$.

Интересно рассмотреть большие значения N (теоретически $N \to \infty$) и проанализировать такие параметры кода $\mathcal{X}_N$ как скорость передачи информации $\rho(\mathcal{X}) = \dfrac{\log \#\mathcal{X}}{N}$ и расстояние на одну цифру $\bar{d}(\mathcal{X}) = \dfrac{d(\mathcal{X})}{N}$. Наша цель — сфокусировать внимание на «хороших» кодах с большим числом кодовых слов (для увеличения скорости передачи информации) и большим расстоянием (для увеличения способности обнаружения и исправления).

С этой точки зрения очень важно осознать основные ограничения, накладываемые на коды.

Верхняя граница, обычно обозначаемая $M_q^*(N, d)$, — это наибольший размер q-ичного кода длины N и с расстоянием d. Мы начинаем с элементарных фактов: $M_q^*(N, 1) = q^N$, $M_q^*(N, N) = q$, $M_q^*(N, d) \leqslant M_q^*(N-1, d)$ и (в двоичном случае) $-M_2^*(N, 2s) = M_2^*(N-1, 2s-1)$ (лёгкие упражнения).

Действительно, количество кодовых слов не может быть слишком большим, если мы хотим сохранить свойства обнаружения и исправления ошибок. Существуют различные ограничения на параметры кодов, простейшая граница была обнаружена Хэммингом в конце 1940-х гг.

Теорема 2.1.6 (граница Хэмминга). 1. *Если q-ичный код $\mathcal{X}_N$ исправляет E ошибок, то его размер $M = \#\mathcal{X}_N$ удовлетворяет неравенству*

$$M \leqslant q^N / v_{N,q}(E). \tag{2.1.8а}$$

Для линейного $[N, k]$-кода это можно переписать как

$$N - k \geqslant \log_q(v_{N,q}(E)).$$

2. *Соответственно при $E = \lfloor (d-1)/2 \rfloor$ выполняется неравенство*

$$M_q^*(N, d) \leqslant q^N / v_{N,q}(E). \tag{2.1.8б}$$

Доказательство. 1. E-шары с центрами в $\mathbf{x}^{(N)} \in \mathcal{X}_N$ не должны пересекаться. Следовательно, общее число точек, соответствующих кодовым словам, равно произведению $v_{N,q}(E)M$, что не может превышать q^N, числа всех точек пространства Хэмминга $\mathcal{H}_{N,q}$.

2. Аналогично если $\mathcal{X}_N$ — $[N, M, d]$-код, как было замечено выше, для $E = \lfloor (d-1)/2 \rfloor$ шары $\mathcal{B}_{N,q}(\mathbf{x}^{(N)}, E)$, $\mathbf{x}^{(N)} \in \mathcal{X}_N$ не пересекаются. Объём $\#\mathcal{B}_{N,q}(\mathbf{x}^{(N)}, E)$ равен $v_{N,q}(E) = \sum\limits_{k=0}^{E} C_N^k (q-1)^k$ и объединение шаров $\bigcup\limits_{\mathbf{x}^{(N)} \in \mathcal{X}_N} \mathcal{B}_{N,q}(\mathbf{x}^{(N)}, E)$ должно лежать в пространстве $\mathcal{H}_{N,q}$ с числом точек q^N. □

Если вы не работаете над важной проблемой, то маловероятно, что вы сделаете важное открытие.

Ричард Хэмминг (1915–1998), американский математик и программист

Мы видим, что задача поиска хорошего кода является *геометрической*, поскольку «хороший» код $\mathcal{X}_N$, исправляющий E ошибок, должен дать «плотную упаковку» пространства Хэмминга шарами радиуса E. Код

$\mathcal{X}_N$, который даёт оптимальное плотно упаковывающее разбиение, имеет дополнительные преимущества: код не только исправляет ошибки, но никогда не приводит к отказу декодирования. Дадим точное определение.

Определение 2.1.7. Код $\mathcal{X}_N$ размера $\#\mathcal{X}_N = M$, исправляющий E ошибок, называется *совершенным*, если достигается граница Хэмминга

$$M = q^N / v_{N,q}(E).$$

В совершенном коде $\mathcal{X}_N$ любое слово $\mathbf{y}^{(N)} \in \mathcal{H}_{N,q}$ принадлежит (единственному) шару $\mathcal{B}_E(\mathbf{x}^{(N)})$, т. е. у нас всегда есть возможность декодировать $\mathbf{y}^{(N)}$ кодовым словом, что позволяет корректно исправить ошибки, если их количество не превосходит E, и не обязательно корректно, если их больше. Но мы никогда не «зависнем» при декодировании.

Проблема поиска совершенного двоичного кода была решена около 20 лет назад. Такие коды существует только в следующих случаях:

1) $E = 1$: здесь $N = 2^l - 1$, $M = 2^{2^l - 1 - l}$, это так называемые коды Хэмминга;

2) $E = 3$: здесь $N = 23$, $M = 2^{12}$, это так называемый (двоичный) код Голея.

Как коды Хэмминга, так и код Голея обсуждаются позже. Код Голея используется (с некоторыми изменениями) в американской космической программе: уже в 1970-х гг. качество фотографий, закодированных с помощью этого кода и передававшихся от Марса и Венеры, было настолько отличным, что не требовало никакой улучшающей процедуры. На советских (а ранее американских) космических кораблях использовались и другие коды (мы и их позже обсудим): в целом они давали фотографии более низкого качества, и были необходимы дальнейшие манипуляции, основанные на статистических данных о двоичных изображениях.

Если рассмотреть не двоичные коды, то найдётся ещё один совершенный код для трёх символов (тоже названный в честь Голея).

Сейчас мы опишем несколько простых конструкций, создающих новые коды из уже имеющихся.

Пример 2.1.8. Перечислим основные конструкции новых кодов.

1. **Продолжение**: вы добавляете знак x_{N+1} к каждому кодовому слову $\mathbf{x}^{(N)} = x_1 \dots x_N$ из кода $\mathcal{X}_N$ по некоторому правилу. А именно, так называемое *продолжение с контролем чётности* требует, чтобы выполнялось равенство $x_{N+1} + \sum\limits_{j=1}^{N} x_j = 0$ в поле алфавита $\mathbb{F}_q$. Ясно, что продолженный код $\mathcal{X}^+_{N+1}$ имеет тот же размер, что и исходный код $\mathcal{X}_N$, а расстояние $d(\mathcal{X}^+_{N+1})$ равно либо $d(\mathcal{X}_N)$, либо $d(\mathcal{X}_N) + 1$.

2. **Усечение**: отбрасывание символа из кодовых слов $\mathbf{x} \in \mathcal{X}(= \mathcal{X}_N)$. Получающийся код $\mathcal{X}_{N-1}^{-}$ имеет длину $N-1$ и (если $d(\mathcal{X}_N) \geqslant 2$) тот же размер, что и $\mathcal{X}_N$, в то время как $d(\mathcal{X}_{N-1}^{-}) \geqslant d(\mathcal{X}_N) - 1$, если $d(\mathcal{X}_N) \geqslant 2$.

3. **Прореживание**: просто выбрасываются некоторые кодовые слова $\mathbf{x} \in \mathcal{X}_N$. Например в двоичном коде можно удалить все кодовые слова с нечётным количеством ненулевых цифр. Если это проделать с линейным кодом, то получится линейный подкод; в этом случае если расстояние в исходном коде было нечётным, то в новом коде расстояние будет строго бóльшим.

4. **Расширение**: операция, противоположная прореживанию. Например, можно добавить дополнительные строки к каждому двоичному коду $\mathcal{X}_N$. Скажем, если взять N-слово и все единицы в нём заменить нулями и наоборот, то получится дополнительное слово, которое и добавляется. Обозначим продолженный код через $\bar{\mathcal{X}}_N$. Можно проверить, что $d(\bar{\mathcal{X}}_N) = \min[d(\mathcal{X}_N), N - \bar{d}(\mathcal{X}_N)]$, где $\bar{d}(\mathcal{X}_N) = \max[\delta(\mathbf{x}^{(N)}, \mathbf{x}'^{(N)}) \colon \mathbf{x}^{(N)}, \mathbf{x}'^{(N)} \in \mathcal{X}_N]$.

5. **Сокращение**: возьмём все кодовые слова $\mathbf{x}^{(N)} \in \mathcal{X}_N$, у которых на i-м месте стоит 0, и удалим этот знак (сокращая на $x_i = 0$). Таким образом, исходный двоичный линейный $[N, M, d]$-код $\mathcal{X}_N$ сокращается до двоичного линейного кода $\mathcal{X}_{N-1}^{\mathrm{sh},0}(i)$ длины $N-1$, размер которого может быть равен $M/2$ или M, а расстояние больше d или — в тривиальном случае — 0.

6. **Повторение**: повторяем каждое кодовое слово $\mathbf{x}(= \mathbf{x}^{(N)}) \in \mathcal{X}_N$ фиксированное число раз, скажем m, производя сцепленное (Nm)-слово $\mathbf{x}\mathbf{x}\ldots\mathbf{x}$. В результате получим код $\mathcal{X}_{Nm}^{\mathrm{re}}$ длины Nm и с расстоянием $d(\mathcal{X}_{Nm}^{\mathrm{re}}) = md(\mathcal{X}_N)$.

7. **Прямая сумма**: имея два кода $\mathcal{X}_N$ и $\mathcal{X}'_N$ — строим код $\mathcal{X} + \mathcal{X}' = \{\mathbf{x}\mathbf{x}' \colon \mathbf{x} \in \mathcal{X},\ \ \mathbf{x}' \in \mathcal{X}'\}$.

Такие конструкции, как повторение и прямая сумма, не очень эффективны и не популярны в практическом кодировании. (Хотя мы вернёмся к ним в примерах и задачах.) Более эффективной конструкцией является следующая.

8. **Бар-произведение**[1] $(\mathbf{x}|\mathbf{x}+\mathbf{x}')$: для $[N, M, d]$ и $[N, M', d']$-кодов $\mathcal{X}_N$ и $\mathcal{X}'_N$ определим код $\mathcal{X}_N|\mathcal{X}'_N$ длины $2N$ как набор

$$\{\mathbf{x}(\mathbf{x}+\mathbf{x}') \colon \mathbf{x}(= \mathbf{x}^{(N)}) \in \mathcal{X}_N,\ \mathbf{x}'(= \mathbf{x}'^{(N)}) \in \mathcal{X}'_N\}.$$

Иначе говоря, каждое слово в коде $\mathcal{X}\,|\,\mathcal{X}'$ — это сцепление кодового слова из $\mathcal{X}_N$ и его суммы с кодовым словом из $\mathcal{X}'_N$ (формально ни один из кодов $\mathcal{X}$, $\mathcal{X}'$ не предполагается линейным). Код, получающийся в результате,

[1] Bar-product.

обозначается $\mathcal{X}\,|\,\mathcal{X}'$, его размер

$$\#(\mathcal{X}\,|\,\mathcal{X}') = (\#\mathcal{X}_N)(\#\mathcal{X}'_N).$$

Полезное упражнение заключается в проверке равенства

$$d(\mathcal{X}\,|\,\mathcal{X}') = \min[2d(\mathcal{X}_N),\ d(\#\mathcal{X}'_N)].$$

9. **Двойственный код**. Концепция двойственности основывается на скалярном произведении в пространстве $\mathcal{H}_{N,q}$ (с $q = p^s$): для $\mathbf{x} = x_1 \dots x_N$ и $\mathbf{y} = y_1 \dots y_N$ произведение определяется по правилу

$$\langle \mathbf{x}^{(N)} \cdot \mathbf{y}^{(N)} \rangle = x_1 \cdot y_1 + \dots + x_N \cdot y_N;$$

оно является элементом поля $\mathbb{F}_q$. Для линейного $[N, k]$-кода $\mathcal{X}_N$ его *двойственный код* $\mathcal{X}_N^{\perp}$ определяется как линейный $[N, N-k]$-код:

$$\mathcal{X}_N^{\perp} = \{\mathbf{y}^{(N)} \in \mathcal{H}_{N,q} \colon \mathbf{x}^{(N)} \cdot \mathbf{y}^{(N)} = 0\ \forall \mathbf{x}^{(N)} \in \mathcal{X}_N\}. \tag{2.1.9}$$

Ясно, что $(\mathcal{X}_N^{\perp})^{\perp} = \mathcal{X}_N$. Кроме того, $\dim \mathcal{X}_N + \dim \mathcal{X}_N^{\perp} = N$. Код называется *самодвойственным*, если $\mathcal{X}_N^{\perp} = \mathcal{X}_N$. □

Пример 2.1.9. 1. Докажите, что $[N, M, d]$-код $\mathcal{X}_N$ с нечётным расстоянием d можно продолжить до $[N+1, M, d+1]$-кода $\mathcal{X}^+$ с расстоянием $d+1$.

2. Покажите, что E-исправляющий код $\mathcal{X}_N$ можно продолжить до кода $\mathcal{X}^+$, обнаруживающего $2E+1$ ошибку.

3. Покажите, что расстояние совершенного двоичного кода — нечётное число.

Решение. 1. Добавляя цифру x_{N+1} к кодовому слову $\mathbf{x} = x_1 \dots x_N$ $[N, M]$-кода $\mathcal{X}_N$ так, чтобы выполнялось равенство $x_{N+1} = \sum_{j=1}^{N} x_j$, мы получим $[N+1, M]$-код $\mathcal{X}^+$. Если расстояние d кода $\mathcal{X}_N$ было нечётным, то расстояние кода $\mathcal{X}^+$ станет равным $d+1$. Действительно, если пара кодовых слов $\mathbf{x}^{(N)}$, $\mathbf{x}'^{(N)} \in \mathcal{X}$ имела расстояние $\delta(\mathbf{x}, \mathbf{x}') > d$, то продолженные слова $\mathbf{x}_+$ и $\mathbf{x}'_+$ имеют расстояние $\delta(\mathbf{x}_+, \mathbf{x}'_+) > \delta(\mathbf{x}, \mathbf{x}') > d$. В противном случае если $\delta(\mathbf{x}, \mathbf{x}') = d$, то расстояние возрастает: $\delta(\mathbf{x}_+, \mathbf{x}'_+) = d+1$.

2. Расстояние d исправляющего E ошибок кода больше $2E$. Следовательно, продолжение даёт код с расстоянием, превышающим $2E+1$.

3. Для совершенного исправляющего E ошибок кода расстояние не меньше $2E+1$ и поэтому равно $2E+1$. □

Пример 2.1.10. Покажите, что не существует совершенного исправляющего две ошибки кода длины 90 размера 2^{78} над полем $\mathbb{F}_2$.

Решение. Мы могли бы интересоваться существованием совершенного двоичного исправляющего две ошибки кода длины $N = 90$ и размера $M =$

$= 2^{78}$, поскольку

$$v_{90,2}(2) = 1 + 90 + \frac{90 \cdot 89}{2} = 4096 = 2^{12}$$

и

$$M \times v_{90,2}(2) = 2^{78} \cdot 2^{12} = 2^N.$$

Однако такого кода нет. Предположим, что он существует и нулевое слово $\mathbf{0} = 0 \ldots 0$ является кодовым. Расстояние такого кода должно быть равно $d = 5$. Рассмотрим 88 слов с тремя ненулевыми цифрами и единицами на первых двух позициях.

$$1110 \ldots 00, \quad 1101 \ldots 00, \quad \ldots, \quad 1100 \ldots 01. \tag{2.1.10}$$

Каждое из этих слов должно находиться на расстоянии не больше 2 от единственного кодового слова. Например, это кодовое слово для $1110 \ldots 00$ должно содержать 5 ненулевых цифр. Предположим, что оно равно

$$111110 \ldots 00.$$

Это слово находится на расстоянии 2 от двух следующих слов из выбранных нами:

$$11010 \ldots 00 \quad \text{и} \quad 11001 \ldots 00.$$

Продолжая эту конструкцию, мы видим, что любое слово из списка (2.1.10) «притягивается» к кодовому слову с 5 ненулевыми цифрами вместе с двумя другими словами из списка (2.1.10), но 88 не делится на 3. □

Продолжим искать ограничения (границы) на размер кода.

Теорема 2.1.11 (граница Гильберта—Варшамова). *Для любых $q \geqslant 2$ и $d \geqslant 2$ найдётся такой q-ичный $[N, M, q]$-код $\mathcal{X}_{N,q}$, что*

$$M = \#\mathcal{X}_N \geqslant q^N / v_{N,q}(d-1). \tag{2.1.11}$$

Доказательство. Рассмотрим код максимального размера среди кодов с минимальным расстоянием d и длиной N. Тогда любое слово $\mathbf{y}^{(N)} \in \mathcal{H}_{N,q}$ должно отстоять на расстоянии не больше $d-1$ от некоторого кодового слова: в противном случае можно добавить $\mathbf{y}^{(N)}$ к коду, не меняя минимального расстояния. Следовательно, шары радиуса $d-1$ вокруг кодовых слов покрывают всё пространство Хэмминга $\mathcal{H}_{N,q}$, т. е. для кода максимального размера $\mathcal{X}_N^{\max}$ выполняется неравенство

$$(\#\mathcal{X}_N^{\max}) v_{N,q}(d-1) \geqslant q^N. \qquad \square$$

Как уже было сказано, существуют способы построения нового кода из уже имеющегося (или нескольких). Применим усечение и отбросим последнюю цифру x_N в каждом кодовом слове $\mathbf{x}^{(N)}$ исходного кода $\mathcal{X}_N$.

Если код $\mathcal{X}_N$ обладает минимальным расстоянием $d > 1$, то новый код $\mathcal{X}_{N-1}^-$ имеет минимальное расстояние не меньше $d-1$ и тот же размер, что и $\mathcal{X}_N$. Процедура усечения приводит к следующему ограничению.

Теорема 2.1.12 (граница Синглтона). *Любой q-ичный код $\mathcal{X}_N$ с минимальным расстоянием d имеет размер*

$$M = \#\mathcal{X}_N \leqslant M_q^*(N, d) \leqslant q^{N-d+1}. \tag{2.1.12}$$

Доказательство. Как и ранее, произведём усечение $[N, M, d]$-кода $\mathcal{X}_N$, отбросив последний знак у каждого кодового слова $\mathbf{x} \in \mathcal{X}_N$. Расстояние нового $[N-1, M, d^-]$-кода будет $d^- \geqslant d-1$. Повторяя эту процедуру $d-1$ раз, мы получим $[N-d+1, M]$-код того же размера M и с расстоянием не меньше 1. Этот код должен содержаться в пространстве Хэмминга $\mathcal{H}_{N-d+1,q}$ с $\#\mathcal{H}_{N-d+1,q} = q^{N-d+1}$, откуда следует требуемое утверждение. □

Как и в случае границы Хэмминга, равенство в границе Синглтона представляет особый интерес.

Определение 2.1.13. q-ичный линейный $[N, k, d]$-код называется *кодом с максимальным достижимым расстоянием* (м. д. р.), если на нём достигается равенство в границе Синглтона

$$d = N - k + 1. \tag{2.1.13}$$

□

Далее мы увидим, что, подобно совершенным кодам, семейство м. д. р.-кодов довольно «тонкое».

Следствие 2.1.14. *Если $M_q^*(N, d)$ — максимальный размер кода $\mathcal{X}_N$ с минимальным расстоянием d, то*

$$\frac{q^N}{v_{N,q}(d-1)} \leqslant M_q^*(N, d) \leqslant \min\left[\frac{q^N}{v_{N,q}(\lfloor (d-1)/2 \rfloor)}, q^{N-d+1}\right]. \tag{2.1.14}$$

Далее мы будем опускать индекс N, если это не приведёт к недоразумениям. Верхняя граница в неравенстве (2.1.14) становится слишком грубой при $d \sim N/2$. Скажем, в случае двоичного $[N, M, d]$-кода с $N = 10$ и $d = 5$ (2.1.14) даёт ограничение $M_2^*(10, 5) \leqslant 18$, когда фактически не существует кодов с $M > 13$, но есть код с $M = 12$. Вот кодовые слова последнего:

$$\begin{gathered}0000000000,\ 1111100000,\ 1001011010,\ 0100110110,\\ 1100001101,\ 0011010101,\ 0010011011,\ 1110010011,\\ 1001100111,\ 1010111100,\ 0111001110,\ 0101111001.\end{gathered}$$

Нижняя граница в этом случае даёт число 2 (так как $2^{10}/v_{10,2}(4) = 2{,}6585$) и это тоже далеко не идеально. (Более эффективные границы будут получены ниже.)

Теорема 2.1.15 (граница Плоткина). *Размер M двоичного кода длины N и с расстоянием d при условии $N < 2d$ подчиняется неравенству*

$$M = \#\mathcal{X} \leqslant 2\left\lfloor \frac{d}{2d-N} \right\rfloor. \tag{2.1.15}$$

Доказательство. Минимальное расстояние не может превышать среднее расстояние, т. е.

$$M(M-1)d \leqslant \sum_{\mathbf{x}\in\mathcal{X}} \sum_{\mathbf{x}'\in\mathcal{X}} \delta(\mathbf{x}, \mathbf{x}').$$

С другой стороны, выпишем код $\mathcal{X}$ как $M \times N$-матрицу с кодовыми словами в качестве строк. Предположим, что столбец i этой матрицы содержит s_i нулей и $M - s_i$ единиц. Тогда

$$\sum_{\mathbf{x}\in\mathcal{X}} \sum_{\mathbf{x}'\in\mathcal{X}} \delta(\mathbf{x}, \mathbf{x}') \leqslant 2\sum_{i=1}^{N} s_i(M - s_i). \tag{2.1.16}$$

Если M чётное, то п. ч. последнего неравенства становится максимальной при $s_i = M/2$, откуда получаем

$$M(M-1)d \leqslant \frac{1}{2}NM^2, \quad \text{или} \quad M \leqslant \frac{2d}{2d-N}.$$

При чётном M из этого следует, что

$$M \leqslant 2\left\lfloor \frac{d}{2d-N} \right\rfloor.$$

Если M нечётно, то п. ч. формулы (2.1.16) не превосходит $N(M^2-1)/2$, т. е.

$$M \leqslant \frac{N}{2d-N} = \frac{2d}{2d-N} - 1.$$

Отсюда вновь следует, что

$$M \leqslant \left\lfloor \frac{2d}{2d-N} \right\rfloor - 1 \leqslant 2\left\lfloor \frac{d}{2d-N} \right\rfloor,$$

поскольку $\lfloor 2x \rfloor \leqslant 2\lfloor x \rfloor + 1 \ \forall x > 0$. □

Теорема 2.1.16. *Пусть $M_2^*(N, d)$ — максимальный размер двоичного $[N, d]$-кода. Тогда для любых N и d выполнены равенства*

$$M_2^*(N, 2d-1) = M_2^*(N+1, 2d), \tag{2.1.17}$$

$$2M_2^*(N-1, d) = M_2^*(N, d). \tag{2.1.18}$$

Доказательство. Пусть $\mathcal{X}$ — код длины N с расстоянием $2d-1$ размера $M_2^*(N, 2d-1)$. Возьмём его продолжение с контролем чётности $\mathcal{X}^+$, т. е. добавим знак x_{N+1} к каждому кодовому слову $\mathbf{x} = x_1 \dots x_N$, так что $\sum\limits_{i=1}^{N+1} x_i = 0$. Тогда $\mathcal{X}^+$ — код длины $N+1$ того же размера $M_2^*(N, 2d-1)$ с расстоянием $2d$. Следовательно,

$$M_2^*(N, 2d-1) \leqslant M_2^*(N+1, 2d).$$

Аналогично удаление последнего символа приводит к обратному неравенству

$$M_2^*(N, 2d-1) \geqslant M_2^*(N+1, 2d).$$

Равенство (2.1.17) доказано.

Возьмём $[N, d]$-код и разобьём кодовые слова на два класса: заканчивающиеся нулём и единицей. Поскольку один из классов содержит по крайней мере половину всех слов, то равенство (2.1.18) доказано. □

Следствие 2.1.17. *Если чётное d подчиняется неравенству $2d > N$, то*

$$M_2^*(N, d) \leqslant 2\left\lfloor \frac{d}{2d-N} \right\rfloor \tag{2.1.19}$$

и

$$M_2^*(2d, d) \leqslant 4d. \tag{2.1.20}$$

Если d нечётно и $2d+1 > N$, то

$$M_2^*(N, d) \leqslant 2\left\lfloor \frac{d+1}{2d+1-N} \right\rfloor \tag{2.1.21}$$

и

$$M_2^*(2d+1, d) \leqslant 4d+4. \tag{2.1.22}$$

Доказательство. Неравенство (2.1.19) следует из (2.1.15), а неравенство (2.1.20) — из (2.1.18) и (2.1.19): если $d = 2d'$, то

$$M_2^*(4d', 2d') = 2M_2^*(4d'-1, 2d') \leqslant 8d' = 4d.$$

Далее, неравенство (2.1.21) следует из (2.1.17):

$$M_2^*(N, d) = M_2^*(N+1, d+1) \leqslant 2\left\lfloor \frac{d+1}{2d+1-N} \right\rfloor.$$

Наконец, неравенство (2.1.22) следует из (2.1.17) и (2.1.20). □

Пример 2.1.18. Докажите границу Плоткина для q-ичного кода

$$M_q^*(N, d) \leqslant \left\lfloor d \Big/ \left(d - N\frac{q-1}{q}\right) \right\rfloor. \tag{2.1.23}$$

Решение. Минимальное расстояние q-ичного $[N, M, d]$-кода d не превосходит его среднего расстояния

$$d \leqslant \frac{1}{M(M-1)} S, \quad \text{где} \quad S = \sum_{\mathbf{x} \in \mathcal{X}} \sum_{\mathbf{x}' \in \mathcal{X}} \delta(\mathbf{x}, \mathbf{x}').$$

Как и раньше обозначим символом k_{ij} количество букв $j \in \{0, \ldots, q-1\}$ на i-й позиции во всех кодовых словах из $\mathcal{X}$, $i = 1, \ldots, N$. Тогда, очевидно, $\sum\limits_{j=0}^{q-1} k_{ij} = M$ и вклад i-й позиции в S равен

$$\sum_{j=0}^{q-1} k_{ij}(M - k_{ij}) = M^2 - \sum_{j=0}^{q-1} k_{ij}^2 \leqslant M^2 - \frac{M^2}{q},$$

поскольку квадратичная функция $(u_1, \ldots, u_q) \mapsto \sum\limits_{j=1}^{q} u_j^2$ достигает своего минимума на множестве $\left\{\mathbf{u} = u_1 \ldots u_q \colon u_j \geqslant 0, \ \sum u_j = M\right\}$ в точке $u_1 = \ldots = u_q = M/q$. Суммируя по всем N позициям, мы получаем

$$M(M-1)d \leqslant \theta M^2 N,$$

где $\theta = (q-1)/q$, что даёт неравенство $M \leqslant d(d - \theta N)^{-1}$. Заканчивается доказательство, как в двоичном случае. □

Существует солидная теория, относящаяся к случаю равенства в границе Плоткина (коды Адамара), но мы не будем обсуждать её в этой книге. Хотелось бы также указать на тот факт, что все границы, установленные до сих пор (Хэмминга, Синглтона, Гильберта—Варшамова и Плоткина), справедливы для кодов, которые не обязательно линейны. Только лишь неравенство Гильберта—Варшамова имеет отношение к линейности: можно доказать, что равенство там может быть достигнуто на линейных кодах (см. теорему 2.3.26).

Пример 2.1.19. Докажите, что исправляющий две ошибки двоичный код длины 10 может иметь не более 12 кодовых слов.

Решение. Расстояние этого кода должно быть не меньше пяти. Предположим, что в нём есть M кодовых слов, и продолжим его до $[11, M]$-кода с расстоянием 6. Граница Плоткина работает следующим образом. Перечислим все кодовые слова продолженного кода в виде строк $M \times 11$ матрицы. Если i-й столбец в ней состоит из s_i нулей и $M - s_i$ единиц, то

$$6(M-1)M \leqslant \sum_{\mathbf{x} \in \mathcal{X}^+} \sum_{\mathbf{x}' \in \mathcal{X}^+} \delta(\mathbf{x}, \mathbf{x}') \leqslant \sum_{i=1}^{11} s_i(M - s_i).$$

П. ч. неравенства не превосходит $(1/2)\cdot 11M^2$, если M чётное, и не превосходит $(1/2)\cdot 11(M^2-1)$, если M нечётное. Следовательно, $M\leqslant 12$. $\square$

Пример 2.1.20 (асимптотика объема двоичного шара). Пусть $q=2$ и $\tau\in(0,\,1/2)$. Тогда

$$\lim_{N\to\infty}\frac{1}{N}\log v_{N,2}(\lfloor\tau N\rfloor)=\lim_{N\to\infty}\frac{1}{N}\log v_{N,2}(\lceil\tau N\rceil)=\eta(\tau), \tag{2.1.24}$$

где $\eta(\tau)=-\tau\log_2\tau-(1-\tau)\log_2(1-\tau)$ (см. формулу (1.2.2a)).

Решение. Заметим, что при $R=\lceil\tau N\rceil$ последний член суммы

$$v_{N,2}(R)=\sum_{i=0}^{R}C_N^i,\qquad R=\lceil\tau N\rceil$$

максимален. Действительно, отношение двух соседних членов равно

$$\frac{C_N^{i+1}}{C_N^i}=\frac{N-1}{i+1},$$

и эта величина ограничена снизу 1 при $0\leqslant i\leqslant R$. Следовательно,

$$C_N^R\leqslant v_{N,2}(R)\leqslant(R+1)C_N^R.$$

Воспользовавшись формулой Стирлинга ($N!\sim N^{N+1/2}e^{-N}\sqrt{2\pi}$), получим

$$\log C_N^R=-(N-R)\log\frac{N-R}{N}-R\log\frac{R}{N}+O(\log N) \tag{2.1.25}$$

и

$$\eta\Big(\frac{R}{N}\Big)+\frac{O(\log N)}{N}\leqslant\frac{\log v_{N,2}(R)}{N}\leqslant\frac{1}{N}\log(R+1)+\eta\Big(\frac{R}{N}\Big)+\frac{O(\log N)}{N}.$$

Переходя к пределу при $R/N\to\tau$, получим требуемое утверждение. Случай, когда $R=\lfloor\tau N\rfloor$ рассматривается аналогичным образом. $\square$

Пример 2.1.20 полезен при изучении асимптотики следующего выражения:

$$\alpha(N,\,\tau)=\frac{1}{N}\log M_2^*(N,\,\lceil\tau N\rceil), \tag{2.1.26}$$

т. е. скорости передачи информации кода максимального размера, обнаруживающего $\sim\tau N/2$ ошибок (линейной части общего числа знаков N). Положим

$$\underline{a}(\tau):=\liminf_{N\to\infty}\alpha(N,\,\tau)\leqslant\limsup_{N\to\infty}\alpha(N,\,\tau)=:\overline{a}(\tau). \tag{2.1.27}$$

Для этих пределов справедлива следующая теорема.

Теорема 2.1.21. *Для двоичного кода выполнены следующие асимптотические неравенства*:

$$1)\ \overline{a}(\tau) \leqslant 1 - \eta(\tau/2), \quad 0 \leqslant \tau \leqslant 1/2 \quad (\textit{Хэмминг}), \tag{2.1.28}$$

$$2)\ \overline{a}(\tau) \leqslant 1 - \tau, \quad 0 \leqslant \tau \leqslant 1/2 \quad (\textit{Синглетон}), \tag{2.1.29}$$

$$3)\ \underline{a}(\tau) \geqslant 1 - \eta(\tau), \quad 0 \leqslant \tau \leqslant 1/2 \quad (\textit{Гильберт—Варшамов}), \tag{2.1.30}$$

$$4)\ \overline{a}(\tau) = 0, \quad 1/2 \leqslant \tau \leqslant 1 \quad (\textit{Плоткин}). \tag{2.1.31}$$

Опираясь на более тонкие ограничения (*в том числе и границу Плоткина в задаче* 2.6.10) *мы покажем*, *что*

$$4')\quad \overline{a}(\tau) \leqslant 1 - 2\tau, \quad 0 \leqslant \tau \leqslant 1/2. \tag{2.1.32}$$

Доказательство теоремы 2.1.21 основано на прямой проверке перечисленных неравенств; для границ Хэмминга и Гильберта—Варшамова детали приведены в примере 2.1.22.

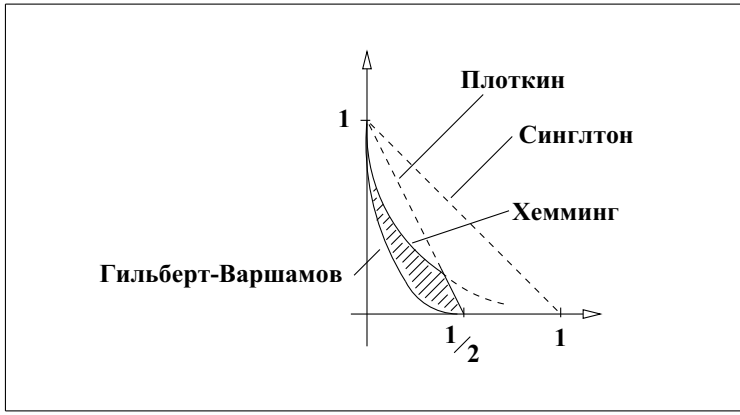


Рис. 2.2

Рисунок 2.2 показывает поведение установленных границ. «Хорошими» последовательностями кодов являются те, для которых пара $(\tau,\ \alpha(N,\ \lceil \tau N \rceil))$ при больших N попадает в область между кривыми, указывающими асимптотические границы. В частности, «хорошие» коды должны «лежать» выше кривой, соответствующей границе Гильберта—Варшамова. Построение такой последовательности относится к трудным проблемам: первые примеры, обеспечивающие асимптотику Гильберта—Варшамова, появились в 1973 г. (коды Гоппы, основанные на идеях из алгебраической геометрии). Все остальные семейства кодов, обсуждаемые в этой книге (за

исключением кодов Юстенсена), лежат ниже кривой Гильберта—Варшамова и дают $\alpha(\tau) = 0$, хотя эти коды демонстрируют весьма впечатляющие свойства для конкретных значений N, M и d.

Что касается верхней границы, неравенства Хэмминга и Плоткина дополняют друг друга, в то время как граница Синглтона оказывается асимптотически пренебрежимой (хотя и очень важной для конкретных значений N, M и d). Существует ещё около дюжины других различных верхних оценок; некоторые из них будут обсуждаться в этой книге.

Граница Гильберта—Варшамова не обязательно является оптимальной. До 1987 г. не было известно лучшей нижней границы (и в случае двоичного кодирования всё ещё не известно лучшей нижней границы). Однако если алфавит насчитывает $q \geqslant 49$ символов, где $q = p^{2m}$ и $p \geqslant 7$ — простое число, то существует конструкция, основанная на алгебраической геометрии, которая даёт лучшую нижнюю границу и примеры линейных кодов, которые асимптотически при $N \to \infty$ лежат выше границы Гильберта—Варшамова [TVZ]. Более того, конструкция, предложенная в работе [TVZ], имеет полиномиальную сложность. Далее, недавно были предложены две новые границы: а) граница Элки при $q = p^{2m+1}$, см. [El], и б) граница Хинга [X]. Используя различные неэлементарные конструкции, границу Гильберта—Варшамова можно улучшить и для некоторых других алфавитов.

Пример 2.1.22. Докажите неравенства (2.1.28) и (2.1.30) (т. е. часть теоремы 2.1.21, относящуюся к асимптотике границ Хэмминга и Гильберта—Варшамова).

Решение. Воспользуемся соотношением (2.1.14), которое относится к границам Хэмминга и Гильберта—Варшамова:

$$2^N / v_{N,2}(d-1) \leqslant M_2^*(N, d) \leqslant 2^N / v_{N,2}(\lfloor (d-1)/2 \rfloor). \tag{2.1.33}$$

Нижняя граница для объёма Хэмминга тривиальна:

$$v_{N,2}(\lfloor (d-1)/2 \rfloor) \geqslant C_N^{\lfloor (d-1)/2 \rfloor}.$$

Для доказательства верхней границы заметим, что при $d/N \leqslant \tau < 1/2$ справедливы оценки

$$v_{N,2}(d-1) \leqslant \sum_{i=0}^{d-1} \left(\frac{d-1}{N-d+1} \right)^{d-1-i} C_N^{d-1} \leqslant$$

$$\leqslant \sum_{i=0}^{d-1} \left(\frac{\tau}{1-\tau} \right)^{d-1-i} C_N^{d-1} \leqslant \frac{1-\tau}{1-2\tau} C_N^{d-1}.$$

Здесь использовано неравенство $C_N^i \leqslant \left(\frac{d-1}{N-d+1} \right)^{d-1-i} C_N^{d-1}$ при $i \leqslant d-1$.

Тогда скорость передачи информации $\log M_2^*(N, d)/N$ удовлетворяет неравенствам

$$1 - \frac{1}{N}\log\left[\frac{1-\tau}{1-2\tau}C_N^{d-1}\right] \leqslant \frac{1}{N}\log M_2^*(N, d) \leqslant 1 - \frac{1}{N}\log C_N^{\lfloor (d-1)/2\rfloor}.$$

По формуле Стирлинга при $N \to \infty$ имеем

$$\frac{1}{N}\log C_N^{\lfloor (d-1)/2\rfloor} \to \eta(\tau/2), \qquad \frac{1}{N}\log C_N^{d-1} \to \eta(\tau).$$

Отсюда немедленно следуют границы (2.1.28) и (2.1.30). □

Рассмотрим теперь случай общего q-ичного алфавита.

Пример 2.1.23. Положим $\theta := (q-1)/q$. Подправив рассуждения в предыдущем примере, докажите, что для любых $q \geqslant 2$ и $\tau \in (0, \theta)$ объём q-ичного шара Хэмминга обладает следующей логарифмической асимптотикой:

$$\lim_{N\to\infty}\frac{1}{N}\log_q v_{N,q}(\lfloor \tau N\rfloor) = \lim_{N\to\infty}\frac{1}{N}\log_q v_{N,q}(\lceil \tau N\rceil) = \eta^{(q)}(\tau) + \tau\varkappa, \quad (2.1.34)$$

где

$$\eta^{(q)}(\tau) := -\tau\log_q\tau - (1-\tau)\log_q(1-\tau), \qquad \varkappa := \log_q(q-1). \quad (2.1.35)$$

Далее, как и в формуле (2.1.26), введём

$$\alpha^{(q)}(N, \tau) = \frac{1}{N}M_q^*(N, \lceil \tau N\rceil) \quad (2.1.36)$$

и пределы

$$\underline{a}^{(q)}(\tau) := \liminf_{N\to\infty}\alpha^{(q)}(N, \tau) \leqslant \limsup_{N\to\infty}\alpha^{(q)}(N, \tau) =: \overline{a}^{(q)}(\tau). \quad (2.1.37)$$

Теорема 2.1.24. *Для всех* $\tau\theta > 0$ *имеют место неравенства*:

1) $\overline{a}^{(q)}(\tau) \leqslant 1 - \eta^{(q)}(\tau/2) - \varkappa\tau/2$ (*Хэмминг*), (2.1.38)

2) $\overline{a}^{(q)}(\tau) \leqslant 1 - \tau$ (*Синглетон*), (2.1.39)

3) $\underline{a}^{(q)}(\tau) \geqslant 1 - \eta^{(q)}(\tau) - \varkappa\tau$ (*Гильберт—Варшамов*), (2.1.40)

4) $\overline{a}^{(q)}(\tau) \leqslant \max[1 - \tau/\theta, 0]$ (*Плоткин*). (2.1.41)

Естественно, минимум правых частей неравенств (2.1.38), (2.1.39) и (2.1.41) является лучшей из этих трёх верхних границ. Мы оставляем доказательство теоремы 2.1.24 в качестве упражнения на повторение рассуждений из примера 2.1.22.

Пример 2.1.25. Используя рассуждения из примера 2.1.22, докажите неравенства (2.1.38) и (2.1.40).

Эдгар Нельсон Гильберт (1923–2011) — ветеран теории кодирования и информации. В течение многих лет он работал в Центре математики и статистики в Bell Telephone Laboratories. Его статьи, содержащие границы, появились в 1952 г., за пять лет до работы Варшамова.

Ром Рубенович Варшамов (1927–1999) был армянским математиком. Родился в Тбилиси (Грузия) и закончил Тбилисский государственный университет. Он работал в «ящике» (т. е. секретном научно-исследовательском институте) в Москве, когда открыл свою границу в 1957 г. (не зная работ Гильберта). Его доклад на эту тему был оценён Колмогоровым, предложившим Варшамову представить статью для публикации, которую Колмогорову предстоит рекомендовать в «Доклады Академии наук». Однако Варшамов было слишком скромным, чтобы отнимать время у Колмогорова, и не стал оформлять свой доклад в виде статьи: согласно легенде, это сделал, наконец, сам Колмогоров. (Есть и другие примеры, когда Колмогоров, видя большой потенциал в результатах других математиков (например, своих учеников), писал бóльшую часть или даже всю статью за фактического автора. Как правило, такие работы приобретали большую известность.)

Специалист по теории кодирования делает это без ограничений.

Специалист по теории кодирования может сделать это, только чувствуя свободу от всех границ.

(Из серии «Как они делают это».)

§ 2.2. Геометрическое доказательство второй теоремы Шеннона о кодировании. Тонкие границы на размер кода

Специалист по теории информации не может делать это без шума.

(Из серии «Как они делают это».)

В этом параграфе даются альтернативные доказательства обеих частей второй теоремы Шеннона о кодировании (ВТШК, или теоремы Шеннона для канала с шумом; см. теоремы 1.4.14 и 1.4.15), в которых используется геометрия пространства Хэмминга. Затем мы применяем методы, которые развиваются в ходе этого доказательства, для получения некоторых «тонких» границ для кодов, которые усиливают границу Хэмминга из теоремы 2.1.6 и ее асимптотический аналог из теорем 2.1.21 и 2.1.24.

Прямая часть ВТШК дана в теореме 2.2.1 в несколько видоизмененной форме по сравнению с теоремами 1.4.14 и 1.4.15. Для простоты мы будем рассматривать здесь только д. с. к. б. п., работая в пространстве $\mathcal{H}_{N,2} = \{0, 1\}^N$ (индекс 2 будет опускаться). Как и в § 1.4, прямая часть ВТШК утверждает, что для любой скорости передачи $R < C$ существуют 1) последовательность кодов $f_n : \mathcal{U}_n \to \mathcal{H}_N$, кодирующих все $\#\mathcal{U}_n = 2^n$ сооб-

щения, и 2) последовательность таких декодеров $\hat{f}_N\colon \mathcal{H}_N \to \mathcal{U}_n$, что $n \sim NR$ и вероятность ошибочного декодирования стремится к нулю при $n \to \infty$. Константа C определена в формуле (1.4.27):

$$C = 1 - \eta(p), \quad \text{где } \eta(p) = -p\log p - (1-p)\log(1-p), \tag{2.2.1}$$

а матрица канала равна

$$\Pi = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}. \tag{2.2.2}$$

Такой канал корректно передаёт букву с вероятностью $1-p$ и обращает её с вероятностью p независимо от остальных передаваемых букв.

В теореме 2.2.1 утверждается, что существует кодирующее отображение f_n, являющееся вложением, для которого задача декодирования сводится к угадыванию кодового слова $f_n(\mathbf{u}) \in \mathcal{H}_N$. Иными словами, теорема гарантирует, что $\forall R < C$ существует последовательность подмножеств $\mathcal{X}_N \subset \mathcal{H}_N$ с $\#\mathcal{X}_N \sim 2^{NR}$, для которых вероятность неверного угадывания стремится к нулю, и точная информация о кодирующем отображении f_n не существенна. Тем не менее, удобно помнить об отображении f_n, так как существование будет следовать из вероятностной конструкции (случайного кодирования), когда код не обязан быть вложением. Кроме того, правило декодирования геометрично: при получении слова $\mathbf{a}^{(N)} \in \mathcal{H}_N$ мы ищем ближайшее кодовое слово $f_n(\mathbf{u}) \in \mathcal{X}_N$. Следовательно, ошибка объявляется каждый раз, когда такое кодовое слово не единственно, или это результат нескольких кодировок, или декодер дает неправильное сообщение. Как мы уже видели, геометрическое правило декодирования соответствует декодеру м. п., когда $p \in (0,\, 1/2)$. Такой декодер позволяет использовать геометрические аргументы, составляющие основу доказательства.

Вновь, как и в § 1.4, новое доказательство прямой части ВТШК только гарантирует существование «хороших» кодов (и даже их «преобладание» среди всех возможных кодов), но не показывает, как построить такие коды. (Единственный рецепт — это использование случайного кодирования и выбора «типичной» реализации.)

В формулировке ВТШК, приведённой ниже, мы имеем дело с максимальной вероятностью ошибки (2.2.4), а не со средней вероятностью по всем возможным сообщениям. Однако большая часть доказательства всё ещё основывается на анализе усреднённой вероятности ошибки, полученной по всем кодовым словам.

Теорема 2.2.1 (вторая теорема Шеннона о канале с шумами, прямая часть). *Рассмотрим симметричный двоичный канал без памяти с матрицей канала* Π, *определённой в формуле* (2.2.2), *где* $0 \leqslant p \leqslant 1/2$, *и пусть* C *дано формулой* (2.2.1). *Тогда для любого*

$R \in (0, C)$ существует последовательность таких кодирующих вложений $f_n : \mathcal{U}_n \to \mathcal{H}_N$, что

1) *выполнены условия*

$$\#\mathcal{U}_n = 2^n, \quad \text{где } n = \lfloor NR \rfloor, \tag{2.2.3}$$

2) *максимальная вероятность ошибки при геометрическом декодировании стремится к нулю при $n \to \infty$:*

$$e^{\max}(f_n) = \max[\mathbf{P}_{\mathrm{ch}}(\text{ошибка при геометрическом декодировании} \mid f_n(\mathbf{u}) \text{ послано}) : \mathbf{u} \in \mathcal{U}_n] \to 0. \tag{2.2.4}$$

Здесь $\mathbf{P}_{\mathrm{ch}}(\cdot \mid f_n(\mathbf{u})$ послано$)$ обозначает распределение вероятностей полученного слова в $\mathcal{H}_N$, генерируемое каналом, при условии, что послано кодовое слово $f_n(\mathbf{u})$, где $\mathbf{u} \in \mathcal{U}_n$ — оригинальное сообщение, сгенерированное источником.

В качестве иллюстрации рассмотрим следующий пример.

Пример 2.2.2. Мы хотим послать сообщение $\mathbf{u} \in \mathcal{A}^n$, где размер алфавита $\#\mathcal{A} = K$, через д. с. к. б. п. с матрицей канала $\begin{pmatrix} 0{,}85 & 0{,}15 \\ 0{,}15 & 0{,}85 \end{pmatrix}$. Какой скорости передачи можно добиться при сколь угодно малой вероятности ошибки?

Здесь $C = 1 - \eta(0{,}15) = 0{,}577291$. Следовательно, по теореме 2.2.1 может быть достигнута любая скорость передачи, меньшая чем 0,577291, при достаточно большом n и со сколь угодно малой вероятностью ошибки. Например, если нам нужна скорость передачи $0{,}5 < R < 0{,}577291$ и $e^{\max} < 0{,}015$, то существует код $f_n : \mathcal{A}^n \to \{0, 1\}^{\lceil n/R \rceil}$, удовлетворяющий этим требованиям при достаточно большом $n > n_0$.

Предположим, что нам известен такой код f_n. Как закодировать сообщение m? Сначала надо разбить сообщение m на блоки длины L, где

$$L = \left\lfloor \frac{0{,}5772N}{\log K} \right\rfloor, \text{ так что } |\mathcal{A}^L| = K^L \leqslant 2^{0{,}5772N}.$$

Тогда мы можем вставлять блоки из $\mathcal{A}^L$ в алфавит $\mathcal{A}^n$ и кодировать целые блоки. Скорость передачи составит $\log |\mathcal{A}^L| / \lceil n/R \rceil \sim 0{,}57729$. К сожалению, ВТШК гарантирует существование таких кодов, но не даёт никаких идей, как их найти (или создать), что трудно сделать. □

Прежде чем приступить к доказательству теоремы 2.2.1, обсудим связь между геометрией пространства Хэмминга $\mathcal{H}_N$ и случайностью, создаваемую каналом. Как и в § 1.4, мы используем символ $\mathbf{P}(\cdot \mid f_n(\mathbf{u}))$ как сокращение для $\mathbf{P}_{\mathrm{ch}}(\cdot \mid f_n(\mathbf{u})$ послано$)$. Среднее и дисперсия этого распределения будут обозначаться $\mathbf{E}(\cdot \mid f_n(\mathbf{u}))$ и $\mathrm{Var}(\cdot \mid f_n(\mathbf{u}))$.

Заметим, что при распределении $\mathbf{P}(\cdot\,|f_n(\mathbf{u}))$ число искаженных знаков в (случайном) полученном слове $\mathbf{Y}^{(N)}$ можно записать как

$$\sum_{j=1}^{N} \mathbf{1}(\text{символ } j \text{ в } \mathbf{Y}^{(N)} \neq \text{символ } j \text{ в } f_n(\mathbf{u})).$$

Это с. в. с биномиальным распределением $\mathrm{Bin}(N, p)$, средним значением

$$\mathbf{E}\left[\sum_{j=1}^{N} \mathbf{1}(\text{символ } j \text{ в } \mathbf{Y}^{(N)} \neq \text{символ } j \text{ в } f_n(\mathbf{u}))\,|\,f_n(\mathbf{u})\right] =$$

$$= \sum_{j=1}^{N} \mathbf{E}[\mathbf{1}(\text{символ } j \text{ в } \mathbf{Y}^{(N)} \neq \text{символ } j \text{ в } f_n(\mathbf{u}))\,|\,f_n(\mathbf{u})] = Np$$

и дисперсией

$$\mathrm{Var}\left[\sum_{j=1}^{N} \mathbf{1}(\text{символ } j \text{ в } \mathbf{Y}^{(N)} \neq \text{символ } j \text{ в } f_n(\mathbf{u}))\,|\,f_n(\mathbf{u})\right] =$$

$$= \sum_{j=1}^{N} \mathrm{Var}[\mathbf{1}(\text{символ } j \text{ в } \mathbf{Y}^{(N)} \neq \text{символ } j \text{ в } f_n(\mathbf{u}))\,|\,f_n(\mathbf{u})] = Np(1-p).$$

Тогда по неравенству Чебышёва для любого $\varepsilon \in (0,\, 1-p)$ и произвольного натурального числа $N > 1/\varepsilon$ вероятность того, что по крайней мере $\lfloor N(p+\varepsilon)\rfloor$ знаков были искажены, при условии, что посылалось кодовое слово $f_n(\mathbf{u})$, не превосходит

$$\mathbf{P}(\geqslant N(p+\varepsilon) - 1 \text{ испорчены}\,|\,f_n(\mathbf{u})) \leqslant \frac{p(1-p)}{N(\varepsilon - 1/N)^2}. \tag{2.2.5}$$

Доказательство теоремы 2.2.1. Положим $2^N = M$. Индексы n и N, связанные соотношением (2.2.3), часто опускаются. Будем использовать м. п./геометрический декодер без дополнительных упоминаний. Аналогично § 1.4 мы отождествляем множество сообщений источника $\mathcal{U}_n$ с пространством Хэмминга $\mathcal{H}_n$. Как предлагал Шеннон, мы привлекаем случайное кодирование. Более точно, сообщение $\mathbf{u} \in \mathcal{H}_n$ отображается случайным кодом $F_n(\mathbf{u}) \in \mathcal{H}_N$ с н. о. р. буквами, принимающими значения 0 и 1 с вероятностью $1/2$ независимо друг от друга. Кроме того, мы считаем кодовое слово $F_n(\mathbf{u})$ независимым от других сообщений $\mathbf{u} \in \mathcal{H}_n$; обозначив строчки из $\mathcal{H}_n$ через $\mathbf{u}(1), \ldots, \mathbf{u}(M)$ (порядок не существен), мы получим семейство н. о. р. строк $F_n(\mathbf{u}(1)), \ldots, F_n(\mathbf{u}(M))$ из $\mathcal{H}_N$. Наконец, мы считаем, что кодовые слова не зависят от канала. Вновь, по аналогии с § 1.4,

можно представить себе рассматриваемый случайный код как случайную мегастроку/кодовую книгу из $\mathcal{H}_{NM} = \{0, 1\}^{NM}$ с н. о. р. знаками 0 и 1 равных вероятностей. Каждый выборочный элемент $f(= f_n)$ этой случайной кодовой книги (т. е. любая данная мегастрока из $\mathcal{H}_{NM}$) задает детерминированное кодирование $f(\mathbf{u}(1)), \ldots, f(\mathbf{u}(M))$ сообщения $\mathbf{u}(1), \ldots, \mathbf{u}(M)$, т. е. код f (см. рис. 2.3).

Как в § 1.4 символом $\mathcal{P}_n$ мы обозначим распределение вероятностей случайного кода:

$$\boldsymbol{\mathcal{P}}_n(F_n = f) = \frac{1}{2^{NM}} \quad \text{для каждой мегастроки } f \tag{2.2.6}$$

и $\boldsymbol{\mathcal{E}}_n$ обозначим математическое ожидание относительно $\boldsymbol{\mathcal{P}}_n$.

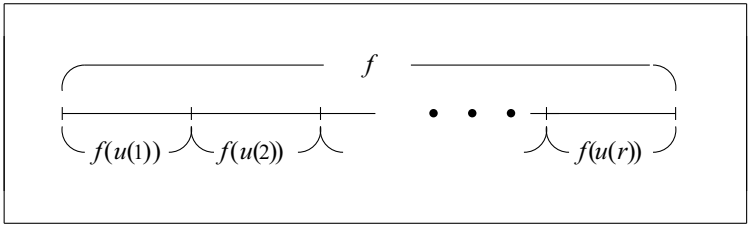


Рис. 2.3

План окончания доказательства следующий. Сначала мы докажем (частично повторяя рассуждения из § 1.4), что для скорости передачи $R \in (0, C)$ усредненная по коду средняя вероятность для упоминавшегося уже случайного кодирования стремится к нулю при $n \to \infty$:

$$\lim_{n\to\infty} \boldsymbol{\mathcal{E}}_n[e^{\text{ave}}(F_n)] = 0. \tag{2.2.7}$$

Здесь $e^{\text{ave}}(F_n)(= e^{\text{ave}}(F_n(\mathbf{u}(1)), \ldots, F_n(\mathbf{u}(M))))$ — с. в., принимающая значения в интервале $(0, 1)$ и представляющая среднюю по коду вероятность ошибки при случайном кодировании. Более точно, как и в § 1.4 для любой данной выборки кодовых слов $f(\mathbf{u}(1)), \ldots, f(\mathbf{u}(M)) \in \mathcal{H}_N$ (т. е. для любой мегастроки f из $\mathcal{H}_{NM}$) мы определяем

$$e^{\text{ave}}(f_n) = \frac{1}{M}\sum_{i=1}^{M} \mathbf{P}(\text{ошибка при использовании кодовой книги } f \,|\, f(\mathbf{u}(i))). \tag{2.2.8}$$

Тогда математическое ожидание усредненной по коду вероятности ошибки равно

$$\mathbf{E}[e^{\text{ave}}(F_n)] = \frac{1}{2^{NM}} \sum_{f(\mathbf{u}(1)),\ldots,f(\mathbf{u}(M))} e^{\text{ave}}(f). \tag{2.2.9}$$

Из равенства (2.2.7) следует (так же как и в § 1.4), что существует такая последовательность детерминированных кодов f_n, что усредненная по коду вероятность ошибки $e^{\rm ave}(f_n) = e^{\rm ave}(f_n(\mathbf{u}(1)), \ldots, f_n(\mathbf{u}(2^n)))$ стремится к нулю

$$\lim_{n\to\infty} e^{\rm ave}(f_n) = 0. \tag{2.2.10}$$

Наконец, мы выведем формулу (2.2.4) из соотношения (2.2.10) (см. лемму 2.2.6).

Замечание 2.2.3. Так как кодовые слова $f(\mathbf{u}(1)), \ldots, f(\mathbf{u}(M))$ случайно выбираются из случайной кодовой книги, мы должны допустить, что они могут совпадать ($f(\mathbf{u}(i)) = f(\mathbf{u}(j))$ при $i \neq j$), в этом случае по умолчанию декодер м. п. сообщает об ошибке. Это необходимо учитывать при рассмотрении вероятности в п. ч. равенства (2.2.8). Поэтому для $i = 1, \ldots, M$ положим

$$\begin{aligned}\mathbf{P}(\text{ошибка при использовании кодовой книги } f \,|\, f(\mathbf{u}(i))) = \\ = \mathbf{P}(\delta(\mathbf{Y}^{(N)}, f(\mathbf{u}(j))) \leqslant \delta(\mathbf{Y}^{(N)}, f(\mathbf{u}(i)) \text{ для некоторого } j \neq i \,|\, f(\mathbf{u}(i))), \\ \text{если } f(\mathbf{u}(i)) \neq f(\mathbf{u}(i')) \ \forall i' \neq i,\end{aligned} \tag{2.2.11}$$

и равна 1, если $f(\mathbf{u}(i)) = f(\mathbf{u}(i'))$ при некотором $i' \neq i$. □

Теперь приступим к детальному доказательству. Первый его шаг заключается в следующей лемме.

Лемма 2.2.4. *Рассмотрим матрицу канала* Π (*см. формулу* (2.2.2)), $0 \leqslant p < 1/2$. *Предположим, что скорость передачи* $R < C = 1 - \eta(p)$. *Пусть* $N > 1/\varepsilon$. *Тогда для любого* $\varepsilon \in (0,\, 1/2 - p)$ *математическое ожидание усредненной по коду вероятности ошибки* $\boldsymbol{\mathcal{E}}_n[e^{\rm ave}(F_n)]$, *определённое формулами* (2.2.8) *и* (2.2.9), *подчиняется неравенству*

$$\boldsymbol{\mathcal{E}}_n[e^{\rm ave}(F_n)] \leqslant \frac{p(1-p)}{N(\varepsilon - 1/N)^2} + \frac{M-1}{2^N} \upsilon_N(\lceil N(p+\varepsilon)\rceil), \tag{2.2.12}$$

где $\upsilon_N(b)$ *обозначает число точек в шаре радиуса* b *в двоичном пространстве Хэмминга* $\mathcal{H}_N$.

Доказательство. Положим $m(= m_N(p, \varepsilon)) := \lceil N(p+\varepsilon)\rceil$. Декодер м. п. заведомо находит правильное кодовое слово $f_n(\mathbf{u}(i))$, посланное через канал, когда $f_n(\mathbf{u}(i))$ — единственное кодовое слово в шаре Хэмминга $\mathcal{B}_N(\mathbf{y}, m)$ с центром в полученном слове $\mathbf{y}(= \mathbf{y}^{(N)}) \in \mathcal{H}_N$. В любой другой ситуации (когда $f_n(\mathbf{u}(i)) \notin \mathcal{B}_N(\mathbf{y}, m)$ или $f_n(\mathbf{u}(k)) \in \mathcal{B}_N(\mathbf{y}, m)$ для некоторого $k \neq i$) возникает возможность ошибки.

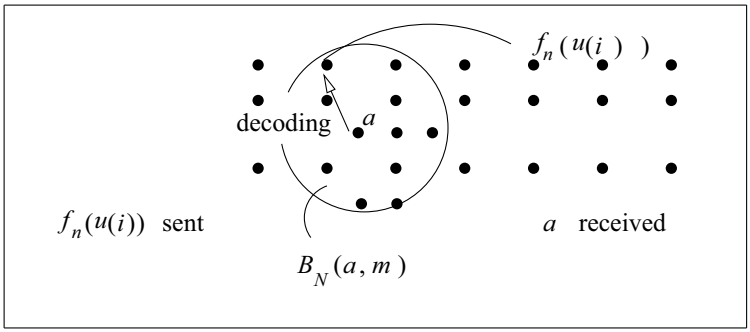


Рис. 2.4

Следовательно,

$$\mathbf{P}(\text{ошибка при использовании кодовой книги } f \,|\, f(\mathbf{u}(i))) \leqslant$$
$$\leqslant \sum_{\mathbf{y}\in\mathcal{H}_N} \mathbf{P}(\mathbf{y}\,|\,f_n(\mathbf{u}(i)))\,\mathbf{1}(f_n(\mathbf{u}(i)) \notin \mathcal{B}_N(\mathbf{y},\, m)) +$$
$$+ \sum_{\mathbf{z}\in\mathcal{H}_N} \mathbf{P}(\mathbf{z}\,|\,f_n(\mathbf{u}(i))) \sum_{k\neq i} \mathbf{1}(f_n(\mathbf{u}(k)) \in \mathcal{B}_N(\mathbf{z},\, m)). \quad (2.2.13)$$

Первую сумму легко оценить:

$$\sum_{\mathbf{y}\in\mathcal{H}_N} \mathbf{P}(\mathbf{y}\,|\,f_n(\mathbf{u}(i)))\,\mathbf{1}(f_n(\mathbf{u}(i)) \notin \mathcal{B}_N(\mathbf{y},\, m)) =$$
$$= \sum_{\mathbf{y}\in\mathcal{H}_N} \mathbf{P}(\mathbf{y}\,|\,f_n(\mathbf{u}(i)))\,\mathbf{1}(\text{расстояние } \delta(\mathbf{y},\, f_n(\mathbf{u}(i))) \geqslant m) =$$
$$= \mathbf{P}(\geqslant m \text{ испорченных знаков}\,|\,f(\mathbf{u}(i))) \leqslant \frac{p(1-p)}{N(\varepsilon - 1/N)^2} \quad (2.2.14)$$

в силу формулы (2.2.5). Неравенство (2.2.14) останется справедливым, если мы сначала возьмём среднее $\frac{1}{M}\sum_{i=1}^{M}$, а затем математическое ожидание $\boldsymbol{\mathcal{E}}_n$, поскольку п. ч. в формуле (2.2.14) не зависит от выбора кода f,

При оценке второй суммы в п. ч. формулы (2.2.13) нужно поступить хитрее: сначала усредним, а затем возьмём математическое ожидание.

Здесь мы имеем

$$\mathcal{E}_n\left[\sum_{i=1}^{M}\sum_{\mathbf{z}\in\mathcal{H}_N}\mathbf{P}(\mathbf{z}\,|\,F_n(\mathbf{u}(i)))\sum_{k\neq i}\mathbf{1}(F_n(\mathbf{u}(k))\in\mathcal{B}_N(\mathbf{z},\,m))\right]=$$

$$=\sum_{i=1}^{M}\sum_{k\neq i}\sum_{\mathbf{z}\in\mathcal{H}_N}\mathcal{E}_n[\mathbf{P}(\mathbf{z}\,|\,F_n(\mathbf{u}(i)))\mathbf{1}(F_n(\mathbf{u}(k))\in\mathcal{B}_N(\mathbf{z},\,m))]=$$

$$=\sum_{i=1}^{M}\sum_{k\neq i}\sum_{\mathbf{z}\in\mathcal{H}_N}\mathcal{E}_n[\mathbf{P}(\mathbf{z}\,|\,F_n(\mathbf{u}(i)))]\mathcal{E}_n[\mathbf{1}(F_n(\mathbf{u}(k))\in\mathcal{B}_N(\mathbf{z},\,m)))], \quad (2.2.15)$$

так как кодовые слова $F_n(\mathbf{u}(1)),\,\ldots,\,F_n(\mathbf{u}(M))$ независимы. Далее, поскольку каждое из этих слов равномерно распределено на $\mathcal{H}_N$, математические ожидания $\mathcal{E}_n[\mathbf{P}(\mathbf{z}\,|\,F_n(\mathbf{u}(i))]$ и $\mathcal{E}_n[\mathbf{1}(F_n(\mathbf{u}(k))\in\mathcal{B}_N(\mathbf{z},\,m))]$ можно вычислить как

$$\mathcal{E}_n[\mathbf{P}(\mathbf{z}\,|\,F_n(\mathbf{u}(i))]=\frac{1}{2^N}\sum_{\mathbf{x}\in\mathcal{H}_N}\mathbf{P}(\mathbf{z}\,|\,\mathbf{x}) \quad (2.2.16\text{а})$$

и

$$\mathcal{E}_n[\mathbf{1}(F_n(\mathbf{u}(k))\in\mathcal{B}_N(\mathbf{z},\,m))]=\frac{v_N(m)}{2^N}. \quad (2.2.16\text{б})$$

Суммируя по $\mathbf{z}$, получаем

$$\sum_{\mathbf{z}\in\mathcal{H}_N}\sum_{\mathbf{x}\in\mathcal{H}_N}\mathbf{P}(\mathbf{z}\,|\,\mathbf{x})=\sum_{\mathbf{x}\in\mathcal{H}_N}\sum_{\mathbf{z}\in\mathcal{H}_N}\mathbf{P}(\mathbf{z}\,|\,\mathbf{x})=2^N. \quad (2.2.17)$$

Наконец, после суммирования по $k\neq i$ имеем

$$\text{п. ч. формулы (2.2.15)}=\frac{1}{M}\sum_{i=1}^{M}\sum_{k\neq i}\frac{v_N(m)}{2^N}=$$

$$=\frac{v_N(m)M(M-1)}{2^NM}=\frac{(M-1)v_N(m)}{2^N}. \quad (2.2.18)$$

Собирая формулы (2.2.12)–(2.2.18), получаем, что $\mathcal{E}_n[e^{\mathrm{ave}}(F_n)]$ не превышает п. ч. формулы (2.2.12), что завершает доказательство леммы 2.2.4. □

Следующим шагом мы выразим объём $v_N(m)$ через энтропию $\boldsymbol{\eta}(p+\varepsilon)$, где, напомним, $m=\lceil N(p+\varepsilon)\rceil$. Рассуждение здесь близко к аналогичному рассуждению из § 1.4 и опирается на следующую лемму.

Лемма 2.2.5. *Предположим, что* $0<p<1/2$, $\varepsilon>0$ *и* N *достаточно велико, так что* $p+\varepsilon+1/N<1/2$. *Тогда справедливо неравенство*

$$v_N(\lceil N(p+\varepsilon)\rceil)\leqslant 2^{N\boldsymbol{\eta}(p+\varepsilon)}. \quad (2.2.19)$$

Доказательство леммы 2.2.5 будет дано позже, после примера 2.2.7. А сейчас продолжим доказательство теоремы 2.2.1. Напомним, что мы хотим доказать формулу (2.2.7). Фактически если $p < 1/2$ и $R < C = 1 - \eta(p)$, то мы положим $\zeta = C - R > 0$ и возьмём $\varepsilon > 0$ настолько маленьким, что 1) $p + \varepsilon < 1/2$ и 2) $R + \zeta/2 < 1 - \eta(p + \varepsilon)$. Затем мы выберем N настолько большим, что 3) $N > 2/\varepsilon$. С таким образом выбранными N и ε мы имеем

$$\varepsilon - \frac{1}{N} > \frac{\varepsilon}{2} \quad \text{и} \quad R - 1 + \eta(p + \varepsilon) < -\frac{\zeta}{2}. \tag{2.2.20}$$

Тогда, начиная с неравенства (2.2.12), мы можем написать

$$\mathcal{E}_N[e(F_n)] \leqslant \frac{4p(1-p)}{N\varepsilon^2} + \frac{2^{NR}}{2^N} 2^{N\eta(p+\varepsilon)} < \frac{4}{N\varepsilon^2} p(1-p) + 2^{-\zeta N/2}. \tag{2.2.21}$$

Отсюда следует формула (2.2.7) и, значит, существование последовательности кодов $f_n\colon \mathcal{H}_n \to \mathcal{H}_N$, удовлетворяющей требованию (2.2.10).

Для завершения доказательства теоремы 2.2.1 мы выведем формулу (2.2.10) из соотношения (2.2.7) в виде следующей леммы.

Лемма 2.2.6. *Рассмотрим двоичный канал* (*не обязательно без памяти*), *и пусть* $C > 0$ — *константа. При данных* $0 < R < C$ *и* $n = \lfloor NR \rfloor$ *определим величины* $e^{\max}(f_n)$ *и* $e^{\mathrm{ave}}(\tilde{f}_n)$ *в соответствии с формулами* (2.2.4), (2.2.8) *и* (2.2.11) *для кодов* $f_n\colon \mathcal{H}_n \to \mathcal{H}_N$ *и* $\tilde{f}_n\colon \mathcal{H}_n \to \mathcal{H}_N$. *Тогда следующие высказывания эквивалентны*:

1) $\forall R \in (0, C)$ *существует такой код* f_n, *что* $\lim\limits_{n\to\infty} e^{\max}(f_n) = 0$,

2) $\forall R \in (0, C)$ *существует такой код* $\tilde{f}_n$, *что* $\lim\limits_{n\to\infty} e^{\mathrm{ave}}(\tilde{f}_n) = 0$.

Доказательство. Ясно, что утверждение 2) следует из утверждения 1). Для вывода обратной импликации возьмём $R < C$ и для достаточно большого N положим

$$R' = R + \frac{1}{N} < C, \quad n' = \lfloor NR' \rfloor, \quad M' = 2^{n'}. \tag{2.2.22}$$

Мы знаем, что существует последовательность кодов $\tilde{f}_n\colon \mathcal{H}_{n'} \to \mathcal{H}_N$, удовлетворяющая условию $\lim\limits_{n\to\infty} e^{\mathrm{ave}}(\tilde{f}_n) = 0$. Напомним, что

$$e^{\mathrm{ave}}(\tilde{f}_n) = \frac{1}{M'} \sum_{i=1}^{M'} \mathbf{P}(\text{ошибка при использовании } \tilde{f}_n \,|\, \tilde{f}_n(\mathbf{u}(i))). \tag{2.2.23}$$

Здесь и далее $M' = 2^{\lfloor NR' \rfloor}$ и $\tilde{f}_n(\mathbf{u}(1)), \ldots, \tilde{f}_n(\mathbf{u}(M')) \in \mathcal{H}_{n'}$ — кодовые слова сообщения источника $\mathbf{u}(1), \ldots, \mathbf{u}(M') \in \mathcal{H}_{n'}$.

Вместо $\mathbf{P}(\text{ошибка при использовании } \tilde{f}_n \,|\, \tilde{f}_n(\mathbf{u}(i)))$ мы для краткости будем писать $\mathbf{P}(f_n\text{-ошибка} \,|\, \tilde{f}_n(\mathbf{u}(i)))$. Теперь заметим, что по крайней мере

половина слагаемых в п. ч. формулы (2.2.23) должна быть меньше чем $2e^{\mathrm{ave}}(\tilde{f}_n)$. Ввиду формулы (2.2.22) имеем

$$M'/2 \geqslant 2^{\lfloor NR \rfloor - 1}. \tag{2.2.24}$$

Следовательно, в нашем распоряжении есть не менее $2^{\lfloor NR \rfloor - 1}$ кодовых слов $f(u(i))$ с $\mathbf{P}(f_n\text{-ошибка} \,|\, \tilde{f}_n(\mathbf{u}(i))) < 2e^{\mathrm{ave}}(\tilde{f}_n)$. Перечислим эти слова как новый двоичный код длины N со скоростью передачи информации $(\log M'/2)/N$. Обозначив этот новый код символом f_n, мы получим

$$e^{\max}(f_n) \leqslant 2e^{\mathrm{ave}}(\tilde{f}_n).$$

Следовательно, $e^{\max}(f_n) \to 0$ при $n \to \infty$, поскольку $(\log M'/2)/N \to R$. Это доказывает утверждение 1) и завершает доказательство леммы 2.2.6. □

Пример 2.2.7 (ср. пример 2.1.20). Докажите, что для натуральных чисел N и m, удовлетворяющих условиям $m < N/2$ и $\beta = m/N$, верно неравенство

$$2^{N\eta(\beta)}/(N+1) < v_N(m) < 2^{N\eta(\beta)}. \tag{2.2.25}$$

Решение. При $\beta = m/N < 1/2$ и $0 \leqslant k < m$ имеем

$$\beta^k(1-\beta)^{N-k} = \left(\frac{\beta}{1-\beta}\right)^k (1-\beta)^N > \left(\frac{\beta}{1-\beta}\right)^m (1-\beta)^N = \beta^m (1-\beta)^{N-m},$$

так как $\beta/(1-\beta) < 1$. Следовательно,

$$1 = \sum_{k=0}^{N} C_N^k \beta^k (1-\beta)^{N-k} > \sum_{k=0}^{m} C_N^k \beta^k (1-\beta)^{N-k} >$$

$$> \beta^m (1-\beta)^{N-m} \sum_{k=0}^{m} C_N^k = v_N(m) \beta^m (1-\beta)^{N-m} = v_N(m) 2^{-N\eta(\beta)},$$

где

$$v_N(m) = \#\{\text{точки на расстоянии не больше } m \text{ от } \mathbf{0} \text{ в } \mathcal{H}_N\} = \sum_{k=0}^{m} C_N^k.$$

Итак, $v_N(m) < 2^{N\eta(\beta)}$. Для доказательства л. ч. (2.2.25) проверим неравенство

$$v_N(m) > C_N^m \geqslant 2^{N\eta(\beta)}/(N+1). \tag{2.2.26}$$

Рассмотрим биномиальную с. в. $Y \sim \mathrm{Bin}(N, \beta)$, для которой

$$p_k = \mathsf{P}(Y = k) = C_N^k \beta^k (1-\beta)^{N-k}, \quad k = 0, \ldots, N.$$

Достаточно доказать, что p_k достигает своего максимального значения при $k = m$, так как тогда

$$p_m = C_N^m \beta^m (1-\beta)^{N-m} \geqslant \frac{1}{N+1} \text{ с } \beta^m (1-\beta)^{N-m} = 2^{-N\eta(\beta)}.$$

Предположим сначала, что $k \leqslant m$ и запишем

$$\frac{p_k}{p_m} = \frac{m!(N-m)!(N-m)^{m-k}}{k!(N-k)!m^{m-k}} = = \frac{(k+1)\dots m}{m^{m-k}} \cdot \frac{(N-m)^{m-k}}{(N-m+1)\dots(N-k)}.$$

Здесь п. ч. не превосходит 1, так как представляет собой произведение $2(m-k)$ сомножителей, каждый из которых не больше 1. Аналогично при $k \geqslant m$ мы приходим к произведению

$$\frac{m^{k-m}}{(m+1)\dots k} \cdot \frac{(N-k+1)\dots(N-m)}{(N-m)^{k-m}},$$

которое тоже не превосходит 1, как произведение $2(k-m)$ сомножителей, не превосходящих 1. Итак, $p_k/p_m \leqslant 1$, откуда вытекает оценка (2.2.26). □

Теперь мы готовы к доказательству леммы 2.2.5.

Доказательство леммы 2.2.5. Так как $p + \varepsilon < 1/2$, получаем, что $m = \lfloor N(p+\varepsilon) \rfloor < N/2$ и

$$\beta := \frac{m}{N} = \frac{\lfloor N(p+\varepsilon) \rfloor}{N} < p + \varepsilon,$$

откуда, в свою очередь, следует, что $\eta(\beta) < \eta(p+\varepsilon)$, $\eta(x)$ — строго возрастающая функция при $x \in (0, 1/2)$. Это доказывает лемму в силу оценки из леммы 2.2.5. □

Геометрическое доказательство прямой части теорем Шеннона проясняют смысл понятия «пропускная способность» канала (по крайней мере, в случае д. с. к. б. п.). Физически говоря, в выражениях (1.4.27) и (2.2.1) для пропускной способности $C = 1 - \eta(p)$ д. с. к. б. п. положительный член, т. е. 1, указывает на скорость, с которой случайный код производит «пустой» объём между кодовыми словами, а отрицательный член $-\eta(p)$ указывает скорость, с которой слова постепенно заполняют этот объём.

Пример 2.2.8. Опираясь на теоремы Шеннона, получите выражение для пропускной способности д. с. к. б. п. Оцените, в частности, пропускную способность 1) симметричного канала без памяти и 2) идеального канала с входным алфавитом 0, 1, входные сигналы которого подчиняются ограничению: нули никогда не стоят рядом друг с другом.

Решение. Пропускная способность канала определяется как точная верхняя граница скоростей передач R, при которых полученные сообщения (с вероятностью, приближающейся к 1, при длине сообщения, стремящейся к бесконечности) можно корректно декодировать. Популярный класс

составляют каналы без памяти, где для данного входного слова $\mathbf{x}^{(N)} = x_1 \dots x_N$ вероятность равна

$$\mathbf{P}^{(N)}(\mathbf{y}^{(N)} \text{ получено} \,|\, \mathbf{x}^{(N)} \text{ послано}) = \prod_{i=1}^{N} P(y_i \,|\, x_i).$$

Иначе говоря, шум воздействует на каждый символ x_i входной строки $\mathbf{x}$ независимо, и $P(y\,|\,x)$ — вероятность принятия символа y при условии, что был послан символ x.

Символ x «бегает» по входному алфавиту $\mathcal{A}_{\text{in}}$ данного размера q, а y принадлежит выходному алфавиту $\mathcal{A}_{\text{out}}$ размера r. В этой ситуации вероятности $P(y\,|\,x)$ образуют стохастическую матрицу размера $q \times r$ (матрицу канала). Канал без памяти называется симметричным, если сроки его матрицы получаются друг из друга перестановками элементов, т. е. состоят из одного набора вероятностей, скажем $p_1, \dots, p_r$. Симметричный канал без памяти называют дважды симметричным, если и столбцы матрицы канала получаются друг из друга перестановками элементов. Если $r = n = 2$ (обычно $\mathcal{A}_{\text{in}} = \mathcal{A}_{\text{out}} = \{0, 1\}$), то канал без памяти называют двоичным. Элементы матрицы д. с. к. б. п. выглядят следующим образом: $P(0\,|\,0) = P(1\,|\,1) = 1 - p$, $P(1\,|\,0) = P(0\,|\,1) = p$, $p \in (0, 1)$ — вероятность обращения, а $1 - p$ — вероятность корректной передачи двоичного символа.

Пропускная способность канала — это такое число $C \geqslant 0$, что любое значение $R < C$ является скоростью надёжной передачи. Здесь R называется скоростью надёжной передачи, если существуют последовательность кодов $f_n \colon \mathcal{H}_n \to \mathcal{H}_N$ и правила декодирования $\hat{f}_N \colon \mathcal{H}_N \to \mathcal{H}_n$, для которых $n \sim NR$ и (подходящим образом определённая) вероятность ошибки подчиняется условию

$$\lim_{N\to\infty} e(f_n, \hat{f}_N) = 0.$$

Иначе говоря,

$$C = \lim_{N\to\infty} \frac{1}{N} \log M_N,$$

где M_N — максимальное число кодовых слов $\mathbf{x} \in \mathcal{H}_N$, для которых вероятность ошибочного декодирования стремится к нулю.

Вторая теорема Шеннона утверждает, что для канала без памяти

$$C = \max_{p_X} I(X : Y),$$

где $I(X : Y)$ — взаимная информация между (случайным) входным символом X и соответствующим выходным символом Y, а максимум берётся по всем возможным распределениям p_X с. в. X.

1) В случае симметричного канала без памяти описанная процедура максимизации применяется только к выходным символам:

$$C = \bigl(\max_{p_X} h(Y)\bigr) + \sum_{i=1}^{r} p_i \log p_i;$$

Сумма $-\sum_i p_i \log p_i$ — энтропия строк матрицы канала $(P(y\,|\,x))$. Для дважды симметричного канала выражение для пропускной способности ещё более упрощается:

$$C = \log M - h(p_1, \ldots, p_r),$$

так как $h(Y)$ достигается на равномерном распределении p_X с $p_X(x) \equiv 1/q$ (и $p_Y(y) \equiv 1/r$). В случае д. с. к. б. п. мы имеем

$$C = 1 - \eta(p),$$

что завершает решение части 1).

Далее, канал из части 2) не является каналом без памяти, но общие определения к нему вполне применимы. Обозначим через $n(j;\, t)$ число разрешённых строк длины t, оканчивающихся символом j, $j = 0,\, 1$. Тогда

$$n(0,\, t) = n(1,\, t-1), \quad n(1,\, t) = n(0,\, t-1) + n(1,\, t-1),$$

где

$$n(1,\, t) = n(1,\, t-1) + n(1,\, t-2).$$

Запишем это в виде рекурсии:

$$\begin{pmatrix} n(1,\, t) \\ n(1,\, t-1) \end{pmatrix} = A \begin{pmatrix} n(1,\, t-1) \\ n(1,\, t-2) \end{pmatrix},$$

с матрицей рекурсии

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Общее решение имеет вид

$$n(1,\, t) = c_1 \lambda_1^t + c_2 \lambda_2^t,$$

где $\lambda_1,\, \lambda_2$ — собственные числа матрицы A, т. е. корни характеристического уравнения

$$\det(A - \lambda \mathbf{1}) = (1-\lambda)(-\lambda) - 1 = \lambda^2 - \lambda - 1 = 0.$$

Таким образом, $\lambda = (1 \pm \sqrt{5})/2$ и

$$\lim_{t\to\infty} \frac{1}{t} \log n(1,\, t) = \log\Bigl(\frac{\sqrt{5}+1}{2}\Bigr).$$

Пропускная способность канала равна

$$C = \lim_{t\to\infty} \frac{1}{t} \log \#(\text{ разрешённые входные строки длины } t) =$$
$$= \lim_{t\to\infty} \frac{1}{t} \log[n(1,\, t) + n(0,\, t)] = \log\left(\frac{\sqrt{5}+1}{2}\right). \quad \square$$

Замечание 2.2.9. Можно видоизменить последний вопрос, рассмотрев д. с. к. б. п. $\Pi = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$, входной сигнал которого удовлетворяет тому ограничению, что нули в нём не могут стоять рядом. Такой канал можно рассматривать как композицию двух последовательных каналов (см. пример 1.4.31, п. 1), что даёт следующий ответ для пропускной способности:

$$C = \min\left[\log\left(\frac{\sqrt{5}+1}{2}\right),\, 1 - \eta(p)\right]. \quad \square$$

Далее мы представляем обратную часть ВТШК для д. с. к. б. п. в сильной форме (см. теорему 1.4.14); для её доказательства мы вновь используем геометрию пространства Хэмминга. «Сильная» форма утверждения означает, что для любой скорости передачи R, превышающей пропускную способность канала C, максимальная вероятность ошибки будет сколь угодно близкой к 1. Вновь для простоты мы докажем ее для д. с. к. б. п.

Теорема 2.2.10 (вторая теорема Шеннона о канале с шумом, обратная часть). *Пусть C — пропускная способность д. с. к. б. п. с матрицей канала $\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$, где $0 < p < 1/2$, и пусть $R > C$. Тогда при $n = \lfloor NR \rfloor$ для любого кода $f_n\colon \mathcal{H}_n \to \mathcal{H}_N$ и декодера $\hat{f}_N\colon \mathcal{H}_N \to \mathcal{H}_n$ максимальная вероятность ошибки*

$$\varepsilon^{\max}(f_n,\, \hat{f}_N) := \max[\mathbf{P}(\textit{ошибка при использовании } \hat{f}_N \,|\, f_n(\mathbf{u}))\colon \mathbf{u} \in \mathcal{H}_n] \tag{2.2.27а}$$

подчиняется условию

$$\limsup_{N\to\infty} \varepsilon^{\max}(f_n,\, \hat{f}_N) = 1. \tag{2.2.27б}$$

Доказательство. Как в § 1.4, можно предполагать, что коды f_n являются кодами без потерь (см. определение 1.1.3) и удовлетворяют равенству $\hat{f}_N(f_n(\mathbf{u})) = \mathbf{u}\ \ \forall \mathbf{u} \in \mathcal{H}_n$ (в противном случае шансы ошибочного декодирования станут даже выше). Предположим обратное неравенству (2.2.27б):

$$\varepsilon^{\max}(f_n,\, \hat{f}_N) \leqslant c \text{ для некоторого } c < 1 \text{ и достаточно большого } N. \tag{2.2.28}$$

Наша цель — вывести из этого предположения неравенство $R \leqslant C$. Как и ранее, положим $n = \lfloor NR \rfloor$ и пусть $f_n(\mathbf{u}(i))$ — кодовое слово для строки

$\mathbf{u}(i) \in \mathcal{H}_n$, $i = 1, \ldots, 2^n$. Пусть $\mathcal{D}_i \subset \mathcal{H}_N$ — множество двоичных строк, составляющих множество значений декодера: $\hat{f}_N(\mathbf{a}) = f_n(\mathbf{u}(i))$ тогда и только тогда, когда $\mathbf{a} \in \mathcal{D}_i$. Тогда $\mathcal{D}_i \ni f_n(\mathbf{u}(i))$, множества $\mathcal{D}_i$ попарно не пересекаются и если $\bigcup\limits_i \mathcal{D}_i \neq \mathcal{H}_N$, то на дополнении $\mathcal{H}_N \setminus \bigcup\limits_i \mathcal{D}_i$ канал сообщает об ошибке. Пусть $s_i = \#\mathcal{D}_i$ — размер множества $\mathcal{D}_i$.

Наш первый шаг заключается в «улучшении» декодера путём приближения его к декодеру м. п. Другими словами, мы хотим заменить каждое $\mathcal{D}_i$ новым множеством $\mathcal{C}_i \subset \mathcal{H}_N$ того же размера $s_i = \#\mathcal{C}_i$, но более «округлой» формы (т. е. близкой к шару Хэмминга $\mathcal{B}(f(\mathbf{u}(i)), b_i)$. Точнее говоря, мы ищем попарно непересекающиеся множества $\mathcal{C}_i$ размера $\#\mathcal{C}_i = s_i$, удовлетворяющие условию

$$\mathcal{B}_N(f(\mathbf{u}(i)), b_i) \subseteq \mathcal{C}_i \subset \mathcal{B}_N(f(\mathbf{u}(i)), b_i + 1), \quad i = 1, \ldots, 2^n, \tag{2.2.29}$$

для некоторых значений радиуса $b_i \geqslant 0$, которые будут конкретизированы позже. Мы можем считать, что $\mathcal{C}_i$ получается из $\mathcal{D}_i$ путём нескольких «непересекающихся обменов», когда мы удаляем строку $\mathbf{a}$ и добавляем другую строку $\mathbf{b}$ с расстоянием Хэмминга

$$\delta(\mathbf{b}, f_n(\mathbf{u}_i)) \leqslant \delta(\mathbf{a}, f_n(\mathbf{u}_i)). \tag{2.2.30}$$

Обозначим новый декодер символом $\hat{g}_N$. Поскольку вероятность обращения символов $p < 1/2$, из формулы (2.2.30) следует, что

$$\begin{aligned}\mathbf{P}(\hat{f}_N \text{ возвращает } f_n(\mathbf{u}(i)) \,|\, f_n(\mathbf{u}(i))) = \mathbf{P}(\mathcal{D}_i \,|\, f_n(\mathbf{u}(i))) \leqslant \\ \leqslant \mathbf{P}(\mathcal{C}_i \,|\, f_n(\mathbf{u}(i))) = \mathbf{P}(\hat{g}_N \text{ возвращает } f_n(\mathbf{u}(i)) \,|\, f_n(\mathbf{u}(i))),\end{aligned}$$

что, в свою очередь, эквивалентно неравенству

$$\begin{aligned}\mathbf{P}(\text{ошибка при использовании } \hat{g}_N \,|\, f_n(\mathbf{u}(i))) \leqslant \\ \leqslant \mathbf{P}(\text{ошибка при использовании } \hat{f}_N \,|\, f_n(\mathbf{u}(i)))\end{aligned} \tag{2.2.31}$$

Тогда очевидно, что

$$\varepsilon^{\max}(f_n, \hat{g}_N) \leqslant \varepsilon^{\max}(f_n, \hat{f}_N) \leqslant c. \tag{2.2.32}$$

Теперь предположим, что найдётся такое число $p' < p$, что для любого достаточно большого N выполняется неравенство

$$b_i + 1 \leqslant \lceil Np' \rceil \text{ для некоторого } 1 \leqslant i \leqslant 2^n. \tag{2.2.33}$$

Тогда ввиду формул (2.2.29) и (2.2.32) для дополнения $\mathcal{C}_i^c = \mathcal{H}_N \setminus \mathcal{C}_i$ имеем

$$\begin{aligned}\mathbf{P}(\text{по крайней мере } Np' \text{ знаков искажены} \,|\, f_n(\mathbf{u}(i))) \leqslant \\ \leqslant \mathbf{P}(\text{по крайней мере } b_i + 1 \text{ знаков искажены} \,|\, f_n(\mathbf{u}(i))) \leqslant \\ \leqslant \mathbf{P}(\mathcal{C}_i^c \,|\, f_n(\mathbf{u}(i))) \varepsilon^{\max}(f_n, \hat{g}_N) \leqslant c.\end{aligned}$$

Это приводит к противоречию, поскольку по закону больших чисел

$$\mathbf{P}(\text{по крайней мере } Np' \text{ знаков искажены} \,|\, \mathbf{x} \text{ послано}) \to 1 \quad \text{при } N \to \infty$$

равномерно по всем способам выбора входного слова $\mathbf{x} \in \mathcal{H}_N$. (На самом деле эта вероятность не зависит от $\mathbf{x} \in \mathcal{H}_N$.)

Таким образом, мы не можем выбрать $p' \in (0,\ p)$ так, что при достаточно большом N формула (2.2.32) останется в силе, т. е. верно обратное: при любом данном $p' \in (0,\ 1)$ мы можем найти сколь угодно большое N, для которого

$$b_i > Np' \ \forall i = 1,\ \ldots,\ 2^n. \tag{2.2.34}$$

(Как мы требуем в формуле (2.2.34), для всех $p' \in (0,\ p)$ не имеет значения, какое из чисел b_i или $b_i + 1$ в л. ч. формулы (2.2.34) мы поставим.)

Теперь вновь используем явное выражение для объёма шара Хэмминга:

$$s_i = \#\mathcal{D}_i = \#\mathcal{C}_i \geqslant v_N(b_i) = \sum_{j=0}^{b_i} C_N^j \geqslant C_N^{b_i} \geqslant$$
$$\geqslant C_N^{\lfloor Np' \rfloor} \text{ в предположении, что } b_i > Np'. \tag{2.2.35}$$

В примере 2.1.20 было установлено полезное неравенство:

$$v_N(R) \geqslant \frac{1}{N+1} 2^{N\eta(R/N)}. \tag{2.2.36}$$

Great Hamming Balls of Fire[2]

(Из серии «Фильмы, которые не вышли на большой экран».)

Теперь мы готовы завершить доказательство теоремы 2.2.10. В силу (2.2.36) для любого $p' \in (0,\ p)$ можно найти такое сколь угодно большое N, что

$$s_i \geqslant 2^{N(\eta(p') - \varepsilon_N)} \ \forall 1 \leqslant i \leqslant 2^n,$$

где $\lim\limits_{N\to\infty} \varepsilon_N = 0$. Так как исходные множества $\mathcal{D}_1,\ \ldots,\ \mathcal{D}_{2^n}$ не пересекаются, мы получаем, что

$$s_1 + \ldots + s_{2^n} \leqslant 2^N \ \Rightarrow\ 2^{N(\eta(p') - \varepsilon_N)} \times 2^{\lfloor NR \rfloor} \leqslant 2^N,$$

или

$$\eta(p') - \varepsilon_N + \frac{\lfloor NR \rfloor}{N} \leqslant 1 \ \Rightarrow\ R \leqslant 1 - \eta(p') + \varepsilon_N + \frac{1}{N}.$$

[2] Ср. с названием фильма «Ball of Fire» о группе профессоров, изучавших сленг с помощью танцовщицы из ночного клуба. Одна из ролей принадлежит Леониду Кински (1903-1998), эмигранту из России, известному также по фильму «Касабланка».

При $N \to \infty$ п. ч. стремится к $1 - \eta(p')$, так что при любом $p' \in (0, p)$ имеем $R \leqslant 1 - \eta(p')$, следовательно, $R \leqslant 1 - \eta(p) = C$. Теорема 2.2.10 доказана. □

Мы видели, что анализ пересечения заданного множества $\mathcal{X}$ в пространстве Хэмминга $\mathcal{H}_N$ (и вообще в $\mathcal{H}_{N,q}$) с различными шарами $\mathcal{B}_N(\mathbf{y}, s)$ много говорит о самом множестве $\mathcal{X}$. В оставшейся части этого параграфа такой подход будет использоваться для получения некоторых дополнительных границ на q-ичные коды: неравенств Элайеса и Джонсона. Эти границы относятся к наиболее известным общим границам для кодов и соперничают друг с другом.

Метод, используемый для доказательства неравенства Элайеса, во многом следует тому, который применялся для доказательства границы Плоткина (см. теорему 2.1.15 и пример 2.1.18). Мы подсчитываем кодовые слова q-ичного $[N, M, d]$-кода $\mathcal{X}$ в шаре $\mathcal{B}_{N,q}(\mathbf{y}, s)$ радиуса s с центром в слове $\mathbf{y} \in \mathcal{H}_{N,q}$. Точнее, мы подсчитываем пары $(\mathbf{x}, \mathcal{B}_{N,q}(\mathbf{y}, s))$, где $\mathbf{x} \in \mathcal{X} \cap \mathcal{B}_{N,q}(\mathbf{y}, s)$. Если шар $\mathcal{B}_{N,q}(\mathbf{y}, s)$ содержит $K_{\mathbf{y}}$ кодовых слов, то

$$\sum_{\mathbf{y} \in \mathcal{H}_N} K_{\mathbf{y}} = M v_{N,q}(s), \tag{2.2.37}$$

так как каждое слово $\mathbf{x} \in \mathcal{X}$ попадает $v_{N,q}(s)$ раз в шар $\mathcal{B}_{N,q}(\mathbf{y}, s)$.

Лемма 2.2.11. *Если $\mathcal{X}$ — q-ичный $[N, M]$-код, то для любого $s = 1, \ldots, N$ существует шар $\mathcal{B}_{N,q}(\mathbf{y}, s)$ с центром в N-слове $\mathbf{y} \in \mathcal{H}_{N,q}$, содержащий $K_{\mathbf{y}} = \#(\mathcal{X} \cap \mathcal{B}_{N,q}(\mathbf{y}, s))$ кодовых слов, причём*

$$K_{\mathbf{y}} \geqslant M v_{N,q}(s)/q^N. \tag{2.2.38}$$

Доказательство. Разделим обе части равенства (2.2.37) на q^N. Тогда $\dfrac{1}{q^N} \sum\limits_{\mathbf{y}} K_{\mathbf{y}}$ будет средним числом кодовых слов в шаре $\mathcal{B}_{N,q}(\mathbf{y}, s)$. Но должен существовать шар, содержащий по крайней мере среднее количество кодовых слов. □

Шар $\mathcal{B}_{N,q}(\mathbf{y}, s)$, обладающий свойством (2.2.38), называется критическим (для кода $\mathcal{X}$).

Теорема 2.2.12 (неравенство Элайеса). *Положим $\theta = (q-1)/q$. Тогда для любого целого числа s со свойствами $1 \leqslant s < \theta N$ и $s^2 - 2\theta N s + \theta N d > 0$ максимальный размер $M_q^*(N, d)$ q-ичного кода длины N и с расстоянием d удовлетворяет неравенству*

$$M_q^*(N, d) \leqslant \frac{\theta N d}{s^2 - 2\theta N s + \theta N d} \cdot \frac{q^N}{v_{N,q}(s)}. \tag{2.2.39}$$

Доказательство. Фиксируем критический шар $\mathcal{B}_{N,q}(\mathbf{y}, s)$ и рассмотрим код $\mathcal{X}'$, полученный вычитанием слова $\mathbf{y}$ из кодовых слов кода

$\mathcal{X}$: $\mathcal{X}' = \{\mathbf{x} - \mathbf{y}\colon \mathbf{x} \in \mathcal{X}\}$. Код $\mathcal{X}'$ тоже будет $[N, M, d]$-кодом, так что мы можем предполагать, что $\mathbf{y} = \mathbf{0}$ и $\mathcal{B}_{N,q}(\mathbf{0}, s)$ — критический шар.

Будем обозначать через $w(x)$ вес слова x, см. (2.3.6). Возьмём $\mathcal{X}_1 = \mathcal{X} \cap \mathcal{B}_{N,q}(\mathbf{0}, s) = \{\mathbf{x} \in \mathcal{X}\colon w(\mathbf{x}) \leqslant s\}$. Код $\mathcal{X}_1$ будет кодом $[N, K, e]$, где $e \geqslant d$ и $K = K_0 \geqslant Mv_{N,q}(s)/q^N$. Как при доказательстве границы Плоткина, рассмотрим сумму расстояний между кодовыми словами в коде $\mathcal{X}_1$:

$$S_1 = \sum_{\mathbf{x} \in \mathcal{X}_1} \sum_{\mathbf{x}' \in \mathcal{X}_1} \delta(\mathbf{x}, \mathbf{x}').$$

Мы опять получаем $S_1 \geqslant K(K-1)e$. С другой стороны, если k_{ij} — число букв $j \in J_q = \{0, \ldots, q-1\}$, стоящих в i-й позиции во всех кодовых словах $\mathbf{x} \in \mathcal{X}$, то

$$S_1 = \sum_{i=1}^{N} \sum_{j=0}^{q-1} k_{ij}(K - k_{ij}).$$

Заметим, что $\sum\limits_{j=0}^{q-1} k_{ij} = K$. Кроме того, так как $w(\mathbf{x}) \leqslant s$, то число нулей в каждом слове $\mathbf{x} \in \mathcal{X}_1$ не меньше чем $N - s$. Тогда общее число нулей во всех кодовых словах составит $\sum\limits_{i=1}^{K} k_{i0} \geqslant K(N-s)$. Теперь запишем

$$S = NK^2 - \sum_{i=1}^{N} \left(k_{i0}^2 + \sum_{j=1}^{q-1} k_{ij}^2 \right),$$

и используем неравенство Коши—Шварца для доказательства следующего неравенства

$$\sum_{j=1}^{q-1} k_{ij}^2 \geqslant \frac{1}{q-1} \left(\sum_{j=1}^{q-1} k_{ij}^2 \right)^2 = \frac{1}{q-1}(K - k_{i0})^2.$$

Тогда

$$S \leqslant NK^2 - \sum_{i=1}^{N}\left(k_{i0}^2 + \frac{1}{q-1}(K-k_{i0})^2\right) =$$

$$= NK^2 - \frac{1}{q-1}\sum_{i=1}^{N}((q-1)k_{i0}^2 + K^2 - 2Kk_{i0} + k_{i0}^2) =$$

$$= NK^2 - \frac{1}{q-1}\sum_{i=1}^{N}(qk_{i0}^2 + K^2 - 2Kk_{i0}) =$$

$$= NK^2 - \frac{N}{q-1}K^2 - \frac{q}{q-1}\sum_{i=1}^{N}k_{i0}^2 + \frac{2}{q-1}K\sum_{i=1}^{N}k_{i0} =$$

$$= \frac{q-2}{q-1}NK^2 - \frac{q}{q-1}\sum_{i=1}^{N}k_{i0}^2 + \frac{2}{q-1}KL,$$

где $L = \sum\limits_{i=1}^{N} k_{i0}$. Применим неравенство Коши—Шварца ещё раз:

$$\sum_{i=1}^{N}k_{i0}^2 \geqslant \frac{1}{N}\left(\sum_{i=1}^{N}k_{i0}\right)^2 = \frac{1}{N}L^2.$$

Отсюда

$$S \leqslant \frac{q-2}{q-1}NK^2 - \frac{q}{q-1}\frac{1}{N}L^2 + \frac{2}{q-1}KL = \frac{1}{q-1}\left[(q-2)NK^2 - \frac{q}{N}L^2 + 2KL\right].$$

Квадратичное выражение в квадратных скобках достигает максимума в точке $L = NK/q$. Напомним, что $L \geqslant K(N-s)$, так что, выбирая $K(N-s) \geqslant NK/q$, т. е. $s \leqslant N(q-1)/q$, получаем, что

$$S \leqslant \frac{1}{q-1}\left[(q-2)NK^2 - \frac{q}{N}K^2(N-s)^2 + 2K^2(N-s)\right] =$$

$$= \frac{1}{q-1}K^2 s\left[2(q-1) - \frac{qs}{N}\right].$$

Отсюда следует неравенство $K(K-1)e \leqslant \dfrac{1}{q-1}K^2 s\left[2(q-1) - \dfrac{qs}{N}\right]$, которое можно разрешить относительно K:

$$K \leqslant \frac{\theta Ne}{s^2 - 2\theta Ns + \theta Ne}$$

в том случае, если $s < \theta N$ и $s^2 - 2\theta Ns + \theta Ne > 0$. Наконец, напомним, что код $\mathcal{X}_1$ получился из $[N, M, d]$-кода $\mathcal{X}$, $K \geqslant Mv(s)/q^N$ и $e \geqslant d$. Восполь-

зовавшись неравенством $s < \theta N$, получаем, что

$$\frac{Mv_{N,q}(s)}{q^N} \leqslant \frac{\theta N d}{s^2 - 2\theta N s + \theta N d},$$

что доказывает неравенство Элайеса (2.2.39). □

Весом $w(\mathbf{x})$ двоичного слова называется число его ненулевых знаков, см. (2.3.5). Значительный интерес представляют такие нелинейные коды, для которых вес любого слова постоянен, скажем $w(\mathbf{x}) \equiv l$, $\mathbf{x} \in \mathcal{X}$. Скалярное произведение $\langle \mathbf{x} \cdot \mathbf{y} \rangle$ векторов $\mathbf{x}, \mathbf{y} \in \mathcal{H}_N$ определено формулой (2.3.2). Идеи, применённые при доказательстве неравенства Элайеса (и при доказательстве границы Плоткина) также полезны при выводе ограничений на $W_2^*(N, d, l)$ — максимальный размер двоичного (нелинейного) кода $\mathcal{X} \in \mathcal{H}_{N,2}$ длины N с расстоянием $d(\mathcal{X}) \geqslant d$ и со свойством $w(\mathbf{x}) \equiv l$, $\mathbf{x} \in \mathcal{X}$. Сформулируем сначала три очевидных утверждения:

$$1) \quad W_2^*(N, 2k, k) = \left\lfloor \frac{N}{k} \right\rfloor, \quad 2) \quad W_2^*(N, 2k, l) = W_2^*(N, 2k, N - l)$$

и

$$3) \quad W_2^*(N, 2k - 1, l) = W_2^*(N, 2k, l), \quad l/2 \leqslant k \leqslant l.$$

(Их доказательство оставляется читателю в качестве упражнения.)

Пример 2.2.13. Докажите, что для любых натуральных чисел $N \geqslant 1$, $k \leqslant N/2$ и $l < N/2 - \sqrt{N^2/4 - kN}$ верно неравенство

$$W_2^*(N, 2k, l) \leqslant \left\lfloor \frac{kN}{l^2 - lN + kN} \right\rfloor. \tag{2.2.40}$$

Решение. Возьмём такой $[N, M, k]$-код $\mathcal{X}$, что $w(\mathbf{x}) \equiv l$, $\mathbf{x} \in \mathcal{X}$. Как и раньше, пусть k_{i1} обозначает число единиц на i-й позиции во всех кодовых словах. Рассмотрим сумму скалярных произведений

$$D = \sum_{\mathbf{x}, \mathbf{x}' \in \mathcal{X}} \mathbf{1}(\mathbf{x} \neq \mathbf{x}') \langle \mathbf{x} \cdot \mathbf{x}' \rangle.$$

Имеем

$$\langle \mathbf{x} \cdot \mathbf{x}' \rangle = w(\mathbf{x} \wedge \mathbf{x}') = \frac{1}{2}(w(\mathbf{x}) + w(\mathbf{x}') - \delta(\mathbf{x}, \mathbf{x}') \leqslant \frac{1}{2}(2l - 2k) = l - k.$$

Следовательно,

$$D \leqslant (l - k)M(M - 1).$$

С другой стороны, вклад в D из позиции i равен $k_{i1}(k_{i1} - 1)$, т. е.

$$D = \sum_{i=1}^{N} k_{i1}(k_{i1} - 1) = \sum_{i=1}^{N} (k_{i1}^2 - k_{i1}) = \sum_{i=1}^{N} k_{i1}^2 - lM.$$

Последняя сумма минимальна при $k_{i1} = lM/N$, т. е.

$$\frac{l^2M^2}{N} - lM \leqslant D \leqslant (l-k)M(M-1),$$

что немедленно приводит к формуле (2.2.40). □

Другая полезная граница устанавливается ниже.

Пример 2.2.14. Докажите, что для любых натуральных чисел $N \geqslant 1$, $k \leqslant N/2$ и $l \in [2k, 4k]$ верно неравенство

$$W_2^*(N, 2k, l) \leqslant \left\lfloor \frac{N}{l} W_2^*(N-1, 2k, l-1) \right\rfloor. \qquad (2.2.41)$$

Решение. Вновь возьмём такой $[N, M, k]$-код $\mathcal{X}$, что $w(\mathbf{x}) \equiv l \ \forall \mathbf{x} \in \mathcal{X}$. Рассмотрим сокращение кода $\mathcal{X}$ на $x_1 = 1$ (см. пример 2.1.8, п. 5); это будет код длины $(N-1)$ с расстоянием не меньше $2k$ и постоянным весом $l-1$. Следовательно, размер сокращённого кода не превосходит $W_2^*(N-1, 2k, l-1)$. Значит, число единиц на позиции 1 в кодовых словах кода $\mathcal{X}$ не превышает $W_2^*(N-1, 2k, l-1)$. Повторяя этот приём, мы получим, что общее число единиц во всех позициях не превосходит $NW_2^*(N-1, 2k, l-1)$. Но это число равно lM, т. е. $lM \leqslant NW_2^*(N-1, 2k, l-1)$, откуда следует неравенство (2.2.41). □

Следствие 2.2.15. *Для любых чисел $N \geqslant 1$, $k \leqslant N/2$ и $l \in [2k, 4k]$ верно неравенство*

$$W_2^*(N, 2k-1, l) = W_2^*(N, 2k, l) \leqslant$$
$$\leqslant \left\lfloor \frac{N}{l} \left\lfloor \frac{N-1}{l-1} \left\lfloor \dots \left\lfloor \frac{N-l+k}{k} \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor. \qquad (2.2.42)$$

Оставшаяся часть § 2.2 посвящена неравенству Джонсона, которое призвано усилить двоичную границу Хэмминга (см. теорему 2.1.6).

$$M_2^*(N, 2E+1) \leqslant 2^N/v_N(E), \quad \text{или} \quad v_N(E)M_2^*(N, 2E+1) \leqslant 2^N. \qquad (2.2.43)$$

А именно, неравенство Джонсона утверждает, что

$$M_2^*(N, 2E+1) \leqslant 2^N/v_N^*(E) \quad \text{или} \quad v_N^*(E)M_2^*(N, 2E+1) \leqslant 2^N, \qquad (2.2.44)$$

где

$$v_N^*(E) = v_N(E) + \frac{1}{\lceil N/(E+1) \rceil}[C_N^{E+1} - W_2^*(N, 2E+1, 2E+1)C_{2E+1}^E] \qquad (2.2.45)$$

Напомним, что $v_N(E) = \sum\limits_{s=0}^{E} C_N^s$ обозначает объём двоичного шара Хэмминга радиуса E. Мы начнём вывод неравенства (2.2.44) с леммы, доказательство которой — полезное упражнение.

Лемма 2.2.16. *Если* $\mathbf{x}$, $\mathbf{y}$ — *двоичные слова*, $\delta(\mathbf{x}, \mathbf{y}) = 2l + 1$, *то найдётся* C_{2l+1}^{l} *таких двоичных слов* $\mathbf{z}$, *что* $\delta(\mathbf{x}, \mathbf{z}) = l + 1$ *и* $\delta(\mathbf{y}, \mathbf{z}) = l$.

Рассмотрим множество $T(= T_{N,E+1})$ всех двоичных N-слов, лежащих в точности на расстоянии $E + 1$ от кодовых слов кода $\mathcal{X}$:

$$T = \{\mathbf{z} \in \mathcal{H}_N \colon \delta(\mathbf{z}, \mathbf{x}) = E + 1 \text{ для некоторого } \mathbf{x} \in \mathcal{X} \text{ и } \delta(\mathbf{z}, \mathbf{y}) \geqslant E + 1 \ \forall \mathbf{y} \in \mathcal{X}\}. \quad (2.2.46)$$

Тогда можно написать, что

$$M v_N(E) + \#T \leqslant 2^N, \quad (2.2.47)$$

поскольку ни одно слово из множества T не попадает в шар радиуса E с центром в кодовом слове $\mathbf{y}$. Теперь неравенство Джонсона (2.2.44) будет следовать из примера 2.2.17.

Пример 2.2.17. Докажите, что размер $\#T$ не меньше второго члена п. ч. формулы (2.2.45):

$$\frac{M}{\lceil N/(E+1) \rceil}[C_N^{E+1} - W_2^*(N, 2E+1, 2E+1) C_{2E+1}^{E}]. \quad (2.2.48)$$

Решение. Мы хотим отыскать нижнюю границу для $\#T$. Рассмотрим множество $\mathcal{W}(= \mathcal{W}_{N,E+1})$ «согласованных» пар N-слов, определённое следующим образом:

$$\mathcal{W} = \{(\mathbf{x}, \mathbf{z}) \colon \mathbf{x} \in \mathcal{X}, \mathbf{z} \in T_{E+1}, \ \delta(\mathbf{x}, \mathbf{z}) = E+1\} =$$
$$= \{(\mathbf{x}, \mathbf{z}) \colon \mathbf{x} \in \mathcal{X}, \mathbf{z} \in \mathcal{H}_N \colon \delta(\mathbf{x}, \mathbf{z}) = E+1 \text{ и } \delta(\mathbf{y}, \mathbf{z}) \geqslant E+1 \ \forall \mathbf{y} \in \mathcal{X}\}. \quad (2.2.49)$$

Для фиксированного $\mathbf{x} \in \mathcal{X}$ $\mathbf{x}$-сечение $\mathcal{W}^{\mathbf{x}}$ определяется так:

$$\mathcal{W}^{\mathbf{x}} = \{\mathbf{z} \in \mathcal{H}_N \colon (\mathbf{x}, \mathbf{z}) \in \mathcal{W}\} =$$
$$= \{\mathbf{z} \colon \delta(\mathbf{x}, \mathbf{z}) = E + 1, \ \ \delta(\mathbf{y}, \mathbf{z}) \geqslant E + 1 \ \forall \mathbf{y} \in \mathcal{X}\}. \quad (2.2.50)$$

Заметим, что если $\delta(\mathbf{x}, \mathbf{z}) = E + 1$, то $\delta(\mathbf{y}, \mathbf{z}) \geqslant E + 1 \ \forall \mathbf{y} \in \mathcal{X} \setminus \{\mathbf{x}\}$, так как в противном случае $\delta(\mathbf{x}, \mathbf{y}) < 2E + 1$. Следовательно,

$$\mathcal{W}^{\mathbf{x}} = \{\mathbf{z} \colon \delta(\mathbf{x}, \mathbf{z}) = E + 1, \ \ \delta(\mathbf{y}, \mathbf{z}) \neq E \ \forall \mathbf{y} \in \mathcal{X}\}. \quad (2.2.51)$$

Мы видим, что для оценки $\#\mathcal{W}^{\mathbf{x}}$ мы должны вычесть из числа двоичных N-слов, лежащих на расстоянии $E + 1$ от $\mathbf{x}$, т. е. из C_N^{E+1}, число слов, лежащих также на расстоянии E от некоторого другого кодового слова $\mathbf{y} \in \mathcal{X}$. Но если $\delta(\mathbf{x}, \mathbf{z}) = E + 1$ и $\delta(\mathbf{y}, \mathbf{z}) = E$, то $\delta(\mathbf{x}, \mathbf{y}) = 2E + 1$. Кроме того никакая пара различных кодовых слов не можем находиться на расстоянии E от одного и того же N-слова $\mathbf{z}$. Значит, по предыдущему замечанию

$$\#\mathcal{W}^{\mathbf{x}} = C_N^{E+1} - C_{2E+1}^{E} \times \#\{\mathbf{y} \in \mathcal{X} \colon \delta(\mathbf{x}, \mathbf{y}) = 2E + 1\}.$$

Более того, если вычесть $\mathbf{x}$ из каждого $\mathbf{y} \in \mathcal{X}$, для которого $\delta(\mathbf{x}, \mathbf{y}) = 2E+1$, то в результате получится код длины N, у которого вес кодового слова $\mathbf{z}$ будет равен $w(\mathbf{z}) \equiv 2E+1$. Следовательно, найдётся не более чем $W^*(N, 2E+1, 2E+1)$ таких кодовых слов $\mathbf{y} \in \mathcal{X}$, что $\delta(\mathbf{x}, \mathbf{y}) = 2E+1$. Значит,

$$\#\mathcal{W}^{\mathbf{x}} \geqslant C_N^{E+1} - \mathcal{W}^*(N, 2E+1, 2E+1) C_{2E+1}^{E}, \tag{2.2.52}$$

и

$$\#\mathcal{W} \geqslant M \times \text{п. ч. формулы (2.2.52)}. \tag{2.2.53}$$

Теперь зафиксируем $\mathbf{v} \in T$ и рассмотрим $\mathbf{v}$-сечение

$$\mathcal{W}^{\mathbf{v}} = \{\mathbf{y} \in \mathcal{X} \colon (\mathbf{y}, \mathbf{v}) \in \mathcal{W}\} = \{\mathbf{y} \in \mathcal{X} \colon \delta(\mathbf{y}, \mathbf{v}) = E+1\}. \tag{2.2.54}$$

Если $\mathbf{y}, \mathbf{z} \in \mathcal{W}^{\mathbf{v}}$, то $\delta(\mathbf{y}, \mathbf{v}) = \delta(\mathbf{z}, \mathbf{v}) = E+1$, откуда

$$w(\mathbf{y} - \mathbf{v}) = w(\mathbf{z} - \mathbf{v}) = E+1$$

и

$$\begin{aligned} 2E+1 \leqslant \delta(\mathbf{y}, \mathbf{z}) &= \delta(\mathbf{y} - \mathbf{v}, \mathbf{z} - \mathbf{v}) = \\ &= w(\mathbf{y} - \mathbf{v}) + w(\mathbf{z} - \mathbf{v}) - 2w((\mathbf{y} - \mathbf{v}) \wedge (\mathbf{z} - \mathbf{v})) = \\ &= 2E + 2 - 2w((\mathbf{y} - \mathbf{v}) \wedge (\mathbf{z} - \mathbf{v})). \end{aligned}$$

Отсюда вытекает, что

$$w((\mathbf{y} - \mathbf{v}) \wedge (\mathbf{z} - \mathbf{v})) = 0 \quad \text{и} \quad \delta(\mathbf{y}, \mathbf{z}) = 2E+2.$$

Таким образом, $\mathbf{y} - \mathbf{v}$ и $\mathbf{z} - \mathbf{v}$ не имеют единиц на общих позициях. Следовательно, найдётся не более чем $\lceil N/(E+1) \rceil$ слов вида $\mathbf{y} - \mathbf{v}$, где $\mathbf{y} \in \mathcal{W}^{\mathbf{v}}$, т. е. сечение $\mathcal{W}^{\mathbf{v}}$ насчитывает не более чем $\lceil N/(E+1) \rceil$ слов. Значит,

$$\#\mathcal{W} \leqslant \left\lceil \frac{N}{E+1} \right\rceil \#T. \tag{2.2.55}$$

Из формул (2.2.52), (2.2.53) и (2.2.55) вытекает неравенство (2.2.48). □

С помощью следствия 2.2.15 мы получаем ещё одно следствие.

Следствие 2.2.18. *Имеет место следующее неравенство*:

$$M^*(N, 2E+1) \leqslant 2^N \left[\upsilon_N(E) - \frac{1}{\lceil N/(E+1) \rceil} C_N^E \left(\frac{N-E}{E+1} - \left\lfloor \frac{N-E}{E+1} \right\rfloor \right) \right]^{-1}. \tag{2.2.56}$$

□

Пример 2.2.19. Пусть $N = 13$ и $E = 2$, т. е. $d = 5$. Из неравенства (2.2.42) следует, что $\mathcal{W}^*(13, 5, 5) \leqslant \left\lfloor \frac{13}{5} \left\lfloor \frac{12}{4} \left\lfloor \frac{11}{3} \right\rfloor \right\rfloor \right\rfloor = 23$, а из неравенства

Джонсона (2.2.44) следует, что

$$M^*(13,\,5) \leqslant \left\lfloor \frac{2^{13}}{1+13+78+(286-10\times 23)/4} \right\rfloor = 77.$$

Это ограничение намного лучше границы Хэмминга, по которой $M^*(13,\,5) \leqslant 89$. На самом деле из границы линейного программирования известно, что $M^*(13,\,5) \leqslant 64$ (см. § 3.4). □

Strictly Hamming Ballroom Dirty Dancing[3]

(Из серии «Фильмы, которые не вышли на большой экран».)

Размер (кода) имеет значение.

(Из серии «Так говорил суперлектор».)

§ 2.3. Линейные коды: основные конструкции

> Есть цвета с такими длинами волн, что люди не могут их видеть, есть звуки, которые человек не слышит, и, возможно, у компьютеров есть мысли, которые люди не могут понять.
>
> *Ричард Хэмминг* (1915–1998),
> американский математик и программист

В этом параграфе изучается класс линейных кодов. Для начала ограничимся двоичными кодами. Соответственно $\mathcal{H}_N$ будет обозначать двоичное пространство Хэмминга длины N; слова, $\mathbf{x}^{(N)} = x_1 \dots x_N$ из $\mathcal{H}_N$ будем также называть (строковыми) векторами. Все операции над двоичными цифрами выполняются в двоичной арифметике (т. е. по $\bmod 2$). Когда это не приводит к недоразумению, мы будем опускать индексы N. Повторим определение линейного кода (см. определение 2.1.5).

Определение 2.3.1. Двоичный код $\mathcal{X} \subseteq \mathcal{H}_N$ называется *линейным*, если вместе с парой векторов $\mathbf{x} = x_1 \dots x_N$ и $\mathbf{x}' = x'_1 \dots x'_N$ он содержит сумму $\mathbf{x} + \mathbf{x}'$ со знаками $x_i + x'_i$. Иначе говоря, линейный код — это *линейное подпространство* в $\mathcal{H}_N$ над полем $\mathbb{F}_2 = \{0,\,1\}$. Следовательно, линейный код всегда содержит нулевую вектор-строку $\mathbf{0} = 0 \dots 0$. *Базис* линейного кода $\mathcal{X}$ — это максимальная линейно независимая система слов из $\mathcal{X}$; линейный код *порождается* своим базисом в том смысле, что каждый вектор $\mathbf{x} \in \mathcal{X}$ (однозначно) представляется в виде суммы (некоторых) векторов базиса. Все базисы данного линейного кода состоят из

[3] Ср. с названием фильмов «Strictly Ballroom» и «Dirty Dancing» (хиты 1990-х годов).

одного и того же числа элементов, которое называется *размерностью* или *рангом* кода $\mathcal{X}$. Линейный код длины N и ранга k называют также $[N, k]$-кодом или $[N, k, d]$-кодом, если его расстояние равно d. □

Практически все коды, используемые на современном этапе на практике, относятся к линейным. Их популярность объясняется лёгкостью работы с ними. Например, для идентификации линейного кода достаточно зафиксировать его базис, что, как будет видно из дальнейшего, даёт существенную экономию.

Лемма 2.3.2. *Любой двоичный линейный код ранга k содержит 2^k векторов, т. е. его размер $M = 2^k$.*

Доказательство. Базис этого кода содержит k линейно независимых векторов. Код порождается базисом, значит, он состоит из сумм базисных векторов. Но существует ровно 2^k таких сумм (число подмножеств в $\{1, \ldots, k\}$, соответствующих слагаемым). Все они дают разные векторы. □

Следовательно, линейный двоичный код ранга k можно использовать для кодирования *всех* возможных строк источника длины k. Скорость передачи информации двоичного линейного $[N, k]$-кода равна k/N. Таким образом, указывая $k \leqslant N$ линейно независимых слов $\mathbf{x} \in \mathcal{H}_N$, мы задаём (единственный) линейный код $\mathcal{X} \subset \mathcal{H}_N$ ранга k. Иначе говоря, линейный двоичный код ранга k характеризуется $k \times N$-матрицей из нулей и единиц с линейно независимыми строками

$$G = \begin{pmatrix} g_{11} & \ldots & \ldots & \ldots & g_{1N} \\ g_{21} & \ldots & \ldots & \ldots & g_{2N} \\ & \vdots & & \vdots & \\ g_{k1} & \ldots & \ldots & \ldots & g_{kN} \end{pmatrix}.$$

А именно, мы рассматриваем строку $\mathbf{g}(i) = g_{i1} \ldots g_{iN}$, $1 \leqslant i \leqslant k$, как базисный вектор линейного кода.

Определение 2.3.3. Матрица G называется *образующей матрицей* линейного кода. Ясно, что образующая матрица далеко не единственная.

Линейный $[N, k]$-код $\mathcal{X}$ можно эквивалентно описать как ядро подходящей $(N - k) \times N$-матрицы H тоже с 0 и 1 в качестве элементов: $\mathcal{X} = \ker H$, где

$$\begin{pmatrix} h_{11} & h_{12} & \ldots & \ldots & h_{1N} \\ h_{21} & h_{22} & \ldots & \ldots & h_{2N} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ h_{(N-k)1} & h_{(N-k)2} & \ldots & \ldots & h_{(N-k)N} \end{pmatrix}$$

и

$$\ker H = \{\mathbf{x} = x_1 \ldots x_N \colon \mathbf{x}H^{\mathrm{T}} = \mathbf{0}^{(N-k)}\}. \tag{2.3.1}$$

Ясно, что строки $\mathbf{h}(j)$, $1 \leqslant j \leqslant N-k$, матрицы H — векторы, ортогональные $\mathcal{X}$ в смысле скалярного произведения:

$$\langle \mathbf{x} \cdot \mathbf{h}(j) \rangle = 0 \ \forall \mathbf{x} \in \mathcal{X},\ 1 \leqslant j \leqslant N-k.$$

Здесь для $\mathbf{x}, \mathbf{y} \in \mathcal{H}_N$ скалярное произведение определяется как

$$\langle \mathbf{x} \cdot \mathbf{y} \rangle = \langle \mathbf{y} \cdot \mathbf{x} \rangle = \sum_{i=1}^{N} x_i y_i, \quad \text{где } \mathbf{x} = x_1 \dots x_N,\ \ \mathbf{y} = y_1 \dots y_N. \tag{2.3.2}$$

Скалярное произведение (2.3.2) обладает всеми свойствами евклидова скалярного произведения в $\mathbb{R}^N$, кроме одного: оно не является положительно определённым (и, следовательно, не определяет нормы), т. е. существует такой ненулевой вектор $\mathbf{x} \in \mathcal{H}_N$, что $\langle \mathbf{x} \cdot \mathbf{x} \rangle = 0$. К счастью, нам не нужно положительной определённости.

Тем не менее свойство дополнительности остаётся в силе: если $\mathcal{L}$ — линейное подпространство в $\mathcal{H}_N$ ранга k, то ранг его ортогонального дополнения $\mathcal{L}^\perp$ (т. е. множества таких векторов $\mathbf{z} \in \mathcal{H}_N$, что $\langle \mathbf{x} \cdot \mathbf{z} \rangle = 0 \ \forall \mathbf{x} \in \mathcal{L}$), которое тоже оказывается линейным подпространством, равен $N-k$. Таким образом, $(N-k)$-строчки матрицы H можно рассматривать как базис пространства $\mathcal{X}^\perp$ — ортогонального дополнения к $\mathcal{X}$.

Матрица H (или иногда транспонированная к ней H^{T}) со свойством $\mathcal{X} = \ker H$, или $\langle \mathbf{x} \cdot \mathbf{h}(j) \rangle \equiv 0$ (см. (2.3.1))) называется матрицей *проверки на чётность* (или просто проверочной) кода $\mathcal{X}$. Во многих случаях описание кода через проверочную матрицу оказывается более удобным, чем через порождающую матрицу. □

Матрица проверки на чётность тоже не единственная, поскольку базис в $\mathcal{X}^\perp$ выбирается не однозначно. Кроме того, в некоторых ситуациях, когда рассматривается семейство кодов разных длин N, более естественно рассматривать проверочные матрицы с числом строк, превышающим $N-k$ (но некоторые из них линейно зависимы); такой пример появится в гл. 3. Однако пока мы будем представлять себе матрицу H как $(N-k) \times N$-матрицу с линейно независимыми строками.

Пример 2.3.4. Пусть $\mathcal{X}$ — двоичный линейный $[N, k, d]$-код со скоростью передачи информации $\rho = k/N$. Пусть G и H соответственно обозначают порождающую и проверочную матрицы кода $\mathcal{X}$. В этом примере мы ссылаемся на конструкции, введённые в примере 2.1.8.

1. Продолжение проверкой на чётность кода $\mathcal{X}$ — это двоичный код $\mathcal{X}^+$ длины $N+1$, полученный добавлением к каждому кодовому слову $\mathbf{x} \in \mathcal{X}$ символа $x_{N+1} = \sum_{i=1}^{N} x_i$, так что сумма $\sum_{i=1}^{N+1} x_i$ будет нулевой. Докажите, что $\mathcal{X}^+$ — линейный код, найдите его ранг и минимальное расстояние.

Как соотносятся скорости передачи информации, порождающие матрицы и матрицы проверки на чётность кодов $\mathcal{X}$ и $\mathcal{X}^+$?

2. Усечение $\mathcal{X}^-$ кода $\mathcal{X}$ определяется как линейный код длины $N-1$, полученный отбрасыванием последнего символа у каждого кодового слова $\mathbf{x} \in \mathcal{X}$. Предположим, что минимальное расстояние кода $\mathcal{X}$ равно $d \geqslant 2$. Докажите, что код $\mathcal{X}^-$ линеен, найдите его ранг, порождающую и проверочную матрицы. Покажите, что минимальное расстояние кода $\mathcal{X}^-$ не меньше $d-1$.

3. m-повторение кода $\mathcal{X}$ — это код $\mathcal{X}^{\mathrm{re}}(m)$ длины Nm, получающийся повторением каждого кодового слова m раз. Докажите, что код $\mathcal{X}^{\mathrm{re}}(m)$ линеен, найдите его ранг и минимальное расстояние. Как связаны скорости передачи информации и порождающая и проверочная матрицы кодов $\mathcal{X}^{\mathrm{re}}(m)$ и $\mathcal{X}$?

Решение. 1. Порождающая и проверочная матрицы имеют вид

$$G^+ = \begin{pmatrix} \sum\limits_{i=1}^{N} g_{1i} \\ \vdots \\ G \quad \vdots \\ \sum\limits_{i=1}^{N} g_{1i} \end{pmatrix}, \qquad H^+ = \left(\begin{array}{c|c} & 1 \\ & 1 \\ H & \vdots \\ & 1 \\ \hline 0\ldots0 & 1 \end{array}\right).$$

Ранги кодов $\mathcal{X}^+$ и $\mathcal{X}$ совпадают. Если минимальное расстояние кода $\mathcal{X}$ было чётным, то оно не изменится при переходе к коду $\mathcal{X}^+$, а если нечётным, то увеличится на 1. Скорость передачи информации станет равной $\rho^+ = N\rho/(N+1)$.

2. Порождающая матрица G^- получается отбрасыванием последнего столбца. Проверочную матрицу кода $\mathcal{X}^-$ можно отождествить с блоком проверочной матрицы H кода $\mathcal{X}$ после некоторых операций над столбцами:

$$G^- = \begin{pmatrix} g_{11} & \cdots & g_{1N-1} \\ & \vdots & \\ & \vdots & \\ & \vdots & \\ g_{k1} & \cdots & g_{kN-1} \end{pmatrix}, \qquad H = \left(\begin{array}{c|c} & \cdot \\ & \cdot \\ H^- & \vdots \\ & \cdot \\ \hline 0\ldots0 & * \end{array}\right).$$

Ранг не изменится, расстояние может уменьшится максимум на 1, а скорость передачи информации станет равной $\rho^- = N\rho/(N-1)$.

3. Образующая и проверочная матрицы выглядят следующим образом:

$$G^{\mathrm{re}}(m) = (\underbrace{G \dots G}_{m \text{ раз}})$$

и

$$H^{\mathrm{re}}(m) = \begin{pmatrix} H & 0 & 0 & \dots & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \dots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{1} \end{pmatrix}.$$

Здесь $\mathbf{1}$ — единичная $(N \times N)$ матрица, а 0 и $\mathbf{0}$ — нулевые матрицы (размера $(N-k) \times N$ и $N \times N$ соответственно). Число единичных матриц в первом столбце равно $m-1$ (это не единственный вид матрицы $H^{\mathrm{re}}(m)$.) Размер матрицы $H^{\mathrm{re}}(m)$ равен $(Nm-k) \times Nm$.

Ранг не изменится, минимальное расстояние кода $\mathcal{X}^{\mathrm{re}}(m)$ составит md, а скорость передачи информации уменьшится до ρ/m. □

Пример 2.3.5. Двойственный код линейного двоичного $[N, k]$-кода $\mathcal{X}$ определяется как множество $\mathcal{X}^{\perp}$ таких слов $\mathbf{y} = y_1 \dots y_N$, что

$$\langle \mathbf{y} \cdot \mathbf{x} \rangle = \sum_{i=1}^{N} y_i \cdot x_i = 0 \quad \text{для каждого } \mathbf{x} = x_1 \dots x_N \text{ из } \mathcal{X}$$

(см. пример 2.1.8, 9). Докажите, что матрица H размера $(N-k) \times N$ является проверочной матрицей кода $\mathcal{X}$ тогда и только тогда, когда она является порождающей матрицей двойственного кода. Выведите отсюда, что G и H являются порождающей и проверочной матрицей соответственно тогда и только тогда, когда

1) строки матрицы G линейно независимы,
2) столбцы матрицы H линейно независимы,
3) число строк матрицы G плюс число строк матрицы H равно числу столбцов матрицы G плюс числу столбцов матрицы H,
4) $GH^{\mathrm{T}} = 0$.

Решение. Строки $\mathbf{h}(j)$, $j = 1, \dots, N$ матрицы H удовлетворяют условию: $\langle \mathbf{x} \cdot \mathbf{h}(j) \rangle \equiv 0$, $\mathbf{x} \in \mathcal{X}$. Более того, если вектор $\mathbf{y}$ тоже обладает таким свойством: $\langle \mathbf{x} \cdot \mathbf{y} \rangle \equiv 0$, $\mathbf{x} \in \mathcal{X}$, то $\mathbf{y}$ — линейная комбинация строк $\mathbf{h}(j)$. Значит, H — порождающая матрица кода $\mathcal{X}^{\perp}$. С другой стороны, любая порождающая матрица для $\mathcal{X}^{\perp}$ является проверочной матрицей $\mathcal{X}$.

Следовательно, для любой пары G, H, представляющей образующую и проверочную матрицы линейного кода п. 1, 2 и 4 выполнены по опреде-

лению, а п. 3 следует из ортогонального разложения.

$$\mathcal{H}_N = (\text{пространство строк } G) \oplus (\text{пространство столбцов } H),$$

что является следствием п. 4 и максимальности матриц G и H.

С другой стороны, любая пара матриц G, H, удовлетворяющая свойствам п. 1–4, обладает свойством максимальности (на основании п. 1–3) и ортогональности п. 4. Таким образом, они являются порождающей и проверочной матрицей кода $\mathcal{X}$, равному пространству строк матрицы G. □

Пример 2.3.6. Сколько кодовых слов имеет двоичный линейный $[N, k]$-код? Сколько различных базисов в нём? Подсчитайте число базисов при $k = 4$. Перечислите все базисы при $k = 2$ и $k = 3$.

Покажите, что подмножество линейного двоичного кода, состоящее из всех слов чётного веса, тоже является линейным кодом. Пусть d — чётное число. Покажите, что если существует линейный $[N, k, d]$-код, то найдётся линейный $[N, k, d]$-код с кодовыми словами чётного веса.

Решение. Размер кода равен 2^k, а число различных базисов равно $\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$. Действительно, если l первых базисных векторов уже выбрано, все 2^l линейные комбинации этих векторов нужно исключить из следующего шага. Это даёт 840 для $k = 4$ и 28 для $k = 3$.

Наконец, если d — чётное число, то мы можем усечь исходный код и затем использовать расширение проверкой на чётность. □

Пример 2.3.7. Двоичный $[7, 4]$-код Хэмминга определяется проверочной матрицей 3×7. Столбцы этой матрицы — ненулевые слова длины 3. Упорядочив эти слова длины 3 лексикографически, мы получим

$$H_{\text{lex}}^{\text{Ham}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{2.3.3}$$

Соответствующую порождающую матрицу можно записать как

$$G_{\text{lex}}^{\text{Ham}} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.3.4}$$

□

Во многих случаях удобно записывать проверочную матрицу линейного $[N, k]$-кода в *каноническом* (или стандартном) виде:

$$H_{\text{can}} = (\mathbf{1}_{N-k} H'). \tag{2.3.5a}$$

Для [7, 4]-кода Хэмминга отсюда получаем

$$H_{\text{can}}^{\text{Ham}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

Канонический вид определён и для порождающей матрицы:

$$G_{\text{can}} = (G' \mathbf{1}_k). \tag{2.3.5б}$$

А именно,

$$G_{\text{can}}^{\text{Ham}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

С формальной точки зрения матрицы G_{lex} и G_{can} определяют *разные* коды. Однако эти коды будут *эквивалентны*.

Определение 2.3.8. Два кода называются *эквивалентными*, если они отличаются друг от друга только перестановкой символов в кодовых словах. Для линейных кодов эквивалентность означает, что их порождающие матрицы могут получаться друг из друга перестановкой столбцов и операциями над строками, состоящими в сложении и умножении строк на скаляры. Ясно, что эквивалентные коды имеют одинаковые параметры (длину, ранг, расстояние). □

В дальнейшем мы не будем различать эквивалентные линейные коды.

Замечание 2.3.9. Преимущество записи G в каноническом виде заключается в том, что строка источника $\mathbf{u}^{(k)} \in \mathcal{H}_k$ кодируется в виде N-вектора $\mathbf{u}^{(k)} G_{\text{can}}$; согласно формуле (2.3.5б) последние k цифр в $\mathbf{u}^{(k)} G_{\text{can}}$ образуют слово $\mathbf{u}^{(k)}$ (они называются информационными цифрами), в то время как первые $N - k$ цифр предназначены для проверки чётности (и называется цифрами проверки чётности). Наглядно, цифры проверки чётности несут в себе избыточность, что позволяет декодеру обнаруживать и исправлять ошибки. □

> Like following life thro' creatures you dissect
> You lose it at the moment you detect.
>
> Подобно жизни, вы создаёте то, что разрушаете, и теряете это в момент, когда обнаруживаете.
>
> *Александр Поп* (1668–1744),
> английский поэт

Определение 2.3.10. *Весом* $w(\mathbf{x})$ двоичного слова $\mathbf{x} = x_1 \dots x_N$ называется число ненулевых знаков в $\mathbf{x}$:

$$w(x) = \#\{i\colon 1 \leqslant i \leqslant N,\ \ x_i \neq 0\}. \tag{2.3.6}$$

□

Теорема 2.3.11. 1. *Расстояние линейного двоичного кода* (*см. формулу* (2.1.5)) *совпадает с минимальным весом ненулевого кодового слова.*

2. *Расстояние линейного двоичного кода равно минимальному числу линейно зависимых столбцов проверочной матрицы.*

Доказательство. 1. Так как код $\mathcal{X}$ линеен, сумма $\mathbf{x} + \mathbf{y} \in \mathcal{X}$ для каждой пары кодовых слов $\mathbf{x}, \mathbf{y} \in \mathcal{X}$. Расстояние Хэмминга инвариантно относительно сдвигов (см. лемму 2.1.1), поэтому $\delta(\mathbf{x}, \mathbf{y}) = \delta(0, \mathbf{x} + \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$ для любой пары кодовых слов. Следовательно, минимальное расстояние $\mathcal{X}$ равно минимальному расстоянию от $\mathbf{0}$ до остального кода, т. е. минимальному весу ненулевого кодового слова из $\mathcal{X}$.

2. Пусть $\mathcal{X}$ — линейный код с проверочной матрицей H и минимальным расстоянием d. Тогда существует кодовое слово $\mathbf{x} \in \mathcal{X}$, у которого ровно d ненулевых знаков. Так как $\mathbf{x}H^{\mathrm{T}} = 0$, можно заключить, что найдётся d столбцов матрицы H, которые будут линейно зависимы (они соответствуют ненулевым знакам слова $\mathbf{x}$). С другой стороны, если найдётся $d - 1$ линейно зависимый столбец, то их сумма будет равна нулю. Но это означает, что найдётся такое слово $\mathbf{y}$ веса $w(\mathbf{y}) = d - 1$, что $\mathbf{y}H^{\mathrm{T}} = 0$. Поэтому $\mathbf{y} \in \mathcal{X}$, что невозможно, так как $\min[w(\mathbf{x})\colon \mathbf{x} \in \mathcal{X},\ \mathbf{x} \neq \mathbf{0}] = d$. □

Теорема 2.3.12. [7, 4]-*код Хэмминга имеет минимальное расстояние* 3, *т. е. обнаруживает две ошибки и исправляет одну. Более того, это совершенный код, исправляющий одну ошибку.*

Доказательство. Вместе с любой парой столбцов проверочная матрица H^{lex} содержит их сумму, чтобы получилась линейно зависимая тройка (например, столбцы 1, 6, 7 в формуле (2.3.3)). Любые два из них линейно независимы, поскольку они различны (равенство $\mathbf{x} + \mathbf{y} = \mathbf{0}$ означает, что $\mathbf{x} = \mathbf{y}$). Кроме того, $v_7(1) = 1 + 7 = 2^3$, и код совершенен, поскольку размер равен 2^4 и $2^4 \times 2^3 = 2^7$. □

Конструкция [7, 4]-кода Хэмминга допускает прямое обобщение на коды длины $N = 2^l - 1$. А именно, рассмотрим $(2^l - 1) \times l$-матрицу H^{Ham}, столбцы которой представляют все возможные ненулевые двоичные век-

торы длины l:

$$H^{\mathrm{Ham}} = \begin{pmatrix} 1 & 0 & \dots & 0 & 1 & \dots & 1 \\ 0 & 1 & \dots & 0 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 1 \end{pmatrix}. \tag{2.3.7}$$

Строки матрицы H^{Ham} линейно независимы, и поэтому, H^{Ham} можно рассматривать как проверочную матрицу линейного кода длины $N = 2^l - 1$ и ранга $N - l = 2^l - 1 - l$. Любые два столбца матрицы H^{Ham} линейно независимы, но существуют линейно зависимые тройки столбцов, например, $\mathbf{x}$, $\mathbf{y}$ и $\mathbf{x} + \mathbf{y}$. Значит, минимальное расстояние кода $\mathcal{X}^{\mathrm{Ham}}$ равно 3, т. е. он обнаруживает две и исправляет одну ошибку.

Такой код называется $[2^l - 1,\, 2^l - 1 - l]$-кодом Хэмминга. Он является совершенным кодом, исправляющим одну ошибку: объём шара равен $v_{2^l-1}(1) = 1 + 2^l - 1 = 2^l$, а произведение размера на объём составляет $2^{2^l-1-l} \times 2^l = 2^{2^l-1} = 2^N$. Скорость передачи информации $\dfrac{2^l - 1 - l}{2^l - 1} \to 1$ при $l \to \infty$. Это доказывает следующую теорему.

Теорема 2.3.13. *Изложенная выше конструкция определяет семейство* $[2^l - 1,\, 2^l - 1 - l,\, 3]$ *линейных двоичных кодов* $\mathcal{X}^{\mathrm{Ham}}_{2^l-1}$, $l = 1, 2, \dots$, *являющихся совершенными, исправляющими одну ошибку кодами.*

Пример 2.3.14. Предположим, что вероятность ошибки в любом знаке равна $p \ll 1$ вне зависимости от того, что происходит с другими знаками. Тогда ошибка при передаче некодированного $4N$-значного сообщения составит

$$1 - (1 - p)^{4N} \simeq 4Np.$$

Но при использовании $[7, 4]$-кода нам нужно передать $7N$ знаков. Передача ошибочна, если неверны по крайней мере два знака, что получается с вероятностью приближённо равной

$$1 - (1 - C_7^2 p^2)^N \simeq 21Np^2 \ll 4Np.$$

Мы видим, что дополнительные усилия при использовании трёх контрольных знаков в коде Хэмминга оправданы. □

Стандартная процедура декодирования линейных кодов основана на понятиях «смежный класс» и «синдром». Напомним, что правило декодирования м. п. декодирует вектор $\mathbf{y} = y_1, \dots, y_N$ ближайшим кодовым словом $\mathbf{x} \in \mathcal{X}$.

Определение 2.3.15. Пусть $\mathcal{X}$ — двоичный линейный код длины N и $\mathbf{w} = w_1 \dots w_N$ — слово из $\mathcal{H}_N$. *Смежным классом* кода $\mathcal{X}$, определённым

словом $\mathbf{w}$, называется множество двоичных векторов вида $\mathbf{w}+\mathbf{x}$, где $\mathbf{x}\in\mathcal{X}$. Мы будем обозначать его $\mathbf{w}+\mathcal{X}$. □

Сформулируем лёгкое (и полезное) упражнение по линейной алгебре.

Пример 2.3.16. Пусть $\mathcal{X}$ — двоичный линейный код, а $\mathbf{w}$, $\mathbf{v}$ — слова длины N. Тогда

1) если $\mathbf{w}$ попало в смежный класс $\mathbf{v}+\mathcal{X}$, то $\mathbf{v}$ лежит в смежном классе $\mathbf{w}+\mathcal{X}$; иначе говоря, любое слово смежного класса определяет его;

2) $\mathbf{w}\in\mathbf{w}+\mathcal{X}$;

3) $\mathbf{w}$ и $\mathbf{v}$ лежат в одном смежном классе тогда и только тогда, когда $\mathbf{w}+\mathbf{v}\in\mathcal{X}$;

4) каждое слово длины N лежит в одном и только одном смежном классе, иными словами, смежные классы образуют разбиение всего пространства Хэмминга $\mathcal{H}_N$;

5) количество слов в любом смежном классе равно $\#\mathcal{X}$; если ранг кода $\mathcal{X}$ равен k, то существует 2^{N-k} различных смежных класса, каждый из которых содержит 2^k слов; код $\mathcal{X}$ является смежным классом любого кодового слова;

6) смежный класс, определённый словом $\mathbf{w}+\mathbf{v}$, состоит из множества элементов вида $\mathbf{x}+\mathbf{y}$, где $\mathbf{x}\in\mathbf{w}+\mathcal{X}$, $\mathbf{y}\in\mathbf{v}+\mathcal{X}$. □

Теперь обратимся к правилам декодирования линейного кода: заранее зная код $\mathcal{X}$, можно рассчитать все смежные классы. Получив слово $\mathbf{y}$, ищем его смежный класс $\mathbf{y}+\mathcal{X}$ и слово $\mathbf{w}\in\mathbf{y}+\mathcal{X}$ наименьшего веса. Такое слово называют *лидером* смежного класса $\mathbf{y}+\mathcal{X}$. Лидер может и не быть единственным: в этом случае придётся сделать выбор среди списка лидеров (списка декодирования) или отказаться от декодирования и потребовать повторной передачи. Предположим, что выбран лидер $\mathbf{w}$. Тогда декодируем $\mathbf{y}$ словом

$$\mathbf{x}_*=\mathbf{y}+\mathbf{w}. \tag{2.3.8}$$

Пример 2.3.17. Покажите, что слово $\mathbf{x}_*$ всегда является кодовым словом, минимизирующим расстояние между $\mathbf{y}$ и кодовыми словами из $\mathcal{X}$.

Решение. Поскольку $\mathbf{y}$ и $\mathbf{w}$ лежат в одном смежном классе, $\mathbf{y}+\mathbf{w}\in\mathcal{X}$ (см. пример 2.3.16, 3.). Все остальные слова из $\mathcal{X}$ получаются как суммы $\mathbf{y}+\mathbf{v}$, где $\mathbf{v}$ пробегает смежный класс $\mathbf{y}+\mathcal{X}$. Следовательно, для любого $\mathbf{x}\in\mathcal{X}$ имеем

$$\delta(\mathbf{y},\,\mathbf{x})=w(\mathbf{y}+\mathbf{x})\geqslant\min_{\mathbf{v}\in\mathbf{y}+\mathcal{X}}w(\mathbf{v})=\delta(\mathbf{y},\,\mathbf{x}_*).$$ □

Матрица проверки на чётность предоставляет удобное описание смежного класса $\mathbf{y}+\mathcal{X}$.

Теорема 2.3.18. *Смежные классы $\mathbf{w}+\mathcal{X}$ взаимно однозначно соответствуют векторам вида $\mathbf{y}H^{\mathrm{T}}$: два вектора $\mathbf{y}$ и $\mathbf{y}'$ лежат в од-*

ном смежном классе тогда и только тогда, когда $\mathbf{y}H^{\mathrm{T}} = \mathbf{y}'H^{\mathrm{T}}$. *Иначе говоря, смежные классы отождествляются с пространством образов* H^{T} *порожденной столбцами проверочной матрицы*[4].

Доказательство. Слова $\mathbf{y}$ и $\mathbf{y}'$ находятся в одном смежном классе тогда и только тогда, когда $\mathbf{y} + \mathbf{y}' \in \mathcal{X}$, т. е.

$$(\mathbf{y} + \mathbf{y}')H^{\mathrm{T}} = \mathbf{y}H^{\mathrm{T}} + \mathbf{y}'H^{\mathrm{T}} = 0, \qquad \text{т. е.} \quad \mathbf{y}H^{\mathrm{T}} = \mathbf{y}'H^{\mathrm{T}}. \qquad \square$$

На практике правило декодирования применяется следующим образом. Векторы вида $\mathbf{y}H^{\mathrm{T}}$ называются *синдромами*: для линейного $[N, k]$-кода есть 2^{N-k} синдромов. Все они перечислены в «таблице» синдромов, и для каждого синдрома вычисляется лидер соответствующего смежного класса. Получив слово $\mathbf{y}$, можно подсчитать синдром $\mathbf{y}H^{\mathrm{T}}$ и найти в таблице синдромов соответствующий лидер $\mathbf{w}$, а затем, следуя правилу (2.3.8), декодировать $\mathbf{y}$ как $\mathbf{x}_* = \mathbf{y} + \mathbf{w}$.

Описанная процедура называется *синдромным декодированием*. Хотя оно относительно просто, нужно выписывать довольно длинные таблицы лидеров. Кроме того, желательно, чтобы вся процедура декодирования была алгоритмически независимой от конкретного выбора кода, т. е. его порождающей матрицы. Эта цель достигается в случае кодов Хэмминга.

Теорема 2.3.19. *В коде Хэмминга каждому синдрому соответствует единственный лидер* $\mathbf{w}$, *причём он содержит не более одного ненулевого знака. Более точно, если синдром* $\mathbf{y}(H^{\mathrm{Ham}})^{\mathrm{T}} = \mathbf{s}$ *даёт* i*-й столбец проверочной матрицы* H^{Ham}, *то лидер соответствующего смежного класса имеет единственный ненулевой знак, стоящий на* i*-м месте.*

Доказательство. Лидер минимизирует расстояние между полученным словом и кодом. Код Хэмминга является совершенным исправляющим одну ошибку. Следовательно, любое слово либо является кодовым, либо находится на расстоянии 1 от единственного кодового слова. Значит, лидер определён однозначно и содержит не более одного ненулевого знака. Если синдром $\mathbf{y}H^{\mathrm{T}} = \mathbf{s}$ попадает на i-й столбец проверочной матрицы, то для слова $\mathbf{e}_i = 0 \ldots 010 \ldots 0$ с единственной 1 на i-м месте имеем

$$(\mathbf{y} + \mathbf{e}_i)H^{\mathrm{T}} = \mathbf{s} + \mathbf{s} = \mathbf{0}.$$

Иначе говоря, $\mathbf{y} + \mathbf{e}_i \in \mathcal{X}$ и $\mathbf{e}_i \in \mathbf{y} + \mathcal{X}$. Очевидно, $\mathbf{e}_i$ является лидером. $\square$

Коды $\mathcal{X}^{\mathrm{Ham}\perp}$, двойственные к двоичным кодам Хэмминга, образуют особый класс, называемый классом *симплексных кодов*. Если $\mathcal{X}^{\mathrm{Ham}}$ — $[2^l - 1, 2^l - 1 - l]$-код, то двойственный код $\mathcal{X}^{\mathrm{Ham}\perp}$ — это $[2^l - 1, l]$-код,

[4] Rank or range space.

а проверочная матрица H^{Ham} исходного кода становится порождающей для двойственного.

Пример 2.3.20. Докажите, что вес каждого ненулевого кодового слово двоичного симплексного кода $\mathcal{X}^{\mathrm{Ham}\perp}$ равен 2^{l-1}, и расстояние между любыми двумя кодовыми словами тоже равно 2^{l-1}. Этим объясняется термин «симплекс».

Решение. Если $\mathcal{X} = \mathcal{X}^{\mathrm{Ham}}$ — это двоичный $[2^l - 1, 2^l - 1 - l]$-код Хэмминга, то двойственный код $\mathcal{X}^{\mathrm{Ham}\perp}$ — это $[2^l - 1, l]$-код и его порождающая матрица размера $l \times (2^l - 1)$ совпадает с проверочной матрицей исходного кода H^{Ham}. Вес каждой строки матрицы H^{Ham} равен 2^{l-1} (и поэтому $d(\mathcal{X}^\perp) = 2^l - 1$). Действительно, вес j-й строки равен числу ненулевых векторов длины l с единицей в j-й позиции. Это даёт 2^{l-1}, так как половина всех 2^l векторов из $\mathcal{H}_l$ имеет 1 в любой данной позиции.

Рассмотрим теперь общее кодовое слово из $\mathcal{X}^{\mathrm{Ham}\perp}$. Оно представляется суммой строк $j_1, \ldots, j_s$ из H^{Ham}, где $s \leqslant l$ и $1 \leqslant j_1 < \ldots < j_s \leqslant l$. Вес этого слова тоже равен 2^{l-1}, что даёт некоторое количество ненулевых слов $\mathbf{v} = v_1 \ldots v_l \in \mathcal{H}_{l,2}$, для которых $v_{j_1} + \ldots + v_{j_s} = 1$. Более того, 2^{l-1} — это половина всех векторов пространства $\mathcal{H}_{l,2}$. Действительно, нам нужно, чтобы выполнялось равенство $v_{j_1} + \ldots + v_{j_s} = 1$, что даёт 2^{s-1} возможностей получить 1, суммируя s знаков. Далее, на остающиеся $l - s$ знаков мы не накладываем никаких ограничений, что даёт 2^{l-s} возможностей. Итого, $2^{s-1} \times 2^{l-s} = 2^{l-1}$, как и требовалось. Таким образом, $w(\mathbf{x}) = 2^{l-1}$ для любого ненулевого $\mathbf{x} \in \mathcal{X}^\perp$. Наконец, для любых $\mathbf{x}, \mathbf{x}' \in \mathcal{X}^\perp$, $\mathbf{x} \neq \mathbf{x}'$ имеем $\delta(\mathbf{x}, \mathbf{x}') = \delta(\mathbf{0}, \mathbf{x} + \mathbf{x}') = w(\mathbf{x} + \mathbf{x}')$, что всегда равно 2^{l-1}, так что кодовые слова $\mathbf{x} \in \mathcal{X}^\perp$ образуют «симплекс» с 2^l «вершинами». □

Теперь мы коротко суммируем основные факты о линейных кодах над конечным полем–алфавитом $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ размера $q = p^s$. Теперь пространство Хэмминга $\mathcal{H}_{N,q}$ будем обозначать символом $\mathbb{F}_q^{\times N}$.

Определение 2.3.21. Назовем q-ичный код $\mathcal{X} \subseteq \mathbb{F}_q^{\times N}$ *линейным*, если вместе с парой векторов $\mathbf{x} = x_1 \ldots x_N$ и $\mathbf{x}' = x'_1 \ldots x'_N$ код $\mathcal{X}$ содержит линейные комбинации $\gamma \cdot \mathbf{x} + \gamma' \cdot \mathbf{x}'$ с компонентами $\gamma x_i + \gamma' x'_i$ для всех коэффициентов $\gamma, \gamma' \in \mathbb{F}_q$. Иными словами, $\mathcal{X}$ — *линейное подпространство* в $\mathbb{F}_q^{\times N}$. Следовательно, как и в двоичном случае, линейный код всегда содержит нулевой вектор $\mathbf{0} = 0 \ldots 0$. *Базис* двоичного кода снова определяется как максимальная линейно независимая совокупность его векторов; линейный код порождается своим базисом в том смысле, что любое кодовое слово (единственным образом) представляется в виде линейной комбинации базисных. Число базисных векторов, как и ранее, называется *размерностью* или *рангом* кода. Поскольку это число не зависит от конкретного базиса данного кода, ранг корректно определён.

Как обычно, линейный код длины N и ранга k называют $[N, k]$-кодом или $[N, k, d]$-кодом, если его расстояние равно d.

Как и в двоичном случае, минимальное расстояние линейного кода равно минимальному ненулевому весу —

$$d(\mathcal{X}) = \min[w(\mathbf{x})\colon \mathbf{x} \in \mathcal{X},\ \ \mathbf{x} \neq \mathbf{0}],$$

где

$$w(\mathbf{x}) = \#\{j\colon 1 \leqslant j \leqslant N,\quad x_j \neq 0 \text{ в } \mathbb{F}_q\},\quad \mathbf{x} = x_1 \dots x_N \in \mathbb{F}_q^{\times N}. \quad (2.3.9)$$

Линейный код $\mathcal{X}$ определяется *образующей* матрицей G или *проверочной* матрицей H. *Образующая* матрица линейного $[N, k]$-кода — это $k \times N$-матрица G с элементами из поля $\mathbb{F}_q$, строки $\mathbf{g}(i) = g_{i1} \dots g_{iN}$, $1 \leqslant i \leqslant k$, которой образуют базис кода $\mathcal{X}$. *Проверочная* матрица — это $(N - k) \times N$-матрица с элементами из $\mathbb{F}_q$ с линейно независимыми строками $\mathbf{h}(j) = h_{j1} \dots h_{jN}$, $1 \leqslant j \leqslant N - k$, скалярно ортогональными коду $\mathcal{X}$, а именно, для любых $j = 1, \dots, N - k$ и кодового слова $\mathbf{x} \in \mathcal{X}$ выполнено равенство

$$\langle \mathbf{x} \cdot \mathbf{h}(j) \rangle = \sum_{i=1}^{N} x_i h_{ji} = 0. \qquad \square$$

Другими словами, все q^k кодовых слов из $\mathcal{X}$ получаются в виде линейных комбинаций строк матрицы G, т. е. подпространство $\mathcal{X}$ можно рассматривать как результат действия матрицы G на пространстве Хэмминга $\mathbb{F}_q^{\times k}$ (длины k): символически, $\mathcal{X} = \mathbb{F}_q^{\times k} G$. Это показывает, как код $\mathcal{X}$ может использоваться для кодирования q^k «сообщений» длины k (и оправдывает термин «скорость передачи информации» для отношения $\varrho(\mathcal{X}) = k/N$). С другой стороны, $\mathcal{X}$ определяется как ядро (нуль-пространство) матрицы H^{T}: $\mathcal{X} H^{\mathrm{T}} = 0$. Будет полезно проверить, что для двойственного кода $\mathcal{X}^{\perp}$ ситуация противоположна: H является порождающей матрицей, а G — проверяющей. (См. пример 2.3.5.)

Конечно, как порождающая, так и проверяющая матрицы данного кода определены не однозначно; можно, например, переставить строки $\mathbf{g}(j)$ в G или применить к G элементарные операции над строками, прибавив к одной из них линейную комбинацию остальных. Переставив столбцы матрицы G, мы получим другой, но эквивалентный код, геометрические параметры базиса в котором идентичны соответствующим параметрам базиса исходного кода.

Лемма 2.3.22. *Для любого* $[N, k]$*-кода, существует эквивалентный код, порождающая матрица* G *которого имеет канонический вид*: $G = (G'\ \ \mathbf{1}_k)$, *где* $\mathbf{1}_k$ *— единичная* $k \times k$*-матрица, а* G' —

$k \times (N-k)$-матрица. Аналогично проверочная матрица может быть записана в каноническом виде $(\mathbf{1}_{N-k}\ H')$.

Обсудим сейчас процедуру декодирования общего линейного кода $\mathcal{X}$ ранга k. Как уже отмечалось, им можно кодировать сообщения (строки) источника $\mathbf{u} = u_1 \dots u_k$ длины k. Кодирование источника $\mathbf{u} \in \mathbb{F}_q^k \mapsto \mathcal{X}$ — относительно простая процедура, если порождающая и проверяющая матрицы записаны в каноническом виде.

Теорема 2.3.23. *Для любого линейного кода $\mathcal{X}$ найдётся эквивалентный ему код с порождающей матрицей G^{can} и проверяющей матрицей H^{can} канонического вида* (2.3.5а) *и* (2.3.5б), *причём* $G' = -(H')^{\mathrm{T}}$.

Доказательство. Предположим, что код $\mathcal{X}$ нетривиален (т. е. не сводится лишь к нулевому слову $\mathbf{0}$). Выпишем базис кода $\mathcal{X}$ и соответствующую порождающую матрицу G. Выполнив ряд операций над строками (пара строк меняются местами или к i-й строке прибавляется j-я, умноженная на число), можно изменить базис, не меняя кода. Наша матрица G содержит ненулевой столбец, скажем l_1. Выполним ряд операций над строками, чтобы сделать g_{1l_1} единственным элементом в этом столбце. Переставляя цифры (столбцы), поместим столбец l_1 на место $N-k$. Удалим первую строку и столбец с номером $N-k$ (т. е. старый столбец l_1) и выполним аналогичную процедуру с оставшейся матрицей, закончив её ненулевым элементом g_{2l_2} в столбце l_2. Место столбца l_2 в позиции $N-k+1$. Продолжаем эти действия, пока не получим верхнетреугольную $k \times k$-подматрицу. Дальнейшие операции можно ограничить лишь этой подматрицей. Если она единичная, то алгоритм закончен. Если нет, то берём первый столбец, в котором по крайней мере два ненулевых элемента. Прибавим соответствующую строку, чтобы «убить» лишний ненулевой элемент. Продолжаем так действовать, пока не получится единичная матрица. Теперь порождающая матрица приобрела канонический вид, а новый код эквивалентен исходному.

Для завершения доказательства заметим, что матрицы G^{can} и H^{can}, фигурирующие в формулах (2.3.5а) и (2.3.5б), обладающие свойством $G' = -(H')^{\mathrm{T}}$, имеют k независимых строк и $N-k$ независимых столбцов соответственно. Кроме того, $(k \times (N-k))$-матрица $G^{\mathrm{can}}(H^{\mathrm{can}})^{\mathrm{T}}$ равна нулевой. Действительно,

$$(G^{\mathrm{can}}(H^{\mathrm{can}})^{\mathrm{T}})_{ij} = \langle i\text{-я строка } G' \cdot j\text{-й столбец } (H')^{\mathrm{T}} \rangle = g'_{ij} - g'_{ij} = 0.$$

Следовательно, H^{can} является проверочной матрицей для G^{can}. □

Возвращаясь к кодированию источника, выберем порождающую матрицу в каноническом виде G^{can}. Тогда для строки $\mathbf{u} = u_1, \dots, u_k$ положим

$\mathbf{x} = \sum_{i=1}^{k} u_i \mathbf{g}^{\mathrm{can}}(i)$, где $\mathbf{g}^{\mathrm{can}}(i)$ — i-я строка матрицы G^{can}. Последние k знаков в $\mathbf{x}$ дают строку $\mathbf{u}$: они называются информационными знаками, а первые $N-k$ знаков используются для проверки того, что $\mathbf{x} \in \mathcal{X}$; они называются проверочными знаками.

Канонический вид удобен, так как в предыдущем представлении $\mathcal{X} = \mathbb{F}^{\times k} G$ начальная $(N-k)$-подстрока каждого кодового слова используется для кодирования (возможность обнаружения и исправления ошибок) и последняя k-подстрока даёт сообщение из $\mathbb{F}_q^{\times k}$. Как и в двоичном случае, проверочная матрица H удовлетворяет теореме 2.3.11. В частности, *минимальное расстояние кода равно минимальному числу линейно зависимых столбцов его проверочной матрицы H.*

Определение 2.3.24. Пусть дан q-ичный линейный $[N, k]$-код с проверочной матрицей H. *Синдромом* N-вектора $\mathbf{y} \in \mathbb{F}_q^{\times N}$ называется k-вектор $\mathbf{y}H^{\mathrm{T}} \in \mathbb{F}_q^{\times k}$, а синдромное подпространство — это образ $\mathbb{F}_q^{\times N} H^{\mathrm{T}}$. *Смежным классом* кода $\mathcal{X}$ с представителем $\mathbf{w} \in \mathbb{F}_q^{\times N}$ называется множество $\mathbf{w} + \mathcal{X}$, состоящее из всех слов вида $\mathbf{w} + \mathbf{x}$, $\mathbf{x} \in \mathcal{X}$. Все смежные классы насчитывают одинаковое число элементов, равное 2^k, и разбивают всё пространство Хэмминга $\mathbb{F}_q^{\times N}$ на $N-k$ непересекающихся подмножеств; код $\mathcal{X}$ — одно из них. Синдромы $\mathbf{y}H^{\mathrm{T}}$ взаимно однозначно соответствуют смежным классам. Процедура *синдромного декодирования* осуществляется, как в двоичном случае: полученный вектор $\mathbf{y}$ декодируется словом $\mathbf{x}_* = \mathbf{y} + \mathbf{w}$, где $\mathbf{w}$ — лидер смежного класса $\mathbf{y} + \mathcal{X}$ (т. е. слово из $\mathbf{y} + \mathcal{X}$ с минимальным весом). □

Все недостатки, встреченные нами в случае двоичного синдромного декодирования, сохраняются и в общем q-ичном случае (и даже более ярко выражены): таблицы смежных классов очень громоздкие, лидер в смежном классе может быть не единственным. Однако для q-ичных кодов Хэмминга процедура синдромного декодирования, как мы увидим в § 2.4, работает хорошо.

Для линейных кодов можно улучшить некоторые из границ на их размеры или найти новые.

Пример 2.3.25. Пусть $\mathcal{X}$ — двоичный линейный $[N, k, d]$-код.

1. Зафиксируем кодовое слово $\mathbf{x} \in \mathcal{X}$, содержащее ровно d ненулевых знаков. Докажите, что в результате усечения $\mathcal{X}$ на ненулевые знаки слова $\mathbf{x}$ получится код $\mathcal{X}'_{N-d}$ длины $N-d$, ранга $k-1$ и с расстоянием d' для некоторого $d' \geqslant \lceil d/2 \rceil$.

2. Выведите *неравенство Грайсмера*, улучшающее границу Синглтона (2.1.12) для линейного кода ранга $k \leqslant N - d + 1$:

$$N \geqslant d + \sum_{l=1}^{k-1} \left\lceil \frac{d}{2^l} \right\rceil. \tag{2.3.10}$$

Решение. 1. Без ограничения общности можно считать, что ненулевые знаки в слове $\mathbf{x}$ — это $x_1 = \ldots = x_d = 1$. Усечение знаков $1, \ldots, d$ приведёт к коду $\mathcal{X}'_{N-d}$ на единицу меньшего ранга. Действительно, предположим, что линейная комбинация $k-1$ вектора имеет нули на позициях $d+1, \ldots, N$. Тогда на позициях $1, \ldots, d$ все значения равны 0 или 1, поскольку d — это минимальное расстояние. Но первый случай возможен только в случае линейно зависимых векторов. Второй случай также приводит к противоречию, поскольку, добавив строку $\mathbf{x}$, мы получим k линейно зависимых векторов в коде $\mathcal{X}$. Далее предположим, что минимальное расстояние d' кода $\mathcal{X}'$ удовлетворяет неравенству $d' < \left\lceil \frac{d}{2} \right\rceil$ и возьмём слово $\mathbf{y}' \in \mathcal{X}'$ с весом $w(\mathbf{y}') = \sum\limits_{j=d+1}^{N} y'_j = d'$.

Пусть $\mathbf{y} \in \mathcal{X}$ — обратный образ слова $\mathbf{y}'$ при усечении. Ссылаясь на определение (2.1.6б), выпишем следующее свойство двоичной конъюнкции:

$$w(\mathbf{y}) = w(\mathbf{x} \wedge \mathbf{y}) + w(\mathbf{y} + (\mathbf{x} \wedge \mathbf{y})) \geqslant d.$$

Следовательно, должно выполняться неравенство $w(\mathbf{x} \wedge \mathbf{y}) > d - \lceil d/2 \rceil$ (см. рис. 2.5).

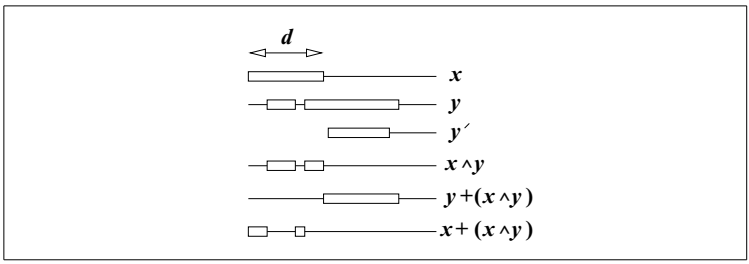


Рис. 2.5

Тогда из равенства

$$w(\mathbf{x}) = w(\mathbf{x} \wedge \mathbf{y}) + w(\mathbf{x} + (\mathbf{x} \wedge \mathbf{y})) = d$$

следует, что $w(\mathbf{x}+(\mathbf{x}\wedge\mathbf{y}))<\lceil d/2\rceil$. Но из этого, в свою очередь, следует неравенство

$$w(\mathbf{x}+\mathbf{y})=w(\mathbf{x}+(\mathbf{x}\wedge\mathbf{y}))+w(\mathbf{y}+(\mathbf{x}\wedge\mathbf{y}))<d,$$

что невозможно для кода с расстоянием d. Отсюда делаем вывод: $d'\geqslant\lceil d/2\rceil$.

2. Повторяя рассуждения первого пункта, получаем

$$N\geqslant d+d_1+\ldots+d_{k-1},$$

где $d_1\geqslant\left\lceil\frac{d_{l-1}}{2}\right\rceil$. Учитывая неравенство $\left\lceil\frac{\lceil d/2\rceil}{2}\right\rceil\geqslant\left\lceil\frac{d}{4}\right\rceil$, приходим к выводу:

$$N\geqslant d+\sum_{l=1}^{k-1}\left\lceil\frac{d}{2^l}\right\rceil.$$ □

Заканчивая этот параграф, уточним неравенство Гильберта—Варшамова для линейных кодов.

Теорема 2.3.26 (неравенство Гильберта). *Если $q=p^s$ — степень простого числа, то для любых таких целых чисел N и d, что $2\leqslant d\leqslant N/2$, найдётся q-ичный линейный $[N, k, d]$-код с минимальным расстоянием не меньше d, в том случае, если*

$$q^k\geqslant q^N/v_{N,q}(d-1). \tag{2.3.11}$$

Доказательство. Пусть $\mathcal{X}$ — линейный код, минимальное расстояние у которого по крайней мере d, максимального размера. Если неравенство (2.3.11) не выполняется, то объединение всех шаров Хэмминга радиуса $d-1$ с центрами в кодовых словах не может покрывать всё пространство Хэмминга. Значит, должна найтись точка $\mathbf{y}\in\mathcal{H}_N$, которая не попала ни в один шар. Поэтому при любом кодовом слове $\mathbf{x}$ и скаляре $\gamma\in\mathbb{F}_q$ векторы $\mathbf{y}$ и $\mathbf{y}+\gamma\cdot\mathbf{x}$ попадают в один смежный класс по $\mathcal{X}$, т. е. $\mathbf{y}+\gamma\cdot\mathbf{x}-\mathbf{y}=\gamma\cdot\mathbf{x}\in\mathcal{X}$. Кроме того, $\mathbf{y}+\gamma\cdot\mathbf{x}$ не может попасть ни в один из шаров Хэмминга радиуса $d-1$. То же самое можно сказать и о векторе $\mathbf{x}+\gamma\cdot\mathbf{y}$, потому что если это не так, то $\mathbf{y}$ попадает в шар Хэмминга вокруг другого кодового слова. Здесь мы используем тот факт, что $\mathbb{F}_q$ — поле. Векторное подпространство, натянутое на $\mathcal{X}$ и $\mathbf{y}$, — это линейный код, больший, чем $\mathcal{X}$, и с минимальным расстоянием по крайней мере d. Это противоречие завершает доказательство. □

Пусть, например, $q=2$ и $N=10$. Тогда $2^5<v_{10,2}(2)=56<2^6$. При $d=3$ неравенство Гильберта гарантирует существование двоичного $[10, 5]$-кода с расстоянием $d\geqslant 3$.

... ошибки более полезны, чем истинное значение: истина механична, ошибка — жива; правда успокаивает, ошибка беспокоит.

Евгений Замятин (1884–1937), русский писатель (о литературе, революции, энтропии и о прочем)

Чтобы создать хороший код, сначала выберите коды больших размеров. Затем из выбранных отберите коды с большим расстоянием. Из последних выберите линейные. Наконец, из линейных возьмите коды с красивыми проверочными матрицами. Просто.

(Из серии «Так говорил суперлектор».)

§ 2.4. Коды Хэмминга, Голея и Рида—Маллера

Цель расчётов — понимание, а не числа.

Ричард Хэмминг (1915–1998), американский математик и программист

В этом параграфе мы систематически изучаем коды с алфавитом $\mathbb{F}_q$ из q элементов, который предполагается полем. Повторим, что в этом случае $q = p^s$, где p — простое число, а s — натуральное число, и в поле заданы соответствующие операции сложения $(+)$ и умножения $(\cdot)$. (Как уже было сказано, если $q = p$ — простое, то можно считать, что $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ и сложение и умножение в $\mathbb{F}_q$ — стандартные операции по модулю q (см. § 2.1)). Соответственно пространство Хэмминга $\mathcal{H}_{N,q}$ длины N с символами из поля $\mathbb{F}_q$ определяется, как и прежде, декартовой степенью $\mathbb{F}_q^{\times N}$ и наследует покомпонентное сложение и умножение на скаляры.

Определение 2.4.1. Для данных натуральных чисел q, $l \geqslant 2$ положим: $N = \dfrac{q^l - 1}{q-1}$, $k = N - l$ и построим q-ичный $[N, k, 3]$ — *код Хэмминга* $\mathcal{X}^{\mathrm{Ham}}_{N,q}$ с алфавитом $\mathbb{F}_q$ следующим образом.

1. Возьмём произвольное ненулевое q-ичное l-слово $\mathbf{h}^{(1)} \in \mathcal{H}_{l,q}$.

2. Возьмём произвольное ненулевое q-ичное l-слово $\mathbf{h}^{(2)} \in \mathcal{H}_{l,q}$, не пропорциональное слову $\mathbf{h}^{(1)}$.

3. Когда выбраны слова $\mathbf{h}^{(1)}, \ldots, \mathbf{h}^{(s)}$, выбираем следующий вектор $\mathbf{h}^{(s+1)} \in \mathcal{H}_{l,q}$ как произвольный вектор, не пропорциональный ни одному из ранее выбранных слов $\mathbf{h}^{(1)}, \ldots, \mathbf{h}^{(s)}$.

4. Процесс заканчивается, когда будут выбраны N векторов $\mathbf{h}^{(1)}, \ldots, \mathbf{h}^{(N)}$; формируем из них $l \times N$-матрицу H^{Ham} со столбцами $\mathbf{h}^{(1)\mathrm{T}}, \ldots, \mathbf{h}^{(N)\mathrm{T}}$. Код $\mathcal{X}^{\mathrm{Ham}}_{N,q} \subset \mathbb{F}_q^{\times N}$ определяется проверочной матрицей

H^{Ham}. (На самом деле мы здесь имеем дело с семейством эквивалентных кодов по модулю выбора слов $\mathbf{h}^{(j)}$, $1 \leqslant j \leqslant N$.) □

Для краткости будем теперь писать $\mathcal{X}^{\mathrm{H}}$ и H^{H} (или даже по возможности просто H) вместо $\mathcal{X}^{\mathrm{Ham}}$ и H^{Ham}. В двоичном случае ($q = 2$) матрица H^{H} составляется из всех ненулевых двоичных вектор-столбцов длины l. При общем q следует исключить пропорциональные столбцы. Чтобы сделать это, нужно в качестве столбцов выбирать все ненулевые l-слова, у которых самый верхний ненулевой символ равен 1. Все они не пропорциональны, а их общее число равно $\dfrac{q^l - 1}{q - 1}$. Далее, как в двоичном случае, можно упорядочить слова с символами из поля $\mathbb{F}_q$ лексикографически. По построению любые два столбца матрицы H^{H} линейно независимы, но существуют тройки линейно зависимых столбцов. Значит, $d(\mathcal{X}^{\mathrm{H}}) = 3$, и $\mathcal{X}^{\mathrm{H}}$ обнаруживает две ошибки и исправляет одну. Более того, $\mathcal{X}^{\mathrm{H}}$ — совершенный код, исправляющий единственную ошибку, поскольку

$$M(1 + (q-1)N) = q^k\left(1 + (q-1)\frac{q^l - 1}{q-1}\right) = q^{k+l} = q^N.$$

Как и в двоичном случае, общие коды Хэмминга допускают эффективную (и элегантную) процедуру декодирования. Предположим, что проверочная матрица H ($= H^{\mathrm{H}}$) построена, как описано выше. Получив слово $\mathbf{y} \in \mathbb{F}_q^{\times N}$, мы вычисляем синдром $\mathbf{y}H^{\mathrm{T}} \in \mathbb{F}_q^{\times l}$. Если $\mathbf{y}H^{\mathrm{T}} = 0$, то $\mathbf{y}$ — кодовое слово. В другом случае вектор-столбец $H\mathbf{y}^{\mathrm{T}}$ пропорционален какому-то столбцу $\mathbf{h}^{(j)}$ матрицы H: $H\mathbf{y}^{\mathrm{T}} = a \cdot \mathbf{h}^j$ для некоторого $j = 1, \ldots, N$ и $a \in \mathbb{F}_q \setminus \{0\}$. Иначе говоря, $\mathbf{y}H^{\mathrm{T}} = a \cdot \mathbf{e}(j)H^{\mathrm{T}}$, где $\mathbf{e}(j) = 0 \ldots 1 \ldots 0 \in \mathcal{H}_{N,q}$ (с единицей в позиции j и нулями в остальных местах). В этом случае мы декодируем $\mathbf{y}$ как $\mathbf{x}_* = \mathbf{y} - a \cdot \mathbf{e}(j)$, т. е. просто меняем символ y_j на $y_j - a$.

Подводя итог, получаем следующую теорему.

Теорема 2.4.2. *q-ичные коды Хэмминга образуют семейство* $\left[\dfrac{q^l - 1}{q-1}, \dfrac{q^l - 1}{q-1} - l, 3\right]$ *совершенных кодов $\mathcal{X}_N^{\mathrm{H}}$ при $N = \dfrac{q^l - 1}{q-1}$, $l = 1, 2, \ldots$, исправляющих одну ошибку, с правилом декодирования, меняющим символ y_j на $y_j - a$ в полученном слове $\mathbf{y} = y_1 \ldots y_N \in \mathbb{F}_q^{\times N}$, где $1 \leqslant j \leqslant N$ и $a \in \mathbb{F}_q \setminus \{0\}$ находится из того условия, что $H\mathbf{y}^{\mathrm{T}} = a \cdot \mathbf{h}^j$, т. е. вектор $H\mathbf{y}^{\mathrm{T}}$ пропорционален столбцу проверочной матрицы H с коэффициентом a.*

Коды Хэмминга были изобретены Р. Хэммингом и М. Голеем в конце 1940-х гг. В то время Хэмминг, инженер-электрик, стал программистом на заре компьютерной эры и работал на Лос-Аламосе (по его собственным словам «как интеллектуальной дворник» для местных физиков-ядерщиков). Это открытие определило развитие теории кодов на более

чем два десятилетия: люди работали, чтобы продолжить свойства кодов Хэмминга на более широкий класс кодов (с переменным успехом). Большинство тем о кодах, обсуждаемых в этой книге, связаны в той или иной мере с кодами Хэмминга. Ричард Хэмминг был не только знаменитым учёным, но и яркой личностью; его творчество (и описание его жизни) занимательно и вызывает на размышления.

До конца 1950-х гг. коды Хэмминга были уникальным семейством кодов, существующих в размерности $N \gg 1$, с «регулярными» свойствами. Как позже выяснилось, эти коды имеют глубокое алгебраическое обоснование. Развитие алгебраических методов, основанных на этом наблюдении, всё ещё остаётся доминирующей темой в современной теории кодирования.

Другим важным примером служат четыре *кода Голея* (два двоичных и два троичных). Марсель Голей (1902–1989), швейцарский инженер-электрик, в течение длительного времени жил и работал в США. Он обладал необыкновенным умением «видеть» дискретную геометрию пространства Хэмминга и «угадывать» конструкции различных кодов, не утруждая себя доказательствами.

Двоичный код Голея $\mathcal{X}_{24}^{\mathrm{Gol}}$ — это [24, 12]-код с образующей матрицей $G = (\mathbf{1}_{12} \,|\, G')$, где $\mathbf{1}_{12}$ — единичная матрица размера 12×12 и $G' (= G'_{(2)})$ имеет следующий вид:

$$G' = \begin{pmatrix} 0&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&1&0&1&1&1&0&0&0&1&0\\ 1&1&0&1&1&1&0&0&0&1&0&1\\ 1&0&1&1&1&0&0&0&1&0&1&1\\ 1&1&1&1&0&0&0&1&0&1&1&0\\ 1&1&1&0&0&0&1&0&1&1&0&1\\ 1&1&0&0&0&1&0&1&1&0&1&1\\ 1&0&0&0&1&0&1&1&0&1&1&1\\ 1&0&0&1&0&1&1&0&1&1&1&0\\ 1&0&1&0&1&1&0&1&1&1&0&0\\ 1&1&0&1&1&0&1&1&1&0&0&0\\ 1&0&1&1&0&1&1&1&0&0&0&1 \end{pmatrix}. \tag{2.4.1}$$

Правило построения матрицы G' весьма специфично (оно было предложено самим М. Голеем в 1949 г.) Далее мы встретимся и с другими специфическими алгоритмами при анализе кодов Голея.

Замечание 2.4.3. Любопытно, что существует систематический способ построения всех кодовых слов кода $\mathcal{X}_{24}^{\mathrm{Gol}}$ (или эквивалентного ему) путём компоновки двух версий [7, 4]-кода Хэмминга $\mathcal{X}_7^{\mathrm{H}}$. Во-первых, отметим, что обращая порядок следования всех цифры из кода Хэмминга $\mathcal{X}_7^{\mathrm{H}}$, мы получаем эквивалентный код, который обозначим через $\mathcal{X}_7^{\mathrm{K}}$. Затем применим к обоим кодам $\mathcal{X}_7^{\mathrm{H}}$ и $\mathcal{X}_7^{\mathrm{K}}$ продолжение с контролем чётности и получим

коды $\mathcal{X}_8^{\mathrm{H},+}$ и $\mathcal{X}_8^{\mathrm{K},+}$. И наконец выберем два разных слова $\mathbf{a}, \mathbf{b} \in \mathcal{X}_8^{\mathrm{H},+}$ и слово $\mathbf{x} \in \mathcal{X}_8^{\mathrm{K},+}$. В результате все 2^{12} кодовых слова из $\mathcal{X}_{24}^{\mathrm{Gol}}$ длины 24 можно будет записать в виде сцепления $(\mathbf{a}+\mathbf{x})(\mathbf{b}+\mathbf{x})(\mathbf{a}+\mathbf{b}+\mathbf{x})$. Это можно проверить с помощью порождающей матрицы. □

Лемма 2.4.4. *Код $\mathcal{X}_{24}^{\mathrm{Gol}}$ является самодвойственным, т. е. $\mathcal{X}_{24}^{\mathrm{Gol}\perp} = \mathcal{X}_{24}^{\mathrm{Gol}}$. Он порождается также матрицей $\tilde{G} = (G' \,|\, \mathbf{1}_{12})$.*

Доказательство. Прямая проверка показывает, что любые две строки матрицы G ортогональны друг другу. Поэтому $\mathcal{X}_{24}^{\mathrm{Gol}} \subset \mathcal{X}_{24}^{\mathrm{Gol}\perp}$. Но размерности кодов $\mathcal{X}_{24}^{\mathrm{Gol}}$ и $\mathcal{X}_{24}^{\mathrm{Gol}\perp}$ совпадают. Следовательно, $\mathcal{X}_{24}^{\mathrm{Gol}\perp} = \mathcal{X}_{24}^{\mathrm{Gol}}$. Последнее утверждение леммы вытекает из равенства $(G')^{\mathrm{T}} = G'$. □

Пример 2.4.5. Покажите, что $d(\mathcal{X}_{24}^{\mathrm{Gol}}) = 8$.

Решение. Прежде всего проверим, что вес всех слов $\mathbf{x} \in \mathcal{X}_{24}^{\mathrm{Gol}}$ делится на 4. Это верно для каждой строки матрицы $G = (\mathbf{1}_{12} \,|\, G')$: число единиц там — либо 12, либо 8. Далее, для всех двоичных N-слов $\mathbf{x}$, $\mathbf{x}'$ имеем

$$w(\mathbf{x}+\mathbf{x}') = w(\mathbf{x}) + w(\mathbf{x}') - 2w(\mathbf{x} \wedge \mathbf{x}'),$$

где $(\mathbf{x} \wedge \mathbf{x}')$ — конъюнкция, определённая по правилу $(\mathbf{x} \wedge \mathbf{x}')_j = \min[x_j, x'_j]$, $1 \leqslant j \leqslant N$ (см. формулу (2.1.6б). Однако для любой пары $\mathbf{g}(j)$, $\mathbf{g}(j')$ строк матрицы G получаем $w(\mathbf{g}(j) \wedge \mathbf{g}(j')) = 0 \bmod 2$, так что 4 делит $w(\mathbf{x})$ для всех $\mathbf{x} \in \mathcal{X}_{24}^{\mathrm{Gol}}$.

С другой стороны, в коде $\mathcal{X}_{24}^{\mathrm{Gol}}$ нет слов веса 4. Для доказательства сравним две порождающие матрицы $(\mathbf{1}_{12} \,|\, G')$ и $(G' \,|\, \mathbf{1}_{12})$. Если вес слова $\mathbf{x} \in \mathcal{X}_{24}^{\mathrm{Gol}}$ равен 4, то запишем $\mathbf{x}$ как сцепление $\mathbf{x}_L\mathbf{x}_R$. Любая нетривиальная сумма строк матрицы $(\mathbf{1}_{12} \,|\, G')$ имеет вес левой половины по крайней мере 1, откуда $w(\mathbf{x}_L) \geqslant 1$. Аналогично $w(\mathbf{x}_R) \geqslant 1$. Но если $w(\mathbf{x}_L) = 1$, то $\mathbf{x}$ должно совпадать с одной из строк матрицы $(\mathbf{1}_{12} \,|\, G')$, ни одна из которых не имеет веса $w(\mathbf{x}_R) = 3$. Следовательно, $w(\mathbf{x}_L) \geqslant 2$, и аналогично $w(\mathbf{x}_R) \geqslant 2$. Но тогда остаётся единственная возможность: $w(\mathbf{x}_L) = w(\mathbf{x}_R) = 2$, что тоже невозможно, как легко убедиться прямой проверкой. Значит, $w(\mathbf{x}) \geqslant 8$. Но строки матрицы $(\mathbf{1}_{12} \,|\, G')$ имеют вес 8, откуда $d(\mathcal{X}_{24}^{\mathrm{Gol}}) = 8$. □

При усечении кода $\mathcal{X}_{24}^{\mathrm{Gol}}$ в любом знаке получается [23, 12, 7]-код $\mathcal{X}_{23}^{\mathrm{Gol}}$. Это совершенный код, исправляющий 3 ошибки. Код $\mathcal{X}_{24}^{\mathrm{Gol}}$ восстанавливается из него в результате продолжения с контролем чётности.

Коды Хэмминга $[2^l - 1, 2^l - 1 - l, 3]$ и Голея [23, 12, 7] исчерпывают все совершенные двоичные линейные коды.

Порождающая матрица троичного кода Голея $\mathcal{X}_{12,3}^{\mathrm{Gol}}$ длины 12 имеет вид $(\mathbf{1}_6 \,|\, G'_{(3)})$, где

$$G'_{(3)} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}, \tag{2.4.2}$$

причём $(G'_{(3)})^{\mathrm{T}} = G'_{(3)}$.

Троичный код Голея $\mathcal{X}_{11,3}^{\mathrm{Gol}}$ получается усечением кода $\mathcal{X}_{12,3}^{\mathrm{Gol}}$ в последнем знаке.

Теорема 2.4.6. *Код* $\mathcal{X}_{12,3}^{\mathrm{Gol}\,\perp} = \mathcal{X}_{12,3}^{\mathrm{Gol}}$ *— это* [12, 6, 6]*-код. Код* $\mathcal{X}_{11,3}^{\mathrm{Gol}}$ *— это* [11, 6, 5]*-код, и поэтому он совершенен.*

Доказательство. Код [11, 6, 5] совершенен, так как $v_{11,3}(2) = 1 + 11 \times 2 + \dfrac{11 \times 10}{2} \times 2^2 = 3^5$. Доказательство остальных утверждений теоремы мы оставляем читателю в качестве упражнения. □

Совершенные троичные линейные коды — это только коды Хэмминга $[(3^l - 1)/2,\, 3^l - 1 - l,\, 3]$ и код Голея [11, 6, 5]. Более того, эти коды исчерпывают все совершенные коды среди линейных кодов над полем $\mathbb{F}_q$, где $q = p^s$ — степень простого числа. Таким образом, кроме этих кодов, больше нет линейных совершенных кодов.

И даже нелинейные совершенные коды не приносят ничего принципиально нового: все они имеют те же параметры (длину, размер и расстояние), как коды Хэмминга и Голея. Коды Голея в 1980-х гг. использовались в американских космических аппаратах программы «Вояджер» для передачи детальных фотографий Юпитера и Сатурна.

Следующий популярный пример кода — это коды Рида—Маллера. Для $N = 2^m$ рассмотрим двоичные пространства Хэмминга $\mathcal{H}_{m,2}$ и $\mathcal{H}_{N,2}$. Пусть $\mathbf{M}(= \mathbf{M}_m)$ — $m \times N$-матрицы, столбцы которых — это двоичные представления целых чисел $j = 0, 1, \ldots, N-1$ с наименее значимым битом на первом месте:

$$j = j_1 \cdot 2^0 + j_2 \cdot 2^1 + \ldots + j_m \cdot 2^{m-1}, \tag{2.4.3}$$

т. е.

$$\mathbf{M} = \begin{matrix} \begin{matrix} 0 & 1 & 2 & \ldots & 2^m-1 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 0 & \ldots & 1 \\ 0 & 0 & 1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \end{matrix} \begin{matrix} \mathbf{v}^{(1)} \\ \mathbf{v}^{(2)} \\ \vdots \\ \mathbf{v}^{(m-1)} \\ \mathbf{v}^{(m)} \end{matrix}.$$

В столбцах матрицы $\mathbf{M}$ перечислены все векторы из пространства $\mathcal{H}_{m,2}$, а строки — это векторы из пространства $\mathcal{H}_{N,2}$, обозначенные символами $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m)}$. В частности, первые 2^{m-1} элементов строки $\mathbf{v}^{(m)}$ равны 0, а последние 2^{m-1} элементов — 1. Чтобы перейти от матрицы $\mathbf{M}_m$ к матрице $\mathbf{M}_{m-1}$, выбросим последнюю строку и возьмём одну из одинаковых половин оставшейся $(m-1) \times N$-матрицы. Следовательно, для перехода от $\mathbf{M}_{m-1}$ к $\mathbf{M}_m$ нужно соединить две копии матрицы $\mathbf{M}_{m-1}$ и добавить строку $\mathbf{v}^{(m)}$:

$$\mathbf{M}_m = \begin{pmatrix} \mathbf{M}_{m-1} & \mathbf{M}_{m-1} \\ 0\ldots0 & 1\ldots1 \end{pmatrix}. \tag{2.4.4}$$

Рассмотрим столбцы $\mathbf{w}^{(1)}, \ldots, \mathbf{w}^{(m)}$ матрицы $\mathbf{M}_m$, соответствующие числам 1, 2, 4, …, 2^{m-1}: они составляют стандартный базис пространства $\mathcal{H}_{m,2}$:

$$\begin{matrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{matrix}.$$

Тогда столбец с номером $j = \sum\limits_{i=1}^{m} j_i 2^{i-1}$ равен $\sum\limits_{i=1}^{m} j_i \mathbf{w}^{(i)}$. Вектор $\mathbf{v}^{(i)}$ можно интерпретировать как характеристическую функцию множества $\mathcal{A}_i \subset \mathcal{H}_{m,2}$, состоящего из слов с единицей на i-м месте:

$$\mathcal{A}_i = \{j \in \mathcal{H}_{m,2} \colon j_i = 1\}. \tag{2.4.5}$$

В терминах конъюнкции (см. формулу (2.1.6б)) $\mathbf{v}^{(i_1)} \wedge \mathbf{v}^{(i_2)} \wedge \ldots \wedge \mathbf{v}^{(i_k)}$ интерпретируется как характеристическая функция пересечения $\mathcal{A}_{i_1} \cap \ldots \cap \mathcal{A}_{i_k}$. Если все индексы $i_1, \ldots, i_k$ различны, то $\#\Big(\bigcap\limits_{j=1}^{k} \mathcal{A}_{i_j}\Big) = 2^{m-k}$. Иначе говоря, имеет место следующая лемма.

Лемма 2.4.7. *Вес* $w\Big(\bigwedge\limits_{j=1}^{k} \mathbf{v}^{(i_j)}\Big) = 2^{m-k}$.

К важным фактам относится следующая теорема.

Теорема 2.4.8. *Векторы* $\mathbf{v}^{(0)} = 11\ldots1$ *и* $\bigwedge\limits_{j=1}^{k} \mathbf{v}^{(i_j)}$, $1 \leqslant i_1 < \ldots < i_k \leqslant m$, $k = 1, \ldots, m$, *образуют базис пространства* $\mathcal{H}_{N,2}$.

Доказательство. Достаточно проверить, что стандартный базис из N-слов $\mathbf{e}(j) = 0\ldots1\ldots0$ (единица стоит на j-м месте, а остальные — нули) выражается в виде линейной комбинации перечисленных выше век-

торов. Но

$$\mathbf{e}(j) = \bigwedge_{i=1}^{m} (\mathbf{v}^{(i)} + (1 + v_j^{(i)})\mathbf{v}^{(0)}), \quad 0 \leqslant j \leqslant N-1 \tag{2.4.6}$$

(j-й знак у всех сомножителей равен 1, а для любого другого номера l найдётся множитель, у которого на l-м месте стоит 0). □

Пример 2.4.9. Для $m = 4$, $N = 16$ имеем

$$\begin{aligned}
\mathbf{v}^{(0)} &= 1111111111111111\\
\mathbf{v}^{(1)} &= 0101010101010101\\
\mathbf{v}^{(2)} &= 0011001100110011\\
\mathbf{v}^{(3)} &= 0000111100001111\\
\mathbf{v}^{(4)} &= 0000000011111111\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(2)} &= 0001000100010001\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(3)} &= 0000010100000101\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(4)} &= 0000000001010101\\
\mathbf{v}^{(2)} \wedge \mathbf{v}^{(3)} &= 0000001100000011\\
\mathbf{v}^{(2)} \wedge \mathbf{v}^{(4)} &= 0000000000110011\\
\mathbf{v}^{(3)} \wedge \mathbf{v}^{(4)} &= 0000000000001111\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(2)} \wedge \mathbf{v}^{(3)} &= 0000000100000001\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(2)} \wedge \mathbf{v}^{(4)} &= 0000000000010001\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(3)} \wedge \mathbf{v}^{(4)} &= 0000000000000101\\
\mathbf{v}^{(2)} \wedge \mathbf{v}^{(3)} \wedge \mathbf{v}^{(4)} &= 0000000000000011\\
\mathbf{v}^{(1)} \wedge \mathbf{v}^{(2)} \wedge \mathbf{v}^{(3)} \wedge \mathbf{v}^{(4)} &= 0000000000000001
\end{aligned}$$

Определение 2.4.10. Пусть r — такое натуральное число, что $0 \leqslant r \leqslant m$. Кодом Рида—Маллера (РМ) $\mathcal{X}^{\mathrm{PM}}(r, m)$ порядка r называется двоичный код длины $N = 2^m$, натянутый на конъюнкции $\bigwedge_{j=1}^{k} \mathbf{v}^{(i_j)}$ и $\mathbf{v}^{(0)}$, где $1 \leqslant k \leqslant r$ и $1 \leqslant i_1 < \ldots < i_k \leqslant m$. Ранг кода $\mathcal{X}^{\mathrm{PM}}(r, m)$ равен $1 + C_m^1 + \ldots + C_m^r$. □

Итак, $\mathcal{X}^{\mathrm{PM}}(0, m) \subset \mathcal{X}^{\mathrm{PM}}(1, m) \subset \ldots \subset \mathcal{X}^{\mathrm{PM}}(m-1, m) \subset \mathcal{X}^{\mathrm{PM}}(m, m)$. Здесь $\mathcal{X}^{\mathrm{PM}}(m, m) = \mathcal{H}_{N,2}$ — всё пространство Хэмминга и $\mathcal{X}^{\mathrm{PM}}(0, m) = \{00\ldots00, 11\ldots11\}$ — код повторений. Далее, $\mathcal{X}^{\mathrm{PM}}(m-1, m)$ состоит из всех слов $\mathbf{x} \in \mathcal{H}_{N,2}$ чётного веса (коротко: чётных слов). Действительно, любой базисный вектор чётен, поэтому

$$w(\mathbf{x} + \mathbf{x}') = w(\mathbf{x}) + w(\mathbf{x}') - 2w(\mathbf{x} \wedge \mathbf{x}')$$

тоже чётно. Значит, все кодовые слова $\mathbf{x} \in \mathcal{X}^{\mathrm{PM}}(m-1, m)$ чётны. Наконец, $\dim \mathcal{X}^{\mathrm{PM}}(m-1, m) = N-1$ совпадает с размерностью подпространства всех чётных слов, что доказывает утверждение. Так как $\mathcal{X}^{\mathrm{PM}}(r, m) \subset \subset \mathcal{X}^{\mathrm{PM}}(m-1, m)$ при $r \leqslant m-1$, любой код РМ состоит из чётных слов.

Двойственный код — это $\mathcal{X}^{\mathrm{PM}}(r,\, m)^{\perp} = \mathcal{X}^{\mathrm{PM}}(m-r-1,\, m)$. Действительно, если $\mathbf{a} \in \mathcal{X}^{\mathrm{PM}}(r,\, m)$, $\mathbf{b} \in \mathcal{X}^{\mathrm{PM}}(m-r-1,\, m)$, то конъюнкция $\mathbf{a} \wedge \mathbf{b}$ — чётное слово и поэтому $\langle \mathbf{a} \cdot \mathbf{b} \rangle = 0$. Но

$$\dim(\mathcal{X}^{\mathrm{PM}}(r,\, m)) + \dim(\mathcal{X}^{\mathrm{PM}}(m-r-1,\, m)) = N,$$

откуда следует утверждение. В качестве следствия получаем, что код $\mathcal{X}^{\mathrm{PM}}(m-2,\, m)$ — продолжение с контролем чётности кода Хэмминга.

По определению кодовые слова $\mathbf{x} \in \mathcal{X}^{\mathrm{PM}}(r,\, m)$ ассоциированы с $\wedge$-полиномами от независимых «переменных» $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m)}$ с коэффициентами 0 и 1, степень которых не превышает r (здесь степень полинома — это максимальное количество переменных $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m)}$ в складываемых мономах). Мономом нулевой степени считается многочлен, пропорциональный $\mathbf{v}^{(0)}$.

Запишем это соответствие в виде формулы

$$\mathbf{x} \in \mathcal{X}^{\mathrm{PM}}(r,\, m) \leftrightarrow p_{\mathbf{x}}(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m)}), \quad \deg p_{\mathbf{x}} \leqslant r. \tag{2.4.7}$$

Каждый такой полином можно записать в виде

$$p_{\mathbf{x}}(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m)}) = \mathbf{v}^{(m)} \wedge q(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m-1)}) + l(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m-1)}),$$

где $\deg q \leqslant r-1$, $\deg l \leqslant r$. У слова $\mathbf{v}^{(m)} \wedge q(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m-1)})$ на первых 2^{m-1} местах стоят нули.

В тех же обозначениях можно записать

$$\begin{aligned} &q(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m-1)}) \leftrightarrow \mathbf{b} \in \mathcal{X}^{\mathrm{PM}}(r-1,\, m-1), \\ &l(\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m-1)}) \leftrightarrow \mathbf{a} \in \mathcal{X}^{\mathrm{PM}}(r,\, m-1). \end{aligned} \tag{2.4.8}$$

Кроме того, 2^m-слово $\mathbf{x}$ можно представить как сумму сцеплений 2^{m-1}-слов:

$$\mathbf{x} = (\mathbf{a}\,|\,\mathbf{a}) + (\mathbf{0}\,|\,\mathbf{b}) = (\mathbf{a}\,|\,\mathbf{a}+\mathbf{b}). \tag{2.4.9}$$

Это означает, что коды Рида—Маллера связаны посредством конструкции бар-произведения (см. пример 2.1.8, п. 8):

$$\mathcal{X}^{\mathrm{PM}}(r,\, m) = \mathcal{X}^{\mathrm{PM}}(r,\, m-1) \bar{|} \mathcal{X}^{\mathrm{PM}}(r-1,\, m-1). \tag{2.4.10}$$

Следовательно, по индукции находим, что

$$d(\mathcal{X}^{\mathrm{PM}}(r,\, m)) = 2^{m-r}. \tag{2.4.11}$$

Действительно, при $m = r = 0$ $d(\mathcal{X}^{\mathrm{PM}}(0,\, 0)) = 2^m$ и при всех m $d(\mathcal{X}^{\mathrm{PM}}(m,\, m)) = 1 = 2^0$. Предположим, что $d(\mathcal{X}^{\mathrm{PM}}(r-1,\, \tilde{m}) = 2^{\tilde{m}-r+1}$ для всех $\tilde{m} \geqslant r-1$ и $d(\mathcal{X}^{\mathrm{PM}}(r-1,\, m-1)) = 2^{m-r}$. Тогда, ср. (2.4.13),

$$\begin{aligned} d(\mathcal{X}^{\mathrm{PM}}(r,\, m)) &= \min\{2d(\mathcal{X}^{\mathrm{PM}}(r,\, m-1)),\, d(\mathcal{X}^{\mathrm{PM}}(r-1,\, m-1))\} = \\ &= \min\{2 \times 2^{m-1-r},\, 2^{m-1-r+1}\} = 2^{m-r}. \end{aligned} \tag{2.4.12}$$

В итоге получаем теорему.

Теорема 2.4.11. *Код РМ* $\mathcal{X}^{\mathrm{PM}}(r, m)$ *при* $0 \leqslant r \leqslant m$ *является двоичным кодом длины* $N = 2^m$, *ранга* $k = \sum\limits_{l=1}^{r} C_N^l$ *и с расстоянием* $d = 2^{m-r}$. *Более того*,

1) $\mathcal{X}^{\mathrm{PM}}(0, m) = \{0 \ldots 0, 1 \ldots 1\} \subset \mathcal{X}^{\mathrm{PM}}(1, m) \subset \ldots \subset \mathcal{X}^{\mathrm{PM}}(m-1, m) \subset \subset \mathcal{X}^{\mathrm{PM}}(m, m) = \mathcal{H}_{N,2}$; $\mathcal{X}^{\mathrm{PM}}(m-1, m)$ — *множество всех чётных* N*-слов и* $\mathcal{X}^{\mathrm{PM}}(m-2, m)$ — *расширение с контролем чётности* $[2^m - 1, 2^m - 1 - m]$*-кода Хэмминга*,

2) $\mathcal{X}^{\mathrm{PM}}(r, m) = \mathcal{X}^{\mathrm{PM}}(r, m-1) \overline{|} \mathcal{X}^{\mathrm{PM}}(r-1, m-1)$, $1 \leqslant r \leqslant m-1$,

3) $\mathcal{X}^{\mathrm{PM}}(r, m)^{\perp} = \mathcal{X}^{\mathrm{PM}}(m-r-1, m)$, $0 \leqslant r \leqslant m-1$.

A Detective Story in a Correcting Facility
Детективная история в исправительном заведении

The Parity Checkpoint Charlie[5]
Контрольно-пропускной пункт «Чарли»

The Generating Matrix Revolutions Reloaded[6]
Перезагрузка генерирующей матрицы революций

(Из серии «Фильмы, которые не вышли на большой экран».)

Пример 2.4.12. Определим бар-произведение $\mathcal{X}_1 \overline{|} \mathcal{X}_2$ двоичных линейных кодов $\mathcal{X}_1$ и $\mathcal{X}_2$, где $\mathcal{X}_2$ — подкод кода $\mathcal{X}_1$. Выразите ранг и минимальное расстояние кода $\mathcal{X}_1 \overline{|} \mathcal{X}_2$ через соответствующие параметры кодов $\mathcal{X}_1$ и $\mathcal{X}_2$. Покажите, что если $\mathcal{X}^{\perp}$ обозначает двойственный код к коду $\mathcal{X}$, то

$$(\mathcal{X}_1 \overline{|} \mathcal{X}_2)^{\perp} = \mathcal{X}_2^{\perp} \overline{|} \mathcal{X}_1^{\perp}.$$

С помощью конструкции бар-произведения или любым другим способом определите код Рида—Маллера $\mathcal{X}^{\mathrm{PM}}(r, m)$ для $0 \leqslant r \leqslant m$. Покажите, что при $0 \leqslant r \leqslant m-1$ код, двойственный коду $\mathcal{X}^{\mathrm{PM}}(r, m)$, тоже является кодом Рида—Маллера.

Решение. Бар-произведение $\mathcal{X}_1 \overline{|} \mathcal{X}_2$ двух линейных кодов $\mathcal{X}_2 \subseteq \mathcal{X}_1 \subseteq \mathbb{F}_2^N$ — это линейный код длины $2N$, определяемый как

$$\mathcal{X}_1 \overline{|} \mathcal{X}_2 = \{(\mathbf{x} \,|\, \mathbf{x} + \mathbf{y}) \colon \mathbf{x} \in \mathcal{X}_1, \ \ \mathbf{y} \in \mathcal{X}_2\}.$$

Если $\mathbf{x}_1, \ldots, \mathbf{x}_k$ и $\mathbf{y}_1, \ldots, \mathbf{y}_l$ — базисы кодов $\mathcal{X}_2$ и $\mathcal{X}_1$ соответственно, то базисом их бар-произведения $\mathcal{X}_1 \overline{|} \mathcal{X}_2$ будет

$$(\mathbf{x}_1 \,|\, \mathbf{x}_1), \ \ldots, \ (\mathbf{x}_k \,|\, \mathbf{x}_k), \ (\mathbf{0} \,|\, \mathbf{y}_1), \ \ldots, \ (\mathbf{0} \,|\, \mathbf{y}_l),$$

[5]Пограничный пункт между Восточным и Западным Берлином в годы холодной войны. Ныне популярное место туризма.

[6]Ср. с названиями фильмов «The Matrix Reloaded» и «The Matrix Revolution» (хиты 2000-х годов).

и ранг произведения $\mathcal{X}_1|\mathcal{X}_2$ будет равен сумме рангов сомножителей $\mathcal{X}_1$ и $\mathcal{X}_2$.

Далее мы проверим, что минимальное расстояние определяется формулой

$$d(\mathcal{X}_1|\mathcal{X}_2) = \min[2d(\mathcal{X}_1),\, d(\mathcal{X}_2)]. \tag{2.4.13}$$

Действительно, пусть $\mathbf{0} \neq (\mathbf{x}\,|\,\mathbf{x}+\mathbf{y}) \in \mathcal{X}_1|\mathcal{X}_2$. Если $\mathbf{y} \neq \mathbf{0}$, то $w(\mathbf{x}\,|\,\mathbf{x}+\mathbf{y}) \geqslant$ $\geqslant w(\mathbf{y}) \geqslant d(\mathcal{X}_2)$. Если $\mathbf{y} = \mathbf{0}$, то $w(\mathbf{x}\,|\,\mathbf{x}+\mathbf{y}) = 2w(\mathbf{x}) \geqslant 2d(\mathcal{X}_1)$. Отсюда следует, что

$$d(\mathcal{X}_1|\mathcal{X}_2) \geqslant \min[2d(\mathcal{X}_1),\, d(\mathcal{X}_2)]. \tag{2.4.14}$$

С другой стороны, если вес слова $\mathbf{x} \in \mathcal{X}_1$ равен $w(\mathbf{x}) = d(\mathcal{X}_1)$, то $d(\mathcal{X}_1|\mathcal{X}_2) \leqslant$ $\leqslant w(\mathbf{x}\,|\,\mathbf{x}) = 2d(\mathcal{X}_1)$. Наконец, если вес слова $\mathbf{y} \in \mathcal{X}_2$ равен $w(\mathbf{y}) = d(\mathcal{X}_2)$, то $d(\mathcal{X}_1|\mathcal{X}_2) \leqslant w(\mathbf{0}\,|\,\mathbf{y}) = d(\mathcal{X}_2)$. Мы заключаем, что

$$d(\mathcal{X}_1|\mathcal{X}_2) \leqslant \min[2d(\mathcal{X}_1),\, d(\mathcal{X}_2)], \tag{2.4.15}$$

что доказывает равенство (2.4.13).

Теперь проверим включение

$$(\mathcal{X}_2^{\perp}|\mathcal{X}_1^{\perp}) \subseteq (\mathcal{X}_1|\mathcal{X}_2)^{\perp}.$$

Действительно, пусть $(\mathbf{u}\,|\,\mathbf{u}+\mathbf{v}) \in \mathcal{X}_2^{\perp}|\mathcal{X}_1^{\perp}$ и $(\mathbf{x}\,|\,\mathbf{x}+\mathbf{y}) \in (\mathcal{X}_1|\mathcal{X}_2)$. Найдём скалярное произведение:

$$\langle(\mathbf{u}\,|\,\mathbf{u}+\mathbf{v})\cdot(\mathbf{x}\,|\,\mathbf{x}+\mathbf{y})\rangle = \mathbf{u}\cdot\mathbf{x} + (\mathbf{u}+\mathbf{v})\cdot(\mathbf{x}+\mathbf{y}) = \mathbf{u}\cdot\mathbf{y} + \mathbf{v}\cdot(\mathbf{x}+\mathbf{y}) = 0.$$

так как $\mathbf{u} \in \mathcal{X}_2^{\perp}$, $\mathbf{y} \in \mathcal{X}_2$, $\mathbf{v} \in \mathcal{X}_1^{\perp}$ и $(\mathbf{x}+\mathbf{y}) \in \mathcal{X}_1$. Кроме того, мы знаем, что

$$\dim(\mathcal{X}_2^{\perp}|\mathcal{X}_1^{\perp}) = N - \dim(\mathcal{X}_2) + N - \dim(\mathcal{X}_1) =$$
$$= 2N - \dim(\mathcal{X}_1|\mathcal{X}_2) = \dim(\mathcal{X}_1|\mathcal{X}_2)^{\perp}.$$

Отсюда фактически следует, что

$$(\mathcal{X}_1|\mathcal{X}_2)^{\perp} = \mathcal{X}_2^{\perp}|\mathcal{X}_1^{\perp}. \tag{2.4.16}$$

Вернёмся к кодам РМ. Они определяются следующим образом:

$\mathcal{X}^{\mathrm{PM}}(0,\, m)$ = двоичный код повторений длины $N = 2^m$,

$\mathcal{X}^{\mathrm{PM}}(m,\, m)$ = всё пространство $\mathcal{H}_{N,2}$ длины $N = 2^m$,

$\mathcal{X}^{\mathrm{PM}}(r,\, m)$ при $0 < r < m$ определяется рекуррентно по формуле

$\mathcal{X}^{\mathrm{PM}}(r,\, m) = \mathcal{X}^{\mathrm{PM}}(r,\, m-1)|\mathcal{X}^{\mathrm{PM}}(r-1,\, m-1)$.

При этом ранг кода $\mathcal{X}^{\mathrm{PM}}(r,\, m)$ равен $\sum\limits_{j=0}^{r} C_m^j$, а его минимальное расстояние — 2^{m-r}. В частности, $\mathcal{X}^{\mathrm{PM}}(m-1,\, m)$ — это код проверки на чётность

и, следовательно, двойственный коду $\mathcal{X}^{\mathrm{PM}}(0,\, m)$. Приведем альтернативное доказательство того, что при $0 \leqslant r \leqslant m-1$ имеет место двойственность:

$$\mathcal{X}^{\mathrm{PM}}(r,\, m)^{\perp} = \mathcal{X}^{\mathrm{PM}}(m-r-1,\, m).$$

Это можно сделать индукцией по $m \geqslant 3$: по индуктивному предположению равенство $\mathcal{X}^{\mathrm{PM}}(r,\, m-1)^{\perp} = \mathcal{X}^{\mathrm{PM}}(m-r-2,\, m-1)$ выполнено при $0 \leqslant r < m-1$. Тогда при $0 \leqslant r < m$ получаем

$$\begin{aligned}\mathcal{X}^{\mathrm{PM}}(r,\, m)^{\perp} &= (\mathcal{X}^{\mathrm{PM}}(r,\, m-1) \,\bar{|}\, \mathcal{X}^{\mathrm{PM}}(r-1,\, m-1))^{\perp} = \\ &= \mathcal{X}^{\mathrm{PM}}(r-1,\, m-1)^{\perp} \,\bar{|}\, \mathcal{X}^{\mathrm{PM}}(r,\, m-1)^{\perp} = \\ &= \mathcal{X}^{\mathrm{PM}}(m-r-1,\, m-1) \,\bar{|}\, \mathcal{X}^{\mathrm{PM}}(m-r-2,\, m-1) = \\ &= \mathcal{X}^{\mathrm{PM}}(m-r-1,\, m). \quad \square\end{aligned}$$

Кодирование и декодирование кодов PM основывается на следующем наблюдении. Благодаря формуле (2.4.6) конъюнкция $\mathbf{v}^{(i_1)} \wedge \ldots \wedge \mathbf{v}^{(i_k)}$ возникает при раскрытии $\mathbf{e}(j) \in \mathcal{H}_{m,2}$ тогда и только тогда, когда $v_j^{(i)} = 0$ для всех $i \notin \{i_1,\, \ldots,\, i_k\}$.

Определение 2.4.13. Для $1 \leqslant i_1 < \ldots < i_k \leqslant m$ определим

$$C(i_1,\, \ldots,\, i_k) := \text{множество всех целых чисел } j = \sum_{i=1}^{m} j_i 2^{i-1},$$

$$j_i = 0 \text{ для } i \notin \{i_1,\, \ldots,\, i_k\}. \quad (2.4.17)$$

Для пустого множества ($k = 0$) положим $C(\varnothing) = \{1,\, \ldots,\, 2^m - 1\}$. Более того, положим

$$C(i_1,\, \ldots,\, i_k) + t = \{j + t\colon j \in C(i_1,\, \ldots,\, i_k)\}. \quad (2.4.18)$$

$\square$

Тогда ввиду формулы (2.4.6) для всех $\mathbf{y} = y_0 \ldots y_{N-1} \in \mathcal{H}_{N,2}$ имеем

$$\mathbf{y} = \sum_{k=0}^{m} \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant m} \left(\sum_{j \in C(i_1,\ldots,i_k)} y_j \right) \mathbf{v}^{(i_1)} \wedge \ldots \wedge \mathbf{v}^{(i_k)} \quad (2.4.19)$$

(для $k = 0$ берём $\mathbf{y} = \mathbf{v}^{(0)}$).

Чтобы закодировать последовательность $a = a_0 \ldots a_{k-1}$ информационных символов из $\mathcal{H}_{k,2}$, где $k = 1 + C_m^1 + \ldots + C_m^r$, кодом $\mathcal{X}^{\mathrm{PM}}(r,\, m)$, перепишем её в виде $(a_{i_1,\ldots,i_l})$; здесь $i_1,\, \ldots,\, i_l$ — последовательность номеров позиций, занятых единицами. Тогда построим кодовое слово как $\mathbf{x} = x_0 \ldots x_{N-1} \in \mathcal{X}^{\mathrm{PM}}(r,\, m)$, где

$$\mathbf{x} = \sum_{l=0}^{r} \sum_{1 \leqslant i_1 < \ldots < i_l \leqslant m} a_{i_1,\ldots,i_l} \mathbf{v}^{(i_1)} \wedge \ldots \wedge \mathbf{v}^{(i_l)}. \quad (2.4.20)$$

Мы видим, что «информационное пространство» $\mathcal{H}_{k,2}$ вкладывается в $\mathcal{H}_{N,2}$ при отождествлении элементов $a_j \sim a_{i_1,\dots,i_l}$, где $j = j_0 2^0 + j_1 2^1 + \dots$ $\dots j_{m-1} 2^{m-1}$ и $i_1, \dots, i_l$ — последовательность позиций, на которых стоят единицы, среди $j_1, \dots, j_m$, $1 \leqslant l \leqslant r$. При таком отождествлении мы получаем следующий результат.

Лемма 2.4.14. *Для всех l, $0 \leqslant l \leqslant m$ и $i_1, \dots, i_l$, $1 \leqslant i_1 < \dots < i_l \leqslant m$, выполнено равенство*

$$\sum_{j \in C(i_1,\dots,i_l)} x_j = \begin{cases} a_{i_1,\dots,i_l}, & \text{если } l \leqslant r, \\ 0, & \text{если } l > r. \end{cases} \tag{2.4.21}$$

Доказательство следует из формулы (2.4.19). □

Лемма 2.4.15. *Для всех $i_1, \dots, i_l$, $1 \leqslant i_1 < \dots < i_r \leqslant m$, и для любого t, $1 \leqslant t \leqslant m$, такого что $t \notin \{i_1, \dots, i_r\}$, выполнено равенство*

$$a_{i_1,\dots,i_r} = \sum_{j \in C(i_1,\dots,i_r) + 2^{t-1}} x_j. \tag{2.4.22}$$

Доказательство. Доказательство следует из того факта, что $C(i_1, \dots, i_r, t)$ — это объединение непересекающихся подмножеств $C(i_1, \dots, i_r) \cup (C(i_1, \dots, i_r) + 2^{t-1})$, и равенства $\sum\limits_{j \in C(i_1,\dots,i_r,t)} x_j = 0$ (см. формулу (2.4.18)). □

Более того, верна следующая теорема.

Теорема 2.4.16. *Для любого информационного символа $a_{i_1,\dots,i_r}$, соответствующего слову $\mathbf{v}^{(i_1,\dots,i_r)}$, можно расщепить множество $\{0, \dots, N-1\}$ на 2^{m-r} таких непересекающихся подмножеств S по 2^r элементов каждое, что для каждого такого S выполнено равенство*: $a_{i_1,\dots,i_r} = \sum\limits_{j \in S} x_j$.

Доказательство. Список множеств S начинается с множества $C(i_1, \dots, i_r)$ и продолжается $m - r$ непересекающимися подмножествами $C(i_1, \dots, i_r) + 2^{t-1}$, где $1 \leqslant t \leqslant m$, $t \notin \{i_1, \dots, i_r\}$. Далее, возьмём такую произвольную пару $1 \leqslant t_1 < t_2 \leqslant m$, что $\{t_1, t_2\} \cap \{i_1, \dots, i_r\} = \varnothing$. Тогда множество $C(i_1, \dots, i_r, t_1, t_2)$ содержит непересекающиеся подмножества $C(i_1, \dots, i_r)$, $C(i_1, \dots, i_r) + 2^{t_1-1}$ и $C(i_1, \dots, i_r) + 2^{t_2-1}$, причём для каждого из них $a_{i_1,\dots,i_r} = \sum\limits_{j \in C(i_1,\dots,i_r) + 2^{t_k-1}} x_j$, $k = 1, 2$. Тогда то же самое верно для оставшихся множеств

$$C(i_1, \dots, i_r) + 2^{t_1-1} + 2^{t_2-1} = C(i_1, \dots, i_r, t_1, t_2) \setminus$$
$$\setminus [C(i_1, \dots, i_r) \cup (C(i_1, \dots, i_r) + 2^{t_1-1}) \cup (C(i_1, \dots, i_r) + 2^{t_2-1})]. \tag{2.4.23}$$

Существует C_{m-r}^2 из них, и они всё ещё не пересекаются ни друг с другом, ни с предыдущими множествами. Множества (2.4.23) образуют дальнейший пучок множеств S.

И так далее: в общем виде множество S можно записать как

$$C(i_1, \ldots, i_r) + 2^{t_1-1} + \ldots + 2^{t_s-1},$$

что совпадает с разностью множеств

$$C(i_1, \ldots, i_r, t_1, \ldots, t_s) \Big\backslash \Big(\bigcup_{\{t'_1,\ldots,t'_{s'}\} \subset \{t_1,\ldots,t_s\}} (C(i_1, \ldots, i_r) + 2^{t'_1-1} + \cdots 2^{t'_{s'}-1}) \Big). \tag{2.4.24}$$

Каждое такое множество отмечено набором $\{i_1, \ldots, i_s\}$, где $0 \leqslant s \leqslant m-r$, $t_1 < \ldots < t_s$ и $\{t_1, \ldots, t_s\} \cap \{i_1, \ldots, i_r\} = \varnothing$. (Объединение $\bigcup\limits_{\{t'_1,\ldots,t'_{s'}\} \subset \{i_1,\ldots,i_r\}}$ в формуле (2.4.24) берётся по всем «строгим» подмножествам $\{t'_1, \ldots, t'_{s'}\}$ в множестве $\{i_1, \ldots, i_r\}$, $t'_1 < \ldots < t'_{s'}$ и $s' = 0, \ldots s-1$ (случай $s' = 0$ соответствует пустому подмножеству). Общее число подмножеств $C(i_1, \ldots, i_r)$ равно 2^{m-r}, и каждое из них по построению состоит из 2^r элементов. □

Теорема 2.4.16 обосновывает так называемое *мажоритарное* декодирование кодов Рида—Маллера. А именно, получив слово $\mathbf{y} = y_0 \ldots y_{N-1}$, произошедшее из кодового слова $\hat{\mathbf{x}} \in \mathcal{X}^{\mathrm{PM}}(r, m)$, мы берём произвольный набор $i_1, \ldots, i_r$, $1 < i_1 < \ldots < i_r \leqslant m$, и рассматриваем суммы $\sum\limits_{j \in C} y_j$ для всех 2^{m-r} описанных ранее множеств S. Если $\mathbf{y} \in \mathcal{X}^{\mathrm{PM}}(r, m)$, то все эти суммы совпадают и дают $a_{i_1,\ldots,i_r}$. Если число ошибок в $\mathbf{y}$ (т. е. расстояние Хэмминга $\delta(\hat{\mathbf{x}}, \mathbf{y})$) меньше чем $2^{m-r-1} = d(\mathcal{X}^{\mathrm{PM}}(r, m))/2$, то большинство сумм всё ещё будут давать правильный результат $a_{i_1,\ldots,i_r}$ (наихудший случай — когда каждое множество S не содержит ни одной или содержит единственную ошибку). Меняя множество $\{i_1, \ldots, i_r\}$, мы определим кодовое слово $\mathbf{x}^{(1)} \in \mathcal{X}^{\mathrm{PM}}(r, m)$, содержащее лишь мономы степени r. Заметим,что $\hat{\mathbf{x}} - \mathbf{x}^{(1)}$ будет кодовым словом кода $\mathcal{X}^{\mathrm{PM}}(r-1, m)$.

Теперь $\mathbf{y}$ можно «уменьшить» до $\mathbf{y} - \mathbf{x}^{(1)}$ и уменьшенное слово $\mathbf{y} - \mathbf{x}^{(1)}$ будет иметь $\delta(\hat{\mathbf{x}} - \mathbf{x}^{(1)}, \mathbf{y} - \mathbf{x}^{(1)}) = \delta(\hat{\mathbf{x}}, \mathbf{y})$ ошибок, что меньше чем $2^{m-r} = d(\mathcal{X}^{\mathrm{PM}}(r-1, m))/2$. Мы можем повторить описанную процедуру и получить корректный ответ $a_{i_1,\ldots,i_{r-1}}$ для любого набора $1 \leqslant i_1 < \ldots i_{r-1} \leqslant m$, и т. д. В итоге мы восстановим всю последовательность информационных символов $a_{i_1,\ldots,i_r}$.

Таким образом, любое слово $\mathbf{y} \in \mathcal{H}_{N,2}$ с расстоянием $\delta(\mathbf{y}, \mathcal{X}^{\mathrm{PM}}(r, m)) < d(\mathcal{X}^{\mathrm{PM}}(r, m)))$ однозначно декодируется.

... correct, insert, refine, enlarge, diminish, interline.
... исправлять, вставлять, уточнять, увеличивать, уменьшать, вписывать между строк.

Джонатан Свифт (1667–1745),
англо-ирландский писатель

Коды Рида—Маллера были открыты в начале 1950-х гг. Дэвидом Маллером (1924–2008), а Ирвинг Рид (1923–2012) предложил изложенную выше процедуру декодирования. В начале 1970-х гг. коды РМ были использованы для передачи снимков с космических аппаратов (на расстояниях, сравнимых с расстоянием до Луны). Качество передачи расценивалось тогда как исключительно хорошее. Тем не менее, позже, во время фотографирования Юпитера и Сатурна инженеры НАСА отдали предпочтение кодам Голея.

Дэвид Маллер родился в ноябре 1924 года в г. Остин, Техас, где его отец, Герман Джозеф Маллер, был профессором генетики. Г. Д. Маллер получил Нобелевскую премию по физиологии и медицине в 1946 г. В 1933 г. семья Малера переехала в Ленинград, где его отец работал в Институте генетики до 1937 г. В 1933 году Г. Д. Маллер был избран член-корреспондентом АН СССР. Однако в 1948 г. он направил в адрес АН СССР письмо с отказом от этого звания в знак протеста против преследования генетики в СССР (в 1990 г. звание было восстановлено). Многие детали жизни Дэвида между 1935 г. и началом 1940-х гг. не ясны, поскольку его родители развелись в 1935 г. Во всяком случае, известно, что Дэвид и его мать вернулись в Остин в 1934 г., в 1947 г. он закончил Калифорнийский технологический институт, Пасадена, а в 1951 г. закончил там же аспирантуру и защитил диссертацию. Сразу после этого он начал работать в департаменте математики университета Иллинойса, а позднее перешел в университет Нью-Мексико, где работал до выхода на пенсию в 1992 г.

Основные научные интересы Дэвида Малера относились к теории автоматов и переключательных схем, кодированию и теории сложности. По отзывам коллег Дэвид был застенчивым и необщительным человеком[7], было нелегко установить с ним творческий контакт, но в случае успеха он длился десятилетиями. Дэвид был глубоким мыслителем и исключительно знающим ученым. Нередко он проводил долгие часы с соавтором, всесторонне анализируя трудную задачу. Наконец наступал момент просветления, когда открывался путь к ее решению. Дэвид преображался и начинал искать наиболее элегантный путь изложения. У него была привычка аккуратно записывать свои мысли, примеры, теоремы и т. д. в тетради большого формата, используя чернильницу и старинную ручку, эти тетради нумеровались римскими цифрами. Тетради Дэвида все еще хранятся его бывшими соавторами (один из них сообщил, что хранит тетрадь под номером XXXVII), возможно, что многое из их содержания все еще имеет значительный научный интерес.

Ирвинг Стой Рид (1923–2012) внёс значительный вклад в развитие ряда областей электроники. Он, в частности, участвовал в 1950 г. в создании Magnetic Drum Digital Differential Analyzer (MADDIDA), одного из первых цифровых компьютеров. Когда Рид и его соавторы показали прототип компьютера MADDIDA Джону фон-Нейману, они запрограммировали вычисление одной сложной специальной функции. Фон-Нейман, известный своими быстрыми вычислениями в уме и на бумаге, был в состоянии получить результат более или менее одновременно с компьютером и, тем самым, проверить всё на месте. Их ответы совпали, и фон-Нейман дал добро на завершение проекта. Позднее, в 1960-е гг., Рид участвовал в создании навигационной системы для крылатых ракет "Snark".

[7] private and unassuming personality

Одна из историй, доступных в интернете, относится к его ранним годам в Калифорнийском Технологическом институте, где Рид изучал математику. Поскольку он не закончил необходимого курса по физике и, тем самым, не выполнил условие для получения диплома, его собирались призвать на службу в Военно-Морской флот США (аналогичная практика существовала в бывшем СССР до его распада: неудачливые студенты неизбежно забирались на военную службу, где нередко подвергались унижениям со стороны других военнослужащих). Для того, чтобы получить диплом об окончании КАЛТЕХа, Рид должен был добиться специального разрешения от Роберта Милликена, который в то время являлся ректором КАЛТЕХа. Милликен был в свое время преподавателем курса физики, а в последствии получил Нобелевскую премию; в КАЛТЕХе он неуклонно следил за соблюдением установленных правил, в особенности, применительно к студентам-математикам, пренебрежительно относившихся к физике, как к нестрогой дисциплине. (Подобное отношение профессоров-физиков к блестящим, но самоуверенным студентам-математикам, которые превозносят математику, но с пренебрежением относятся к физике, нередко наблюдается во многих университетах.) К счастью для Рида, когда он вошёл в кабинет Милликена с просьбой о получении диплома, он заметил оттиски своих опубликованных статей на его рабочем столе и обратил на это внимание ректора. Милликен улыбнулся и подписал распоряжение о выдаче диплома.

Пример 2.4.17. Кодом с максимально достижимым расстоянием (м. д. р.) называется такой q-ичный линейный $[N, k, d]$-код, что $d = N - k + 1$ (равенство в границе Синглтона, см. определение 2.1.13).

1. Докажите, что код $\mathcal{X}$ принадлежит семейству м. д. р. тогда и только тогда, когда 1) любые $N - k$ столбцов его проверочной матрицы H линейно независимы и 2) в ней найдётся $N - k + 1$ линейно зависимых столбцов.

2. Докажите, что двойственный код к м. д. р.-коду тоже м. д. р.-код и выведите отсюда, что код $\mathcal{X}$ — м. д. р.-код, тогда и только тогда, когда любые k столбцов его порождающей матрицы G линейно независимы и k — максимальное число с таким свойством.

3. Докажите, что если матрица G записана в каноническом виде, $(\mathbf{1}_k \,|\, G')$, то $\mathcal{X}$ — м. д. р.-код , тогда и только тогда, когда любая квадратная подматрица в G' невырождена.

4. Проверьте, что $[N, k, d]$-код является м. д. р., тогда и только тогда, когда для любых d позиций $1 \leqslant i_1 < \ldots < i_d \leqslant N$ существует кодовое слово веса d с ненулевыми символами на позициях $i_1, \ldots, i_d$.

Решение. 1. Минимальное расстояние $[N, k, d]$-м. д. р.-кода равно $d = N - k - 1$. Если линейный код $\mathcal{X}$ имеет $d(\mathcal{X}) = d$, то любые $(d - 1)$ столбцов его проверочной матрицы H линейно независимы, причём это максимальное число с таким свойством, и наоборот. Значит, любые $(N - k)$ столбцов матрицы H линейно независимы, и $(N - k)$ — максимальное число с таким свойством, и наоборот. Равносильное утверждение заключается в том, что любые $(N - k) \times (N - k)$-подматрицы в H обратимы.

2. Пусть $\mathcal{X}$ — $[N, k, d]$ м. д. р.-код с проверочной матрицей H. Тогда H — порождающая матрица двойственного кода $\mathcal{X}^\perp$. Любая $(N - k) \times (N - k)$-подматрица в H обратима. Значит, любая нетриви-

альная комбинация строк матрицы H^{T} имеет не более $N-k-1$ нулевых элементов, т. е. вес не менее чем $k+1$; минимальный вес равен $k+1$. Таким образом, $d(\mathcal{X}^{\perp}) = k+1 = N-(N-k)+1$, а так как $\mathcal{X}^{\perp}$ — это $[N, N-k]$-код, он тоже является м. д. р.

Таким образом, $[N, k]$-код $\mathcal{X}$ является м. д. р.-кодом, тогда и только тогда, когда k — это максимальное из чисел l, для которых любые l столбцов порождающей матрицы G линейно независимы. Эквивалентно, $\mathcal{X}$ систематический в любых k позициях.

3. И вновь, пусть $\mathcal{X}$ — $[N, k, d]$ м. д. р.-код, и $G = (\mathbf{1}_k \,|\, G')$. Возьмём $u \times u$-подматрицу $\tilde{G}_u$ в G'. За счёт перестановок строк и столбцов можно считать, что $\tilde{G}_u$ расположена в левом верхнем углу матрицы G'. Рассмотрим последние $k-u$ столбцов матрицы $\mathbf{1}_k$ и u столбцов матрицы G', содержащих $\tilde{G}_u$; соответствующая $k \times k$-подматрица G_k неособа и имеет вид

$$G_k = \begin{pmatrix} 0 & \tilde{G}_u \\ \mathbf{1}_{k-u} & * \end{pmatrix},$$

причём

$$\det G_k = \pm \det \tilde{G}_u \det \mathbf{1}_{k-u} = \pm \det \tilde{G}_u \neq 0 \quad \text{по п. 2.}$$

Таким образом, матрица $\tilde{G}_u$ тоже неособа. Доказательство обратного утверждения получается аналогично.

4. Выберем, наконец, $d = N-k+1$ символов, скажем $i_1, \ldots, i_d$. Рассмотрим i_1 вместе с оставшимися символами $j_1, \ldots, j_{k-1}$. Тогда символы с номерами $i_1, j_1, \ldots, j_{k-1}$ являются информационными. Поэтому существует кодовое слово $\mathbf{x}^{(i)}$ с ненулевым i_1-символом и нулевыми символами с номерами $j_1, \ldots, j_{k-1}$. Поскольку минимальное расстояние кода равно d, все символы с номерами $i_1, \ldots, i_d$ у слова $\mathbf{x} = \sum\limits_{i=1}^{d} \mathbf{x}^{(i)}$ должны быть отличны от нуля. В обратную сторону, если сумма любых d столбцов матрицы H равна $\mathbf{0}$, то $\dim H^{\perp} = N-k < d$, т. е. $N-k+1 \leqslant d$, откуда по неравенству Синглтона $N-k+1 = d$ и код является м. д. р. □

Пример 2.4.18. М. д. р.-коды $[N, N, 1]$, $[N, 1, N]$ и $[N, N-1, 2]$ существуют и являются тривиальными. Любой $[N, k]$-м. д. р. код, для которого $2 \leqslant k \leqslant N-2$ называется нетривиальным. Покажите, что не существует нетривиальных м. д. р.-кодов над полем $\mathbb{F}_q$, $q \leqslant k \leqslant N-q$. В частности, не существует нетривиального двоичного м. д. р.-кода (что вызывает заметное отсутствие интереса к работе с двоичными м. д. р.-кодами).

Решение. Действительно, $[N, N, 1]$, $[N, 1, N]$ и $[N, N-1, 2]$-коды являются м. д. р.-кодами. Выберем $q \leqslant k \leqslant N-q$ и предположим, что $\mathcal{X}$ — q-ичный м. д. р.-код. Возьмём его порождающую матрицу G в каноническом виде $(\mathbf{1}_k \,|\, G')$, где размер матрицы G' равен $k \times (N-k)$, $N-k \geqslant q$.

Если некоторые элементы в столбце матрицы G' нулевые, тогда этот столбец является линейной комбинацией $k-1$ столбца матрицы $\mathbf{1}_{k-1}$. Но это невозможно по п. 2 примера 2.4.17, значит, G' не имеет нулевых элементов. Предположим, далее, что первая строка матрицы G' равна $11\ldots1$: в противном случае можно умножить столбцы на подходящие константы, переходя к эквивалентному коду.

Теперь возьмём вторую строку матрицы G': её длина равна $N-k \geqslant q$ и она не имеет нулей. Поэтому в ней должны быть повторяющиеся символы, т. е.

$$G' = \left(\mathbf{1}_k \left| \begin{array}{ccccccc} 1 & \ldots & 1 & \ldots & 1 & \ldots & 1 \\ \ldots & \ldots & a & \ldots & a & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array} \right. \right), \quad a \neq 0.$$

Возьмём кодовое слово

$$\mathbf{x} = \text{строка } 1 - a^{-1}(\text{строка } 2);$$

его вес $w(\mathbf{x}) \leqslant 2 + (N-k-2) < N-k+1$, и $\mathcal{X}$ не может быть м. д. р.-кодом.

Привлекая двойственный код, получим, что не существует нетривиальных q-ичных м. д. р.-кодов с $k \geqslant q$. Следовательно, для нетривиального м. д. р.-кода должно быть выполнено одно из неравенств

$$N - q + 1 \leqslant k \quad \text{или} \quad k \leqslant q - 1.$$

Иными словами, не существует нетривиального двоичного м. д. р.-кода, но существует нетривиальный троичный $[3, 2, 2]$ м. д. р.-код. □

Замечание 2.4.19. Интересно по заданным k и q найти максимальное значение N, для которого существует q-ичный м. д. р. $[N, k]$-код. Мы показали, что N не превосходит $k+q-1$, но вычислительное доказательство показывает, что это значение равно $q+1$.

§ 2.5. Циклические коды и алгебра многочленов.

Введение в БЧХ-коды

Ring out the old, ring in the new,
Ring, happy bells, across the snow,
The year is going, let him go;
Ring out the false, ring in the true.

Альфред Теннисон (1809–1892),
английский поэт

Полезный класс линейных кодов состоит из так называемых циклических кодов (в частности, коды Хэмминга, Голея и Рида—Маллера относятся к циклическим). Циклические коды были предложены Юджином Пранджом в 1957 г., и сразу же стало понятно их значение, им посвящена многочисленная литература. Но более важно то, что идея циклических кодов вместе с некоторыми другими блестящими наблюдениями, сделанными в конце 1950-х гг., особенно создание БЧХ-кодов (Боуз—Чоудхури—Хоквингем, 1959 г.), открыла связь теории линейных кодов (которая была тогда в начальной стадии) с алгеброй, в частности с теорией конечных полей. Это привело к возникновению алгебраической теории кодирования, процветающей и в наши дни.

Мы начнём с двоичных циклических кодов. Процедуры кодирования и декодирования для двоичных циклических кодов длины N основаны на алгебре многочленов $\mathbb{F}_2[X]$ с двоичными коэффициентами:

$$a(X) = a_0 + a_1 X + \ldots + a_{N-1} X^{N-1}, \text{ где } a_k \in \mathbb{F}_2 \text{ для } k = 0, \ldots, N-1. \tag{2.5.1}$$

Эти многочлены можно складывать и перемножать по модулю полинома $1 + X^N$, при этом $X^k + X^k = 0$. Это определяет двоичную *алгебру многочленов* по модулю $1 + X^N$. Далее мы проверим, что это коммутативное кольцо, и используем обозначение $\mathbb{F}_2[X]/\langle 1 + X^N \rangle$; операции над двоичными многочленами, степень которых меньше N, относятся к этому кольцу. Степень $\deg a(X)$ многочлена $a(X)$ — это максимальный индекс его ненулевых коэффициентов. Степень нулевого многочлена равна 0.

Пример 2.5.1. Для двоичных многочленов выполнены соотношения

1) $(1 + X + X^3 + X^4)(X + X^2 + X^3) = X + X^7$,
2) $1 + X^N = (1 + X)(1 + X + \ldots + X^{N-1})$,
3) $(1 + X)^{2^l} = 1 + X^{2^l}$ (мечта первокурсника). □

Теорема 2.5.2 (алгоритм деления). *Пусть $f(X)$ и $h(X)$ — двоичные многочлены и $h(X) \not\equiv 0$. Тогда существуют такие единственные многочлены $g(X)$ и $r(X)$, что*

$$f(X) = g(X)h(X) + r(X), \quad \textit{где } \deg r(X) < \deg h(X). \tag{2.5.2}$$

Многочлен $g(X)$ называется отношением или частным, а $r(X)$ — остатком.

Доказательство. Если $\deg h(X) > \deg f(X)$, то просто положим

$$f(X) = 0 \cdot h(X) + f(X).$$

Если $\deg h(X) \leqslant \deg f(X)$, то можно осуществить процедуру «стандартного» деления в столбик с правилами сложения и умножения по модулю 2. □

Пример 2.5.3. Частное при делении $X + X^2 + X^6 + X^7 + X^8$ на $1 + X + X^2 + X^4$ равно $X^3 + X^4$, а остаток равен $X + X^2 + X^3$. □

Определение 2.5.4. Многочлены $f_1(X)$ и $f_2(X)$ называются эквивалентными (сравнимыми) по модулю $h(X)$, или $f_1(X) = f_2(X) \bmod (h(X))$, если их остатки от деления на $h(X)$ совпадают, т. е.

$$f_i(X) = g_i(X)h(X) + r(X), \quad i = 1, 2,$$

и $\deg r(X) < \deg h(X)$. □

Теорема 2.5.5. *Сложение и умножение многочленов сохраняет отношение эквивалентности, т. е. если*

$$f_1(X) = f_2(X) \bmod (h(X)) \quad и \quad p_1(X) = p_2(X) \bmod (h(X)), \tag{2.5.3}$$

то

$$\begin{cases} f_1(X) + p_1(X) = f_2(X) + p_2(X) \bmod (h(X)), \\ f_1(X)p_1(X) = f_2(X)p_2(X) \bmod (h(X)). \end{cases} \tag{2.5.4}$$

Доказательство. Для $i = 1, 2$ мы имеем

$$f_i(X) = g_i(X)h(X) + r(X), \quad p_i(X) = q_i(X)h(X) + s(X),$$

где

$$\deg r(X),\ \deg s(X) < \deg h(X).$$

Следовательно,

$$f_i(X) + p_i(X) = (g_i(X) + q_i(X))h(X) + (r(X) + s(X)),$$

причём

$$\deg(r(X) + s(X)) \leqslant \max[\deg r(X),\ \deg s(X)] < \deg h(X).$$

Отсюда

$$f_1(X) + p_1(X) = f_2(X) + p_2(X) \bmod (h(X)).$$

Более того, для $i = 1, 2$ произведение $f_i(X)p_i(X)$ представляется как

$$(g_i(X)q_i(X)h(X) + r(X)q_i(X) + s(X)g_i(X))h(X) + r(X)s(X).$$

Следовательно, остаток для обоих многочленов $f_1(X)p_1(X)$ и $f_2(X)p_2(X)$ может получиться только из $r(X)s(X)$, т. е. произведения имеют одинаковые остатки. □

Заметим, что каждый линейный двоичный код $\mathcal{X}_N$ соответствует множеству многочленов с коэффициентами 0 и 1 степени $N-1$, замкнутому относительно сложения по модулю 2:

$$\begin{aligned} a(X) &= a_0 + a_1X + \ldots + a_{N-1}X^{N-1} \leftrightarrow \mathbf{a}^{(N)} = a_0 \ldots a_{N-1}, \\ b(X) &= b_0 + b_1X + \ldots + b_{N-1}X^{N-1} \leftrightarrow \mathbf{b}^{(N)} = b_0 \ldots b_{N-1}, \\ a(X) &+ b(X) \leftrightarrow \mathbf{a}^{(N)} + \mathbf{b}^{(N)} = (a_0 + b_0) \ldots (a_{N-1} + b_{N-1}). \end{aligned} \tag{2.5.5}$$

(Нумерация знаков в слове, в которой используются номера $0, \ldots, N-1$ вместо $1, \ldots, N$, более удобна.)

Будем систематически писать $a(X) \in \mathcal{X}$, когда слово $\mathbf{a}^{(N)} = a_0 \ldots a_{N-1}$, представляющее многочлен $a(X)$, принадлежит коду $\mathcal{X}$.

Определение 2.5.6. Определим *циклический сдвиг* $\pi\mathbf{a}$ слова $\mathbf{a} = a_0a_1 \ldots a_{N-1}$ как слово $a_{N-1}a_0 \ldots a_{N-2}$. Линейный двоичный код называется *циклическим*, если циклический сдвиг каждого кодового слова тоже является кодовым словом. □

Простой способ построения циклического кода заключается в следующем. Возьмём слово $\mathbf{a}$ и все его последовательные циклические сдвиги $\pi\mathbf{a}$, $\pi^2\mathbf{a}$ и т. д. и добавим суммы всех получившихся векторов. Такая конструкция позволяет построить код из единственного слова, и в конечном счёте, все свойства этого кода можно будет интерпретировать через свойства самого слова. Заметим, что *каждый* циклический код можно получить таким образом. Соответствующее слово называется образующей циклического кода.

Лемма 2.5.7. *Двоичный линейный код $\mathcal{X}$ является циклическим тогда и только тогда, когда для любого вектора $\mathbf{u}$ из базиса кода $\mathcal{X}$ его циклический сдвиг $\pi\mathbf{u} \in \mathcal{X}$.*

Доказательство. Каждое кодовое слово из $\mathcal{X}$ является суммой векторов базиса, но $\pi(\mathbf{u}+\mathbf{v}) = \pi\mathbf{u} + \pi\mathbf{v}$, откуда следует требуемое утверждение. □

Сформулируем полезное свойство циклического сдвига.

Лемма 2.5.8. *Если слово $\mathbf{a}$ соответствует многочлену $a(X)$, то слово $\pi\mathbf{a}$ соответствует многочлену $Xa(X) \bmod (1+X^N)$.*

Доказательство. Соотношение

$$\begin{aligned} Xa(X) = a_0X + a_1X^2 + \ldots + a_{N-2}X^{N-1} + a_{N-1}X^N = \\ = a_{N-1} + a_0X + a_1X^2 + \ldots + a_{N-2}X^{N-1} \bmod (1+X^N) \end{aligned}$$

означает, что многочлен

$$a_{N-1} + a_0 X + \ldots + a_{N-2} X^{N-1},$$

соответствующий слову $\pi\mathbf{a}$, равен $Xa(X) \bmod (1 + X^N)$. □

Аналогично доказывается, что слово $\pi^2\mathbf{a}$ соответствует многочлену $X^2 a(X) \bmod (1 + X^N)$, и т. д. Справедливо и более общее утверждение.

Теорема 2.5.9. *Двоичный циклический код вместе с любой парой многочленов $a(X)$ и $b(X)$ содержит их сумму $a(X) + b(X)$ и все многочлены вида $v(X)a(X) \bmod (1 + X^N)$.*

Доказательство. Ввиду линейности сумма $a(X) + b(X) \in \mathcal{X}$. Если $v(X) = v_0 + v_1 X + \ldots + v_{N-1} X^{N-1}$, то каждый многочлен $X^k a(X) \bmod (1 + X^N)$ соответствует сдвигу $\pi^k\mathbf{a}$ и поэтому лежит в $\mathcal{X}$. Поэтому л. ч. следующего равенства также принадлежит коду:

$$v(X)a(X) \bmod (1 + X^N) = \sum_{i=0}^{N-1} v_i X^i a(X) \bmod (1 + X^N) \in \mathcal{X}. \qquad \square$$

Иначе говоря, двоичные многочлены с обычным сложением в $\mathbb{F}_2[X]$ и умножением $*$, определяемым как

$$a * b(X) = a(X)b(X) \bmod (1 + X^N), \tag{2.5.6}$$

образуют коммутативное *кольцо*, обозначаемое $\mathbb{F}_2[X]/\langle 1 + X^N \rangle$. Двоичные циклические коды — *идеал* этого кольца.

Пример 2.5.10. Обратный циклический сдвиг $\pi^{-1}\colon a_0 \ldots a_{N-2} a_{N-1} \in \in \{0, 1\}^N \mapsto a_1 a_2 \ldots a_{N-1} a_0$ действует на многочлен $a(X)$ степени не выше $N - 1$ по правилу

$$\pi^{-1} a(X) = \frac{1}{X}[a(X) + a_0] + a_0 X^{N-1}. \qquad \square$$

> Теоретик циклических кодов делает это, пока не зациклится.
>
> Теоретик циклических кодов делает это в кольце (желательно, полиномиальном и над конечным полем).
>
> (Из серии «Как они делают это».)

Теорема 2.5.11. *Пусть $g(X) = \sum\limits_{i=0}^{N-k} g_i X^i$ — ненулевой многочлен минимальной степени в двоичном циклическом коде $\mathcal{X}$. Тогда*

1) *$g(X)$ — единственный многочлен минимальной степени,*
2) *ранг кода $\mathcal{X}$ равен k,*

3) *кодовые слова, соответствующие многочленам* $g(X)$, $Xg(X)$, $\ldots$ $\ldots$, $X^{k-1}g(X)$, *составляют базис кода* $\mathcal{X}$; *они являются циклическими сдвигами слова* $\mathbf{g} = g_0 \ldots g_{N-k}0 \ldots 0$,

4) $a(X) \in \mathcal{X}$ *тогда и только тогда, когда* $a(X) = v(X)g(X)$ *для некоторого многочлена* $v(X)$ *степени меньше* k (*т. е.* $g(X)$ — *делитель любого многочлена из* $\mathcal{X}$).

Доказательство. 1) Предположим, что $c(X) = \sum\limits_{i=0}^{N-k} c_i X^i$ — другой многочлен минимальной степени $N-k$ из $\mathcal{X}$. Тогда $g_{N-k} = c_{N-k} = 1$ и, следовательно, $\deg(c(X) + g(X)) < N-k$. Но поскольку $N-k$ — минимальная степень, $c(X) + g(X)$ должен быть равен нулю. Такое бывает тогда и только тогда, когда $g(X) = c(X)$, т. е. $g(X)$ — единственный.

Утверждение 2) следует из п. 3).

3) Допустим, что имеет место свойство 4). Тогда каждый многочлен $a(X) \in \mathcal{X}$ имеет вид

$$g(X)v(X) = \sum_{i=0}^{r} v_i X^i g(X), \qquad r < k.$$

Значит, любой многочлен $a(X) \in \mathcal{X}$ является линейной комбинацией многочленов $g(X)$, $Xg(X)$, $\ldots X^{k-1}g(X)$ (все они лежат в $\mathcal{X}$). С другой стороны, многочлены $g(X)$, $Xg(X)$, $\ldots$, $X^{k-1}g(X)$ имеют разные степени и поэтому линейно независимы. Следовательно, слова $\mathbf{g}$, $\pi\mathbf{g}$, $\ldots$, $\pi^{k-1}\mathbf{g}$, соответствующие многочленам $g(X)$, $Xg(X)$, $\ldots$, $X^{k-1}g(X)$, образуют базис в $\mathcal{X}$.

4) Нам известно, что степень любого многочлена $a(X) \in \mathcal{X}$ строго больше $\deg g(X)$. Из алгоритма деления следует, что

$$a(X) = v(X)g(X) + r(X).$$

Здесь мы должны иметь

$$\deg v(X) < k \quad \text{и} \quad \deg r(X) < \deg g(X) = N - k.$$

Но тогда произведение $v(X)g(X)$ принадлежит $\mathcal{X}$ по теореме 2.5.9 (так как $\deg v(X)g(X) \leqslant N-1$, то это произведение совпадает с $v(X)g(X) \bmod (1 + X^N)$). Отсюда

$$r(X) = a(X) + v(X)g(X) \in \mathcal{X}$$

по линейности. Поскольку $g(X)$ — единственный многочлен минимальной степени из $\mathcal{X}$, получаем, что $r(X) = 0$. □

Следствие 2.5.12. *Любой двоичный циклический код получается из кодового слова, соответствующего многочлену минимальной степени, с помощью циклических сдвигов и линейных комбинаций.*

Определение 2.5.13. Многочлен $g(X)$ минимальной степени в $\mathcal{X}$ называется *образующей минимальной степени* двоичного (циклического) кода $\mathcal{X}$ (или просто образующей кода $\mathcal{X}$).

Замечание 2.5.14. Возможно есть и другие многочлены, порождающие $\mathcal{X}$ в смысле следствия 2.5.12. Но образующая минимальной степени определена однозначно.

Теорема 2.5.15. *Многочлен $g(X)$ степени не выше $N-1$ является образующей двоичного циклического кода длины N тогда и только тогда, когда $g(X)$ делит многочлен $1+X^N$, т. е.*

$$1+X^N = h(X)g(X) \tag{2.5.7}$$

для некоторого многочлена $h(X)$ (степени $N - \deg d(X)$).

Доказательство. (Часть «и только тогда».) По алгоритму деления

$$1+X^N = h(X)g(X) + r(X), \quad \deg r(X) < \deg g(X).$$

Иначе говоря,

$$r(X) = h(X)g(X) + 1 + X^N, \quad \text{т. е. } r(X) = h(X)g(X) \bmod (1+X^N).$$

По теореме 2.5.11 многочлен $r(X)$ принадлежит циклическому коду $\mathcal{X}$, порождённому многочленом $g(X)$. Но $g(X)$ должен быть единственным многочленом минимальной степени в $\mathcal{X}$. Значит, $r(X)=0$ и $1+X^N = h(X)g(X)$.

(Часть «тогда».) Пусть $1+X^N = h(X)g(X)$, $\deg h(X) = N - \deg g(X)$. Рассмотрим множество $\{a(X)\colon a(X) = u(X)g(X) \bmod (1+X^N)\}$, т. е. *главный идеал* кольца многочленов с умножением $*$, соответствующий $g(X)$. Это множество является линейным кодом, который содержит $g(X)$, $Xg(X)$, …, $X^{k-1}g(X)$, где $k = \deg h(X)$. Достаточно доказать, что $X^k g(X)$ также входит в это множество. Но $X^k g(X) = 1 + X^N + \sum\limits_{j=0}^{k-1} h_j X^j g(X)$, т. е. многочлен $X^k g(X)$ эквивалентен линейной комбинации многочленов $g(X)$, $Xg(X)$, …, $X^{k-1}g(X)$. □

Следствие 2.5.16. *Множество всех циклических кодов длины N взаимно однозначно соответствует множеству делителей многочлена $1+X^N$.*

Итак, циклические коды описываются через разложение на множители многочлена $1+X^N$. Более точно, нас интересует разложение многочлена $1+X^N$ на неприводимые множители; компоновка этих множителей в произведения даёт все возможные циклические коды длины N.

Определение 2.5.17. Многочлен $a(X) = a_0 + a_1 X + \ldots a_{N-1}X^{N-1}$ называется *неприводимым*, если $a(X)$ нельзя представить в виде произведе-

ния двух таких многочленов $b(X)$ и $b'(X)$, что $\min[\deg b(X), \deg b'(X)] \geqslant 1$. □

Важность (и удобство) неприводимых многочленов при описании циклических кодов очевидно: любой образующий многочлен циклического кода длины N является произведением неприводимых множителей многочлена $1 + X^N$.

Пример 2.5.18. 1. Многочлен $1 + X^N$ имеет два «стандартных» делителя:

$$1 + X^N = (1 + X)(1 + X + \ldots + X^{N-1}).$$

Первый множитель $1 + X$ порождает двоичный код с проверкой чётности $\mathcal{P}_N = \left\{\mathbf{x} = x_0 \ldots x_{N-1} \colon \sum\limits_i x_i = 0\right\}$, тогда как второй многочлен (возможно, приводимый) порождает код повторений $\mathcal{R}_N = \{0 \ldots 0,\, 1 \ldots 1\}$.

2. Выпишите порождающую и проверочную матрицы [7, 4]-кода Хэмминга в лексикографическом порядке. Если мы переставим цифры $x_4x_7x_5x_3x_2x_6x_1$ (что ведёт к эквивалентному коду), то строки образующей матрицы получаются из первой последовательными циклическими сдвигами:

$$G^{\mathrm{H}} = \begin{pmatrix} \underline{1\ 1\ 0\ 1}\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{pmatrix}.$$

Циклический сдвиг последней строки тоже принадлежит коду:

$$\pi(0001101) = (1000110) = (1101000) + (0110100) + (0011010).$$

По лемме 2.5.7 этот код является циклическим. По теореме 2.5.11, п. 3) образующий многочлен $g(X)$ соответствует подчёркнутой части матрицы $G^{\mathrm{H}}_{\mathrm{cycl}}$:

$$\underline{1101} \sim g(X) = 1 + X + X^3 = \text{образующая}.$$

Можно показать, что, выбрав другой порядок столбцов в проверочной матрице, мы получим код, эквивалентный исходному. Например, код с образующим многочленом $1 + X^2 + X^3$ тоже будет [7, 4]-кодом Хэмминга. Отметим, что [15, 11]-код Хэмминга получается из слова $11001 \sim 1 + X + X^4$, см. п. 3 примера 2.5.36.

В задаче 2.6.3 мы проверим, что [23, 12, 7]-код Голея порождается многочленом $g(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$. □

Пример 2.5.19. Используя разложение

$$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1) \tag{2.5.8}$$

в кольце $\mathbb{F}_2[X]$, найдите все двоичные циклические коды длины 7. Отождествите их с кодами Хэмминга или двойственными к ним.

Решение. См. таблицу, расположенную ниже.

код $\mathcal{X}$	образующая для $\mathcal{X}$	образующая для $\mathcal{X}^\perp$
$\{0,\,1\}^7$	1	$1+X^7$
проверка на чётность	$1+X$	$\sum\limits_{i=0}^{6} X^i$
Хэмминга	$1+X+X^3$	$1+X^2+X^3+X^4$
Хэмминга	$1+X^2+X^3$	$1+X+X^2+X^4$
двойственный к коду Хэмминга	$1+X^2+X^3+X^4$	$1+X+X^3$
двойственный к коду Хэмминга	$1+X+X^2+X^4$	$1+X^2+X^3$
повторений	$\sum\limits_{i=0}^{6} X^i$	$1+X$
нулевой	$1+X^7$	1

Легко проверить, что все множители в разложении (2.5.8) неприводимы. Каждый из них можно включать или не включать в разложение образующего многочлена. Таким образом, существует ровно 8 двоичных циклических кодов в $\mathcal{H}_{7,2}$, что отражено в таблице. □

Пример 2.5.20. 1. Многочлены первой степени $1+X$ и X неприводимы (но X не появляется в разложении многочлена $1+X^N$). Существует один неприводимый многочлен степени 2: $1+X+X^2$, два многочлена степени 3: $1+X+X^3$ и $1+X^2+X^3$ и три многочлена степени 4:

$$1+X+X^4, \quad 1+X^3+X^4 \quad \text{и} \quad 1+X+X^2+X^3+X^4, \tag{2.5.9}$$

каждый из которых появляется в разложении многочлена $1+X^N$ при различных значениях N (см. ниже). С другой стороны, многочлены

$$1+X^8, \quad 1+X^4+X^6+X^7+X^8 \quad \text{и} \quad 1+X^2+X^6+X^8 \tag{2.5.10}$$

приводимы. Многочлен $1+X^N$ всегда приводим:

$$1+X^N=(1+X)(1+X+\ldots+X^{N-1}).$$

2. В общем случае разложение многочлена $1+X^N$ на неприводимые множители представляет собой трудную задачу. Скажем, что разложение вида $(1+X)P_1(X)$, где $P_1(X)$ — неприводимый многочлен, тривиально. Для первых 13 нечетных значений N перечислим полиномы $1+X^N$, допускающие только тривиальное разложение на неприводимые факторы:

$$1+X, \quad 1+X^3, \quad 1+X^5, \quad 1+X^{11}, \quad 1+X^{13}.$$

Приведём разложение на неприводимые многочлены некоторых полиномов $1+X^N$ нечётных степеней (общий множитель $(1+X)$ опускается):

$$
\begin{aligned}
&1+X^7\colon (1+X+X^3)(1+X^2+X^3),\\
&1+X^9\colon (1+X+X^2)(1+X^3+X^6),\\
&1+X^{15}\colon (1+X+X^2)(1+X+X^4)(1+X^3+X^4)\times\\
&\qquad\times(1+X+X^2+X^3+X^4),\\
&1+X^{17}\colon (1+X^3+X^4+X^5+X^8)\times\\
&\qquad\times(1+X+X^2+X^4+X^6+X^7+X^8),\\
&1+X^{21}\colon (1+X+X^2)(1+X+X^3)(1+X^2+X^3)\times\\
&\qquad\times(1+X+X^2+X^4+X^6)(1+X^2+X^4+X^5+X^6),\\
&1+X^{23}\colon (1+X+X^5+X^6+X^7+X^9+X^{11})\times\\
&\qquad\times(1+X^2+X^4+X^5+X^6+X^{10}+X^{11}),\\
&1+X^{25}\colon (1+X+X^2+X^3+X^4)(1+X^5+X^{10}+X^{15}+X^{20}).
\end{aligned}
$$

При чётном N многочлен $1+X^N$ может иметь кратные корни (см. пример 2.5.1, п. 3). □

Пример 2.5.21. Перечислим неприводимые многочлены степеней 2 и 3 над полем $\mathbb{F}_3$, т. е. из кольца $\mathbb{F}_3[X]$. Существуют три неприводимых многочлена степени 2 над $\mathbb{F}_3$: X^2+1, X^2+X+2 и X^2+2X+2. Существуют 8 неприводимых многочленов степени 3 над $\mathbb{F}_3$: X^3+2X+2, X^3+X^2+2, X^3+X^2+X+2, X^3+2X^2+2X+2, X^3+2X+1, X^3+X^2+2X+1, X^3+2X^2+1 и X^3+2X^2+X+1. □

Циклические коды допускают процедуру кодирования и декодирования в терминах многочленов. Порождающую матрицу циклического кода удобно записывать в виде, похожем на G_{cycl} для $[7,4]$-кода Хэмминга (см. пример 2.5.18, п. 2). А именно, найдем базис в $\mathcal{X}$, который даёт следующую картинку для соответствующей порождающей матрицы:

$$
G_{\text{cycl}} = \begin{pmatrix}
\boxed{} & & & \\
& \boxed{} & & \mathbf{0} \\
& & \boxed{} & \\
& \mathbf{0} & \ddots & \\
& & & \boxed{}
\end{pmatrix}. \tag{2.5.11}
$$

Существование такого базиса следует из п. 3 теоремы 2.5.11. Действительно, возьмём образующий многочлен $g(X)$ и его кратности:

$$
g(X),\ \ Xg(X),\ \ \ldots,\ \ X^{k-1}g(X),\quad \deg g(X) = N-k.
$$

Символически

$$G_{\text{cycl}} = \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix}. \tag{2.5.12}$$

Ранг этого кода равен k. Код используется для кодирования слов длины k следующим образом. По данному слову $\mathbf{a} = a_0 \dots a_{k-1}$ создаётся многочлен $a(X) = \sum_{i=0}^{k-1} a_i X^i$ и вычисляется произведение $a(X)g(X) \bmod (1 + X^N)$. По теореме 2.5.9 это произведение принадлежит коду $\mathcal{X}$ и, следовательно, определяет кодовое слово. Поэтому достаточно хранить многочлен $g(X)$: кодирование будет соответствовать умножению многочленов. Если кодирование происходит через умножение, то декодирование должно быть связано с делением. Напомним, что при геометрическом декодировании мы декодируем полученное слово ближайшим кодовым словом в смысле расстояния Хэмминга. Такое слово связано с лидером соответствующего смежного класса. Мы видели, что смежные классы взаимно однозначно соответствуют синдромным словам вида $\mathbf{y}H^{\mathrm{T}}$. В случае циклических кодов синдромы вычисляются непосредственно. Напомним, что если $g(X)$ — образующий многочлен циклического кода $\mathcal{X}$ и $\deg g(X) = N - k$, то ранг кода $\mathcal{X}$ равен k и должно быть 2^{N-k} различных смежных класса (см. п. 5 примера 2.3.16).

Теорема 2.5.22. *Смежные классы* $\mathbf{y} + \mathcal{X}$ *взаимно однозначно соответствуют остаткам* $y(X) = u(X) \bmod (g(X))$. *Иначе говоря, слова* $\mathbf{y}$, $\mathbf{y}'$ *лежат в одном смежном классе тогда и только тогда, когда в алгоритме деления*

$$y(X) = a(X)g(X) + u(X), \qquad y'(X) = a'(X)g(X) + u'(X)$$

и $u(X) = u'(X)$.

Доказательство. Слова $\mathbf{y}, \mathbf{y}'$ лежат в одном смежном классе тогда и только тогда, когда $\mathbf{y} + \mathbf{y}' \in \mathcal{X}$ (см. п. 3 примера 2.3.16). Это эквивалентно тому, что $u(X) + u'(X) = 0$, т. е. $u(X) = u'(X)$. □

Значит, смежные классы нумеруются многочленами $u(X)$, степень которых меньше чем $\deg g(X) = N - k$: существует в точности 2^{N-k} таких многочленов. Для задания смежного класса $\mathbf{y} + \mathcal{X}$ достаточно вычислить остаток $u(X) = y(X) \bmod (g(X))$. К сожалению, всё ещё остаётся задача поиска лидера в каждом смежном классе: не существует простого алгоритма поиска лидеров в общем циклическом коде. Однако известны специальные классы циклических кодов, допускающих относительно простое декодиро-

вание: первый из них — класс так называемых БЧХ-кодов, был открыт в 1959 г. (см. 2.5.38).

Вообще говоря, циклический код может порождаться не только своим многочленом минимальной степени: для некоторых целей могут быть полезны другие образующие. Однако все они делят многочлен $1 + X^N$.

Теорема 2.5.23. *Пусть $\mathcal{X}$ — двоичный циклический код длины N. тогда любой многочлен $\tilde{g}(X)$, для которого $\mathcal{X}$ является главным идеалом, порождённым $\tilde{g}(X)$, делит многочлен $1 + X^N$.*

Доказательство — упражнение по алгебре. □

Мы видим, что циклические коды естественно нумеруются своими образующими многочленами.

Определение 2.5.24. Пусть $\mathcal{X}$ — циклический двоичный код длины N, порождённый многочленом $g(X)$. *Проверочным многочленом* $h(X)$ кода $\mathcal{X}$ называется отношение $(1 + X^N)/\langle g(X)\rangle$, т. е. единственный многочлен, для которого $h(X)g(X) = 1 + X^N$. □

Будем использовать стандартные обозначения НОД $(f(X), g(X))$ для наибольшего общего делителя многочленов $f(X)$ и $g(X)$ и НОК $(f(X), g(X))$ для их наименьшего общего кратного. Символом $\mathcal{X}_1 + \mathcal{X}_2$ обозначим прямую сумму кодов $\mathcal{X}_1$, $\mathcal{X}_2 \subset \mathcal{H}_{N,2}$, т. е. $\mathcal{X}_1 + \mathcal{X}_2$ состоит из линейных комбинаций $\alpha_1\mathbf{a}^{(1)} + \alpha_2\mathbf{a}^{(2)}$, где α_1, $\alpha_2 = 0$, 1 и $\mathbf{a}^{(i)} \in \mathcal{X}_i$, $i = 1, 2$ (см. п. 7 примера 2.1.8).

Пример 2.5.25. Пусть $\mathcal{X}_1$ и $\mathcal{X}_2$ — двоичные циклические коды длины N с образующими $g_1(X)$ и $g_2(X)$. Докажите, что 1) $\mathcal{X}_1 \subset \mathcal{X}_2$ тогда и только тогда, когда $g_2(X)$ делит $g_1(X)$, 2) пересечение $\mathcal{X}_1 \cap \mathcal{X}_2$ тоже циклический код, порождённый НОК $(g_1(X), g_2(X))$, 3) прямая сумма $\mathcal{X}_1 + \mathcal{X}_2$ — циклический код с образующей НОД $(g_1(X), g_2(X))$.

Решение. 1) Мы знаем, что $a(X) \in \mathcal{X}_i$ тогда и только тогда, когда в кольце $\mathbb{F}_2[X]/\langle 1 + X^N\rangle$ многочлен $a(X)$ представляется в виде $f_i * g_i(X)$, $i = 1, 2$. Предположим, что $g_2(X)$ делит $g_1(X)$, и запишем $g_1(X) = r(X)g_2(X)$. Тогда любой многочлен $a(X)$ вида $f_1 * g_1(X)$ представляется как $f_i * r * g_i(X)$. Иначе говоря, если $a(X) \in \mathcal{X}_1$, то $a(X) \in \mathcal{X}_2$, т. е. $\mathcal{X}_1 \subset \mathcal{X}_2$.

В обратную сторону, пусть $\mathcal{X}_1 \subset \mathcal{X}_2$. Положим $d_i = \deg g_i(X)$, $1 \leqslant d_i < N$, $i = 1, 2$, и запишем

$$g_1(X) = f(X)g_2(X) + r(X), \quad \deg r(X) < d_2.$$

Тогда каждый многочлен, $*$-делящийся на $g_1(X)$ в кольце $\mathbb{F}_2[X]/\langle 1 + X^N\rangle$ также $*$-делится и на $g_2(X)$. В частности, базисные многочлены $X^i g_1(X)$, $0 \leqslant i \leqslant N - d_1 - 1$, $*$-делятся на $g_2(X)$, т. е. имеют вид

$$X^i g_1(X) = h^{(i)}(X)g_2(X) + \alpha_i(1 + X^N), \qquad \text{где } \alpha_i = 0 \text{ или } 1.$$

Если для некоторого i коэффициент α_i равен 0, то мы сравним два тождества:

$$X^i g_1(X) = X^i f(X) g_2(X) + X^i r(X) \quad \text{и} \quad X^i g_1(X) = h^{(i)}(X) g_2(X)$$

и заключим, что $X^i r(X) = 0$. Отсюда следует, что $r(X) = 0$ и поэтому $g_2(X)$ делит $g_1(X)$.

Остался случай, когда все коэффициенты α_i тождественно равны 1. Тогда сравним

$$X g_1(X) = X h^{(0)}(X) g_2(X) + X + X^{N+1}$$

и

$$X g_1(X) = h^{(1)}(X) g_2(X) + 1 + X^N$$

и убедимся, что такая ситуация невозможна.

2. Эта часть получается просто: пересечение $\mathcal{X}_1 \cap \mathcal{X}_2$ является подкодом как в $\mathcal{X}_1$, так и в $\mathcal{X}_2$. Это, очевидно, циклический код, и по первой части его образующая $g(X)$ делится как на $g_1(X)$, так и на $g_2(X)$. Значит, она делится на НОК$(g_1(X), g_2(X))$. Нам нужно исключить случай, когда при таком делении возникает нетривиальное частное. Но НОК$(g_1(X), g_2(X))$ порождает циклический код (той же исходной длины), содержащийся как в $\mathcal{X}_1$, так и в $\mathcal{X}_2$, так что если образующая $g(X) \neq$ НОК$(g_1(X), g_2(X))$, то код, порождённый НОК$(g_1(X), g_2(X))$, должен быть строго больше пересечения $\mathcal{X}_1 \cap \mathcal{X}_2$, а это противоречит определению $\mathcal{X}_1 \cap \mathcal{X}_2$.

3. Аналогично $\mathcal{X}_1 + \mathcal{X}_2$ — минимальный линейный код, содержащий оба исходных: $\mathcal{X}_1$ и $\mathcal{X}_2$. Следовательно, его образующая делит как $g_1(X)$, так и $g_2(X)$, т. е. является их общем делителем. Если же он не равен НОД$(g_1(X), g_2(X))$, то получается противоречие со свойством минимальности. □

Пример 2.5.26. Пусть $\mathcal{X}$ — двоичный циклический код длины N с образующей $g(X)$ и проверочным многочленом $h(X)$. Докажите, что $a(X) \in \mathcal{X}$ тогда и только тогда, когда многочлен $1 + X^N$ делит произведение $a(X)h(X)$, т. е. $a * h(X) = 0$ в кольце $\mathbb{F}_2[X]/\langle 1 + X^N \rangle$.

Решение. Если $a(X) \in \mathcal{X}$, то $a(X) = f(X)g(X)$ для некоторого многочлена $f(X) \in \mathbb{F}_2[X]/\langle 1 + X^N \rangle$. Тогда

$$a(X)h(X) = f(X)g(X)h(X) = f(X)(1 + X^N),$$

что равно 0 в кольце $\mathbb{F}_2[X]/\langle 1 + X^N \rangle$. В обратную сторону, пусть $a(X) \in \mathbb{F}_2[X]/\langle 1 + X^N \rangle$, и предположим, что $a(X)h(X) = 0 \bmod (1 + X^N)$. Запишем $a(X) = f(X)g(X) + r(X)$, где $\deg r(X) < \deg g(X)$. Тогда

$$a(X)h(X) = f(X)(1 + X^N) + r(X)h(X) = r(X)h(X) \bmod (1 + X^N).$$

Следовательно, $r(X)h(X) = 0 \bmod (1 + X^N)$, что возможно только при $r(X) = 0$ (так как $\deg r(X)h(X) < N$). Итак, $a(X) = f(X)g(X)$ и $a(X) \in \mathcal{X}$.

Пример 2.5.27. Докажите, что двойственный к циклическому коду тоже циклический код, и найдите его образующий многочлен.

Решение. Если $\mathbf{y} \in \mathcal{X}^\perp$, двойственному коду, то скалярное произведение $\langle \pi\mathbf{x} \cdot \mathbf{y} \rangle = 0 \ \forall \mathbf{x} \in \mathcal{X}$. Но $\langle \pi\mathbf{x} \cdot \mathbf{y} \rangle = \langle \mathbf{x} \cdot \pi\mathbf{y} \rangle$, т. е. $\pi\mathbf{y} \in \mathcal{X}^\perp$, что означает цикличность двойственного кода.

Пусть $g(X) = g_0 + g_1 X + \ldots + g_{N-k}X^{N-k}$ — образующий многочлен кода $\mathcal{X}$, где $N - k = d$ — степень многочлена $g(X)$ и k совпадает с рангом кода $\mathcal{X}$. Мы знаем, что образующая матрица G кода $\mathcal{X}$ может быть записана в виде

$$G = \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix} \sim \begin{pmatrix} \boxed{} & & \\ & \boxed{} & \mathbf{0} \\ & & \boxed{} \\ & \mathbf{0} & \ddots \\ & & \boxed{} \end{pmatrix}. \tag{2.5.13}$$

Возьмём $h(X) = (1 + X^N)/g(X)$ и положим $\mathbf{h} = h_0 \ldots h_{N-1}$, если $h(X) = \sum\limits_{j=0}^{N-1} h_j X^j$. Тогда

$$\sum_{j=0}^{i} g_j h_{i-j} = \begin{cases} 1, & i = 0,\ N, \\ 0, & 1 \leqslant i < N. \end{cases}$$

Действительно, при $i = 0,\ N$ мы имеем $h_0 g_0 = 1$ и $h_k g_{N-k} = 1$. При $1 \leqslant i < N$ мы получим, что

$$\langle \pi^j \mathbf{g} \cdot \pi^{j'} \mathbf{h}^\perp \rangle = 0 \text{ для } j = 0,\ 1,\ \ldots,\ d-1,\ \ j' = 0,\ \ldots,\ k-1,$$

где $\mathbf{h}^\perp = h_k h_{k-1} \ldots h_0$. Легко видеть, что $\mathbf{h}^\perp$ является образующей кода $\mathcal{X}^\perp$.

Альтернативное решение основывается на примере 2.5.26. Мы знаем, что $a(X) \in \mathcal{X}$ тогда и только тогда, когда $a * h(X) = 0$. Пусть k — это степень образующей $g(X)$, тогда $\deg h(X) = N - k$. Полином $1 + X^N$ делит $a(X)h(X)$ степени $\deg(a(X)h(X)) < 2N - k$, поэтому коэффициенты при X^{N-k}, X^{N-k+1}, $\ldots$, X^{N-1} в произведении $a(X)h(X)$ равны нулю, т. е.

$$\begin{gathered} a_0 h_{N-k} + a_1 h_{N-k-1} + \ldots + a_{N-k} h_0 = 0, \\ a_1 h_{N-k} + a_2 h_{N-k-1} + \ldots + a_{N-k+1} h_0 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k-1} h_{N-k} + a_k h_{N-k-1} + \ldots + a_{N-1} h_0 = 0. \end{gathered}$$

Иначе говоря, $\mathbf{a}H^{\mathrm{T}} = 0$, где $\mathbf{a} = a_0 \dots a_{N-1}$ — слово двоичных коэффициентов многочлена $a(X)$, а $(N-k) \times N$-матрица H символически записывается в виде

$$H = \begin{pmatrix} h^{\perp}(X) \\ Xh^{\perp}(X) \\ \vdots \\ X^{N-k-1}h^{\perp}(X) \end{pmatrix} \sim \begin{pmatrix} \boxed{} & & & \\ & \boxed{} & & \mathbf{0} \\ & & \boxed{} & \\ & \mathbf{0} & & \ddots \\ & & & \boxed{} \end{pmatrix}, \tag{2.5.14}$$

где $h^{\perp}(X) = X^{N-k}h(X^{-1})$ со строкой коэффициентов $\mathbf{h}^{\perp} = h_k h_{k-1} \dots h_0$.

Уже можно сделать вывод о том, что матрица H порождает код $\mathcal{X}' \subseteq \mathcal{X}^{\perp}$. Но, поскольку $h_{N-k} = 1$, ранг кода $\mathcal{X}'$ равен d, откуда $\mathcal{X}' = \mathcal{X}^{\perp}$.

Осталось проверить, что многочлен $h^{\perp}(X)$ делит $1 + X^N$. Для этого мы выведем из равенства $g(X)h(X) = 1 + X^N$, что $h(X^{-1})g(X^{-1}) = X^{-N} + 1$. Умножая на X^N, получим $h^{\perp}(X)X^k g(X^{-1}) = 1 + X^N$ и, поскольку $X^k g(X^{-1}) = g_k + g_{k-1}X + \dots + g_0 X^k$, $h^{\perp}(X)$ — делитель $1 + X^N$. □

Пример 2.5.28. Пусть $\mathcal{X}$ — двоичный циклический код длины N с образующей $g(X)$.

1. Покажите, что множество кодовых слов $\mathbf{a} \in \mathcal{X}$ чётного веса тоже образует циклический код и найдите его образующую.

2. Покажите, что $\mathcal{X}$ содержит кодовое слово нечётного веса тогда и только тогда, когда $g(1) \neq 0$, или, что эквивалентно, слово $\mathbf{1} \in \mathcal{X}$.

Решение. 1. Если код $\mathcal{X}$ чётный (т. е. содержит лишь слова чётного веса), то для любого многочлена $a(X) \in \mathcal{X}$ выполнено равенство $a(1) = \sum_{i=0}^{N-1} a_i = 0$. Следовательно, $1 + X$ — делитель многочлена $a(X)$. Значит, образующая $g(X)$ тоже делится на $1 + X$. Обратное тоже верно. Если многочлен $g(X)$ делится на $1 + X$, или, что эквивалентно, $g(1) = 0$, то любое кодовое слово $\mathbf{a} \in \mathcal{X}$ будет иметь чётный вес.

Теперь предположим, что в коде $\mathcal{X}$ есть слово нечётного веса, т. е. $g(1) = 1$, и $1 + X$ не делит $g(X)$. Символом $\mathcal{X}^{\mathrm{ev}}$ обозначим подкод в $\mathcal{X}$, состоящий из всех чётных кодовых слов. Циклический сдвиг не меняет веса, поэтому $\mathcal{X}^{\mathrm{ev}}$ — циклический код. Здесь все соответствующие многочлены $a(X)$ делятся на $1 + X$. Поэтому и образующая $g^{\mathrm{ev}}(X)$ кода $\mathcal{X}^{\mathrm{ev}}$ делится на него. Из примера 2.5.18 п. 1 мы получаем соотношение $g^{\mathrm{ev}}(X) = g(X)(1 + X)$.

2. Осталось показать, что $g(1) = 1$ тогда и только тогда, когда $\mathbf{1} \in \mathcal{X}$. Поскольку многочлен $1 + \dots + X^{N-1}$ дополняет $1 + X$ в разложении $1 + X^N = (1 + X)(1 + \dots + X^{N-1})$, из предположения, что $g(1) = 1$, т. е. что $g(X)$ не содержит множителя $1 + X$, следует, что $g(X)$ должен быть дели-

телем многочлена $1 + \ldots + X^{N-1}$. Отсюда вытекает, что $\mathbf{1} \in \mathcal{X}$. Обратное утверждение проверяется аналогично. □

Пример 2.5.29. Пусть $\mathcal{X}$ — двоичный циклический код длины N с образующей $g(X)$ и проверочным многочленом $h(X)$.

1. Докажите, что код $\mathcal{X}$ ортогонален себе тогда и только тогда, когда $h^{\perp}(X)$ делит $g(X)$, и самодвойствен тогда и только тогда, когда $h^{\perp}(X) = g(X)$. где $h^{\perp}(X) = h_k + h_{k-1}X + \ldots + h_0X^{k-1}$ и $h(X) = h_0 + \ldots + h_{k-1}X^{k-1} + h_kX^k$ — проверяющий многочлен со свойством $g(X)h(X) = 1 + X^N$.

2. Пусть r — делитель числа N: $r \,|\, N$. Двоичный код $\mathcal{X}$ называется r-вырожденным, если каждое кодовое слово $\mathbf{a} \in \mathcal{X}$ является сцеплением $\mathbf{c} \ldots \mathbf{c}$, где $\mathbf{c}$ — строка длины r. Докажите, что код $\mathcal{X}$ является r-вырожденным, тогда и только тогда, когда $h(X)$ делит $1 + X^r$.

Решение. 1. Ортогональность себе означает, что $\mathcal{X} \subseteq \mathcal{X}^{\perp}$, т. е. $\langle \mathbf{a} \cdot \mathbf{b} \rangle = 0 \ \forall \mathbf{a}, \mathbf{b} \in \mathcal{X}$. Из примера 2.5.27 мы знаем, что $h^{\perp}(X)$ порождает код $\mathcal{X}^{\perp}$. Следовательно, благодаря примеру 2.5.25 можно заключить, что $\mathcal{X} \subseteq \mathcal{X}^{\perp}$ тогда и только тогда, когда $h^{\perp}(X)$ делит $g(X)$.

Самодвойственность означает, что $\mathcal{X} = \mathcal{X}^{\perp}$, т. е. $h^{\perp}(X) = g(X)$.

2. При $N = rs$ имеем разложение

$$1 + X^N = (1 + X^r)(1 + X^r + \ldots + X^{r(s-1)}).$$

Предположим теперь, что циклический код $\mathcal{X}$ длины N с образующей $g(X)$ является r-вырожденным. Тогда слово $\mathbf{g}$ имеет вид $1\tilde{\mathbf{c}}1\tilde{\mathbf{c}} \ldots 1\tilde{\mathbf{c}}$ для некоторой строки $\tilde{\mathbf{c}}$ длины $r - 1$ (где $\mathbf{c} = 1\tilde{\mathbf{c}}$). Пусть $\tilde{c}(X)$ — многочлен, соответствующий строке $\tilde{\mathbf{c}}$ (степени не выше $r - 2$). Тогда $g(X)$ записывается как

$$1 + X\tilde{c}(X) + X^r + X^{r+1}\tilde{c}(X) + \ldots + X^{r(s-1)} + X^{r(s-1)+1}\tilde{c}(X) = \\ = (1 + X^r + \ldots + X^{r(s-1)})(1 + X\tilde{c}(X)).$$

Для проверочного многочлена $h(X)$ мы получаем

$$h(X) = (1 + X^N)/(1 + X^r + \ldots + X^{r(s-1)})(1 + X\tilde{c}(X)) = (1 + X^r)/(1 + X\tilde{c}(X)).$$

Значит, $h(X)$ — делитель многочлена $1 + X^r$.

В обратную сторону, пусть $h(X) \,|\, (1 + X^r)$, причём $h(X)g(X) = 1 + X^r$, где $g(X) = \sum\limits_{j=0}^{r-1} c_jX^j$ и $c_0 = 1$. Возьмём $\mathbf{c} = c_0 \ldots c_{r-1}$. Повторяя предыдущие рассуждения в обратном порядке, мы заключаем, что слово $\mathbf{g}$ — это сцепление $\mathbf{c} \ldots \mathbf{c}$. Тогда циклический сдвиг $\pi\mathbf{g}$ — это сцепление $\mathbf{c}^{(1)} \ldots \mathbf{c}^{(1)}$, где $\mathbf{c}^{(1)} = c_{r-1}c_0 \ldots c_{r-2}$ (т. е. циклическому сдвигу $\pi\mathbf{c}$ строки $\mathbf{c}$ в $\{0, 1\}^r$). Аналогичное свойство выполнено для последовательных сдвигов $\pi^2\mathbf{g}$, ...

Следовательно, базисные векторы в $\mathcal{X}$ являются r-вырожденными, а значит, r-вырожден и весь код $\mathcal{X}$. □

В «стандартной» арифметике (вещественный или комплексный) многочлен $p(X)$ данной степени d удобно отождествлять с его корнями (или нулями) $\alpha_1, \ldots, \alpha_d$ (комплексными в общем случае), имея в виду разложение на мономы

$$p(X) = \prod_{i=1}^{d} (X - \alpha_i). \tag{2.5.15}$$

В двоичной арифметике над полем $\mathbb{F}_{2^s}$ (и, более общим образом, в q-ичной арифметике) корни многочлена остаются очень полезным понятием и помогают построить порождающий многочлен $g(X) = \sum_{i=0}^{d} g_i X^i$ двоичного циклического кода с важными наперёд заданными свойствами. Несколько забегая вперед, предположим, что корни $\alpha_1, \ldots, \alpha_d$ корректно определены и представление (2.5.15) имеет непротиворечивый смысл (который уточняется в теории конечных полей). Даже не зная формальной теории, можно сделать несколько полезных наблюдений.

Первое наблюдение состоит в том, что α_i являются корнями из единицы N-й степени, так как они должны быть среди нулей многочлена $1 + X^N$. Следовательно, их можно перемножать и обращать, т. е. они образуют абелеву мультипликативную группу порядка N, возможно циклическую. Во-вторых, если α — нуль многочлена $g(X)$ в двоичной арифметике, то таковым будет и α^2, так как $g(X)^2 = g(X^2)$. Далее, α^4 тоже нуль, как и α^8, и т. д. Мы делаем вывод, что последовательность $\alpha, \alpha^2, \ldots$ начинает цикл: $\alpha^{2^d} = \alpha$ (или $\alpha^{2^d - 1} = 1$), где d — степень многочлена $g(X)$. Иначе говоря, все корни N-й степени из единицы разбиваются на непересекающиеся классы вида $C = \{\alpha, \alpha^2, \ldots, \alpha^{2^c - 1}\}$ размера c, где $c = c(C)$ — натуральное число ($2^c - 1$ делит N). Обозначение $C(\alpha)$, где $c = c(\alpha)$, поучительно. Члены одного класса называются *сопряжёнными* друг другу. Если мы ищем порождающий многочлен $g(X)$ с корнем α, то все сопряжённые корни из единицы $\alpha' \in C(\alpha)$ будут среди корней многочлена $g(X)$.

Таким образом, для построения образующей $g(X)$ мы должны собрать все корни из классов C и использовать их в построении. Вместе с каждым выбранным корнем из единицы в построении участвуют все члены его класса. Затем, поскольку любой многочлен $a(X)$ из циклического кода, порождённого $g(X)$, является кратным $g(X)$ (см. п. 4 теоремы 2.5.11), корни $g(X)$ будут среди корней многочлена $a(X)$. И наоборот, если $a(X)$ имеет все корни α_i многочлена $g(X)$ среди своих корней, то $a(X)$ принадлежит коду. Мы видим, что циклические коды удобно описываются в терминах корней из единицы.

Deep N th Roots of Our Unity[8]

(Из серии «Фильмы, которые не вышли на большой экран».)

Пример 2.5.30 ([7,4]-код Хэмминга). Напомним, что проверочная матрица H для двоичного [7, 4]-кода Хэмминга $\mathcal{X}^{\mathrm{H}}$ имеет размер 3×7; её столбцы — это ненулевые двоичные слова длины 3: различные порядки этих столбцов отвечают эквивалентным кодам. Как мы увидим, последовательность ненулевых двоичных слов любой данной длины $2^l - 1$, записанных в некотором особом порядке (или порядках), можно интерпретировать как последовательность степеней единственного элемента ω: ω^0, ω, ω^2, …, ω^{2^l-2}. Правило умножения, порождающее эти степени, специфично (это умножение многочленов по модулю специального неприводимого многочлена степени l).

Чтобы подчеркнуть этот факт, мы используем в этом параграфе обозначение $*$ для этого правила умножения, записывая ω^{*i} вместо ω^i. Во всяком случае, для $l = 3$, один подходящий порядок ненулевых 3-слов (из двух возможных) имеет следующий вид:

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \sim (\omega^{*0}\omega\omega^{*2}\omega^{*3}\omega^{*4}\omega^{*5}\omega^{*6}).$$

При такой интерпретации равенство $\mathbf{a}H^{\mathrm{T}} = 0$, устанавливающее принадлежность слова $\mathbf{a} = a_0 \dots a_6$ (или многочлена $a(X) = \sum_{i=0}^{6} a_i X^i$) коду $\mathcal{X}^{\mathrm{H}}$, можно переписать в виде

$$\sum_{i=0}^{6} a_i \omega^{*i} = 0, \quad \text{или} \quad a(*\omega) = 0.$$

Другими словами, $a(X) \in \mathcal{X}^{\mathrm{H}}$ тогда и только тогда, когда ω — корень $a(X)$ при умножении $*$ (которое в этом случае означает умножение двоичных многочленов степени не выше 2 по модулю $1 + X + X^3$).

Иными словами, [7, 4]-код Хэмминга эквивалентен циклическому коду с образующей $g(X)$, обращающейся в нуль в точке ω; в этом случае образующая имеет вид $g(X) = 1 + X + X^3$ и $g(*\omega) = \omega^{*0} + \omega + \omega^{*3} = 0$. Альтернативный порядок строк матрицы H^{T} возникает, если в качестве порождающего выбирается многочлен $1 + X^2 + X^3$.

Мы видим, что [7, 4]-код Хэмминга определяется единственным корнем ω при условии, что используются подходящие правила оперирования с его степенями. Поэтому можно назвать ω *определяющим корнем* (*или*

[8] Ср. с названием фильма «Deep Throat» (1972 г.).

нулём) для этого кода. Более того, ω является «примитивным» элементом (см. § 3.1–3.3).

Пример 2.5.31. Код $\mathcal{X}$ называется *обратимым*, если из условия $\mathbf{a} = a_0 a_1 \dots a_{N-1} \in \mathcal{X}$ следует, что $\mathbf{a}^{\leftarrow} = a_{N-1} \dots a_1 a_0 \in \mathcal{X}$. Докажите, что циклический код с образующей $g(X)$ обратим тогда и только тогда, когда из равенства $g(\alpha) = 0$ следует, что $g(\alpha^{-1}) = 0$.

Решение. Если $g(X) = \sum\limits_{i=0}^{d} g_i X^i$ — образующий многочлен степени $d < N$ с коэффициентами $g_0 = g_d = 1$, то обращённый многочлен равен $g^{\mathrm{rev}}(X) = X^{N-1} g(X^{-1})$, поэтому если циклический код $\mathcal{X}$ обратим и α — корень многочлена $g(X)$, то α будет также корнем $g^{\mathrm{rev}}(X)$, а это возможно, только если $g(\alpha^{-1}) = 0$.

Теперь рассмотрим полином $g(X)$, обладающий таким свойством: из равенства $g(\alpha) = 0$ следует равенство $g(\alpha^{-1}) = 0$. Тогда этим свойством будет обладать любой многочлен $a(X)$ степени меньше N: $a^{\mathrm{rev}}(X) = X^{N-1} a(X^{-1})$. Если $a(X) \in \mathcal{X}$, то $a(\alpha) = a(\alpha^{-1}) = 0$ для любого корня α образующей $g(X)$. Тогда $a^{\mathrm{rev}}(\alpha) = a^{\mathrm{rev}}(\alpha^{-1}) = 0$ для любого корня α образующей $g(X)$. Поэтому многочлен $a^{\mathrm{rev}}(X)$ кратен $g(X)$ и $a^{\mathrm{rev}}(X) \in \mathcal{X}$. □

Корни многочленов изучаются в теории конечных полей, или теории Галуа (мы уже знакомы с полиномиальными полями). В оставшейся части этого параграфа даётся краткое введение в некоторые аспекты теории Галуа, что позволит лучше понять некоторые примеры кодов, приведённых в дальнейшем. В гл. 3 мы погрузимся глубже в теорию Галуа, с тем чтобы получить достаточно знаний для знакомства с более сложными конструкциями кодов.

Замечание 2.5.32. *Поле* — это коммутативное кольцо, в котором каждый ненулевой элемент обратим. Иными словами, кольцо является полем, если оно образует группу по умножению. На самом деле группа по умножению ненулевых элементов поля $\mathbb{F}_q$ циклическая. □

Теорема 2.5.33. *Пусть $g(X) \in \mathbb{F}_2[X]$ — неприводимый двоичный многочлен степени d. Тогда умножение по* $\mathrm{mod}(g(X))$ *наделяет множество двоичных многочленов степени не выше $d-1$ (т. е. пространство $\mathbb{F}_2^{\times d}$) структурой поля с 2^d элементами. Верно и обратное: если умножение по* $\mathrm{mod}(g(X))$ *приводит к полю, то многочлен $g(X)$ неприводим.*

Доказательство. Нужно проверить единственное нетривиальное свойство: обратимость каждого ненулевого элемента. Возьмём ненулевой многочлен $f(X)$, $\deg f < d$, и рассмотрим многочлены вида $f(X)h(X)$, где $h(X)$ пробегает всё множество многочленов степени не выше $d-1$. Эти

многочлены должны быть различны по $\mathrm{mod}(g(X))$. Действительно, если

$$f(X)h_1(X) = f(X)h_2(X) \bmod g(X),$$

то для некоторого многочлена $v(X)$ степени не выше $d-2$ выполнено равенство:

$$f(X)(h_1(X) - h_2(X)) = v(X)g(X). \tag{2.5.16}$$

Многочлен $g(X)$ неприводим, поэтому либо $g(X)\,|\,f(X)$, либо $g(X)\,|\,(h_1(X) - h_2(X))$, что возможно лишь тогда, когда $h_1(X) = h_2(X)$ и $v(X) = 0$. Поскольку поле конечно, для одного и только одного многочлена $h(X)$ имеем равенство $f(X)h(X) = 1 \bmod (g(X))$; этот многочлен $h(X)$ представляет обратный для $f(X)$ относительно умножения по $\mathrm{mod}(g(X))$. Обозначим его через $h(X) = f(X)^{*-1}$.

С другой стороны, если многочлен $g(X)$ приводим, то $g(X) = b(X)b'(X)$, где степень многочленов $b(X)$ и $b'(X)$ больше нуля и меньше d, т. е. $b(X)b'(X) = 0 \bmod (g(X))$. Если умножение по $\mathrm{mod}(g(X))$ приводит к полю, то как $b(X)$, так и $b'(X)$ должны иметь обратный элемент $b(X)^{*-1}$ и $b'(X)^{*-1}$. Но тогда

$$b(X)^{*-1} * b(X) * b'(X) = b'(X) = 0.$$

Равенство $b(X) = 0$ доказывается аналогично. □

Поле, полученное описанной выше процедурой, называется *полиномиальным* полем и обозначается $\mathbb{F}_2[X]/\langle g(X)\rangle$. Оно состоит из 2^d элементов, где $d = \deg g(X)$ (представляемых многочленами степени меньше d). Будем называть $g(X)$ *основным многочленом* поля и умножение в этом полиномиальном поле обозначать символом $*$. Нулевой и единичный многочлены обозначаем через $\mathbf{0}$ и $\mathbf{1}$ соответственно. Они, очевидно, будут нулём и единицей полиномиального поля. Следующая теорема играет в этой теории ключевую роль.

Теорема 2.5.34. 1. *Мультипликативная группа ненулевых элементов полиномиального поля $\mathbb{F}_2[X]/\langle g(X)\rangle$ изоморфна циклической группе $\mathbb{Z}_{2^d-1}$ порядка $2^d - 1$.*

2. *Полиномиальные поля, полученные при помощи разных неприводимых многочленов степени d, изоморфны.*

Доказательство. Сейчас мы докажем только первое утверждение, второе будет доказано в §3.1. Возьмём произвольный элемент из поля $a(X) \in \mathbb{F}_2[X]/\langle g(X)\rangle$ и заметим, что $a^{*i}(X) = \underbrace{a * \ldots * a(X)}_{i \text{ раз}}$ (умножение в поле) принимает не более $2^d - 1$ значений (число элементов поля минус один, поскольку $\mathbf{0}$ исключён). Поэтому найдётся такое натуральное число r, для которого $a^{*r}(X) = \mathbf{1}$; наименьшее значение r навязывается *порядком* элемента $a(X)$.

Выберем многочлен $a(X) \in \mathbb{F}_2[X]/\langle g(X)\rangle$ с наибольшим порядком r. Тогда мы утверждаем, что порядок любого другого элемента $b(X)$ делит r. Действительно, пусть s — порядок многочлена $b(X)$. Возьмём простой делитель p числа s и запишем

$$s = p^{c'} l' \quad \text{и} \quad r = p^c l$$

с целыми числами c', $c \geqslant 0$ и l, $l' \geqslant 1$, где l и l' не делятся на p. Мы хотим показать, что $c \geqslant c'$. Действительно, элемент $a^{*p^c}(X)$ имеет порядок l, $b^{*l'}(X)$ имеет порядок $p^{c'}$ и произведение $a^{*p^c} * b^{*l'}(X)$ имеет порядок $lp^{(c')}$. Следовательно, $c' \leqslant c$ или r не максимальный порядок. Это верно для любого простого делителя p, поэтому s делит r.

Итак, если r — максимальный порядок, то любой элемент поля обладает свойством $b^{*r}(X) = \mathbf{1}$. Опираясь на принцип Дирихле, мы заключаем, что $r = 2^d - 1$ — число ненулевых элементов поля. Следовательно, если многочлен $a(X)$ имеет максимальный порядок, то его степени $\mathbf{1}$, $a(X)$, …, $a^{*(2^d-1)}(X)$ исчерпывают все элементы мультипликативной группы поля. □

В свете теоремы 2.5.34 можно использовать обозначение $\mathbb{F}_{2^d}$ для любого полиномиального поля $\mathbb{F}_2[X]/\langle g(X)\rangle$, где $g(X)$ — неприводимый двоичный многочлен степени d. Далее мультипликативную группу ненулевых элементов поля $\mathbb{F}_{2^d}$ обозначаем через $\mathbb{F}^*_{2^d}$, она циклическая ($\simeq \mathbb{Z}_{2^d-1}$ согласно теореме 2.5.34). Любая образующая группы $\mathbb{F}^*_{2^d}$ ($*$-степени которой исчерпывают $\mathbb{F}^*_{2^d}$) называется *примитивным элементом* поля $\mathbb{F}_{2^d}$.

Dial p For Primitives[9]

(Из серии «Фильмы, которые не вышли на большой экран».)

Пример 2.5.35. Мы видели, что важно иметь полный список неприводимых многочленов данной степени. Существует шесть двоичных неприводимых многочленов степени 5:

$$\begin{gathered} 1 + X^2 + X^5, \quad 1 + X^3 + X^5, \quad 1 + X + X^2 + X^3 + X^5, \\ 1 + X + X^2 + X^4 + X^5, \quad 1 + X + X^3 + X^4 + X^5, \\ 1 + X^2 + X^3 + X^4 + X^5 \end{gathered} \tag{2.5.17}$$

[9] Ср. с названием фильма А. Хичкока «Dial M For Murder» (1954 г.).

и девять степени 6:

$$\begin{gathered} 1+X+X^6,\quad 1+X+X^3+X^4+X^6,\quad 1+X^5+X^6,\\ 1+X+X^2+X^5+X^6,\quad 1+X^2+X^3+X^5+X^6,\\ 1+X+X^4+X^5+X^6,\\ 1+X+X^2+X^4+X^6,\quad 1+X^2+X^4+X^5+X^6,\\ 1+X^3+X^6. \end{gathered} \tag{2.5.18}$$

Далее их число быстро растёт: 18 степени 7, 30 степени 8 и т. д. Однако существуют и доступны в интернете большие таблицы неприводимых многочленов над различными конечными полями. □

Пример 2.5.36. 1. Поле $\mathbb{F}_2[X]/(1+X+X^2)$ имеет 4 элемента: $\mathbf{0}$, $\mathbf{1}$, X, $1+X$ с таблицей умножения

$$\begin{gathered} X*X=1+X,\ \text{так как } X^2=1+X \bmod (1+X+X^2),\\ X*(1+X)=X+X*X=\mathbf{1},\\ (1+X)*(1+X)=1+X+X+X*X=1+1+X=X. \end{gathered}$$

Так как $X^{*3}=(1+X)*X=\mathbf{1}$, мультипликативная группа поля изоморфна $\mathbb{Z}_3$. Альтернативное обозначение этого поля — это $\mathbb{F}_4$.

2. Каждое из полей $\mathbb{F}_2[X]/\langle 1+X+X^3\rangle$ и $\mathbb{F}_2[X]/\langle 1+X^2+X^3\rangle$ состоит из восьми элементов, представляющихся всеми многочленами степени не выше 2. Каждый такой многочлен $a_0+a_1X+a_2X^2$ отождествляется со строкой своих коэффициентов $a_0a_1a_2$ (двоичным словом). Таблицы поля можно найти, глядя на последовательные степени X^{*i}:

	$1+X+X^3$			$1+X^2+X^3$	
X^{*i}	многочлен	слово	X^{*i}	многочлен	слово
–	$\mathbf{0}$	000	–	$\mathbf{0}$	000
X^{*0}	$\mathbf{1}$	100	X^{*0}	$\mathbf{1}$	100
X	X	010	X	X	010
X^{*2}	X^2	001	X^{*2}	X^2	001
X^{*3}	$1+X$	110	X^{*3}	$1+X^2$	101
X^{*4}	$X+X^2$	011	X^{*4}	$1+X+X^2$	111
X^{*5}	$1+X+X^2$	111	X^{*5}	$1+X$	110
X^{*6}	$1+X^2$	101	X^{*6}	$X+X^2$	011

В обоих случаях мультипликативная группа ненулевых элементов изоморфна $\mathbb{Z}_7$. Эти поля, очевидно, изоморфны, поскольку разделяют общий формализм умножения в циклической группе. Общее обозначение для этих полей — $\mathbb{F}_8$. Заметим, что таблицы степеней X^{*i} совпадают при $0\leqslant i<3$; на самом деле это общий факт, который будет обсуждаться в § 3.1–3.3.

Более того, элемент $X = X^{*1} \in \mathbb{F}_2[X]/\langle 1 + X + X^3\rangle$ можно интерпретировать как корень основного многочлена $1 + X + X^3$, а элемент $X = X^{*1} \in \mathbb{F}_2/\langle 1 + X^2 + X^3\rangle$, как корень многочлена $1 + X^2 + X^3$, так как эти многочлены будут иметь нули в своих соответствующих полях. Оставшиеся два корня — это X^{*2} и X^{*4} (тоже вычисленные в соответствующих полях).

Применим этот пример к [7, 4]-коду Хэмминга (см. пример 2.5.30): поле $\mathbb{F}_2[X]/\langle 1 + X + X^3\rangle$ приводит к корню образующей $1 + X + X^3$, а $\mathbb{F}_2[X]/\langle 1 + X^2 + X^3\rangle$ — к корню образующей $1 + X^2 + X^3$, т. е. [7, 4]-код Хэмминга эквивалентен циклическому коду длины 7 с определяющим корнем $\omega = X$ в одном из двух изоморфных полей $\mathbb{F}_2[X]/\langle 1 + X + X^3\rangle$ или $\mathbb{F}_2[X]/\langle 1 + X^2 + X^3\rangle$. С некоторой неоднозначностью (которая будет устранена в § 3.1) можно сказать, что этот код определяется своим корнем ω, т. е. примитивным элементом поля $\mathbb{F}_8$.

3. Поле $\mathbb{F}_2[X]/\langle 1 + X + X^4\rangle$ состоит из 16 элементов. Таблица поля имеет следующий вид;

степень X^{*i}	многочлен	слово
–	**0**	0000
X^{*0}	**1**	1000
X	X	0100
X^{*2}	X^2	0010
X^{*3}	X^3	0001
X^{*4}	$1 + X$	1100
X^{*5}	$X + X^2$	0110
X^{*6}	$X^2 + X^3$	0011
X^{*7}	$1 + X + X^3$	1101
X^{*8}	$1 + X^2$	1010
X^{*9}	$X + X^3$	0101
X^{*10}	$1 + X + X^2$	1110
X^{*11}	$X + X^2 + X^3$	0111
X^{*12}	$1 + X + X^2 + X^3$	1111
X^{*13}	$1 + X^2 + X^3$	1011
X^{*14}	$1 + X^3$	1001

Следовательно, мультипликативная группа — это $\mathbb{Z}_{15}$. Элемент $X \in \mathbb{F}_2[X]/\langle 1 + X + X^4\rangle$ даёт корень многочлена $1 + X + X^4$; остальные корни — X^{*2}, X^{*4} и X^{*8}.

Этот пример можно использовать для отождествления [15, 11]-кода Хэмминга (с точностью до эквивалентности) с циклическим кодом, порождённым многочленом $g(X) = 1 + X + X^4$. Теперь мы можем сказать, что [15, 11]-код Хэмминга (по модулю эквивалентности) — это циклический код длины 15 с определяющим корнем $\omega (= X)$ в поле $\mathbb{F}_2[X]/\langle 1 + X + X^4\rangle$.

Поскольку X — образующая мультипликативной группы поля, мы вновь можем утверждать, что определяющий корень ω — примитивный элемент поля $\mathbb{F}_{16}$. □

В общем случае возьмём поле $\mathbb{F}_2[X]/\langle g(X)\rangle$, где $g(X) = \sum\limits_{i=0}^{d} g_i X^i$ — неприводимый двоичный многочлен степени d. Тогда элементы X, X^{*2}, X^{*4}, …, X^{*2^d-1} будут удовлетворять уравнению

$$\sum_{i=0}^{d} g_i (X^{*s})^{*i} = 0, \quad s = 1, 2, \ldots, 2^{d-1}.$$

Иначе говоря, X, X^{*2}, X^{*4}, …, X^{*2^d-1} — в точности все корни в поле $\mathbb{F}_2[X]/\langle g(X)\rangle$ неприводимого основного многочлена g.

Ещё одно свойство, следующее из примера 2.5.36, заключается в том, что во всех трёх частях этого примера элемент X представляет собой корень порождающего многочлена $g(X)$. Однако это не так в общей ситуации: такое происходит только тогда, когда $g(X)$ — «примитивный» двоичный многочлен; подробное обсуждение этого свойства приведено в §3.1–3.3. В случае примитивного основного многочлена $g(X)$, кроме всего прочего, степени X^i при $i < d = \deg g(X)$ совпадают со степенями X^{*i}, а остальные степени X^{*i}, $d \leqslant i \leqslant 2^d - 1$, относительно легко вычислить. Помня об этом, мы можем перейти к общим двоичным кодам Хэмминга.

Пример 2.5.37. Пусть $\mathcal{X}^{\mathrm{H}}$ — двоичный $[2^l - 1, 2^l - 1 - l]$-код Хэмминга. Мы знаем, что его проверочная матрица H состоит из всех ненулевых вектор-столбцов длины l. Эти векторы, выписанные в определённом порядке, перечисляют последовательные степени ω^{*i}, $i = 0, 1, \ldots, 2^l - 2$ в поле $\mathbb{F}_2[X]/\langle g(X)\rangle$, где $\omega = X$ и $g(X) = g_0 + g_1 X + \ldots + g_l X^{l-1} + X^l$ — примитивный многочлен степени l. Таким образом,

$$H = \begin{pmatrix} 1 & 0 & \ldots & 0 & g_0 & \ldots \\ 0 & 1 & \ldots & 0 & g_1 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & g_{l-2} & \ldots \\ 0 & 0 & \ldots & 1 & g_{l-1} & \ldots \end{pmatrix}, \tag{2.5.19}$$

или $H \sim (\mathbf{1}\omega \ldots \omega^{*(l-1)}\omega^{*l} \ldots \omega^{*(2^l-2)})$. Значит, как и раньше, уравнение $\mathbf{a}H^{\mathrm{T}} = \mathbf{0}$ для кодового слова имеет вид $a(*\omega) = 0$ для соответствующего многочлена. Итак, можно сказать, что $a(X) \in \mathcal{X}^{\mathrm{H}}$ тогда и только тогда, когда ω — корень многочлена $a(X)$.

С другой стороны, по построению ω является корнем многочлена $g(X)$: $g(*X) = 0$. Поэтому мы отождествляем $[2^l - 1, 2^l - 1 - l]$-код Хэмминга с эквивалентным ему циклическим кодом длины $2^l - 1$ с порождающим

многочленом $g(X)$ и определяющем корнем ω. Роль ω может играть любой сопряжённый элемент из $\{\omega, \omega^{*2}, \ldots, \omega^{*2^{l-1}}\}$. □

Описанная идея приводит к немедленному (и далеко идущему) обобщению. Возьмём $N = 2^l - 1$ и пусть ω — примитивный элемент поля $\mathbb{F}_{2^l} \simeq \mathbb{F}_2[X]/\langle g(X)\rangle$, где $g(X)$ — примитивный многочлен. (Во всех примерах и задачах этого параграфа и § 2.6 эти требования выполнены.) Рассмотрим определяющее множество корней, для начала ω, ω^2, ω^3, но в общем случае ω, ω^2, …, $\omega^{(\delta-1)}$. (Традиционно здесь используется целое число $\delta \geqslant 3$.) Что можно сказать о циклическом коде с этими корнями? Поскольку его длина $N = 2^l - 1$, можно предположить, что это подкод $[2^l - 1, 2^l - 1 - l]$-кода Хэмминга и он исправляет более одной ошибки. В этом суть конструкции так называемых (двоичных) БЧХ-кодов.

Здесь мы ограничимся кратким введением в БЧХ-коды; подробности и обобщения обсуждаются в § 3.2. Для $N = 2^l - 1$ поле $\mathbb{F}_2[X]/\langle g(X)\rangle$ обладает тем свойством, что его ненулевые элементы — это корни степени N из единицы (т. е. нули многочлена $1 + X^N$). Иначе говоря, многочлен $1 + X^N$ раскладывается в произведение линейных множителей $\prod_{j=1}^{N}(X - \omega_j)$, где корни ω_j пробегают всю мультипликативную группу $\mathbb{F}^*_{2^l}$. (В терминологии § 3.1 поле $\mathbb{F}_{2^l}$ — поле разложения многочлена $1 + X^N$ над $\mathbb{F}_2$.) Как обычно, образующую мультипликативной циклической группы $\mathbb{F}^*_{2^l}$ обозначаем символом $\omega := X$. (Можно выбирать любую образующую этой группы.)

Определение 2.5.38. При данных $N = 2^l - 1$ и $\delta = 3, \ldots, N$ определим *двоичный БЧХ-код в узком смысле* $\mathcal{X}^{\mathrm{BCH}}_{N,\delta}$ длины N и с проектируемым расстоянием δ как циклический код, построенный по двоичному многочлену $a(X)$ степени меньше N такой, что

$$a(\omega) = a(\omega^2) = \ldots = a(\omega^{(\delta-1)}) = 0. \tag{2.5.20}$$

Иначе говоря, $\mathcal{X}^{\mathrm{BCH}}_{N,\delta}$ — циклический код длины N, образующий многочлен $g(X)$ которого — это минимальный двоичный многочлен, имеющий корни ω, ω^2, …, $\omega^{(\delta-1)}$:

$$g(X) = \mathrm{НОК}\{(X - \omega), \ldots, (X - \omega^{(\delta-1)})\} = \mathrm{НОК}\{M_\omega(X), \ldots, M_{\omega^{(\delta-1)}}(X)\}. \tag{2.5.21}$$

Здесь НОК обозначает наименьшее общее кратное и $M_\alpha(X)$ — минимальный двоичный многочлен с корнем α. Для краткости в этой главе мы используем термин БЧХ-коды. (Более общий класс БЧХ-кодов вводится в § 3.2.) □

Пример 2.5.39. Для $N = 7$ подходит полиномиальное кольцо $\mathbb{F}_2[X]/\langle 1 + X + X^3\rangle$ или $\mathbb{F}_2[X]/\langle 1 + X^2 + X^3\rangle$, т. е. одна из двух реализаций поля $\mathbb{F}_8$. Поскольку 7 — простое число, любой ненулевой многочлен из

этого поля имеет мультипликативный порядок 7, т. е. является образующей мультипликативной группы в поле $\mathbb{F}_2[X]/\langle 1+X^2+X^3\rangle$. На самом деле мы имеем разложение многочлена $1+X^7$ на неприводимые множители:

$$1+X^7=(1+X)(1+X+X^3)(1+X^2+X^3).$$

Если мы выберем полиномиальное кольцо $\mathbb{F}_2[X]/\langle 1+X+X^3\rangle$, то $\omega=X$ удовлетворяет равенствам

$$\omega^3=1+\omega,\quad (\omega^2)^3=1+\omega^2,\quad (\omega^4)^3=1+\omega^5,$$

т. е. сопряжённые элементы ω, ω^2 и ω^4 являются корнями минимального многочлена $1+X+X^3$:

$$1+X+X^3=(X-\omega)(X-\omega^2)(X-\omega^4).$$

Далее, ω^3, ω^6 и $\omega^{12}=\omega^5$ — корни многочлена $1+X^2+X^3$:

$$1+X^2+X^3=(X-\omega^3)(X-\omega^5)(X-\omega^6).$$

Следовательно, двоичный БЧХ-код задается такими двоичными многочленами $a(X)$, степени которых не превышает 6, что

$$a(\omega)=a(\omega^2)=0,\quad \text{т. е. } a(X) \text{ кратен многочлену } 1+X+X^3.$$

Этот код эквивалентен $[4,7]$-коду Хэмминга, в частности, его «истинное» расстояние равно 3.

Далее, двоичный БЧХ-код длины 7 с проектируемым расстоянием 4 задается такими многочленами $a(X)$ степени, не выше 6, что

$$a(\omega)=a(\omega^2)=a(\omega^3)=0,\ \text{ т. е. } a(X) \text{ кратен многочлену}$$
$$(1+X+X^3)(1+X^2+X^3)=1+X+X^2+X^5+X^4+X^5+X^6. \quad \square$$

Теория БЧХ-кодов основывается на следующей теореме.

Теорема 2.5.40. *Минимальное расстояние двоичного БЧХ-кода с проектируемым расстоянием δ не меньше чем δ.*

Доказательство теоремы опирается на следующую лемму.

Лемма 2.5.41. *Рассмотрим определитель Δ матрицы Вандермонда размера $m\times m$ с элементами из коммутативного кольца*

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^m & \alpha_2^m & \dots & \alpha_m^m \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_1^2 & \dots & \alpha_1^m \\ \alpha_2 & \alpha_2^2 & \dots & \alpha_2^m \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_m & \alpha_m^2 & \dots & \alpha_m^m \end{pmatrix}. \tag{2.5.22}$$

Значение этого определителя

$$\Delta = \prod_{l=1}^{m} \alpha_l \times \prod_{1 \leqslant i < j \leqslant m} (\alpha_i - \alpha_j). \tag{2.5.23}$$

Доказательство. Оба определителя — это полиномиальные выражения от переменных $\alpha_1, \ldots, \alpha_m$. Если $\alpha_i = \alpha_j$ при $i < j$, то определитель имеет две повторяющиеся строки (столбца) и, поэтому, равен нулю (как и в стандартной арифметике). Следовательно, Δ делится на произведение $\prod_{1 \leqslant i < j \leqslant m} (\alpha_i - \alpha_j)$. Сравнивая затем степени α_i в формулах (2.5.22) и (2.5.23), получаем требуемое утверждение. □

Доказательство теоремы 2.5.40. Пусть $a(X) \in \mathcal{X}$. Тогда $a(*\omega^{*j}) = 0 \ \forall j = 1, \ldots, \delta - 1$, т. е.

$$\begin{pmatrix} 1 & \omega & \omega^2 & \ldots & \omega^{*(N-1)} \\ 1 & \omega^{*2} & \omega^{*4} & \ldots & \omega^{*2(N-1)} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & \omega^{*(\delta-1)} & \omega^{*2(\delta-1)} & \ldots & \omega^{*(N-1)(\delta-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} = 0.$$

По лемме 2.5.41 любые $\delta - 1$ столбцов $(\delta - 1) \times N$-матрицы линейно независимы. Следовательно, у многочлена $a(X)$ найдётся по крайней мере δ ненулевых коэффициентов. Поэтому расстояние не меньше δ. □

Пример 2.5.42. (Здесь исправляется ошибка, допущенная в книге [Bl, с. 106.].) 1. Рассмотрим БЧХ-код с $N = 15$ и $\delta = 5$. Воспользуемся следующим разложением на неприводимые множители:

$$X^{15} - 1 = (X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1).$$

Образующий полином равен

$$g(X) = (X^4+X+1)(X^4+X^3+X^2+X+1) = X^8+X^7+X^6+X^4+1.$$

Действительно, $g(\omega^3) = g(\omega^9) = 0$. Множество нулей многочлена $X^4+X^3+X^2+X+1$ равно $\{\omega^3, \omega^9, \omega^{12}, \omega^9\}$. Множество нулей многочлена X^4+X+1 — это $\{\omega, \omega^2, \omega^4, \omega^8\}$. Множество нулей многочлена X^4+X^3+1 — это $\{\omega^7, \omega^{14}, \omega^{13}, \omega^{11}\}$. Множество нулей многочлена X^2+X+1 — это $\{\omega^5, \omega^{10}\}$.

2. Пусть $N = 31$ и ω — примитивный элемент поля $\mathbb{F}_{32}$. Минимальный многочлен с корнем ω выглядит как

$$M_\omega(X) = (X-\omega)(X-\omega^2)(X-\omega^4)(X-\omega^8)(X-\omega^{16}).$$

Найдём также минимальный многочлен для ω^5:

$$M_{\omega^5}(X) = (X-\omega^5)(X-\omega^{10})(X-\omega^{20})(X-\omega^9)(X-\omega^{18}).$$

По определению образующий полином БЧХ-кода длины 31 с предполагаемым расстоянием $\delta = 8$ равен $g(X) = \text{НОК}(M_\omega(X), M_{\omega^3}(X), M_{\omega^5}(X), M_{\omega^7}(X))$. Фактически минимальное расстояние БЧХ-кода (которое, очевидно равно, по крайней мере 9) не менее 11. Это следует из теоремы 2.5.40, поскольку все степени ω, ω^2, …, ω^{10} являются корнями многочлена $g(X)$. □

Существует простая в применении процедура декодирования БЧХ-кодов: она обобщает декодирование кода Хэмминга. Ввиду теоремы 2.5.40 БЧХ-код с проектируемым расстоянием δ исправляет по крайней мере $t = \left\lfloor \dfrac{\delta - 1}{2} \right\rfloor$ ошибок. Предположим, что посланное кодовое слово $\mathbf{c} = c_0 \dots c_{N-1}$ исказилось до $\mathbf{r} = \mathbf{c} + \mathbf{b}$, где $\mathbf{b} = e_0 \dots e_{N-1}$. Предположим также, что в слове $\mathbf{b}$ не менее t ненулевых символов. Рассмотрим соответствующие многочлены $c(X)$, $r(X)$ и $e(X)$, степени которых меньше чем N. Про $c(X)$ мы знаем, что $c(\omega) = c(\omega^2) = \dots = c(\omega^{(\delta-1)}) = 0$. Поэтому

$$r(\omega) = e(\omega), \quad r(\omega^2) = e(\omega^2), \quad \dots, \quad r(\omega^{(\delta-1)}) = e(\omega^{(\delta-1)}). \tag{2.5.24}$$

Итак, мы вычисляем $r(\omega^i)$ для $i = 1, \dots, \delta - 1$. Если все эти значения нулевые, то $r(X) \in \mathcal{X}$ (нет ошибок или по крайней мере $t + 1$ ошибка). В противном случае пусть множество $E = \{i\colon e_i = 1\}$ указывает на ошибочные знаки и допустим, что $0 < \#E \leqslant t$. Введём *многочлен обнаружения ошибок*

$$\sigma(X) = \prod_{i \in E} (1 - \omega^i X) \tag{2.5.25}$$

с двоичными коэффициентами степени $\#E$. Если известен многочлен $\sigma(X)$, мы можем определить, какие из степеней ω^{-i} являются его корнями, и тем самым обнаружить ошибочные символы $i \in E$. Мы просто обратим их и исправим ошибки.

Для вычисления $\sigma(X)$ рассмотрим формальный степенной ряд

$$\zeta(X) = \sum_{j \geqslant 1} e(\omega^j) X^j.$$

(Заметим, что ввиду равенства $\omega^N = 1$ коэффициенты этого ряда повторяются.) В силу формулы (2.5.24) первые $\delta - 1$ коэффициентов удовлетворяют уравнениям

$$e(\omega^j) = r(\omega^j), \quad j = 1, \dots, \delta - 1.$$

Это единственное, что нам нужно. Эти уравнения можно решить в терминах полученного слова $\mathbf{r}$.

Теперь положим

$$\omega(X) = \sum_{i \in E} \omega^i X \prod_{j \in E\colon j \neq i} (1 - \omega^j X) \tag{2.5.26}$$

и перепишем формальный ряд:

$$\zeta(X) = \sum_{j\geqslant 1}\sum_{i\in E}\omega^{ij}X^j = \sum_{i\in E}\sum_{j\geqslant 1}\omega^{ij}X^j = \sum_{i\in E}\frac{\omega^i X}{1-\omega^i X} = \frac{\omega(X)}{\sigma(X)}. \qquad (2.5.27)$$

Заметим, что степень многочленов $\omega(X)$ и $\sigma(X)$ равна $\#E \leqslant t$.

Далее, уравнение $\zeta(X)\sigma(X) = \omega(X)$ из формулы (2.5.27) можно переписать через коэффициенты, опираясь на свойство

$$e(\omega^j) = r(\omega^j), \quad j = 1, \ldots, 2t.$$

А именно,

$$(\sigma_0 + \sigma_1 X + \ldots + \sigma_t X^t)(r(\omega)X + \ldots + r(\omega^{2t})X^{2t} + e(\omega^{(2t+1)})X^{2t+1} + \ldots) = \\ = \omega_0 + \omega_1 X + \ldots + \omega_t X^t. \quad (2.5.28)$$

Нас интересуют коэффициенты при X^k для $t < k \leqslant 2t$: они удовлетворяют равенству

$$\sum_{j=0}^{t}\sigma_j r(\omega^{(k-j)}) = 0, \qquad (2.5.29)$$

в которое не входят все члены $e(\omega^i)$. Мы получаем следующие уравнения:

$$\begin{pmatrix} r(\omega^{(t+1)}) & r(\omega^t) & \ldots & r(\omega) \\ r(\omega^{(t+2)}) & r(\omega^{(t+1)}) & \ldots & r(\omega^2) \\ \vdots & \vdots & \ddots & \vdots \\ r(\omega^{(2t)}) & r(\omega^{(2t-1)}) & \ldots & r(\omega^t) \end{pmatrix}\begin{pmatrix}\sigma_0\\ \sigma_1\\ \vdots\\ \sigma_t\end{pmatrix} = 0.$$

Размер левой матрицы равен $t \times (t+1)$, так что у неё всегда есть ненулевой вектор в ядре; он отождествляется с многочленом обнаружения ошибок $\sigma(X)$. Мы видим, что описанная выше рутинная процедура (называемая *алгоритмом декодирования Берлекэмпа—Мэсси*) позволяет нам указать множество E и поэтому исправить не менее t ошибок.

К сожалению, БЧХ-коды асимптотически «плохие»: для любой последовательности БЧХ-кодов длины $N \to \infty$ либо k/N, либо d/N стремится к нулю. Иначе говоря, они лежат ниже нижней границы на рис. 1.11. Чтобы построить коды, отвечающие неравенству Гильберта—Варшамова, нужны более сильные методы, основанные на алгебраической геометрии. Такие коды были построены в начале 1970-х гг. (коды Гоппы и Юстенсена). Построение кодов, расположенных *над* кривой Гильберта—Варшамова, — всё ещё нерешённая задача (кривая Гильберта—Варшамова даёт нижнюю границу для лучших кодов, но не исключает существование кодов выше неё: проблема заключается в том, чтобы найти такие коды или доказать,

что их нет). В 1983 г. был открыт новый класс кодов, лежащий *над* кривой Гильберта—Варшамова, но с алфавитом, состоящим из не менее чем 49 символов. Задача для двоичных кодов ожидает своего решения.

Пример 2.5.43. Вычислите ранг и минимальное расстояние циклического кода с образующим многочленом $g(X) = X^3 + X + 1$ и проверочным многочленом $h(X) = X^4 + X^2 + X + 1$. Пусть теперь ω — корень многочлена $g(X)$ в поле $\mathbb{F}_8$. Мы получили слово $r(X) = X^5 + X^3 + X \bmod(X^7 + 1)$. Проверьте, что $r(\omega) = \omega^4$, и декодируйте $r(X)$ м. п.-декодером.

Решение. Циклический код $\mathcal{X}$ длины N имеет образующую $g(X)$ и проверочный многочлен $h(X)$ со свойством $g(X)h(X) = 1 + X^N$. Заметим, что если степень многочлена $g(X)$ равна k, т. е. $g(X) = a_0 + a_1X + \ldots + a_kX^k$, где $a_k \neq 0$, то $g(X)$, $Xg(X)$, $\ldots X^{N-k-1}g(X)$ — базис кода $\mathcal{X}$. В частности, ранг кода $\mathcal{X}$ равен $N - k$. В нашем примере $N = 7$, $k = 3$ и $\dim \mathcal{X} = 4$.

Если $h(X) = b_0 + b_1X + \ldots + b_{N-k}X^{N-k}$, то проверочная матрица H кода $\mathcal{X}$ имеет вид

$$\underbrace{\begin{pmatrix} b_{N-k} & b_{N-k-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 & 0 \\ 0 & b_{N-k} & b_{N-k-1} & \ldots & b_1 & b_0 & \ldots & 0 & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ 0 & 0 & \ldots & 0 & b_{N-k} & b_{N-k-1} & \ldots & b_1 & b_0 \end{pmatrix}}_{N}.$$

Кодовые слова из $\mathcal{X}$ дают соотношения линейной зависимости между столбцами матрицы H. В нашем примере

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

и возникают следующие импликации:

$$\text{нет нулевых столбцов} \Rightarrow \text{нет кодовых слов веса 1},$$

$$\text{нет повторяющихся столбцов} \Rightarrow \text{нет кодовых слов веса 2}.$$

Минимальное расстояние $d(\mathcal{X})$ линейного кода $\mathcal{X}$ совпадает с минимальным ненулевым весом кодового слова. В нашем примере $d(\mathcal{X}) = 3$. (На самом деле $\mathcal{X}$ эквивалентен $[7, 4]$-коду Хэмминга.)

Поскольку многочлен $g(X) \in \mathbb{F}_2[X]$ неприводим, код $\mathcal{X} \in \mathbb{F}_2[X]/(X^7 - 1)$ — циклический код, определённый элементом ω. Мультипликативная циклическая группа $\mathbb{Z}_7^\times$ ненулевых элементов поля $\mathbb{F}_8$ — это

$$\omega^0 = 1,\ \omega,\ \omega^2,\ \omega^3 = \omega + 1,\ \omega^4 = \omega^2 + \omega,$$
$$\omega^5 = \omega^3 + \omega^2 = \omega^2 + \omega + 1,\ \omega^6 = \omega^3 + \omega^2 + \omega = \omega^2 + 1,$$
$$\omega^7 = \omega^3 + \omega = 1.$$

Далее вычисляем $r(\omega)$:

$$r(\omega) = \omega + \omega^3 + \omega^5 = \omega + (\omega + 1) + (\omega^2 + \omega + 1) = \omega^2 + \omega = \omega^4,$$

что и требовалось. Пусть $c(X) = r(X) + X^4 \bmod (1 + X^7)$. Тогда $c(\omega) = 0$, т. е. $c(X)$ — кодовое слово. Так как $d(\mathcal{X}) = 3$, код исправляет одну ошибку. Мы только что нашли кодовое слово $c(X)$ на расстоянии 1 от $r(X)$. Значит, $r(X) = X + X^3 + X^5$ декодируется м. п.-декодером как

$$c(X) = X + X^3 + X^4 + X^5 \bmod (1 + X^7). \qquad \square$$

Простые числа предназначены для умножения, а не сложения.

Лев Ландау (1908–1968), советский физик, лауреат Нобелевской премии по физике

Закончим этот параграф двумя полезными утверждениями.

Пример 2.5.44. (алгоритм Евклида для многочленов). Алгоритм Евклида представляет собой способ вычисления наибольшего общего делителя двух многочленов $f(X)$ и $g(X)$ над некоторым конечным (на самом деле, над любым) полем $\mathbb{F}$. Предположим, что $\deg g(X) \leqslant \deg f(X)$, и положим $f(X) = r_{-1}(X)$, $g(X) = r_0(X)$. Тогда

1) делим $r_{-1}(X)$ на $r_0(X)$:

$$r_{-1}(X) = q_1(X) r_0(X) + r_1(X), \quad \deg r_1(X) < \deg r_0(X),$$

2) делим $r_0(X)$ на $r_1(X)$:

$$r_0(X) = q_2(X) r_1(X) + r_2(X), \quad \deg r_2(X) < \deg r_1(X),$$

$\vdots$

k) делим $r_{k-2}(X)$ на $r_{k-1}(X)$:

$$r_{k-2}(X) = q_k(X) r_{k-1}(X) + r_k(X), \quad \deg r_k(X) < \deg r_{k-1}(X),$$

$\vdots$

алгоритм продолжается до тех пор, пока не получится нулевой остаток:

s) делим $r_{s-2}(X)$ на $r_{s-1}(X)$:

$$r_{s-2}(X) = q_s(X) r_{s-1}(X).$$

В результате

$$\text{НОД}\,(f(X),\, g(X)) = r_{s-1}(X). \tag{2.5.30}$$

На каждом шаге соотношение на очередной остаток $r_k(X)$ включает в себя два предыдущих остатка. Поэтому все остатки, и НОД $(f(X),\, g(X))$

в том числе, можно выразить через $f(X)$ и $g(X)$. А именно, справедлива следующая лемма.

Лемма 2.5.45. *Остаток $r_k(X)$ в алгоритме Евклида удовлетворяет соотношению*

$$r_k(X) = a_k(X)f(X) + b_k(X)g(X), \quad k \geqslant -1,$$

где

$$\begin{aligned} a_{-1} &= 1, \quad b_{-1} = 0, \\ a_0 &= 0, \quad b_0 = 1, \\ a_k(X) &= -q_k(X)a_{k-1}(X) + a_{k-2}(X), \quad k \geqslant 1, \\ b_k(X) &= -q_k(X)b_{k-1}(X) + b_{k-2}(X), \quad k \geqslant 1. \end{aligned}$$

В частности, существуют такие многочлены $a(X)$, $b(X)$, что

$$\text{НОД}\,(f(X),\, g(X)) = a(X)f(X) + b(X)g(X).$$

Более того,

1) $\deg a_k(X) = \sum\limits_{i=2}^{k} \deg q_i(X)$, $\deg b_k(X) = \sum\limits_{i=1}^{k} \deg q_i(X)$,

2) $\deg r_k(X) = \deg f(X) - \sum\limits_{i=1}^{k+1} \deg q_i(X)$,

3) $\deg b_k(X) = \deg f(X) - \deg r_{k-1}(X)$,

4) $a_k b_{k+1}(X) - a_{k+1}b_k(X) = (-1)^{k+1}$,

5) *$a_k(X)$ и $b_k(X)$ взаимно просты*,

6) $r_k(X)b_{k+1}(X) - r_{k+1}(X)b_k(X) = (-1)^{k+1}f(X)$,

7) $r_{k+1}(X)a_k(X) - r_r(X)a_{k+1}(X) = (-1)^{k+1}g(X)$.

Доказательство оставляется в качестве упражнения. □

§ 2.6. Дополнительные задачи к главе 2

> An unsophisticated forecaster uses statistics as a drunken man uses lampposts: for support rather than for illumination
>
> Наивный прогнозист использует статистику, как пьяный человек использует фонарные столбы: для поддержки, а не для освещения.
>
> *Эндрю Лэнг* (1844–1912), шотландский ученый-антрополог и литератор

Задача 2.6.1. Проверочный многочлен $h(X)$ двоичного циклического кода $\mathcal{X}$ длины N определяется следующим условием: $a(X) \in \mathcal{X}$ тогда и только тогда, когда $a(X)h(X) = 0 \bmod (1 + X^N)$. Как проверочный многочлен связан с образующей кода $\mathcal{X}$? Для данного многочлена $h(X)$ рассмотрите проверочную матрицу и интерпретируйте смежный класс $\mathcal{X} + \mathbf{y}$ кода $\mathcal{X}$.

Опишите все циклические коды длин 16 и 15. Найдите порождающий и проверочный многочлены кода повторений и кода проверки на чётность. Найдите порождающий и проверочный многочлены кода Хэмминга длины 7.

Решение. Все циклические коды длины 16 порождаются делителями многочлена $1 + X^{16} = (1 + X)^{16}$, т. е. многочленами $g(X) = (1 + X)^k$, где $k = 0, 1, \ldots, 16$. Здесь $k = 0$ соответствует всему пространству $\{0, 1\}^{16}$, $k = 1$ — коду проверки на чётность, $k = 15$ — коду повторений $\{0 \ldots 0, 1 \ldots 1\}$ и $k = 16$ — нулевому коду. При $N = 15$ разложение на неприводимые множители имеет вид

$$1 + X^{15} = (1 + X)(1 + X + X^2)(1 + X + X^4)(1 + X^3 + X^4)(1 + X + X^2 + X^3 + X^4).$$

Любое произведение перечисленных неприводимых многочленов порождает циклический код.

В общей ситуации $1 + X^N = (1 + X)(1 + X + \ldots + X^{N-1})$; $g(X) = 1 + X$ порождает код проверки на чётность, а $g(X) = 1 + X + \ldots + X^{N-1}$ — код повторений. В случае $[7, 4]$-кода Хэмминга образующий многочлен имеет вид $g(X) = 1 + X + X^3$, что проверяется непосредственно.

Проверочный многочлен равен отношению $(1 + X^N)/\langle g(X)\rangle$. Действительно, для всех $a(X) \in \mathcal{X}$ имеем $a(X)h(X) = v(X)g(X)h(X) = v(X)(1 + X^N) = 0 \bmod (1 + X^N)$. Обратно, если $a(X)h(X) = v(X)(1 + X^N)$, то $a(X)$ должен иметь вид $v(X)g(X)$ из-за единственности разложения на неприводимые множители.

Смежные классы $\mathbf{y} + \mathcal{X}$ находятся во взаимно однозначном соответствии с остатками $y(X) = u(X) \bmod (g(X))$. Иными словами, два слова $\mathbf{y}^{(1)}$

и $\mathbf{y}^{(2)}$ лежат в одном смежном классе тогда и только тогда, когда

$$y^{(i)}(X) = v^{(i)}(X)g(X) + u^{(i)}(X), \quad i = 1, 2, \quad u^{(1)}(X) = u^{(2)}(X).$$

Действительно, $\mathbf{y}^{(1)}$ и $\mathbf{y}^{(2)}$ лежат в одном смежном классе тогда и только тогда, когда $\mathbf{y}^{(1)} + \mathbf{y}^{(2)} \in \mathcal{X}$. Это эквивалентно тому, что $u^{(1)}(X) + u^{(2)}(X) = 0$, т. е. $u^{(1)}(X) = u^{(2)}(X)$. Если $h(X) = \sum\limits_{j=0}^{k} h_j X^j$, то

$$\sum_{j=0}^{i} g_j h_{i-j} = \begin{cases} 1, & i = 0, N, \\ 0, & 1 \leqslant i < N. \end{cases}$$

Поэтому $\langle \mathbf{g} \cdot \mathbf{h}^{\perp} \rangle = 0$, где $\mathbf{h}^{\perp}$ — вектор коэффициентов полинома $h^{\perp}(X) = h_k + h_{k-1}X + \ldots + h_0 X^k$. Следовательно, строки проверочной матрицы H для $\mathcal{X}$ получаются циклическими сдвигами строки $\mathbf{h} = h_k h_{k-1} \ldots h_0 0 \ldots 0$. Проверочные многочлены для кода повторений и проверки на чётность — это $1 + X$ и $1 + X + \ldots + X^{N-1}$. Они двойственны друг другу. Проверочный многочлен $[7, 4]$-кода Хэмминга равен $1 + X + X^2 + X^4$, что легко проверить. □

Задача 2.6.2. 1. Докажите неравенства Хэмминга и Гильберта—Варшамова на размер двоичного $[N, d]$-кода в терминах $v_N(d)$ — объёма N-мерного шара Хэмминга радиуса d.

Пусть минимальное расстояние $d = \lfloor \tau N \rfloor$ для некоторого фиксированного $\tau \in (0, 1/2)$ и $\alpha(N, \lfloor \tau N \rfloor)$ — наибольшая скорость передачи информации двоичного кода, исправляющего $\lfloor \tau N/2 \rfloor$ ошибок. Покажите, что

$$1 - \eta(\tau) \leqslant \liminf_{N\to\infty} \alpha(N, \lfloor \tau N \rfloor) \leqslant \limsup_{N\to\infty} \alpha(N, \lfloor \tau N \rfloor) \leqslant 1 - \eta(\tau/2). \quad (2.6.1)$$

2. Зафиксируем число $R \in (0, 1)$ и предположим, что нужно переслать набор U_N сообщений длины N, где $\#U_N = 2^{NR}$. Сообщение передаётся по д. с. к. б. п. с вероятностью ошибки $p < 1/2$, так что мы ожидаем около pN ошибок. Учитывая асимптотическую границу из п. 1, ответьте, при каких значениях p можно исправлять pN ошибок при больших N.

Решение. 1. Говорят, что код $\mathcal{X} \subset \mathbb{F}_2^N$ исправляет E ошибок, если $\mathcal{B}(\mathbf{x}, E) \cap \mathcal{B}(\mathbf{y}, E) = \varnothing \ \forall \mathbf{x}, \mathbf{y} \in \mathcal{X}$ при $\mathbf{x} \neq \mathbf{y}$. Неравенство Хэмминга для кода размера M с расстоянием d, исправляющего $E = \lfloor (d-1)/2 \rfloor$ ошибок, получается следующим образом. Шары радиуса E с центрами в кодовых словах не пересекаются, и их общий объём равен $M \times v_N(E)$. Но их объединение лежит внутри $\mathbb{F}_2^N$, поэтому $M \leqslant 2^N / v_N(E)$.

С другой стороны, возьмём код $\mathcal{X}^*$, исправляющий E ошибок, максимального размера $\#\mathcal{X}$. Тогда не будет слов

$$\mathbf{y} \in \mathbb{F}_2^N \setminus \bigcup_{\mathbf{x}\in\mathcal{X}^*} \mathcal{B}(\mathbf{x}, 2E+1),$$

или мы смогли бы добавить такое слово к $\mathcal{X}^*$, увеличив размер, не меняя при этом свойство исправления ошибок. Каждое слово $\mathbf{y} \in \mathbb{F}_2^N$ расположено на расстоянии, не больше чем $d-1$ от кодового слова, ибо в противном случае мы можем добавить $\mathbf{y}$ к коду. Следовательно, шары радиуса $d-1$ покрывают всё пространство $\mathbb{F}_2^N$, т. е. $M \times v_N(d-1) \geqslant 2^N$, или

$$M \geqslant 2^N / v_N(d-1) \quad \text{(неравенство Гильберта—Варшамова).}$$

Из комбинации этих неравенств следует, что для $\alpha(N, E) = (\log \#\mathcal{X})/N$ справедлива оценка

$$1 - \frac{\log v_N(2E+1)}{N} \leqslant \alpha(N, E) \leqslant 1 - \frac{\log v_N(E)}{N}. \tag{2.6.2}$$

Заметим, что для любого $s < \varkappa N$, где $0 < \varkappa < 1/2$, имеет место неравенство

$$C_N^{s-1} = \frac{s}{N-s+1} C_N^s < \frac{\varkappa}{1-\varkappa} C_N^s.$$

Следовательно,

$$C_N^E \leqslant v_N(E) \leqslant C_N^E \sum_{j=0}^{E} \left(\frac{\varkappa}{1-\varkappa}\right)^j.$$

Теперь по формуле Стирлинга при $N,\ E \to \infty$ и $E/N \to \tau \in (0,\ 1/4)$ получаем

$$\frac{1}{N} \log C_N^E \to \eta(\tau/2).$$

Итак, мы доказали, что $\lim\limits_{N\to\infty} \dfrac{1}{N} \log v_N(\lfloor \tau N \rfloor) = \eta(\tau)$ и из неравенства (2.6.2) следует оценка (2.6.1).

2. Мы можем исправить pN ошибок, если минимальное расстояние d подчиняется неравенству $\left\lfloor \dfrac{d-1}{2} \right\rfloor \geqslant pN$, т. е. $\tau/2 \geqslant p$. Опираясь на асимптотическое неравенства Хэмминга, мы получаем, что $R \leqslant 1 - \eta(\tau/2) \leqslant 1 - \eta(p)$. Поэтому надёжная передача возможна, если $p \leqslant \eta^{-1}(1-R)$.

Вторая теорема Шеннона утверждает, что

$$\text{пропускная способность } C \text{ канала без памяти} = \sup_{p_X} I(X:Y).$$

Здесь $I(X:Y) = h(Y) - h(Y|X)$ — взаимная энтропия между отдельным символом случайного входа и выхода канала, максимизированная по всем распределениям входной буквы X. Для д. с. к. б. п. с вероятностью ошибки p условная энтропия $h(Y|X)$ равна $\eta(p)$. Поэтому

$$C = \sup_{p_X} h(Y) - \eta(p).$$

Но $h(Y)$ достигает максимального значения 1 при равномерном распределении входного сигнала X (тогда с. в. Y тоже равномерно распределена). Следовательно, пропускная способность д. с. к. б. п. равна $C = 1 - \eta(p)$, т. е. $p \leqslant \eta^{-1}(1-R)$. Эти два аргумента приводят к одному ответу. □

Если вы обнаружили, то не забывайте.
Если вы исправили, то не жалейте.

(Из серии «Так говорил суперлектор».)

Задача 2.6.3. Докажите, что минимальное расстояние двоичного кода длины 23, порождённого многочленом $g(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$, равно 7, и что он совершенен.

Указание. Заметим, что согласно БЧХ-теореме 2.5.40 если порождающий многочлен циклического кода имеет корни $\{\omega, \omega^2, \ldots, \omega^{\delta-1}\}$, то расстояние кода не меньше δ. Проверьте, что $X^{23} + 1 \equiv (X+1)g(X)g^{\mathrm{rev}}(X) \bmod 2$, где $g^{\mathrm{rev}}(X) = X^{11}g(X^{-1})$ — обращение[10] многочлена $g(X)$.

Решение. Покажем сначала, что это БЧХ-код с проектируемым расстоянием 5. Напомним, что если ω — корень многочлена $p(X) \in \mathbb{F}_2[X]$, то его корнем также будет ω^2. Значит, если ω — корень многочлена $g(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$, то таковыми будут и ω^2, ω^4, ω^8, ω^{16}, ω^9, ω^{18}, ω^{13}, ω^3, ω^6, ω^{12}. Это приводит к последовательным корням $\{\omega, \omega^2, \omega^3, \omega^4\}$. По БЧХ-теореме код $\mathcal{X} = \langle g(X)\rangle$ имеет расстояние не меньше 5.

Далее, расширение проверкой на чётность $\mathcal{X}^+$ ортогонально себе. Для проверки этого нужно только показать, что любые две строки образующей матрицы кода $\mathcal{X}^+$ ортогональны. Их можно записать в виде

$$(X^i g(X)|1) \quad \text{и} \quad (X^j g(X)|1).$$

Их скалярное произведение равно

$$1 + (X^i g(X))(X^j g(X)) = 1 + \sum_r g_{i+r}g_{j+r} = 1 + \sum_r g_{i+r}g^{\mathrm{rev}}_{11-j-r} =$$

$$= 1 + \text{коэффициент при } X^{11+i-j} \text{ в многочлене } \underbrace{(g(X) \times g^{\mathrm{rev}}(X))}_{\substack{\| \\ 1+\ldots+X^{22}}} = 1 + 1 = 0.$$

Таким образом,

$$\text{любые два слова в } \mathcal{X}^+ \text{ ортогональны.} \tag{2.6.3}$$

[10] Если $p(X) = a_0 + a_1X + \ldots + a_nX^n$, то его обращение имеет вид $p^{\mathrm{rev}}(X) = a_n + a_{n-1}X + \ldots + a_0X^n$.

Отсюда следует, что вес любого слова из $\mathcal{X}^+$ делится на 4. Действительно, прямой проверкой убеждаемся, что все строки $(X^i g(X)|1)$ образующей матрицы кода $\mathcal{X}^+$ имеют вес 8. Тогда индукцией по числу строк, участвующих в сумме, можно показать, что если $\mathbf{c} \in \mathcal{X}^+$ и $\mathbf{g}^{(i)} \sim (X^i g(X)|1)$ — строка образующей матрицы, то

$$w(\mathbf{g}^{(i)} + \mathbf{c}) = w(\mathbf{g}^{(i)}) + w(\mathbf{c}) - 2w(\mathbf{g}^{(i)} \wedge \mathbf{c}),$$

где $(\mathbf{g}^{(i)} \wedge \mathbf{c})_l = \min[(g^{(i)})_l, c_l]$, $l = 1, \ldots, 24$. Мы знаем, что $8|w(\mathbf{g}^{(i)})$ и по индуктивному предположению $4|w(\mathbf{c})$. Далее, по формуле (2.6.3) вес $w(\mathbf{g}^{(i)} \wedge \mathbf{c})$ чётен, и, значит, $2w(\mathbf{g}^{(i)} \wedge \mathbf{c})$ делится на 4. Следовательно, л. ч., т. е. $w(\mathbf{g}^{(i)} + \mathbf{c})$, тоже делится на 4. Отсюда можно сделать вывод, что расстояние кода $\mathcal{X}^+$ равно 8, так как это число больше 5 и делится на 4. (Ясно, что оно не может превышать 8, так как тогда оно равно 12.) Итак, расстояние исходного кода $\mathcal{X}$ равно 7.

Наконец, код $\mathcal{X}$ совершенный, исправляющий три ошибки, поскольку объём 3-шара в $\mathbb{F}_2^{23}$ равен

$$C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3 = 1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

и $2^{12} \times 2^{11} = 2^{23}$. Здесь, очевидно, 12 представляет ранг, а 23 — длину кода. □

> Специалист по алгебраическому кодированию делает это в поле (желательно большом, но конечном).
>
> (Из серии «Как они делают это».)

Задача 2.6.4. Покажите, что код Хэмминга является циклическим кодом с проверочным многочленом $X^4 + X^2 + X + 1$. Чему равна его образующая? Содержит ли исходный код Хэмминга подкод, эквивалентный двойственному к нему? Пусть разложение на неприводимые приведённые многочлены $M_j(X)$ имеет вид

$$X^N + 1 = \prod_{j=1}^{l} M_j(X)^{k_j}. \tag{2.6.4}$$

Докажите, что число циклических кодов длины N равно $\prod\limits_{j=1}^{l}(k_j + 1)$.

Решение. Циклический код с образующей $g(X) = X^3 + X + 1$ имеет проверочный многочлен $h(X) = X^4 + X^2 + X + 1$ в силу разложения

$$X^7 + 1 = (X^3 + X + 1)(X^4 + X^2 + X + 1).$$

Проверочная матрица кода имеет своими столбцами все ненулевые элементы из $\mathbb{F}_2^3$:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{2.6.5}$$

Поэтому H задаёт код, эквивалентный исходному $[7, 4]$-коду Хэмминга.

Двойственный к $[7, 4]$-коду Хэмминга порождается многочленом $X^4 + X^3 + X^2 + 1$ (обращенный к $h(X)$). Поскольку $X^4 + X^3 + X^2 + 1 = (X + 1)g(X)$, он порождает подкод $[7, 4]$-кода Хэмминга.

Наконец, любой неприводимый многочлен $M_j(X)$ можно включить в разложение образующей циклического кода в любой степени $0, \ldots, k_j$. Поэтому количество способов построения этого кода равно $\prod\limits_{j=1}^{l}(k_j + 1)$. □

Задача 2.6.5. Опишите конструкцию кода Рида—Маллера. Определите для него скорость передачи информации и минимальное расстояние.

Решение. Пространство $\mathbb{F}_2^m$ имеет $N = 2^m$ точек. Пусть $A \subset \mathbb{F}_2^m$ и $\mathbf{1}_A$ — характеристическая функция множества A. Рассмотрим набор гиперплоскостей

$$\Pi_j = \{\mathbf{p} \in \mathbb{F}_2^m : p_j = 0\}.$$

Положим $h^j = \mathbf{1}_{\Pi_j}$, $j = 1, \ldots, m$, и $h^0 = \mathbf{1}_{\mathbb{F}_2^m} \equiv 1$. Определим множество функций $\mathbb{F}_2^m \to \mathbb{F}_2$:

$$\begin{aligned}
&\mathcal{A}_0 = \{h^0\},\\
&\mathcal{A}_1 = \{h^j;\ \ j = 1, 2, \ldots, m\},\\
&\mathcal{A}_2 = \{h^i \cdot h^j;\ \ i, j = 1, 2, \ldots, m,\ i < j\},\\
&\qquad\vdots\\
&\mathcal{A}_{k+1} = \{a \cdot h^j;\ \ a \in \mathcal{A}_k,\ \ j = 1, 2, \ldots, m,\ h^j \not| a\},\\
&\qquad\vdots\\
&\mathcal{A}_m = \{h^1 \ldots h^m\}.
\end{aligned}$$

Объединение этих множеств насчитывает $N = 2^m$ элементов (всего 2^m функций). Следовательно, функции из $\bigcup\limits_{i=0}^{m} \mathcal{A}_i$ можно взять в качестве базиса пространства $\mathbb{F}_2^N$.

Тогда код Рида—Маллера $\mathrm{PM}(r, m) = \mathcal{X}^{\mathrm{PM}}(r, m)$ длины $N = 2^m$ определяется как линейная оболочка $\bigcup\limits_{i=0}^{r} \mathcal{A}_i$, его ранг равен $\sum\limits_{i=0}^{r} C_m^i$. Его скорость

передачи информации равна

$$\frac{1}{2^m}\sum_{i=0}^{r} C_m^i.$$

Далее, если $\mathbf{a} \in \mathrm{PM}(r, m)$, то

$$\mathbf{a} = (\mathbf{y}, \mathbf{y})h^j + (\mathbf{x}, \mathbf{x}) = (\mathbf{x}, \mathbf{x}+\mathbf{y}),$$

для некоторого $\mathbf{x} \in \mathrm{PM}(r, m-1)$ и $\mathbf{y} \in \mathrm{PM}(r-1, m-1)$. Таким образом, $\mathrm{PM}(r, m)$ совпадает с бар-произведением $(\mathrm{PM}(r, m-1)|\mathrm{PM}(r-1, m-1))$. По неравенству бар-произведения (2.4.14) имеем

$$d[\mathrm{PM}(k, m)] \geqslant \min[2d[\mathrm{PM}(k, m-1)], d[\mathrm{PM}(k-1, m-1)]],$$

откуда по индукции получаем

$$d[\mathrm{PM}(r, m)] \geqslant 2^{m-r}.$$

С другой стороны, вектор $h^1 \cdot h^2 \cdot \ldots \cdot h^m$ расположен на расстоянии 2^{m-r} от кода $\mathrm{PM}(r, m)$. Значит,

$$d[\mathrm{PM}(r, m)] = 2^{m-r}. \qquad \square$$

Задача 2.6.6. 1. Определите код проверки на чётность длины N над полем $\mathbb{F}_2$. Покажите, что код является линейным тогда и только тогда, когда он является кодом проверки на чётность. Определите исходный код Хэмминга в терминах проверки на чётность и найдите его образующую матрицу.

2. Пусть $\mathcal{X}$ — циклический код. Определим двойственный код

$$\mathcal{X}^{\perp} = \{\mathbf{y} = y_1 \ldots y_N \colon \sum_{i=1}^{N} x_i y_i = 0 \ \forall \mathbf{x} = x_1 \ldots x_n \in \mathcal{X}\}.$$

Докажите линейность кода $\mathcal{X}^{\perp}$ и установите зависимость между образующими полиномами кодов $\mathcal{X}$ и $\mathcal{X}^{\perp}$. Покажите, что коды повторений и проверки на чётность циклические и найдите их образующие.

Решение. 1. Код проверки на чётность $\mathcal{X}^{\mathrm{PC}}$ (не обязательно линейного) кода $\mathcal{X}$ — это набор таких векторов $\mathbf{y} = y_1 \ldots y_N \in \mathbb{F}_2^N$, что

$$\langle \mathbf{y} \cdot \mathbf{x} \rangle = \sum_{i=1}^{N} x_i y_i = 0 \ (\text{ в } \mathbb{F}_2) \ \forall \mathbf{x} = x_1 \ldots x_N \in \mathcal{X}.$$

Из определения ясно, что $\mathcal{X}^{\mathrm{PC}}$ является также кодом проверки чётности для кода $\bar{\mathcal{X}}$ — линейного кода, натянутого на $\mathcal{X}$: $\mathcal{X}^{\mathrm{PC}} = \bar{\mathcal{X}}^{\mathrm{PC}}$. Действительно, если $\langle \mathbf{y} \cdot \mathbf{x} \rangle = 0$ и $\langle \mathbf{y} \cdot \mathbf{x}' \rangle = 0$, то $\langle \mathbf{y} \cdot (\mathbf{x} + \mathbf{x}') \rangle = 0$. Следовательно,

код проверки на чётность $\mathcal{X}^{\mathrm{PC}}$ всегда линеен и образует подпространство в ортогональном дополнении к $\mathcal{X}$. Данный код $\mathcal{X}$ линеен тогда и только тогда, когда он является кодом проверки на чётность двойственного кода $\mathcal{X}^{\mathrm{PC}}$. Пара линейных кодов $\mathcal{X}$ и $\mathcal{X}^{\mathrm{PC}}$ образуют двойственную пару: код $\mathcal{X}^{\mathrm{PC}}$ двойствен $\mathcal{X}$, и наоборот. Образующая матрица H кода $\mathcal{X}^{\mathrm{PC}}$ служит проверочной матрицей для $\mathcal{X}$, и наоборот.

Для кода Хэмминга длины $N = 2^l - 1$ проверочная матрица имеет размер $l \times N$ и состоит из всех ненулевых столбцов пространства $\mathbb{F}_2^l$ (в некотором порядке). Так, $[7, 4]$-код Хэмминга соответствует $l = 3$; его проверка на чётность имеет вид

$$\begin{aligned} x_1 + x_3 + x_5 + x_7 &= 0, \\ x_2 + x_3 + x_6 + x_7 &= 0, \\ x_4 + x_5 + x_6 + x_7 &= 0, \end{aligned}$$

а образующая матрица равна

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

2. Образующий полином двойственного кода имеет вид $g^{\perp}(X) = X^{N-1}g(X^{-1})$. Код повторений порождён многочленом $g(X) = 1 + X + \ldots + X^{N-1}$ и имеет ранг 1. Код проверки на чётность порождается многочленом $g(X) = 1 + X$, его ранг равен $N - 1$. □

Задача 2.6.7. 1. Как применяется теория кодирования при коэффициенте ошибки $p > 1/2$?

2. Приведите пример нелинейного кода.

3. Приведите пример линейного, но не циклического кода.

4. Дайте определение двоичного кода Хэмминга и двойственного к нему. Докажите, что код Хэмминга совершенен. Объясните, почему код Хэмминга не всегда исправляет две ошибки.

5. Докажите, что в двойственном коде к коду Хэмминга

а) вес любого ненулевого кодового слова равен 2^{l-1},

б) расстояние между любой парой кодовых слов равно 2^{l-1}.

Решение. 1. Если $p > 1/2$, мы обратим выходной сигнал и получим $p' = 1 - p$.

2. Код $\mathcal{X} = \{11\} \subset \mathbb{F}_2^2$ не линеен, поскольку $00 \notin \mathcal{X}$.

3. Код $\mathcal{X} = \{00, 10\} \subset \mathbb{F}_2^2$ линейный, но не циклический, так как $01 \notin \mathcal{X}$.

4. Поскольку $[7, 4]$-код Хэмминга имеет расстояние 3 и является совершенным, он исправляет одну ошибку. Поэтому, сделав две ошибки

в кодовом слове, мы всегда выйдем из шара радиуса 1 с центром в кодовом слове, т. е. попадём в шар радиуса 1, описанный вокруг другого кодового слова (на расстоянии 1 от ближайшего и 2 от исходного слова). Таким образом, мы обнаружим две ошибки, но не сможем их исправить.

5. Двойственный код к $[2^l - 1, 2^l - l - 1, 3]$-коду Хэмминга линеен и имеет длину $N = 2^l - 1$, а ранг l; размер его образующей матрицы равен $l \times (2^l - 1)$, а её столбцы — это список всех ненулевых векторов длины l (проверочная матрица исходного кода). Строки этой матрицы линейно независимы; более того, любая строка с номером $i = 1, \ldots, l$ имеет 2^{l-1} единиц. Так получается потому, что каждая такая единица приходит из столбца, т. е. ненулевого вектора длины l с 1 на i-м месте; существует ровно 2^{l-1} таких векторов. Кроме того, любая пара столбцов этой матрицы линейно независима (но три столбца могут быть зависимы — пара столбцов дополняется их суммой).

Каждое ненулевое кодовое слово $\mathbf{x}$ двойственного кода представляется суммой строк описанной выше образующей матрицы. Предположим, что эти слагаемые — строки с номерами $i_1, \ldots, i_s$, где $1 \leqslant i_1 < \ldots < i_s \leqslant l$. Тогда, как и раньше, число единиц в сумме равно числу столбцов этой матрицы, для которых сумма знаков $i_1, \ldots, i_s$ равна 1. У нас нет ограничений на оставшиеся $l - s$ знаков, поэтому для них существует 2^{l-s} возможностей. Для знаков $i_1, \ldots, i_s$ у нас есть 2^{s-1} возможностей (половина всех 2^s). Тогда $2^{l-s} \times 2^{s-1} = 2^{l-1}$.

Более формально, пусть $J \subset \{1, \ldots, l\}$ — множество суммируемых строк:

$$\mathbf{x} = \sum_{i \in J} g^{(i)}.$$

Тогда $\delta(\mathbf{0}, \mathbf{x})$, т. е. число ненулевых знаков в слове $\mathbf{x}$ вычисляется как

$$\underbrace{2^{l-|J|}}_{\substack{\#\text{способов расставить} \\ \text{нули и единицы в множестве } J}} \times \underbrace{\Big(\#\text{подмножеств } R \subseteq J \text{ с нечётным } |K|\Big)}_{\#\text{способов получить } \sum\limits_{i \in J} x_i = 1 \bmod 2 \text{с } x_i \in \{0,1\}},$$

откуда получим $2^{l-|J|}2^{|J|-1} = 2^{l-1}$. Другими словами, чтобы получить вклад от символа $x_j = \sum\limits_{i \in J} g^{(i)} = 1$, нужно зафиксировать а) вклад нулей и единиц из $\{1, \ldots, \} \setminus J$ (как часть описания ненулевого вектора длины N) и б) расположение нулей и единиц в J с нечётным числом единиц. Для проверки равенства $d(\mathcal{X}^{\mathrm{H}^\perp}) = 2^{l-1}$ достаточно установить, что расстояние между нулевым словом и любым другим словом $\mathbf{x} \in \mathcal{X}^{\mathrm{H}^\perp}$ равно 2^{l-1}.

Итак, вес каждого ненулевого кодового слова составляет 2^{l-1}. Иначе говоря, расстояние от нулевого вектора до любого слова двойственного

кода равно 2^{l-1}. Так как двойственный код линеен, расстояние между любой парой различных кодовых слов $\mathbf{x}$, $\mathbf{x}'$ равно 2^{l-1}:

$$\delta(\mathbf{x}, \mathbf{x}') = \delta(\mathbf{0}, \mathbf{x}' - \mathbf{x}) = w(\mathbf{x}' - \mathbf{x}) = 2^{l-1}. \qquad \square$$

Задача 2.6.8. 1. Сформулируйте необходимые и достаточные условия, при которых многочлен $g(X)$ порождает циклический код длины N. Что такое БЧХ-код? Покажите, что БЧХ-код, ассоциированный с $\{\omega, \omega^2\}$, где ω — корень многочлена $X^3 + X + 1$ в подходящем поле, совпадает с кодом Хэмминга.

2. Определите и вычислите определитель Вандермонда. Определите БЧХ-код и получите хорошую оценку на его минимальное расстояние.

Решение. 1. Необходимое и достаточное условие, при котором $g(X)$ порождает циклический код длины N, заключается в том, что $g(X)|(1 + X^N)$. Образующая $g(X)$ может быть неприводимым или приводимым многочленом; в последнем случае он представляется в виде произведения $g(X) = M_1(X) \dots M_k(X)$ неприводимых множителей, где $k \leqslant d = \deg g$. Пусть s — такое минимальное число, что $N|2^s - 1$. Тогда $g(X)$ раскладывается в произведение линейных множителей в поле $\mathbb{K} = \mathbb{F}_{2^s} \supseteq \mathbb{F}_2$: $g(X) = \prod_{i=1}^{d} (X - \omega_j)$ с $\omega_1, \dots, \omega_d \in \mathbb{K}$. (Обычно используется минимальное такое поле, называемое полем разложения многочлена $g(X)$, но это не обязательно.) Каждый элемент ω_i является корнем $g(X)$ и также корнем по крайней мере одного неприводимого множителя $M_1(X), \dots, M_k(X)$. (Более точно, каждый из $M_i(X)$ получается как произведение некоторых из перечисленных выше линейных множителей.) Возникает естественный соблазн взять минимальное определяющее множество D, где каждый неприводимый множитель представлен одним корнем, но может оказаться, что такое множество трудно описать точно. Очевидно, что $k \leqslant \#D \leqslant d$, где $\#D$ — мощность D. Корни, составляющие D, принадлежат полю $\mathbb{K}$, но на самом деле они могут попасть в его подполе $\mathbb{K}' \subset \mathbb{K}$, содержащее все ω_{j_i}. (Конечно, $\mathbb{F}_2 \subset \mathbb{K}'$.) Теперь можно отождествить код $\mathcal{X}$, порождённый многочленом $g(X)$, с множеством многочленов

$$\{f(X) \in \mathbb{F}_2[X]/(X^N - 1) \colon f(\omega) = 0 \ \forall \omega \in D\}.$$

Говорят, что $\mathcal{X}$ — циклический код с определяющим множеством корней (или нулей) D.

Я бы предпочёл крыльям корни[11], но если у меня нет корней, я должен иметь крылья.

Лео Силард (1898–1964), американский физик, родившийся в Венгрии

2. Двоичный БЧХ-код длины N (при $N = 2^s - 1$) и с проектируемым расстоянием δ — это циклический код с определяющим множеством $\{\omega, \omega^2, \ldots, \omega^{\delta-1}\}$, где $\delta \leqslant N$ и ω — примитивный корень из единицы степени N, т. е. $\omega^N = 1$. Полезно отметить, что если ω — корень многочлена $g(X)$, то его же корнями будут элементы $\omega^2, \omega^4, \ldots, \omega^{2^{s-1}}$. Рассматривая определяющее множество вида $\{\omega, \omega^2, \ldots, \omega^{\delta-1}\}$, мы «заполним пробелы» в приведенной выше последовательности и создадим идеал многочленов, свойства которых можно исследовать аналитически.

Простейший пример получается при $N = 7$ и $D = \{\omega, \omega^2\}$, где ω — корень многочлена $X^3 + X + 1$. Здесь $\omega^7 = (\omega^3)^2\omega = (\omega + 1)^2\omega = \omega^3 + \omega = 1$, так что ω — корень седьмой степени из единицы. На самом деле это примитивный корень. Кроме того, как уже говорилось, ω^2 тоже является корнем многочлена $X^3 + X + 1$: $(\omega^2)^3 + \omega^2 + 1 = (\omega^3 + \omega + 1)^2 = 0$, аналогично ω^4 — тоже его корень. Таким образом, циклический код с определяющим множеством $\{\omega, \omega^2\}$ порождается многочленом $X^3 + X + 1$, поскольку все корни этого многочлена вошли в определяющее множество. Мы знаем, что он совпадает с $[7, 4]$-кодом Хэмминга.

Определителем Вандермонда называется определитель

$$\Delta = \det \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{pmatrix}.$$

Заметим, что если $x_i = x_j$ $(i \neq j)$, то $\Delta = 0$ (две одинаковые строки). Поэтому Δ делится на $x_i - x_j$:

$$\Delta = P(\mathbf{x}) \prod_{i<j} (x_i - x_j),$$

где P — многочлен от $x_1, \ldots, x_n$. Далее рассмотрим члены в выражении Δ как суммы членов вида $a \prod_i x_i^{m(i)}$, где $\sum m(i) = 0 + 1 + \ldots + (n-1) = n(n-1)/2$. Но $\prod_{i<j}(x_i - x_j)$ — сумма членов $a \prod_i x_i^{m(i)}$, где $\sum m(i) = n(n-1)/2$. Значит, $P(\mathbf{x}) = \text{const}$. Рассматривая $x_2 x_3^2 \ldots x_n^{n-1}$, мы заме-

[11] roots-корни.

чаем, что $\mathrm{const} = 1$, т. е.

$$\Delta = \prod_{i<j} (x_i - x_j). \tag{2.6.6}$$

Предположим, что N нечётно и $\mathbb{K}$ — поле, содержащее $\mathbb{F}_2$, в котором $X^N - 1$ раскладывается на линейные множители. (В качестве этого поля можно выбрать $\mathbb{F}_{2^s}$, где $N | 2^s - 1$.) Циклический код, состоящий из таких слов $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{N-1}$, что $\sum\limits_{j=0}^{N-1} \mathbf{c}_j \omega^{rj} = 0$ для всех $r = 1, 2, \ldots, \delta - 1$, где ω — примитивный корень степени N из единицы, называется БЧХ-кодом с проектируемым расстоянием $\delta < N$. Далее, $\mathcal{X}$ — это векторное пространство над $\mathbb{F}_2$, и $\mathbf{c} \in \mathcal{X}$ тогда и только тогда, когда

$$\mathbf{c} H^{\mathrm{T}} = 0, \tag{2.6.7}$$

где

$$H = \begin{pmatrix} 1 & \omega & \omega^2 & \ldots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{\delta-1} & \omega^{2\delta-2} & \ldots & \omega^{(N-1)(\delta-1)} \end{pmatrix}. \tag{2.6.8}$$

Ранг матрицы H равен δ. Действительно, по формуле (2.6.6) для любого минора $\bar{H}$ размера $(\delta - 1) \times (\delta - 1)$ имеем $\det \bar{H} \neq 0$, и этот детерминант имеет вид $\omega^a \prod\limits_{i<j}{}' (\omega^i - \omega^j)$, где все корни различны. Поскольку любые $\delta - 1$ столбцов линейно независимы, минимальное расстояние кода $\mathcal{X}$ не меньше δ:

$$\mathbf{c} \in \mathcal{X}, \ \ \mathbf{c} \neq \mathbf{0} \Rightarrow \sum |c_j| \geqslant \delta. \qquad \square$$

> Верит ли кто-нибудь, что разница между интегралами Лебега и Римана может иметь физический смысл и тот факт, полетит самолет или рухнет, может зависеть от этой разницы? Если бы такие объявились, я бы не хотел лететь на самолётах.
>
> *Ричард Хэмминг* (1915–1998),
> американский математик и программист

Задача 2.6.9. Подмножество $\mathcal{X} \subset \mathcal{H}_N$ пространства Хэмминга мощности $\#\mathcal{X} = M$ и минимальным расстоянием $d = \min[\delta(\mathbf{x}, \mathbf{x}') \colon \mathbf{x}, \mathbf{x}' \in \mathcal{X}, \mathbf{x} \neq \mathbf{x}']$ называется $[N, M, d]$-кодом (не обязательно линейным). $[N, M, d]$-код называется *максимальным*, если он не содержится ни в каком $[N, M + 1, d]$-коде. Докажите, что $[N, M, d]$-код максимален тогда и только тогда, когда для любого $\mathbf{y} \in \{0, 1\}^N$ найдётся такое кодовое

слово $\mathbf{x} \in \mathcal{X}$, что $\delta(\mathbf{x}, \mathbf{y}) < d$. Заключите отсюда, что если в кодовое слово внесены d или более изменений, то новое слово станет ближе к некоторому другому кодовому слову, чем к исходному.

Предположим, что максимальный $[N, M, d]$-код применяется для передачи информации по д. с. к. б. п. с вероятностью ошибки p, а получатель пользуется декодером максимального правдоподобия. Докажите, что вероятность ошибочного декодирования $\pi_{\text{err}}^{\text{ML}}$ подчиняется неравенству:

$$1 - b(N, d-1) \leqslant \pi_{\text{err}}^{\text{ML}} \leqslant 1 - b(N, \lfloor (d-1)/2 \rfloor),$$

где $b(N, m)$ — частичная биномиальная сумма

$$b(N, m) = \sum_{k=0}^{m} C_N^k p^k (1-p)^{N-k}.$$

Решение. Если код максимален, то добавление любого нового слова ведёт к уменьшению расстояния. Следовательно, для любого $\mathbf{y}$ найдётся такое $\mathbf{x} \in \mathcal{X}$, что $\delta(\mathbf{y}, \mathbf{x}) < d$. Обратно, если выполняется это свойство, то код нельзя увеличить, не уменьшив при этом d. Поэтому внеся d или более изменений в кодовое слово, мы получим слово, расположенное ближе к другому кодовому слову. Это, конечно, ведет к ошибке для декодера м. п., поскольку он выбирает ближайшее кодовое слово.

Следовательно,

$$\pi_{\text{err}}^{\text{ML}} \geqslant \sum_{k=d}^{N} C_N^k p^k (1-p)^{N-k} = 1 - b(N, d-1).$$

С другой стороны, код исправляет $\lfloor (d-1)/2 \rfloor$ ошибок. Значит,

$$\pi_{\text{err}}^{\text{ML}} \leqslant 1 - b(N, \lfloor (d-1)/2 \rfloor). \qquad \square$$

Задача 2.6.10. Граница Плоткина для $[N, M, d]$ двоичного кода утверждает, что $M \leqslant \left\lfloor \dfrac{d}{d - N/2} \right\rfloor$, если $d > N/2$. Пусть $M_2^*(N, d)$ обозначает максимальный размер кода длины N и с расстоянием d, и пусть

$$\alpha(\tau) = \lim_{N \to \infty} \frac{1}{N} \log_2 M_2^*(N, \lfloor \tau N \rfloor).$$

Выведите из границы Плоткина, что $\alpha(\tau) = 0$ при $\tau \geqslant 1/2$.

Опираясь на предыдущую границу, покажите, что если $d \leqslant N/2$, то

$$M \leqslant 2^{N-(2d-1)} \frac{d}{d - (2d-1)/2} = 2d2^{N-(2d-1)}.$$

Решение. Если $d > N/2$, то из границы Плоткина непосредственно получаем, что $\alpha(\tau) = 0$. Если $d \leqslant N/2$, то разобьём $\mathcal{X}$ на непересекающиеся подмножества с фиксированными $N - (2d-1)$ последними цифрами. Одно из этих подмножеств $\mathcal{X}'$ должно иметь такое размер M', что $M'2^{N-(2d-1)} \geqslant M$.

Следовательно, $\mathcal{X}'$ — код длины $N' = 2d-1$ и с расстоянием $d' = d$, где $d' > N'/2$. Применяя границу Плоткина к коду $\mathcal{X}'$, получаем, что

$$M' \leqslant \frac{d'}{d' - N/2} = \frac{d}{d - (2d-1)/2} = 2d.$$

Значит,

$$M \leqslant 2^{N-(2d-1)}2d.$$

Взяв $d = \lfloor \tau N \rfloor$ и переходя к пределу при $N \to \infty$, получим, что $\alpha(\tau) \leqslant 1 - 2\tau$ при $0 \leqslant \tau \leqslant 1/2$. □

Задача 2.6.11. Сформулируйте и докажите неравенства Хэмминга, Синглтона и Гильберта—Варшамова. Приведите примеры кода, на котором достигается

а) граница Хэмминга,

б) граница Синглтона.

Решение. Граница Хэмминга для $[N, M]$-кода $\mathcal{X}$, исправляющего E ошибок,

$$M \leqslant \frac{2^N}{v_N(E)}, \quad E = \left\lfloor \frac{d-1}{2} \right\rfloor$$

следует из того, что E-шары с центрами в кодовых словах $\mathbf{x} \in \mathcal{X}$ не должны пересекаться:

$$M \times v_N(E) = \text{число точек, покрытых любым из } M \text{ } E\text{-шаров} \leqslant$$
$$\leqslant 2^N = \text{число всех точек пространства } \{0, 1\}^N.$$

Здесь $v_N(E) = \sum\limits_{i=0}^{E} C_N^i$ — объём E-шара в пространстве Хэмминга $\{0, 1\}^N$. Граница Синглтона

$$M \leqslant 2^{N-d+1}$$

для $[N, M, d]$-кода $\mathcal{X}$ следует из того наблюдения, что при усечении кода $\mathcal{X}$ (т. е. отбрасывании знака у кодовых слов $\mathbf{x} \in \mathcal{X}$) $d-1$ раз кодовые слова не слипаются (т. е. сохраняется M), в то время как код, полученный в результате этой процедуры, вкладывается в пространство $\{0, 1\}^{N-d-1}$.

Неравенство Гильберта—Варшамова утверждает, что максимальный размер $M^* = M_2^*(N, d)$ двоичного $[N, d]$-кода удовлетворяет оценке

$$M^* \geqslant \frac{2^N}{v_N(d-1)}.$$

Это следует из того, что любое слово $\mathbf{y} \in \{0, 1\}^N$ должно лежать на расстоянии не больше $d-1$ от кода максимального размера $\mathcal{X}^*$, так что

$$M^* \times v_N(d-1) \geqslant \text{число точек на расстоянии } d-1 = 2^N.$$

Коды, на которых достигается граница Хэмминга, называются совершенными: это, например, $[2^l - 1, 2^l - 1 - l, 3]$-коды Хэмминга. Здесь $E = 1$, $v_N(1) = 1 + 2^l - 1 = 2^l$ и $M = 2^{2^l - l - 1}$. Кроме этих кодов существует только один пример двоичного совершенного кода: $[23, 12, 7]$-код Голея.

Коды, на которых достигается граница Синглтона, называют кодами с максимальным достижимым расстоянием (м. д. р.): $d = N - k + 1$, и любые $N - k$ строк проверочной матрицы линейно независимы. Приведем примеры двоичных м. д. р.-кодов: а) всё пространство $\{0, 1\}^N$, б) код повторений $\{0 \ldots 0, 1 \ldots 1\}$ и множество всех слов $\mathbf{x} \in \{0, 1\}^N$ чётного веса. Более интересные примеры доставляют так называемые коды Рида—Соломона, они не двоичные. Двоичные коды, на которых достигается граница Гильберта—Варшамова, пока неизвестны (хотя они построены для недвоичных алфавитов). □

Beyond the utmost bound of human thought.

Альфред Теннисон (1809–1892),
английский поэт

Задача 2.6.12. 1. Объясните существование и важность кодов, исправляющих ошибки инженерам компьютеров на примере кода Хэмминга.

2. Сколько кодовых слов в коде Хэмминга веса 1, 2, 3, 4, 5?

Решение. 1. Рассмотрим линейное отображение $\mathbb{F}_2^7 \to \mathbb{F}_2^3$, заданное матрицей H из формулы (2.6.5). Код Хэмминга $\mathcal{X}$ — это его ядро $\operatorname{Ker} H$, т. е. множество таких слов $\mathbf{x} = x_1x_2x_3x_4x_5x_6x_7 \in \{0, 1\}^7$, что $\mathbf{x}H^{\mathrm{T}} = \mathbf{0}$. Можно выбрать 4 знака, например x_4, x_5, x_6, x_7 произвольно из множества $\{0, 1\}$, а остальные выразить через них:

$$\begin{aligned} x_1 &= x_4 + x_5 + x_7, \\ x_2 &= x_4 + x_6 + x_7, \\ x_3 &= x_5 + x_6 + x_7. \end{aligned}$$

Это означает, что код $\mathcal{X}$ можно использовать для кодирования 16 двоичных «сообщений» длины 4. Если $\mathbf{y} = y_1y_2y_3y_4y_5y_6y_7$ отличается от кодового

слова $\mathbf{x} \in \mathcal{X}$ в одном месте, скажем $\mathbf{y} = \mathbf{x} + \mathbf{e}_k$, то уравнение $\mathbf{y}H^{\mathrm{T}} = \mathbf{e}_k H^{\mathrm{T}}$ даёт двоичное разложение числа k, что ведёт к декодированию $\mathbf{x}$. Следовательно, код $\mathcal{X}$ позволяет исправить одну ошибку.

Пусть вероятность ошибки в любом знаке $p \ll 1$ вне зависимости от того, что происходит с другими знаками. Тогда вероятность ошибки при передаче некодированного $4N$-значного сообщения составит

$$1 - (1-p)^{4N} \simeq 4Np.$$

Но, используя код Хэмминга, мы должны передать $7N$ бит. Ошибка происходит при передаче по крайней мере двух неправильных символов. Поэтому вероятность ошибки приближённо равна

$$1 - (1 - C_7^2 p^2)^N \simeq 21Np^2 \ll 4Np.$$

Это обосновывает дополнительные затраты на три проверочных знака в коде Хэмминга.

2. Код Хэмминга $\mathcal{X}_{\mathrm{H},l}$ длины $N = 2^l - 1$ $(l \geqslant 3)$ состоит из таких двоичных слов $\mathbf{x} = x_1 \ldots x_N$, что $\mathbf{x}H^{\mathrm{T}} = 0$, где H — $l \times N$-матрица, столбцы которой $h^{(1)}, \ldots, h^{(N)}$ — все ненулевые двоичные векторы длины l. Значит, число кодовых слов веса $w(\mathbf{x}) = \sum\limits_{j=1}^{N} x_j = s$ равно числу (неупорядоченных) наборов s двоичных ненулевых попарно различных l-векторов с нулевой общей суммой. Действительно, если $\mathbf{x}H^{\mathrm{T}} = 0$, $w(\mathbf{x}) = s$ и $x_{j_1} = x_{j_2} = \ldots = x_{j_s} = 1$, то сумма вектор-строк $h^{(j_1)} + \ldots + h^{(j_s)} = \mathbf{0}$.

Таким образом, есть одно кодовое слово веса 0, нет кодовых слов весов 1 и 2, и существует $N(N-1)/3!$ кодовых слов веса 3 (т. е. 7 и 35 слов веса 3 при $l = 3$ и $l = 4$). Далее, мы имеем $(N(N-1)(N-2) - N(N-1))/4! = N(N-1)(N-3)/4!$ слов веса 4 (т. е. 7 и 105 слов веса 4 при $l = 3$ и $l = 4$). Наконец, у нас есть $N(N-1)(N-3)(N-7)/5!$ слов веса 5 (т. е. 0 и 168 слов веса 5 при $l = 3$ и $l = 4$). Каждый раз при добавлении множителя нам нужно удалить l-вектор, равный линейной комбинации ранее отобранных векторов. В задаче 3.6.9 мы вычислим производящий полином весов для двоичного кода Хэмминга. В частности, при $N = 15$ получаем

$$1 + 35X^3 + 105X^4 + 168X^5 + 280X^6 + 435X^7 + 435X^8 + \\ + 280X^9 + 168X^{10} + 105X^{11} + 35X^{12} + X^{15}. \quad \square$$

Задача 2.6.13. 1. Что означает фраза: $\mathcal{X} \subseteq \mathcal{H}_N$ — линейный $[N, k]$-код с образующей матрицей G и проверочной матрицей H? Покажите, что

$$\mathcal{X}^{\perp} = \{\mathbf{x} \in \mathcal{H}_N \colon \langle \mathbf{x} \cdot \mathbf{y} \rangle = 0 \ \forall \mathbf{y} \in \mathcal{X}\}$$

является линейным $[N, N-k]$-кодом, и найдите его образующую и проверочную матрицы.

2. Линейный код называется самоортогональным, если $\mathcal{X} \subseteq \mathcal{X}^{\perp}$. Докажите, что код $\mathcal{X}$ самоортогонален, если строки матрицы G ортогональны себе и друг другу. Линейный код называется самодвойственным, если $\mathcal{X} = \mathcal{X}^{\perp}$. Докажите, что самодвойственный код должен быть $[N, N/2]$-кодом (и, следовательно, N должно быть чётным). В обратную сторону, докажите, что самоортогональный $[N, N/2]$-код при чётном N является и самодвойственным. Приведите пример такого кода для любого чётного N и докажите, что самодвойственный код всегда содержит слово $1 \ldots 1$.

3. Рассмотрим $[2^l - 1, 2^l - l - 1]$-код Хэмминга $\mathcal{X}_{\mathrm{H},l}$. Опишите образующую матрицу кода $\mathcal{X}_{\mathrm{H},l}^{\perp}$. Докажите, что расстояние между любыми двумя кодовыми словами в $\mathcal{X}_{\mathrm{H},l}^{\perp}$ равно 2^{l-1}.

Решение. По определению код $\mathcal{X}^{\perp}$ получается в результате линейных операций и поэтому линеен. Как следует из линейной алгебры, $\dim \mathcal{X}^{\perp} = N - k$. Образующая матрица $G^{\perp}$ кода $\mathcal{X}^{\perp}$ совпадает с H, а проверочная матрица $H^{\perp}$ — с G.

Если $\mathcal{X} \subseteq \mathcal{X}^{\perp}$, то строки $\mathbf{g}^{(1)}, \ldots \mathbf{g}^{(k)}$ матрицы G взаимно и попарно ортогональны. Верно и обратное утверждение. Из предыдущего замечания следует, что ранг самодвойственного кода $k = N - k$, т. е. $k = N/2$ и N должно быть чётным. Аналогично если $\mathcal{X}$ — самоортогональный код и $k = N/2$, то $\mathcal{X}$ — самодвойственный код.

Пусть $\mathbf{1} = 1 \ldots 1$. Если $\mathcal{X} = \mathcal{X}^{\perp}$, то $\mathbf{1} \cdot \mathbf{g}^{(i)} = \mathbf{g}^{(i)} \cdot \mathbf{g}^{(i)} = 0$. Поэтому $\mathbf{1} \in \mathcal{X}$. Примером может служить код с образующей матрицей

$$G = \left.\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 & \ldots & 1 \\ 1 & 1 & 0 & \ldots & 0 & 1 & \ldots & 0 \\ 1 & 0 & 1 & \ldots & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \ldots & 1 & 1 & \ldots & 1 \end{pmatrix}\right\} N/2 \;.$$
$$\begin{matrix} \leftarrow & N/2 & \rightarrow & \leftarrow N/2 \rightarrow \end{matrix}$$

Код $\mathcal{X}_{\mathrm{H}}^{\perp}$, двойственный к коду Хэмминга $\mathcal{X}_{\mathrm{H}}$ называется симплексным кодом. По предыдущему его длина равна $2^l - 1$, а ранг равен l, размер его образующей матрицы равен $l \times (2^l - 1)$, а её столбцы представляют собой список всех ненулевых векторов длины l. Для проверки того, что расстояние кода $\mathcal{X}_{\mathrm{H}}^{\perp}$ равно 2^{l-1}, достаточно установить, что вес ненулевого слова $\mathbf{x} \in \mathcal{X}_{\mathrm{H}}^{\perp}$ равен 2^{l-1}. Но ненулевое слово $\mathbf{x} \in \mathcal{X}_{\mathrm{H}}^{\perp}$ — это ненулевая линейная комбинация строк матрицы $G_{\mathrm{H}}^{\perp}$. Пусть $J \subset \{1, \ldots, l\}$ — множество суммируемых строк и $\mathbf{x} = \sum\limits_{i \in J} \mathbf{g}^{(i)}$. Ясно, что $w(\mathbf{g}^{(i)}) = 2^{l-1}$, поскольку ровно половина всех 2^l векторов имеют 1 на любых заданных местах. Доказательство завершается индукцией по $\#J$.

Простой и элегантный способ состоит в применении тождества Мак-Вильямс (см. теорему 3.4.4), из которого немедленно следует, что

$$W_{\mathcal{X}^\perp}(s) = 1 + (2^l - 1)s^{2^{l-1}}. \tag{2.6.9}$$

Поучительно познакомиться с этим выводом. В задаче 3.6.9 мы выведем формулу для производящего полинома весов кода Хэмминга. Подставив это выражение в тождество Мак-Вильямс, получим

$$W_{\mathcal{X}^\perp}(s) = \frac{1}{2^{N-l}}\left[\frac{1}{N+1}\left(1+\frac{1-s}{1+s}\right)^N + \right.$$
$$\left. + \frac{N}{N+1}\left(1+\frac{1-s}{1+s}\right)^{(N-1)/2}\left(1-\frac{1-s}{1+s}\right)^{(N+1)/2}\right](1+s)^N =$$
$$= 2^l\left(\frac{1}{2^l} + \frac{2^l-1}{2^l}s^{2^{l-1}}\right),$$

что эквивалентно равенству (2.6.9). □

Задача 2.6.14. Опишите процедуру декодирования $[2^l - 1, 2^l - l - 1]$-кода Хэмминга.

Кодовые слова [7, 4]-кода Хэмминга с лексикографически упорядоченной проверочной матрицей H из формулы (2.3.3) используется для кодирования 16 символов, первых 15 букв и символа пробела $*$. Применяется следующее правило кодирования:

A	0011001	E	0111100	I	1010101	M	1111111
B	0100101	F	0001111	J	1100110	N	1000011
C	0010110	G	1101001	K	0101010	O	0000000
D	1110000	H	0110001	L	1001100	*	1011010

Вы получили 105-значное сообщение

1000110 0000000 0110001 1000011 1000011 1110101
0111100 0011010 0100101 0111100 1011000 1101001
0000000 0010000 1010000

в котором некоторые слова имеют ошибки. Декодируйте полученное сообщение

Решение. Заметим, что $[2^l - 1, 2^l - 1 - l]$-код Хэмминга, $l = 2, 3, \ldots$, получается как набор таких двоичных строк $\mathbf{x} = x_1 \ldots x_N$ длины $N = 2^l - 1$, что $\mathbf{x}H^{\mathrm{T}} = \mathbf{0}$. Матрица H — это $l \times (2^l - 1)$-матрица, столбцы которой — ненулевые двоичные строки, упорядоченные лексикографически. Матрицы, полученные из этой перестановками строк, задают другие, но эквивалентные коды: все они называются кодами Хэмминга.

Для декодирования следует зафиксировать проверочную матрицу H и считать её известной как отправителю, так и получателю. Получив слово (строку) $\mathbf{y} = y_1 \dots y_N$, строим синдром $\mathbf{y}H^{\mathrm{T}}$. Если $\mathbf{y}H^{\mathrm{T}} = 0$, то декодируем $\mathbf{y}$ им самим. (У нас нет средств для выяснения, было ли оригинальное кодовое слово повреждено в канале или нет.)

Если $\mathbf{y}H^{\mathrm{T}} \neq 0$, то $\mathbf{y}H^{\mathrm{T}}$ совпадает со столбцом матрицы H, например, j-м. Тогда декодируем $\mathbf{y}$ как

$$\mathbf{x}^* = \mathbf{y} + \mathbf{e}_j, \text{ где } \mathbf{e}_j = 0 \dots 1 \dots 0 \text{ (1 на } j\text{-м месте)}.$$

Иначе говоря, меняем j-й знак у $\mathbf{y}$ и решаем, что полученное слово было передано по каналу. Этот метод хорошо работает, если ошибки в канале встречаются редко.

Если $l = 3$, то $[7, 4]$-код Хэмминга содержит $2^4 = 16$ кодовых слов. Эти слова фиксированы при заданной матрице H: в примере они используются для кодирования 15 букв от A до O и символа пробела $*$. Получив сообщение, разбиваем его на слова длины 7: в примере есть всего 15 таких слов. Осуществив процедуру декодирования, получим

JOHNNIE*BE*GOOD □

Задача 2.6.15. Найдите ранг двоичного кода Хэмминга длины $N = 2^l - 1$, где $l \geqslant 2$, и число его кодовых слов. Вычислите минимальное расстояние этого кода и докажите, что он исправляет одну ошибку. Докажите, что код совершенный (т. е. объединение 1-шаров с центрами в кодовых словах покрывает пространство всех слов).

Выпишите проверочную и образующую матрицы кода Хэмминга с $l = 3$. Что можно сказать о скорости передачи информации такого кода? Почему случай $l = 2$ не представляет интереса?

Решение. Проверочная матрица H кода Хэмминга имеет размер $l \times (2^l - 1)$ и образована всеми ненулевыми столбцами длины l, значит, в матрице H есть l линейно независимых столбцов. Так как $\mathcal{X}_{\mathrm{Ham}} = \ker H$, мы получаем, что $\dim \mathcal{X} = 2^l - 1 - l = \operatorname{rank} \mathcal{X}$. Тем самым, число кодовых слов равно $2^{2^l - l - 1}$.

Поскольку все столбцы матрицы H различны, любая пара её столбцов линейно независима. Следовательно минимальное расстояние кода $\mathcal{X}$ больше 2. Но H имеет три линейно зависимых столбца, например,

$$100 \dots 0^{\mathrm{T}}, \quad 010 \dots 0^{\mathrm{T}} \text{ и } 110 \dots 0^{\mathrm{T}},$$

т. е. минимальное расстояние равно 3. Значит, если возникает одна ошибка, то полученное слово будет отстоять от кодового на расстоянии 1 и исходное кодовое слово однозначно определится. Таким образом, код Хэмминга

исправляет одну ошибку. Покажем, что код совершенен, т. е.

$$\text{число кодовых слов} \times \text{объём 1-шара} = \text{общее число слов}.$$

Обозначив $2^l - 1 = N$, получим

$$\begin{aligned}
&\text{число кодовых слов} = 2^{2^l-1-l} = 2^{N-l},\\
&\text{объём 1-шара} = C_N^0 + C_N^1 = 1 + N,\\
&\text{общее число слов} = 2^N
\end{aligned}$$

и

$$(1+N)2^{N-l} = 2^l 2^{N-l} = 2^N.$$

Скорость передачи информации кода равна

$$\text{ранг}/\text{длина} = \frac{2^l - l - 1}{2^l - 1}.$$

Код с $l = 3$ обладает проверочной матрицей размера 3×7 вида (2.6.5), любая перестановка строк ведёт к эквивалентному коду. Размер образующей матрицы равен 4×7, скорость передачи информации равна $4/7$. Код Хэмминга при $l = 2$ тривиален: он содержит единственное ненулевое слово 1 1 1. □

Задача 2.6.16. Определите БЧХ-код длины N над полем $\mathbb{F}_q$ с проектируемым расстоянием δ. Покажите, что минимальный вес в таком коде по крайней мере δ.

Рассмотрим БЧХ-код длины 31 над полем $\mathbb{F}_2$ с проектируемым расстоянием 8. Покажите, что его минимальное расстояние не меньше 11.

Решение. БЧХ-код длины N над полем $\mathbb{F}_q$ определяется как циклический код $\mathcal{X}$, образующий многочлен $g(X) \in \mathbb{F}_q[X]$ которого имеет минимальную степень (причём $g(X)|(1+X^N)$ и поэтому $\deg g(X) \leqslant N$) содержит среди своих корней последовательность степеней $\omega, \omega^2, \ldots, \omega^{\delta-1}$. Здесь $\omega \in \mathbb{F}_{q^s}$ — примитивный корень из единицы степени N (ω лежит в расширении $\mathbb{F}_{q^s}$ исходного поля — поля разложения многочлена $X^N + 1$ над $\mathbb{F}_q$, в частности, $N|(q^s - 1)$). При этом δ называют проектируемым расстоянием кода $\mathcal{X}$: истинное расстояние (которое в общей ситуации может оказаться трудно вычислимым) может быть больше δ.

Если рассмотреть двоичный БЧХ-код $\mathcal{X}$ длины 31, то ω будет примитивным корнем из единицы степени 31, в частности, $\omega^{31} = 1$ (ω лежит в расширении поля $\mathbb{F}_{32}$). Мы знаем, что если многочлен $f(X) \in \mathbb{F}_2[X]$ порядка s обращается в нуль на элементе ω, то его корнями будут также его степени $\omega^2, \omega^4, \ldots, \omega^{2^{s-1}}$, т. е.

$$(X - \omega^{2^r})|f(X), \quad r = 0, \ldots, s-1.$$

Поэтому если образующая $g(X)$ имеет своими корнями ω, ω^2, ω^3, ω^4, ω^5, ω^6, ω^7, то его же корнями будут

$$\omega^8 = (\omega^4)^2, \quad \omega^9 = (\omega^5)^8 \text{ и } \omega^{10} = (\omega^5)^2.$$

Иными словами, определяющее множество можно расширить до

$$\omega,\ \omega^2,\ \omega^3,\ \omega^4,\ \omega^5,\ \omega^6,\ \omega^7,\ \omega^8,\ \omega^9,\ \omega^{10}$$

(все перечисленные элементы различны, поскольку ω — примитивный корень из единицы степени 31). Таким образом, проектируемое расстояние кода $\mathcal{X}$ не меньше чем 11. Значит и минимальное расстояние этого кода не меньше 11. □

Задача 2.6.17. Пусть $\mathcal{X}$ — линейный $[N, k, d]$-код над двоичным полем $\mathbb{F}_2$ и G — его порождающая матрица с k строками и N столбцами, в которой ровно d позиций в первой строке заняты единицами. Пусть G_1 — матрица с $k-1$ строками и $N-d$ столбцами, полученная из G удалением первой строки и столбцов с ненулевыми элементами в первой строке. Покажите, что линейный код $\mathcal{X}_1$, порождённый G_1, имеет расстояние $d' \geqslant \lceil d/2 \rceil$.

Покажите также, что ранг кода $\mathcal{X}_1$ равен $k-1$, и выведите, что

$$N \geqslant \sum_{i=0}^{k-1} \lceil d/2^i \rceil.$$

Решение. Пусть $\mathbf{x}$ — кодовое слово в $\mathcal{X}$, представленное первой строкой матрицы G. Возьмём пару других строк, скажем $\mathbf{y}$ и $\mathbf{z}$. После первого удаления они превратятся в $\mathbf{y}'$ и $\mathbf{z}'$ соответственно. Оба веса $w(\mathbf{y}')$ и $w(\mathbf{z}')$ должны быть больше чем $\lceil d/2 \rceil$: в противном случае по крайней мере у одного из исходных слов, $\mathbf{y}$ или $\mathbf{z}$, скажем у $\mathbf{y}$, должно было быть не меньше $\lceil d/2 \rceil$ единиц среди удалённых d знаков (так как по условию $w(\mathbf{y}) \geqslant d$). Но тогда

$$w(\mathbf{x}+\mathbf{y}) = w(\mathbf{y}') + d - \lceil d/2 \rceil < d,$$

что противоречит предположению о том, что расстояние кода $\mathcal{X}$ равно d.

Мы хотим проверить, что $w(\mathbf{y}'+\mathbf{z}') \geqslant \lceil d/2 \rceil$. Предположим противное:

$$w(\mathbf{y}'+\mathbf{z}') < \lceil d/2 \rceil.$$

Тогда $m' = w(\mathbf{y}^0 + \mathbf{z}^0)$ должно быть не менее $d - m \geqslant \lceil d/2 \rceil$, где $\mathbf{y}^0$ — удалённая часть слова $\mathbf{y}$ длины d, а $\mathbf{z}^0$ — удалённая часть слова $\mathbf{z}$ той же длины d. Действительно, если, как и раньше, $m' < d - m$, то $w(\mathbf{y}+\mathbf{z}) < d$, что невозможно. Но если $m' \geqslant d - m$, то

$$w(\mathbf{x}+\mathbf{y}+\mathbf{z}) = d - m' + m < d,$$

а это тоже невозможно. Итак, вес суммы любых двух строк матрицы G_1 не меньше чем $\lceil d/2\rceil$.

Это рассуждение можно повторить с суммой любого числа строк G_1 (не превышающего $k-1$). Действительно, в случае такой суммы $\mathbf{x}+\mathbf{y}+\ldots+\mathbf{z}$ мы можем перейти к матрицам меньшего размера $\tilde{G}$ и $\tilde{G}_1$, которые будут иметь такую же сумму строк. Мы заключаем, что расстояние d' кода $\mathcal{X}_1$ не меньше чем $\lceil d/2\rceil$. Ранг кода $\mathcal{X}_1$ равен $k-1$, любые $k-1$ строки матрицы G_1 линейно независимы. (Предыдущая сумма не могла быть нулевой.)

Далее, процесс удаления можно применить к коду $\mathcal{X}_1$ (удалить d' столбцов из G_1 устраняя цифру 1 в строке G_1, в которой ровно d' единиц). И так далее, пока вы не исчерпаете начальный ранг k, снизив его на 1. Это приводит к нужному неравенству

$$N \geqslant d + \lceil d/2\rceil + \lceil d/2^2\rceil + \ldots + \lceil d/2^{k-1}\rceil. \qquad \square$$

Задача 2.6.18. Дайте определение линейного циклического кода $\mathcal{X}$ и покажите, что в нём есть единственное кодовое слово минимальной длины. Многочлен $g(X)$, коэффициенты которого суть символы этого слова (минимальной степени), является образующим многочленом этого кода. Докажите, что все слова этого кода однозначно определяются по $g(X)$.

Приведите необходимое и достаточное условие на полином $g(X)$, для того чтобы он был образующим некоторого циклического кода длины N.

Есть по крайней мере три способа задания проверочной матрицы кода через образующий многочлен. Объясните один из них.

Решение. Пусть $\mathcal{X}$ — циклический код длины N с образующей $g(X)=\sum\limits_{i=0}^{d} g_i X^i$ степени d. Не ограничивая общности, предположим, что код не тривиален и $1<d<N-1$. Пусть $\mathbf{g}$ — соответствующее кодовое слово $g_0\ldots g_d 0\ldots 0$ ($d+1$ коэффициентов многочлена дополняются $N-d-1$ нулями). Тогда а) $g(X)|(1+X^N)$, т. е. $g(X)h(X)=1+X^N$ для некоторого многочлена $h(X)=\sum\limits_{i=0}^{k} h_i X^i$ степени $k=N-d$, б) строка $\mathbf{a}=a_0\ldots a_{N-1}\in\mathcal{X}$ тогда и только тогда, когда многочлен $a(X)=\sum\limits_{i=0}^{N-1} a_i X^i$ представим в виде $a(X)=f(X)g(X) \bmod (1+X^N)$, и в) строка $\mathbf{g}$ и её циклические сдвиги $\pi\mathbf{g}$, $\pi^2\mathbf{g}$, …, $\pi^{k-1}\mathbf{g}$ (соответствующие многочленам $g(X)$, $Xg(X)$, …, $X^{k-1}g(X)$) образуют базис $\mathcal{X}$. Благодаря п. а) имеем $g_0=h_0=1$, и сумма, представляющая l-й коэффициент произведения $g(X)h(X)$, $\sum\limits_{i=0}^{l} g_i h_{l-i}=0$ для всех $l=1,\ldots,N-1$. Ввиду п. в) ранг кода $\mathcal{X}$ равен k.

Один из способов построения проверочной матрицы заключается в том, чтобы взять отношение $(1+X^N)/\langle g(X)\rangle = h(X) = h_0 + h_1 X + \ldots + h_k X^k$ и сформировать $N \times (N-k)$-матрицу

$$H = \begin{pmatrix} h_k & h_{k-1} & \ldots & 0 & \ldots & 0 & 0 \\ 0 & h_k & h_{k-1} & \ldots & h_1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & h_k & \ldots & h_1 & h_0 \end{pmatrix}. \tag{2.6.10}$$

Строки матрицы H — это циклические сдвиги $(\pi^j \mathbf{h}^{\downarrow})$, $0 \leqslant j \leqslant d-1 = N-k-1$ строки $\mathbf{h}^{\downarrow} = h_k \ldots h_0 0 \ldots 0$.

Проверим, что $\mathbf{a}H^{\mathrm{T}} = 0$ $\forall \mathbf{a} \in \mathcal{X}$. Действительно, достаточно показать, что для базисных слов $\pi^j \mathbf{g}$ выполняется равенство $\pi^j \mathbf{g} H^{\mathrm{T}} = 0$, $j = 0, \ldots, k-1$, т. е.

$$\langle \pi^{j_1} \mathbf{g} \cdot \pi^{j_2} \mathbf{h}^{\downarrow} \rangle = 0, \quad 0 \leqslant j_1 < k, \quad 0 \leqslant j_2 < N-k-1. \tag{2.6.11}$$

Но при $j_1 = k-1$ и $j_2 = 0$ получаем

$$\langle \pi^{k-1} \mathbf{g} \cdot \mathbf{h}^{\downarrow} \rangle = g_0 h_k + g_1 h_{k-1} = 0,$$

так как это первый коэффициент (при члене X) в произведении $g(X)h(X) = 1 + X^N$. Аналогично при $j_1 = k-2$ и $j_2 = 0$, скалярное произведение $\langle \pi^{k-2} \mathbf{g} \cdot \mathbf{h}^{\downarrow} \rangle$ даёт второй коэффициент произведения $g(X)h(X)$ (при члене X^2) и тоже равно 0. И так далее: при $j_1 = j_2 = 0$ получаем $\langle \mathbf{g} \cdot \mathbf{h}^{\downarrow} \rangle = 0$ как коэффициент при k-й степени произведения $g(X)h(X)$.

Продолжая, мы видим, что $\langle \mathbf{g} \cdot \pi \mathbf{h}^{\downarrow} \rangle$ совпадает с коэффициентом при $(k+1)$-й степени произведения $g(X)h(X)$, $\langle \mathbf{g} \cdot \pi^2 \mathbf{h}^{\downarrow} \rangle$ — с $(k+2)$-м и т. д., а $\langle \mathbf{g} \cdot \pi^{N-k-1} \mathbf{h}^{\downarrow} \rangle = g_{d-1} h_k + g_d h_{k-1}$ — коэффициент при $(N-1)$-й степени. Как и выше, все они нулевые.

То же самое будет верно, если одновременно сдвинуть циклически оба слова (когда возможно), что приводит к формуле (2.6.11).

В обратную сторону: пусть $\mathbf{a}H^{\mathrm{T}} = 0$ для некоторого слова $\mathbf{a} = a_0 \ldots, a_{N-1}$. Запишем соответствующий многочлен $a(X)$ как $a(X) = f(X)g(X) + r(X)$, где $f(X) = \sum\limits_{i=0}^{k-1} f_i X^i$ и $r(X)$ — остаток. Тогда либо $r(X) = 0$, либо $1 \leqslant \deg r(X) = d' < d$ (и $r_{d'} = 1$, $r_l = 0$ при $d' < l \leqslant N-1$). Положим $\mathbf{r} = r_0 \ldots r_{d'}$.

Предположим, что $r(X) \neq 0$. Как следует из предыдущих рассуждений, 1) $\mathbf{a}H^{\mathrm{T}} = \mathbf{r}H^{\mathrm{T}}$ и, следовательно, $\mathbf{r}H^{\mathrm{T}} = 0$, 2) элементы вектора $\mathbf{r}H^{\mathrm{T}}$ совпадают с коэффициентами произведения $r(X)h(X)$, начиная с $r_0 h_k + \ldots + r_{d'} h_{k-d}$ и заканчивая $r_{d'} h_k$. Значит, эти коэффициенты равны 0. Но равенство $r_{d'} h_k = 0$ невозможно, поскольку $r_{d'} = h_k = 1$, откуда

$r(X) = 0$ и $a(X) = f(X)g(X)$, т. е. $\mathbf{a} \in \mathcal{X}$. Отсюда вывод: H — проверочная матрица кода $\mathcal{X}$.

Эквивалентно матрицу H можно описать, сказав, что она сформирована словами, соответствующими многочленам $X^i h^{\downarrow}(X)$, где $h^{\downarrow}(X)$ определяется как

$$h^{\downarrow}(X) = \sum_{i=1}^{k-1} h_i X^{k-i}.$$

В заключение, пусть $h(X)$ — проверочный многочлен циклического кода $\mathcal{X}$ длины N с образующей $g(X)$, т. е. $g(X)h(X) = 1 + X^N$. Тогда 1) $\mathcal{X} = \{f(X)\colon f(X)h(X) = 0 \bmod (1 + X^N)\}$; 2) если $h(X) = h_0 + h_1 X + \ldots + h_{N-r}X^{N-r}$, то проверочная матрица H кода $\mathcal{X}$ имеет вид (2.6.10); 3) двойственный код $\mathcal{X}^{\perp}$ является циклическим кодом ранга r, порождённым многочленом $h^{\perp}(X)$: $\mathcal{X}^{\perp} = \langle h^{\perp}(X)\rangle$, где $h^{\perp}(X) = h_0^{-1}X^{N-r}h(X^{-1}) = h_0^{-1}(h_0 X^{n-r} + h_1 X^{N-r-1} + \ldots + h_{N-r})$. □

Задача 2.6.19. Рассмотрим проверочную матрицу H $[2^l - 1, 2^l - l - 1]$ двоичного кода Хэмминга. Построим проверочную матрицу H^* $[2^l, 2^l - l - 1]$-кода, дополнив H столбцом нулей, а затем строкой из единиц. Двойственный к полученному коду называется кодом Рида—Маллера первого порядка. Покажите, что код Рида—Маллера первого порядка исправляет ошибки до $2^{l-2} - 1$ бит на кодовое слово.

Такой код с $l = 5$ был использован для фотографий Марса, сделанных в 1972 г. с космической станции «Маринер». Что можно сказать о скорости кодирования? Почему она была гораздо меньше, чем пропускная способность канала?

Решение. Код, использованный НАСА, — это $[2^l, l + 1, 2^{l-1}]$-код с $l = 5$. Его скорость передачи информации равна $6/32 \approx 1/5$. Проверим, что все кодовые слова, за исключением $\mathbf{0}$ и $\mathbf{1}$, имеют вес 2^{l-1}. При $l \geqslant 1$ код $\mathrm{PM}(l)$ определяется рекуррентно

$$\mathrm{PM}(l+1) = \{\mathbf{xx}|\ \mathbf{x} \in \mathrm{PM}(l)\} \vee \{\mathbf{x}, \mathbf{x} + \mathbf{1}|\ \mathbf{x} \in \mathrm{PM}(l)\}.$$

Таким образом, очевидно, что длина кодовых слов кода $\mathrm{PM}(l + 1)$ равна 2^{l+1}. Поскольку множества $\{\mathbf{xx}|\ \mathbf{x} \in \mathrm{PM}(l)\}$ и $\{\mathbf{x}, \mathbf{x} + \mathbf{1}|\ \mathbf{x} \in \mathrm{PM}(l)\}$ не пересекаются, число слов удваивается, т. е. $\#\mathrm{PM}(l + 1) = 2^{l+2}$. Наконец, предполагая, что вес всех кодовых слов кода $\mathrm{PM}(l)$, кроме $\mathbf{0}$ и $\mathbf{1}$, равен 2^{l-1}, рассмотрим кодовое слово $\mathbf{y} \in \mathrm{PM}(l + 1)$. Если $\mathbf{y} = \mathbf{xx}$ отлично от $\mathbf{0}$ и $\mathbf{1}$, то $\mathbf{x} \neq \mathbf{0}$ и $\mathbf{x} \neq \mathbf{1}$ и поэтому $w(\mathbf{y}) = 2w(\mathbf{x}) = 2 \times 2^{l-1} = 2^l$.

Если $\mathbf{y} = (\mathbf{x}, \mathbf{x} + \mathbf{1})$, нужно рассмотреть несколько случаев. Если $\mathbf{x} = \mathbf{0}$, то $\mathbf{y} = \mathbf{01}$ и $w(\mathbf{y}) = 2^l$. Если $\mathbf{x} = \mathbf{1}$, то вес слова $\mathbf{y} = \mathbf{10}$ тоже равен 2^l. Наконец, если $\mathbf{x} \neq \mathbf{0}$ и $\mathbf{x} \neq \mathbf{1}$, то $w(\mathbf{x} + \mathbf{1}) = 2^l - 2^{l-1} = 2^{l-1}$ и $w(\mathbf{y}) =$

$= 2 \times 2^{l-1} = 2^l$. Теперь ясно, что кодовые слова $\mathbf{xx}$ и $(\mathbf{x}, \mathbf{x}+\mathbf{1})$, для которых $w(\mathbf{x}) = 2^{l-1}$ ортогональны строкам проверочной матрицы H^*.

Поскольку $d = 2^4$, ошибочными могут быть до 7 битов. Таким образом, вероятность ошибочной передачи p_{e} для двоичного симметричного канала без памяти (д. с. к. б. п.) с вероятностью ошибки p подчиняется неравенству

$$p_{\mathrm{e}} \leqslant \sum_{i=8}^{32} C_{32}^i p^i (1-p)^{32-i},$$

что мало при малом p. (В качестве оценки приемлемого p можно взять решение уравнения $1 - \eta(p) = 26/32$.) Если длина блока фиксирована (и довольно мала) и $p \ll 1$, то мы не можем приблизиться к пропускной способности.

Действительно, при $l = 5$ рассматриваемый $[32, 6, 16]$-код будет обнаруживать 15 и исправлять 7 ошибок, т. е. код может исправить более $1/5$ от всех 32 знаков. Его скорость передачи информации достигает $6/32$, и если пропускная способность д. с. к. б. п. равна $C = 1 - \eta(p)$ (где p — вероятность ошибки в одном знаке), то для надёжной передачи должно выполняться ограничение $\eta(p) + 6/32 < 1$. Это даёт неравенство $|p - 1/2| > |p^* - 1/2|$, где $p^* \in (0, 1)$ удовлетворяет соотношению $26/32 = \eta(p^*)$. Заведомо подойдут все $p \in [0, 1/5] \cup [4/5, 1]$. В действительности вероятность ошибки была гораздо меньше. □

... a new channel, fair and evently.

Вильям Шекспир (1564–1616), английский драматург и поэт; «Генрих IV», часть I

Задача 2.6.20. Докажите, что для любого двоичного $[5, M, 3]$-кода должно выполняться условие $M \leqslant 4$. Проверьте, что с точностью до эквивалентности существует единственный $[5, 4, 3]$-код.

Решение. По границе Плоткина (2.1.21) если d нечётно и $2d + 1 > N$, то

$$M_2^*(N, d) \leqslant 2\left\lfloor \frac{d+1}{2d+1-N} \right\rfloor.$$

В частности, $M_2^*(5, 3) \leqslant 2\left\lfloor \dfrac{4}{6+1-5} \right\rfloor = 4$. Все $[5, 4, 3]$-коды эквивалентны коду 00000, 00111, 11001, 11110. □

Задача 2.6.21. Пусть $\mathcal{X}$ — двоичный линейный $[N, k, d]$-код с образующей матрицей G. Образующую матрицу G линейного $[N, k, d]$-кода можно выбрать так, что первая её строка имеет вид $1 \ldots 10 \ldots 0$ с d единицами. Запишем

$$G = \begin{pmatrix} 1 \ldots 1 & 0 \ldots 0 \\ G_1 & G_2 \end{pmatrix}.$$

Покажите, что минимальное расстояние d_2 кода с образующей матрицей G_2 удовлетворяет неравенству $d_2 \geqslant d/2$.

Решение. Пусть $\mathcal{X}$ — $[N, k, d]$-код. Всегда можем построить образующую матрицу G этого кода так, что её первая строка будет кодовым словом $\mathbf{x}$ веса $w(\mathbf{x}) = d$. За счёт перестановки столбцов можно считать, что первая строка матрицы G выглядит как $\underbrace{1\ldots1}_{d}\underbrace{0\ldots0}_{N-d}$. Поэтому, с точностью до эквивалентности,

$$G = \begin{pmatrix} 1\ldots1 & 0\ldots0 \\ G_1 & G_2 \end{pmatrix}.$$

Допустим, что $d(G_2) < d/2$, тогда существует строка матрицы $(G_1 G_2)$, в которой число единиц на позициях с номерами $d+1, \ldots, N$ меньше чем $d/2$. В этом случае число единиц на позициях $1, \ldots, d$ окажется больше чем $d/2$, поскольку вес строки не меньше d. Значит, сумма этой строки со словом $1\ldots10\ldots0$ даст кодовое слово веса меньше чем d. Следовательно, $d(G_2) \geqslant d/2$. □

Задача 2.6.22 (ослабленная граница Гильберта—Варшамова). Докажите, что существует p-ичный линейный $[N, k, d]$-код, если $p^k < p^N/v_{N-1}(d-2)$. Поэтому если p^k — наибольшая степень p, удовлетворяющая этому неравенству, то $M_p^*(N, d) \geqslant p^k$.

Решение. Построим проверочную матрицу, выбрав N столбцов длины $N-k$ так, чтобы $d-1$ из них были линейно независимы. Первым столбцом может быть любая ненулевая строка из $\mathbb{Z}_p^{N-k}$. На i-м шаге $(i > 1)$ мы должны выбрать столбец, линейно независимый от любых $d-2$ (или меньше) ранее выбранных столбцов. Число линейных комбинаций ранее выбранных столбцов (с ненулевыми коэффициентами) равно

$$S_i = \sum_{j=1}^{d-2} C_{i-1}^j (p-1)^j,$$

так что проверочную матрицу можно построить тогда и только тогда, когда $S_N + 1 < p^{N-k}$. Наконец заметим, что $S_N + 1 = v_{N-1}(d-2)$. Например, $[5, 2^k, 3]$-код существует, если $2^k < 32/5$, т. е. $k = 2$ и $M_2^*(5, 3) \geqslant 4$, и такой код на самом деле легко построить. □

Задача 2.6.23. Элемент $b \in \mathbb{F}_q^*$ называется примитивным, если его порядок (наименьшее такое натуральное число k, что $b^k = 1 \bmod q$) равен $q-1$. Несложно явно найти примитивный элемент в мультипликативной группе $\mathbb{F}_q^*$. Рассмотрим разложение на простые множители

$$q - 1 = \prod_{j=1}^{s} p_j^{\nu_j}.$$

Для любого $j = 1, \ldots, s$ выберем такое $a_j \in \mathbb{F}_q$, что $a_j^{(q-1)/p_j} \neq 1$. Положим $b_j = a_j^{(q-1)/p_j^{\nu_j}}$. Проверьте, что порядок произведения $b = \prod_{j=1}^{s} b_j$ равен $q-1$.

Решение. Действительно, порядок элементов b_j равен $p_j^{\nu_j}$. Далее, если $b^n = 1$ при некотором n, то $n = 0 \bmod p_j^{\nu_j}$, так как из равенства $b^{n\prod\limits_{i\neq j} p_i^{\nu_i}} = 1$ следует, что $b_j^{n\prod\limits_{i\neq j} p_i^{\nu_i}} = 1$, т. е. $n\prod\limits_{i\neq j} p_i^{\nu_i} = 0 \bmod p_j^{\nu_j}$. Поскольку p_j — различные простые числа, получаем, что $n = 0 \bmod p_j^{\nu_j}$ при любом j. Значит, $n = \prod\limits_{j=1}^{s} p_j^{\nu_j}$. □

Задача 2.6.24. Минимальный многочлен с примитивным корнем называется *примитивным многочленом* Проверьте, что среди неприводимых двоичных многочленов степени 4 (см. формулу (2.5.9)) многочлены $1 + X + X^4$ и $1 + X^3 + X^4$ примитивные, а $1 + X + X^2 + X^3 + X^4$ к ним не принадлежит. Проверьте, что шесть неприводимых многочленов двоичных многочленов степени 5 (см. пример 3.1.37) примитивны; на практике предпочитают работать с многочленом $1 + X^2 + X^5$, так как вычисления по модулю этого многочлена относительно короткие. Выпишите девять неприводимых двоичных многочленов степени 6 и проверьте, что среди них есть шесть примитивных, которые выписаны в первых трёх строчках. Докажите, что существуют примитивные многочлены любой степени.

Решение. В силу теоремы 3.1.27 число неприводимых многочленов степени 6 равно $\frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9$. Доказательство последнего утверждения также можно найти в § 3.1. □

Задача 2.6.25. Циклический код $\mathcal{X}$ длины N с порождающим многочленом $g(X)$ степени $d = N - k$ можно описать через корни многочлена $g(X)$, т. е. через такие элементы $\alpha_1, \ldots, \alpha_{N-k}$, что $g(\alpha_j) = 0$. Эти элементы называют *нулями* кода $\mathcal{X}$, они принадлежат полю Галуа $\mathbb{F}_{2^d}$. Так как $g(X) | (1 + X^N)$, нули кода являются также корнями многочлена $1 + X^N$, т. е. $\alpha_j^N = 1$, $j = 1, \ldots, N - k$. Значит, α_j — корни N-й степени из единицы. Оставшиеся k корней из единицы $\alpha'_1, \ldots, \alpha'_k$ называют *не нулями* кода $\mathcal{X}$. Многочлен $a(X) \in \mathcal{X}$ тогда и только тогда, когда в поле Галуа $\mathbb{F}_{2^d}$ выполняются равенства $a(\alpha_j) = 0$, $j = 1, \ldots, N - k$.

1. Покажите, что если $\mathcal{X}^\perp$ — двойственный код, то его нулями будут элементы ${\alpha'_1}^{-1}, \ldots, {\alpha'_k}^{-1}$, т. е. обратные элементы к не нулям исходного кода.

2. Циклический код $\mathcal{X}$ с образующей $g(X)$ называется *обратимым*, если $\forall \mathbf{x} = x_0 \ldots x_{N-1} \in \mathcal{X}$ слово $x_{N-1} \ldots x_0 \in \mathcal{X}$. Покажите, что код $\mathcal{X}$

обратим тогда и только тогда, когда из равенства $g(\alpha) = 0$ следует условие $g(\alpha^{-1}) = 0$.

3. Покажите, что q-ичный циклический код $\mathcal{X}$ длины N, для которого НОД $(q, N) = 1$, инвариантен относительно перестановок знаков $\pi_q(i) = qi \bmod N$ (т. е. $x \mapsto x^q$). Если $s = \mathrm{ord}_N(q)$, то перестановки $i \mapsto i + 1$ и $\pi_q(i)$ порождают подгруппу порядка Ns в группе автоморфизмов кода $\mathrm{Aut}(\mathcal{X})$.

Решение. Действительно, так как $a(x^q) = a(x)^q$, они пропорциональны одному и тому же порождающему многочлену и принадлежат одному коду. Доказательство последнего утверждения можно найти в § 3.1. □

Задача 2.6.26. Докажите, что существует 129 неэквивалентных циклических двоичных кодов длины 128 (включая тривиальные коды $\{0 \ldots 0\}$ и $\{0, 1\}^{128}$). Найдите все двоичные циклические коды длины 7.

Решение. Классы эквивалентности циклического кода длины 2^k взаимно однозначно соответствуют делителям многочлена $1 + X^{2^k}$, число которых равно $2^k + 1$. Наконец, существует 8 кодов, соответствующих своим образующим — делителям многочлена $1 + X^7$, которые можно задать, комбинируя любые множители разложения

$$1 + X^7 = (1 + X)(1 + X + X^3)(1 + X^2 + X^3).$$ □

Человеческий мозг просто не способен осознать всё, что является действительно сложным.

Андрей Колмогоров (1903–1987),
советский математик

Глава 3

Дальнейшие темы из теории кодирования

§ 3.1. Сведения по теории конечных полей

Специалист по конечным полям делает это с помощью умножения.

Специалист по конечным полям делает это в башнях.

(Из серии «Как они делают это».)

В этом параграфе мы представляем краткое изложение теории конечных полей в объёме, необходимом в дальнейшем. *Конечное поле* — это (конечное) множество $\mathbb{F}$, обладающее по крайней мере двумя различными элементами 0 (нуль) и e (единица) и оснащённое двумя коммутативными групповыми операциями сложением и умножением (где $0 \cdot b = 0 \ \forall b \in \mathbb{F}$), связанными стандартным правилом дистрибутивности.

Векторное пространство над полем $\mathbb{F}$ — это (конечное) множество $\mathbb{V}$, снабжённое коммутативной групповой операцией сложения и операцией умножения на скаляры, т. е. элементы поля $\mathbb{F}$. И здесь эти операции обладают стандартным свойством дистрибутивности. Размерностью $\dim \mathbb{V}$ векторного пространства $\mathbb{V}$ называется минимальное число d, такое что любые различные элементы $v_1, \ldots, v_{d+1} \in \mathbb{V}$ линейно зависимы, т. е. найдутся элементы $k_1, \ldots, k_{d+1} \in \mathbb{F}$, не все равные 0 такие, что $k_1 v_1 + \ldots + k_{d+1} v_{d+1} = 0$. В этом случае существует такой набор элементов $b_1, \ldots, b_d \in \mathbb{V}$, называемый базисом, что каждый элемент $v \in \mathbb{V}$ может быть записан как линейная комбинация $a_1 b_1 + \ldots + a_d b_d$, где $a_1, \ldots, a_d$ — элементы поля $\mathbb{F}$ (однозначно) определённые элементом v. Если не оговорено противное, мы рассматриваем поля с точностью до изоморфизма.

К важным параметрам поля относится его *характеристика*, т. е. минимальное целое число $p \geqslant 1$, для которого $pe = \underbrace{e + \ldots + e}_{p \text{ раз}} = 0$. Это число обозначаемое через $\mathrm{char}(\mathbb{F})$, существует по принципу Дирихле. Более того, характеристика — это простое число: если $p = q_1 q_2$, то $pe = (q_1 q_2)e =$

$= (q_1 e)(q_2 e) = 0$, откуда следует, что $q_1 e = 0$ или $q_2 e = 0$, что противоречит выбору p.

Пример 3.1.1. Пусть p — простое число. Аддитивная циклическая группа $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, порождённая 1, становится полем после введения умножения $(qe)(qe') = (qq')e$. Характеристика этого поля равна p. □

Пусть $\mathbb{K}$ и $\mathbb{F}$ — поля. Если $\mathbb{F} \subseteq \mathbb{K}$, мы будем говорить, что $\mathbb{K}$ — расширение поля $\mathbb{F}$. Поле $\mathbb{K}$ в этом случае будет векторным пространством над $\mathbb{F}$, размерность которого обозначается символом $[\mathbb{K} : \mathbb{F}]$.

Лемма 3.1.2. *Пусть $\mathbb{K}$ — расширение $\mathbb{F}$ и $d = [\mathbb{K} : \mathbb{F}]$. Тогда $\#\mathbb{K} = (\#\mathbb{F})^d$.*

Доказательство. Пусть $b_1, \ldots, b_d$ — базис поля $\mathbb{K}$ над $\mathbb{F}$ с однозначным представлением $k = \sum_{j=1}^{d} a_j b_j \ \forall k \in \mathbb{K}$. Тогда для всех j мы имеем $\#\mathbb{F}$ возможностей для a_j. Поэтому всего существует ровно $(\#\mathbb{F})^d$ способов выписать все комбинации. □

Лемма 3.1.3. *Если $\mathrm{char}(\mathbb{F}) = p$, то $\#\mathbb{F} = p^d$ для некоторого натурального числа d.*

Доказательство. Рассмотрим элементы $0, e, 2e, \ldots, (p-1)e$. Они образуют поле $\mathbb{Z}_p$, т. е. $\mathbb{Z}_p \subseteq \mathbb{F}$. Тогда $\#\mathbb{F} = p^d$ по лемме 3.1.2. □

Следствие 3.1.4. *Число элементов конечного поля $\mathbb{F}$ равно $q = p^s$, где $p = \mathrm{char}(\mathbb{F})$ и $s \geqslant 1$ — натуральное число.*

С этого момента, если не сказано обратного, p обозначает простое число, а $q = p^s$ — его степень.

Лемма 3.1.5 (мечта первокурсника). *Если $\mathrm{char}(\mathbb{F}) = p$, то $\forall a, b \in \mathbb{F}$ и натурального числа n имеет место равенство*

$$(a \pm b)^{p^n} = a^{p^n} + (\pm b)^{p^n}. \tag{3.1.1}$$

Доказательство. Применяем индукцию по n: при $n = 1$ имеем

$$(a \pm b)^p = \sum_{k=0}^{p} C_p^k a^r (\pm b)^{p-k}.$$

При $1 \leqslant k \leqslant p-1$ коэффициент C_p^k кратен p и соответствующее слагаемое равно нулю. Следовательно, $(a \pm b)^p = a^p + (\pm b)^p$. Индуктивный переход получается аналогично, если заменить a и $\pm b$ на $a^{p^{n-1}}$ и $b^{p^{n-1}}$. □

Лемма 3.1.6. *Мультипликативная группа $\mathbb{F}^*$ ненулевых элементов поля $\mathbb{F}$ размера q изоморфна циклической группе $\mathbb{Z}_{q-1}$.*

Доказательство. Заметим, что для любого делителя $d | (q-1)$ группа $\mathbb{F}^*$ содержит ровно $\varphi(d)$ элементов мультипликативного порядка d, где φ — функция Эйлера. Действительно, все такие элементы имеют вид

$a^{\frac{q-1}{d}r}$, где a — примитивный элемент, $r \leqslant d$ и r, d взаимно просты. На самом деле $q-1 = \sum\limits_{d:d|(q-1)} \varphi(d)$ и $\mathbb{F}^*$ должно иметь по крайней мере один элемент порядка $q-1$, откуда следует утверждение леммы. □

Пусть $a \in \mathbb{F}^*$ — элемент порядка d, где $d|(q-1)$. Возьмём циклическую подгруппу $\{e, a, \ldots, a^{d-1}\}$. Порядок каждого элемента этой подгруппы делит d, т. е. является корнем многочлена $X^d - e$ (корнем степени d из единицы). Но $X^d - e$ имеет не более d различных корней в $\mathbb{F}$ (так как $\mathbb{F}$ — поле). Таким образом, $\{e, a, \ldots, a^{d-1}\}$ — множество всех корней многочлена $X^d - e$ в поле $\mathbb{F}$. В частности, любой элемент из $\mathbb{F}$ порядка d принадлежит множеству $\{e, a, \ldots, a^{d-1}\}$. Заметим, что циклическая группа $\mathbb{Z}_d$ имеет ровно $\varphi(d)$ элементов порядка d. Тем самым во всей группе $\mathbb{F}^*$ есть ровно $\varphi(d)$ элементов порядка d, иначе говоря, если через $\psi(d)$ обозначить число элементов порядка d в поле $\mathbb{F}$, то либо $\psi(d) = 0$, либо $\psi(d) = \varphi(d)$ и

$$q - 1 = \sum_{d:d|n} \psi(d) \leqslant \sum_{d:d|n} \varphi(d) = q - 1,$$

откуда следует, что $\psi(d) = \varphi(d)\, \forall d|n$.

Определение 3.1.7. Образующая группы $\mathbb{F}^*$ (т. е. элемент мультипликативного порядка $q-1$) называется *примитивным* элементом поля $\mathbb{F}$. Хотя такой элемент не один, мы, как правило, выделяем один из них и обозначаем его через ω. Разумеется, степень ω^r при r взаимно простом с $(q-1)$ также является примитивным элементом. □

Если $a \in \mathbb{F}^*$ с $\#\mathbb{F}^* = q-1$, то $a^{q-1} = e$ (порядок любого элемента делит порядок группы). Следовательно, $a^q = a$, т. е. a — корень многочлена $X^q - X$ в поле $\mathbb{F}$. Но у такого многочлена не более, чем q корней (включая 0), поэтому $\mathbb{F}$ представляет собой множество всех корней многочлена $X^q - X$.

Определение 3.1.8. Пусть даны поля $\mathbb{F} \subseteq \mathbb{K}$. Поле $\mathbb{K}$ называется *полем разложения* многочлена $g(X)$ с коэффициентами из $\mathbb{F}$, если 1) в поле $\mathbb{K}$ находятся все корни этого многочлена, 2) не существует поля $\tilde{\mathbb{K}}$ со свойством $\mathbb{F} \subset \tilde{\mathbb{K}} \subset \mathbb{K}$, удовлетворяющего первому условию. Поле разложения многочлена $g(X)$ мы будем обозначать $\mathrm{Spl}\big(g(X)\big)$.

Итак, если $\#\mathbb{F} = q$, то $\mathbb{F}$ содержит все корни многочлена $X^q - X$ и является его полем разложения.

Лемма 3.1.9. *Любые два поля разложения $\mathbb{K}$, $\mathbb{K}'$ одного и того же многочлена $g(X)$ с коэффициентами из $\mathbb{F}$ совпадают.*

Доказательство. Действительно, рассмотрим пересечение $\mathbb{K} \cap \mathbb{K}'$: оно содержит $\mathbb{F}$ и является подполем как в $\mathbb{K}$, так и в $\mathbb{K}'$ и содержит также

все корни многочлена $g(X)$, поэтому должно совпадать с каждым из них из-за минимальности поля разложения. □

Следствие 3.1.10. *Для любого простого числа p и целого $s \geqslant 1$ существует не более одного поля с p^s элементами.*

Доказательство. Каждое такое поле является полем разложения многочлена $X^q - X$ с коэффициентами из $\mathbb{Z}_p$, где $q = p^s$. Поэтому любые два таких поля совпадают. □

С другой стороны, позже мы докажем следующую теорему.

Теорема 3.1.11. *Для любого непостоянного многочлена с коэффициентами из $\mathbb{F}$ существует поле разложения.*

Следствие 3.1.12. *Для любого простого числа p и натурального $s \geqslant 1$ существует ровно одно поле из p^s элементов.*

Доказательство следствия 3.1.12. Вновь возьмём многочлен $X^q - X$ с коэффициентами из $\mathbb{Z}_p$ при $q = p^s$. По теореме 3.1.11 существует поле разложения $\mathrm{Spl}\big(X^q - X\big)$, где $X^q - X = X(X^{q-1} - e)$ разлагается на линейные множители. Таким образом, $\mathrm{Spl}\big(X^q - X\big)$ содержит корни многочлена $X^q - X$ и имеет характеристику p (поскольку включает в себя $\mathbb{Z}_p$).

Однако корни многочлена $X^q - X$ образуют подполе: если $a^q = a$ и $b^q = b$, то по лемме 3.1.5 $(a \pm b)^q = a^q + (\pm b)^q$, что совпадает с $a \pm b$. Кроме того, $(ab^{-1})^q = a^q(b^q)^{-1} = ab^{-1}$. Поскольку это подполе не может строго содержаться в $\mathrm{Spl}\big(X^q - X\big)$, оно с ним совпадает.

Осталось проверить, что все корни многочлена $X^q - X$ различны: тогда мощность $\#\mathrm{Spl}\big(X^q - X\big)$ должна быть равна q. Если $X^q - X$ имеет кратные корни, то этот многочлен должен иметь общий множитель со своей производной $\partial_X(X^q - X) = qX^{q-1} - e$. Однако $qX^{q-1} = 0$ в поле $\mathrm{Spl}\big(X^q - X\big)$ и такого множителя не может быть. □

Суммируя всё изложенное выше, можно сформулировать две характеризующие теоремы о конечных полях.

Теорема 3.1.13. *Размер любого конечного поля равен p^s, где p — простое, а s — натуральное число. Для каждой такой пары p, s существует единственное поле такого размера.*

Поле размера $q = p^s$ принято обозначать символом $\mathbb{F}_q$ (другое популярное обозначение — $\mathrm{GF}(q)$ (*поле Галуа*). В случае простейших полей $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ (для простого p) мы обозначаем единицу поля символом 1 вместо e.

Теорема 3.1.14. *Все конечные поля можно организовать в последовательность* (*называемую* «башней»): *для простого p и натуральных чисел s_1, s_2, ... имеет место цепочка гомоморфизмов*

$$
\begin{array}{c}
\dots \\
\dots \\
\dots \\
\uparrow \\
\mathbb{F}_{p^{s_1 s_2 \dots s_i}} \\
\uparrow \\
\dots \\
\uparrow \\
\mathbb{F}_{p^{s_1 s_2}} \\
\uparrow \\
\mathbb{F}_{p^{s_1}} \\
\uparrow \\
\mathbb{F}_p \simeq \mathbb{Z}_p
\end{array}
$$

каждая стрелка здесь — однозначно определённый инъективный гомоморфизм.

Пример 3.1.15. В § 2.5 мы работали с полиномиальным полем $\mathbb{F}_2[X]/\langle g(X)\rangle$, где $g(X)$ — неприводимый двоичный многочлен; см. теоремы 2.5.33 и 2.5.34. Продолжая п. 3 примера 2.5.36, рассмотрим поле $\mathbb{F}_{16}$, реализованное как $\mathbb{F}_2[X]/\langle 1 + X^3 + X^4\rangle$. Структура этого поля отражена

в следующей таблице.

степень X	многочлен $\bmod(1+X^3+X^4)$	вектор (строка)
$-$	0	0000
X^0	1	1000
X	X	0100
X^2	X^2	0010
X^3	X^3	0001
X^4	$1+X^3$	1001
X^5	$1+X+X^3$	1101
X^6	$1+X+X^2+X^3$	1111
X^7	$1+X+X^2$	1110
X^8	$X+X^2+X^3$	0111
X^9	$1+X^2$	1010
X^{10}	$X+X^3$	0101
X^{11}	$1+X^2+X^3$	1011
X^{12}	$1+X$	1100
X^{13}	$X+X^2$	0110
X^{14}	X^2+X^3	0011

(3.1.2)

Выбор в качестве реализации поля $\mathbb{F}_2[X]/\langle 1+X+X^2+X^3+X^4\rangle$ не так удобен, поскольку вычисления, необходимые для заполнения аналогичной таблицы, окажутся значительно длиннее (и организованы иначе). Дело в том, что в такой реализации моном X уже не будет примитивным элементом, поскольку $X^5 = 1 \bmod (1+X+X^2+X^3+X^4)$. Примитивным элементом будет, например, $1+X$. □

Пример 3.1.16. 1. Сколько элементов в наименьшем расширении поля $\mathbb{F}_5$, содержащем все корни многочленов X^2+X+1 и X^3+X+1?

2. Найдите число подполей в $\mathbb{F}_{1024}$, $\mathbb{F}_{729}$. Найдите все примитивные элементы в полях $\mathbb{F}_7$, $\mathbb{F}_9$, $\mathbb{F}_{16}$. Вычислите $(\omega^{10}+\omega^5)(\omega^4+\omega^2)$, где ω — примитивный элемент поля $\mathbb{F}_{16}$.

Решение. 1. Очевидно, 5^6.

2. Поле $\mathbb{F}_{1024} = \mathbb{F}_{2^{10}}$ имеет 4 подполя: $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_{32}$ и $\mathbb{F}_{1024}$. Поле $\mathbb{F}_{729} = \mathbb{F}_{3^6}$ имеет 4 подполя: $\mathbb{F}_3$, $\mathbb{F}_9$, $\mathbb{F}_{27}$ и $\mathbb{F}_{729}$. В поле $\mathbb{F}_7$ есть 2 примитивных элемента: ω, ω^5 (с $(\omega^5)^6 = e$). Поле $\mathbb{F}_9$ содержит 4 примитивных элемента: ω, ω^3, ω^5, ω^7. В поле $\mathbb{F}_{16}$ присутствуют 8 примитивных элементов: ω, ω^2, ω^4, ω^7, ω^8, ω^{11}, ω^{13}, ω^{14}.

Основываясь на таблице поля $\mathbb{F}_2[X]/\langle 1 + X + X^4\rangle$ (см. п. 3 примера 2.5.36), находим, что

$$(\omega^{10} + \omega^5)(\omega^4 + \omega^2) = \omega^{14} + \omega^9 + \omega^{12} + \omega^7 =$$
$$= 1001 + 0101 + 1111 + 1101 = 1110 = \omega^{10}.$$

Однако если в качестве примитивного элемента взять $\omega' = \omega^7$, то п. ч. перепишется как

$$\omega^8 + \omega^3 + \omega^9 + \omega^4 = 1010 + 0001 + 0101 + 1100 = 0010 = \omega^2 = (\omega')^{11}. \ \square$$

Существует лишь 10 типов людей в этом мире:
те, которые знают $\mathbb{F}_2$ и те, которые не знают.

(Из серии «Так говорил суперлектор».)

С этого момента мы сфокусируем внимание на полиномиальных реализациях конечных полей, обобщая концепции, введённые в § 2.5.

Определение 3.1.17. Множество многочленов с коэффициентами из $\mathbb{F}_q$ представляет собой коммутативное кольцо, обозначаемое $\mathbb{F}_q[X]$. *Факторкольцо* $\mathbb{F}_q[X]/\langle g(X)\rangle$ — это кольцо многочленов с операциями по модулю фиксированного многочлена $g(X) \in \mathbb{F}_q[X]$. $\square$

Определение 3.1.18. Многочлен $g(X) \in \mathbb{F}_q[X]$ называется *неприводимым* (над $\mathbb{F}_q$), если его нельзя представить в виде

$$g(X) = g_1(X)g_2(X),$$

где $g_1(X)$, $g_2(X) \in \mathbb{F}_q[X]$ — многочлены положительной степени. $\square$

Обобщение теоремы 2.5.33 представлено теоремой 3.1.19.

Теорема 3.1.19. *Пусть $g(X) \in \mathbb{F}_q[X]$ — многочлен степени d. Тогда факторкольцо $\mathbb{F}_q[X]/\langle g(X)\rangle$ будет полем в том и только том случае, если многочлен $g(X)$ неприводим.*

Доказательство. Пусть $g(X)$ — неприводимый многочлен над $\mathbb{F}_q$. Чтобы показать, что $\mathbb{F}_q[X]/\langle g(X)\rangle$ — поле, нам нужно проверить, что каждый ненулевой элемент $f(X) \in \mathbb{F}_q[X]/\langle g(X)\rangle$ обладает обратным. Рассмотрим множество $\mathbb{F}(f)$ многочленов вида $f(X)h(X) \bmod (g(X))$, где $h(X) \in \mathbb{F}_q[X]/\langle g(X)\rangle$ (главный идеал, порождённый $f(X)$). Если $\mathbb{F}(f)$ содержит единицу $e \in \mathbb{F}_q$ (постоянный многочлен, равный e), то соответствующий многочлен имеет вид $h(X) = f(X)^{-1}$. Если это не так, то отображение $h(X) \mapsto f(X)h(X) \bmod (g(X))$ из $\mathbb{F}_q[X]/\langle g(X)\rangle$ в себя не сюръективно. Но, ввиду конечности $\mathbb{F}_q[X]/\langle g(X)\rangle$ оно не будет и инъективным, т. е. $f(X)h_1(X) = f(X)h_2(X) \bmod (g(X))$ для некоторых разных $h_1(X)$, $h_2(X)$, значит,

$$f(X)(h_1(X) - h_2(X)) = r(X)g(X).$$

Следовательно, либо $g(X)|f(X)$, либо $g(X)|(h_1(X)-h_2(X))$, так как многочлен $g(X)$ неприводим. Поэтому либо $f(X)=0 \bmod (g(X))$ (что противоречит условию), либо $h_1(X)=h_2(X) \bmod (g(X))$. Итак, $\mathbb{F}_q[X]/\langle g(X)\rangle$ — поле.

Обратное утверждение проверяется аналогично: если $g(X)$ приводим, то кольцо $\mathbb{F}_q[X]/\langle g(X)\rangle$ содержит такие ненулевые многочлены $g_1(X)$, $g_2(X)$, что $g_1(X)g_2(X)=0$. Поэтому $\mathbb{F}_q[X]/\langle g(X)\rangle$ не может быть полем.

Размерность поля $[\mathbb{F}_q[X]/\langle g(X)\rangle : \mathbb{F}_q]$ равна d, т. е. совпадает со степенью $g(X)$, откуда $\mathbb{F}_q[X]/\langle g(X)\rangle \simeq \mathbb{F}_{q^d}$. □

Пример 3.1.20. Докажите, что $g(X)$ обратим в полиномиальном кольце $\mathbb{F}_q[X]/\langle X^N-e\rangle$ тогда и только тогда, когда НОД $(g(X), X^N-e)=e$.

Решение. Рассмотрим отображение $\mathbb{F}_q[X]/\langle X^N-e\rangle \to \mathbb{F}_q[X]/\langle X^N-e\rangle$, заданное по правилу $h(X)\mapsto h(X)g(X) \bmod (X^N-e)$. Если оно сюръективно, то найдётся $h(X)$, для которого $h(X)g(X)=e$ и $h(X)=g(X)^{-1}$. Допустим, что это не так. Тогда существует такая пара многочленов $h^{(1)}(X)\neq h^{(2)}(X) \bmod (X^N-e)$, что $h^{(1)}(X)g(X)=h^{(2)}(X)g(X) \bmod (X^N-e)$, т. е.

$$(h^{(1)}(X)-h^{(2)}(X))g(X)=s(X)(X^N-e).$$

Поскольку $(X^N-e)\not|(h^{(1)}(X)-h^{(2)}(X))$, имеем НОД $(g(X), X^N-e)\neq e$.

Обратно, если НОД $(g(X), X^N-e)=d(X)\neq e$, то из уравнения $h(X)g(X)=e \bmod (X^N-e)$ получаем, что

$$h(X)g(X)=e+q(X)(X^N-e),$$

где $d(X)$ делит л. ч. и $d(X)|q(X)(X^N-e)$, откуда $d(X)|e$: противоречие. Следовательно, $g(X)^{-1}$ не существует. □

Пример 3.1.21 (продолжение примера 2.5.20). Есть шесть неприводимых многочленов над полем $\mathbb{F}_2$ степени 5:

$$\begin{gathered}1+X^2+X^5,\quad 1+X^3+X^5,\quad 1+X+X^2+X^3+X^5,\\ 1+X+X^2+X^4+X^5,\quad 1+X+X^3+X^4+X^5,\\ 1+X^2+X^3+X^4+X^5.\end{gathered}\tag{3.1.3}$$

Существует девять неприводимых многочленов степени 6 и т. д. Вычисление неприводимых многочленов большой степени — непростая задача, хотя в интернете сейчас можно найти таблицы таких многочленов больших степеней. □

Теперь мы собираемся доказать теорему 3.1.11.

Доказательство теоремы 3.1.11. Ключевой факт состоит в том, что любой непостоянный многочлен $g(X)\in\mathbb{F}_q[X]$ имеет корень в некотором расширении поля $\mathbb{F}_q$. Не ограничивая общности, можно считать, что многочлен $g(X)$ неприводим и $\deg g(X)=d$. Возьмём поле $\mathbb{F}_q[X]/\langle g(X)\rangle = \mathbb{F}_{q^d}$ в качестве расширения. В этом поле $g(\alpha)=0$, где α — многочлен

$X \in \mathbb{F}_q[X]/\langle g(X)\rangle$, так что $g(X)$ там имеет корень. Мы можем разделить $g(X)$ на $X - \alpha$ в поле $\mathbb{F}_{q^d}$, воспользоваться той же конструкцией для многочлена $g_1(X) = g(X)/(X - \alpha)$ и увидеть, что он имеет корень в некотором расширении $\mathbb{F}_{q^t}$, $t > d$. Наконец, мы получим поле, содержащее все d корней многочлена $g(X)$, т. е. построим поле разложения $\mathrm{Spl}\big(g(X)\big)$. □

Определение 3.1.22. Для данных полей $\mathbb{F} \subset \mathbb{K}$ и элемента $\gamma \in \mathbb{K}$ обозначим через $\mathbb{F}(\gamma)$ наименьшее поле, содержащее $\mathbb{F}$ и γ (очевидно, $\mathbb{F} \subset \mathbb{F}(\gamma) \subset \mathbb{K}$). Аналогично $\mathbb{F}(\gamma_1, \ldots, \gamma_r)$ — наименьшее поле, содержащее $\mathbb{F}$ и элементы $\gamma_1, \ldots, \gamma_r \in \mathbb{K}$. Для $\mathbb{F} = \mathbb{F}_q$ и $\alpha \in \mathbb{K}$ положим

$$M_{\alpha,\mathbb{F}}(X) = (X - \alpha)(X - \alpha^q) \ldots (X - \alpha^{q^{d-1}}), \tag{3.1.4}$$

где d — наименьшее натуральное число, при котором $\alpha^{q^d} = \alpha$ (такое число d существует в силу леммы 3.1.24).

Приведённым называется многочлен со старшим коэффициентом один. *Минимальным* многочленом элемента $\alpha \in \mathbb{K}$ над $\mathbb{F}$ называется единственный такой приведённый многочлен $M_\alpha(X)(= M_{\alpha,\mathbb{F}}(X)) \in \mathbb{F}[X]$, что $M_\alpha(\alpha) = 0$ и $M_\alpha(X) | g(X)$ для каждого $g(X) \in \mathbb{F}[X]$, удовлетворяющий условию $g(\alpha) = 0$. Когда ω — примитивный элемент поля $\mathbb{K}$ (образующая группы $\mathbb{K}^*$), $M_\omega(X)$ называется *примитивным* многочленом (над $\mathbb{F}$). *Порядком* многочлена (над $\mathbb{F}$) $p(X) \in \mathbb{F}[X]$ называется наименьшее натуральное число n, при котором $p(X) | (X^n - e)$. □

Maxims of Minimal Polynomials
Принципы, которым следуют минимальные многочлены
(Из серии «Фильмы, которые не вышли на большой экран».)

Пример 3.1.23. (продолжение примера 3.1.21). В этом примере мы имеем дело с многочленами над полем $\mathbb{F}_2$. Неприводимый многочлен $X^2 + X + 1$ примитивен и имеет порядок 3. Неприводимые многочлены $X^3 + X + 1$ и $X^3 + X^2 + 1$ примитивны и имеют порядок 7. Многочлены $X^4 + X^3 + 1$ и $X^4 + X + 1$ примитивны и имеют порядок 15, тогда как многочлен $X^4 + X^3 + X^2 + X + 1$ не примитивен и имеет порядок 5. (Полезно отметить, что при $d = 4$ порядок многочленов $X^4 + X^3 + 1$ и $X^4 + X + 1$ равен $2^d - 1$; с другой стороны, порядок элемента X в поле $\mathbb{F}_2[X]/\langle 1 + X + X^2 + X^3 + X^4\rangle$ равен 5, но его порядок, скажем, в поле $\mathbb{F}_2[X]/\langle 1 + X + X^4\rangle$ равен 15.) Все шесть многочленов, перечисленных в формуле (3.1.3), примитивны и имеют порядок 31 (т. е. появляются в разложении многочлена $X^{31} + 1$). □

Лемма 3.1.24. *Пусть* $\mathbb{F}_q \subset \mathbb{F}_{q^d}$ *и* $\alpha \in \mathbb{F}_{q^d}$. *Пусть* $M_\alpha(X) \in \mathbb{F}[X]$ — *минимальный многочлен для* α *степени* $\deg M_\alpha(X) = d$. *Тогда*

1) $M_\alpha(X)$ — *неприводимый многочлен в* $\mathbb{F}_q[X]$ *с корнем* α;

2) $M_\alpha(X)$ — *приведённый многочлен в* $\mathbb{F}_q[X]$ *степени* d *с корнем* α;
3) $M_\alpha(X)$ *имеет вид* (3.1.4).

Доказательство. Первые два утверждения следуют из определения. Для доказательства последнего предположим, что $\gamma \in \mathbb{K}$ — корень многочлена $g(X) = a_0 + a_1X + \ldots + a_dX^d$ из $\mathbb{F}[X]$, т. е. $\sum\limits_{i=0}^{d} a_i\gamma^i = 0$. Так как $a_i^q = a_i$ (что верно $\forall a \in \mathbb{F}$), с учётом леммы 3.1.5 получаем, что

$$g(\gamma^q) = \sum_{i=0}^{d} a_i\gamma^{qi} = \sum_{i=0}^{d} (a_i\gamma^i)^q = \left(\sum_{i=0}^{d} a_i\gamma^i\right)^q = 0,$$

откуда следует, что γ^q — тоже корень и т. д.

Для $M_\alpha(X)$ это означает, что его корнями будут элементы α, α^q, α^{q^2}, … Последовательность корней заканчивается элементом $\alpha^{q^s} = \alpha$, появившимся в первый раз (такое s всегда существует в конечном поле). Наконец, $s = d$, поскольку все степени α, α^q, …, $\alpha^{q^{d-1}}$ различны. Действительно, если это не так, то $\alpha^{q^i} = \alpha^{q^j}$, где, скажем, $i < j$. Возведя обе части этого равенства в степень q^{d-i}, мы получим $\alpha^{q^{d+i-j}} = \alpha^{q^d} = \alpha$, значит, α — корень многочлена $P(X) = X^{q^{d+i-j}} - X$, и $\mathrm{Spl}\big(P(X)\big) = \mathbb{F}_{q^{d+i-j}}$. С другой стороны, α — корень неприводимого многочлена степени d, и $\mathrm{Spl}\big(M_\alpha(X)\big) = \mathbb{F}_{q^d}$. Следовательно, $d|(d+i-j)$ или $d|(i-j)$, что невозможно. Это и означает, что все корни α^{q^i} при $i < d$ различны. □

Теорема 3.1.25. *Для любого поля* $\mathbb{F}_q$ *и натурального числа* $d \geqslant 1$ *существует неприводимый многочлен* $g(X) \in \mathbb{F}_q[X]$ *степени* d.

Доказательство. Возьмём примитивный элемент $\omega \in \mathbb{F}_{q^d}$. Тогда поле $\mathbb{F}_q(\omega)$ — минимальное расширение поля $\mathbb{F}_q$, содержащее ω — совпадает с $\mathbb{F}_{q^d}$. Размерность $[\mathbb{F}_q(\omega) : \mathbb{F}_q]$ векторного пространства $\mathbb{F}_q(\omega)$ над $\mathbb{F}_q$ равно $[\mathbb{F}_q(\omega) : \mathbb{F}_q] = d$. Минимальный многочлен $M_\omega(X)$ для ω над $\mathbb{F}_q$ имеет различные корни ω, ω^q, …, $\omega^{q^{d-1}}$ и, следовательно, его степень равна d. □

Хотя доказательство неприводимости конкретного многочлена представляет собой задачу, не имеющую общего решения, число неприводимых многочленов данной степени можно вычислить элегантным (и не очень сложным) способом, с помощью так называемой *функции Мёбиуса*.

Определение 3.1.26. Функция Мёбиуса μ на $\mathbb{Z}_+$ определяется следующим образом: $\mu(1) = 1$, $\mu(n) = 0$, если n делится на квадрат простого числа, и

$$\mu(n) = (-1)^k, \text{ если } n \text{ — произведение } k \text{ различных простых чисел.}$$ □

The Polynomial Always Rings Twice

Lord of Polynomial Rings[1]

(Из серии «Фильмы, которые не вышли на большой экран».)

Теорема 3.1.27. *Число $N_q(n)$ неприводимых многочленов степени n в полиномиальном кольце $\mathbb{F}_q[X]$ составляет*

$$N_q(n) = \frac{1}{n} \sum_{d:d|n} \mu(d) q^{n/d}. \tag{3.1.5}$$

Например, $N_q(20)$ равно

$$\frac{1}{20}(\mu(1)q^{20} + \mu(2)q^{10} + \mu(4)q^5 + \mu(5)q^4 + \mu(10)q^2 + \mu(20)q) = \\ = \frac{1}{20}(q^{20} - q^{10} - q^4 + q^2).$$

Доказательство. Прежде всего мы выведем аддитивную формулу обращения Мёбиуса. Пусть ψ и Ψ — две функции из $\mathbb{Z}_+$ в абелеву группу G с аддитивной групповой операцией. Тогда следующие равенства эквивалентны:

$$\Psi(n) = \sum_{d|n} \psi(d) \tag{3.1.6}$$

и

$$\psi(n) = \sum_{d|n} \mu(d) \Psi\left(\frac{n}{d}\right). \tag{3.1.7}$$

Эквивалентность вытекает из следующих наблюдений: а) сумма $\sum_{d|n} \mu(d)$ равна 0, если $n > 1$, и 1, если $n = 1$, б) для любого n выполняется равенство

$$\sum_{d:\, d|n} \mu(d)\Psi(n/d) = \sum_{d:\, d|n} \mu(d) \sum_{c:\, c|n/d} \psi(c) = \sum_{c:\, c|n} \psi(c) \sum_{d:\, d|n/c} \mu(d) = \psi(n).$$

Чтобы проверить а), рассмотрим различные простые делители числа n: $p_1, \ldots, p_k$, тогда

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \ldots + \mu(p_1 \ldots p_k) = \\ = 1 + C_k^1(-1) + C_k^2(-1)^2 + \ldots + C_k^k(-1)^k = 0.$$

[1] Ср. с названием фильмов «The Postman Always Rings Twice» (1946 и 1981 г., по повести Дж. Кейна) и «Lord of the Rings» (2001–2003, по книгам Дж. Толкиена).

Разложим теперь многочлен $X^{q^n} - X$ в произведение неприводимых множителей. Тогда формула (3.1.6) будет выполнена при выборе полиномов $\psi(n) = nN_q(n)$ и $\Psi(n) = q^n$, так как степень q^n многочлена $X^{q^n} - X$ совпадает с суммой степеней всех неприводимых многочленов, степени которых делят n. Действительно, мы просто запишем $X^{q^n} - X$ как произведение неприводимых многочленов и заметим, что неприводимый многочлен входит в это разложение тогда и только тогда, когда его степень делит n (см. следствие 3.1.30). Применяя формулу (3.1.7) к аддитивной группе целых чисел $G = \mathbb{Z}$, получим формулу (3.1.5). □

Пример 3.1.28. Найдите все неприводимые многочлены степеней 2 и 3 над полем $\mathbb{F}_3$ и определите их порядок.

Решение. Над полем $\mathbb{F}_3 = \{0, 1, 2\}$ существуют 3 неприводимых многочлена степени 2: $X^2 + 1$ порядка 4, а именно

$$(X^4 - 1)/(X^2 + 1) = X^2 - 1,$$

$X^2 + X + 2$ и $X^2 + 2X + 2$ порядка 8, а именно,

$$(X^8 - 1)/(X^2 + X + 2)(X^2 + 2X + 2) = X^4 - 1.$$

Далее, существуют $(3^3 - 3)/3 = 8$ неприводимых многочленов степени 3 над полем $\mathbb{F}_3$. Порядок четырёх из них равен 13 (поэтому они не относятся к примитивным):

$$X^3 + 2X + 2, \quad X^3 + X^2 + 2, \quad X^3 + X^2 + X + 2, \quad X^3 + 2X^2 + 2X + 2.$$

Порядок остальных четырёх равен 26 (и, значит, они примитивны):

$$X^3 + 2X + 1, \quad X^3 + X^2 + 2X + 1, \quad X^3 + 2X^2 + 1, \quad X^3 + 2X^2 + X + 1.$$

Действительно, если $p(X)$ обозначает произведение первых четырёх многочленов, то $(X^{13} - 1)/p(X) = X - 1$. С другой стороны, если через $r(X)$ обозначить произведение остальных четырёх многочленов, то $(X^{26} - 1)/r(X)$ равно

$$(X - 1)(X + 1)(X^3 + 2X + 2)(X^3 + X^2 + 2)\times \\ \times (X^3 + X^2 + X + 2)(X^3 + 2X^2 + 2X + 2). \quad \square$$

Теорема 3.1.29. *Если $g(X) \in \mathbb{F}_q[X]$ — неприводимый многочлен степени d и α — его корень, то поле разложения $\mathrm{Spl}\big(g(X)\big)$ и минимальное расширение $\mathbb{F}_q(\alpha)$ совпадают с полем $\mathbb{F}_{q^d}$.*

Доказательство. Мы знаем, что $g(X) = M_{\alpha,\mathbb{F}_q}(X)$ (по лемме 3.1.24 из-за неприводимости $g(X)$). Кроме того, нам известно, что $\mathbb{F}_q \subset \mathbb{F}_q(\alpha) \subseteq \mathrm{Spl}\big(g(X)\big)$. Остаётся проверить, что любой корень γ многочлена $g(X)$ принадлежит полю $\mathbb{F}_q(\alpha)$: отсюда будет следовать включение

$\mathrm{Spl}\big(g(X)\big) \subseteq \mathbb{F}_q(\alpha)$. Поле Галуа с q^d элементами $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$, единственное в силу теоремы 3.1.13, является полем разложения $\mathrm{Spl}\big(X^{q^d} - X\big)$, т. е. содержит все корни многочлена $X^{q^d} - X$ (один из которых равен α). Так как $g(X) = M_{\alpha,\mathbb{F}_q}(X)$, получаем, что $g(X) | (X^{q^d} - X)$. Поэтому все корни многочлена $g(X)$ являются и корнями многочлена $X^{q^d} - X$ и, следовательно, лежат в $\mathbb{F}_q(\alpha)$. □

Следствие 3.1.30. *Предположим, что $g(X) \in \mathbb{F}_q[X]$ — неприводимый многочлен степени d. Тогда $g(X) | (X^{q^n} - X)$ в том и только том случае, если $d | n$.*

Доказательство. У нас есть поля разложения: $\mathrm{Spl}\big(g(X)\big) = \mathbb{F}_{q^d}$ и $\mathrm{Spl}\big(X^{q^n} - X\big) = \mathbb{F}_{q^n}$. По теореме 3.1.29 $\mathrm{Spl}\big(g(X)\big) \subseteq \mathrm{Spl}\big(X^{q^n} - X\big)$ тогда и только тогда, когда $d | n$.

Если $g(X) | (X^{q^n} - X)$, то каждый корень многочлена $g(X)$ является нулём многочлена $(X^{q^n} - X)$, откуда $\mathrm{Spl}\big(g(X)\big) \subseteq \mathrm{Spl}\big(X^{q^n} - X\big)$ и $d | n$.

В другую сторону, если $d | n$, т. е. $\mathrm{Spl}\big(g(X)\big) \subseteq \mathrm{Spl}\big(X^{q^n} - X\big)$, то все корни многочлена $g(X)$ лежат в поле $\mathrm{Spl}\big(X^{q^n} - X\big)$. Но $\mathrm{Spl}\big(X^{q^n} - X\big)$ состоит ровно из всех корней многочлена $X^{q^n} - X$, так что каждый корень многочлена $g(X)$ обращает в нуль многочлен $X^{q^n} - X$, т. е. $g(X) | (X^{q^n} - X)$. □

Теорема 3.1.31. *Если $g(X) \in \mathbb{F}_q[X]$ — неприводимый многочлен степени d и $\alpha \in \mathrm{Spl}\big(g(X)\big) = \mathbb{F}_{q^d}$ — его корень, то все корни многочлена $g(X)$ исчерпываются списком $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$. Более того, d — наименьшее натуральное число, для которого $\alpha^{q^d} = \alpha$.*

Доказательство. Как в доказательстве леммы 3.1.24, $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ — различные корни. Поэтому все корни перечислены и d — наименьшее натуральное число с указанным свойством. □

Следствие 3.1.32. *Все корни неприводимого многочлена $g(X) \in \mathbb{F}_q[X]$ степени d имеют в поле $\mathrm{Spl}\big(g(X)\big)$ один и тот же мультипликативный порядок, делящий $q^d - 1$, совпадающий с порядком многочлена $g(X)$ (см. определение* 3.1.22). □

Порядок неприводимого многочлена $g(x)$ будет обозначаться через $\mathrm{ord}(g(X))$.

Пример 3.1.33. 1. Докажите, что для любых взаимно простых натуральных чисел n, q найдётся натуральное число s, при котором $n | (q^s - 1)$.

2. Докажите, что неприводимый многочлен $g(X) \in \mathbb{F}_2[X]$ делит $(X^n + 1)$ тогда и только тогда, когда $\mathrm{ord}(g(X)) | n$.

Решение. 1. Положим $q^l - 1 = na_l + b_l$, где $b_l < n$ и $l = 1, 2, \ldots$ По принципу Дирихле $b_{l_1} = b_{l_2}$ для некоторых $l_1 < l_2$. Тогда $n | q^{l_1}(q^{l_2 - l_1} - 1)$. Так как по условию n и q взаимно просты, получаем, что $n | (q^s - 1)$ при $s = l_2 - l_1$.

2. Порядок неприводимого многочлена был введён в определении 3.1.22:

$$\operatorname{ord}(g(X)) = \min[n\colon g(X)|(X^n+1)].$$

Нам предстоит проверить, что если $m = \operatorname{ord}(g(X))$, то $m|n$ тогда и только тогда, когда $g(X)|(X^n+1)$. Действительно, предположим, что $m|n$: $n = mr$. Тогда $(X^n+1) = (X^m+1)(1+X^m+\ldots+X^{m(r-1)})$. Так как $g(X)|(X^m+1)$, получаем, что $g(X)|(X^n+1)$.

Обратно, если $g(X)|(X^n+1)$, то корни $\alpha_1, \ldots, \alpha_d$ многочлена $g(X)$ находятся среди корней многочлена X^n+1 в $\operatorname{Spl}\bigl(X^n+1\bigr)$. Поэтому $\alpha_j^m = \alpha_j^n = 1$ в $\operatorname{Spl}\bigl(X^n+1\bigr)$, $1 \leqslant j \leqslant d$. Запишем $n = mb + a$, где $0 \leqslant a < m$. Тогда $\alpha_j^n = \alpha_j^{bm}\alpha_j^a = \alpha_j^a = 1$, т. е. все α_j — корни многочлена X^a+1. Значит, при $a > 0$ имеем $g(X)|(X^a+1)$, что противоречит определению порядка. Следовательно, $a = 0$ и $m|n$. □

Вычисление неприводимого многочлена $g(X) \in \mathbb{F}_q[X]$ с данным корнем $\alpha \in \mathbb{F}_{q^n}$, в частности минимального многочлена $M_{\alpha,\mathbb{F}_q}(X)$ представляет собой нелёгкую задачу. Причина заключается в сложном соотношении между q, n, α и $d = \deg M_\alpha(X)$. Однако если $\alpha = \omega$ — примитивный элемент поля $\mathbb{F}_{q^n}$, то $d = n$, поскольку $\omega^{q^n-1} = e$, $\omega^{q^n} = \omega$ и n — наименьшее натуральное число с таким свойством. В этом случае $M_\omega(X) = \prod\limits_{b\in\mathbb{F}_{q^n}} (X-b)$.

Для общего неприводимого многочлена полезно понятие «сопряжённость»: см. определение 3.1.34. Это понятие было неформально введено (и использовалось) в § 2.5 для полей $\mathbb{F}_{2^d}$.

Определение 3.1.34. Элементы α, $\alpha' \in \mathbb{F}_{q^d}$ называются *сопряжёнными* над $\mathbb{F}_q$, если $M_{\alpha,\mathbb{F}_q}(X) = M_{\alpha',\mathbb{F}_q}(X)$. □

The field of Golgotha and dead men's skulls.

Вильям Шекспир (1564–1616),
английский драматург и поэт; «Ричард II»

Подводя итог сказанному выше, сформулируем следующую теорему.

Теорема 3.1.35. *К сопряженным элементу $\alpha \in \mathbb{F}_{q^d}$ над полем $\mathbb{F}_q$ относятся α, α^q, $\ldots$, $\alpha^{q^{d-1}} \in \mathbb{F}_{q^d}$, где d — такое минимальное число, что $\alpha^{q^d} = \alpha$. В частности, коэффициенты многочлена $\prod\limits_{j=0}^{d-1}(X-\alpha^{q^j})$ принадлежат полю $\mathbb{F}_q$, а сам многочлен — это единственный многочлен из $\mathbb{F}_q[X]$ с корнем α. Кроме того, это единственный приведённый многочлен минимальной степени в кольце $\mathbb{F}_q[X]$ с корнем α.*

Пример 3.1.36. Продолжая пример 3.1.28, мы отождествим $\mathbb{F}_{16}$ с $\mathbb{F}_2(\omega)$ — наименьшим полем, содержащим корень ω примитивного мно-

гочлена порядка 4. Если выбрать $1 + X + X^4$, то ω будет удовлетворять соотношению $\omega^4 = 1 + \omega$, а если остановиться на $1 + X^3 + X^4$, то ω будет подчиняться соотношению $\omega^4 = 1 + \omega^3$. В обоих случаях его сопряжёнными будут элементы ω, ω^2, ω^4 и ω^8.

Соответственно таблица (3.1.2) принимает вид

	$1 + X + X^4$	$1 + X^3 + X^4$
степень ω	вектор (строка)	вектор (строка)
–	0000	0000
0	1000	1000
1	0100	0100
2	0010	0010
3	0001	0001
4	1100	1001
5	0110	1101
6	0011	1111
7	1101	1110
8	1010	0111
9	0101	1010
10	1110	0101
11	0111	1011
12	1111	1100
13	1011	0110
14	1001	0011

(3.1.8)

В поле с правилом сложения из левого столбца минимальным многочленом $M_{\omega^i}(X)$ для степени ω^i будет $1 + X + X^4$ при $i = 1, 2, 4, 8$ и $1 + X^3 + X^4$ для $i = 7, 14, 13, 11$, в то время как при $i = 3, 6, 12, 9$ таким многочленом будет $1 + X + X^2 + X^3 + X^4$, а для $i = 5, 10$ он минимальный многочлен $1 + X + X^2$. Если правило сложения задаётся правым столбцом, то нужно переставить многочлены $1 + X + X^4$ и $1 + X^3 + X^4$. Порядок многочленов $1 + X + X^4$ и $1 + X^3 + X^4$ равен 15, порядок многочлена $1 + X + X^2 + X^3 + X^4$ равен 5 и порядок многочлена $1 + X + X^2$ равен 3.

Простой способ получить эти ответы состоит в том, чтобы выразить $(\omega^i)^4$ в виде линейной комбинации элементов 1, ω^i, $(\omega^i)^2$ и $(\omega^i)^3$. Например, из левого столбца таблицы для элемента ω^7 мы имеем

$$(\omega^7)^4 = \omega^{28} = \omega^3 + \omega^2 + 1,$$
$$(\omega^7)^3 = \omega^{21} = \omega^3 + \omega^2$$

и легко видеть, что $(\omega^7)^4 = 1 + (\omega^7)^3$, т. е. ω^7 — корень многочлена $1 + X^3 + X^4$. Для полноты картины выпишем неиспользованное выражение

для $(\omega^7)^2$:

$$(\omega^7)^2 = \omega^{14} = \omega^{12}\omega^2 = (1+\omega)^3\omega^2 = (1+\omega+\omega^2+\omega^3)\omega^2 = \\ = \omega^2+\omega^3+\omega^4+\omega^5 = \omega^2+\omega^3+1+\omega+(1+\omega)\omega = 1+\omega^3.$$

Для $M_{\omega^5}(X)$ стандартный подход даёт короткое выражение:

$$M_{\omega^5}(X) = (X-\omega^5)(X-\omega^{10}) = X^2+(\omega^5+\omega^{10})X+\omega^{15} = X^2+X+1.$$

Таким образом, полный список минимальных многочленов поля $\mathbb{F}_{16}$ имеет вид

$$M_{\omega^0}(X) = 1+X, \quad M_{\omega}(X) = 1+X+X^4,$$
$$M_{\omega^3}(X) = 1+X+X^2+X^3+X^4,$$
$$M_{\omega^5}(X) = 1+X+X^2, \quad M_{\omega^7}(X) = 1+X^3+X^4. \qquad \square$$

Пример 3.1.37. Таблица сложения поля $\mathbb{F}_{32} \simeq \mathbb{F}_2[X]/\langle 1+X^2+X^5\rangle$ выписана ниже. Выпишем минимальные многочлены в $\mathbb{F}_{32}$:

а) $1+X^2+X^5$ для сопряжённых элементов $\{\omega, \omega^2, \omega^4, \omega^8, \omega^{16}\}$,

б) $1+X^2+X^3+X^4+X^5$ для $\{\omega^3, \omega^6, \omega^{12}, \omega^{24}, \omega^{17}\}$,

в) $1+X+X^2+X^4+X^5$ для $\{\omega^5, \omega^{10}, \omega^{20}, \omega^9, \omega^{18}\}$,

г) $1+X+X^2+X^3+X^5$ для $\{\omega^7, \omega^{14}, \omega^{28}, \omega^{25}, \omega^{19}\}$,

д) $1+X+X^3+X^4+X^5$ для $\{\omega^{11}, \omega^{22}, \omega^{13}, \omega^{26}, \omega^{21}\}$, и наконец,

е) $1+X^3+X^5$ для $\{\omega^{15}, \omega^{30}, \omega^{29}, \omega^{27}, \omega^{23}\}$.

Порядок всех минимальных многочленов равен 31. Таблица 3.1.2 принимает вид

степень ω	вектор (слово)	степень ω	вектор (слово)
...	00000	15	11111
0	10000	16	11011
1	01000	17	11001
2	00100	18	11000
3	00010	19	01100
4	00001	20	00110
5	10100	21	00011
6	01010	22	10101
7	00101	23	11110
8	10110	24	01111
9	01011	25	10011
10	10001	26	11101
11	11100	27	11010
12	01110	28	01101
13	00111	29	10010
14	10111	30	01001

(3.1.9)

□

Определение 3.1.38. *Автоморфизм* поля $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$ (или, короче, $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-автоморфизм) — это биекция $\sigma\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ со следующими свойствами: а) $\sigma(a+b) = \sigma(a) + \sigma(b)$, б) $\sigma(ab) = \sigma(a)\sigma(b)$, в) $\sigma(c) = c\ \forall a,\ b \in \mathbb{F}_{q^n},\ c \in \mathbb{F}_q$. □

Теорема 3.1.39. *Множество* $(\mathbb{F}_{q^n}, \mathbb{F}_q)$*-автоморфизмов изоморфно циклической группе* $\mathbb{Z}_n$ *и порождено* отображением Фробениуса $\sigma_q(a) = a^q,\ a \in \mathbb{F}_{q^n}$.

Доказательство. Пусть $\omega \in \mathbb{F}_{q^n}$ — примитивный элемент. Тогда $\omega^{q^n-1} = e$ и $M_\omega(X) \in \mathbb{F}_q[X]$ имеет корни $\omega, \omega^q, \omega^{q^2}, \ldots, \omega^{q^{n-1}}$. Заметим, что $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-автоморфизм τ сохраняет коэффициенты многочлена $M_\omega(X)$ и переставляет его корни, поэтому $\tau(\omega) = \omega^{q^j}$ для некоторого j, $0 \leqslant j \leqslant n-1$. Но, поскольку ω — примитивный элемент, τ полностью определяется зна-

чением $\tau(\omega)$. Значит, так как $\sigma_{q^j}(\omega) = \omega^{q^j} = \tau(\omega)$, мы получаем равенство $\tau = \sigma_{q^j}$. □

Нам понадобятся некоторые факты о корнях из единицы, т. е. корнях многочлена $X^n - e$ над полем $\mathbb{F}_q$, где $q = p^l$ и $p = \mathrm{char}(\mathbb{F}_q)$. Не теряя общности, будем предполагать, что n и q взаимно просты, т. е.

$$\text{НОД}\,(n,\, q) = 1. \tag{3.1.10}$$

Действительно, если это не так, то можно написать, что $n = mp^k$. Тогда по лемме 3.1.5 имеем

$$X^n - e = X^{mp^k} - e = (X^m - e)^{p^k},$$

и наш анализ сводится к многочлену $X^m - e$.

Определение 3.1.40. Корни многочлена $(X^n - e) \in \mathbb{F}_q[X]$ в поле разложения $\mathrm{Spl}\big(X^n - e\big) = \mathbb{F}_{q^s}$ называются *корнями n-й степени из единицы* над $\mathbb{F}_q$ (или $(n, \mathbb{F}_q)$-корнями из единицы). Множество всех $(n, \mathbb{F}_q)$-корней из единицы обозначается символом $\mathsf{E}^{(n)}$. Получается, что значение s — наименьшее такое целое число $s \geqslant 1$, что $q^s = 1 \bmod n$. Этот факт отражён в обозначении s символом $\mathrm{ord}_n(q)$, который называется *порядком* элемента $q \bmod n$ (ср. теорему 3.1.44 ниже). □

В предположениях (3.1.10) многочлен $X^n - e$ не имеет кратных корней (поскольку производная $\partial_X(X^n - e) = nX^{n-1}$ не имеет корней в поле $\mathrm{Spl}\big(X^n - e\big) = \mathbb{F}_{q^s}$). Поэтому $\#\,\mathsf{E}^{(n)} = n$.

Теорема 3.1.41. *Группа $\mathsf{E}^{(n)}$ — циклическая подгруппа в $\mathbb{F}_{q^s}^*$.*

Доказательство. Предположим, что $\alpha, \beta \in \mathsf{E}^{(n)}$. Тогда $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = e$, т. е. $\alpha\beta^{-1} \in \mathsf{E}^{(n)}$, так что $\mathsf{E}^{(n)}$ — подгруппа циклической группы $\mathbb{F}_{q^s}^*$ и поэтому она тоже циклическая. □

Определение 3.1.42. Образующая группы $\mathsf{E}^{(n)}$ (т. е. корень из единицы степени n, мультипликативный порядок которой равен n) называется *примитивным* $(n, \mathbb{F}_q)$-корнем из единицы. Мы его будем обозначать через β. □

Следствие 3.1.43. *Существует ровно $\varphi(n)$, где φ — функция Эйлера, примитивных $(n, \mathbb{F}_q)$-корней из единицы. В частности, примитивный $(n, \mathbb{F}_q)$-корень из единицы существует для любого n, взаимно простого с q.*

Это позволяет нам вычислить s в поле разложения $\mathbb{F}_{q^s} = \mathrm{Spl}\big(X^n - e\big)$. Если β — примитивный $(n, \mathbb{F}_q)$-корень из единицы, то его мультипликативный порядок равен n. Поскольку $\beta \neq 0$, имеем $\beta \in \mathbb{F}_{q^r}$, если $\beta^{q^r} = \beta$, т. е. $\beta^{q^r - 1} = e$. Такое бывает тогда и только тогда, когда $n | (q^r - 1)$. Но s — это наименьшее r, при котором $\mathbb{F}_{q^r} \ni \beta$.

Примитивные корни утончённых желаний

(Из серии «Фильмы, которые не вышли на большой экран».)

Теорема 3.1.44. *Справедливо равенство* $\mathrm{Spl}\bigl(X^n - e\bigr) = \mathbb{F}_{q^s}$, *где* $s = \mathrm{ord}_n(q)$ — *наименьшее натуральное число, для которого* $n \mid (q^s - 1)$, *т. е.* $q^s = 1 \bmod n$.

Полезно подчеркнуть сходство и различия между примитивными элементами и примитивными $(n, \mathbb{F}_q)$-корнями из единицы в поле F_{q^s}, $s = \mathrm{ord}_n(q)$. Примитивный элемент поля ω порождает циклическую группу $\mathbb{F}_{q^s}^* = \{e, \omega, \ldots, \omega^{q^s-2}\}$; его мультипликативный порядок равен $q^s - 1$. Примитивный корень из единицы β порождает мультипликативную циклическую группу $\mathsf{E}^{(n)} = \{e, \beta, \ldots, \beta^{n-1}\}$; его мультипликативный порядок равен n. (С другой стороны, β порождает $\mathbb{F}_{q^s}$ как элемент поля: $\mathbb{F}_{q^s} = \mathbb{F}_q(\beta) = \mathbb{F}_q(\mathsf{E}^{(n)})$.) Это говорит о том, что $\beta = \omega$ тогда и только тогда, когда $n = q^s - 1$. Действительно, выясним, при каких условиях ω^k является примитивным корнем n-й степени из единицы. Как мы узнали из примера 3.1.33, такое бывает, когда $n \mid (q^s - 1)$, т. е. $q^s - 1 = nr$. На самом деле если $k \geqslant 1$, таково, что

$$\mathrm{НОД}\,(k,\, nr) = \mathrm{НОД}\,(k,\, q^s - 1) = r,$$

то элемент ω^k — примитивный корень степени n из единицы, поскольку его мультипликативный порядок равен

$$\frac{q^s - 1}{\mathrm{НОД}\,(k,\, q^s - 1)} = \frac{nr}{r} = n.$$

Это выполнено, когда $k = ru$ и u взаимно просто с n. Обратно, если ω^k — примитивный корень из единицы, то $\mathrm{НОД}\,(k, q^s - 1) = (q^s - 1)/n$. Следовательно, имеет место следующий результат.

Теорема 3.1.45. *Пусть* $\mathsf{P}^{(n)}$ — *множество примитивных* $(n, \mathbb{F}_q)$-*корней из единицы и* $\mathbb{T}^{(n)}$ — *множество примитивных элементов в поле* $\mathbb{F}_{q^s} = \mathrm{Spl}\bigl(X^n - e\bigr)$. *Тогда либо* 1) $\mathsf{P}^{(n)} \cap \mathbb{T}^{(n)} = \varnothing$, *либо* 2) $\mathsf{P}^{(n)} = \mathbb{T}^{(n)}$; *случай* 2) *имеет место тогда и только тогда, когда* $n = q^s - 1$.

Теперь мы можем разложить многочлен $X^n - e$ над $\mathbb{F}_q$, взяв произведение различных минимальных многочленов для $(n, \mathbb{F}_q)$-корней из единицы:

$$X^n - e = \mathrm{НОК}\,\bigl(M_\beta(X) \colon \beta \in \mathsf{E}^{(n)}\bigr). \tag{3.1.11a}$$

Если мы начинаем с примитивного элемента $\omega \in \mathbb{F}_{q^s}$, где $s = \mathrm{ord}_n(q)$, то $\beta = \omega^{(q^s-1)/n}$ — примитивный корень из единицы и $\mathsf{E}^{(n)} = \{e, \beta, \ldots, \beta^{n-1}\}$.

Это даёт возможность вычислить минимальный многочлен $M_{\beta^i}(X)$. Для всех $i = 0, \ldots, n-1$ сопряжёнными к β^i являются элементы $\beta^i, \beta^{iq}, \ldots, \beta^{iq^{d-1}} = e$, где $d\ (= d(i))$ — наименьшее натуральное число, для

которого $\beta^{iq^d} = \beta^i$, т. е. $\beta^{iq^d - i} = e$. Это равносильно тому, что $n|(id^d - i)$, т. е. $iq^d = i \bmod n$. Следовательно,

$$M_i(X)(= M_{\beta^i}(X)) = (X - \beta^i)(X - \beta^{iq}) \dots (X - \beta^{iq^{d-1}}) \qquad (3.1.11б)$$

Определение 3.1.46. Множество показателей $i, iq, \dots, iq^{d-1}$, где d $(= d(i))$ — минимальное натуральное число, для которого $iq^d = i \bmod n$, называется *циклотомическим классом* (для i) и обозначается C_i $(= C_i(n, q))$ (в качестве альтернативы C_{ω^i} обозначает множество ненулевых элементов поля $\omega^i, \omega^{iq}, \dots, \omega^{iq^{d-1}}$). □

Пример 3.1.47. Проверьте, что многочлены $X^2 + X + 2$ и $X^3 + 2X^2 + 1$ примитивны над полем $\mathbb{F}_3$ и вычислите таблицы сложения для полей $\mathbb{F}_9$ и $\mathbb{F}_{27}$, порождённых этими многочленами.

Решение. Поле $\mathbb{F}_9$ изоморфно полю $\mathbb{F}_3[X]/\langle X^2 + X + 2\rangle$. Мультипликативными степенями элемента $\omega \sim X$ являются элементы

$$\omega^2 \sim 2X + 1, \quad \omega^3 \sim 2X + 2, \quad \omega^4 \sim 2,$$
$$\omega^5 \sim 2X, \quad \omega^6 \sim X + 2, \quad \omega^7 \sim X + 1, \quad \omega^8 \sim 1.$$

Циклотомический класс элемента ω равен $\{\omega, \omega^3\}$ (поскольку $\omega^9 = \omega$). Тогда минимальный многочлен равен

$$M_\omega(X) = (X - \omega)(X - \omega^3) = X^2 - (\omega + \omega^3)X + \omega^4 = = X^2 - 2X + 2 = X^2 + X + 2.$$

Следовательно, $X^2 + X + 2$ — примитивный многочлен.

Далее, $\mathbb{F}_{27} \simeq \mathbb{F}_3[X]/\langle X^3 + 2X^2 + 1\rangle$ и для $\omega \sim X$ мы имеем

$$\omega^2 \sim X^2, \quad \omega^3 \sim X^2 + 2, \quad \omega^4 \sim X^2 + 2X + 2, \quad \omega^5 \sim 2X + 2,$$
$$\omega^6 \sim 2X^2 + 2X, \quad \omega^7 \sim X^2 + 1, \quad \omega^8 \sim X^2 + X + 2,$$
$$\omega^9 \sim 2X^2 + 2X + 2, \quad \omega^{10} \sim X^2 + 2X + 1, \quad \omega^{11} \sim X + 2,$$
$$\omega^{12} \sim X^2 + 2X, \quad \omega^{13} \sim 2, \quad \omega^{14} \sim 2X, \quad \omega^{15} \sim 2X^2, \quad \omega^{16} \sim 2X^2 + 1,$$
$$\omega^{17} \sim 2X^2 + X + 1, \quad \omega^{18} \sim X + 1, \quad \omega^{19} \sim X^2 + X,$$
$$\omega^{20} \sim 2X^2 + 2, \quad \omega^{21} \sim 2X^2 + 2X + 1, \quad \omega^{22} \sim X^2 + X + 1,$$
$$\omega^{23} \sim 2X^2 + X + 2, \quad \omega^{24} \sim 2X + 1, \quad \omega^{25} \sim 2X^2 + X, \quad \omega^{26} \sim 1.$$

Циклотомический класс элемента ω в поле $\mathbb{F}_{27}$ совпадает с $\{\omega, \omega^3, \omega^9\}$. Значит, примитивный многочлен выглядит следующим образом:

$$M_\omega(X) = (X - \omega)(X - \omega^3)(X - \omega^9) =$$
$$= X^3 - (\omega + \omega^3 + \omega^9)X^2 + (\omega^4 + \omega^{10} + \omega^{12})X - \omega^{13} = X^3 + 2X^2 + 1,$$

что и требовалось.

Пример 3.1.48. 1. Рассмотрим многочлен $X^{15}-1$ над полем $\mathbb{F}_2$ (здесь $n=15$, $q=2$). Тогда $\omega=2$, $s=\operatorname{ord}_{15}(2)=4$ и $\operatorname{Spl}\bigl(X^{15}-1\bigr)=\mathbb{F}_{2^4}=\mathbb{F}_{16}$.

Многочлен $g(X)=1+X+X^4$ примитивный: любой его корень β — примитивный элемент в поле $\mathbb{F}_{16}$. Поэтому к примитивным $(15, \mathbb{F}_2)$-корням из единицы относятся элементы

$$\beta=\omega^{(2^4-1)/15}=\omega.$$

Значит, корни многочлена $X^{15}-1$ — это $1, \beta, \ldots, \beta^{14}$. Минимальный многочлен для них был вычислен в примере 3.1.36. Итак, у нас есть разложение

$$X^{15}-1=(1+X)(1+X+X^4)(1+X+X^2+X^3+X^4)\times \\ \times(1+X+X^2)(1+X^3+X^4).$$

2. Зная циклотомические классы, можно найти разложение многочлена X^n-1 на неприводимые множители. Например, возьмём многочлен X^9-1 над $\mathbb{F}_2$ (здесь $n=9$, $q=2$). Есть 3 циклотомических класса:

$$C_0=\{0\},\quad C_1=\{1, 2, 4, 8, 7, 5\},\quad C_3=\{3, 6\},$$

и соответствующие минимальные многочлены степеней 1, 6 и 2 соответственно:

$$1+X,\quad 1+X^3+X^6 \text{ и } 1+X+X^2.$$

Отсюда получаем

$$X^9-1=(1+X)(1+X+X^2)(1+X^3+X^6).$$

3. Проверим примитивность многочлена

$$g_1(X)=1+X+X^6$$

над $\mathbb{F}_2$ с $n=6$, $q=2$. Здесь $2^6-1=63=3^2\cdot 7$. Поскольку $63/3=21$, имеем $3^2|\operatorname{ord}(f(X)) \Leftrightarrow X^{21}-1\neq 0 \bmod (1+X+X^6)$. Но $X^{21}=1+X+X^3+X^4+X^5\neq 1 \bmod (1+X+X^6)$, откуда $3^2|\operatorname{ord}(f(X))$.

Далее, так как $63/7=9$, имеем $7|\operatorname{ord}(g_1(X)) \Leftrightarrow X^9-1\neq 0 \bmod (1+X+X^6)$. Но $X^9=X^4+X^3+1\neq 1 \bmod (1+X+X^6)$, откуда $7|\operatorname{ord}(g_1(X))$. Следовательно, $\operatorname{ord}(g_1(X))=63$, и многочлен $g_1(X)$ примитивен. Теорема 3.1.53, приведённая ниже, показывает, что степень любого неприводимого многочлена порядка 63 равна 6, так как $2^6=1 \bmod 63$.

4. Теперь рассмотрим многочлен

$$g_2(X)=1+X+X^2+X^4+X^6$$

тоже над полем $\mathbb{F}_2$ (здесь $n=6$, $q=2$, как и раньше). Здесь тоже $3^2|\operatorname{ord}(g_2(X)) \Leftrightarrow X^{21}\neq 1 \bmod (1+X+X^2+X^4+X^6)$. Однако в поле $\mathbb{F}_2$

имеет место представление

$$X^{21}-1=(1+X)(1+X+X^2)(1+X+X^3)(1+X^2+X^3)\times \\ \times(1+X+X^2+X^4+X^6)(1+X^2+X^4+X^5+X^6).$$

Следовательно, $X^{21}-1=0 \bmod (1+X+X^2+X^4+X^6)$. Значит, 3^2 не делит $\operatorname{ord}(g_2(X))$.

Далее, $3|\operatorname{ord}(g_2(X)) \Leftrightarrow X^7 \neq 1 \bmod (1+X+X^2+X^4+X^6)$. Так как $X^7 = X+X^2+X^3+X^5 \neq 1 \bmod (1+X+X^2+X^4+X^6)$, получаем, что 3 делит $\operatorname{ord}(g_2(X))$.

Наконец, $7|\operatorname{ord}(g(X)) \Leftrightarrow X^9 \neq 1 \bmod (1+X+X^2+X^4+X^6)$, и так как $X^9 = 1+X^2+X^4 \neq 1 \bmod (1+X+X^2+X^4+X^6)$, получаем, что 7 делит $\operatorname{ord}(g(X))$, откуда $\operatorname{ord}(g(X))=21$. □

Подведем итоги о минимальных многочленах и корнях из единицы. Мы знаем из теоремы 3.1.25, что для любого целого числа $d \geqslant 1$ и любого $q = p^d$, где p — простое число и d натуральное, существует примитивный многочлен степени d: $M_\omega(X)$, где ω — примитивный элемент поля $\mathbb{F}_{q^d}$. С другой стороны, корни любого неприводимого многочлена $g(X) \in \mathbb{F}_q[X]$ степени d лежат в поле $\operatorname{Spl}\big(g(X)\big) = \mathbb{F}_{q^d}$ и имеют один и тот же мультипликативный порядок, равный $\operatorname{ord}(g(X))$.

Теорема 3.1.49. *Пусть $g(X) \in \mathbb{F}_q[X]$ — неприводимый многочлен степени d и $\operatorname{ord}(g(X)) = l$. Тогда*

1) $l|(q^d-1)$,

2) $g(X)|(X^l-e)$,

3) *$l|n$ тогда и только тогда, когда $g(X)|(X^n-e)$,*

4) *l — такое наименьшее натуральное число, что $g(X)|(X^l-e)$.*

Доказательство. 1) Поле $\operatorname{Spl}\big(g(X)\big) = \mathbb{F}_{q^d}$, следовательно, каждый корень α многочлена $g(X)$ является корнем многочлена $X^{q^d-1}-e$, так что $\operatorname{ord}(\alpha)|(q^d-1)$.

2) Каждый корень α многочлена $g(X)$ в поле $\operatorname{Spl}\big(g(X)\big)$ имеет $\operatorname{ord}(\alpha)=l$ и поэтому является корнем многочлена (X^l-e). Значит, $g(X)|(X^l-e)$.

3) Если $g(X)|(X^n-e)$, то каждый корень многочлена $g(X)$ является корнем многочлена X^n-e, т. е. $\operatorname{ord}(\alpha)|n$, откуда $l|n$. Обратно, если $n=kl$, то $(X^l-e)|(X^{kl}-e)$ и $g(X)|(X^n-e)$ по п. 2)

4) следует из утверждения п. 3). □

Теорема 3.1.50. *Если $f(X) \in \mathbb{F}_q[X]$ — неприводимый многочлен степени d и порядка l, то $d = \operatorname{ord}_l(q)$.*

Доказательство. Если для $\alpha \in \mathbb{F}_{q^d}$ имеет место равенство $f(\alpha)=0$, то по теореме 3.1.29 получаем $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d} = \operatorname{Spl}\big(f(X)\big)$. Но α также являет-

ся $(l, \mathbb{F}_q)$-корнем из единицы, поэтому $\mathbb{F}_q(\alpha) = \mathbb{F}_q(\mathsf{E}^{(l)}) = \mathrm{Spl}\big(X^l - e\big) = \mathbb{F}_{q^s}$, где $s = \mathrm{ord}_l(q)$. Следовательно, $d = \mathrm{ord}_l(q)$. □

Пример 3.1.51. Привлекая отображение Фробениуса $\sigma\colon a \mapsto a^q$, докажите, что из каждого элемента $a \in \mathbb{F}_{q^n}$ извлекается единственный корень степени q^j, $j = 1, \ldots, n-1$.

Предположим, что $q = p^s$ нечётно. Покажите, что ровно из половины ненулевых элементов поля $\mathbb{F}_q$ извлекается квадратный корень.

Решение. Отображение Фробениуса $\sigma\colon a \mapsto a^q$ биективно. Поэтому для каждого $b \in \mathbb{F}_{q^n}$ найдётся единственный элемент a, для которого $a^q = b$ (корень степени q). Далее, j-я степень отображения Фробениуса $\sigma^j\colon a \mapsto a^{q^j}$ тоже биективно. Значит, для всех $b \in \mathbb{F}_{q^n}$ существует единственный элемент a со свойством $a^{q^j} = b$. Заметим, что $\forall c \in \mathbb{F}_q$ имеем $c^{1/q^j} = c$.

Теперь рассмотрим мультипликативный гомоморфизм из $\mathbb{F}_q^*$ в себя: $\tau\colon a \mapsto a^2$. Если q нечётно, то в группе $\mathbb{F}_q^* \simeq \mathbb{Z}_{q-1}$ насчитывается чётное число элементов $q-1$. Мы хотим показать, что если $\tau(a) = b$, то $\tau^{-1}(b)$ состоит из двух элементов, a и $-a$. Действительно, многочлен $X^2 - b$ над полем $\mathbb{F}_q$ имеет не более двух корней, поэтому $\tau(-a) = b$. Кроме того, если $\tau(a') = b$, то $\tau(a'a^{-1}) = e$.

Поэтому нам нужно проанализировать прообраз единицы $\tau^{-1}(e)$. Ясно, что $\pm e \in \tau^{-1}(e)$. С другой стороны, если ω — примитивный элемент, то $\tau(\omega^{(q-1)/2}) = \omega^{q-1} = e$ и $\tau^{-1}(e)$ состоит из $e = \omega^0$ и $\omega^{(q-1)/2} = -e$.

Если $\tau(a'a^{-1}) = e$, то $a'a^{-1} = \pm e$ и $a' = \pm a$. Следовательно, τ переводит ровно два элемента a и $-a$ в один и тот же, а значит образ $\tau(\mathbb{F}_q^*)$ занимает ровно половину всего поля $\mathbb{F}_q$. □

Теорема 3.1.52. *Пусть многочлен $p(X) \in \mathbb{F}_q[X]$ неприводим и имеет степень d. Положим $m = \mathrm{НОД}(d, q)$. Тогда $m \mid d$ и $p(X)$ разлагается над $\mathbb{F}_{q^d}$ на m неприводимых многочленов, степени d/m каждый. Следовательно, многочлен $p(X)$ неприводим над $\mathbb{F}_{q^d}$ тогда и только тогда, когда $m = 1$.*

Теорема 3.1.53. *Пусть* $\mathrm{НОД}(d, q) = 1$. *Число приведённых неприводимых многочленов порядка l и степени d равно $\varphi(l)/d$, если $l \geqslant 2$ и при этом степень $d = \mathrm{ord}_l(q)$; равно 2, если $l = d = 1$; и 0 во всех остальных случаях. В частности, степень неприводимого многочлена порядка l всегда равна $\mathrm{ord}_l(q)$, т.е. минимальному числу s, для которого $q^s = 1 \bmod l$.*

Доказательства теорем 3.1.52 и 3.1.53 мы опускаем (их можно найти в книге [LN]). Мы дадим лишь короткий комментарий к теореме 3.1.53. Если $p(0) \neq 0$, то порядок неприводимого многочлена $p(X)$ степени d совпадает с порядком любого его корня в мультипликативной группе $\mathbb{F}_{q^d}^*$.

Поэтому порядок равен l тогда и только тогда, когда $d = \mathrm{ord}_l(q)$ и $p(X)$ делит так называемый *круговой многочлен*

$$Q_l(X) = \prod_{s:\ \text{НОД}\,(s,l)=1} (X - \omega^s).$$

На самом деле круговой многочлен можно разложить в произведение неприводимых многочленов степени $d = \mathrm{ord}_l(q)$ и их число равно $\varphi(l)/d$. (В случае $d = l = 1$ многочлен $p(X) = X$ тоже нужно учитывать.)

В заключение этого параграфа мы дадим короткие резюме фактов из теории конечных полей, обсуждаемых выше.

Резюме 3.1.54. Поле — это кольцо, ненулевые элементы которого образуют коммутативную группу по умножению.

1. Любое конечное поле $\mathbb{F}$ состоит из $q = p^s$ элементов, где p — простое число, и $\mathrm{char}(\mathbb{F}) = p$.

2. Два конечных поля с одинаковым числом элементов изоморфны. Поэтому для данного $q = p^s$ существует единственное (с точностью до изоморфизма) поле мощности q; оно обозначается символом $\mathbb{F}_q$ (часто его называют полем Галуа размера q). Когда $q = p$ — простое число, поле $\mathbb{F}_q$ изоморфно аддитивной циклической группе $\mathbb{Z}_p$ из p элементов, оснащённой умножением по $\bmod p$.

3. Мультипликативная группа $\mathbb{F}_q^*$ ненулевых элементов поля $\mathbb{F}_q$ изоморфна аддитивной циклической группе $\mathbb{Z}_{q-1}$ из $q - 1$ элементов.

4. Поле $\mathbb{F}_q$ содержит подполе $\mathbb{F}_r$ тогда и только тогда, когда $r|q$; в этом случае $\mathbb{F}_q$ изоморфно линейному пространству над (с коэффициентами из) $\mathbb{F}_r$ размерности $\log_p(q/r)$. Таким образом, каждое простое число p даёт возрастающую последовательность конечных полей $\mathbb{F}_{p^s}$, $s = 1, 2, \ldots$ Элемент $\omega \in \mathbb{F}_q$, порождающий мультипликативную группу $\mathbb{F}_q^*$, называется примитивным элементом поля $\mathbb{F}_q$. □

Резюме 3.1.55. Полиномиальное кольцо над $\mathbb{F}_q$ обозначается символом $\mathbb{F}_q[X]$; если многочлены рассматриваются по модулю $g(X)$, фиксированного многочлена из $\mathbb{F}_q[X]$, то соответствующее кольцо обозначается $\mathbb{F}_q[X]/\langle g(X)\rangle$.

1. Кольцо $\mathbb{F}_q[X]/\langle g(X)\rangle$ является полем тогда и только тогда, когда многочлен $g(X)$ неприводим над $\mathbb{F}_q$ (т. е. не раскладывается в произведение $g(X) = g_1(X)g_2(X)$, где $\deg g_1(X)$, $\deg g_2(X) < \deg g(X)$.

2. Для любого q и натурального числа d существует неприводимый многочлен $g(X)$ над $\mathbb{F}_q$ степени d.

3. Если многочлен $g(X)$ неприводим и его степень равна d, то мощность поля $\mathbb{F}_q[X]/\langle g(X)\rangle$ равна q^d, т. е. $\mathbb{F}_q[X]/\langle g(X)\rangle$ изоморфно полю $\mathbb{F}_{q^d}$ и лежит в той же последовательности полей, что и $\mathbb{F}_q$ (т. е. $\mathrm{char}(\mathbb{F}_{q^d}) = \mathrm{char}(\mathbb{F}_q)$). □

Резюме 3.1.56. Расширение поля $\mathbb{F}_q$ конечным числом элементов $\alpha_1, \ldots, \alpha_d$ (содержащихся в бóльшем поле из той же последовательности) — это наименьшее поле, содержащее как $\mathbb{F}_q$, так и α_i, $1 \leqslant i \leqslant d$. Такое поле обозначается символом $\mathbb{F}_q(\alpha_1, \ldots, \alpha_d)$.

1. Для любого приведённого многочлена $p(X) \in \mathbb{F}_q[X]$ существует такое бóльшее поле $\mathbb{F}_{q'}$ из той же последовательности, что и $\mathbb{F}_q$, что $p(X)$ разлагается над $\mathbb{F}_{q'}$:

$$p(X) = \prod_{j=1}^{d} (X - \alpha_j), \quad d = \deg p(X), \quad \alpha_1, \ldots, \alpha_d \in \mathbb{F}_{q'}. \tag{3.1.12}$$

Наименьшее поле $\mathbb{F}_{q'}$ с таким свойством (т. е. поле $\mathbb{F}_q(\alpha_1, \ldots, \alpha_d)$) называется *полем разложения* многочлена $p(X)$; мы также говорим, что $p(X)$ разлагается над $\mathbb{F}_q(\alpha_1, \ldots, \alpha_d)$ на линейные множители. Поле разложения многочлена $p(X)$ обозначается символом $\operatorname{Spl}\bigl(p(X)\bigr)$, элемент $\alpha \in \operatorname{Spl}\bigl(p(X)\bigr)$ участвует в разложении (3.1.12) тогда и только тогда, когда $p(\alpha) = 0$. Поле $\operatorname{Spl}\bigl(p(X)\bigr)$ можно описать как множество $\{g(\alpha_j)\}$, где $j = 1, \ldots, d$ и $g(X) \in \mathbb{F}_q[X]$ — многочлены степени меньше $\deg(p(X))$.

2. Поле $\mathbb{F}_q$ является полем разложения многочлена $\mathbf{X}^q - X$.

3. Если многочлен $p(X)$ степени d неприводим над $\mathbb{F}_q$ и α — его корень в поле $\operatorname{Spl}\bigl(p(X)\bigr)$, то $\mathbb{F}_{q^d} \simeq \mathbb{F}_q[X]/\langle p(X)\rangle$ изоморфно полю $\mathbb{F}_q(\alpha)$ и все корни многочлена $p(X)$ из $\operatorname{Spl}\bigl(p(X)\bigr)$ совпадают с сопряжёнными элементами $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. Таким образом, d — наименьшее натуральное число, для которого $\alpha^{q^d} = \alpha$.

4. Предположим, что для приведённого многочлена $p(X) \in \mathbb{F}_q[X]$ и элемента α из некоторого бóльшего поля мы имеем $p(\alpha) = 0$. Тогда существует единственный минимальный многочлен $M_\alpha(X)$ со свойством $M_\alpha(\alpha) = 0$ (т. е. такой, что любой многочлен $p(X)$, для которого $p(\alpha) = 0$, делится на $M_\alpha(X)$). Многочлен $M_\alpha(X)$ — единственный неприводимый многочлен над $\mathbb{F}_q$, имеющий корень α. Он также является единственным многочленом минимальной степени с корнем α. Мы называем $M_\alpha(X)$ минимальным многочленом α над $\mathbb{F}_q$. Если ω — примитивный элемент поля $\mathbb{F}_{q^d}$, то многочлен $M_\omega(X)$ называется примитивным многочленом поля $\mathbb{F}_{q^d}$ над $\mathbb{F}_q$. Элементы $\alpha, \beta \in \mathbb{F}_{q^d}$ называются сопряжёнными над $\mathbb{F}_q$, если у них один и тот же минимальный многочлен над $\mathbb{F}_q$.

5. Сопряжённые элементы к $\alpha \in \mathbb{F}_{q^d}$ над $\mathbb{F}_q$ исчерпываются списком: $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, где d — минимальное натуральное число, для которого $\alpha^{q^d} = \alpha$. Когда $\alpha = \omega^i$, где ω — примитивный элемент, класс сопряжённых элементов ассоциирован с циклотомическим классом $C_{\omega^i} = \{\omega^i, \omega^{iq}, \ldots, \omega^{iq^{d-1}}\}$. □

Резюме 3.1.57. Теперь предположим, что n и $q = p^s$ взаимно просты и рассмотрим многочлен $X^n - e$. Его корни в поле разложения $\mathrm{Spl}\big(X^n - e\big)$ называются корнями n-й степени из единицы над $\mathbb{F}_q$. Множество всех таких корней обозначается E_n.

1. Множество E_n является циклической подгруппой порядка n в мультипликативной группе поля $\mathrm{Spl}\big(X^n - e\big)$. Корень степени n из единицы, порождающий E_n, называется примитивным корнем из единицы степени n.

2. Если $\mathbb{F}_{q^s} = \mathrm{Spl}\big(X^n - e\big)$, то s — наименьшее натуральное число, при котором $n|(q^s - 1)$.

3. Пусть Π_n — множество примитивных корней степени n из единицы над полем $\mathbb{F}_q$ и Φ_n — множество примитивных элементов поля $\mathbb{F}_{q^s} = \mathrm{Spl}\big(X^n - e\big)$. Тогда либо $\Pi_n \cap \Phi_n = \varnothing$, либо $\Pi_n = \Phi_n$, причём последнее равенство имеет место тогда и только тогда, когда $n = q^s - 1$. □

§ 3.2. Коды Рида—Соломона. Развитие теории БЧХ-кодов

> Специалист по циклическим кодам делает это, пока не зациклится.
>
> (Из серии «Как они делают это».)

Как обычно, конечное поле $\mathbb{F}_q$ рассматривается с точностью до изоморфизма, но иногда нам будет нужна конкретная таблица поля (например, при отождествлении $\mathbb{F}_{p^d}$ с $\mathbb{F}_p[X]/\langle g(X)\rangle$, где $g(X) \in \mathbb{F}_p[X]$ — неприводимый многочлен степени d).

В определении 2.5.38 мы ввели двоичные БЧХ-коды в узком смысле. Общие БЧХ-коды $\mathcal{X}_{q,N,\delta,\omega,b}$ над полем $\mathbb{F}_q$ длины N с проектируемым расстоянием δ и нулями $\omega^b, \dots, \omega^{b+\delta-1}$ вводятся дальше, в определении 3.2.7. Мы же начнём с интересного специального класса, сформированного *кодами Рида—Соломона* (РС), они относятся к кодам с максимальным достижимым расстоянием (м. д. р.).

Определение 3.2.1. q-ичным кодом Рида—Соломона ($q \geqslant 3$) называется циклический код длины $N = q - 1$ с порождающим полиномом

$$g(X) = (X - \omega^b)(X - \omega^{b+1}) \dots (X - \omega^{b+\delta-2}), \tag{3.2.1}$$

где $\delta < q - 1$, ω — примитивный элемент группы $\mathbb{F}_q^*$ и $b \in \mathbb{F}_q^*$. Он обозначается $\mathcal{X}^{\mathrm{PC}} (= \mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b})$. □

Согласно определению 3.2.7, приведённому ниже, код Рида—Соломона — это $\mathcal{X}_{q,q-1,\delta,\omega,b}$, т. е. q-ичный БЧХ-код длины $q - 1$ и с проектируемым

расстоянием δ. Не существует разумных двоичных РС-кодов, имеющих в этом случае длину $N = q - 1 = 1$. Заметим, что длина q-ичного $\mathcal{X}^{\mathrm{PC}}$ равна числу ненулевых элементов в поле алфавита $\mathbb{F}_q$. Для $N = q - 1$ мы имеем:

$$X^{q-1} - e = \prod_{\alpha \in \mathbb{F}_q^*} (X - \alpha)$$

(так как поле разложения $\mathrm{Spl}\big(X^q - X\big) = \mathbb{F}_q$). Если ω — примитивный $(q-1, \mathbb{F}_q)$-корень из единицы (т. е. примитивный элемент из $\mathbb{F}_q^*$), то $M_i(X) = X - \omega^i$.

К важным свойствам РС-кодов относится то, что они удовлетворяют оценке м. д. р. (кодами с максимальным достижимым расстоянием). Действительно, порождающий полином кода $\mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b}$ имеет степень $\deg g(X) = \delta - 1$. Следовательно,

$$k = \dim(\mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b}) = N - \deg g(X) = N - \delta + 1. \tag{3.2.2}$$

По лемме 2.3.8 (граница БЧХ) минимальное расстояние удовлетворяет оценке $d(\mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b}) \geqslant \delta = N - k + 1$. Но по неравенству Синглтона $d(\mathcal{X}^{\mathrm{PC}}) \leqslant N - k + 1$, откуда

$$d(\mathcal{X}^{\mathrm{PC}}) = N - k + 1 = \delta. \tag{3.2.3}$$

Таким образом, РС-коды обладают наибольшим из возможных минимальных расстояний среди q-ичных кодов длины $N = q - 1$ размерности $k = N - \delta + 1$. Подводя итог, получаем теорему.

Теорема 3.2.2. *Код $\mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b}$ является м. д. р. и имеет расстояние $d(\mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b}) = \delta$.*

Доказательство. Для РС-кода $\delta = N - k + 1$. Однако $\delta \leqslant N - k + 1$ по неравенству Синглтона. □

Двойственный к БЧХ-коду не всегда оказывается БЧХ-кодом. Однако справедлива следующая теорема.

Теорема 3.2.3. *Двойственный к* РС-*коду является* РС-*кодом.*

Доказательство следует из прямого вычисления, поскольку $(\mathcal{X}^{\mathrm{PC}}_{q,\delta,\omega,b})^{\perp} = \mathcal{X}^{\mathrm{PC}}_{q,q-\delta,\omega,b+\delta-1}$. □

Теорема 3.2.4. *Пусть $\mathcal{X}^{\mathrm{PC}}$ — $[N, k, \delta]$ — РС-код. Тогда его расширение проверкой на чётность является $[N+1, k, \delta+1]$-кодом с расстоянием на* 1 *большим, чем у исходного кода.*

Доказательство. Пусть $c(X) = c_0 + c_1 X + \ldots + c_{N-1} X^{N-1} \in \mathcal{X}^{\mathrm{PC}}$ с весом $w(c(X)) = \delta$. Его расширение равно $\hat{c}(X) = c(X) + c_N X^N$, где $c_N =$

$= -\sum_{i=0}^{N-1} c_i = -c(e)$. Мы хотим показать, что $c(e) \neq 0$ и поэтому $w(\hat{c}(X)) = \delta + 1$.

Для упрощения обозначений предположим, что $b = 1$, и запишем порождающий полином кода $\mathcal{X}^{\mathrm{PC}}$ как $g(X) = (X - \omega)(X - \omega^2) \dots (X - \omega^{\delta-1})$. Тогда $c(X) = g(X)p(X)$ для некоторого $p(X)$ и $c(e) = g(e)p(e)$. Ясно, что $g(e) \neq 0$, так как $\omega^i \neq e$ для всех $i = 1, \dots, \delta - 1$. Если $p(e) = 0$, то многочлен $g_1(X) = (X - e)g(X)$ делит $c(X)$. Значит, $c(X) \in \langle g_1(X) \rangle$, где $g_1(X) = (X - e)(X - \omega) \dots (X - \omega^{\delta-1})$, т. е. $\langle g_1(X) \rangle$ — БЧХ-код с проектируемым расстоянием не меньше $\delta + 1$. Но это противоречит выбору $c(X)$. □

РС-коды допускают специфические (и элегантные) процедуры кодирования и декодирования. Пусть $\mathcal{X}^{\mathrm{PC}}$ — $[N, k, \delta]$-РС-код, $N = q - 1$. Для строки сообщения $a_0 \dots a_{k-1}$ положим $a(X) = \sum_{i=0}^{k-1} a_i X^i$ и закодируем $a(X)$ как $c(X) = \sum_{j=0}^{N-1} a(\omega^j) X^j$. Чтобы доказать включение $c(X) \in \mathcal{X}^{\mathrm{PC}}$, нам следует проверить, что $c(\omega) = \dots = c(\omega^{\delta-1}) = 0$. Представим $a(X)$ как многочлен $\sum_{i=0}^{N-1} a_i X^i$ с $a_i = 0$ при $i \geqslant k$ и воспользуемся следующей леммой.

Лемма 3.2.5. *Пусть* $a(X) = a_0 + a_1 X + \dots + a_{N-1} X^{N-1} \in \mathbb{F}_q[X]$ *и* ω — *примитивный* $(N, \mathbb{F}_q)$*-корень из единицы*, $N = q - 1$. *Тогда*

$$a_i = \frac{1}{N} \sum_{j=0}^{N-1} a(\omega^j) \omega^{-ij}. \tag{3.2.4}$$

Доказательство представлено после леммы 3.2.12. □

Действительно, по лемме 3.2.5 имеем

$$a_i = \frac{1}{N} \sum_{j=0}^{N-1} a(\omega^j) \omega^{-ij} = \frac{1}{N} c(\omega^{-i}) = \frac{1}{N} c(\omega^{N-i}),$$

откуда $c(\omega^j) = N a_{N-j}$. Для $0 \leqslant j \leqslant \delta - 1 = N - k$ справедливо равенство $c(\omega^j) = N a_{N-j} = 0$. Следовательно, $c(X) \in \mathcal{X}^{\mathrm{PC}}$. Кроме того, исходное сообщение легко восстановить из $c(X)$: $a_i = \frac{1}{N} c(\omega^{N-i})$.

Для декодирования полученного слова $u(X) = c(X) + e(X)$ запишем

$$u_i = c_i + e_i = e_i + a(\omega^i), \quad 0 \leqslant i \leqslant N - 1.$$

После этого получим

$$
\begin{aligned}
u_0 &= e_0 + a_0 + a_1 + \ldots + a_{k-1},\\
u_1 &= e_1 + a_0 + a_1\omega + \ldots + a_{k-1}\omega^{k-1},\\
u_2 &= e_2 + a_0 + a_1\omega^2 + \ldots + a_{k-1}\omega^{2(k-1)},\\
&\vdots\\
u_{N-1} &= e_{N-1} + a_0 + a_1\omega^{N-1} + \ldots + a_{k-1}\omega^{(N-1)(k-1)}.
\end{aligned}
$$

Если ошибок нет, т. е. $e_0 = \ldots = e_{k-1} = 0$, то любые k из этих уравнений можно разрешить относительно k неизвестных $a_0, \ldots, a_{k-1}$, поскольку соответствующая матрица — это матрица Вандермонда. На самом деле любую подсистему из k уравнений можно решить для любого вектора ошибок (другое дело, будет ли решение давать правильную строку $a_0, \ldots, a_{k-1}$, или нет).

Предположим теперь, что в сообщение закралось t ошибок, $t < N - k$. Уравнения с $e_i = 0$ будем называть хорошими, а с $e_i \neq 0$ — плохими, тогда у нас есть t плохих и $N - t$ хороших уравнений. Если мы решим все подсистемы из k уравнений, то C^k_{N-t} подсистем, состоящих из k хороших уравнений, будут давать правильные значения неизвестных a_i. Более того, данное неверное решение не может удовлетворять никакому множеству из k хороших уравнений; оно может удовлетворять только $k - 1$ хорошему уравнению. Таким образом, оно является решением не более чем $t + k - 1$ уравнений, т. е. может быть получено не более чем C^k_{t+k-1} раз из системы k уравнений. Значит, если

$$C^k_{N-t} > C^k_{t+k-1},$$

то большинство из C^k_N решений дают верные значения коэффициентов a_i. Последнее неравенство выполняется тогда и только тогда, когда $N - t > t + k - 1$, т. е. $\delta = N - k + 1 > 2t$.

Теорема 3.2.6. *Для* $[N, k, \delta]$ РС-*кода* $\mathcal{X}^{\mathrm{PC}}$ *логическое декодирование по правилу большинства исправляет до* $t < \delta/2$ *ошибок за счёт решения* C^k_N *систем уравнений размера* $k \times k$.

Коды Рида—Соломона были открыты в 1960 г. Ирвингом Ридом и Густавом Соломоном; в то время они оба работали в лаборатории Линкольна при MIT. На момент опубликования их совместной статьи с описанием нового класса кодов, эффективные алгоритмы декодирования этих кодов оставались неизвестными. Первый такой алгоритм был найден в 1969 г. Элвином Берлекэмпом (Elwyn Berlekamp) и Джеймсом Мэсси (James Massey) и получил название алгоритма Берлекэмпа—Мэсси. См. § 3.3, а также [?]. Впоследствии были обнаружены и другие алгоритмы: алгоритм непрерывных дробей и Евклидов алгоритм: см. [McE3].

Коды Рида—Соломона играли важную роль в передаче цифровых изображений с американских космических кораблей в 1970–1980-х гг., часто в комбинации с другими кодовыми

конструкциями. Эти коды до сих пор заметным образом используются при космических полётах, несмотря на то, что развитие *турбо-кодов* предоставило гораздо более широкий выбор процедур кодирования и декодирования. Коды Рида—Соломона также играют ключевую роль в производстве компакт-дисков и компьютерных игр. Используемые здесь схемы кодирования и декодирования способны исправить серии ошибок длиной до 4000 знаков (что занимает около 2,5 мм на поверхности диска).

Густав Соломон (1930–1996) защитил диссертацию в MIT в 1956 г. под руководством Кенкити Ивасава (Kenkichi Iwasawa), известного специалиста по теории алгебраических групп. Помимо конструкции кодов RC, Соломон участвовал в открытии полиномов Маттсона—Соломона (см. ниже) и является соавтором весовых формул Соломона—Мак-Элайеса.

В поздний период своей жизни Соломон работал консультантом в Jet-Propulsion Laboratory (JPL) в Пасадене. Он был приверженным поклонником оперы и театра. Согласно сведениями из Википедии в свободное время Соломон преподавал английский язык инженерам-иностранцам, работавшим в JPL, демонстрируя слушателям различные образцы американской продукции, как современной, так и более традиционной. Кроме того, он был последователем школы улучшения здоровья и самолечения с помощью специальной техники дыхания. Соломон также являлся знатоком философской теории, связанной с популярной методикой Фельденкрайза (Moshé Feldenkrais). У него была сильная привязанность к музыке как в качестве обычного слушателя, так и в качестве композитора-любителя.

Коды БЧХ (в широком смысле) определяются следующим образом.

Определение 3.2.7. БЧХ-код $\mathcal{X}_{q,N,\delta,\omega,b}$ с параметрами q, N, δ, ω, b — это циклический код $\mathcal{X}_N = \langle g(X)\rangle$ длины N и с проектируемым расстоянием δ, порождённый многочленом

$$g(X) = \text{НОК}\,(M_{\omega^b}(X),\, M_{\omega^{b+1}}(X),\, \ldots,\, M_{\omega^{b+\delta-2}}(X)), \tag{3.2.5}$$

т. е.

$$\mathcal{X}_{q,N,\delta,\omega,b} = \{c(X) \in \mathbb{F}_2[X] \bmod (X^N - 1)\colon c(\omega^{b+i}) = 0,\ \ 0 \leqslant i \leqslant \delta - 1\}.$$

Если $b = 1$, то это *БЧХ-код в узком смысле*. Если ω — примитивный корень из единицы степени N, т. е. примитивный корень многочлена $X^N - 1$, то БЧХ-код называется *примитивным*. (Напомним, что при условии НОД $(q, N) = 1$ эти корни образуют циклическую мультипликативную группу порядка N и ω — образующая этой группы.) □

Лемма 3.2.8. *Минимальное расстояние БЧХ-кода $\mathcal{X}_{q,N,\delta,\omega,b}$ не меньше чем δ.*

Доказательство. Не ограничивая общности рассмотрим код в узком смысле. Положим проверочную $((\delta - 1) \times N)$-матрицу

$$H = \begin{pmatrix} 1 & \omega & \omega^2 & \ldots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(N-1)} \\ \vdots & \vdots & \ddots & \vdots & \\ 1 & \omega^{\delta-1} & \omega^{2(\delta-1)} & \ldots & \omega^{(N-1)(\delta-1)} \end{pmatrix}.$$

Кодовые слова кода $\mathcal{X}$ — это соотношения линейной зависимости на столбцы матрицы H. Из леммы 2.5.41 следует, что любые $\delta - 1$ столбца в H

линейно независимы. Действительно, выберем столбцы с элементами из первой строки $\omega^{k_1}, \ldots, \omega^{k_{\delta-1}}$, где $0 < k_1 \ldots < k_{\delta-1} < N-1$. Из них получается квадратная матрица

$$D = \begin{pmatrix} \omega^{k_1}\cdot 1 & \omega^{k_2}\cdot 1 & \ldots & \omega^{k_{\delta-1}}\cdot 1 \\ \omega^{k_1}\cdot\omega^{k_1} & \omega^{k_2}\cdot\omega^{k_2} & \ldots & \omega^{k_{\delta-1}}\cdot\omega^{k_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{k_1}\cdot\omega^{k_1(\delta-2)} & \omega^{k_2}\cdot\omega^{k_2(\delta-2)} & \ldots & \omega^{k_{\delta-1}}\cdot\omega^{k_{\delta-1}(\delta-2)} \end{pmatrix}$$

размера $(\delta-1)\times(\delta-1)$, отличающаяся от матрицы Вандермонда множителем ω^{k_s} в s-м столбце. Поэтому её определитель равен

$$\det Q = \left(\prod_{s=1}^{\delta-1}\omega^{k_s}\right)\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \omega^{k_1} & \omega^{k_2} & \ldots & \omega^{k_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{k_1(\delta-2)} & \omega^{k_2(\delta-2)} & \ldots & \omega^{k_{\delta-1}(\delta-2)} \end{vmatrix} =$$

$$= \left(\prod_{s=1}^{\delta-1}\omega^{k_s}\right)\times\left(\prod_{i>j}(\omega^{k_i}-\omega^{k_j})\right)\neq 0.$$

Отсюда следует, что любые наборы $\delta-1$ столбцов матрицы H действительно линейно независимы. Это, в свою очередь, означает, что вес любого кодового слова из $\mathcal{X}$ по крайней мере δ, а значит, минимальное расстояние этого кода не менее δ. □

Пример 3.2.9 (обобщение неравенства БЧХ). Пусть ω — примитивный корень из единицы степени N и b, $r \geqslant 1$, $\delta > 2$ — целые числа, причём НОД$(r, N) = 1$. Рассмотрим циклический код $\mathcal{X} = \langle g(X)\rangle$ длины N, где $g(X)$ — приведённый многочлен минимальной степени со свойством $g(\omega^b) = g(\omega^{b+r}) = g(\omega^{b+(\delta-2)r}) = 0$. Докажите, что расстояние кода $\mathcal{X}$ подчиняется неравенству $d(\mathcal{X}) \geqslant \delta$.

Решение. Так как НОД$(r, N) = 1$, получаем, что ω^r — примитивный корень из единицы. Поэтому можно повторить предыдущее доказательство: матрица

$$H^T = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \omega^b & \omega^{b+r} & \ldots & \omega^{b+(\delta-2)r} \\ \omega^{2b} & \omega^{2(b+r)} & \ldots & \omega^{2(b+(\delta-2)r)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{(N-1)b} & \omega^{(N-1)b+r} & \ldots & \omega^{(N-1)(b+(\delta-2)r)} \end{pmatrix}$$

размера $N\times(\delta-1)$ служит проверочной для кода $\mathcal{X} = \langle g(X)\rangle$. Возьмём любую её подматрицу размера $(\delta-1)\times(\delta-1)$, скажем, со строками $i_1 <$

$< i_2 < \ldots < i_{\delta-1}$. Обозначим её через $K_{\underline{i}}$. Тогда

$$\det K_{\underline{i}} = \prod_{l=1}^{\delta-1} \omega^{(i_l-1)b} \det(\omega^{r(i_j-1)k}) = \prod_{l=1}^{\delta-1} \omega^{(i_l-1)b} \det \text{ (Вандермонда)} \neq 0.$$

Таким образом, $d(\mathcal{X}) \geqslant \delta$. □

Пример 3.2.10. Пусть ω — примитивный корень из единицы степени n в некотором расширении поля $\mathbb{F}_q$ и $a(X) = \sum\limits_{i=0}^{n-1} a_i X^i$ — многочлен степени не более чем $n-1$. *Многочлен Маттсона—Соломона* определяется формулой

$$a_{\mathrm{MS}}(X) = \sum_{j=0}^{n-1} a(\omega^j) X^{n-j}. \tag{3.2.6}$$

Пусть $q = 2$ и $a(X) \in \mathbb{F}_2[X]/\langle X^n - 1\rangle$. Докажите, что многочлен Маттсона—Соломона $a_{\mathrm{MS}}(X)$ является идемпотентом, т. е. $a_{\mathrm{MS}}(X)^2 = a_{\mathrm{MS}}(X)$ в поле $\mathbb{F}_2[X]/\langle X^n - 1\rangle$.

Решение. Пусть $a(X) = \sum\limits_{i=0}^{n-1} a_i X^i$, тогда $na_i = a_{\mathrm{MS}}(\omega^{-i})$, $0 \leqslant i \leqslant n-1$, по лемме 3.2.5. В поле $\mathbb{F}_2$ выполнено равенство $(na_i)^2 = na_i$, поэтому $a_{\mathrm{MS}}(\omega^{-i})^2 = a_{\mathrm{MS}}(\omega^{-i})$. Квадрат многочлена в кольце $\mathbb{F}_2[X]$ будем обозначать через $b^{(2)}(X)$, а в кольце $\mathbb{F}_2[X]/\langle X^n - 1\rangle$ — через $b(X)^2$:

$$b^{(2)}(X) = c(X)(X^n - 1) + b(X)^2.$$

Тогда

$$a_{\mathrm{MS}}(X) \mid_{X=\omega^i} = (a_{\mathrm{MS}}(X) \mid_{X=\omega^i})^2 = a^{(2)}_{\mathrm{MS}}(X) \mid_{X=\omega^i} = a_{\mathrm{MS}}(X)^2 \mid_{X=\omega^i},$$

т. е. многочлены $a_{\mathrm{MS}}(X)$ и $a_{\mathrm{MS}}(X)^2$ согласованы в точках $\omega^0 = e$, ω, $\ldots$ $\ldots$, ω^{n-1}. В терминах полиномов

$$a_{\mathrm{MS}}(X) = a_{0,\mathrm{MS}} + a_{1,\mathrm{MS}} X + \ldots + a_{n-1,\mathrm{MS}} X^{n-1},$$
$$a_{\mathrm{MS}}(X)^2 = a'_{0,\mathrm{MS}} X + \ldots + a'_{n-1,\mathrm{MS}} X^{n-1}$$

этот факт записывается в матричном виде:

$$(a_{\mathrm{MS}} - a^{(2)'}_{\mathrm{MS}}) \begin{pmatrix} e & e & \ldots & e \\ e & \omega & \ldots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ e & \omega^{n-1} & \ldots & \omega^{(n-1)^2} \end{pmatrix} = 0.$$

Так как это матрица Вандермонда, её определитель равен

$$\prod_{0\leqslant i<j\leqslant n-1}(\omega^j-\omega^i)\neq 0$$

и $a_{\mathrm{MS}}=a_{\mathrm{MS}}^{(2)'}$. Значит, $a_{\mathrm{MS}}(X)=a_{\mathrm{MS}}(X)^2$. □

Определение 3.2.11. Пусть $v=v_0v_1\dots v_{N-1}$ — вектор над $\mathbb{F}_q$ и ω — примитивный $(N, \mathbb{F}_q)$-корень из единицы. *Преобразованием Фурье* вектора v называется вектор $V=V_0V_1\dots V_{N-1}$, компоненты которого задаются по формуле

$$V_j=\sum_{i=0}^{N-1}\omega^{ij}v_i,\quad j=0,\dots,N-1. \tag{3.2.7}$$

□

Лемма 3.2.12 (формула обращения). *Вектор v восстанавливается по своему преобразованию Фурье по следующей формуле*:

$$v_i=\frac{1}{N}\sum_{j=0}^{N-1}\omega^{-ij}V_i. \tag{3.2.8}$$

Доказательство. В любом поле справедливо тождество

$$X^N-1=(X-1)(X^{N-1}+\dots+X+1).$$

Так как порядок элемента ω равен N, для любого r получаем, что ω^r — корень л. ч. Значит, для любого $r\neq 0 \bmod N$ элемент ω^r обращает в нуль второй сомножитель, т. е.

$$\sum_{j=0}^{N-1}\omega^{rj}=0 \bmod N.$$

С другой стороны, при $r=0$ имеем

$$\sum_{j=0}^{N-1}\omega^{rj}=N \bmod p,$$

что отлично от нуля, если N не делится на характеристику поля p. Но $q-1=p^s-1$ кратно N, значит, N не делится на p. Итак, $N\neq 0 \bmod p$. Наконец, меняя порядок суммирования, получим, что

$$\frac{1}{N}\sum_{j=0}^{N-1}\omega^{-ij}V_j=\frac{1}{N}\sum_{k=1}^{N-1}v_k\sum_{j=0}^{N-1}\omega^{(k-i)j}=v_i.$$ □

Доказательство леммы 3.2.5. Пусть

$$a(X) = a_0 + a_1 X + \ldots + a_{N-1} X^{N-1} \in \mathbb{F}_q[X]$$

и ω — примитивный $(N, \mathbb{F}_q)$-корень из единицы. Тогда запишем

$$N^{-1} \sum_{j=0}^{N-1} a(\omega^j)\omega^{-ij} = N^{-1} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} a_k \omega^{jk} \omega^{-ij} =$$

$$= N^{-1} \sum_{k=0}^{N-1} a_k \sum_{j=0}^{N-1} \omega^{j(k-i)} = N^{-1} \sum_{k=0}^{N-1} a_k N \delta_{ki} = a_i.$$

Мы воспользовались тем фактом, что при $1 \leqslant l \leqslant N-1$ выполняются условия $\omega^l \neq e$ и

$$\sum_{j=0}^{N-1} \omega^{jl} = \sum_{j=0}^{N-1} (\omega^l)^j (e - (\omega^l)^N)(e - \omega^l)^{-1} = 0.$$

Следовательно,

$$a_i = \frac{1}{N} \sum_{j=0}^{N-1} a(\omega^j)\omega^{-ij}. \tag{3.2.9}$$

□

Пример 3.2.13. Используйте многочлен Маттсона—Соломона для доказательства неравенства БЧХ: пусть ω — примитивный $(N, \mathbb{F}_q)$-корень из единицы и $b \geqslant 1$, $\delta \geqslant 2$ — целые числа. Пусть $\mathcal{X}_N = \langle g(X) \rangle$ — циклический код, где $g(X) \in \mathbb{F}_q[X]/\langle X^N - e \rangle$ — приведённый многочлен минимальной степени, аннулирующийся элементами ω^b, ω^{b+1}, …, $\omega^{b+\delta-2}$. Тогда минимальное расстояние кода $\mathcal{X}_N$ не меньше чем δ.

Решение. Пусть многочлен $a(X) = \sum\limits_{j=0}^{N-1} a_j X^j \in \mathcal{X}_N$ обладает свойством $g(X) | a(X)$ и $a(\omega^i) = 0$ при $i = b, \ldots, b + \delta - 2$. Рассмотрим многочлен Маттсона—Соломона для $a(X)$:

$$c_{\mathrm{MS}}(X) = \sum_{i=0}^{N} a(\omega^i) X^{N-i} = \sum_{j=1}^{b-1} a(\omega^j) X^{N-j} + 0 + \ldots$$

$$\ldots + 0 \text{ (из } \omega^b, \ldots, \omega^{b+\delta-2}) + a(\omega^{b+\delta-1}) X^{N-b-\delta+1} + \ldots + a(\omega^N). \tag{3.2.10}$$

Умножаем на X^{b-1} и группируем:

$$X^{b-1}c_{\mathrm{MS}}(X) = a(\omega)X^{N+b-2} + \ldots + a(\omega^{b-1})X^N + \\ + a(\omega^{b+\delta-1})X^{N-\delta} + \ldots + a(\omega^N)X^{b-1} = \\ = X^N[a(\omega)X^{b-2} + \ldots + a(\omega^{b-1})] + [a(\omega^{b+\delta-1})X^{N-\delta} + \ldots + a(\omega^N)X^{b-1}] = \\ = X^N p_1(X) + q(X) = (X^N - e)p_1(X) + p_1(X) + q(X).$$

Мы видим, что $c_{\mathrm{MS}}(\omega^i) = 0$ тогда и только тогда, когда $p_1(\omega^i) + q(\omega^i) = 0$. Но $p_1(X) + q(X)$ — многочлен степени не выше $N - \delta$, так что у него не более чем $N - \delta$ корней. Таким образом, c_{MS} имеет не более $N - \delta$ корней вида ω^i.

Следовательно, из формулы обращения (3.2.9) получаем, что вес $w(a(X))$ (т. е. вес строки коэффициентов $a_0 \ldots a_{N-1}$) ограничен снизу:

$$w(a(X)) \geqslant N \text{ — число корней многочлена } c_{\mathrm{MS}} \text{ вида } \omega^i. \qquad (3.2.11)$$

Мы получаем неравенство

$$w(a(X)) \geqslant N - (N - \delta) = \delta. \qquad \square$$

Завершим этот параграф кратким обсуждением алгоритма списочного декодирования кодов Рида—Соломона, см. [GS]. Для этого мы приведем ниже альтернативное определение кода Рида—Соломона, которое и было предложено в их оригинальной статье [ReS]. Для краткости положим $b = 1$ (однако мы сможем расширить определение для $N > q - 1$).

При $N \leqslant q$ пусть $S = x_1, \ldots, x_N \in \mathbb{F}_q$ — т. н. опорное множество N различных точек в $\mathbb{F}_q$. Определим отображение

$$\mathrm{Ev}\colon f \in \mathbb{F}_q[X] \mapsto \mathrm{Ev}(f) = (f(x_1), \ldots, f(x_N)) \in \mathbb{F}_q^N \qquad (3.2.12)$$

и положим

$$L = \{f \in \mathbb{F}_q[X]\colon \deg f < k\}. \qquad (3.2.13)$$

Определим код Рида—Соломона над $\mathbb{F}_q$ длины N и размерности k:

$$\mathcal{X} = \mathrm{Ev}(L). \qquad (3.2.14)$$

Он обладает минимальным расстоянием $d = d(\mathcal{X}) = N - k + 1$ и исправляет до $\left\lfloor \dfrac{d-1}{2} \right\rfloor$ ошибок. Кодирование исходного сообщения $\mathbf{u} = u_0 \ldots u_{k-1} \in \mathbb{F}_q^k$ состоит в вычислении значений полинома $f(X) = u_0 + u_1 X + \ldots + u_{k-1}X^{k-1}$ в точках $x_i \in S$.

Определение 3.2.1, где $\mathcal{X}$ определяется как множество полиномов $c(X) = \sum\limits_{0 \leqslant l \leqslant q-1} c_l X^l \in \mathbb{F}_q[X]$, таких что $c(\omega) = c(\omega^2) = \ldots = c(\omega^{\delta-1}) = 0$,

возникает, когда $N = q - 1$, $k = N - \delta + 1 = q - \delta$, а опорное множество $S = \{e, \omega, \ldots, \omega^{N-1}\}$. В этом случае коэффициенты $c_0, c_1, \ldots, c_{N-1}$ связаны с полиномом $f(X)$ соотношением

$$c_i = f(\omega^i), \quad 0 \leqslant i \leqslant N - 1.$$

Это однозначно определяет коэффициенты f_j полинома $f(X) = \sum\limits_{0 \leqslant l < N} f_j X^j$ в терминах дискретного обратного преобразования Фурье

$$Nf_l = c(\omega^{N-l}) \quad \text{или} \quad Nf_{N-l-1} = c(\omega^{l+1}), \quad l = 0, 1, \ldots, N - 1,$$

и гарантирует, в частности, что $f_k = \ldots = f_{N-1} = 0$.

При заданных $f \in \mathbb{F}_q[X]$ и $\mathbf{y} = y_1 \ldots y_N \in \mathbb{F}_q^N$ положим

$$\operatorname{dist}(f, \mathbf{y}) = \sum_{i=1}^{N} \mathbf{1}(f(x_i) \neq y_i.$$

Пусть получено слово $\mathbf{y} = y_1 \ldots y_N$ и $t = \left\lfloor \dfrac{d-1}{2} \right\rfloor$. «Традиционные» алгоритмы декодирования (например, алгоритм Берлекэмпа—Мэсси) или находят единственный полином f, такой что $\operatorname{dist}(f, \mathbf{y}) \leqslant t$, или устанавливает, что такого f не существует. При списочном декодировании выбирается $s > t$ и находится список всех таких f, что $\operatorname{dist}(f, \mathbf{y}) \leqslant s$. При определённом везении такой f оказывается единственным или может быть найден из дополнительных соображений. Таким образом, мы сможем исправить s ошибок, что превосходит традиционный предел разрешения t ошибок. Этом метод восходит к идее Шеннона о декодировании по расстоянию Хэмминга: получив сообщение $\mathbf{y}$, последовательно изучаются шары Хэмминга вокруг $\mathbf{y}$ до тех пор, пока не найдено ближайшее к $\mathbf{y}$ кодовое слово (или несколько ближайших слов). Желательно обеспечить, чтобы (i) при s «умеренно» больших t шансы обнаружить два или более кодовых слова на расстоянии s малы, и (ii) алгоритм имеет не слишком большую вычислительную сложность.

Пример 3.2.14. Рассмотрим [32,8]-код Рида—Соломона над полем $\mathbb{F}_{32}$, для которого $d = 25$ и $t = 12$. Если выбрать $s = 13$, то шар Хэмминга вокруг полученного слова $\mathbf{y}$ может содержать два кодовых слова. Однако если предположить, что все векторы ошибок β веса 13 равновероятны, то вероятность этого события равна $2{,}08437 \times 10^{-12}$. Алгоритм списочного кодирования Гурусмани—Судана, см. [GS], находит все кодовые слова на расстоянии s, где $t \leqslant s \leqslant t_{GS}$ за полиномиальное время. Здесь

$$t_{GS} = n - 1 - \sqrt{(k-1)n},$$

т. е. t_{GS} может значительно превышать t.

В приведённом выше примере $t_{GS} = 17$. Асимптотически для РС-кода скорости надёжной передачи R традиционные алгоритмы декодирования исправляют долю ошибок, равную $(1 - R)/2$, в то время как алгоритм Гурусмани—Судана может исправить $1 - \sqrt{R}$. Среднее число кодовых слов в шаре Хэмминга радиуса $s \leqslant t_{GS}$ может быть найдено явно при условии равнораспределённости векторов ошибок. Алгоритм Гурусмани—Судана применим не только к РС-кодам. В оригинальной работе [GS] показано, что он хорошо работает для целого класса кодов. Его усовершенствование для случая РС-кодов было найдено позднее, см. [AS].

§ 3.3. Развитие теории циклических кодов. Декодирование БЧХ-кодов

Напомним определение циклического кода. Как и в гл. 2, предполагаем, что НОД $(N, q) = 1$ (так что N нечётно при $q = 2$), и записываем слово $\mathbf{x} \in \mathcal{H}_{N,q}$ как $x_0 \dots x_{N-1}$. Линейный код $\mathcal{X} \subseteq \mathcal{H}_N$ называется циклическим, если вместе с каждым словом $\mathbf{x} = x_0 \dots x_{N-1} \in \mathcal{X}$ коду принадлежит его циклический сдвиг $\pi\mathbf{x} = x_{N-1}x_0 \dots x_{N-2}$. Каждому слову $\mathbf{c} = c_0 \dots c_{N-1}$ мы сопоставляем многочлен $c(X) \in \mathbb{F}_q[X]$:

$$c(X) = c_0 + c_1 X + \ldots + c_{N-1}X^{N-1}.$$

Отображение $\mathbf{c} \leftrightarrow c(X)$ осуществляет изоморфизм между $\mathcal{X}$ и линейным подпространством в $\mathbb{F}_q[X]$. Запись $c(X) \in \mathcal{X}$ просто означает, что строка коэффициентов $c_0 \dots c_{N-1} \in \mathcal{X}$.

Лемма 3.3.1. *Код $\mathcal{X}$ является циклическим тогда и только тогда, когда его образ при описанном изоморфизме образует идеал в факторкольце $\mathbb{F}_q[X]/\langle X^N - e\rangle$.*

Доказательство. Циклический сдвиг соответствует умножению многочлена $c(X)$ на X. Следовательно, умножение на любой многочлен сохраняет $\mathcal{X}$. □

Полезно представлять себе циклический код $\mathcal{X}$ как идеал в $\mathbb{F}_q[X]/\langle X^N - e\rangle$, более того, $\mathbb{F}_q[X]/\langle X^N - e\rangle$ — кольцо главных идеалов: любой идеал в нём имеет вид

$$\langle g(X)\rangle = \{f(X)\colon f(X) = g(X)h(X),\ \ h(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle\}, \qquad (3.3.1)$$

где $g(X)$ — фиксированный многочлен.

Теорема 3.3.2. *Если код $\mathcal{X} \subseteq \mathcal{H}_{N,q}$ циклический, то существует такой единственный приведённый многочлен $g(X) \in \mathcal{X}$, что* 1) $\mathcal{X} = \langle g(X)\rangle$ *и* 2) $g(X)$ *обладает минимальной степенью из всех многочленов $f(X) \in \mathcal{X}$. Более того,*

а) $g(X)|(X^N - e)$,

б) *если* $\deg g(X) = d$, *то* $\dim \mathcal{X} = N - d$,

в) $\mathcal{X} = \{f(X)\colon f(X) = g(X)h(X),\ \ h(X) \in \mathbb{F}_q[X],\ \ \deg h(X) < N - d\}$,

г) *если* $g(X) = g_0 + g_1X + \ldots + g_dX^d$, $g_d = e$, *то* $g_0 \neq 0$ *и*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_d & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_{d-1} & g_d & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & g_0 & g_1 & \ldots & g_d & 0 \end{pmatrix}$$

является образующей матрицей, у которой i*-я строка — это циклический сдвиг* $(i-1)$*-й строки,* $i = 2, \ldots, N - d$.

Верно и обратное: для любого многочлена $g(X)|(X^N - e)$ *множество* $\langle g(X)\rangle = \{f(X)\colon f(X) = g(X)h(X),\ \ h(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle\}$ *— идеал в* $\mathbb{F}_q[X]/\langle X^N - e\rangle$, *т. е. циклический код* $\mathcal{X}$ *с перечисленными выше свойствами б)–г).*

Доказательство. Пусть $g(X) \in \mathbb{F}_q[X]$ — ненулевой многочлен наименьшей степени из $\mathcal{X}$. Выберем $p(X) \in \mathcal{X}$ и запишем

$$p(X) = h(X)g(X) + r(X), \quad \deg r(X) < \deg g(X).$$

Тогда $r(X) \bmod (X^N - e)$ лежит в $\mathcal{X}$. Это противоречит выбору $g(X)$, если $r(X) \neq 0$. Следовательно, $g(X)|p(X)$, что доказывает п. а). Если в качестве $p(X)$ взять $X^N - e$, то докажем п. б). Наконец, если $g(X)$ и $\hat{g}(X)$ удовлетворяют пунктам а) и б), то $g(X)|\hat{g}(X)$ и $\hat{g}(X)|g(X)$, т. е. $\hat{g}(X) = g(X)$. □

Следствие 3.3.3. *Циклические коды длины* N *взаимно однозначно соответствуют делителям многочлена* $X^N - e$. *Иначе говоря, отображение*

$$\begin{array}{rcl} \{\textit{циклические коды длины } N\} & \longrightarrow & \{\textit{делители многочлена } X^N - e\} \\ \mathcal{X} & \longrightarrow & g(X) \end{array}$$

биективно.

При отождествлении

$$\mathbb{F}_q[X]/\langle X^N - e\rangle = \{f \in \mathbb{F}_q[X]\colon \deg f < N\} = \mathbb{F}_q^N$$

циклические коды соответствуют идеалам полиномиального кольца $\mathbb{F}_q[X]/\langle X^N - e\rangle$. Они взаимно однозначно соответствуют идеалам кольца $\mathbb{F}_q[X]$, содержащим многочлен $X^N - e$. Так как кольцо $\mathbb{F}_q[X]$ евклидово,все его идеалы главные, т. е. имеют вид $\{f(X)g(X)\colon f(X) \in \mathbb{F}_q[X]\}$. На самом деле все идеалы в $\mathbb{F}_q[X]/\langle X^N - e\rangle$ тоже главные.

Определение 3.3.4. Многочлен $g(X)$ называется *порождающим полиномом минимальной степени* (или просто *порождающим полиномом*) циклического кода $\mathcal{X}$. Отношение $h(X) = (X^N - e)/g(X)$ степени $N - \deg g(X)$ называется *проверочным многочленом* циклического кода $\mathcal{X} = \langle g(X) \rangle$. □

Пример 3.3.5. Многочлен $X - e$ порождает код проверки на чётность $\{\mathbf{x}\colon \sum\limits_i x_i = 0\}$, а $e + X + \ldots + X^{N-1}$ — код повторений $\{a \ldots a, \ \ a \in \mathbb{F}_q\}$; $X \equiv e$ порождает $\mathcal{X} = \mathcal{H}$. □

Пример 3.3.6. Покажите, что [7, 4]-код Хэмминга — это циклический код с проверочным многочленом $X^4 + X^2 + X + 1$. Что можно сказать о его порождающем полиноме? Найдите подкод кода Хэмминга, эквивалентный двойственному коду.

Решение. Проверочный многочлен циклического кода, порождённого многочленом $g(X) = X^3 + X + 1$, равен $h(X) = X^4 + X^3 + X + 1$ в силу разложения

$$X^7 - 1 = (X^3 + X + 1)(X^4 + X^2 + X + 1).$$

Проверочная матрица этого кода равна

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Столбцы этой матрицы — ненулевые элементы пространства $\mathbb{F}_2^3$, так что код, задаваемый этой матрицей, эквивалентен [7, 4]-коду Хэмминга.

Двойственный код к [7, 4]-коду Хэмминга порождён многочленом $X^4 + X^3 + X^2 + 1$ (обращенный к $h(X)$). Так как $X^4 + X^3 + X^2 + 1 = (X + 1)g(X)$, двойственный код является подкодом [7, 4]-кода Хэмминга. □

Пример 3.3.7. Пусть ω — примитивный корень из единицы степени N. Пусть $\mathcal{X} = \langle g(X) \rangle$ — циклический код длины N. Покажите, что ранг этого кода $\dim \mathcal{X}$ совпадает с числом степеней ω^j, для которых $g(\omega^j) \neq 0$.

Решение. Обозначим $\mathsf{E}^{(N)} = \{\omega, \omega^2, \ldots, \omega^N = e\}$, $\dim\langle g(X) \rangle = N - d$, $d = \deg g(X)$. Но $g(X) = \prod\limits_{j=1}^{d} (X - \omega^{i_j})$, где $\omega^{i_1}, \ldots, \omega^{i_d}$ — нули многочлена $g(X)$. Следовательно, для оставшихся $N - d$ корней из единицы ω^i выполняется условие $g(\omega^i) \neq 0$. □

Важно отметить, что в качестве порождающего полинома циклического кода $\mathcal{X} = \langle g(X) \rangle$ может выступать не единственный многочлен. В частности, существует такой единственный многочлен $i(X) \in \mathcal{X}$, что $i(X)^2 = i(X)$ и $\mathcal{X} = \langle i(X) \rangle$ (идемпотентная образующая).

Теорема 3.3.8. *Если* $\mathcal{X}_1 = \langle g_1(X)\rangle$ *и* $\mathcal{X}_2 = \langle g_2(X)\rangle$ *— циклические коды с порождающими полиномами* $g_1(X)$ *и* $g_2(X)$, *то* 1) $\mathcal{X}_1 \subset \mathcal{X}_2$ *тогда и только тогда, когда* $g_2(X) | g_1(X)$, 2) $\mathcal{X}_1 \cap \mathcal{X}_2 = \langle \text{НОК}\,(g_1(X), g_2(X))\rangle$, 3) $\mathcal{X}_1 | \mathcal{X}_2 = \langle \text{НОД}\,(g_1(X), g_2(X))\rangle$.

Теорема 3.3.9. *Пусть* $h(X)$ *— проверочный многочлен кода* $\mathcal{X}$. *Тогда*

1) $\mathcal{X} = \{f(X)\colon f(X)h(X) = 0 \bmod (X^N - e)\}$;

2) *если* $h(X) = h_0 + h_1 X + \ldots + h_{N-r}X^{N-r}$, *то проверочная матрица* H *кода* $\mathcal{X}$ *равна*

$$H = \begin{pmatrix} h_{N-r} & h_{N-r-1} & \ldots & h_1 & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_{N-r} & h_{N-r-1} & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & h_{N-r} & h_{N-r-1} & \ldots & \ldots & \ldots & h_0 \end{pmatrix};$$

3) *двойственный код* $\mathcal{X}^\perp$ *имеет ранг* $\dim \mathcal{X}^\perp = r$ *и* $\mathcal{X}^\perp = \langle g^\perp(X)\rangle$, *где* $g^\perp(X) = h_0^{-1}X^{N-r}h(X^{-1}) = h_0^{-1}(h_0X^{N-r} + h_1X^{N-r-1} + \ldots + h_{N-r})$.

Образующая $g(X)$ циклического кода характеризуется в терминах разложения многочлена

$$X^N - e = \text{НОК}\,(M_\omega(X)\colon \omega \in \mathsf{E}^{(N)}) \tag{3.3.2}$$

как произведение некоторых минимальных многочленов $M_\omega(X)$. Удобно охарактеризовать циклический код через корни порождающего полинома $g(X)$. Если ω — корень многочлена $M_\omega(X)$ в расширении $\mathbb{F}_q(\omega)$, то $M_\omega(X)$ — минимальный многочлен элемента ω над $\mathbb{F}_q$. Для любого многочлена $f(X) \in \mathbb{F}_q[X]$ мы имеем, что $f(\omega) = 0$ тогда и только тогда, когда $f(X) = a(X)M_\omega(X)$, и если к тому же, $f(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle$, то $f(\omega) = 0$ тогда и только тогда, когда $f(X) \in \langle M_\omega(X)\rangle$. Таким образом, справедлив следующий результат.

Теорема 3.3.10. *Пусть* $g(X) = q_1(X)\ldots q_t(X)$ *— произведение неприводимых множителей многочлена* $X^N - e$ *и* $\omega_1, \ldots, \omega_u$ *— корни* $g(X)$ *в поле* $\text{Spl}\big(X^N - e\big)$ *над* $\mathbb{F}_q$. *Тогда*

$$\langle g(X)\rangle = \{f(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle\colon f(\omega_1) = \ldots = f(\omega_u) = 0\}. \tag{3.3.3}$$

Более того, достаточно указать единственный корень каждого неприводимого множителя: если ω'_j — любой корень многочлена $M_\omega(X)$, $1 \leqslant j \leqslant t$, то

$$\langle g(X)\rangle = \{f(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle\colon f(\omega'_1) = \ldots = f(\omega'_t) = 0\}. \tag{3.3.4}$$

Обратно, если $\omega_1, \ldots, \omega_u$ — некоторое подмножество корней многочлена $X^N - e$, то код $\{f(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle\colon f(\omega_1) = \ldots = f(\omega_u) = 0\}$ порождается полиномом $g(X)$, который является НОК минимальных многочленов элементов $\omega_1, \ldots, \omega_u$.

Определение 3.3.11. Корни порождающего полинома $g(X)$ называются *нулями циклического кода* $\langle g(X)\rangle$. □

Пусть $\{\omega_1, \ldots, \omega_u\}$ — множество корней многочлена $X^N - e$, лежащих в расширении $\mathbb{F}_{q^l}$. Напомним, что l — это минимальное целое число, при котором $N | q^l - 1$. Если

$$f(X) = \sum_i^u f_i X^i \in \mathbb{F}_q[X]/\langle X^N - e\rangle$$

— многочлен степени u, то $f(\omega_j) = 0$ тогда и только тогда, когда $\sum\limits_{i=0}^{u} f_i \omega_j^i = 0$. Представляя $\mathbb{F}_{q^l}$ как векторное пространство над $\mathbb{F}_q$ размерности l, сопоставим элементу ω_j^i вектор-(столбец) $\vec{\omega}_j^i$ длины l над $\mathbb{F}_q$. Запишем последнее равенство как $\sum\limits_i f_i \vec{\omega}_j^i = \overrightarrow{\sum\limits_i f_i \omega_j^i} = 0$. Таким образом, $(ul) \times N$-матрицу

$$\tilde{H} = \begin{pmatrix} \vec{\omega}_1^0 & \vec{\omega}_1^1 & \ldots & \vec{\omega}_1^{N-1} \\ \vec{\omega}_2^0 & \vec{\omega}_2^1 & \ldots & \vec{\omega}_2^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ \vec{\omega}_u^0 & \vec{\omega}_u^1 & \ldots & \vec{\omega}_u^{N-1} \end{pmatrix} \tag{3.3.5}$$

можно рассматривать как проверочную матрицу кода с нулями $\omega_1, \ldots, \omega_u$ (с той оговоркой, что её строки не обязательно будут линейно независимы).

Теорема 3.3.12. *Двоичный* $[2^l - 1, 2^l - l - 1]$*-код Хэмминга эквивалентен циклическому коду с порождающим полиномом степени* l *вида*

$$g(X) = \langle M_\omega(X)\rangle = \prod_{i=0}^{l-1} (X - \omega^{2^i}),$$

где ω *— примитивный элемент поля* $\mathbb{F}_{2^l}$.

Доказательство. Пусть ω — примитивный $(N, \mathbb{F}_2)$-корень из единицы, где $N = 2^l - 1$. Поле разложения $\mathrm{Spl}\big(X^N - e\big) = \mathbb{F}_{2^l}$ (так как $\mathrm{ord}_N(2) = l$). Поэтому ω — примитивный элемент в $\mathbb{F}_{2^l}$. Возьмём $M_\omega(X) = (X - \omega)(X - \omega^2)\ldots(X - \omega^{2^{l-1}})$ степени l. Элементы $\omega^0 = e, \omega, \ldots, \omega^{N-1}$ образуют группу $\mathbb{F}_{2^l}^*$, содержащую все ненулевые элементы и столбцы $l \times N$-матрицы

$$H = (\vec{\omega}^0, \vec{\omega}, \ldots, \vec{\omega}^{N-1}), \tag{3.3.6}$$

состоящей из всех ненулевых двоичных векторов длины l. Следовательно, $[2^l - 1, 2^l - l - 1, 3]$-код Хэмминга эквивалентен циклическому коду $\langle M_\omega(X)\rangle$, нули которого — примитивный $(2^l - 1, \mathbb{F}_2)$-корень из единицы

ω и (с необходимостью) все остальные корни минимального многочлена для ω. $\square$

Теорема 3.3.13. *Если* НОД$(l, q-1)=1$, *то q-ичный код Хэмминга с параметрами* $\left[\dfrac{q^l-1}{q-1}, \dfrac{q^l-1}{q-1}-l, 3\right]$ *эквивалентен циклическому коду.*

Доказательство. Рассмотрим $\mathrm{Spl}\left(X^N-e\right)=\mathbb{F}_{q^l}$, где $l=\mathrm{ord}_N(q)$, $N=(q^l-1)/(q-1)$. Чтобы обосновать выбор l, заметим, что $(q^l-1)/N=q-1$ и $l=\min\left[n\colon \dfrac{q^n-1}{N}\text{ — целое число}\right]$, так как $(q^l-1)/(q-1)>q^{l-1}-1$. Следовательно, $\mathrm{Spl}\left(X^N-e\right)=\mathbb{F}_{q^l}$. Возьмём примитивный элемент $\beta\in\mathbb{F}_{q^l}$. Тогда $\omega=\beta^{(q^l-1)/N}=\beta^{q-1}$ — примитивный $(N, \mathbb{F}_q)$-корень из единицы. Как и раньше, рассмотрим минимальный многочлен $M_\omega(X)=(X-\omega)(X-\omega^q)\ldots(X-\omega^{q^{l-1}})$ и циклический код $\langle M_\omega(X)\rangle$ с нулями ω (и обязательно $\omega^q, \ldots, \omega^{q^{l-1}}$). Снова рассмотрим $l\times N$-матрицу H из формулы (3.3.6) и проверим, что любые два её столбца линейно независимы над $\mathbb{F}_q$. Если это не так, то найдётся такая пара $i<j$, что ω^i и ω^j окажутся пропорциональны элементу $\omega^{j-i}\in\mathbb{F}_q$. Но тогда $(\omega^{j-i})^{q-1}=\omega^{(j-i)(q-1)}=e$ в поле $\mathbb{F}_q$, так как ω — примитивный корень из единицы степени N. Это верно тогда и только тогда, когда $(j-i)(q-1)=0 \bmod N$. Запишем

$$N=\frac{q^l-1}{q-1}=1+\ldots+q^{l-1}.$$

Так как $(q-1)|(q^r-1)\ \forall r\geqslant 1$, мы получаем $q^r=(q-1)v_r+1$ для некоторого натурального v_r. Суммируя по $0\leqslant r\leqslant s-1$, получаем

$$N=(q-1)\sum_r v_r+l. \tag{3.3.7}$$

Поскольку $q-1$ и l взаимно просты, НОД$(q-1, N)=1$. Но тогда равенство $(j-i)(q-1)=0 \bmod N$ невозможно.

Таким образом, проверочная матрица H задает $[N, k, d]$-код, где $k\geqslant N-l$, а $d\geqslant 3$. Но из границы Хэмминга

$$q^k\leqslant q^N\left(\sum_{m=0}^{E}C_N^m(q-1)^m\right)^{-1},\quad E=\left\lfloor\frac{d-1}{2}\right\rfloor.$$

Так как объём шара $v_{N,q}(E)\geqslant q^l$, в действительности $k=N-l$, $E=1$ и $d=3$. Поэтому такой код эквивалентен коду Хэмминга. $\square$

Теперь более подробно остановимся на БЧХ-кодах, исправляющих несколько ошибок. Напомним, что если $\omega_1, \ldots, \omega_u\in\mathsf{E}_{(N,q)}$ — $(N, \mathbb{F}_q)$-кор-

ни из единицы, то код

$$\mathcal{X}_N = \{f(X) \in \mathbb{F}_q[X]/\langle X^N - e\rangle \colon f(\omega_1) = \ldots = f(\omega_u) = 0\}$$

является циклическим кодом $\langle g(X)\rangle$, где

$$g(X) = \mathrm{HOK}\,(M_{\omega_1,\mathbb{F}_q}(X), \ldots, M_{\omega_u,\mathbb{F}_q}(X)) \tag{3.3.8}$$

представляет собой произведение различных минимальных многочленов для $\omega_1, \ldots, \omega_u$ над $\mathbb{F}_q$. В частности, если $q = 2$, $N = 2^l - 1$ и ω — примитивный элемент поля $\mathbb{F}_{2^l}$, то циклический код с корнями $\omega, \omega^2, \ldots, \omega^{2^{l-1}}$ (что то же самое, что и с единственным корнем ω) совпадает с $\langle M_\omega(X)\rangle$ и эквивалентен коду Хэмминга. Хотелось бы попробовать другие возможности для нулей кода $\mathcal{X}$, чтобы увидеть, не приведёт ли это к интересным примерам. Таким способом были открыты БЧХ-коды (Боуз—Чоудхури—Хоквингем, 1959 г.), см. [BR, Hoc].

Напомним, что разложение на минимальные многочлены $M_i(X)(= M_{\omega^i,\mathbb{F}_q}(X))$ имеет вид

$$X^N - e = \mathrm{HOK}\,(M_i(X)\colon i = 0, \ldots, t), \tag{3.3.9}$$

где ω — примитивный $(N, \mathbb{F}_q)$-корень из единицы. Корни многочлена $M_i(X)$ сопряжены, т. е. имеют вид $\omega^i, \omega^{iq}, \ldots, \omega^{iq^{d-1}}$, где $d\ (= d(i))$ — наименьшее целое число большее 1 такое, что $iq^d = i \bmod N$, так что

$$M_i(X) = \prod_{j \in C_i} (X - \omega^j), \tag{3.3.10}$$

где C_i — циклотомический класс, см. определение 3.1.46.

В § 3.2 мы получили циклический код с минимальным расстоянием не меньше δ, потребовав, чтобы порождающий полином $g(X)$ имел $\delta - 1$ корней вида $\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$.

Пример 3.3.14. Двоичный код Хэмминга является двоичным БЧХ-кодом в узком смысле с проектируемым расстоянием $\delta = 3$. □

По лемме 3.2.8 имеем $d(\mathcal{X}_{q,N,\delta}) \geqslant \delta$. Так как $\mathrm{Spl}\big(X^N - e\big) = \mathbb{F}_{q^l}$, где $l = \mathrm{ord}_N(q)$, то имеет место неравенство

$$\deg M_{\omega^{b+j}}(X) \leqslant l. \tag{3.3.11}$$

Следовательно, $\mathrm{rank}(\mathcal{X}_{q,N,\delta}) = N - \deg g(X) \geqslant N - (\delta - 1)l$, так что выполнена следующая теорема.

Теорема 3.3.15. *Расстояние q-ичного БЧХ-кода $\mathcal{X}_{q,N,\delta}$ имеет расстояние не меньше чем δ, а его ранг не меньше чем $N - (\delta - 1)\mathrm{ord}_N(q)$.*

Как и раньше, можно построить проверочную матрицу кода $\mathcal{X}$, записав ω^b, ω^{b+1}, …, $\omega^{b+\delta-2}$ и их степени как векторы из $\mathbb{F}_{q^l}$, где $l = \operatorname{ord}_N(q)$. Положим

$$\tilde{H} = \begin{pmatrix} \vec{e} & \vec{\omega}^b & \vec{\omega}^{2b} & \dots & \vec{\omega}^{(N-1)b} \\ \vec{e} & \vec{\omega}^{b+1} & \vec{\omega}^{2(b+1)} & \dots & \vec{\omega}^{(N-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vec{e} & \vec{\omega}^{b+\delta-2} & \vec{\omega}^{2(b+\delta-2)} & \dots & \vec{\omega}^{(N-1)(b+\delta-2)} \end{pmatrix}. \tag{3.3.12}$$

Корректная проверочная матрица H получается удалением линейно зависимых строк.

С двоичным БЧХ-кодом легко работать. Пусть $C_i = \{i, 2i, \dots, i2^{d-1}\}$ — i-й циклотомический класс (где $d(=d(i))$ — такое наименьшее натуральное число $\geqslant 1$, что $i \cdot 2^d = i \bmod N$). Тогда $u \in C_i$ в том и только том случае, если $2u \bmod N \in C_i$, так что $M_i(X) = M_{2i}(X)$ и $\forall s \geqslant 1$ имеем

$$g_{2s-1}(X) = g_{2s}(X) = \text{НОК}\,\{M_1(X),\, M_2(X),\, \dots,\, M_{2s}(X)\}.$$

Мы немедленно получаем, что $\mathcal{X}_{2,N,2s+1} = \mathcal{X}_{2,N,2s}$. Поэтому можно сфокусировать внимание на БЧХ-кодах в узком смысле с нечётным проектируемым расстоянием $\delta = 2E + 1$ и получить усиление теоремы 3.3.15.

Теорема 3.3.16. *Ранг двоичного БЧХ-кода $\mathcal{X}_{2,N,2E+1}$ не меньше*

$$N - E\operatorname{ord}_N(2).$$

Задача точного вычисления минимального расстояния БЧХ-кода была решена лишь частично (хотя в литературе можно найти немало результатов). Мы представляем следующую теорему без доказательства.

Теорема 3.3.17. *Минимальное расстояние примитивного БЧХ-кода в узком смысле нечётно.*

Предыдущие результаты можно усилить в некоторых конкретных ситуациях.

Пример 3.3.18. Докажите, что из неравенства $\log_2(N+1) > 1 + \log_2(E+1)!$ следует, что

$$(N+1)^E < \sum_{i=0}^{E+1} C_N^i. \tag{3.3.13}$$

Решение. Для $i \leqslant E+1$ мы получаем, что $i! \leqslant (E+1)! < (N+1)/2$. Значит, формула (3.3.13) следует из неравенства

$$(N+1)^{E+1} \leqslant 2\sum_{i=0}^{E+1} N(N-1)\dots(N-i+1) = S(E). \tag{3.3.14}$$

Неравенство (3.3.14) верно при $E = 0$ и проверяется индукцией по E. Запишем п. ч. неравенства (3.3.14) как $S(E+1) = S(E) + N(N-1)\dots(N-E)$.

Тогда $S(E) > (N+1)^{E+1}$ по предположению индукции и остаётся проверить, что

$$N(N+1)^{E+1} < 2N(N-1)\dots(N-E)(N-E-1) \text{ при } N+1 > 2(E+2)!. \tag{3.3.15}$$

Рассмотрим многочлен $p(y) = (y+1)^{E+1} - 2(y-1)\dots(y-E)(y-E-1)$ и сгруппируем вместе мономы степеней $E+1$ и E. Ясно, что $p(y) < 0$ при $y > 2(E+2)!$. Продолжая эту процедуру, приходим к выводу, что неравенство (3.3.13) верное. □

Теорема 3.3.19. *Пусть $N = 2^s - 1$. Если $2^{sE} < \sum\limits_{i=1}^{E+1} C_N^i$, то примитивный БЧХ-код в узком смысле $\mathcal{X}_{2,2^s-1,2E+1}$ имеет расстояние $2E+1$.*

Доказательство. По теореме 3.3.17 расстояние нечётно. Поэтому $d = d(\mathcal{X}_{2,2^s-1,2E+1}) \neq 2E+2$. Предположим, что $d > 2E+3$. Заметим, что $\operatorname{rank} \mathcal{X}_{2,2^s-1,2E+1} \geqslant N - sE$ и воспользуемся границей Хэмминга

$$2^{N-sE} \sum_{i=0}^{E+1} C_N^i \leqslant 2^N, \quad \text{т. е. } 2^{sE} \geqslant \sum_{i=0}^{E+1} C_N^i,$$

что ведет к противоречию. Поэтому $d(\mathcal{X}_{2,2^s-1,2E+1}) = 2E+1$. □

Следствие 3.3.20. *Если $N = 2^s - 1$ и $s > 1 + \log_2(E+1)!$, то $d(\mathcal{X}_{2,2^s-1,2E+1}) = 2E+1$. В частности, пусть $N = 31$ и $s = 5$. Тогда мы легко проверим, что*

$$2^{5E} < \sum_{i=1}^{E+1} C_{31}^i$$

для $E = 1, 2$ и 3. Это доказывает, что реальное расстояние кода $\mathcal{X}_{2,31,\delta}$ действительно равно δ для $\delta = 3, 5, 7$.

Доказательство получается легко, так как из неравенства $s > 1 + \log_2(E+1)!$ следует, что $2^{sE} < \sum\limits_{i=0}^{E+1} C_N^i$. □

Теорема 3.3.21. *Если $\delta | N$, то минимальное расстояние примитивного двоичного БЧХ-кода в узком смысле с проектируемым расстоянием δ равно δ.*

Доказательство. Положим $N = \delta m$. Тогда

$$X^N - 1 = X^{\delta m} - 1 = (X^m - 1)(1 + X^m + \dots + X^{(\delta-1)m}).$$

Поскольку $\omega^{jm} \neq 1$ при $j = 1, \dots, \delta - 1$, ни один из элементов $\omega, \dots, \omega^{\delta-1}$ не является корнем многочлена $X^m - 1$. Поэтому они должны быть корнями второго сомножителя: $1 + X^m + \dots + X^{(\delta-1)m}$. Однако этот многочлен даёт кодовое слово веса δ, так что δ — это минимальное расстояние. □

Ещё два факта о минимальном расстоянии БЧХ-кодов представлены в теоремах 3.3.22–3.3.24. Полное доказательство выходит за рамки данной книги и опускается.

Теорема 3.3.22. *Пусть $N = q^s - 1$. Минимальное расстояние примитивного q-ичного БЧХ-кода в узком смысле $\mathcal{X}_{q,q^s-1,q^k-1,\omega,1}$ с проектируемым расстоянием $q^k - 1$ равно $q^k - 1$.*

Теорема 3.3.23. *Минимальное расстояние примитивного q-ичного БЧХ-кода в узком смысле $\mathcal{X} = \mathcal{X}_{q,q^s-1,\delta,\omega,1}$ с проектируемым расстоянием δ не превышает $q\delta - 1$.*

Доказательство. Возьмём такое натуральное число $k \geqslant 1$, что $q^{k-1} \leqslant \delta \leqslant q^k - 1$. Положим $\delta' = q^k - 1$ и рассмотрим код $\mathcal{X}'$ $(= \mathcal{X}_{q,q^s-1,\delta',\omega,1})$, q-ичный примитивный БЧХ-код в узком смысле той же длины $N = q^s - 1$ и с проектируемым расстоянием δ'. Корни порождающего полинома кода $\mathcal{X}$ обращают в нуль порождающий полином кода $\mathcal{X}'$, так что $\mathcal{X}' \subseteq \mathcal{X}$. Но по теореме 3.3.22 имеем $d(\mathcal{X}') = \delta'$, что не больше чем $\delta q - 1$. □

Следующий результат показывает, что БЧХ-коды не относятся к «асимптотически хорошим». Однако при малых N (несколько тысяч или меньше) БЧХ-коды находятся среди лучших известных кодов.

Теорема 3.3.24. *Не существует такой бесконечной последовательности q-ичных примитивных БЧХ-кодов $\mathcal{X}_N$ длины N, что пределы $d(\mathcal{X}_N)/N$ и $\operatorname{rank}(\mathcal{X}_N)/N$ будут отделены от нуля.*

Декодирование БЧХ-кодов можно осуществить с помощью так называемого алгоритма Берлекэмпа—Мэсси. Рассмотрим для начала двоичный примитивный БЧХ-код в узком смысле $\mathcal{X}(= \mathcal{X}_{2,N,5})$ длины $N = 2^l - 1$ и с проектируемым расстоянием 5. При $E = 2$ и $l \geqslant 4$ выполнено неравенство $2^{sE} < \sum_{i=0}^{E+1} C_N^i$ и по теореме 3.3.19 имеем $d(\mathcal{X}) = 5$. Значит, этот код исправляет 2 ошибки. Кроме того, по теореме 3.3.16 имеем $\operatorname{rank} \mathcal{X} \geqslant N - 2s$. (Для $s = 4$ ранг на самом деле равен $N - 2s = 15 - 8 = 7$.) Так что $\mathcal{X}$ является $[2^s - 1, \geqslant 2^s - 1 - 2s, 5]$-кодом.

Определяющие корни — это $\omega, \omega^2, \omega^3, \omega^4$, где ω — примитивный $(N, \mathbb{F}_2)$-корень из единицы (совпадающий с примитивным элементом поля $\mathbb{F}_{2^s}$). Мы знаем, что в качестве определяющих корней достаточно взять ω и ω^3: $\mathcal{X} = \{c(X) \in \mathbb{F}_2[X]/\langle X^N - 1\rangle : c(\omega) = c(\omega^3) = 0\}$. Поэтому проверочную матрицу $\tilde{H}$ из формулы (3.3.12) можно взять в виде

$$\tilde{H} = \begin{pmatrix} \vec{e} & \vec{\omega} & \vec{\omega}^2 & \dots & \vec{\omega}^{N-1} \\ \vec{e} & \vec{\omega}^3 & \vec{\omega}^6 & \dots & \vec{\omega}^{3(N-1)} \end{pmatrix}. \tag{3.3.16}$$

Поучительно сравнить эту ситуацию с $[2^l - 1, 2^l - 1 - l]$-кодом Хэмминга $\mathcal{X}^{(\mathrm{H})}$. В случае кода $\mathcal{X}$ вновь предположим, что было послано кодовое слово $c(X) \in \mathcal{X}$ и полученное слово $r(X)$ имеет не более двух ошибок. Запишем $r(X) = c(X) + e(X)$, где вес многочлена ошибок $e(X)$ не превышает 2. Нужно рассмотреть три случая: $e(X) = 0$, $e(X) = X^i$ или $e(X) = X^i + X^j$, $0 \leqslant i \neq j \leqslant N - 1$. Если $r(\omega) = r_1$ и $r(\omega^3) = r_3$, то $e(\omega) = r_1$ и $e(\omega^3) = r_3$. Когда ошибок нет ($e(X) = 0$), получаем, что $r_1 = r_3 = 0$ и наоборот. В случае единственной ошибки ($e(X) = X^i$) имеем

$$r_3 = e(\omega^3) = \omega^{3i} = (\omega^i)^3 = (e(\omega))^3 = r_1^3 \neq 0.$$

Обратно, если $r_3 = r_1^3 \neq 0$, то $e(\omega^3) = e(\omega)^3$. Если $e(X) = X^i + X^j$ с $i \neq j$, то

$$\omega^{3i} + \omega^{3j} = (\omega^i + \omega^j)^3 = \omega^{3i} + \omega^{2i}\omega^j + \omega^i\omega^{2j} + \omega^{3j},$$

т. е. $\omega^{2i}\omega^j + \omega^i\omega^{2j} = 0$ или $\omega^i + \omega^j = 0$, откуда следует, что $i = j$ — противоречие. Таким образом, единственная ошибка возникает тогда и только тогда, когда $r_3 = r_1^3 \neq 0$ и номер ошибочного символа i находится из условия $r_1 = \omega^i$. Значит, в случае одной ошибки мы отождествляем столбцы матрицы $\tilde{H}$, т. е. $(\omega^i, \omega^{3i}) = (r_1, r_3)$ и меняем знак i в слове $r(X)$. Это полностью аналогично процедуре декодирования кода Хэмминга.

В случае двух ошибок ($e(X) = X^i + X^j$, $i \neq j$) в духе кода Хэмминга мы пытаемся отыскать такую пару столбцов (ω^i, ω^{3i}) и (ω^j, ω^{3j}), что $(\omega^i + \omega^j, \omega^{3i} + \omega^{3j}) = (r_1, r_3)$, т. е. решаем уравнения

$$r_1 = \omega^i + \omega^j, \quad r_3 = \omega^{3i} + \omega^{3j}.$$

Затем найдём такие i, j, что $y_1 = \omega^i$, $y_2 = \omega^j$ (y_1, y_2 называются *локаторами ошибок*.) Если такие i, j (или, что эквивалентно, локаторы y_1, y_2) найдены, мы знаем, что ошибки возникают на позициях i и j.

Удобно ввести *многочлен обнаружения ошибок* $\sigma(X)$, корнями которого являются y_1^{-1}, y_2^{-1}:

$$\sigma(X) = (1 - y_1X)(1 - y_2X) = 1 - (y_1 + y_2)X + y_1y_2X^2 = \\ = 1 - r_1X + (r_3r_1^{-1} - r_1^2)X^2. \quad (3.3.17)$$

Поскольку $y_1 + y_2 = r_1$, можно убедиться, что $y_1y_2 = r_3r_1^{-1} - r_1^2$. Действительно,

$$r_3 = y_1^3 + y_2^3 = (y_1 + y_2)(y_1^2 + y_1y_2 + y_2^2) = r_1(r_1^2 + y_1y_2).$$

Если N невелико, корни многочлена $\sigma(X)$ можно найти, подставляя все $2^s - 1$ ненулевые элементы поля $\mathbb{F}_{2^s}$. (Стандартная формула корней квадратного многочлена неприменима над $\mathbb{F}_2$.) Эти наблюдения суммирует следующий результат.

Теорема 3.3.25. *Для $N = 2^l - 1$ рассмотрим двоичный примитивный БЧХ-код в узком смысле $\mathcal{X}(=\mathcal{X})$, исправляющий 2 ошибки, длины N с проектируемым расстоянием 5 и проверочной матрицей*

$$\tilde{H} = \begin{pmatrix} e & \omega & \omega^2 & \dots & \omega^{N-1} \\ e & \omega^3 & \omega^6 & \dots & \omega^{3(N-1)} \end{pmatrix},$$

возможно после удаления линейно зависимых столбцов. Здесь ω — примитивный элемент поля $\mathbb{F}_{2^l}$. (Ранг кода не меньше $N - 2l$, и при $l \geqslant 4$ расстояние равно 5, т.е. $\mathcal{X}$ — $[2^l - 1, \geqslant 2^l - 1 - 2l, 5]$-код, исправляющий 2 ошибки.) Предположим, что в полученном слове $r(X)$ не более 2 ошибок, и пусть $r(\omega) = r_1$, $r(\omega^3) = r_3$. Тогда

а) *если $r_1 = 0$, то $r_3 = 0$ и ошибок нет,*

б) *если $r_3 = r_1^3 \neq 0$, то возникла единственная ошибка на месте i, где $r_1 = \omega^i$,*

в) *если $r_1 \neq 0$ и $r_3 \neq r_1^3$, то возникло 2 ошибки. Многочлен обнаружения ошибок $\sigma(X) = 1 - r_1 X + (r_3 r_1^{-1} - r_1^2)X^2$ имеет два разных корня ω^{N-i+1}, ω^{N-j+1}, и номера ошибочных знаков — i и j.*

Для общего двоичного БЧХ-кода с проектируемым расстоянием δ ($\delta = 2E + 1$ предполагается нечётным) мы руководствуемся той же идеей: вычисляем

$$r_1 = e(\omega),\ r_3 = e(\omega^3),\ \dots,\ r_{\delta-2} = e(\omega^{\delta-2})$$

для полученного слова $r(X) = c(X) + e(X)$. Предположим, что ошибки появляются на местах с номерами $i_1, \dots, i_t$. Тогда

$$e(X) = \sum_{j=1}^{t} X^{t_j}.$$

Как и раньше, рассмотрим систему

$$\sum_{j=1}^{t} \omega^{i_j} = r_1, \quad \sum_{j=1}^{t} \omega^{3i_j} = r_3, \quad \dots, \quad \sum_{j=1}^{t} \omega^{(\delta-2)i_j} = r_{\delta-2}$$

и введём локаторы ошибок $y_j = \omega^{i_j}$:

$$\sum_{j=1}^{t} y_j = r_1, \quad \sum_{j=1}^{t} y_j^3 = r_3, \quad \dots, \quad \sum_{j=1}^{t} y_j^{\delta-2} = r_{\delta-2}.$$

Корнями многочлена обнаружения ошибок

$$\sigma(X) = \prod_{j=1}^{t} (1 - y_j X)$$

будут элементы y_j^{-1}. Коэффициенты σ_i многочлена $\sigma(X) = \sum_{i=0}^{t} \sigma_i X^i$ определяются из следующего уравнения:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ r_2 & r_1 & 1 & 0 & 0 & \dots & 0 \\ r_4 & r_3 & r_2 & r_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ r_{2t-4} & r_{2t-5} & \dots & \dots & \dots & \dots & r_{t-3} \\ r_{2t-2} & r_{2t-3} & \dots & \dots & \dots & \dots & r_{t-1} \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_{2t-3} \\ \sigma_{2t-1} \end{pmatrix} = \begin{pmatrix} r_1 \\ r_3 \\ r_5 \\ \vdots \\ r_{2t-3} \\ r_{2t-1} \end{pmatrix},$$

причем достаточно найти r_k только с нечётными k, поскольку

$$r_{2j} = e(\omega^{2j}) = e(\omega^j)^2 = r_j^2.$$

По найденным σ_i можно найти y_j^{-1} методом проб и ошибок.

Пример 3.3.26. Рассмотрим код $\mathcal{X}_{2,15,\omega,5}$, где ω — примитивный элемент поля $\mathbb{F}_{16}$. Мы знаем, что к примитивным многочленам относятся $M_1(X) = X^4 + X + 1$ и $M_3(X) = X^4 + X^3 + X^2 + X + 1$. Значит, порождающий полином кода равен

$$g(X) = M_1(X)M_3(X) = X^8 + X^7 + X^6 + X^4 + 1.$$

Внесём две ошибки в кодовое слово $\mathbf{c} = 100010111000000$ на 5-е и 13-е места, взяв $e(X) = X^{12} + X^8 + X^7 + X^6 + 1$. Тогда

$$r_1 = e(\omega) = \omega^{12} + \omega^8 + \omega^7 + \omega^6 + 1 = \omega^6,$$
$$r_3 = e(\omega^3) = \omega^{36} + \omega^{24} + \omega^{21} + \omega^{18} + 1 = \omega^9 + \omega^3 + 1 = \omega^4.$$

Так как $r_3 \neq r_1^3$, рассмотрим многочлен обнаружения ошибок

$$\sigma(X) = 1 + \omega^6 X + (\omega^{13} + \omega^{12})X^2.$$

Его корни — это ω^3 и ω^{11}, что проверятся подстановкой. Следовательно, мы найдём ошибки на 5-м и 13-м местах. □

§ 3.4. Тождество Мак-Вильямс. Граница линейного программирования

> Специалист по алгебраическому кодированию делает это в группах (или даже в групповых алгебрах).
>
> (Из серии «Как они делают это».)

Тождество Мак-Вильямс для линейных кодов имеет дело с так называемой производящей функции весов $W_{\mathcal{X}}(z)$ и $W_{\mathcal{X}^\perp}(z)$, где $\mathcal{X}$ и $\mathcal{X}^\perp$ —

пара двойственных кодов длины N. *Производящие функции весов* $W_{\mathcal{X}}(z)$ и $W_{\mathcal{X}^\perp}(z)$ определяются по правилу

$$W_{\mathcal{X}}(z) = \sum_{k=0}^{N} A_k z^k \quad \text{и} \quad W_{\mathcal{X}^\perp}(z) = \sum_{k=0}^{N} A_k^\perp z^k, \tag{3.4.1}$$

где A_k $(= A_k(\mathcal{X}))$ равно числу кодовых слов веса k в $\mathcal{X}$, а $A_k^\perp$ — тому же числу в коде $\mathcal{X}^\perp$. Лемма 3.4.6 устанавливает тождество

$$W_{\mathcal{X}^\perp}(z) = \frac{1}{\#\mathcal{X}}(1 + (q-1)z)^N W_{\mathcal{X}}\left(\frac{1-z}{1+(q-1)z}\right), \quad z \in \mathbb{C}, \tag{3.4.2}$$

которое принимает особенно красивый вид в двоичном случае $(q = 2)$:

$$W_{\mathcal{X}^\perp}(z) = \frac{1}{\#\mathcal{X}}(1+z)^N W_{\mathcal{X}}\left(\frac{1-z}{1+z}\right). \tag{3.4.3}$$

Короткий вывод абстрактного тождества Мак-Вильямс довольно алгебраичен. При первом чтении его можно пропустить, так как в дальнейшем будет использоваться его конкретизация для линейных кодов.

Определение 3.4.1. Пусть $(G, +)$ — группа. Гомоморфизм χ из G в мультипликативную группу комплексных чисел $\mathbb{S}' = \{z \in \mathbb{C}\colon |z| = 1\}$ называется (одномерным) *характером* группы G. Поскольку $\mathcal{X}$ — гомоморфизм, имеем

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2), \quad \chi(0) = 1. \tag{3.4.4}$$

Назовём характер χ *тривиальным* (или главным), если $\chi(\,\cdot\,) \equiv 1$.

Более общим образом, *линейным представлением* D группы G над полем $\mathbb{F}$ (не обязательно конечным) называется гомоморфизм

$$D\colon G \to \mathrm{GL}(V)\colon g \mapsto D(g) \tag{3.4.5}$$

из G в группу $\mathrm{GL}(V)$ обратимых линейных отображений конечномерного пространства V над $\mathbb{F}$ в себя. Векторное пространство V называется *пространством представления*, а его размерность $\dim V$ — *размерностью представления*.

Пусть D — представление группы G. Тогда отображение

$$\chi^D\colon G \to \mathbb{F}\colon g \mapsto \sum d_{ii}(g) = \mathrm{trace}(D(g)), \tag{3.4.6}$$

переводящее $g \in G$ в $\chi^D(g)$, след отображения $D(g) = (d_{ij}(g))$, называется *характером* представления D. Представления и характеры над полем $\mathbb{C}$ комплексных чисел называются обыкновенными. В ситуации, когда поле коэффициентов $\mathbb{F}$ конечно, они называются *модулярными*. □

В нашем случае $G = \mathbb{F}_q$ с аддитивной групповой операцией. Фиксируем примитивный корень из единицы степени q: $\omega = 2^{2\pi i/q} \in \mathbb{S}'$ и для любого $j \in \mathbb{F}_q$ определим одномерное представление группы $\mathbb{F}_q$ следующим образом:

$$\chi^{(j)} : \mathbb{F}_q \to \mathbb{S}' : u \mapsto \omega^{ju}.$$

Характер $\chi^{(j)}$ нетривиален при $j \neq 0$. Фактически все характеры группы $\mathbb{F}_q$ можно описать таким способом, но мы не будем этого доказывать.

Далее, мы изучаем характеры группы $G = \mathbb{F}_q^N$. Фиксируем нетривиальный одномерный характер $\chi : \mathbb{F}_q \to \mathbb{S}'$ и ненулевой элемент $\mathbf{v} \in \mathbb{F}_q^N$ и определим характер аддитивной группы $G = \mathbb{F}_q^N$ как

$$\chi_{(\mathbf{v})} : \mathbb{F}_q^N \to \mathbb{S}' : \mathbf{u} \mapsto \chi(\langle \mathbf{v} \cdot \mathbf{u} \rangle), \tag{3.4.7}$$

где $\langle \mathbf{v} \cdot \mathbf{u} \rangle$ — скалярное произведение.

Лемма 3.4.2. *Пусть χ — нетривиальный (т. е. $\chi \not\equiv 1$) характер конечной группы G. Тогда*

$$\sum_{g \in G} \chi(g) = 0. \tag{3.4.8}$$

А если характер χ тривиален, то $\sum\limits_{g \in G} \chi(g) = \#G$.

Доказательство. Так как характер χ нетривиален, существует элемент $h \in G$, для которого $\chi(h) \neq 1$. Тогда из соотношения

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g)$$

вытекает, что $(\chi(h) - 1) \sum\limits_{g \in G} \chi(g) = 0$. Значит, $\sum\limits_{g \in G} \chi(g) = 0$. □

В случае $G = \mathbb{F}_q^N$ для тривиального характера имеем $\sum\limits_{\mathbf{x} \in \mathbb{F}_q^N} \chi(\mathbf{x}) = q^N$.

Определение 3.4.3. *Дискретное преобразование Фурье* (ДПФ) функции f на $\mathbb{F}_q^N$ определяется по формуле

$$\hat{f} = \sum_{\mathbf{v} \in \mathbb{F}_q^N} f(\mathbf{v}) \chi_{(\mathbf{v})}. \tag{3.4.9}$$

□

Иногда производящая функция весов кода $\mathcal{X}$ определяется как многочлен от двух формальных переменных x, y (будем писать $W_{\mathcal{X}} \in \mathcal{C}[x, y]$):

$$W_{\mathcal{X}}(x, y) = \sum_{\mathbf{v} \in \mathcal{X}} x^{w(\mathbf{v})} y^{N - w(\mathbf{v})} \tag{3.4.10}$$

(если положить $x = z$, $y = 1$, то формула (3.4.10) совпадёт с (3.4.1)). Итак, мы хотим применить ДПФ к функции (можно сказать, что x, $y \in \mathbb{S}'$)

$$g\colon \mathbb{F}_q^N \to \mathcal{C}[x, y]\colon \mathbf{v} \mapsto x^{w(\mathbf{v})} y^{N-w(\mathbf{v})}. \tag{3.4.11}$$

Лемма 3.4.4 (абстрактное тождество Мак-Вильямс). *Для* $\mathbf{v} \in \mathbb{F}_q^N$ *положим*

$$g\colon \mathbb{F}_q^N \to \mathcal{C}[x, y]\colon \mathbf{v} \mapsto x^{w(\mathbf{v})} y^{N-w(\mathbf{v})}. \tag{3.4.12}$$

Тогда

$$\hat{g}(\mathbf{u}) = (y - x)^{w(\mathbf{u})}(y + (q-1)x)^{N-w(\mathbf{u})}. \tag{3.4.13}$$

Доказательство. Пусть χ обозначает нетривиальный (обыкновенный) характер аддитивной группы $G = \mathbb{F}_q$. Для данного $\alpha \in \mathbb{F}_q$ положим $|\alpha| = 0$, если $\alpha = 0$, и $|\alpha| = 1$ в противном случае. Тогда для произвольного $\mathbf{u} \in \mathbb{F}_q^N$ мы вычисляем

$$\begin{aligned}
\hat{g}(\mathbf{u}) &= \sum_{\mathbf{v}\in\mathbb{F}_q^N} \chi(\langle \mathbf{v}, \mathbf{u}\rangle) g(\mathbf{v}) = \sum_{\mathbf{v}\in\mathbb{F}_q^N} \chi(\langle \mathbf{v}, \mathbf{u}\rangle) x^{w(\mathbf{v})} y^{N-w(\mathbf{v})} = \\
&= \sum_{v_0\in\mathbb{F}_q} \cdots \sum_{v_{N-1}\in\mathbb{F}_q} \chi\left(\sum_{i=0}^{N-1} v_i u_i\right) x^{|v_0|+\ldots+|v_{N-1}|} y^{(1-|v_0|)+\ldots+(1-|v_{N-1}|)} = \\
&= \sum_{v_0\in\mathbb{F}_q} \cdots \sum_{v_{N-1}\in\mathbb{F}_q} \prod_{i=0}^{N-1} \chi(v_i u_i) x^{|v_i|} y^{1-|v_i|} = \prod_{i=0}^{N-1} \sum_{g\in G} \chi(g u_i) x^{|g|} y^{1-|g|}.
\end{aligned}$$

Если $u_i = 0$, то $\chi(g u_i) = \chi(0) = 1$ и

$$\sum_{g\in G} x^{|g|} y^{1-|g|} = y + (q-1)x.$$

Если $u_i \neq 0$, то

$$\sum_{g\in G} \chi(g u_i) x^{|g|} y^{1-|g|} = y + \sum_{g\in G\setminus\{0\}} \chi(g u_i) x = y - \chi(0)x = y - x. \qquad \square$$

Лемма 3.4.5 (тождество Мак-Вильямс для линейных кодов). *Если* $\mathcal{X}$ *— линейный* $[N, k]$*-код над* $\mathbb{F}_q$*, то*

$$\sum_{\mathbf{x}\in\mathcal{X}} \hat{f}(\mathbf{x}) = q^k \sum_{\mathbf{y}\in\mathcal{X}^\perp} f(\mathbf{y}). \tag{3.4.14}$$

Доказательство. Рассмотрим сумму

$$\sum_{\mathbf{x}\in\mathcal{X}}\hat{f}(\mathbf{x})=\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{v}\in\mathbb{F}_q^N}\chi_{(\mathbf{v})}(\mathbf{x})f(\mathbf{v})=\sum_{\mathbf{v}\in\mathbb{F}_q^N}\sum_{\mathbf{x}\in\mathcal{X}}\chi(\langle\mathbf{v},\,\mathbf{x}\rangle)f(\mathbf{v})=$$

$$=\sum_{\mathbf{v}\in\mathcal{X}^\perp}\sum_{\mathbf{x}\in\mathcal{X}}\chi(\langle\mathbf{v},\,\mathbf{x}\rangle)f(\mathbf{v})+\sum_{\mathbf{v}\in\mathbb{F}_q^N\setminus\mathcal{X}^\perp}\sum_{\mathbf{x}\in\mathcal{X}}\chi(\langle\mathbf{v},\,\mathbf{x}\rangle)f(\mathbf{v}).$$

В первой сумме мы имеем $\chi(\langle\mathbf{v},\,\mathbf{x}\rangle)=\chi(0)=1$ для всех $\mathbf{v}\in\mathcal{X}^\perp$ и всех $\mathbf{x}\in\mathcal{X}$. Во второй сумме мы изучаем линейную форму

$$\mathcal{X}\to\mathbb{F}_q\colon\mathbf{x}\mapsto\langle\mathbf{v},\,\mathbf{x}\rangle.$$

Так как $\mathbf{v}\in\mathbb{F}_q^N\setminus\mathcal{X}^\perp$, эта линейная форма сюръективна, а размерность ее ядра равна $k-1$, т. е. для любого $y\in\mathbb{F}_q$ найдётся q^{k-1} таких векторов $\mathbf{x}\in\mathcal{X}$, что $\langle\mathbf{v},\,\mathbf{x}\rangle=g$. Отсюда следует, что

$$\sum_{\mathbf{x}\in\mathcal{X}}\hat{f}(\mathbf{x})=q^k\sum_{\mathbf{y}\in\mathcal{X}^\perp}f(\mathbf{y})+q^{k-1}\sum_{\mathbf{v}\in\mathbb{F}_q^N\setminus\mathcal{X}^\perp}f(\mathbf{v})\sum_{g\in G}\chi(g)=q^k\sum_{\mathbf{y}\in\mathcal{X}^\perp}f(\mathbf{y}),$$

поскольку второе слагаемое равно нулю по лемме 3.4.2. □

Лемма 3.4.6. *Производящая функция весов $[N,\,k]$-кода $\mathcal{X}$ над полем $\mathbb{F}_q$ связана с производящей функцией весов двойственного кода формулой*:

$$W_{\mathcal{X}^\perp}(x,\,y)=q^{-k}W_{\mathcal{X}}(y-x,\,y+(q-1)x).\tag{3.4.15}$$

Доказательство. По лемме 3.4.5 с $g(\mathbf{v})=x^{w(\mathbf{v})}y^{N-w(\mathbf{v})}$ имеем

$$W_{\mathcal{X}^\perp}(x,\,y)=\sum_{\mathbf{v}\in\mathcal{X}^\perp}g(\mathbf{v})=q^{-k}\sum_{\mathbf{v}\in\mathcal{X}}\hat{g}(\mathbf{v})=q^{-k}W_{\mathcal{X}}(y-x,\,y+(q-1)x).$$

Подставляя $x=z$, $y=1$, мы получаем формулу (3.4.2). □

Пример 3.4.7. 1. Для всех кодов $\mathcal{X}$ имеем $W_{\mathcal{X}}(0)=A_0=1$ и $W_{\mathcal{X}}(1)=\#\mathcal{X}$. Когда $\mathcal{X}=\mathbb{F}_q^N$, имеем $W_{\mathcal{X}}(z)=(1+z(q-1))^N$.

2. Для двоичного кода повторений $\mathcal{X}=\{0000,\,1111\}$ имеем $W_{\mathcal{X}}(x,\,y)=x^4+y^4$. Следовательно,

$$W_{\mathcal{X}^\perp}(x,\,y)=\frac{1}{2}((y-x)^4+(y+x)^4)=y^4+6x^2y^2+x^4.$$

3. Пусть $\mathcal{X}$ — $[7,\,4]$-код Хэмминга. В двойственном коде $\mathcal{X}^\perp$ есть 8 кодовых слов, причём вес всех кодовых слов, кроме $\mathbf{0}$, равен 4. Значит, $W_{\mathcal{X}^\perp}(x,\,y)=x^7+7x^4y^3$, и по тождеству Мак-Вильямс

$$W_{\mathcal{X}}=\frac{1}{2^3}W_{\mathcal{X}^\perp}(x-y,\,x+y)=\frac{1}{2^3}((x-y)^7+7(x-y)^4(x+y)^3)=$$

$$=x^7+7x^4y^3+7x^3y^4+y^4.$$

Следовательно, в коде $\mathcal{X}$ есть 7 слов веса 3 и 7 слов веса 4. Вместе со словами $\mathbf{0}$ и $\mathbf{I}$ они дают все 16 слов $[7, 4]$-кода Хэмминга. □

Другой способ получения тождества (3.4.1) состоит в использовании абстрактного результата о групповых алгебрах и характерах преобразования пространства Хэмминга $\mathbb{F}_q^N$ (линейного пространства над полем $\mathbb{F}_q$ размерности N). Для краткости индексы q и (N) будут часто опускаться.

Определение 3.4.8. Комплексной *групповой алгеброй* $\mathbb{C}\mathbb{F}^N$ для пространства $\mathbb{F}^N$ называется линейное пространство комплексных функций $G\colon \mathbf{x} \in \mathbb{F}^N \mapsto G(\mathbf{x}) \in \mathbb{C}$, снабжённое комплексной инволюцией (сопряжением) и умножением. Итак, у нас есть четыре операции над функциями $G(\mathbf{x})$. Сложение и умножение на скаляры стандартны (поточечно): $(G + G')(\mathbf{x}) = G(\mathbf{x}) + G'(\mathbf{x})$ и $(aG)(\mathbf{x}) = aG(\mathbf{x})$, $G, G' \in \mathbb{C}\mathbb{F}^{\times N}$, $a \in \mathbb{C}$, $\mathbf{x} \in \mathbb{F}^N$. Инволюция — это в точности поточечное комплексное сопряжение: $G^*(\mathbf{x}) = G(\mathbf{x})^*$; при этом $G^{**} = G$. С другой стороны, умножение (обозначаемое символом $*$) — это свёртка:

$$(G \star G')(\mathbf{x}) = \sum_{\mathbf{y} \in \mathbb{F}^N} G(\mathbf{y}) G'(\mathbf{x} - \mathbf{y}), \qquad \mathbf{x} \in \mathbb{F}^N. \tag{3.4.16}$$

Эти операции наделяют множество $\mathbb{C}\mathbb{F}^N$ структурой коммутативного кольца и в то же время структурой (комплексного) линейного пространства размерности q^N с инволюцией. (Множество, одновременно являющееся как коммутативным кольцом, так и линейным пространством, называется алгеброй.) Естественный базис в $\mathbb{C}\mathbb{F}^N$ получается с помощью δ-функции Дирака (или Кронекера) $\delta^{\mathbf{y}}$ со значениями $\delta^{\mathbf{y}}(\mathbf{x}) = \mathbf{I}(\mathbf{x} = \mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}^N$.

Если $\mathcal{X} \subseteq \mathbb{F}^N$ — линейный код, мы положим $G_{\mathcal{X}}(\mathbf{x}) = \mathbf{I}(\mathbf{x} \in \mathcal{X})$. □

Правило умножения (3.4.16) требует пояснений. Если переписать п. ч. этой формулы в симметричном виде $\sum_{\substack{\mathbf{y},\mathbf{y}' \in \mathbb{F}^N: \\ \mathbf{y}+\mathbf{y}' = \mathbf{x}}} G(\mathbf{y}) G(\mathbf{y}')$ (что делает коммутативность свёртки очевидной), то возникает аналогия с умножением многочленов. Действительно, если $A(t) = a_0 + a_1 t + \ldots + a_{l-1} t^{l-1}$ и $A'(t) = a'_0 + a'_1 t + \ldots + a'_{l'-1} t^{l'-1}$ — два многочлена со строками коэффициентов $a_0 \ldots a_{l-1}$ и $a'_0 \ldots a'_{l'-1}$, то их произведение $B(t) = A(t)A'(t)$ имеет строку коэффициентов $b_0 \ldots b_{l-1+l'-1}$, где $b_k = \sum_{\substack{m,m' \geqslant 0: \\ m+m' = k}} a_m a'_{m'}$.

С этой точки зрения правило (3.4.16) задаёт что-то похожее на умножение многочленов. Многочлены, степень которых не превосходит $n - 1$, конечно, образуют (комплексное) линейное пространство степени n. Однако они не образуют группу (или даже полугруппу). Чтобы получить группу, нужно присоединить обратные мономы $1/t$, $1/t^2$ и т. д. и либо рассматривать бесконечные ряды, либо согласиться, что $t^n = 1$ (т. е. что

t — элемент конечной циклической группы, а не «свободная» переменная). Аналогичную конструкцию можно провести и с многочленами от нескольких переменных.

Возвращаясь к групповой алгебре $\mathbb{C}\mathcal{H}$, мы делаем следующие шаги.

1) Создаём «мультипликативную» версию группы Хэмминга $\mathcal{H}$, т. е. берём набор «формальных» переменных $t^{(\mathbf{x})}$, помеченных элементами $\mathbf{x} \in \mathcal{H}$ и постулируем правило $t^{(\mathbf{x})}t^{(\mathbf{x}')} = t^{(\mathbf{x}+\mathbf{x}')}$ $\forall \mathbf{x}, \mathbf{x}' \in \mathbb{C}\mathcal{H}$.

2) Затем рассматриваем множество $\mathbb{T}\mathcal{H}$ всех (комплексных) линейных комбинаций $G = \sum_{\mathbf{x}\in\mathcal{H}} \gamma_{\mathbf{x}} t^{(\mathbf{x})}$ и вводим: а) сложение $G + G' = \sum_{\mathbf{x}\in\mathcal{H}} (\gamma_{\mathbf{x}} + \gamma'_{\mathbf{x}}) t^{(\mathbf{x})}$ и б) умножение на скаляры $aG = \sum_{\mathbf{x}\in\mathcal{H}} (a\gamma_{\mathbf{x}}) t^{(\mathbf{x})}$, $G, G' \in \mathbb{T}\mathcal{H}$, $a \in \mathbb{C}$. Мы опять получим линейное пространство размерности q^N с базисом, образованным «базисными» комбинациями $t^{(\mathbf{x})}$, $\mathbf{x} \in \mathcal{H}$.

3) Теперь удалим скобки из обозначения $t^{(\mathbf{x})}$ (но сохраним правило $t^{\mathbf{x}}t^{\mathbf{x}'} = t^{\mathbf{x}+\mathbf{x}'}$) и запишем $\sum_{\mathbf{x}\in\mathcal{H}} \gamma_{\mathbf{x}} t^{\mathbf{x}}$ как $g(t)$, представляя себе это выражение как функцию (более того, полином) некоторых «переменных» t, подчиняющихся описанному выше правилу. Наконец, рассмотрим умножение многочленов $g(t)g'(t)$ из $\mathbb{T}\mathcal{H}$. Очевидно, $\mathbb{T}\mathcal{H}$ и $\mathbb{C}\mathcal{H}$ изоморфны как линейные пространства с $G \leftrightarrow g$, однако $\mathbb{T}\mathcal{H}$ и $\mathbb{C}\mathcal{H}$ изоморфны не только как линейные пространства, но также как и кольца, т. е. как алгебры.

Описанная выше конструкция довольно общая и может быть применена к любой группе, а не только к $\mathcal{H}_N$. Её сила проявится при выводе тождества Мак-Вильямс.

Итак, мы будем представлять себе $\mathbb{C}\mathcal{H}$ как множество функций

$$g(t) = \sum_{\mathbf{x}\in\mathcal{H}_N} \gamma_{\mathbf{x}} t^{\mathbf{x}} \tag{3.4.17}$$

формальной переменной t, подчиняющейся «экспоненциальному» правилу: $t^{\mathbf{x}+\mathbf{x}'} = t^{\mathbf{x}}t^{\mathbf{x}'}$, со сложением и умножением формальных многочленов.

Помня о соглашении (3.4.17), для линейного кода $\mathcal{X} \subset \mathcal{H}_N$ положим

$$g_{\mathcal{X}}(t) = \sum_{\mathbf{x}\in\mathcal{X}} t^{\mathbf{x}}; \tag{3.4.18}$$

$g_{\mathcal{X}}(t)$ часто называют *производящим полиномом кода* $\mathcal{X}$.

Определение 3.4.3 допускает прямое обобщение на любой нетривиальный характер $\chi\colon \mathbb{F} \to \mathbb{S}$. Отметим аналогию с преобразованием Фурье (и другими типами известных преобразований, например, с преобразованием Адамара в теории групп).

Определение 3.4.9. *Преобразование характеров* $g \mapsto \hat{g}$ групповой алгебры $\mathbb{C}\mathcal{H}_N$ определяется как

$$\hat{g}(t) = \sum_{\mathbf{x}\in\mathcal{H}_N} X_{\mathbf{x}}(g) t^{\mathbf{x}}, \tag{3.4.19а}$$

где $g \sim (\gamma_{\mathbf{x}},\ \mathbf{x} \in \mathcal{H}_N)$ и

$$X_{\mathbf{x}}(g) = \sum_{\mathbf{y}\in\mathcal{H}_N} \gamma_{\mathbf{y}} \chi(\langle \mathbf{x}\cdot\mathbf{y}\rangle), \tag{3.4.19б}$$

а $\langle \mathbf{x}\cdot\mathbf{y}\rangle$ — скалярное произведение $\sum\limits_{j=1}^{N} x_j y_j$ в $\mathcal{H}_N$. □

Теперь определим *производящую функцию весов* элемента групповой алгебры $g \in \mathbb{C}\mathcal{H}$ как многочлен $W_g(s)$ от переменной s (которую можно считать комплексной переменной):

$$W_g(s) = \sum_{\mathbf{x}\in\mathcal{H}_N} \gamma_{\mathbf{x}} s^{w(\mathbf{x})} = \sum_{k=0}^{N} \left[\sum_{\mathbf{x}:\ w(\mathbf{x})=k} \gamma_{\mathbf{x}} \right] s^k = \sum_{k=0}^{N} A_k s^k, \quad s \in \mathbb{C}. \tag{3.4.20}$$

Здесь

$$A_k = \sum_{\substack{\mathbf{x}\in\mathcal{H}:\\ w(\mathbf{x})=k}} \gamma_k. \tag{3.4.21}$$

Для линейного кода $\mathcal{X}$ с образующей функцией $g_{\mathcal{X}}(t)$ (см. формулу (3.4.18)) коэффициенты A_k означают число кодовых слов веса k:

$$A_k = \#\{\mathbf{x} \in \mathcal{X}\colon w(\mathbf{x}) = k\}. \tag{3.4.22}$$

Производящая функция весов $W_{\hat{g}}(s)$ преобразования характера $\hat{g}$ функции $g \sim (\gamma_k,\ \mathbf{x} \in \mathcal{H})$ определяется формулой

$$W_{\hat{g}}(s) = \sum_{\mathbf{x}\in\mathcal{H}} X_{\mathbf{x}}(g) s^{w(\mathbf{x})} = \sum_{k=0}^{N} \left[\sum_{\mathbf{x}:\ w(\mathbf{x})=k} X_{\mathbf{x}}(g) \right] s^k = \sum_{k} \hat{A}_k s^k, \tag{3.4.23}$$

где

$$\hat{A}_k = \sum_{\substack{\mathbf{x}\in\mathcal{H}:\\ w(\mathbf{x})=k}} X_{\mathbf{x}}(g). \tag{3.4.24}$$

«Абстрактное» тождество Мак-Вильямс устанавливается в следующей теореме.

Теорема 3.4.10. *Справедливо равенство*

$$W_{\hat{g}}(s) = (1 + (q-1)s)^N W_g\left(\frac{1-s}{1+(q-1)s}\right). \tag{3.4.25}$$

Доказательство в основном совпадает с доказательством леммы 3.4.4. □

Перепишем тождество (3.4.25) через коэффициенты A_k и $\hat{F}_k$.

$$\sum_{k=0}^{N} \hat{A}_k s^k = \sum_{k=0}^{N} A_k (1-s)^k (1+(q-1)s)^{N-k} \tag{3.4.26}$$

и раскроем скобки:

$$(1-s)^k (1+(q-1)s)^{N-k} = \sum_{i=0}^{N} K_i(k) s^i. \tag{3.4.27}$$

Здесь $K_i(k) (= K_i(k, N, q))$ — многочлен Кравчука:

$$K_i(k) = \sum_{j=0 \vee (i+k-N)}^{i \wedge k} C_k^j C_{N-k}^{i-j} (-1)^j (q-1)^{i-j} \quad \forall i,\ k = 0, 1, \ldots, N, \tag{3.4.28}$$

где $0 \vee (i+k-N) = \max[0, i+k-N]$, $i \wedge k = \min[i, k]$.

Тогда

$$\sum_{k=0}^{N} \hat{A}_k s^k = \sum_{k=0}^{N} A_k s^k \sum_{i=0}^{N} K_i(k) s^i = \sum_{i=0}^{N} \sum_{k=0}^{N} A_k K_i(k) s^i = \sum_{k=0}^{N} \sum_{i=0}^{N} A_i K_k(i) s^k,$$

т. е.

$$\hat{A}_k = \sum_{i=0}^{N} A_i K_k(i). \tag{3.4.29}$$

Михаил Филиппович Кравчук (1892–1942) — выдающийся украинский математик, работавший в Киевском политехническом институте. Одним из его студентов был Сергей Королёв, будущий глава советской аэрокосмической программы. Кравчук был арестован в 1938 г. советской госбезопасностью по сфабрикованному обвинению (он был обвинён, среди прочего, в разработке проекта независимого украинского государства), осуждён на 20 лет лагерей, и умер в лагере на Колыме.

Лемма 3.4.11. *Для любого линейного кода $\mathcal{X} \subseteq \mathcal{H}_n$ с образующей функцией $g_{\mathcal{X}} \sim \mathbf{I}(\mathbf{x} \in \mathcal{X})$ коэффициенты преобразования характеров связаны соотношением*

$$X_{\mathbf{u}}(g_{\mathcal{X}}) = \#\mathcal{X}\mathbf{I}(\mathbf{u} \in \mathcal{X}^{\perp}) \tag{3.4.30}$$

и преобразование характеров имеет вид

$$\hat{g}_{\mathcal{X}} = \#\mathcal{X} g_{\mathcal{X}^{\perp}}. \tag{3.4.31}$$

Здесь $\mathcal{X}^{\perp}$ — двойственный код.

Доказательство. По лемме 3.4.2 имеем

$$X_{\mathbf{u}}(g_{\mathcal{X}}) = X_{\mathbf{u}}\left(\sum_{\mathbf{x}\in\mathcal{X}} s^{\mathbf{x}}\right) = \sum_{\mathbf{y}\in\mathcal{X}} \chi(\langle \mathbf{y}\cdot\mathbf{u}\rangle) = \#\mathcal{X}\mathbf{I}(\mathbf{u}\in\mathcal{X}^{\perp}).$$

Следовательно,

$$\hat{g}(s) = \sum_{\mathbf{x}\in\mathcal{H}} X_{\mathbf{x}}(g_{\mathcal{X}}) s^{\mathbf{x}} = \sum_{\mathbf{x}\in\mathcal{H}} \#\mathcal{X}\mathbf{I}(\mathbf{x}\in\mathcal{X}^{\perp}) s^{\mathbf{x}} = \#\mathcal{X} \sum_{\mathbf{x}\in\mathcal{X}^{\perp}} s^{\mathbf{x}} = \#\mathcal{X} g_{\mathcal{X}^{\perp}}(s). \quad \square$$

Значит,

$$W_{\hat{g}_{\mathcal{X}}}(s) = \#\mathcal{X} W_{g_{\mathcal{X}^{\perp}}}(s), \tag{3.4.32}$$

и мы получаем тождество Мак-Вильямс для линейных кодов.

Теорема 3.4.12. *Пусть $\mathcal{X}\subset\mathcal{H}_N$ — линейный код, $\mathcal{X}^{\perp}$ — двойственный код и*

$$W_{\mathcal{X}}(s) = \sum_{k=0}^{N} A_k s^k, \quad W_{\mathcal{X}^{\perp}}(s) = \sum_{k=0}^{N} A_k^{\perp} s^k \tag{3.4.33}$$

— производящие функции весов для $\mathcal{X}$ и $\mathcal{X}^{\perp}$ соответственно, где $A_k = \#\{\mathbf{x}\in\mathcal{X}\colon w(\mathbf{x}) = k\}$ и $A_k^{\perp} = \#\{\mathbf{x}\in\mathcal{X}^{\perp}\colon w(\mathbf{x}) = k\}$. Тогда

$$W_{\mathcal{X}^{\perp}}(s) = \frac{1}{\#\mathcal{X}}(1+(q-1)s)^N W_{\mathcal{X}}\left(\frac{1-s}{1+(q-1)s}\right), \quad s\in\mathbb{C}, \tag{3.4.34}$$

или, в эквивалентной записи,

$$A_k^{\perp} = \frac{1}{\#\mathcal{X}} \sum_{i=0}^{N} A_i K_k(i), \tag{3.4.35}$$

где $K_k(i)$ — многочлен Кравчука (см. формулу (3.4.28)).

Для двоичного кода ($q=2$) формула (3.4.34) принимает вид (3.4.3). Иногда производящие функции весов определяются как

$$W_{\mathcal{X}^{\perp}}(s,\, r) = \sum_{k} A_k s^k r^{N-k}.$$

Тогда тождество Мак-Вильямс (3.4.3) принимает следующий вид:

$$W_{\mathcal{X}^{\perp}}(s,\, r) = \frac{1}{\#\mathcal{X}} W_{\mathcal{X}}(s-r,\, s+(q-1)r). \tag{3.4.36}$$

Тождество Мак-Вильямс — это впечатляющий результат, обеспечивающий глубокое проникновение в структуру (линейных) кодов, в частности, когда код самодвойственный. Это тождество названо в честь Джесси Мак-Вильямс (1917–1990), американского математика, англичанки по рождению (она окончила Кембриджский университет в Великобритании в 1939 г.). Мак-Вильямс была, пожалуй, первый женщиной, опубликовавшей работу по

теории кодирования (она первой прочла лекцию в обществе Эмми Нётер, объединяющем женщин-математиков, в 1980 г.). Тождество было одним из результатов её кандидатской диссертации в 1961 г., защищённой в Гарварде, когда ей было 44 года и у неё было трое детей; дочь (Анна Мак-Вильямс) училась в это время в том же университете. (Позже пути дочери и матери в математике пересекались снова, когда научным руководителем дочери стал один из сотрудников её матери.)

Тождество Мак-Вильямс помогает при выводе интересного ограничения на линейные коды, названного границей линейного программирования. Сначала мы обсудим некоторые непосредственные следствия этого тождества. Если $\mathcal{X} \subset \mathcal{H}_{N,q}$ — код размера M, то положим

$$B_k = \frac{1}{M}\#\{(\mathbf{x}, \mathbf{y})\colon \mathbf{x}, \mathbf{y} \in \mathcal{X},\ \ \delta(\mathbf{x}, \mathbf{y}) = k\}, \qquad k = 0, \ldots, N$$

(каждая пара $\mathbf{x}, \mathbf{y}$ учитывается дважды). Числа $B_0, B_1, \ldots, B_N$ образуют *распределение расстояний* кода $\mathcal{X}$. Выражение

$$B_{\mathcal{X}}(s) = \sum_{k=0}^{N} B_k s^k \tag{3.4.37}$$

называется *производящей функцией расстояний* кода $\mathcal{X}$. Ясно, что w- и d-распределения линейного кода совпадают. Более того, справедливо следующее утверждение.

Лемма 3.4.13. *Производящая функция расстояний* (d-*функция*) $[N, M]$-*кода* $\mathcal{X}$ *совпадает с производящей функцией весов* (w-*функцией*) *элемента групповой алгебры*

$$h_{\mathcal{X}}(s) := \frac{1}{M}\zeta_{\mathcal{X}}(s)\zeta_{\mathcal{X}}(s^{-1}), \tag{3.4.38}$$

где образующая функция кода $\mathcal{X}$ *равна*

$$\zeta_{\mathcal{X}}(s) = \sum_{\mathbf{x}\in\mathcal{X}} s^{\mathbf{x}}. \tag{3.4.39}$$

Доказательство. Используя обозначение $(s^{-1})^{\mathbf{x}}$, запишем

$$h_{\mathcal{X}}(s) = \frac{1}{M}\sum_{\mathbf{x}\in\mathcal{X}} s^{\mathbf{x}} \sum_{\mathbf{y}\in\mathcal{X}} s^{-\mathbf{y}} = \frac{1}{M}\sum_{\mathbf{x},\mathbf{y}\in\mathcal{X}} s^{\mathbf{x}-\mathbf{y}}$$

и поэтому

$$W_{h_{\mathcal{X}}}(s) = \frac{1}{M}\sum_{k=0}^{N}\sum_{\mathbf{x},\mathbf{y}\in\mathcal{X}} \mathbf{I}(w(\mathbf{x}-\mathbf{y}) = k)s^k = \sum_{k=0}^{N} B_k s^k = B_{\mathcal{X}}(s). \qquad \square$$

Линейный программист делает это при налагаемых на него ограничениях.

(Из серии «Как они делают это».)

Далее, благодаря тождеству Мак-Вильямс для нетривиального характера χ и соответствующего преобразования $\zeta \mapsto \hat{\zeta}$ мы получаем теорему.

Теорема 3.4.14. *Если $\hat{h}_{\mathcal{X}}(s)$ — преобразование характеров $h_{\mathcal{X}}(s)$, описанное выше, а $W_{\hat{h}_{\mathcal{X}}}(s)$ — его w-функция,*

$$W_{\hat{h}_{\mathcal{X}}}(s) = \sum_{k=0}^{N} \hat{B}_k s^k = \sum_{k=0}^{N} \left(\sum_{w(\mathbf{x})=k} \chi_{\mathbf{x}}(h_{\mathcal{X}}) \right) s^k,$$

то

$$\hat{B}_k = \sum_{i=0}^{N} B_i K_k(i),$$

где $K_k(i)$ — многочлены Кравчука.

Лемма 3.4.15. *Справедливо соотношение $\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s^{-1})) = \overline{\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s))}$, где черта означает комплексное сопряжение.*

Ввиду леммы 3.4.15 можно записать

$$\chi_{\mathbf{x}}(h_{\mathcal{X}}(t)) = \frac{1}{M}\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s)\zeta_{\mathcal{X}}(s^{-1})) = \frac{1}{M}\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s))\chi(\zeta_{\mathcal{X}}(s^{-1})) =$$
$$= \frac{1}{M}\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s))\overline{\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s))} = \frac{1}{M}|\chi_{\mathbf{x}}(\zeta_{\mathcal{X}}(s))|^2,$$

и поэтому

$$\hat{B}_k = \sum_{\mathbf{x}:\ w(\mathbf{x})=k} \chi_{\mathbf{x}}(h_{\mathcal{X}}) = \frac{1}{M} \sum_{w(\mathbf{x})=k} |\chi_{\mathbf{x}}(\zeta_{\mathcal{X}})|^2 \geqslant 0. \qquad \square$$

Теорема 3.4.16. *Для всех $[N, M]$-кодов $\mathcal{X}$ и $k = 0, \ldots, N$ справедливо неравенство*

$$\sum_{i=0}^{N} B_i K_k(i) \geqslant 0. \tag{3.4.40}$$

Далее, подсчитывая число пар $(\mathbf{x}, \mathbf{y}) \in \mathcal{X} \times \mathcal{X}$, получаем

$$\sum_{i=0}^{N} B_i = M^2,$$

или

$$\sum_{i=0}^{N} E_i = M, \quad E_i = \frac{B_i}{M} \tag{3.4.41}$$

(*иногда набор* $E_0, \dots, E_N$ *называют* d*-распределением кода* $\mathcal{X}$). *Тогда из формул* (3.4.40) *и* (3.4.41) *получаем, что*

$$\sum_{i=0}^{N} E_i K_k(i) \geqslant 0. \tag{3.4.42}$$

Кроме того, по определению $E_i \geqslant 0$, $0 \leqslant i \leqslant N$, *и* $E_0 = 1$, *а* $E_i = 0$ *при* $1 \leqslant i < d$.

Доказательство. Пусть ω — примитивный корень из единицы степени q и $\mathbf{x} \in \mathbb{F}_q^N$ — фиксированное слово веса i. Тогда

$$\sum_{\substack{\mathbf{y} \in \mathbb{F}_q^N: \\ w(\mathbf{y}) = k}} \omega^{\langle \mathbf{x}, \mathbf{y} \rangle} = K_k(i). \tag{3.4.43}$$

Действительно, мы можем считать, что $\mathbf{x} = x_1 x_2 \dots x_i 0 \dots 0$, где $x_i \neq 0$. Пусть D — множество слов с ненулевыми координатами на данных i позициях. Предположим, что j позиций из $h_1, \dots, h_i$ попадают в $[0, k]$, а остальные $i - j$ позиций — в $[k+1, N]$. Такое разбиение можно выбрать $C_k^j C_{N-k}^{i-j}$ способами. Поэтому

$$\sum_{\mathbf{y} \in D} \omega^{\langle \mathbf{x}, \mathbf{y} \rangle} = \sum_{y_{h_1} \in \mathbb{F}_q^*} \dots \sum_{y_{h_k} \in \mathbb{F}_q^*} \omega^{x_{h_1} y_{h_1} + \dots + x_{h_k} y_{h_k}} =$$

$$= (q-1)^{i-j} \prod_{l=1}^{j} \sum_{y \in \mathbb{F}_q^*} \omega^{x_{h_l} y} = (-1)^j (q-1)^{i-j}.$$

Следовательно,

$$M \sum_{i=0}^{N} B_i K_k(i) = \sum_{i=0}^{N} \sum_{\substack{\mathbf{x}, \mathbf{y} \in \mathcal{X}: \\ \delta(\mathbf{x}, \mathbf{y}) = i}} \sum_{\substack{\mathbf{z} \in \mathbb{F}_q^N: \\ w(\mathbf{z}) = k}} \omega^{\langle \mathbf{x} - \mathbf{y}, \mathbf{z} \rangle} = \sum_{\substack{\mathbf{z} \in \mathbb{F}_q^N: \\ w(\mathbf{z}) = k}} \left| \sum_{\mathbf{x} \in \mathcal{X}} \omega^{\langle \mathbf{x}, \mathbf{z} \rangle} \right|^2 \geqslant 0. \qquad \square$$

Это подводит нас к так называемой границе линейного программирования.

Теорема 3.4.17 (граница линейного программирования). *Имеет место следующее неравенство*:

$$M_q^*(N, d) \leqslant \max \left[\sum_{i=0}^{N} \tilde{E}_i \colon \tilde{E}_i \geqslant 0,\ \tilde{E}_0 = 1,\ \tilde{E}_i = 0 \text{ при } 1 \leqslant i < d \right.$$

$$\left. \text{и} \quad \sum_{i=0}^{N} \tilde{E}_i K_k(i) \geqslant 0 \text{ при } 0 \leqslant k \leqslant N \right]. \tag{3.4.44}$$

При $q = 2$ неравенство линейного программирования можно немного улучшить.

Лемма 3.4.18. 1. *Если существует двоичный* $[N, M, d]$*-код с чётным* d*, то найдётся двоичный* $[N, M, d]$*-код, вес каждого кодового слова в котором чётный и поэтому все расстояния чётные. Итак, если* $q = 2$ *и* d *чётно, мы можем предполагать, что* $E_i = 0$ *при всех нечётных значениях* i*.*

2. *При* $q = 2$ *выполнено равенство*

$$K_i(2k) = K_{N-i}(2k).$$

Следовательно, для чётных d*, так как мы можем считать, что* $E_{2i+1} = 0$*, ограничения в формуле* (3.4.44) *должны рассматриваться только для* $k = 0, \ldots, [N/2]$.

3. *Для всех* i *выполняется равенство* $K_0(i) = 1$*, и поэтому неравенство* $\sum\limits_{i=0}^{N} \tilde{E}_i K_0(i) \geqslant 0$ *следует из того, что* $\tilde{E}_i \geqslant 0$.

Из леммы 3.4.18 непосредственно вытекает следующий результат.

Теорема 3.4.19 (граница линейного программирования для $q = 2$). *Если* d *чётно, то*

$$M_2^*(N, d) \leqslant \max \left[\sum_{i=0}^{N} \tilde{E}_i : \tilde{E}_i \geqslant 0,\ \tilde{E}_0 = 1,\ \tilde{E}_i = 0 \text{ при } 1 < i < d, \right.$$
$$\left. \tilde{E}_i = 0 \text{ при нечётных } i \ \text{ и } \ C_N^k + \sum_{i=d}^{N} \tilde{E}_i K_k(i) \geqslant 0 \text{ при } k = 1, \ldots, \left\lfloor \frac{N}{2} \right\rfloor \right]. \tag{3.4.45}$$

Так как $M_2^*(N, 2t+1) = M_2^*(N+1, 2t+2)$, теорема 3.4.19 даёт полезное ограничение и для нечётных d.

Граница линейного программирования представляет собой довольно универсальный инструмент в теории кодов. Например, границы Синглтона, Хэмминга и Плоткина могут быть получены в качестве её следствия. Однако мы не будем разбирать все случаи, ограничившись границей Синглтона.

Специалист по кодированию делает это, не чувствуя границ.

(Из серии «Как они делают это».)

Пример 3.4.20. Для натуральных чисел N и $d \leqslant N$ определим многочлен

$$f(x) = 1 + \sum_{j=1}^{N} f_j K_j(x),$$

где $f_i \geqslant 0$, $1 \leqslant j \leqslant N$, и $f(i) \leqslant 0$ при $d \leqslant i \leqslant N$. Докажите, что

$$M_q^*(N, d) \leqslant f(0). \tag{3.4.46}$$

Выведите из этого неравенства границу Синглтона.

Решение. Пусть $M = M_q^*(N, d)$ и $\mathcal{X}$ — q-ичный $[N, M]$-код с распределением расстояний $B_j(\mathcal{X})$, $j = 0, \ldots, N$. Используя границу линейного программирования (3.4.42) для $k = 0$, получаем, что $K_i(0) \geqslant -\sum\limits_{j=d}^{N} B_j(\mathcal{X}) K_i(j)$. Из условия $f(i) \leqslant 0$ при $d \leqslant j \leqslant N$ следует неравенство $\sum\limits_{j=d}^{N} B_j(\mathcal{X}) f(j) \leqslant 0$. Таким обазом,

$$\begin{aligned} f(0) = 1 + \sum_{j=1}^{N} f_j K_j(0) &\geqslant 1 - \sum_{k=1}^{N} f_k \sum_{i=d}^{N} B_i(\mathcal{X}) K_k(i) = \\ &= 1 - \sum_{i=d}^{N} B_i(\mathcal{X}) \sum_{k=1}^{N} f_k K_k(i) = 1 - \sum_{i=d}^{N} B_i(\mathcal{X})(f(i) - 1) \geqslant \\ &\geqslant 1 + \sum_{i=d}^{N} B_i(\mathcal{X}) = M = M_q^*(N, d). \end{aligned}$$

Для получения границы Синглтона выберем

$$f(x) = q^{N-d+1} \prod_{j=d}^{N} \left(1 - \frac{x}{j}\right).$$

Тогда в силу ортогональности полиномов Кравчука $\sum\limits_{i=0}^{N} K_l(i) K_i(k) = \delta_{kl} q^k$ получаем

$$f_k = \frac{1}{q^N} \sum_{i=0}^{N} f(i) K_i(k) = \frac{1}{q^{d-1}} \sum_{i=0}^{d-1} C_{N-i}^{N-d+1} K_i(k) \Big/ C_N^{d-1} = C_{N-k}^{d-1} \Big/ C_N^{d-1} \geqslant 0.$$

Здесь мы воспользовались тождеством

$$\sum_{k=0}^{j} C_{N-k}^{N-j} K_k(x) = q^j C_{N-x}^{j}. \tag{3.4.47}$$

Ясно, что $f(i) = 0$ при $d \leqslant i \leqslant N$. Значит, $M_q^*(N, d) \leqslant f(0) = q^{N-d+1}$. Аналогичным способом можно вывести границы Хэмминга и Плоткина (см. [LX]). □

Пример 3.4.21. Опираясь на границу линейного программирования, докажите, что $M_2^*(13, 5) = M_2^*(14, 6) \leqslant 64$. Сравните это с границей Элайеса.

Указание. Справедливы равенства $E_6 = 42$, $E_8 = 7$, $E_{10} = 14$, $E_{12} = E_{14} = 0$. Для получения решения вам может потребоваться компьютер.

Решение. Граница линейного программирования для линейных кодов заключается в равенстве

$$M_2^*(N, d) = \max \left[\sum_{i=0}^{N} E_i \colon E_i \geqslant 0,\ \ E_0 = 1,\ \ E_j = 0 \text{ для } 1 \leqslant j < d, \right.$$

$$\left. E_i = 0 \text{ при нечётных } j \ \text{ и } \ C_N^k + \sum_{\substack{d \leqslant i \leqslant N \\ i \text{ чётное}}} E_i K_k(i) \geqslant 0 \text{ при } k = 1, \ldots, \left\lfloor \frac{N}{2} \right\rfloor \right].$$

Для $N = 14$, $d = 6$ ограничения имеют вид

$$E_0 = 1, \quad E_1 = E_2 = E_3 = E_4 = E_5 = E_7 = E_9 = E_{11} = E_{13} = 0,$$
$$E_6, E_8, E_{10}, E_{12}, E_{14} \geqslant 0,$$
$$14 + 2E_6 - 2E_8 - 6E_{10} - 10E_{12} - 14E_{14} \geqslant 0,$$
$$91 - 5E_6 - 5E_8 + 11E_{10} + 43E_{12} + 91E_{14} \geqslant 0,$$
$$364 - 12E_6 + 12E_8 + 4E_{10} - 100E_{12} - 364E_{14} \geqslant 0,$$
$$1001 + 9E_6 + 9E_8 - 39E_{10} + 121E_{12} + 1001E_{14} \geqslant 0,$$
$$2002 + 30E_6 - 30E_8 + 38E_{10} - 22E_{12} - 2002E_{14} \geqslant 0,$$
$$3003 - 5E_6 - 5E_8 + 27E_{10} - 165E_{12} + 3003E_{14} \geqslant 0,$$
$$3432 - 40E_6 + 40E_8 - 72E_{10} + 264E_{12} - 3432E_{14} \geqslant 0,$$

а максимума целевая функция $S = E_6 + E_8 + E_{10} + E_{12} + E_{14}$ достигает на

$$E_6 = 42, \quad E_8 = 7, \quad E_{10} = 14, \quad E_{12} = E_{14} = 0.$$

При этом $S = 63$, $E_0 + S = 1 + 63 = 64$, так что из границы линейного программирования получаем

$$M_2^*(13, 5) = M_2^*(14, 6) \leqslant 64.$$

Заметим, что граница достигается, поскольку $[13, 64, 5]$ — двоичный код реально существует. Сравним границы линейного программирования и Хэмминга:

$$M_2^*(13, 5) \leqslant 2^{13}/(1 + 13 + 13 \cdot 6) = 2^{13}/92 = 2^{11}/23,$$

т. е.

$$M_2^*(13,\,5) \leqslant 91.$$

Далее, по границе Синглтона $k \leqslant 13 - 5 - 1 = 7$ и

$$M_2^*(13,\,5) \leqslant 2^7 = 128.$$

Любопытно ещё посмотреть на то, что даёт граница Элайеса:

$$M_2^*(13,\,5) \leqslant \frac{65/2}{s^2 - 13s + 65/2}\,\frac{2^{13}}{1 + 13 + \ldots + C_{13}^5}$$

$\forall s < 13$, при которых $s^2 - 13s + 65/2 > 0$. Подставляя $s = 2$, получаем $s^2 - 13s + 65/2 = 4 - 26 + 65/2 = 21/2 > 0$ и

$$M_2^*(13,\,5) \leqslant \frac{65}{21}2^{13}/(1 + 13 + 13 \cdot 6) = 2{,}33277 \times 10^6:$$

не слишком хорошее ограничение. Далее, при $s = 3$ получаем $s^2 - 13s + 65/2 = 9 - 39 + 65/2 = 5/2 > 0$ и

$$M_2^*(13,\,5) \leqslant \frac{65}{5}2^{13}/(1 + 13 + 13 \cdot 6 + 13 \cdot 2 \cdot 5) = 13 \times \frac{2^{12}}{111} \geqslant \frac{13}{66}2^{11}:$$

хуже границы Хэмминга. Наконец, заметим, что $4^2 - 13 \times 4 + 65/2 < 0$ и процесс останавливается. □

The MacWilliams Identity Theft[2]

(Из серии «Фильмы, которые не вышли на большой экран».)

§ 3.5. Асимптотически хорошие коды

Определение 3.5.1. Последовательность $[N_i.k_i,\, d_i]$-кодов, $N_i \to \infty$ называется *асимптотически хорошей*, если последовательности k_i/N_i и d_i/N_i отделены от нуля. □

Теорема 3.3.24 говорит о том, что не существует асимптотически хорошей последовательности примитивных БЧХ-кодов (на самом деле не существует асимптотически хорошей последовательности БЧХ-кодов любого вида). Теоретически красивый способ получения асимптотически хорошего семейства связан с так называемыми кодами Юстенсена. В качестве первой попытки определить хороший код возьмём $0 \neq \alpha \in \mathbb{F}_{2^m} \simeq \mathbb{F}_2^m$ и определим множество

$$\mathcal{X}_\alpha = \{(\mathbf{a},\, \alpha\mathbf{a})\colon \mathbf{a} \in \mathbb{F}_2^m\}. \tag{3.5.1}$$

[2]Ср. с названием фильма «Identity Theft» (2012 г.).

Тогда $\mathcal{X}_\alpha$ — $[2m, m]$-линейный код со скоростью передачи информации $1/2$. Мы можем восстановить α из любого ненулевого кодового слова $(\mathbf{a}, \mathbf{b}) \in \mathcal{X}_\alpha$ как $\alpha = \mathbf{b}\mathbf{a}^{-1}$ (деление в поле $\mathbb{F}_{2^m}$). Значит, при $\alpha \neq \alpha'$ имеем $\mathcal{X}_\alpha \cap \mathcal{X}_{\alpha'} = \{0\}$.

Теперь по данному $\lambda = \lambda_m \in (0,\, 1/2]$ мы хотим найти такое $\alpha = \alpha_m$, что минимальный вес кода $\mathcal{X}_\alpha$ будет не меньше чем $2m\lambda$. Поскольку ненулевое двоичное $(2m)$-слово может принадлежать не более чем одному коду вида $\mathcal{X}_\alpha$, мы можем найти такое α, если число ненулевых $(2m)$-слов веса меньше $2m\lambda$ ограничено сверху числом различных кодов $\mathcal{X}_\alpha$, равным $2^m - 1$. Таким образом, мы добьёмся успеха, если

$$\sum_{i=1}^{2m\lambda - 1} C_{2m}^i < 2^m - 1,$$

или даже лучше: $\sum\limits_{i=1}^{2m\lambda} C_{2m}^i < 2^m - 1$. Теперь воспользуемся следующей леммой.

Лемма 3.5.2. *Для $0 \leqslant \lambda \leqslant 1/2$ имеет место неравенство*

$$\sum_{k=0}^{\lfloor \lambda N \rfloor} C_N^k \leqslant 2^{N\eta(\lambda)}, \tag{3.5.2}$$

где $\eta(\lambda)$ — двоичная энтропия.

Доказательство. Заметим, что неравенство (3.5.2) выполнено при $\lambda = 0$ (тогда обе его части равны 1) и при $\lambda = 1/2$ (когда п. ч. равна 2^N). Поэтому можно предполагать, что $0 < \lambda < 1/2$. Рассмотрим с. в. ξ с биномиальным распределением

$$\mathsf{P}(\xi = k) = C_N^k (1/2)^N, \quad 0 \leqslant k \leqslant N.$$

Для данного $t \in \mathbb{R}_+$ воспользуемся следующим неравенством типа Чебышева:

$$\sum_{k=0}^{\lambda N} C_N^k \left(\frac{1}{2}\right)^N = \mathsf{P}(\xi \leqslant \lambda N) = \mathsf{P}(\exp(-t\xi) \geqslant \exp(-\lambda N t)) \leqslant$$

$$\leqslant e^{\lambda N t}\, \mathsf{E} e^{-t\xi} = e^{\lambda N t} \left(\frac{1}{2} + \frac{1}{2} e^{-t}\right)^N. \tag{3.5.3}$$

Минимизируем п. ч. формулы (3.5.3) по $x = e^{-t}$ при $t > 0$, т. е. при $0 < x < 1$. Минимум достигается при $e^{-t} = \lambda/(1-\lambda)$ и равен

$$\left(\frac{\lambda}{1-\lambda}\right)^{-\lambda N} \left(\frac{1}{2}\right)^N \left(1 + \frac{\lambda}{1-\lambda}\right)^N = \lambda^{-\lambda N} \mu^{-\mu N} \left(\frac{1}{2}\right)^N = 2^{N\eta(\lambda)} \left(\frac{1}{2}\right)^N,$$

где $\mu = 1 - \lambda$. Значит п. ч. формулы (3.5.3) не превосходит $2^{N\eta(\lambda)}\left(\frac{1}{2}\right)^N$. $\square$

Ввиду леммы 3.5.2 неравенство (3.5.1) получается, когда

$$2^{2m\eta(\lambda)} < 2^m - 1. \tag{3.5.4}$$

Например, если

$$\lambda = \lambda_m = \eta^{-1}\left(\frac{1}{2} - \frac{1}{\log m}\right)$$

$(0 < \lambda < 1/2)$, то неравенство (3.5.4) принимает вид $2^{m-2m/\log m} < 2^m - 1$, что справедливо при достаточно больших m. Кроме того, $\lambda_m \to \eta^{-1}(1/2) > 0$ при $m \to \infty$. Здесь и далее символ η^{-1} обозначает функцию, обратную к $\lambda \in (0, 1/2] \mapsto \eta(\lambda)$. В коде (3.5.1) с фиксированным α скорость передачи и информации равна $1/2$, но гарантировать то, что $d/2m$ отделено от нуля, нельзя. Более того, не существует эффективного способа найти подходящее $\alpha = \alpha_m$. Однако в 1972 г. Юстенсен показал [Ju], как получить хорошую последовательность кодов, остроумно используя сцепление слов кода Рида—Соломона.

Более точно, рассмотрим двоичное (k_1k_2)-слово $\mathbf{a}$, организованное как последовательность k_2-слов: $\mathbf{a} = \mathbf{a}^{(0)}\mathbf{a}^{(1)}\dots\mathbf{a}^{(k_1-1)}$. На картинке это выглядит так:

$$\mathbf{a} = \underbrace{\boxed{\mathbf{a}^{(0)}}}_{k_2} \dots\dots\dots \underbrace{\boxed{\mathbf{a}^{(k_1-1)}}}_{k_2}, \qquad \mathbf{a}^{(i)} \in \mathbb{F}_{2^{k_2}},\ 0 \leqslant i \leqslant k_1 - 1.$$

Фиксируем $[N_1, k_1, d_1]$-код $\mathcal{X}_1$ над $\mathbb{F}_{2^{k_2}}$, называемый внешним кодом: $\mathcal{X}_1 \subset \mathbb{F}_{2^{k_2}}^{N_1}$. Тогда строка $\mathbf{a}$ кодируется как кодовое слово $\mathbf{c} = c_0c_1\dots c_{N-1} \in \mathcal{X}_1$. Далее, каждое $c_i \in \mathbb{F}_{2^{k_2}}$ кодируется кодовым словом $\mathbf{b}_i$ из $[N_2, k_2, d_2]$-кода $\mathcal{X}_2$ над $\mathbb{F}_2$, называемого внутренним кодом. В результате получается строка $\mathbf{b} = \mathbf{b}^{(0)}\dots\mathbf{b}^{(N_1-1)} \in \mathbb{F}_q^{N_1N_2}$ длины N_1N_2:

$$\mathbf{b} = \underbrace{\boxed{\mathbf{b}^{(0)}}}_{N_2} \dots\dots\dots \underbrace{\boxed{\mathbf{b}^{(N_1-1)}}}_{N_2}, \qquad \mathbf{b}^{(i)} \in \mathbb{F}_{2^{N_2}},\ 0 \leqslant i \leqslant N_1 - 1.$$

Кодирование представляется следующей диаграммой:

вход: — (k_1k_2)-строка $\mathbf{a}$, **выход:** — (N_1N_2)-кодовое слово $\mathbf{b}$.

Заметим, что разные символы c_i можно кодировать разными внутренними кодами. Пусть внешний код $\mathcal{X}_1$ — это $[2^m - 1, k, d]$-код Рида—Соломона $\mathcal{X}^{\mathrm{PC}}$ над $\mathbb{F}_{2^m}$. Запишем двоичное $(k2^m)$-слово $\mathbf{a}$ как сцепление $\mathbf{a}^{(0)}\dots\mathbf{a}^{(k-1)}$, $\mathbf{a}^{(i)} \in \mathbb{F}_{2^m}$. Кодирование строки $\mathbf{a}$ с помощью кода $\mathcal{X}^{\mathrm{PC}}$ приводит к кодовому слову $\mathbf{c} = c_0\dots c_{N-1}$, $N = 2^m - 1$ и $c_i \in \mathbb{F}_{2^m}$. Пусть β —

примитивный элемент поля $\mathbb{F}_{2^m}$. Тогда для всех $j = 0, \ldots, N-1 = 2^m - 2$ рассмотрим линейный код

$$\mathcal{X}^{(j)} = \{(c, \beta^j c)\colon c \in \mathbb{F}_{2^m}\}. \tag{3.5.5}$$

Результирующим кодовым словом («кодовым суперсловом») будет

$$\mathbf{b} = (c_0, c_0)(c_1, \beta c_1)(c_2, \beta^2 c_2)\ldots(c_{N-1}, \beta^{N-1} c_{N-1}). \tag{3.5.6}$$

Определение 3.5.3. Кодом Юстенсена $\mathcal{X}^{\mathrm{Ju}}_{m,k}$ называется набор двоичных суперслов $\mathbf{b}$, полученных, как описано выше, с помощью $[2^m - 1, k, d]$-кода РС в качестве внешнего кода $\mathcal{X}_1$ и $\mathcal{X}^{(j)}$ (см. формулу (3.5.5)) в качестве внутренних кодов, где $0 \leqslant j \leqslant 2^m - 2$. Длина кода $\mathcal{X}^{\mathrm{Ju}}_{m,k}$ равна $2m(2^m - 1)$, его ранг — mk, и поэтому скорость передачи информации составляет $k/(2(2^m - 1)) < 1/2$. □

Удобным параметром, описывающим код $\mathcal{X}^{\mathrm{Ju}}_{m,k}$, является длина внешнего кода РС $N = 2^m - 1$. Нам хотелось бы построить последовательность $\mathcal{X}^{\mathrm{Ju}}_{m,k}$ с $N \to \infty$, но с отношениями $k/(2m(2^m - 1))$ и $d/(2m(2^m - 1))$, отделёнными от нуля. Фиксируем $R_0 \in (0, 1/2)$ и выберем последовательность внешних РС кодов $\mathcal{X}^{\mathrm{PC}}_N$ длины $N = 2^m - 1$ и $k = [2NR_0]$. Тогда скорость кода $\mathcal{X}^{\mathrm{Ju}}_{m,k}$ будет составлять $k/(2N) > R_0$.

Теперь рассмотрим минимальный вес

$$w(\mathcal{X}^{\mathrm{Ju}}_{m,k}) = \min[w(\mathbf{x})\colon \mathbf{x} \in \mathcal{X}^{\mathrm{Ju}}_{m,k},\ \ \mathbf{x} \neq \mathbf{0}]\ \ (= d(\mathcal{X}^{\mathrm{Ju}}_{m,k})). \tag{3.5.7}$$

Если при любом фиксированном m минимальный вес внешнего кода $\mathcal{X}^{\mathrm{PC}}_N$, $N = 2^m - 1$, равен d, то у любого суперслова $\mathbf{b} = (c_0, c_0)(c_1, \beta c_1)\ldots$ $\ldots(c_{N-1}, \beta^{N-1} c_{N-1}) \in \mathcal{X}^{\mathrm{Ju}}_{m,k}$ будет не менее d ненулевых первых компонент $c_0, \ldots, c_{N-1}$. Более того, любая пара внутренних кодов из $\mathcal{X}^{(0)}, \ldots, \mathcal{X}^{(N-1)}$ пересекается только по нулю. Поэтому d упорядоченных пар, взятых из различных кодов, должны быть разными. Иначе говоря, у кодового суперслова $\mathbf{b}$ должно быть не менее d разных ненулевых двоичных $(2m)$-строк.

Далее, вес кодового суперслова $\mathbf{b} \in \mathcal{X}^{\mathrm{Ju}}_{m,k}$ не меньше чем сумма весов описанных выше d разных ненулевых двоичных $(2m)$-строк. В связи с этим нам нужно установить нижнюю границу таких сумм. Заметим, что

$$d = N - k + 1 = N\Big(1 - \frac{k-1}{N}\Big) \geqslant N(1 - 2R_0).$$

Следовательно, кодовое суперслово $\mathbf{b} \in \mathcal{X}^{\mathrm{Ju}}_{m,k}$ имеет не меньше $N(1 - 2r_0)$ разных ненулевых двоичных $(2m)$-строк.

Специалист по алгебраическому кодированию
делает это в упорядоченных парах.

(Из серии «Как они делают это».)

Лемма 3.5.4. *Сумма весов любых $N(1-2R_0)$ различных ненулевых двоичных $(2m)$-строк не меньше*

$$2mN(1-2R_0)\Bigl(\eta^{-1}\Bigl(\frac{1}{2}\Bigr)-o(1)\Bigr). \tag{3.5.8}$$

Доказательство. По лемме 3.5.2 для любого $\lambda \in [0,\, 1/2]$ число ненулевых двоичных $(2m)$-строк, вес которых не превосходит $2m\lambda$, не больше чем

$$\sum_{i=1}^{2m\lambda} C_{2m}^{i} \leqslant 2^{2m\eta(\lambda)}.$$

Отбрасывая эти маловесящие строки, получаем, что общий вес не меньше чем

$$2m\lambda(N(1-2R_0)-2^{2m\eta(\lambda)}) = 2mN\lambda(1-2R_0)\Bigl(1-\frac{2^{2m\eta(\lambda)}}{N(1-2R_0)}\Bigr).$$

Выберем $\lambda_m = \eta^{-1}\Bigl(\frac{1}{2}-\frac{1}{\log(2m)}\Bigr) \in (0,\, 1/2)$. Тогда $\lambda_m \to \eta^{-1}(1/2)$, поскольку функция η^{-1} непрерывна на отрезке $[0,\, 1/2]$. Значит,

$$\lambda_m = \eta^{-1}\Bigl(\frac{1}{2}-\frac{1}{\log(2m)}\Bigr) = \eta^{-1}\Bigl(\frac{1}{2}\Bigr)-o(1).$$

Так как $N = 2^m - 1$, получаем, что при $m \to \infty$ одновременно $N \to \infty$ и

$$\frac{2^{2m\eta(\lambda)}}{N(1-2R_0)} = \frac{1}{1-2R_0}\,\frac{2^{m-2m/\log(2m)}}{2^m-1} = \frac{1}{1-2R_0}\,\frac{2^m}{2^m-1}\,\frac{1}{2^{2m/\log(2m)}} \to 0.$$

Так что общий вес $N(1-2R_0)$ разных $(2m)$-строк не меньше чем

$$\begin{aligned}\geqslant 2mN(1-2R_0)(\eta^{-1}(1/2)-o(1))(1-o(1)) = \\ = 2mN(1-2R_0)(\eta^{-1}(1/2)-o(1)),\end{aligned}$$

откуда следует требуемое утверждение. □

> A specialist in entropy does it as a continuous function.
> Специалист по энтропии делает это как свои рутинные обязанности.
>
> (Из серии «Как они делают это».)

Лемма 3.5.4 показывает, что код $\mathcal{X}_{m,k}^{\mathrm{Ju}}$ имеет вес

$$w(\mathcal{X}_{m,k}^{\mathrm{Ju}}) \geqslant 2mN(1-2R_0)\Bigl(\eta^{-1}\Bigl(\frac{1}{2}\Bigr)-o(1)\Bigr). \tag{3.5.9}$$

Поэтому

$$\frac{w(\mathcal{X}^{\mathrm{Ju}}_{m,k})}{\mathrm{length}(\mathcal{X}^{\mathrm{Ju}}_{m,k})} \geqslant (1-2R_0)(\eta^{-1}(1/2)-o(1)) \to (1-2R_0)\eta^{-1}(1/2) \approx$$
$$\approx c(1-2R_0) > 0.$$

Таким образом, последовательность кодов $\mathcal{X}^{\mathrm{Ju}}_{m,k}$ с $k=[2NR_0]$, $N=2^m-1$ и фиксированным $R_0 \in (0,\, 1/2)$ обладает скоростью передачи информации не меньше $R_0 > 0$ и

$$\frac{w(\mathcal{X}^{\mathrm{Ju}}_{m,k})}{\mathrm{length}(\mathcal{X}^{\mathrm{Ju}}_{m,k})} \to (1-2_0), \quad c=\eta^{-1}(1/2) > 0{,}3. \tag{3.5.10}$$

По построению $R_0 \in (0,\, 1/2)$. Однако используя соответствующее усечение, эту константу можно выбирать из интервала $(0,\, 1)$, см. [MWS].

> Остерегайтесь ошибок в приведенном выше коде; я лишь доказал его корректность, но сам его не испытывал.
>
> *Дональд Кнут* (род. в 1938 г.),
> американский программист и математик,
> автор книги «Искусство программирования»

В заключение этого параграфа обсудим так называемые *альтернантные* коды. Альтернантные коды — это обобщение кодов БЧХ, хотя они не обязательно циклические. Подобно кодам Юстенсена они тоже образуют асимптотически хорошее семейство. Пусть M — это $r \times n$-матрица над полем $\mathbb{F}_{q^m}$:

$$M = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{r1} & \dots & c_{rn} \end{pmatrix}.$$

Как и раньше, каждый элемент c_{ij} может быть записан в виде вектор-столбца $\vec{c}_{ij} \in (\mathbb{F}_q)^m$ высоты m над полем $\mathbb{F}_q$. Таким образом, можно представлять себе M как $mr \times n$-матрицу над полем $\mathbb{F}_q$ (сохраняя обозначение M).

При заданных элементах $a_1, \dots, a_n \in \mathbb{F}_{q^m}$ получаем

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{r1} & \dots & c_{rn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \sum\limits_{1 \leqslant j \leqslant n} a_j c_{ij} \\ \vdots \\ \sum\limits_{1 \leqslant j \leqslant n} a_j c_{rj} \end{pmatrix}.$$

Далее, если $b \in \mathbb{F}_q$ и $c,\ d \in \mathbb{F}_{q^m}$, то $b\vec{c} = \vec{bc}$ и $\vec{c} + \vec{d} = (\overrightarrow{c+d})$. Таким образом, если $a_1, \ldots, a_n \in \mathbb{F}_q$, то

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \vec{c}_{11} & \ldots & \vec{c}_{1n} \\ \vdots & \ddots & \vdots \\ \vec{c}_{r1} & \ldots & \vec{c}_{rn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \sum\limits_{1 \leqslant j \leqslant n} a_i \vec{c}_{ij} \\ \vdots \\ \sum\limits_{1 \leqslant j \leqslant n} a_i \vec{c}_{rj} \end{pmatrix}.$$

Итак, если вектор-столбцы M линейно независимы как r-векторы над полем $\mathbb{F}_{q^m}$, то они также линейно независимы как (rm)-векторы над полем $\mathbb{F}_q$.

Напомним, что если ω — примитивный корень $(n, \mathbb{F}_{q^m})$ из единицы и $\delta \geqslant 2$, то $n \times (m\delta)$-матрица Вандермонда над полем $\mathbb{F}_q$ вида

$$H^T = \begin{pmatrix} \vec{e} & \vec{e} & \ldots & \vec{e} \\ \vec{\omega} & \vec{\omega}^2 & \ldots & \vec{\omega}^{\delta-1} \\ \vec{\omega}^2 & \vec{\omega}^4 & \ldots & \vec{\omega}^{2(\delta-1)} \\ & & \ldots & \\ \vec{\omega}^{n-1} & \vec{\omega}^{2(n-1)} & \ldots & \vec{\omega}^{(\delta-1)(n-1)} \end{pmatrix}$$

является матрицей проверки четности БЧХ-кода в узком смысле $\mathcal{X}^{\mathrm{BCH}}_{q,n,\omega,\delta}$ (корректная матрица проверки четности возникает после удаления линейно зависимых столбцов). Обобщим эту конструкцию, выбирая $n \times r$-матрицу над полем $\mathbb{F}_{q^m}$ вида

$$A = \begin{pmatrix} h_1 & h_1\alpha_1 & \ldots & h_1\alpha_1^{r-2} & h_1\alpha_1^{r-1} \\ h_2 & h_2\alpha_2 & \ldots & h_2\alpha_2^{r-2} & h_2\alpha_2^{r-1} \\ \vdots & \vdots & \ddots & \vdots & \\ h_n & h_n\alpha_n & \ldots & h_n\alpha_n^{r-2} & h_n\alpha_n^{r-1} \end{pmatrix}, \tag{3.5.11}$$

или ее $n \times (mr)$-представление над полем $\mathbb{F}_q$:

$$\vec{A} = \begin{pmatrix} \vec{h_1} & \vec{h_1\alpha_1} & \ldots & \vec{h_1\alpha_1}^{r-2} & \vec{h_1\alpha_1}^{r-1} \\ \vec{h_2} & \vec{h_2\alpha_2} & \ldots & \vec{h_2\alpha_2}^{r-2} & \vec{h_2\alpha_2}^{r-1} \\ \vdots & \vdots & \ddots & \vdots & \\ \vec{h_n} & \vec{h_n\alpha_n} & \ldots & \vec{h_n\alpha_n}^{r-2} & \vec{h_n\alpha_n}^{r-1} \end{pmatrix}. \tag{3.5.12}$$

Здесь $r < n$, $h_1, \ldots, h_n$ — ненулевые элементы и $\alpha_1, \ldots, \alpha_n$ — различные элементы поля $\mathbb{F}_q$.

Заметим, что любые r столбцов матрицы A из формулы (3.5.11) образуют квадратную подматрицу K, имеющую форму матрицы Вандермонда. Поэтому она имеет ненулевой определитель и любые r столбцов матрицы A являются линейно независимыми над полем $\mathbb{F}_{q^m}$, а следовательно, и над

полем $\mathbb{F}_q$. Далее, столбцы матрицы A в формуле (3.5.11) линейно независимы над полем $\mathbb{F}_{q^m}$. Однако столбцы матрицы $\vec{A}$ в формуле (3.5.12) могут быть линейно зависимыми, и некоторые из них нужно отбросить, чтобы получить корректную матрицу проверки четности.

Определение 3.5.5. Пусть $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\underline{h} = (h_1, \ldots, h_n)$, где $\alpha_1, \ldots, \alpha_n$ различны и $h_1, \ldots, h_n$ — ненулевые элементы поля $\mathbb{F}_{q^m}$. При заданном $r < n$ альтернантный код $\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}$ определяется как ядро $n \times (rm)$-матрицы A в формуле (3.5.12).

Теорема 3.5.6. *Код $\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}$ имеет длину n, ранг k, удовлетворяющий ограничению $n - mr \leqslant k \leqslant n - r$, и минимальное расстояние $d\bigl(\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}\bigr) \geqslant r + 1$.*

Мы видим, что альтернантные коды действительно являются обобщением кодов БЧХ. Основной результат теории альтернантных кодов содержится в теореме 3.5.7, которая приводится без доказательства.

Теорема 3.5.7. *Существуют произвольно длинные альтернантные коды $\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}$, лежащие выше границы Гильберта—Варшамова.*

Это означает, что альтернантные коды являются асимптотически хорошими. Более точно, примером последовательности асимптотически хороших альтернантных кодов являются так называемые *коды Гоппы*. Эти коды были изобретены российским математиком Валерием Гоппой в 1972 г., в них используется элегантная идея из алгебраической геометрии. Мы приведем эту конструкцию с помощью методов, развитых в этом параграфе.

Пусть $G(X) \in \mathbb{F}_{q^m}[X]$ — это полином над полем $\mathbb{F}_{q^m}$. Рассмотрим полиномиальное кольцо $\mathbb{F}_{q^m}[X]/\langle G(X)\rangle$ по модулю $G(X)$ над полем $\mathbb{F}_{q^m}$. Тогда $\mathbb{F}_{q^m}[X]/\langle G(X)\rangle$ является полем в том и только том случае, если полином $G(X)$ неприводим. Но при заданном $\alpha \in \mathbb{F}_{q^m}$, $G(\alpha) \neq 0$, линейный полином $X - \alpha$ является обратимым в $\mathbb{F}_{q^m}[X]/\langle G(X)\rangle$. Действительно, запишем

$$G(X) = q(X)(X - \alpha) + G(\alpha), \tag{3.5.13}$$

где $q(X) \in \mathbb{F}_q[X]$, $\deg q(X) = \deg G(X) - 1$. Поэтому $q(X)(X - \alpha) = -G(\alpha) \bmod (G(X))$, или

$$(-G(\alpha))^{-1} q(X)(X - \alpha) = e \bmod (G(X))$$

и

$$(X - \alpha)^{-1} = (-G(\alpha))^{-1} q(X) \bmod (G(X)). \tag{3.5.14а}$$

Поскольку $q(X) = (G(X) - G(\alpha))(X - \alpha)^{-1}$, мы получаем, что

$$(X - \alpha)^{-1} = -(G(X) - G(\alpha))(X - \alpha)^{-1} G(\alpha)^{-1} \bmod (G(X)). \tag{3.5.14б}$$

Теперь определим $(X-\alpha)^{-1}$ как полином в кольце $\mathbb{F}_{q^m}[X]/\langle G(X)\rangle$, заданный формулой (3.5.14a).

Определение 3.5.8. Зафиксируем полином $G(X)\in\mathbb{F}_q[X]$ и множество $\underline{\alpha}=\{\alpha_1,\ldots,\alpha_n\}$ различных элементов поля $\mathbb{F}_{q^m}$, $q^m\geqslant n>\deg G(X)$, где $G(\alpha_j)=0$, $1\leqslant j\leqslant n$. При заданном слове $\mathbf{b}=b_1\ldots b_n$, где $b_i\in\mathbb{F}_q$, $1\leqslant i\leqslant n$, положим

$$R_b(X)=\sum_{1\leqslant i\leqslant n} b_i(X-\alpha_i)^{-1}\in\mathbb{F}_{q^m}[X]/\langle G(X)\rangle. \tag{3.5.15}$$

Код Гоппы $\mathcal{X}^{\mathrm{Go}}$ $(=\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G})$ над алфавитом $\mathbb{F}_q$ определяется как множество

$$\{\mathbf{b}\in\mathbb{F}_q^n : R_b(X)=0 \bmod (G(X))\}. \tag{3.5.16}$$

Ясно, что $\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}$ является линейным кодом. Полином $G(X)$ называется *многочленом Гоппы*; если полином $G(X)$ неприводим, будем говорить, что код $\mathcal{X}^{\mathrm{Go}}$ неприводим. □

Итак, $\mathbf{b}=b_1\ldots b_n\in\mathcal{X}^{\mathrm{Go}}$ тогда и только тогда, когда в поле $\mathbb{F}_{q^m}[X]$ выполняется соотношение

$$\sum_{1\leqslant i\leqslant n} b_i(G(X)-G(\alpha_i))(X-\alpha_i)^{-1}G(\alpha_i)^{-1}=0. \tag{3.5.17}$$

Запишем $G(X)=\sum\limits_{0\leqslant i\leqslant r} g_iX^i$, где $\deg G(X)=r$, $g_r=1$ и $r<n$. Тогда в поле $\mathbb{F}_{q^m}[X]$ выполняется соотношение

$$\begin{aligned}(G(X)-G(\alpha_i))(X-\alpha_i)^{-1}&=\\ &=\sum_{0\leqslant j\leqslant r} g_j(X^j-\alpha_i^j)(X-\alpha_i)^{-1}=\sum_{0\leqslant j\leqslant r} g_j\sum_{0\leqslant u\leqslant j-1} X^u\alpha_i^{j-1-u}\end{aligned}$$

и поэтому

$$\begin{aligned}&\sum_{1\leqslant i\leqslant n} b_i(G(X)-G(\alpha_i))(X-\alpha_i)^{-1}G(\alpha_i)^{-1}=\\ &\qquad=\sum_{1\leqslant i\leqslant n} b_i\sum_{0\leqslant j\leqslant r} g_j\sum_{0\leqslant u\leqslant j-1}\alpha_i^{j-1-u}X^uG(\alpha_j)^{-1}=\\ &\qquad\qquad=\sum_{0\leqslant u\leqslant r-1} X^u\sum_{1\leqslant i\leqslant n} b_iG(\alpha_i)^{-1}\sum_{u+1\leqslant j\leqslant r} g_j\alpha_i^{j-1-u}.\end{aligned}$$

Следовательно, $\mathbf{b}\in\mathcal{X}^{\mathrm{Go}}$ тогда и только тогда, когда в поле $\mathbb{F}_{q^m}$ выполняется соотношение

$$\sum_{1\leqslant i\leqslant n} b_iG(\alpha_i)^{-1}\sum_{u+1\leqslant j\leqslant r} g_j\alpha_i^{j-1-u}=0 \tag{3.5.18}$$

при всех $u = 0, \ldots, r-1$.

Уравнение (3.5.18) задает матрицу проверки четности для кода $\mathcal{X}^{\mathrm{Go}}$. Во-первых, мы видим, что матрица

$$\begin{pmatrix} G(\alpha_1)^{-1} & G(\alpha_2)^{-1} & \ldots & G(\alpha_n)^{-1} \\ \alpha_1 G(\alpha_1)^{-1} & \alpha_2 G(\alpha_2)^{-1} & \ldots & \alpha_n G(\alpha_n)^{-1} \\ \alpha_1^2 G(\alpha_1)^{-1} & \alpha_2^2 G(\alpha_2)^{-1} & \ldots & \alpha_n^2 G(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-1} G(\alpha_1)^{-1} & \alpha_2^{r-1} G(\alpha_2)^{-1} & \ldots & \alpha_n^{r-1} G(\alpha_n)^{-1} \end{pmatrix}, \tag{3.5.19}$$

размера $n \times r$ над полем $\mathbb{F}_q^m$ является матрицей четности. Как и раньше, любые r строк матрицы (3.5.19) линейно независимы над полем $\mathbb{F}_{q^m}$ так же, как линейно независимы любые r столбцов. Теперь запишем матрицу (3.5.19) в виде матрицы размера $n \times (mr)$ над полем $\mathbb{F}_q$, отбрасывая линейно зависимые столбцы, и получим корректно определенную матрицу проверки четности H.

Мы видим, что $\mathcal{X}^{\mathrm{Go}}$ является альтернантным кодом $\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}$, где $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\underline{h} = (G(\alpha_1)^{-1}, \ldots, G(\alpha_n)^{-1})$. Таким образом, применима теорема 3.5.6, из которой вытекает следующий результат.

Теорема 3.5.9. *Код Гоппы $\mathcal{X} = \mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}$ с алфавитом $\mathbb{F}_q$, где $\underline{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ и $\deg G(X) = r < n$, имеет длину n, ранг k, удовлетворяющий ограничению $n - mr \leqslant k \leqslant n - r$, и минимальное расстояние $d(\mathcal{X}) \geqslant r + 1$.*

Как и ранее, приведенная выше граница на минимальное расстояние может быть улучшена для двоичного кода. Предположим, что двоичное слово имеет вид $\mathbf{b} = b_1 \ldots b_n \in \mathcal{X}$, где $\mathcal{X}$ — код Гоппы $\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}$, $\underline{\alpha} \subset \mathbb{F}_{2^m}$ и $G(X) \in \mathbb{F}_2[X]$. Предположим, что $w(\mathbf{b}) = w$ и $b_{i_1} = \cdots = b_{i_w} = 1$. Выберем $f_b(X) = \prod\limits_{1 \leqslant j \leqslant w} (X - \alpha_{i_j})$ и запишем производную $\partial_X f_b(X)$ в виде

$$\partial_X f_b(X) = R_b(X) f_b(X), \tag{3.5.20}$$

где $R_b(X) = \sum\limits_{1 \leqslant j \leqslant w} (X - \alpha_{i_j})^{-1}$ (ср. с формулой (3.5.15)). Поскольку полиномы $f_b(X)$ и $R_b(X)$ не имеют общих корней в любом расширении $\mathbb{F}_{2^l}$, они являются взаимно простыми. Тогда $\mathbf{b} \in \mathcal{X}^{\mathrm{Go}}$ в том и только том случае, когда $G(X)$ делит $R_b(X)$, что эквивалентно условию: $G(X)$ делит $\partial_X f_b(X)$. При $q = 2$ $\partial_X f_b(X)$ содержит только четные степени X (поскольку коэффициент при X^ℓ — это сумма произведений некоторых корней $\alpha'_{i_j} s$, причем это выражение равно нулю, когда ℓ нечетно). Другими словами, $\partial_X f_b = h(X^2) = (h(X))^2$ для некоторого полинома $h(X)$. Следовательно, если $g(X)$ — полином наименьшей степени, который является квадратом и делится на $G(X)$, то $G(X)$ делит $\partial_X f_b(X)$ тогда и только тогда, когда $g(X)$ делит $\partial_X f_b(X)$.

Таким образом,

$$\mathbf{b} \in \mathcal{X}^{\mathrm{Go}} \Leftrightarrow g(X) | \partial_X f_b(X) \Leftrightarrow R_b(X) = 0 \bmod (g(X)). \tag{3.5.21}$$

Теорема 3.5.10. *Пусть $\mathcal{X}$ — бинарный код Гоппы $\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}$. Если $g(X)$ — полином наименьшей степени, который является квадратом и делится на $G(X)$, то $\mathcal{X} = \mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},g}$. Следовательно, $d(\mathcal{X}^{\mathrm{Go}}) \geqslant \deg g(X) + 1$.*

Следствие 3.5.11. *Предположим, что полином Гоппы $G(X) \in \mathbb{F}_2[X]$ не имеет кратных корней в поле расширения. Тогда $\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G} = \mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G^2}$, и минимальное расстояние удовлетворяет оценке $d\big(\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}\big) \geqslant 2\deg G(X) + 1$. Поэтому $\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}$ может исправить не менее $\geqslant \deg G(X)$ ошибок.*

Бинарный код Гоппы $\mathcal{X}^{\mathrm{Go}}_{\underline{\alpha},G}$, для которого полином $G(X)$ не имеет кратных корней, называется *разделимым*.

Интересно обсудить процедуру декодирования, применимую к альтернатным кодам и основанную на алгоритме Евклида, см. § 2.5.

Как объяснялось выше, конструкция альтернатного кода $\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}$ над полем $\mathbb{F}_q$ такова. Как и в формуле (3.5.12), выберем $(n \times (mr))$-матрицу $\vec{A} = \left(h_j \vec{\alpha}_j^{\,i-1}\right)$ над полем $\mathbb{F}_q$, которая получается из $(n \times r)$-матрицы $A = (h_j \alpha_j^{i-1})$ над полем $\mathbb{F}_{q^m}$ заменой ее элементов строками длины m. Далее, удалим линейно зависимые столбцы из $\vec{A}$. Напомним, что $h_1, \ldots, h_n$ отличны от нуля и $\alpha_1, \ldots, \alpha_n$ — различные элементы поля $\mathbb{F}_{q^m}$. Предположим, что получено слово $u = c + e$, где c — корректное кодовое слово и e — вектор ошибок. Предположим, что r четно и что $t \leqslant r/2$ ошибок произошли на позициях $1 \leqslant i_1 < \cdots < i_t \leqslant n$. Пусть i_j-я компонента вектора e — это $e_{i_j} \neq \neq 0$. Удобно отождествить локаторы ошибок с элементами α_{i_j}: поскольку $\alpha_i \neq \alpha_{i'}$ при $i \neq i'$ (α_i — различные элементы), мы найдем позиции ошибок, если сможем определить корни $\alpha_{i_1}, \ldots, \alpha_{i_t}$. Более того, если мы определим многочлен обнаружения ошибок формулой

$$\ell(X) = \prod_{j=1}^{t} (1 - \alpha_{i_j} X) = \sum_{0 \leqslant i \leqslant t} \ell_i X^i, \tag{3.5.22}$$

где $\ell_0 = 1$, то достаточно найти его корни корни $\alpha_{i_j}^{-1}$. Итак, достаточно найти $\ell(X)$, т. е. коэффициенты ℓ_i.

Нам нужно вычислить синдром (будем называть его A-синдромом), возникающий при действии матрицы A:

$$uA = eA = 0 \ldots 0 e_{i_1} \ldots e_{i_t} 0 \ldots 0 A.$$

Предположим, что A-синдром имеет вид $s = s_0 \dots s_{r-1}$, где $s(X) = \sum_{0 \leqslant i \leqslant r-1} s_i X^i$. Удобно ввести многочлен обнаружения ошибок $\varepsilon(X)$ по формуле

$$\varepsilon(X) = \sum_{1 \leqslant k \leqslant t} h_{i_k} e_{i_k} \prod_{1 \leqslant j \leqslant t:\ j \neq k} (1 - \alpha_{i_j} X). \tag{3.5.23}$$

Лемма 3.5.12. *Для всех $u = 1, \dots, t$ выполняется равенство*

$$e_{i_j} = \frac{\varepsilon(\alpha_{i_j}^{-1})}{h_{i_j} \prod\limits_{1 \leqslant \tilde{j} \leqslant t,\, \tilde{j} \neq j} (1 - \alpha_{i_{\tilde{j}}} \alpha_{i_j}^{-1})} \tag{3.5.24}$$

Доказательство очевидно. □

Ключевой факт состоит в том, что полиномы $\ell(X)$, $\varepsilon(X)$ и $s(X)$ связаны между собой в соответствии со следующей леммой.

Лемма 3.5.13. *Имеет место следующее уравнение*:

$$\varepsilon(X) = \ell(X) s(X) \bmod (X^r). \tag{3.5.25}$$

Доказательство. Запишем следующую последовательность равенств:

$$\begin{aligned}
\varepsilon(X) - \ell(X)s(X) &= \sum_{1 \leqslant k \leqslant t} h_{i_k} e_{i_k} \prod_{1 \leqslant j \leqslant t: j \neq k} (1 - \alpha_{i_j} X) - \ell(X) \sum_{0 \leqslant l \leqslant r-1} s_l X^l = \\
&= \sum_k h_{i_k} e_{i_k} \prod_{1 \leqslant j \leqslant t: j \neq k} (1 - \alpha_{i_j} X) - \ell(X) \sum_l \sum_{1 \leqslant k \leqslant t} h_{i_k} \alpha_{i_k}^l e_{i_k} X^l = \\
&= \sum_k h_{i_k} e_{i_k} \prod_{j \neq k} (1 - \alpha_{i_j} X) - \ell(X) \sum_k h_{i_k} e_{i_k} \sum_l \alpha_{i_k}^l X^l = \\
&= \sum_k h_{i_k} e_{i_k} \left(\prod_{j \neq k} (1 - \alpha_{i_j} X) - \ell(X) \sum_l \alpha_{i_k}^l X^l \right) = \\
&= \sum_k h_{i_k} e_{i_k} \prod_{j \neq k} (1 - \alpha_{i_j} X)(1 - (1 - e_{i_k} X) \sum_l \alpha_{i_k}^l X^l) = \\
&= \sum_k h_{i_k} e_{i_k} \prod_{j \neq k} (1 - \alpha_{i_j} X) \left(1 - (1 - \alpha_{i_k} X) \frac{1 - \alpha_{i_k}^r X^r}{1 - \alpha_{i_k} X}\right) = \\
&= \sum_k h_{i_k} \alpha_{i_k} \prod_{j \neq k} (1 - \alpha_{i_j} X)\ \alpha_{i_k}^r X^r = 0 \bmod (X^r).
\end{aligned}$$ □

Лемма 3.5.13 задает способ декодирования альтернатного кода. Мы знаем, что существует такой полином $q(X)$, что

$$\varepsilon(X) = q(X) X^r + \ell(X) s(X). \tag{3.5.26}$$

Также имеем соотношение $\deg \varepsilon(X) \leqslant t-1 < r/2$, $\deg \ell(X) = t \leqslant r/2$ и замечаем, что полиномы $\varepsilon(X)$ и $\ell(X)$ взаимно просты, поскольку они не имеют общих корней в любом поле расширения. Предположим, что мы применили алгоритм Евклида к известным полиномам $f(X) = X^r$ и $g(X) = s(X)$ для того, чтобы найти $\varepsilon(X)$ и $\ell(X)$. Согласно лемме 2.5.45 шаг алгоритма произведет остаточный член

$$r_k(X) = a_k(X)X^r + b_k(X)s(X). \tag{3.5.27}$$

Если мы хотим получить по полиномам $r_k(X)$ и $b_k(X)$ полиномы $\varepsilon(X)$ и $\ell(X)$, их степени должны совпадать: по крайней мере должны выполняться соотношения $\deg r_k(X) < r/2$ и $\deg b_k(X) \leqslant r/2$. Итак, алгоритм повторяется, пока выполняется условие $\deg r_{k-1}(X) \geqslant r/2$ и $\deg r_k(X) < r/2$. Тогда в соответствии с леммой 2.5.45, п. 3), выполняется соотношение $\deg b_k(X) = \deg X^r - \deg r_{k-1}(X) \leqslant r - r/2 = r/2$. Это возможно, поскольку алгоритм может итерироваться, пока не достигнуто равенство $r_k(X) = \text{НОД}\,(X^r, s(X))$. Но тогда $r_k(X) | \varepsilon(X)$, а значит, $\deg r_k(X) \leqslant \deg \varepsilon(X) < r/2$. Поэтому можно предположить, что $\deg r_k(X) \leqslant r/2$, $\deg b_k(X) \leqslant r/2$.

Ключевое соотношение имеет вид

$$\begin{aligned} &\varepsilon(X) = q(X)X^r + \ell(X)s(X), \\ &\deg \varepsilon(X) < r/2, \quad \deg \ell(X) \leqslant r/2, \\ &\text{НОД}\,(\varepsilon(X),\ \ell(X)) = 1, \end{aligned}$$

а также

$$r_k(X) = a_k(X)X^r + b_k(X)s(X),\ \ \deg r_k(X) < r/2,\ \ \deg b_k(X) \leqslant r/2.$$

Мы хотим показать, что полиномы $r_k(X)$ и $b_k(X)$ пропорциональны полиномам $\varepsilon(X)$ и $\ell(X)$. Исключив $s(X)$, получим

$$b_k(X)\varepsilon(X) - r_k(X)\ell(X) = (b_k(X)q(X) - a_k(X)\ell(X))X^r.$$

Воспользуемся соотношениями

$$\deg b_k(X)\varepsilon(X) = \deg b_k(X) + \deg \varepsilon(X) < r/2 + r/2 = r$$

и

$$\deg r_k(X)\ell(X) = \deg r_k(X) + \deg \ell(X) < r/2 + r/2 = r,$$

$\deg(b(X)\varepsilon(X) - r_k(X)\ell(X)) < r$. Следовательно, $b_k(X)\varepsilon(X) - r_k(X)\ell(X)$ должен быть равен нулю, т. е.

$$\ell(X)r_k(X) = \varepsilon(X)b_k(X),\ \ b_k(X)q(X) = a_k(X)\ell(X).$$

Итак, $\ell(X) | \varepsilon(X)b_k(X)$ и $b_k(X) | a_k(X)\ell(X)$. Но $\ell(X)$ и $\varepsilon(X)$ являются взаимно простыми так же, как и полиномы $a_k(X)$ и $b_k(X)$ (по лемме 2.5.45, 5)).

Поэтому $\ell(X) = \lambda b_k(X)$ и, следовательно, $\varepsilon(X) = \lambda r_k(X)$. Поскольку $l(0) = 1$, то $\lambda = b_k(0)^{-1}$.

Суммируя, получаем алгоритм декодирования для альтернантных кодов.

Теорема 3.5.14 (алгоритм декодирования для альтернантных кодов). *Пусть $\mathcal{X}^{\mathrm{Alt}}_{\underline{\alpha},\underline{h}}$ — альтернантный код с четным r. Предположим, что в полученном слове и имеется не более чем $t \leqslant r/2$ ошибок. Тогда при получении слова и следует*

а) найти A-синдром $uA = s_0 \dots s_{r-1}$ и соответствующий полином $s(X) = \sum_l s_l X^l$;

б) применить алгоритм Евклида, начиная с полиномов $f(X) = X^r$ и $g(X) = s(X)$, и получить такие полиномы $r_k(X) = a_k(X)X^r + b_k(X)s(X)$, что $\deg r_{k-1}(X) \geqslant r/2$ и $\deg r_k(X) < r/2$;

в) положить $\ell(X) = b_k(0)^{-1} b_k(X)$, $\varepsilon(X) = b_k(0)^{-1} r_k(X)$.

Тогда полином $\ell(X)$ является многочленом обнаружения ошибок корни которого являются обратными элементами $y_1 = \alpha_{i_1}^{-1}, \dots, y_t = \alpha_{i_t}^{-1}$, где $i_1, \dots, i_t$ — позиции ошибок. Значения e_{i_j} задаются соотношениями

$$e_{i_j} = \frac{\varepsilon(\alpha_{i_j}^{-1})}{h_{i_j} \prod_{l \neq j} (1 - \alpha_{i_l} \alpha_{i_j}^{-1})}. \tag{3.5.28}$$

Идеи, использованные в этом параграфе, получили значительное развитие в теории алгебро-геометрических кодов. Алгебраическая геометрия дает мощные средства при создании новых кодов, см. [vLG, TV, TVN].

§ 3.6. Дополнительные задачи к главе 3

Задача 3.6.1. Дайте определение кодов Рида—Соломона (РС) и докажите, что они относятся к кодам с максимальным допустимым расстоянием (м. д. р.). Докажите, что двойственный код к коду РС тоже является кодом РС.

Найдите минимальное расстояние кода РС длины 15 и ранга 11, порождённого многочленом $g_1(X)$ над полем $\mathbb{F}_{16}$. Используйте готовую таблицу поля $\mathbb{F}_{16}$, чтобы представить $g_1(X)$ в виде $\omega^{i_0} + \omega^{i_1} X + \omega^{i_2} X^2 + \dots$, идентифицировав каждый коэффициент со степенью примитивного элемента ω поля $\mathbb{F}_{16}$.

Найдите порождающий полином $g_2(X)$ и минимальное расстояние кода РС длины 10 и ранга 6. Воспользуйтесь готовой таблицей поля $\mathbb{F}_{11}$, чтобы записать $g_2(X)$ как $a_0 + a_1 X + \dots$, где коэффициенты — это числа из множества $\{0, 1, \dots, 10\}$.

Определите код РС, исправляющий две ошибки, над $\mathbb{F}_{16}$, найдите его длину, ранг и порождающий полином.

Таблица поля $\mathbb{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ со сложением и умножением по модулю 11 имеет вид

i	1	2	3	4	5	6	7	8	9	10
ω^i	1	2	4	8	5	10	9	7	3	6

Таблица поля $\mathbb{F}_{16} = \mathbb{F}_2^4$:

i	0	1	2	3	4	5	6	7	8
ω^i	0001	0010	0100	1000	0011	0110	1100	1011	0101

i	9	10	11	12	13	14
ω^i	1010	0111	1110	1111	1101	1001

Решение. Определяем q-ичный код РС $\mathcal{X}^{\mathrm{PC}}$ с проектируемым расстоянием $\delta \leqslant q-1$ как циклический код длины $N = q-1$ над $\mathbb{F}_q$ с порождающим полиномом

$$g(X) = (X - \omega^b)(X - \omega^{b+1}) \dots (X - \omega^{b+\delta-2})$$

степени $\deg g(X) = \delta - 1$. Здесь ω — примитивный $(q-1, \mathbb{F}_q)$-корень из единицы (т. е. примитивный элемент группы $\mathbb{F}_q^*$) и $b = 0, 1, \dots, q-2$. Степени $\omega^b, \dots, \omega^{b+\delta-2}$ называются (определяющими) нулями, а остальные $N - \delta + 1$ степеней элемента ω — не нулями кода $\mathcal{X}^{\mathrm{PC}}$.

Ранг кода $\mathcal{X}^{\mathrm{PC}}$ равен $k = N - \delta + 1$. Его расстояние не меньше $\delta = N - k + 1$, но по границе Синглтона оно не больше $\delta = N - k + 1$, так что расстояние в точности равно $\delta = N - k + 1$, т. е. $\mathcal{X}^{\mathrm{PC}}$ — код с максимальным достижимым расстоянием (м. д. р.).

Двойственный $(\mathcal{X}^{\mathrm{PC}})^\perp$ к $\mathcal{X}^{\mathrm{PC}}$ — тоже код РС, а его нули обратны к не нулям кода $\mathcal{X}^{\mathrm{PC}}$:

$$\omega^{q-1-j} = (\omega^j)^{-1}, \quad j \neq b, \dots, b + \delta - 2.$$

Иначе говоря, нули такие:

$$\omega^{q-b}, \quad \omega^{q-b+1}, \quad , \dots, \quad \omega^{q-b+q-\delta-1},$$

и порождающий многочлен $g^\perp(X)$ кода $(\mathcal{X}^{\mathrm{PC}})^\perp$ равен

$$g^\perp(X) = (X - \omega^{b^\perp})(X - \omega^{b^\perp+1}) \dots (X - \omega^{b^\perp+q-\delta-1}),$$

где $b^\perp = q - b$. Таким образом, $(\mathcal{X}^{\mathrm{PC}})^\perp$ — код РС с проектируемым расстоянием $q - \delta + 1$.

В нашем примере $N = 15$ означает, что $q = 15 + 1 = 16$ и ранг равен 11, находим расстояние: $\delta = 15 - 11 + 1 = 5$. Образующая $g_1(X)$ над $\mathbb{F}_{16} = \mathbb{F}_2^4$ для кода с $b = 1$ выглядит как

$$g_1(X) = (X - \omega)(X - \omega^2)(X - \omega^3)(X - \omega^4) =$$
$$= X^4 - (\omega + \omega^2 + \omega^3 + \omega^4)X^3 + (\omega^3 + \omega^4 + \omega^5 + \omega^5 + \omega^6 + \omega^7)X^2 -$$
$$- (\omega^6 + \omega^7 + \omega^8 + \omega^9)X + \omega^{10} = X^4 + \omega^{13}X^3 + \omega^6X^2 + \omega^3X + \omega^{10},$$

где вычисления производились с помощью таблицы поля $\mathbb{F}_{16}$.

Аналогично длина 10 означает, что $q = 11$, а ранг равен 6, находим расстояние: $\delta = 10 - 6 + 1 = 5$. Образующая $g_2(X)$ определена над полем $\mathbb{F}_{11}$ и при $b = 1$ имеем

$$g_2(X) = (X - \omega)(X - \omega^2)(X - \omega^3)(X - \omega^4) =$$
$$= X^4 - (\omega + \omega^2 + \omega^3 + \omega^4)X^3 + (\omega^3 + \omega^4 + \omega^5 + \omega^5 + \omega^6 + \omega^7)X^2 -$$
$$- (\omega^6 + \omega^7 + \omega^8 + \omega^9)X + \omega^{10} = X^4 + 3X^3 + 5X^2 + 8X + 1,$$

где вычисления осуществлены при помощи таблицы поля $\mathbb{F}_{11}$.

Наконец, код РС над полем $\mathbb{F}_{16}$, исправляющий две ошибки, имеет длину $N = 15$ и расстояние $\delta = 5$, следовательно, его ранг равен 11, так что он совпадает с рассмотренным выше 16-ичным $[15, 11]$-кодом РС. □

The Maximum Sentence Criminal Code[3]

A Maximum Distance Separation Divorce Settlement[4]

(Из серии «Фильмы, которые не вышли на большой экран».)

Задача 3.6.2. Пусть $\mathcal{X}$ — двоичный линейный $[N, k]$-код и $\mathcal{X}^{\mathrm{ev}}$ — множество слов из $\mathcal{X}$ чётного веса. Докажите, что либо а) $\mathcal{X} = \mathcal{X}^{\mathrm{ev}}$, либо б) $\mathcal{X}^{\mathrm{ev}}$ — $[N, k-1]$ линейный подкод кода $\mathcal{X}$.

Докажите, что если в образующей матрице G нет нулевых столбцов, то общий вес кода $\sum\limits_{\mathbf{x}\in\mathcal{X}} w(\mathbf{x}) = N \cdot 2^{k-1}$.

Указание. Исследуйте вклад каждого столбца матрицы G.

Обозначим через $\mathcal{X}_{\mathrm{H},l}$ двоичный код Хэмминга длины $N = 2^l - 1$, а через $\mathcal{X}_{\mathrm{H},l}^{\perp}$ — двойственный симплексный код, $l = 3, 4, \ldots$ Всегда ли N-вектор $1 \ldots 1$ (все единицы) является кодовым словом в $\mathcal{X}_{\mathrm{H},l}$? Пусть A_s и $A_s^{\perp}$ —

[3] Ср. с названием фильма «The Criminal Code».

[4] Ср. с названием фильмов «A Separation» (иранский фильм, получивший премию Оскар в 2012 г.) и «Divorce Italian Style» («Развод по-итальянски», фильм 1961 г. с М. Мастрояни, популярный в СССР в 1960-е годы).

число слов веса s в кодах $\mathcal{X}_{\mathrm{H},l}$ и $\mathcal{X}_{\mathrm{H},l}^{\perp}$ соответственно, $A_0 = A_0^{\perp} = 1$ и $A_1 = A_2 = 0$. Проверьте, что

$$A_3 = N(N-1)/3!, \quad A_4 = N(N-1)(N-3)/4!$$

и

$$A_5 = N(N-1)(N-3)(N-7)/5!.$$

Докажите, что $A_{2^l-1}^{\perp} = 2^l - 1$ (т. е. все ненулевые слова $\mathbf{x} \in \mathcal{X}_{\mathrm{H},l}^{\perp}$ имеют вес $2^l - 1$). Основываясь на этом факте и тождестве Мак-Вильямс для двоичных кодов, выпишите формулу для A_s в терминах значения многочлена Кравчука

$$K_s(2^{l-1}) = \sum_{j=0\vee s+2^{l-1}-2^l+1}^{s\wedge 2^{l-1}} C_{2^{l-1}}^{j} C_{2^l-1-2^{l-1}}^{s-j} (-1)^j.$$

Здесь $0 \vee s + 2^{l-1} - 2^l + 1 = \max[0,\, s + 2^{l-1} - 2^l + 1]$ и $s \wedge 2^{l-1} = \min[s,\, 2^{l-1}]$. Убедитесь, что ваша формула даёт правильный ответ для $s = N = 2^l - 1$.

Решение. Код $\mathcal{X}^{\mathrm{ev}}$ — это всегда линейный подкод в $\mathcal{X}$. Действительно, для двоичных слов $\mathbf{x}$ и $\mathbf{x}'$ имеем $w(\mathbf{x}+\mathbf{x}') = w(\mathbf{x}) + w(\mathbf{x}') - 2w(\mathbf{x}\wedge\mathbf{x}')$, где $(\mathbf{x}\wedge\mathbf{x}')_j = x_j x_j' = \min[x_j,\, x_j']$. Если оба слова $\mathbf{x}$, $\mathbf{x}'$ чётны (имеют чётный вес) или нечётны (имеют нечётный вес), то $\mathbf{x}+\mathbf{x}'$ чётно, а если $\mathbf{x}$ чётно, а $\mathbf{x}'$ нет, то сумма $\mathbf{x}+\mathbf{x}'$ нечётна. Итак, если $\mathcal{X}^{\mathrm{ev}} \neq \mathcal{X}$, то $\mathcal{X}^{\mathrm{ev}}$ — подгруппа в $\mathcal{X}$ индекса $[\mathcal{X}^{\mathrm{ev}} : \mathcal{X}]$ два. Значит, существуют два смежных класса и $\mathcal{X}^{\mathrm{ev}}$ — ровно половине кода $\mathcal{X}$, следовательно, $\mathcal{X}^{\mathrm{ev}}$ — $[N,\, k-1]$-код.

Пусть $\mathbf{g}^{(j)} = (g_{1j},\, \ldots,\, g_{kj})^{\mathrm{T}}$ — j-й столбец образующей матрицы G кода $\mathcal{X}$. Положим $\mathcal{W}_j = \{i = 1,\, \ldots,\, k\colon\, g_{ij} = 1\}$ с $\#\mathcal{W}_j = w(\mathbf{g}^{(j)}) = w_j \geqslant 1$, $1 \leqslant j \leqslant N$. Вклад $\mathbf{g}^{(j)}$ в сумму $\sum\limits_{\mathbf{x}\in\mathcal{X}} w(\mathbf{x})$ равен

$$2^{k-w_j} \times 2^{w_j-1} = 2^{k-1}.$$

Здесь 2^{k-w_j} — число подмножеств дополнения $\{1,\, \ldots,\, k\} \setminus \mathcal{W}_j$, а 2^{w_j-1} — число нечётных подмножеств в $\mathcal{W}_j$. Умножая это число на N (число столбцов), получаем $N2^{k-1}$.

Если $H = H_{\mathrm{H},l}$ — проверочная матрица кода Хэмминга $\mathcal{X}_{\mathrm{H},l}$, то вес её j-й строки совпадает с числом единиц, стоящих в j-й позиции в двоичном представлении чисел $1,\, \ldots,\, 2^l - 1$, $1 \leqslant j \leqslant l$. Поэтому, $w(\mathbf{h}^{(j)}) = 2^{l-1}$ (у половины чисел $0,\, 1,\, \ldots,\, 2^l - 1$ на j-й позиции стоит 1, а у второй половины — 0). Тогда $\forall j = 1,\, \ldots,\, N$ имеем $\langle \mathbf{I}\cdot\mathbf{h}^{(j)}\rangle = w(\mathbf{h}^{(j)}) \bmod 2 = 0$, т. е. $1\ldots1 \in \mathcal{X}_{\mathrm{H},l}$.

Далее, $A_3 = N(N-1)/3!$ — число линейно зависимых троек столбцов матрицы H (так как выбор определяется двумя различными столбцами,

а третий — их сумма), $A_4 = N(N-1)(N-3)/4!$ — число линейно зависимых четвёрок столбцов из H (так как выбор определяется а) парой разных столбцов, б) третьим, отличным от их суммы и в) в качестве последнего столбца берётся сумма первых трёх) и аналогично $A_5 = N(N-1)(N-3)(N-7)/5!$ — число линейно зависимых пятёрок столбцов матрицы H. (Здесь $N-7$ означает, что, выбрав первые четыре столбца, мы должны исключить из дальнейшего рассмотрения все $2^3 - 1 = 7$ линейных комбинаций трёх из них.)

На самом деле вес любого ненулевого слова $\mathbf{X}$ двойственного кода $\mathcal{X}^{\perp}_{\mathrm{H},l}$ равен $w(\mathbf{x}) = 2^{l-1}$. Для доказательства заметим, что образующая матрица кода $\mathcal{X}^{\perp}_{\mathrm{H},l}$ совпадает с H. Поэтому представим $\mathbf{x}$ как сумму строк матрицы H и обозначим через $\mathcal{W}$ множество слагаемых этой суммы, с $\#\mathcal{W} = w \leqslant l$. Тогда $w(\mathbf{x})$ равен числу таких позиций j среди $1, 2, \ldots, 2^l - 1$, что в двоичном представлении $j = 2^0 j_0 + 2^1 j_1 + \ldots + 2^{l-1} j_{l-1}$ сумма $\sum\limits_{t \in \mathcal{W}} j_t \bmod 2 = 1$. Как и раньше, этот вес равен 2^{w-1} (числу подмножеств в $\mathcal{W}$ нечётной мощности). Значит, $w(\mathbf{x}) = 2^{l-w+w-1} = 2^{l-1}$. Заметим, что ранг кода $\mathcal{X}^{\perp}_{\mathrm{H},l}$ составляет $2^l - 1 - (2^l - 1 - l) = l$, а размер $\#\mathcal{X}^{\perp}_{\mathrm{H},l} = 2^l$.

Тождество Мак-Вильямс, примененное к двойственному коду, имеет вид

$$A_s = \frac{1}{\#\mathcal{X}^{\perp}_{\mathrm{H},l}} \sum_{i=1}^{N} A^{\perp}_i K_s(i), \tag{3.6.1}$$

где

$$K_s(i) = \sum_{j=0 \vee s+i-N}^{s \wedge i} C^j_i C^{s-j}_{N-i} (-1)^j, \tag{3.6.2}$$

$0 \vee s + i - N = \max[0,\, s + i - N]$, $s \wedge i = \min[s,\, i]$. В нашем случае $A^{\perp}_0 = 1$, $A^{\perp}_{2^l-1} = 2^l - 1$ (число ненулевых слов в $\mathcal{X}^{\perp}_{\mathrm{H},l}$). Значит,

$$A_s = \frac{1}{2^l}(1 + (2^l - 1)K_s(2^l - 1)) =$$

$$= \frac{1}{2^l}\left(1 + (2^l - 1) \sum_{j=0 \vee s+2^{l-1}-2^l+1}^{s \wedge 2^{l-1}} C^j_{2^{l-1}} C^{2^l-1-j}_{2^l-1-2^{l-1}} (-1)^j\right).$$

При $s = N = 2^l - 1$ значение A_{2^l-1} может быть либо 1 (если 2^l-слово $1 \ldots 1$ лежит в коде $\mathcal{X}_{\mathrm{H},l}$), либо 0 (если нет). Из последней формулы следует, что

$$A_{2^l-1} = \frac{1}{2^l}\left(1 + (2^l - 1) \sum_{j=2^{l-1}}^{2^l-1} C^j_{2^{l-1}} C^{2^l-1-j}_{2^l-1-2^{l-1}}\right) = \frac{1}{2^l}\left(1 + 2^l - 1\right) = 1,$$

что согласуется с включением $1\dots1\in\mathcal{X}_{\mathrm{H},l}$. □

Задача 3.6.3. Пусть ω — корень многочлена $M(X)=X^5+X^2+1$ в поле $\mathbb{F}_{32}$; известно, что $M(X)$ — примитивный многочлен поля $\mathbb{F}_{32}$, а ω — примитивный $(31,\mathbb{F}_{32})$-корень из единицы. С помощью элементов ω, ω^2, ω^3, ω^4 постройте двоичный примитивный БЧХ-код в узком смысле $\mathcal{X}$ длины 31 и с проектируемым расстоянием 5. Выпишите циклотомический класс $\{i,\,2i,\,\dots,\,2^{d-1}i\}$ для каждого из элементов ω, ω^2, ω^3, ω^4. Проверьте, что в качестве определяющих нулей кода $\mathcal{X}$ достаточно взять элементы ω и ω^3 и что минимальное расстояние этого кода равно 5. Покажите, что порождающий полином $g(X)$ кода $\mathcal{X}$ представляется как произведение

$$(X^5+X^2+1)(X^5+X^4+X^3+X^2+1)=X^{10}+X^9+X^8+X^6+X^5+X^3+1.$$

Допустим, вы получили слово $u(X)=X^{12}+X^{11}+X^9+X^7+X^6+X^2+1$ от корреспондента, пользующегося кодом $\mathcal{X}$. Проверьте, что $u(\omega)=\omega^3$ и $u(\omega^3)=\omega^9$. Прокомментируйте, почему полученное слово декодируется как

$$c(X)=X^{12}+X^{11}+X^9+X^7+X^6+X^3+X^2+1$$

и убедитесь, что $c(X)$ действительно является кодовым словом в $\mathcal{X}$.

Для удобства вычислений выпишем таблицу поля $\mathbb{F}_{32}=\mathbb{F}_2^5$ и список неприводимых многочленов степени 5 над $\mathbb{F}_2$.

Таблица поля имеет вид

i	0	1	2	3	4	5	6	7
ω^i	00001	00010	00100	01000	10000	00101	01010	10100
i	8	9	10	11	12	13	14	15
ω^i	01101	11010	10001	00111	01110	11100	11101	
i	16	17	18	19	20	21	22	23
ω^i	11011	10011	00011	00110	01100	11000	10101	01111
i	24	25	26	27	28	29	30	
ω^i	11110	11001	10111	01011	10110	01001	10010	

Список неприводимых многочленов степени 5 над $\mathbb{F}_2$:

$$X^5+X^2+1,\quad X^5+X^3+1,\quad X^5+X^3+X^2+X+1,$$
$$X^5+X^4+X^3+X+1,\quad X^5+X^4+X^3+X^2+1$$

порядок каждого из них равен 31. Многочлен X^5+X^2+1 примитивен.

Решение. Поскольку $M(X)=X^5+X^2+1$ — примитивный многочлен в кольце $\mathbb{F}_2[X]$, любой его корень ω — примитивный $(31,\mathbb{F}_2)$-корень из

единицы, т. е. $\omega^{31}+1=0$. Более того, $M(X)$ — минимальный многочлен для ω.

По построению БЧХ-код $\mathcal{X}$ — это циклический код, порождаемый многочленом минимальной степени, обращающийся в нуль на элементах ω, ω^2, ω^3, ω^4 (т. е. циклический код, нули которого — это минимальное множество, содержащее ω, ω^2, ω^3, ω^4). Таким образом, порождающий полином $g(X)$ кода $\mathcal{X}$ — это наименьшее общее кратное минимальных многочленов для ω, ω^2, ω^3, ω^4.

Циклотомический класс для ω — это $C=\{1, 2, 4, 8, 16\}$, значит,

$$(X-\omega)(X-\omega^2)(X-\omega^2)(X-\omega^4)(X-\omega^8)(X-\omega^{16})=X^5+X^2+1$$

— минимальный многочлен для ω, ω^2 и ω^4. Циклотомический класс для ω^3 равен $C=\{3, 6, 12, 24, 17\}$, и минимальный многочлен $M_{\omega^3}(X)$ для ω^3 равен

$$\begin{aligned}M_{\omega^3}(X)&=(X-\omega^3)(X-\omega^6)(X-\omega^{12})(X-\omega^{24})(X-\omega^{17})=\\&=X^5+(\omega^3+\omega^6+\omega^{12}+\omega^{24}+\omega^{17})X^4+\\&\quad+(\omega^9+\omega^{15}+\omega^{27}+\omega^{20}+\omega^{18}+\omega^{30}+\omega^{23}+\omega^{36}+\omega^{29}+\omega^{41})X^3+\\&\quad+(\omega^{21}+\omega^{33}+\omega^{26}+\omega^{39}+\omega^{32}+\omega^{44}+\omega^{42}+\omega^{35}+\omega^{47}+\omega^{53})X^2+\\&\qquad+(\omega^{45}+\omega^{38}+\omega^{50}+\omega^{56}+\omega^{59})X+\omega^{62}=X^5+X^4+X^3+X^2+1,\end{aligned}$$

что можно проверить вычислениями, основанными на таблице, или сверяясь со списком неприводимых многочленов над $\mathbb{F}_2$ степени 5.

Итак, в качестве определяющих нулей достаточно взять ω и ω^3, и порождающий полином $g(X)$ равен

$$(X^5+X^2+1)(X^5+X^4+X^3+X^2+1)=X^{10}+X^9+X^8+X^6+X^5+X^3+1,$$

что и требовалось. Иначе говоря,

$$\begin{aligned}\mathcal{X}=\{c(X)\in\mathbb{F}_2[X]/\langle X^{31}+1\rangle\colon c(\omega)=c(\omega^3)=0\}=\\=\{c(X)\in\mathbb{F}_2[X]/\langle X^{31}+1\rangle\colon g(X)|c(X)\}.\end{aligned}$$

Ранг кода $\mathcal{X}$ равен 21, а минимальное расстояние — 5 и совпадает с проектируемым расстоянием. Это следует из теоремы 3.3.19.

Пусть $N=2^l-1$. Если $2^{lE}<\sum\limits_{i=0}^{E+1}C_N^i$, то расстояние примитивного БЧХ-кода в узком смысле с проектируемым расстоянием $2E+1$ совпадает с проектируемым.

В нашем случае $N=31=2^5-1$ и $l=5$, $E=2$, т. е. $2E+1=5$ и

$$1024=2^{10}<1+31+\frac{31\times 30}{2}+\frac{31\times 30\times 29}{2\times 3}=4992.$$

Таким образом, код $\mathcal{X}$ исправляет 2 ошибки. Для алгоритма декодирования Берлекэмпа—Мэсси нужны значения полученного многочлена в определяющих нулях кода. Из таблицы поля $\mathbb{F}_{32}$ получаем, что

$$u(\omega) = \omega^{12} + \omega^{11} + \omega^9 + \omega^7 + \omega^6 + \omega^2 + 1 = \omega^3,$$
$$u(\omega^3) = \omega^{36} + \omega^{33} + \omega^{27} + \omega^{18} + \omega^6 + 1 = \omega^9.$$

Отсюда видно, что $u(\omega^3) = u(\omega)^3$. Так как $u(\omega) = \omega^3$, то можно сделать вывод о том, что в сообщение закралась единственная ошибка в третьем знаке, т. е. $u(X)$ декодируется как

$$c(X) = X^{12} + X^{11} + X^9 + X^7 + X^6 + X^3 + X^2 + 1,$$

что, как и должно быть, представляется в виде произведения $(X^2 + 1)g(X)$. □

Задача 3.6.4. Дайте определение двойственного кода $\mathcal{X}^\perp$ к линейному $[N, k]$-коду длины N размерности k с алфавитом $\mathbb{F}$. Докажите или опровергните утверждение о том, что двойственный код $\mathcal{X}^\perp$ к двоичному $[N, (N-1)/2]$-коду $\mathcal{X}$ при нечётном N порождается базисом кода $\mathcal{X}$ и словом $1 \ldots 1$. Докажите или опровергните утверждение о том, что если двоичный код $\mathcal{X}$ самодвойственный ($\mathcal{X}^\perp = \mathcal{X}$), то N чётно и слово $1 \ldots 1 \in \mathcal{X}$. Докажите, что двоичный самодвойственный линейный $[N, N/2]$-код $\mathcal{X}$ существует при всех чётных N. Обратно, докажите, что если двоичный линейный $[N, k]$-код $\mathcal{X}$ самодвойственный, то $k = N/2$.

Приведите пример не двоичного линейного самодвойственного кода.

Решение. Двойственный код к $[N, k]$-линейному коду $\mathcal{X}$ определяется как

$$\mathcal{X}^\perp = \{\mathbf{x} = x_1 \ldots x_N \in \mathbb{F}^N \colon \langle \mathbf{x} \cdot \mathbf{y} \rangle = 0 \ \forall \mathbf{y} \in \mathcal{X}\},$$

где $\langle \mathbf{x} \cdot \mathbf{y} \rangle = x_1 y_1 + \cdots + x_N y_N$. Возьмём $N = 5$, $k = (N-1)/2 = 2$ и

$$\mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Тогда $\mathcal{X}^\perp$ порождается матрицей

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ни один из векторов кода $\mathcal{X}$ не лежит в $\mathcal{X}^\perp$, так что утверждение ложно.

Теперь возьмём самодвойственный код $\mathcal{X} = \mathcal{X}^\perp$. Если слово $\mathbf{l} = 1 \ldots 1 \notin \mathcal{X}^\perp$, то найдётся слово $\mathbf{x} \in \mathcal{X}$, для которого $\langle \mathbf{x} \cdot \mathbf{l} \rangle \neq 0$. Но

$\langle \mathbf{x} \cdot \mathbf{l} \rangle = \sum x_i = w(\mathbf{x}) \mod 2$. С другой стороны, $\sum x_i = \langle \mathbf{x} \cdot \mathbf{x} \rangle$, т. е. $\langle \mathbf{x} \cdot \mathbf{x} \rangle \neq \neq 0$. Но тогда $\mathbf{x} \notin \mathcal{X}^\perp$. Следовательно, $\mathbf{l} \in \mathcal{X}$, но тогда $\langle \mathbf{l} \cdot \mathbf{l} \rangle = 0$, откуда следует чётность N.

Пусть теперь $N = 2k$. Разобьём знаки $1, \ldots, N$ на k непересекающихся пар $(\alpha_1, \beta_1), \ldots, (\alpha_k, \beta_k)$, $\alpha_i < \beta_i$. Рассмотрим k двоичных слов $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(k)}$ длины N и веса 2, причём ненулевые знаки в слове $\mathbf{x}^{(i)}$ расположены на местах α_i и β_i. Сформируем $[N, k]$-код $\mathcal{X}$, порождённый словами $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(k)}$.

Код $\mathcal{X}$ самодвойственный. Действительно, $\langle \mathbf{x}^{(i)} \cdot \mathbf{x}^{(j)} \rangle = 0 \ \forall i, j$. Следовательно, $\mathcal{X} \subset \mathcal{X}^\perp$. Обратно, пусть $\mathbf{y} \in \mathcal{X}^\perp$. Тогда $\langle \mathbf{y} \cdot \mathbf{x}^{(i)} \rangle = 0 \ \forall i$. Это означает, что для всех i у $\mathbf{y}$ на позициях α_i, β_i стоят либо одни нули, либо одни единицы. Значит, $\mathbf{y} \in \mathcal{X}$ и $\mathcal{X} = \mathcal{X}^\perp$.

Предположим теперь, что $\mathcal{X}^\perp = \mathcal{X}$. Тогда N чётно. Но размерность k равна $N/2$ по теореме о размерности ядра и образа.

Не двоичный линейный самодвойственный код — это троичный $[12, 6]$-код Голея с образующей матрицей

$$G = \begin{pmatrix} 1&0&0&0&0&0&0&1&1&1&1&1 \\ 0&1&0&0&0&0&1&0&1&2&2&1 \\ 0&0&1&0&0&0&1&1&0&1&2&2 \\ 0&0&0&1&0&0&1&2&1&0&1&2 \\ 0&0&0&0&1&0&1&2&2&1&0&1 \\ 0&0&0&0&0&1&1&1&2&2&1&0 \end{pmatrix}.$$

Все строки матрицы G ортогональны друг другу (в том числе и себе). Значит, $\mathcal{X} \subset \mathcal{X}^\perp$. Но $\dim(\mathcal{X}) = \dim(\mathcal{X}^\perp)$, откуда $\mathcal{X} = \mathcal{X}^\perp$. □

Задача 3.6.5. Дайте определение конечного поля $\mathbb{F}_q$ из q элементов и докажите, что непременно $q = p^s$, где p — простое число, а $s \geqslant 1$ — натуральное число. Проверьте, что p является характеристикой поля $\mathbb{F}_q$.

Докажите, что всегда существует конечное поле $\mathbb{F}_{p^s}$ из p^s элементов и такое поле единственно с точностью до изоморфизма.

Докажите, что множество $\mathbb{F}_{p^s}^*$ ненулевых элементов поля $\mathbb{F}_{p^s}$ — это циклическая группа $\mathbb{Z}_{p^s-1}$.

Выпишите таблицу поля $\mathbb{F}_9$, отождествляя степени ω^i примитивного элемента $\omega \in \mathbb{F}_9$ с вектором над $\mathbb{F}_3$. Отметьте в этой таблице все векторы α, для которых $\alpha^4 = e$.

Решение. Поле $\mathbb{F}_q$ из q элементов — это множество мощности q с двумя коммутативными операциями: $+$ и $\cdot$, связанными стандартной дистрибутивностью. Легко проверить, что $\mathrm{char}(\mathbb{F}_q) = p$ — простое число. Тогда $\mathbb{F}_p \subset \mathbb{F}_q$ и $q = \#\mathbb{F}_q = p^s$, где $s = [\mathbb{F}_q : \mathbb{F}_p]$ — размерность $\mathbb{F}_q$ как векторного пространства над полем $\mathbb{F}_p$ из p элементов.

Пусть теперь $\mathbb{F}_q^*$ — мультипликативная группа ненулевых элементов из $\mathbb{F}_q$. Она содержит элемент порядка $q-1=\#\mathbb{F}_q^*$. Действительно, каждый элемент $b\in\mathbb{F}_q^*$ имеет конечный порядок $\operatorname{ord}(b)=r(b)$; положим $r_0=$ $=\max[r(b)\colon b\in\mathbb{F}_q^*]$ и зафиксируем $a\in\mathbb{F}_q^*$ с $r(a)=r_0$. Тогда $r(b)|r_0\ \forall b\in\mathbb{F}_q^*$. Возьмём простой делитель γ числа $r(b)$ и запишем $r(b)=\gamma^{s'}\omega$, $r_0=\gamma^s\alpha$. Проверим, что $s\geqslant s'$. Действительно, порядок элемента a^{γ^s} равен α, порядок элемента b^ω — $\gamma^{s'}$, а порядок элемента $a^{\gamma^s}b^\omega$ равен $\gamma^{s'}\alpha$. Значит, если $s'>s$, мы получили элемент порядка больше чем r_0. Следовательно, $s\geqslant s'$, что справедливо для любого простого делителя числа $r(b)$, т. е. $r(b)|r(a)$.

Тогда $b^{r(a)}=e$, т. е. многочлен $X^{r_0}-e$ делится на $X-b\ \forall b\in\mathbb{F}_q^*$. Поэтому он должен равняться произведению $\prod\limits_{b\in\mathbb{F}_q^*}(X-b)$, откуда $r_0=\#\mathbb{F}_q^*=q-1$. Таким образом, $\mathbb{F}_q^*$ — циклическая группа, порождённая элементом a.

Для любого простого числа p и натурального числа s существует не более одного поля $\mathbb{F}_q$, $q=p^s$ с точностью до изоморфизма. Действительно, если $\mathbb{F}_q$ и $\mathbb{F}'_q$ — два таких поля, то они будут изоморфны полю разложения $\operatorname{Spl}\bigl(X^q-X\bigr)$ многочлена X^q-X (над основным полем $\mathbb{F}_p$).

Элементы $\alpha\in\mathbb{F}_9=\mathbb{F}_3\times\mathbb{F}_3$, для которых $\alpha^4=e$ — это $e=01$, $\omega^2=$ $=1+2\omega=21$, $\omega^4=02$, $\omega^6=2+\omega=12$, где $\omega=10$. □

> В случае, если вы ещё не поняли: в троичном исчислении есть 10 типов людей в этом мире (впервые это заметил Д. Б. Шоу): те, кто могут (и делают), те, кто не может (они учат), и те, кто не может учить (они учат учителей).
>
> (Из серии «Так говорил суперлектор»);
> перефразирование Джорджа Бернарда Шоу
> (1856–1950), англо-ирландский драматург и публицист

Задача 3.6.6. Дайте определение циклического кода длины N с алфавитом $\mathbb{F}_q$. Что такое определяющие нули циклического кода и почему они всегда являются $(N,\mathbb{F}_q)$-корнями из единицы? Докажите, что троичный $[(3^3-1)/2,\ (3^s-1)/2-s,\ 3]$-код Хэмминга эквивалентен циклическому коду, и укажите определяющие нули этого циклического кода.

Отправитель пользуется троичным $[13,\ 10,\ 3]$-кодом Хэмминга с алфавитом $\mathbb{F}_3$ и проверочной матрицей вида

$$\begin{pmatrix}1&0&1&2&0&1&2&0&1&2&0&1&2\\0&1&1&1&0&0&0&1&1&1&2&2&2\\0&0&0&0&1&1&1&1&1&1&1&1&1\end{pmatrix}.$$

Получатель читает слово $\mathbf{x}=2120110021120$. Как его следует декодировать?

Решение. Поскольку $g(X)|X^N-1$, все корни многочлена $g(X)$ — корни степени N из единицы. Пусть $\text{НОД}\,(l, q-1)=1$. Докажем, что $\left[\dfrac{q^l-1}{q-1}, \dfrac{q^l-1}{q-1}-l\right]$-код Хэмминга эквивалентен циклическому коду с определяющим нулём $\omega=\beta^{q-1}$, где β — примитивный корень из единицы степени $(q^l-1)/(q-1)$. Действительно, положим $N=(q^l-1)/(q-1)$. Поле разложения имеет вид $\text{Spl}\big(X^N-1\big)=\mathbb{F}_{q^r}$, где $r=\text{ord}_N(q)=$ $=\min[s\colon N|(q^s-1)]$. Тогда $r=l$, поскольку $(q^l-1)/(q-1)|(q^l-1)$ и $l=$ $=\min\left[s\colon q^s=1 \bmod \dfrac{q^l-1}{q-1}\right]$. Значит, $\text{Spl}\big(X^N-1\big)=\mathbb{F}_{q^l}$.

Если β — примитивный элемент поля $\mathbb{F}_{q^l}$, то $\omega=\beta^{(q^l-1)/N}=\beta^{q-1}$ — примитивный корень из единицы степени N в $\mathbb{F}_{q^l}$. Запишем $\omega^0=e$, $\omega, \omega^2, \ldots, \omega^{N-1}$ как вектор-столбец в матрицу H размера $l\times N$. Мы хотим проверить, что любые два разных столбца в H линейно независимы. Это можно сделать точно так же, как в теореме 3.3.13.

Тогда код с проверочной матрицей H имеет расстояние $d\geqslant 3$ и ранг $k\geqslant N-l$. Граница Хэмминга с $N=(q^l-1)/(q-1)$ имеет вид

$$q^k\leqslant q^N\left(\sum_{m=0}^{E} C_N^m(q-1)^m\right)^{-1},\quad E=\left\lfloor\frac{d-1}{2}\right\rfloor, \tag{3.6.3}$$

и показывает, что $d=3$ и $k=N-l$, так что циклический код с проверочной матрицей H эквивалентен коду Хэмминга.

Чтобы декодировать слово из условия, вычислим синдром $\mathbf{x}H^{\mathrm{T}}=2\,0\,2=$ $=2\cdot(1\,0\,1)$, указывающий на ошибку в 6-й позиции. Следовательно, $\mathbf{x}-2\mathbf{e}^{(6)}=\mathbf{y}+\mathbf{e}^{(6)}$, и правильное слово — $\mathbf{c}=2\,1\,2\,0\,1\,2\,0\,0\,2\,1\,1\,2\,0$. □

Задача 3.6.7. Вычислите ранг и минимальное расстояние циклического кода, порождённого многочленом $g(X)=X^3+X+1$, проверочный многочлен которого равен $h(X)=X^4+X^2+X+1$. Пусть теперь ω — корень многочлена $g(X)$ в поле $\mathbb{F}_8$. Мы получили слово $r(X)=X^5+X^3+X \bmod (X^7-1)$. Проверьте, что $r(\omega)=\omega^4$, и декодируйте $r(X)$, используя декодирование минимального расстояния.

Решение. Циклический код $\mathcal{X}$ длины N обладает порождающим полиномом $g(X)\in\mathbb{F}_2[X]$ и проверочным многочленом $h(X)\in\mathbb{F}_2[X]$, причём $h(X)g(X)=X^N-1$. Напомним, что если степень многочлена $g(X)$ равна k, т. е. $g(X)=a_0+a_1X+\ldots+a_kX^k$, где $a_k\neq 0$, то $g(X), Xg(X), \ldots, X^{N-k-1}g(X)$ — базис кода $\mathcal{X}$. В частности, ранг кода $\mathcal{X}$ равен $N-k$. В этой задаче $k=3$ и $\text{rank}(\mathcal{X})=4$.

Если $h(X) = b_0 + b_1 X + \ldots + b_{N-k} X^{N-k}$, то проверочная матрица H кода $\mathcal{X}$ равна

$$\underbrace{\begin{pmatrix} b_{N-k} & b_{N-k-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 & 0 \\ 0 & b_{N-k} & b_{N-k-1} & \ldots & b_1 & b_0 & \ldots & 0 & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ 0 & 0 & \ldots & 0 & b_{N-k} & b_{N-k-1} & \ldots & b_1 & b_0 \end{pmatrix}}_{N}.$$

Кодовые слова в $\mathcal{X}$ — это соотношения линейной зависимости на столбцы матрицы H. Минимальное расстояние $d(\mathcal{X})$ линейного кода $\mathcal{X}$ совпадает с минимальным ненулевым весом его кодовых слов. В этой задаче $N = 7$ и

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

отсутствие нулевых столбцов $\Longrightarrow$ отсутствие кодовых слов веса 1

отсутствие повторяющихся столбцов $\Longrightarrow$ отсутствие кодовых слов веса 2

Следовательно, $d(\mathcal{X}) = 3$. На самом деле код $\mathcal{X}$ эквивалентен $[7, 4]$-коду Хэмминга.

Так как многочлен $g(X) \in \mathbb{F}_2[X]$ неприводим, код $\mathcal{X} \subset \mathbb{F}_2^7 = \mathbb{F}_2[X]/\langle X^7 - 1\rangle$ — циклический, с образующей ω. Мультипликативная циклическая группа $\mathbb{F}_8^* \simeq \mathbb{Z}_7^*$ ненулевых элементов поля $\mathbb{F}_8$ состоит из элементов

$$\begin{aligned} &\omega^0 = 1, && \omega^4 = \omega^2 + \omega, \\ &\omega, && \omega^5 = \omega^3 + \omega^2 = \omega^2 + \omega + 1, \\ &\omega^2, && \omega^6 = \omega^3 + \omega^2 + \omega = \omega^2 + 1, \\ &\omega^3 = \omega + 1, && \omega^7 = \omega^3 + \omega = 1. \end{aligned}$$

Далее, значение $r(\omega)$ равно

$$r(\omega) = \omega + \omega^3 + \omega^5 = \omega + (\omega + 1) + (\omega^2 + \omega + 1) = \omega^2 + \omega = \omega^4,$$

что и требовалось. Пусть $c(X) = r(X) + X^4 \mod (X^7 - 1)$. Тогда $c(\omega) = 0$, т. е. $c(X)$ — кодовое слово. Поскольку $d(\mathcal{X}) = 3$, этот код исправляет одну ошибку. Мы уже нашли кодовое слово $c(X)$, отстоящее на расстоянии 1 от $r(X)$. Значит, $r(X)$ декодируется как

$$c(X) = X + X^3 + X^4 + X^5 \mod (X^7 - 1). \qquad \square$$

Специалист по теории чисел делает это натурально и рационально.

(Из серии «Как они делают это».)

Задача 3.6.8. Определите производящую функцию весов $W_{\mathcal{X}}(s, t)$ линейного $[N, k]$-кода $\mathcal{X}$. Покажите, что

а) $W_{\mathcal{X}}(1, 1) = 2^k$,

б) $W_{\mathcal{X}}(0, 1) = 1$,

в) $W_{\mathcal{X}}(1, 0) = 0$ или 1,

г) $W_{\mathcal{X}}(s, t) = W_{\mathcal{X}}(t, s)$ тогда и только тогда, когда $W_{\mathcal{X}}(1, 0) = 1$.

Решение. Вес $w(\mathbf{x})$ слова $\mathbf{x} \in \mathcal{X}$ по определению равен $w(\mathbf{x}) = \#\{x_i = 1\}$. Определим производящую функцию весов

$$W_{\mathcal{X}}(s, t) = \sum A_j s^j t^{N-j}, \tag{3.6.4}$$

где $A_j = \#\{\mathbf{x} \in \mathcal{X}\colon w(\mathbf{x}) = j\}$. Тогда

а) $W_{\mathcal{X}}(1, 1) = \#\{\mathbf{x}\colon \mathbf{x} \in \mathcal{X}\} = 2^{\dim \mathcal{X}} = 2^k$,

б) $W_{\mathcal{X}}(0, 1) = A_0 = \#\{\mathbf{0}\} = 1$ ($\mathbf{0} \in \mathcal{X}$, так как $\mathcal{X}$ — подпространство),

в) $W_{\mathcal{X}}(1, 0) = 1 \Leftrightarrow A_N = 1$, т. е. $1 \ldots 1 \in \mathcal{X}$, $W_{\mathcal{X}}(1, 0) = 0 \Leftrightarrow A_N = 0$, т. е. $1 \ldots 1 \notin \mathcal{X}$,

г) $W_{\mathcal{X}}(s, t) = W_{\mathcal{X}}(t, s) \Rightarrow W(0, 1) = W(1, 0) \Rightarrow W_{\mathcal{X}}(1, 0) = 1$ по п. б); $W_{\mathcal{X}}(1, 0) = 1 \Rightarrow 1 \ldots 1 \in \mathcal{X} \Rightarrow (\mathbf{x} \in \mathcal{X} \Leftrightarrow \mathbf{x} + 1 \ldots 1 \in \mathcal{X})$.

Поэтому из предположения $W_{\mathcal{X}}(1, 0) = 1$ следует, что

$$\#\{\mathbf{x} \in \mathcal{X}\colon w(\mathbf{x}) = j\} = \#\{\mathbf{x} + 1 \ldots 1\colon \mathbf{x} \in \mathcal{X},\ w(\mathbf{x}) = j\} = \\ = \#\{\mathbf{y} \in \mathcal{X}\colon w(\mathbf{y}) = N - j\},$$

и из равенства $W_{\mathcal{X}}(1, 0) = 1$ следует тождество $A_{N-j} = A_j$ для всех j. Значит, $W_{\mathcal{X}}(s, t) = W_{\mathcal{X}}(t, s)$. □

Задача 3.6.9. Сформулируйте тождество Мак-Вильямс, связывающее производящие функции весов кодов $\mathcal{X}$ и $\mathcal{X}^{\perp}$ (двойственного к $\mathcal{X}$).

Докажите, что производящая функция весов двоичного кода Хэмминга $\mathcal{X}_{\mathrm{H},l}$ длины $N = 2^l - 1$ равна

$$W_{\mathcal{X}_{\mathrm{H},l}}(z) = \frac{1}{2^l}[(1 + z)^{2^l - 1} + (2^l - 1)(1 - z^2)^{(2^l - 2)/2}(1 - z)]. \tag{3.6.5}$$

Решение (только вторая часть). Пусть A_i — число кодовых слов веса i. Рассмотрим $i - 1$ столбцов проверочной матрицы H. Возможны три ситуации: а) сумма этих столбцов равна $\mathbf{0}$; б) сумма этих столбцов равна одному из выбранных столбцов; в) сумма этих столбцов равна одному из оставшихся столбцов.

Ситуация а) возникает A_{i-1} раз, ситуация в) — iA_i раз, так как выбранная комбинация $i-1$ столбцов может быть получена из любого слова веса i отбрасыванием любой его ненулевой компоненты. Заметим далее, что ситуация б) возникает $(N-(i-2))A_{i-2}$ раз. Действительно, эту комбинацию можно получить из кодового слова веса $i-2$ при сложении с любым из $N-(i-2)$ оставшихся столбцом. Однако мы можем выбрать $i-1$ столбцов C_N^{i-1} способами. Следовательно,

$$iA_i = C_N^{i-1} - A_{i-1} - (N-i+2)A_{i-2}, \tag{3.6.6}$$

что, очевидно, справедливо при $i > N+1$. Умножив обе части на z^{i-1} и просуммировав затем по i, мы получим обыкновенное дифференциальное уравнение

$$A'(z) = (1+z)^N - A(z) - NzA(z) + z^2A'(z). \tag{3.6.7}$$

Так как $A(0)=1$, единственным решением этого уравнения служит функция

$$A(z) = \frac{1}{N+1}(1+z)^N + \frac{N}{N+1}(1+z)^{(N-1)/2}(1-z)^{(N+1)/2}, \tag{3.6.8}$$

что совпадает с функцией (3.6.5). □

Задача 3.6.10. Пусть $\mathcal{X}$ — линейный $[N, k]$-код над $\mathbb{F}_2$ и A_i — число его слов веса i, $i=0, \ldots, N$. Определим производящую функцию весов кода $\mathcal{X}$ как

$$W(\mathcal{X}, z) = \sum_{i-0}^{N} A_i z^i.$$

Пусть $\mathcal{X}^\perp$ — двойственный код к коду $\mathcal{X}$. Покажите, что

$$W(\mathcal{X}^\perp, z) = 2^{-k}(1+z)^N W\Big(\mathcal{X}, \frac{1-z}{1+z}\Big). \tag{3.6.9}$$

Указание. Рассмотрите $g(\mathbf{u}) = \sum\limits_{\mathbf{v}\in\mathbb{F}_2^N} (-1)^{\langle \mathbf{u}\cdot\mathbf{v}\rangle} z^{w(\mathbf{v})}$, где $w(\mathbf{v})$ — вес вектора $\mathbf{v}$ и $\dfrac{1}{\#\mathcal{X}} \sum\limits_{u\in\mathcal{X}} g(u)$ — среднее по коду $\mathcal{X}$.

Выведите отсюда, что если $\mathcal{X}$ исправляет хотя бы одну ошибку, то средний вес кода $\mathcal{X}^\perp$ равен $N/2$.

Примените тождество (3.6.9) к производящей функции весов кода Хэмминга

$$W(\mathcal{X}_{\text{Ham}}, z) = \frac{1}{N+1}(1+z)^N + \frac{N}{N+1}(1+z)^{(N-1)/2}(1-z)^{(N+1)/2} \tag{3.6.10}$$

и найдите производящую функцию весов симплексного кода

$$W(\mathcal{X}_{\text{simp}}, z) = 2^{-k}2^N/2^l + 2^{-k}(2^l-1)/2^l \times 2^N z^{l-1} = 1 + (2^l-1)z^{2^{l-1}}.$$

Решение. Двойственный код $\mathcal{X}^\perp$ к линейному коду $\mathcal{X}$ с образующей матрицей G и проверочной матрицей H — это линейный код с образующей матрицей H. Если $\mathcal{X}$ — $[N, k]$-код, то $\mathcal{X}^\perp$ — $[N, N-k]$-код и проверочная матрица двойственного кода совпадает с G.

Эквивалентным образом, $\mathcal{X}^\perp$ — это код, образованный подпространством в $\mathbb{F}_2^N$, ортогональным $\mathcal{X}$ относительно скалярного произведения $\langle \mathbf{x}, \mathbf{y}\rangle$. По определению

$$W(\mathcal{X}, z) = \sum_{\mathbf{u}\in\mathcal{X}} z^{w(\mathbf{u})}, \qquad W(\mathcal{X}^\perp, z) = \sum_{\mathbf{v}\in\mathcal{X}^\perp} z^{w(\mathbf{v})}.$$

Следуя указанию, рассмотрим среднее

$$\frac{1}{\#\mathcal{X}} \sum_{\mathbf{u}\in\mathcal{X}} g(\mathbf{u}), \quad \text{где } g(\mathbf{u}) = \sum_{\mathbf{v}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} z^{w(\mathbf{v})}. \tag{3.6.11}$$

Перепишем выражение (3.6.11) в виде

$$\frac{1}{\#\mathcal{X}} \sum_{\mathbf{v}} z^{w(\mathbf{v})} \sum_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle}. \tag{3.6.12}$$

Заметим, что если $\mathbf{v} \in \mathcal{X}^\perp$, то $\sum\limits_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} = \#\mathcal{X}$. С другой стороны, когда $\mathbf{v} \notin \mathcal{X}^\perp$, то найдётся такое $\mathbf{u}_0 \in \mathcal{X}$, что $\langle \mathbf{u}_0, \mathbf{v}\rangle \neq 0$ (т. е. $\langle \mathbf{u}_0, \mathbf{v}\rangle = 1$). Значит, если $\mathbf{v} \notin \mathcal{X}^\perp$, то при замене переменных $\mathbf{u} \mapsto \mathbf{u} + \mathbf{u}_0$ мы получаем

$$\sum_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} = \sum_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u}+\mathbf{u}_0,\mathbf{v}\rangle} = (-1)^{\langle \mathbf{u}_0,\mathbf{v}\rangle} \sum_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} = -\sum_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle},$$

следовательно, в этом случае $\sum\limits_{\mathbf{u}\in\mathcal{X}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} = 0$. Отсюда можно сделать вывод о том, что сумма в формуле (3.6.11) равна

$$\frac{1}{\#\mathcal{X}} \sum_{\mathbf{v}\in\mathcal{X}^\perp} z^{w(\mathbf{v})} (\#\mathcal{X}) = W(\mathcal{X}^\perp, z). \tag{3.6.13}$$

С другой стороны, для $\mathbf{u} = u_1 \dots u_N$ имеем

$$g(\mathbf{u}) = \sum_{v_1,\dots,v_N} \prod_{i=1}^{N} z^{w(v_i)} (-1)^{u_i v_i} = \prod_{i=1}^{N} \sum_{a=0,1} z^{w(a)} (-1)^{a u_i} = \prod_{i=1}^{N} (1 + z(-1)^{u_i}). \tag{3.6.14}$$

Здесь $w(a) = 0$ при $a = 0$ и $w(a) = 1$ при $a = 1$. П. ч. формулы (3.6.14) равна

$$(1 - z)^{w(\mathbf{u}} (1 + z)^{N - w(\mathbf{u})}.$$

Значит, альтернативное выражение для среднего из формулы (3.6.11) имеет вид

$$\frac{1}{\#\mathcal{X}}(1+z)^N \sum_{\mathbf{u}\in\mathcal{X}} \left(\frac{1-z}{1+z}\right)^{w(\mathbf{u})} = \frac{1}{\#\mathcal{X}}(1+z)^N W\Big(\mathcal{X},\, \frac{1-z}{1+z}\Big). \qquad (3.6.15)$$

Приравнивая формулы (3.6.13) и (3.6.15), получаем

$$\frac{1}{\#\mathcal{X}}(1+z)^N W\Big(\mathcal{X},\, \frac{1-z}{1+z}\Big) = W(\mathcal{X}^\perp,\, z), \qquad (3.6.16)$$

что даёт равенство (3.6.9), поскольку $\#\mathcal{X} = 2^k$.

Вычислим далее производную п. ч. выражения из формулы (3.6.16) по z в точке $z = 1$:

$$\sum_{i=0}^{N} iA_i(\mathcal{X}^\perp) = (\#\mathcal{X}^\perp) \times (\text{средний вес в } \mathcal{X}^\perp).$$

С другой стороны, в л. ч. мы имеем

$$\frac{d}{dz}\left(\frac{1}{\#\mathcal{X}}\sum_{i=0}^{N} A_i(\mathcal{X})(1-z)^i(1+z)^{N-i}\right)\Big|_{z=1} =$$

$$= \frac{1}{\#\mathcal{X}}(N2^{N-1} - A_1(\mathcal{X})2^{N-1}) \text{ (вклад дают члены с номерами } i = 0,\, 1) =$$

$$= \frac{2^N}{\#\mathcal{X}}\frac{N}{2} \ (A_1(\mathcal{X}) = 0, \text{ так как код исправляет по крайней мере 1 ошибку, расстояние не меньше 3}).$$

Далее, учитывая, что

$$(\#\mathcal{X}) \times (\#\mathcal{X}^\perp) = 2^k \times 2^{N-k} = 2^N,$$

получаем равенство

$$\text{средний вес в } \mathcal{X}^\perp = \frac{N}{2}.$$

Производящая функция весов симплексного кода получается подстановкой функции (3.6.10) в тождество Мак-Вильямс. В этом случае средняя длина равна $(2^l - 1)/2$. □

Задача 3.6.11. Опишите двоичный БЧХ-код в узком смысле длины 15 и с проектируемым расстоянием 5 и найдите порождающий полином. Декодируйте сообщение 100000111000100.

Решение. Возьмём двоичный БЧХ-код в узком смысле длины 15 и с проектируемым расстоянием 5. Мы имеем $\mathrm{Spl}\big(X^{15} - 1\big) = \mathbb{F}_{2^4} = \mathbb{F}_{16}$. Мы

знаем, что $X^4 + X + 1$ — примитивный многочлен над $\mathbb{F}_{16}$. Пусть ω — его корень. Тогда

$$M_1(X) = X^4 + X + 1, \quad M_3(X) = X^4 + X^3 + X^2 + X + 1$$

и порождающий полином $g(X)$ кода $\mathcal{X}$ равен

$$g(X) = M_1(X)M_3(X) = X^8 + X^7 + X^6 + X^4 + 1.$$

В качестве примера кодового слова возьмём $g(X)$. На позиции 5 и 13 внесем по ошибке, положив

$$u(X) = X^{12} + X^8 + X^7 + X^6 + 1.$$

Опираясь на таблицу поля $\mathbb{F}_{16}$, получаем

$$u_1 = u(\omega) = \omega^{12} + \omega^8 + \omega^7 + \omega^6 + 1 = \omega^6$$

и

$$u_3 = u(\omega^3) = \omega^{36} + \omega^{24} + \omega^{18} + 1 = \omega^9 + \omega^3 + 1 = \omega^4.$$

Так как $u_1 \neq 0$ и $u_1^3 = \omega^{18} = \omega^3 \neq u_3$, возникло не менее двух ошибок. Вычисляем многочлен обнаружения ошибок.

$$\omega(X) = 1 + \omega^6 X + (\omega^{13} + \omega^{12})X^2.$$

Подставляя в $\omega(X)$ элементы $1, \omega, \ldots, \omega^{14}$, убеждаемся, что ω^3 и ω^{11} — его корни. Это подтверждает, что если возникло ровно 2 ошибки, то было послано слово 100010111000000. □

Задача 3.6.12. Вес слова $\mathbf{x} = x_1 \ldots x_N \in \mathbb{F}_2^N$ — это число его ненулевых знаков $w(\mathbf{x}) = \#\{i\colon x_i \neq 0\}$. Пусть $\mathcal{X}$ — линейный $[N, k]$-код. Обозначим через A_i число слов веса i $(0 \leqslant i \leqslant N)$. Определим производящую функцию весов $W(\mathcal{X}.z) = \sum\limits_{i=0}^{N} A_i z^i$. Покажите, что при применении $\mathcal{X}$ в д. с. к. б. п. с вероятностью ошибки p вероятность не обнаружения ошибочного слова составляет $(1-p)^N \Big(W\Big(\mathcal{X}, \frac{p}{1-p}\Big) - 1\Big)$.

Решение. Предположим, что мы послали нулевое кодовое слово $\mathbf{0}$. Ошибка не замечена, если на выходе появилось слово $\mathbf{x} \in \mathcal{X} \setminus \mathbf{0}$, и вероятность ошибки составляет

$$E = \sum_{\mathbf{x} \in \mathcal{X} \setminus \mathbf{0}} \mathbf{P}(\mathbf{x} | \mathbf{0} \text{ послано}) = \sum_{i \geqslant 1} A_i p^i (1-p)^{N-i} =$$

$$= (1-p)^N \left[\sum_{i \geqslant 0} A_i \Big(\frac{p}{1-p} \Big)^i - 1 \right] = (1-p)^N \Big(W\Big(\mathcal{X}, \frac{p}{1-p}\Big) - 1\Big). \quad \square$$

Задача 3.6.13. Пусть $\mathcal{X}$ — двоичный $[N, k, d]$-код с производящей функцией весов $W_{\mathcal{X}}(s)$. Выразите через $W_{\mathcal{X}}(s)$ производящие функции весов 1) подкода $\mathcal{X}^{\mathrm{ev}} \subseteq \mathcal{X}$, состоящего изо всех кодовых слов $\mathbf{x} \in \mathcal{X}$ чётного веса, 2) расширения проверки на чётность $\mathcal{X}^+$ кода $\mathcal{X}$. Докажите, что при чётном d существует $[N, k, d]$-код, у которого все слова с чётным весом.

Решение. 1) Все слова чётного веса из $\mathcal{X}$ образуют подкод $\mathcal{X}^{\mathrm{ev}}$. Следовательно,

$$W_{\mathcal{X}^{\mathrm{ev}}}(s) = \frac{1}{2}(W_{\mathcal{X}}(s) + W_{\mathcal{X}}(-s)).$$

2) Ясно, что все ненулевые коэффициенты производящей функции весов для $\mathcal{X}^+$ стоят при чётных степенях z и $A_{2i}(\mathcal{X}^+) = A_{2i}(\mathcal{X}) + A_{2i-1}(\mathcal{X})$, $i = 1, 2, \ldots$ Значит,

$$W_{\mathcal{X}^+}(s) = \frac{1}{2}[(1+s)W_{\mathcal{X}}(s) + (1-s)W_{\mathcal{X}}(-s)].$$

Если $\mathcal{X}$ — двоичный $[N, k, d]$-код, то вы сначала усечёте $\mathcal{X}$ до $\mathcal{X}^-$, а затем возьмёте расширение проверкой на чётность $(\mathcal{X}^-)^+$. Это сохранит k и d (если d чётно) и придаст всем кодовым словам чётный вес. □

Задача 3.6.14. Проверьте неприводимость многочленов $X^4 + X^3 + X^2 + X + 1$ и $X^4 + X + 1$ над $\mathbb{F}_2$. Что можно сказать о многочленах $X^3 + X + 1$, $X^3 + X^2 + 1$, $X^4 + X^3 + 1$?

Решение. Так как оба многочлена $X^4 + X^3 + X^2 + X + 1$ и $X^4 + X + 1$ не обращается в нуль в точках 0 и 1, они не делятся ни на X, ни на $X + 1$. Они также не делятся на $X^2 + X + 1$, единственный неприводимый многочлен степени 2, ни на многочлены $X^3 + X + 1$, $X^3 + X^2 + 1$, которыми исчерпываются неприводимые многочлены степени 3. Следовательно, они неприводимы.

Многочлен $X^4 + X^3 + X^2 + X + 1$ не может быть примитивным, поскольку он делит $X^5 + 1$. Проверим, что $X^4 + X + 1$ — примитивный многочлен. Возьмём $\mathbb{F}_2[X]/\langle X^4 + X + 1\rangle$ и воспользуемся таблицей поля $\mathbb{F}_2^4$. Циклотомический класс состоит из $\{\omega, \omega^2, \omega^4, \omega^8\}$ (так как $\omega^{16} = \omega$). Тогда примитивный многочлен $M_\omega(X)$ равен

$$\begin{aligned}
&(X-\omega)(X-\omega^2)(X-\omega^4)(X-\omega^8) = \\
&= X^4 - (\omega + \omega^2 + \omega^4 + \omega^8)X^3 + (\omega\omega^2 + \omega\omega^4 + \omega\omega^8 + \omega^2\omega^4 + \omega^4\omega^8)X^2 - \\
&\qquad - (\omega\omega^2\omega^4 + \omega\omega^2\omega^8 + \omega\omega^4\omega^8 + \omega^2\omega^4\omega^8)X + \omega\omega^2\omega^4\omega^8 = \\
&= X^4 - (\omega + \omega^2 + \omega^4 + \omega^8)X^3 + (\omega^3\omega^5 + \omega^9 + \omega^6 + \omega^{10} + \omega^{12})X^2 - \\
&\qquad - (\omega^7 + \omega^{11} + \omega^{13} + \omega^{14})X + \omega^{15} = X^4 + X + 1.
\end{aligned}$$

Порядок многочлена $X^4 + X + 1$ равен 15, другой примитивный многочлен порядка 15 — это $X^4 + X^3 + 1$. Итак, имеется два примитивных многочлена

степени 4 — это X^4+X+1 и X^4+X^3+1. Аналогично все примитивные многочлены степени 3 — это X^3+X+1 и X^3+X^2+1, оба порядка 7. □

The Cyclotomic Yellow Submarine[5]

(Из серии «Фильмы, которые не вышли на большой экран».)

Задача 3.6.15. Предположим, что используется двоичный БЧХ-код в узком смысле длины 15, с проектируемым расстоянием 5, и получено слово $X^{10}+X^5+X^4+X+1$. Как его декодировать? Сколько ошибок имеется в полученном слове $X^{11}+X^{10}+X^6+X^5+X^4+X+1$?

Решение. Допустим, мы получили слово

$$r(X)=X^{10}+X^5+X^4+X+1$$

и пусть ω — примитивный элемент поля $\mathbb{F}_{16}$. Тогда

$$s_1=r(\omega)=\omega^{10}+\omega^5+\omega^4+\omega+e=$$
$$=0111+0110+0011+0010+0001=0001=e,$$
$$s_3=r(\omega^3)=\omega^{30}+\omega^{15}+\omega^{12}+\omega^3+e=$$
$$=0001+0001+1111+1000+0001=0110=\omega^5.$$

Поскольку $s_3\neq s_1^3$, были допущены две ошибки. Многочлен обнаружения ошибок имеет вид

$$\sigma(X)=e+s_1X+(s_3s_1^{-1}+s_1^2)X^2=e+X+(\omega^5+e)X^2=e+X+\omega^{10}X^2.$$

Прямой подстановкой получаем, что элементы $\omega^0=e$, ω^1, ω^2, ω^3, ω^4, ω^5, ω^6 не являются его корнями, а ω^7 является. Тогда

$$\omega^{10}X^2+X+e)/(X+\omega^7)=\omega^{10}X+\omega^8=\omega^{10}(X+\omega^{13})$$

и мы находим второй корень ω^{13}. Следовательно, ошибочны члены со степенями $15-7=8$ и $15-13=2$. Значит, при декодировании получаем

$$r(X)\mapsto X^{10}+X^8+X^5+X^4+X^2+X+1.$$ □

Задача 3.6.16. Докажите, что двоичный код длины 23, порождённый многочленом $g(X)=g(X)=1+X+X^5+X^6+X^7+X^9+X^{11}$ имеет минимальное расстояние 7 и совершенен.

Указание. Если $g^{\mathrm{rev}}(X)=X^{11}g(1/X)$ — обращение многочлена $g(X)$, то

$$X^{23}+1\equiv(X+1)g(X)g^{\mathrm{rev}}(X)\mod 2.$$

[5]Ср. с названием мультфильма «Yellow submarine» (1981 г., по песням и музыке группы «Битлз»).

Решение. Прежде всего покажем, что это — БЧХ-код с проектируемым расстоянием 5. По лемме 3.1.5 (мечта первокурсника) если ω — корень многочлена $f(X) \in \mathbb{F}_2[X]$, то корнем же будет и ω^2. Значит, если ω — корень многочлена $g(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$, то его корнями будут и ω^2, ω^4, ω^8, ω^{16}, ω^9, ω^{18}, ω^{13}, ω^3, ω^6, ω^{12}. Это даёт последовательность $\{\omega, \omega^2, \omega^3, \omega^4\}$. По границе БЧХ (лемма 3.2.12) циклический код $\mathcal{X}$, порождённый $g(X)$, имеет расстояние не меньше 5.

Далее, расширение проверкой на чётность $\mathcal{X}^+$ ортогонально себе. Для проверки этого факта нам нужно только показать, что любая пара строк порождающей матрицы $\mathcal{X}^+$ ортогональна. Строки представляются сцеплением строк

$$(X^i g(X)|1) \quad \text{и} \quad (X^j g(X)|1).$$

Их скалярное произведение равно

$$1 + (X^i g(X))(X^j g(X)) = 1 + \sum_r g_{i+r} g_{j+r} = 1 + \sum_r g_{i+r} g^{\mathrm{rev}}_{11-j-r} =$$

$$= 1 + (\text{коэффициент при } X^{11+i-j} \text{ в } g(X) \times g^{\mathrm{rev}}(X) = 1 + \ldots + X^{22}) = 1 + 1 = 0.$$

Отсюда следует вывод:

любые два слова в $\mathcal{X}^+$ ортогональны.

Заметим далее, что вес любого слова из $\mathcal{X}^+$ делится на 4. Действительно, простой проверкой убеждаемся, что вес каждой строки $(X^i g(X)|1)$ образующей матрицы $\mathcal{X}^+$ делится на 8. Тогда индукцией по числу строк, участвующих в сумме слова $\mathbf{x}$, показываем, что если $\mathbf{x} \in \mathcal{X}^+$ и $\mathbf{g}^{(i)} \sim (X^i g(X)|1$ — строка порождающей матрицы кода $\mathcal{X}^+$, то

$$w(\mathbf{g}^{(i)} + \mathbf{x}) = w(\mathbf{g}^{(i)}) + w(\mathbf{x}) - 2w(\mathbf{g}^{(i)} \wedge \mathbf{x}), \tag{3.6.15}$$

где $(\mathbf{g}^{(i)} \wedge \mathbf{x}) = \min[(\mathbf{g}^{(i)})_l, x_l)]$, $l = 1, \ldots, 24$. Мы знаем, что $w(\mathbf{g}^{(i)})$ делится на 8. Более того, по предположению индукции 4 делит $w(\mathbf{x})$. Далее, из соотношения (3.6.15) следует, что $w(\mathbf{g}^{(i)} \wedge \mathbf{x})$ чётно, так что $2w(\mathbf{g}^{(i)} \wedge \mathbf{x})$ делится на 4. Значит, л. ч. $w(\mathbf{g}^{(i)} + \mathbf{x})$ делится на 4.

Следовательно, расстояние кода $\mathcal{X}^+$ равно 8, поскольку оно не меньше 5 и делится на 4. (Легко заметить, что оно не больше 8, так как оно должно было бы равняться 12.) Таким образом, расстояние кода $\mathcal{X}$ равно 7.

Код $\mathcal{X}$ — совершенный, исправляющий 3 ошибки, поскольку объём 3-шара в $\mathbb{F}_2^{23}$ равен

$$C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3 = 1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

и

$$2^{11} \times 2^{12} = 2^{23}.$$

Здесь, очевидно, 12 — это ранг, а 23 — длина. □

The Perfect Da Vinci Code[6]

(Из серии «Фильмы, которые не вышли на большой экран».)

Задача 3.6.17. Рассмотрим q-ичный м. д. р.-код $\mathcal{X}_N$ длины N с максимально достижимым расстоянием d. Пусть $A_i = \#\{x \in \mathcal{X}_N\colon w(x) = i\}$. С помощью тождества Мак-Вильямс покажите, что

$$A_i = C_N^i \sum_{j=0}^{i-d} (-1)^j C_i^j (q^{i-d+1-j} - 1) = C_N^i (q-1) \sum_{j=0}^{i-d} (-1)^j C_{i-1}^j q^{i-d-j}, \quad d \leqslant i \leqslant N.$$

Указание. Для начала 1) выпишите стандартное тождество Мак-Вильямс, 2) переставьте $\mathcal{X}$ и $\mathcal{X}^\perp$, 3) сделайте замену $s \mapsto s^{-1}$, 4) умножьте на s^n и 4) возьмите производную d^r/ds^r, $0 \leqslant r \leqslant k(= d(\mathcal{X}^\perp - 1)$. Используйте правило Лейбница

$$\frac{d^r}{ds^r}[f(s)g(s)] = \sum_{j=0}^{r} C_r^j \Big[\frac{d^j}{ds^j} f(s)\Big] \Big[\frac{d^{r-j}}{ds^{r-j}} g(s)\Big]. \tag{3.6.16}$$

Воспользуйтесь теми фактами, что $d(\mathcal{X}) = N - k + 1$ и $d(\mathcal{X}^\perp) = k + 1$, и получите упрощённое уравнение только на $A_{N-k+1}, \ldots, A_{N-r}$. Из него определите $A_{N-k+1}, \ldots, A_{N-r}$. Варьируя r, продолжите до A_N.

Решение. Тождество Мак-Вильямс выглядит так:

$$\sum_{i=1}^{N} A_i^\perp s^i = \frac{1}{q^k} \sum_{i=1}^{N} A_i (1-s)^i [1 + (q-1)s]^{N-i}.$$

Переставив $\mathcal{X}$ и $\mathcal{X}^\perp$, заменим $s \mapsto s^{-1}$ и подставим $s = 1$:

$$\frac{1}{q^k} \sum_{i=0}^{N-r} C_{N-i}^r A_i = \frac{1}{q^r} \sum_{i=0}^{r} A_i^\perp C_{N-i}^{N-r} \tag{3.6.17}$$

(здесь мы воспользовались правилом Лейбница (3.6.16)). Формула (3.6.17) служит отправной точкой. Для разделимого кода с максимальным расстоянием имеем $A_0 = A_0^\perp = 1$ и

$$A_i = 0, \quad 1 \leqslant i \leqslant N - k(= d - 1), \qquad A_i^\perp = 0, \quad 1 \leqslant i \leqslant k(= d^\perp - 1).$$

Поэтому

$$C_N^r \frac{1}{q^k} + \frac{1}{q^k} \sum_{i=N-k+1}^{N-r} C_{N-i}^r A_i = \frac{1}{q^r} C_N^{N-r} = \frac{1}{q^r} C_N^r,$$

[6] Ср. с названием фильма «The Da Vinci Code» (2006 г.).

т. е.

$$\sum_{i=N-k+1}^{N-r} C_{N-i}^{r} A_i = C_N^r (q^{k-r} - 1).$$

При $r = k$ мы получаем, что $0 = 0$, при $r = k-1$ находим

$$A_{N-k+1} = C_N^{k-1}(q-1), \tag{3.6.18}$$

при $r = k-2$ получаем

$$C_{k-1}^{k-2} A_{N-k+1} + A_{N-k+2} = C_N^{k-2}(q^2 - 1)$$

и т. д. Получилась треугольная система уравнений на $A_{N-k+1}, \ldots, A_{N-r}$. Варьируя r, мы можем найти $A_{N-k+1}, \ldots, A_{N-1}$, и в результате получим

$$\begin{aligned} A_i &= C_N^i \sum_{j=0}^{i-d} (-1)^j C_i^j (q^{i-d+1-j} - 1) = \\ &= C_N^i \left[\sum_{j=0}^{i-d} (-1)^j C_{i-1}^j (q q^{i-d-j} - 1) - \sum_{j=0}^{i-d+1} (-1)^{j-1} C_{i-1}^{j-1} (q^{i-d+1-j} - 1) \right] = \\ &= C_N^i (q-1) \sum_{j=0}^{i-d} (-1)^j C_{i-1}^j q^{i-d-j}, \quad d \leqslant i \leqslant N, \end{aligned}$$

как и требовалось.

На самом деле соотношение (3.6.18) можно получить без вычислений: в м. д. р.-коде с максимальным достижимым расстоянием d ранга k любые $k = N - d + 1$ знаков однозначно определяют кодовое слово. При любом выборе $N - d$ позиций существуют ровно q кодовых слов с 0 на этих местах. Одно из них нулевое, а вес оставшихся $q - 1$ слов равен d. Значит,

$$A_{N-k+1} = A_d = C_N^d (q-1). \qquad \square$$

Задача 3.6.18. Докажите следующие свойства многочленов Кравчука $K_k(i)$:

а) для любого q выполнено равенство $(q-1)^i C_N^i K_k(i) = (q-1)^k C_N^k K_i(k)$,

б) при $q = 2$ выполнено равенство $K_k(i) = (-1)^k K_k(N-i)$,

в) при $q = 2$ выполнено равенство $K_k(2i) = K_{N-k}(2i)$.

Решение. Запишем

$$K_k(i) = \sum_{j=0 \vee (i+k-N)}^{k \wedge i} C_i^j C_{N-i}^{k-j} (-1)^j (q-1)^{k-j}.$$

а) Имеет место следующее соотношение:

$$(q-1)^i C_N^i K_k(i) = (q-1)^k C_N^k K_i(k)$$

(поскольку все слагаемые не зависят от замены $i \leftrightarrow k$).

При $q = 2$ из этого следует, что $C_N^i K_k(i) = C_N^k K_i(k)$, в частности, $C_N^i K_0(i) = C_N^o K_i(0) = K_i(0)$.

б) К тому же при $q = 2$ получаем, что $K_k(i) = (-1)^k K_k(N-i)$ (вновь непосредственно после замены $i \leftrightarrow i - j$).

в) Теперь остаётся заметить, что при $q = 2$ имеем $C_N^{2i} K_k(2i) = C_N^k K_{2i}(k)$, что эквивалентно равенству $(-1)^{2i} C_N^{N-k} K_{2i}(N-k) = C_N^{2i} K_{N-k}(2i)$, т. е.

$$K_k(2i) = K_{N-k}(2i). \qquad \square$$

Задача 3.6.19. Дайте определение примитивного $(n, \mathbb{F}_q)$-корня из единицы. Покажите, что множество $(n, \mathbb{F}_q)$-корней из единицы $\mathsf{E}^{(n,q)}$ образует циклическую группу. Проверьте, что порядок группы $\mathsf{E}^{(n,q)}$ равен n, если n и q взаимно просты. Если $\omega \in \mathbb{F}_{q^l}$ — примитивный $(n, \mathbb{F}_q)$-корень из единицы, найдите минимальное l, при котором $\omega \in \mathbb{F}_{q^l}$.

Представьте все элементы поля $\mathbb{F}_9$ как векторы над $\mathbb{F}_3$. Найдите все $(4, \mathbb{F}_9)$-корни из единицы в виде векторов над $\mathbb{F}_3$.

Решение. Любой корень неприводимого многочлена степени 2 над $\mathbb{F}_3 = \{0, 1, 2\}$ принадлежит полю $\mathbb{F}_9$. Возьмём многочлен $f(X) = X^2 + 1$ и обозначим его корень (любой из двух) через α. Тогда элементы поля $\mathbb{F}_9$ представляются в виде $a_0 + a_1\alpha$, где $a_0, a_1 \in \mathbb{F}_3$. Действительно,

$$\mathbb{F}_9 = \{0,\ 1,\ 2,\ \alpha,\ 1+\alpha,\ 2+\alpha,\ 2\alpha,\ 1+2\alpha,\ 2+2\alpha\}.$$

Другой подход состоит в следующем: запишем $X^8 - 1 = \prod\limits_{i=1}^{8} (X - \omega^i)$ в поле $\mathbb{F}_9$, где ω — примитивный $(8, \mathbb{F}_9)$-корень из единицы. В терминах круговых многочленов $X^8 - 1 = Q_1(X)Q_2(X)Q_4(X)Q_8(X)$. Здесь $Q_n(X) = \prod\limits_{s:\ \text{НОД}(s,n)=1} (x - \omega^s)$. Запишем $X^8 - 1 = \prod\limits_{d:\ d|8} Q_d(x)$ и вычислим

$$Q_8(X) = (X^8 - 1)/(Q_1(X)Q_2(X)Q_4(X)) = (X^8 - 1)/(X^4 - 1) = X^4 + 1.$$

Здесь $Q_1(X) = -1 + X$, $Q_2(X) = 1 + X$, $Q_4(X) = 1 + X^2$. Так как $3^2 = 1 \bmod 8$, по теореме 3.1.53 получаем, что многочлен $Q_8(X)$ над полем $\mathbb{F}_3$ должен раскладываться в произведение $\varphi(8)/2 = 2$ неприводимых многочленов степени 2. Действительно,

$$Q_8(X) = (X^2 + X + 2)(X^2 + 2X + 2).$$

Пусть ω — корень многочлена $X^2 + X + 2$, тогда он будет примитивным корнем из единицы степени 8 над $\mathbb{F}_9 = \mathbb{F}_3(\omega)$. Следовательно, $\mathbb{F}_9 =$

$= \{0, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7, \omega^8\}$, и $\omega = 1 + \alpha$. Наконец, выпишем таблицу степеней:

$$\begin{array}{llll} \omega = 1 + \alpha, & \omega^2 = 2\alpha, & \omega^3 = 1 + 2\alpha, & \omega^4 = 2, \\ \omega^5 = 2 + 2\alpha, & \omega^6 = \alpha, & \omega^7 = 2 + \alpha, & \omega^8 = 1. \end{array}$$

Таким образом, у нас есть четыре корня степени 4: ω^2, ω^4, ω^6, ω^8. □

Задача 3.6.20. Дайте определение циклического кода длины N над полем $\mathbb{F}_q$. Докажите, что существует взаимно однозначное соответствие между циклическими кодами длины N и делителями многочлена $X^N - e$ в полиномиальном кольце $\mathbb{F}_q[X]$.

Теперь рассмотрим двоичные циклические коды. Если N — нечётное натуральное число, то можно найти конечное расширение K поля $\mathbb{F}_2$, содержащее примитивный корень степени N из единицы ω. Покажите, что расстояние циклического кода длины N с определяющим множеством $\{\omega, \omega^2, \ldots, \omega^{\delta-1}\}$ равно по крайней мере δ. Покажите, что если $N = 2^l - 1$ и $\delta = 3$, то мы получаем $[2^l - 1, 2^l - 1 - l, 3]$-код Хэмминга.

Решение. Линейный код $\mathcal{X} \subset \mathbb{F}_q^N$ является циклическим, если вместе с каждым словом $x_1 \ldots x_N$ коду $\mathcal{X}$ принадлежит и $x_2 \ldots x_N x_1$. Биекцию между циклическими кодами и делителями многочлена $X^N - 1$ можно установить, как в следствии 3.3.3.

В случае двоичного кода с $N = 2^l - 1$ конечное расширение K — это $\mathbb{F}_{2^N}$. Для краткости рассмотрим случай $N = 7$. Выпишем разложение в $\mathbb{F}_2^7$:

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1) := (X - 1)f_1(X)f_2(X).$$

Пусть ω — корень многочлена $f_1(X)$. Так как $f_1(X)^2 = f_1(X^2)$ в кольце $\mathbb{F}_2[X]$, мы имеем

$$f_1(\omega) = f_1(\omega^2) = 0.$$

Отсюда следует, что циклический код $\mathcal{X}$ с определяющим корнем ω имеет порождающий многочлен $f_1(X)$ и проверочный многочлен $(X - 1)f_2(X) = = X^4 + X^2 + X + 1$. Это свойство характеризует код Хэмминга с точностью до эквивалентности. Случай, когда ω — корень многочлена $f_2(X)$, разбирается аналогично (мы просто обращаем каждое кодовое слово). В общей ситуации $N = 2^l - 1$ возьмём примитивный элемент $\omega \in \mathbb{F}_{2^l}$ и его минимальный многочлен $M_\omega(X)$. Корни этого многочлена — это $\omega, \omega^2, \ldots, \omega^{2^{l-1}}$, значит, $\deg M_\omega(X) = l$. Таким образом, ранг кода с определяющим нулём ω равен $N - l = 2^l - 1 - l$, и это $[2^l - 1, 2^l - l - 1]$-код Хэмминга. □

Задача 3.6.21. Сравните процедуры декодирования кода Хэмминга и БЧХ-кода, исправляющего 2 ошибки.

Решение. Чтобы объяснить идею, лежащую в основе конструкции БЧХ-кода, вернёмся сначала к кодам Хэмминга. Напомним, что

$[2^l - 1, 2^l - 1 - l]$-код Хэмминга — это совершенный код длины $N = 2^l - 1$, исправляющий одну ошибку. Процедура его декодирования заключается в следующем. По слову $\mathbf{y} = y_1 \dots y_N$, $N = 2^l - 1$, строим синдром $\mathbf{s} = \mathbf{y}H^{\mathrm{T}}$. Если $\mathbf{s} = 0$, декодируем $\mathbf{y}$ как $\mathbf{y}$. Если $\mathbf{s} \neq 0$, то $\mathbf{s}$ — один из столбцов матрицы $H = H_{\mathrm{Ham}}$. Если это столбец с номером i, декодируем $\mathbf{y}$ как $\mathbf{x}_* = \mathbf{y} + \mathbf{e}_i$, где $\mathbf{e}_i = 0 \dots 010 \dots 0$ (1 на i-м месте).

Теперь мы хотим построить код, исправляющий более одной ошибки (для начала две) с процедурой декодирования, напоминающей декодирование кода Хэмминга. Выберем $2l$ строк проверочной матрицы вида

$$\tilde{H} = \begin{pmatrix} H \\ \Pi H \end{pmatrix}, \tag{3.6.19}$$

где ΠH получается перестановкой столбцов матрицы H^{Ham} (Π — перестановка степени $2^l - 1$). Новая матрица $\tilde{H}$ содержит $2l$ линейно независимых строк и поэтому определяет $[2^l - 1, 2^l - 1 - 2l]$-линейный код. Синдромами теперь будут слова длины $2l$ (или пары слов длины l): $\mathbf{y}\tilde{H}^{\mathrm{T}} = (\mathbf{s}\mathbf{s}')$. Синдром $(\mathbf{s}\mathbf{s}')$ совпадает или не совпадает с одним из столбцов матрицы $\tilde{H}$. Предположим, что возникло две ошибки, т. е. $\mathbf{y}$ отличается от кодового слова $\mathbf{x}$ в двух знаках, скажем i и j. Тогда синдром выглядит как

$$\mathbf{y}\tilde{H}^{\mathrm{T}} = (\mathbf{s}_i + \mathbf{s}_j,\ \mathbf{s}_{\Pi i} + \mathbf{s}_{\Pi j}),$$

где $\mathbf{s}_k$ — слово, представляющее столбец k из H. Организуем нашу перестановку таким образом, чтобы по известному вектору $(\mathbf{s}_i + \mathbf{s}_j,\ \mathbf{s}_{\Pi i} + \mathbf{s}_{\Pi j})$ мы всегда смогли бы восстановить i и j. Иначе говоря, нужно уметь решать уравнения

$$\mathbf{s}_i + \mathbf{s}_j = \mathbf{z}, \qquad \mathbf{s}_{\Pi i} + \mathbf{s}_{\Pi j} = \mathbf{z}' \tag{3.6.20}$$

для любой пары $(\mathbf{z}, \mathbf{z}')$, которая может получиться в качестве синдрома в результате двух ошибок.

Естественно попробовать перестановку Π, имеющую алгебраический смысл, например $\mathbf{s}_{\Pi i} = \mathbf{s}_i\mathbf{s}_i = (\mathbf{s}_i)^2$ (плохой выбор), что или $\mathbf{s}_{\Pi i} = \mathbf{s}_i\mathbf{s}_i\mathbf{s}_i = (\mathbf{s}_i)^3$ (удачный выбор), или (в общей ситуации) $\mathbf{s}_{\Pi i} = \underbrace{\mathbf{s}_i \dots \mathbf{s}_i}_{k \text{ раз}}$. Скажем, можно попробовать умножение по модулю $1 + X^N$. К сожалению, оно не приводит к полю, поскольку многочлен $1 + X^N$ всегда *приводим*. Итак, пусть проверочная матрица имеет вид

$$\tilde{H}^{\mathrm{T}} = \begin{pmatrix} (1 \dots 00) & \dots & (1 \dots 00)^k \\ \dots\dots\dots\dots\dots & & \\ (1 \dots 11) & \dots & (1 \dots 11)^k \end{pmatrix}.$$

Тогда нам следует решать уравнения вида

$$\mathbf{s}_i + \mathbf{s}_j = \mathbf{z}, \quad \mathbf{s}_i^k + \mathbf{s}_j^k = \mathbf{z}'. \tag{3.6.21}$$

Чтобы найти решения, нам понадобится *структура поля* на пространстве Хэмминга, т. е. не только умножение, но и *деление*. Любая структура поля на пространстве Хэмминга длины N изоморфна $\mathbb{F}_2[X]/\langle g(X)\rangle$ — кольцу многочленов по модулю неприводимого многочлена $g(X)$, при этом желательно выбрать примитивный многочлен. Например, простейшая система вида (3.6.21) — это

$$\mathbf{s} + \mathbf{s}' = \mathbf{z}, \quad \mathbf{s}^3 + \mathbf{s}'^3 = \mathbf{z}';$$

она сводится к одному уравнению $\mathbf{z}\mathbf{s}^2 - \mathbf{z}^2\mathbf{s} + \mathbf{z}^3 - \mathbf{z}' = 0$ и задача сводится к разложению на множители многочлена $zX^2 - z^2X + z^3 - z'$.

Для $N = 2^l - 1$, $l = 4$ получаем [15, 7, 5]-код. Его ранг равен 7, ввиду линейной независимости столбцов матрицы $\tilde{H}$. Проверим, что этот код исправляет до двух ошибок. Предположим сначала, что мы получили слово $\mathbf{y} = y_1 \dots y_{15}$, содержащее 2 ошибки на неизвестных нам местах i и j. Чтобы найти i и j, вычисляем синдром $\mathbf{y}\tilde{H}^{\mathrm{T}} = (\mathbf{z},\ \mathbf{z}')$. Напомним, что $\mathbf{z}$ и $\mathbf{z}'$ — слова длины 4; а общая длина синдрома равна 8. Заметим, что $\mathbf{z}' \neq \mathbf{z}^3$: если $\mathbf{z}' = \mathbf{z}^3$, то ошибка только одна. Выпишем пару уравнений

$$\mathbf{s} + \mathbf{s}' = \mathbf{z}, \quad \mathbf{s}^3 + \mathbf{s}'^3 = \mathbf{z}' \tag{3.6.22}$$

где $\mathbf{s}$ и $\mathbf{s}'$ — слова длины 4 (или их многочлены, что эквивалентно), а умножение производится по модулю $1 + X + X^4$. В случае двух ошибок гарантируется, что существует ровно одно пара решений уравнений (3.6.22): один вектор, занимающий позицию i, а второй — позицию j среди верхней (Хэммингова) половины матрицы $\tilde{H}$. Более того, уравнения (3.6.22) не могут иметь более одной пары решений, поскольку из равенства

$$\mathbf{z}' = \mathbf{s}^3 + \mathbf{s}'^3 = (\mathbf{s} + \mathbf{s}')(\mathbf{s}^2 + \mathbf{s}\mathbf{s}' + \mathbf{s}'^2) = \mathbf{z}(\mathbf{z}^2 + \mathbf{s}\mathbf{s}')$$

следует, что

$$\mathbf{s}\mathbf{s}' = \mathbf{z}'\mathbf{z}^{-1} + \mathbf{z}^2. \tag{3.6.23}$$

Теперь, из соотношения (3.6.23) и первого из уравнений (3.6.22) получаем, что $\mathbf{s}$, $\mathbf{s}'$ — в точности корни квадратного уравнения

$$X^2 + \mathbf{z}X + (\mathbf{z}'\mathbf{z}^{-1} + \mathbf{z}^2) = 0 \tag{3.6.24}$$

(здесь $\mathbf{z}'\mathbf{z}^{-1} + \mathbf{z}^2 \neq 0$). Но многочлен в л. ч. уравнения (3.6.24) не может иметь более двух разных корней (у него может не быть корней или может быть один кратный корень, но эти возможности исключены предположением о наличии ровно двух ошибок). Если возникла единственная ошибка,

то $\mathbf{z}' = \mathbf{z}^3$, в этом случае $\mathbf{s} = \mathbf{z}$ — единственный корень и мы найдём слово $\mathbf{z}$ среди столбцов верхней половины матрицы $\tilde{H}$.

Подведем итог: схема декодирования приведённого выше [15, 7]-кода состоит в следующем. Получив слово $\mathbf{y}$, вычисляем синдром $\mathbf{y}\tilde{H}^{\mathrm{T}} = (\mathbf{z},\ \mathbf{z}')$. Затем

1) если $\mathbf{z} = \mathbf{z}' = \mathbf{0}$, заключаем, что ошибок нет, и декодируем $\mathbf{y}$ как $\mathbf{y}$;

2) если $\mathbf{z} \neq \mathbf{0}$ и $\mathbf{z}^3 = \mathbf{z}'$, то понимаем, что вкралась единственная ошибка, и находим её положение, выделив слово $\mathbf{z}$ среди столбцов проверочной матрицы кода Хэмминга;

3) если $\mathbf{z} \neq \mathbf{0}$ и $\mathbf{z}^3 \neq \mathbf{z}'$, то выписываем квадратный многочлен (3.6.24), и если у него есть два разных корня $\mathbf{s}$ и $\mathbf{s}'$, то делаем вывод о наличии двух ошибок и выясняем их положение, находя $\mathbf{s}$ и $\mathbf{s}'$ среди столбцов проверочной матрицы кода Хэмминга;

4) если $\mathbf{z} \neq \mathbf{0}$, $\mathbf{z}^3 \neq \mathbf{z}'$ и многочлен (3.6.24) не имеет корней или $\mathbf{z}$ — его корень, а $\mathbf{z}'$ — нет, то заключаем, что имеется по крайней мере три ошибки.

Заметим, что ситуация, когда $\mathbf{z} = \mathbf{0}$, $\mathbf{z}^3 \neq \mathbf{z}'$, а многочлен (3.6.24) имеет единственный корень, невозможна: если этот многочлен имеет корень, скажем, $\mathbf{s}$, то либо второй корень $\mathbf{s}' \neq \mathbf{s}$, либо $\mathbf{z} = \mathbf{0}$ и возникла единственная ошибка.

Процедура декодирования в некоторых случаях позволяет выявить, что возникло более трёх ошибок, однако не дает метода их исправить.

Глава 4

Дальнейшие темы из теории информации

We must bring the magic of averages to the rescue of millions.

Мы должны использовать магию средних для спасения миллионов.

Дэвид Ллойд Джордж (1863–1945),
британский политик
(об использовании социального страхования)

В гл. 4 будет удобно работать в общей ситуации, охватывающей как дискретный, так и непрерывный типы распределений вероятностей. А именно, предположим, что рассматриваемые распределения вероятностей задаются их производными по заданным опорным мерам, обозначаемыми, как правило, μ или ν. Роль опорной меры может играть счётная мера с носителем на дискретном множестве или мера Лебега на $\mathbb{R}^d$; нам нужно только, чтобы опорная мера была локально конечной (т. е. компактные множества должны иметь конечную меру). Производные Радона—Никодима будут называться функциями вероятности (ф. в.): они представляют вероятности в дискретном случае и плотности распределения (п. р.) в непрерывном.

Теория пропускной способности канала, развитая для дискретных каналов в гл. 1 (см. § 1.4), подходит практически без изменений для непрерывно распределённого шума, если её адаптировать под изложенную выше схему:

множество $\mathcal{U}$ сообщений мощности $M = \lceil 2^{NR} \rceil \to$

$\to$ кодовая книга $\mathcal{X}$ размера M с кодовыми словами длины $N \to$

$\to$ скорость надёжной передачи по зашумлённому каналу $\to$

$\to$ пропускная способность канала.

Однако для упрощения изложения с этого момента будем предполагать, что кодирование $\mathcal{U} \to \mathcal{X}$ инъективно, и отождествлять код с его кодовой книгой.

§ 4.1. Гауссовский канал и его обобщения

Здесь мы изучаем каналы с непрерывно распределённым шумом; они представляют собой основные модели дистанционной передачи данных, включая как радиосвязь, так и телефонную передачу. Наиболее известной моделью такого канала служит аддитивный гауссовский канал без памяти (а. г. к. б. п.), но полезны также и другие модели непрерывного шума. Случай а. г. к. б. п. особенно заманчив, поскольку позволяет делать простые и наглядные расчёты и получать элегантные ответы.

Однако гауссовские (и другие непрерывно распределённые) каналы представляют собой сложную проблему, которая не возникала в случае конечного алфавита, рассмотренного в гл. 1. А именно, ввиду того, что кодовые слова (точнее, кодовые векторы) могут *априори* принимать значения в евклидовом пространство (как и вектор шума), определение пропускной способности канала нужно изменить, вводя ограничение по мощности. Более общим образом, значение пропускной способности канала будет зависеть от так называемых *региональных ограничений*, которые могут приводить к аналитическим трудностям. В случае а. г. к. способ был указан Шенноном, но потребовалось несколько лет, чтобы сделать его анализ строгим.

Powerless Codes in Pointless Space

(Из серии «Фильмы, которые не вышли на большой экран».)

Входное слово длины N (предполагается, что по каналу передается N последовательных временны́х отсчетов) отождествляется с входным N-вектором $\mathbf{x}(=\mathbf{x}^{(N)}) = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$. Мы предполагаем, что $x_i \in \mathbb{R}$ и поэтому $\mathbf{x}^{(N)} \in \mathbb{R}^N$ (для краткости обозначений верхний индекс (N) будет опускаться).

В аддитивном канале входной вектор $\mathbf{x}$ трансформируется в случайный вектор $\mathbf{Y}^{(N)} = \begin{pmatrix} Y_1 \\ \vdots \\ Y_N \end{pmatrix}$, где $\mathbf{Y} = \mathbf{x} + \mathbf{Z}$, или, покомпонентно,

$$Y_j = x_j + Z_j, \quad 1 \leqslant j \leqslant N. \tag{4.1.1}$$

Здесь и далее $\mathbf{Z} = \begin{pmatrix} Z_1 \\ \vdots \\ Z_N \end{pmatrix}$ — вектор шума, составленный из с. в. $Z_1, \ldots, Z_N$. Таким образом, шум можно охарактеризовать совместной п. р. $f^{\text{по}}(\mathbf{z}) \geqslant 0$,

где $\mathbf{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_N \end{pmatrix}$ и $\int f^{\text{по}}(\mathbf{z}) dz_1 \dots dz_N = 1$. Распределение вероятностей N-мерного шума задается интегрированием по соответствующим множествам значений $\mathbf{Z}$:

$$\mathbf{P}^{\text{по}}(\mathbf{Z} \in A) = \int\limits_A f^{\text{по}}(\mathbf{z}) dz_1 \dots dz_N, \quad A \subset \mathbb{R}^N.$$

Пример 4.1.1. Аддитивный канал называется *гауссовским* (а. г. к.), если для каждого N вектор шума $\begin{pmatrix} Z_1 \\ \vdots \\ Z_N \end{pmatrix}$ распределён по нормальному многомерному закону (см. том 1, с. 114). С этого момента мы считаем, что $\mathsf{E} Z_j = 0$. Напомним, что многомерное нормальное распределение с нулевым средним полностью определяется матрицей ковариации. Более точно, совместная п. р. $f^{\text{по}}_{\mathbf{Z}^{(N)}}(\mathbf{z}^{(N)})$ для а. г. к. имеет вид

$$\frac{1}{(2\pi)^{N/2} (\det \Sigma)^{1/2}} \exp\left(-\frac{1}{2} \mathbf{z}^{\mathrm{T}} \Sigma^{-1} \mathbf{z} \right), \quad \mathbf{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_N \end{pmatrix} \in \mathbb{R}^N. \tag{4.1.2}$$

Здесь Σ — вещественная симметричная строго положительно определённая $(N \times N)$-матрица с элементами $\Sigma_{ij} = \mathsf{E}(Z_i Z_j)$, представляющими ковариацию шумовых с. в. Z_i и Z_j, $1 \leqslant i, j \leqslant N$. (Вещественная строгая положительная определённость означает, что $\Sigma = BB^{\mathrm{T}}$, где B — вещественная обратимая матрица размера $N \times N$; вещественная строго положительно определённая матрица Σ имеет N попарно ортогональных собственных векторов, а все её N собственных значений положительны.) В частности, каждая с. в. Z_j распределена по нормальному закону: $Z_j \sim \mathrm{N}(0, \sigma_j^2)$, где $\sigma_j^2 = \mathsf{E} Z_j^2$ совпадает с диагональными элементами Σ_{jj}. (Благодаря строгой положительной определённости имеем, что $\Sigma_{jj} > 0 \ \forall j = 1, \dots, N$.)

Если, кроме того, с. в. $Z_1, \dots, Z_N$ — н. о. р., говорят о гауссовском канале без памяти (г. к. б. п.) или называют его каналом с (аддитивным) гауссовским *белым* шумом В этом случае матрица Σ диагональная: $\Sigma_{ij} = 0$ при $i \neq j$ и $\Sigma_{ii} > 0$. Это наиболее важный пример (как с обучающей, так и с практической точек зрения), так как он допускает красивые окончательные формулы и служит основой для дальнейших обобщений.

Таким образом, г. к. б. п. имеет н. о. р. шумовые с. в. $Z_i \sim \mathrm{N}(0, \sigma_i^2)$, где $\sigma_i^2 = \mathrm{Var}[Z_i] = \mathsf{E} Z_i^2$. Для нормальных с. в. независимость равносильна некоррелированности, т. е. из условия $\mathsf{E}(Z_i Z_j) = 0 \ \forall i, j = 1, \dots, N$ при $i \neq j$ следует взаимная независимость компонент $Z_1, \dots, Z_N$ вектора $\mathbf{Z}^{(N)}$. Это видно из формулы (4.1.2): если в матрице Σ элементы $\Sigma_{ij} = 0$ при $i \neq j$, то

она диагональна, $\det\Sigma = \prod_{j=1}^{N}\Sigma_{jj}$ и совместная п. р. в формуле (4.1.2) распадается в произведение N множителей, представляющих индивидуальные п. р. компонент Z_j, $1 \leqslant j \leqslant N$:

$$\prod_{j=1}^{N}\frac{1}{(2\pi\Sigma_{jj})^{1/2}}\exp\Big(-\frac{z_j^2}{2\Sigma_{jj}}\Big). \tag{4.1.3}$$

Более того, если предполагать независимость и одинаковую распределённость обозначить $\Sigma_{jj} = \sigma^2 > 0$, то все с. в. $Z_j \sim \mathrm{N}(0, \sigma^2)$ и распределение шума для г. к. б. п. полностью определяется единственным параметром $\sigma > 0$. Более точно, совместная п. р. из формулы (4.1.3) переписывается как

$$\Big(\frac{1}{\sqrt{2\pi}\,\sigma}\Big)^N\exp\Big(-\frac{1}{2\sigma^2}\sum_{j=1}^{N}z_j^2\Big). \qquad \square$$

Гаусс, как правило, не наделал бы такого шума.

(Из серии «Так говорил суперлектор».)

Зачастую полезно представлять себе бесконечную случайную последовательность $\mathbf{Z}_1^\infty = \{Z_1, Z_2, \ldots\}$, а описанный выше вектор шума $\mathbf{Z}^{(N)}$ образован первыми N членами этой последовательности. В гауссовском случае $\mathbf{Z}_1^\infty$ называется случайным гауссовским процессом; при $\mathsf{E}Z_j \equiv 0$ этот процесс определяется, как и раньше, ковариацией Σ, где $\Sigma_{ij} = \mathrm{Cov}(Z_i, Z_j) = \mathsf{E}(ZiZj)$. Термин «белый гауссовский шум» отличает данную модель от более общей модели канала с «цветным» шумом (см. ниже). $\square$

Каналы с непрерывно распределённым шумом анализируются с помощью схемы, аналогичной той, которая использовалась в дискретном случае: в частности, если по каналу передаётся одно из $M \sim 2^{RN}$, $R < 1$ кодированных сообщений, нам нужна кодовая книга, состоящая из M кодовых слов длины N: $\mathbf{x}(i)^T = (x_1(i), \ldots, x_N(i))$, $1 \leqslant i \leqslant M$:

$$\mathcal{X}_{M,N} = \big\{\mathbf{x}^{(N)}(1), \ldots, \mathbf{x}^{(N)}(M)\big\} = \left\{\begin{pmatrix}x_1(1)\\ \vdots \\ x_N(1)\end{pmatrix}, \ldots, \begin{pmatrix}x_1(M)\\ \vdots \\ x_N(M)\end{pmatrix}\right\}. \tag{4.1.4}$$

Предполагается, естественно, что кодовая книга известна как получателю, так и отправителю. Скорость передачи R определяется по формуле

$$R = \frac{\log_2 M}{N}. \tag{4.1.5}$$

Предположим теперь, что было послано кодовое слово $\mathbf{x}(i)$. Тогда полученный случайный вектор $\mathbf{Y}(=\mathbf{Y}(i)) = \begin{pmatrix} x_1(i)+Z_1 \\ \vdots \\ x_N(i)+Z_N \end{pmatrix}$ декодируется при помощи избранного декодера $d\colon \mathbf{Y} \mapsto d(\mathbf{Y}) \in \mathcal{X}_{M,N}$. С геометрической точки зрения декодер ищет ближайшее кодовое слово $\mathbf{x}(k)$ относительно подходящего расстояния (адаптированного под декодер); если, например, мы остановились на евклидовом расстоянии, то $\mathbf{Y}$ декодируется кодовым словом, минимизирующим сумму квадратов

$$d(\mathbf{Y}) = \arg\min \left\{ \sum_{j=1}^{N} (Y_j(i) - x_j(l))^2 \colon \mathbf{x}(l) \in \mathcal{X}_{M,N} \right\}, \tag{4.1.6}$$

когда $d(\mathbf{Y}) \neq \mathbf{x}(i)$, возникает ошибка. К счастью, выбор декодера удобно делать на основе принципа максимального правдоподобия (м. п.), см. ниже.

Здесь есть ещё одна тонкость: предполагается, что успешное декодирование входного слова $\mathbf{x}$ возможно только при условии, что оно принадлежит некоторой «доступной для передачи» области в $\mathbb{R}^N$. Например, работая с а. г. к. б. п., налагают следующее ограничение по мощности:

$$\frac{1}{N}\sum_{j=1}^{N} x_j^2 \leqslant \alpha, \tag{4.1.7}$$

где $\alpha > 0$ — заданная константа. В контексте передачи по каналу без памяти это означает, что средняя амплитуда квадратов на входной сигнал длины N не превосходит α, иначе результат передачи считается «не декодируемым». С геометрической точки зрения, чтобы входное слово $\mathbf{x}(i)$ можно было декодировать, оно должно лежать внутри евклидова шара $\mathbb{B}_{l_2}^{(N)}(\sqrt{\alpha N})$ радиуса $r = \sqrt{\alpha N}$ с центром в точке $\mathbf{0} \in \mathbb{R}^N$:

$$\mathbb{B}_{l_2}^{(N)} = \left\{ \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} : \left(\sum_{j=1}^{N} x_j^2 \right)^{1/2} \leqslant r \right\}.$$

Индекс l_2 указывает, что $\mathbb{R}^N$ со стандартным евклидовым расстоянием рассматривается как гильбертово l_2-пространство.

На самом деле нет нужды, чтобы вся кодовая книга $\mathcal{X}_{M,N}$ лежала в декодируемой области; важно лишь, что если кодовое слово не попадает в эту область, то оно декодируется неверно с вероятностью 1. Можно считать, что «большинство» кодовых слов попадает внутрь шара $\mathbb{B}_{l_2}^{(N)}(\sqrt{N\alpha})$, но не обязательно все из них (см. рис. 4.1).

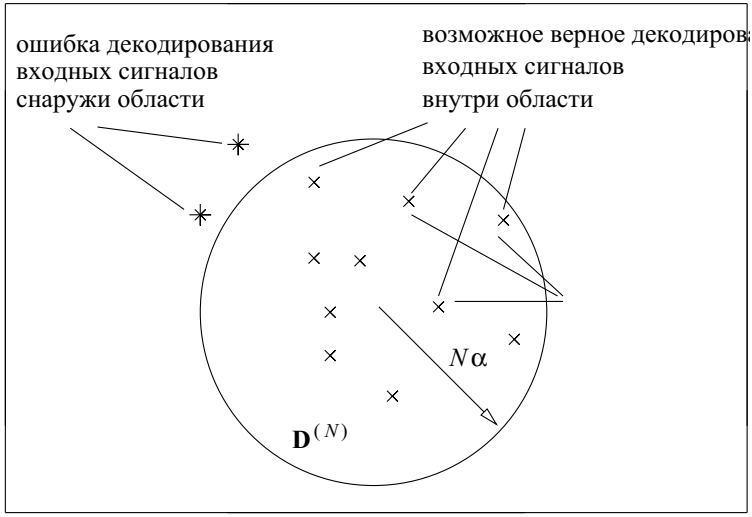


Рис. 4.1

Причина введения области ограничений (4.1.7) заключается в том, что без него кодовые слова могут располагаться в пространстве на сколь угодно большом расстоянии друг от друга и, в конечном счёте, любая скорость передачи становится надёжной. (Это означало бы бесконечную пропускную способность и хотя такие каналы не следует сразу отвергать, в контексте а. г. к. случай бесконечной пропускной способности кажется нереальным.)

Обычно декодируемая область $\mathbb{D}^{(N)} \subset \mathbb{R}^N$ представляется шаром в $\mathbb{R}^N$ с центром в начале координат по отношению к некоторому расстоянию в $\mathbb{R}^N$. Скажем, в случае экспоненциально распределённого шума естественно выбрать

$$\mathbb{D}^{(N)} = \mathbb{B}^{(N)}_{l_1}(N\alpha) = \left\{ \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} : \sum_{j=1}^{N} |x_j| \leqslant N\alpha \right\}$$

— шар в l_1-норме. Когда вектор выходного сигнала попадает внутрь сферы радиуса r с центром в кодовом слове, он декодируется этим словом. У нас получается правильное декодирование, если 1) выходной сигнал попадает внутрь только одной сферы вокруг кодового слова, 2) это кодовое слово лежит внутри $\mathbb{D}^{(N)}$ и 3) это конкретное слово было послано. Если в сферу попадает больше одного слова, то возможны ошибки.

Как и в дискретном случае, более общий канал задается семейством распределений (условных) вероятностей получаемых векторов длины N при условии, что послано слово $\mathbf{x}^{(N)} \in \mathbb{R}^N$

$$\mathbf{P}^{(N)}_{\mathrm{ch}}(\cdot\,|\mathbf{x}^{(N)}) = \mathbf{P}^{(N)}_{\mathrm{ch}}(\cdot\,|\text{послано слово } \mathbf{x}^{(N)}), \quad \mathbf{x} \in \mathbb{R}^N. \tag{4.1.8}$$

Как и ранее, $N = 1, 2, \ldots$ означает количество временных отсчетов, используемых в канале для передачи, и мы будем рассматривать предел при $N \to \infty$. Предположим теперь, что распределение $\mathbf{P}^{(N)}_{\mathrm{ch}}(\cdot\,|\mathbf{x}^{(N)})$ определяется ф. в. $f^{(N)}_{\mathrm{ch}}(\mathbf{y}^{(N)}|\mathbf{x}^{(N)})$ относительно фиксированной меры $\nu^{(N)}$ на $\mathbb{R}^{(N)}$:

$$\mathbf{P}^{(N)}_{\mathrm{ch}}(\mathbf{Y}^{(N)} \in \mathbb{A}|\mathbf{x}^{(N)}) = \int\limits_{\mathbb{A}} f^{(N)}_{\mathrm{ch}}(\cdot\,|\mathbf{x}^{(N)}) d\nu^{(N)}(\mathbf{y}^{(N)}). \tag{4.1.9а}$$

Обычно считают, что $\nu^{(N)}$ — это произведение мер вида

$$\nu^{(N)} = \underbrace{\nu \times \ldots \times \nu}_{N}, \tag{4.1.9б}$$

Например, $\nu^{(N)}$ может быть мерой Лебега на $\mathbb{R}^N$, которая равна произведению мер на $\mathbb{R}$: $d\mathbf{x}^{(N)} = dx_1 \times \ldots \times dx_N$. В дискретном случае, когда знаки x_i представляют буквы из входного алфавита канала $\mathcal{A}$ (скажем, двоичного с $\mathcal{A} = \{0, 1\}$), ν — считающая мера на $\mathcal{A}$, сопоставляющая вес 1 каждому символу алфавита. Тогда $\nu^{(N)}$ — считающая мера на множестве $\mathcal{A}^{(N)}$ всех входных слов длины N, сопоставляющая вес 1 каждому такому слову.

Предполагая, что опорная мера $\nu^{(N)}$ представлена в виде произведения (4.1.9б), мы конкретизируем канал без памяти, взяв ф. в. $f^{(N)}_{\mathrm{ch}}(\mathbf{y}^{(N)}|\mathbf{x}^{(N)})$ в виде произведения

$$f^{(N)}_{\mathrm{ch}}(\mathbf{y}^{(N)}|\mathbf{x}^{(N)}) = \prod_{j=1}^{N} f_{\mathrm{ch}}(y_j|x_j). \tag{4.1.10}$$

Здесь $f_{\mathrm{ch}}(y|x)$ — ф. в. канала символ на символ, описывающая воздействие шума при однократном использовании канала. В случае г. к. б. п. $f_{\mathrm{ch}}(y|x)$ — нормальное распределение $\mathrm{N}(x, \sigma^2)$. Иначе говоря, $f_{\mathrm{ch}}(y|x)$ даёт п. р. с. в. $Y = x + Z$, где $Z \sim \mathrm{N}(0, \sigma^2)$ представляет «белый шум», воздействующий на индивидуальное входное значение x.

Вернёмся к кодовой книге $\mathcal{X}_{M,N}$ — образу вложения $\mathcal{M} \to \mathbb{R}^N$, где $\mathcal{M}$ — конечный набор сообщений (записанных изначально в алфавите источника) (см. (4.1.4)). Как и в дискретном случае, декодер м. п. d_{ML} декодирует полученное слово $\mathbf{y} = \mathbf{y}^{(N)}$, максимизируя $f^{(N)}_{\mathrm{ch}}(\mathbf{y}|\mathbf{x})$ по аргументу $\mathbf{x} = \mathbf{x}^{(N)} \in \mathcal{X}_{M,N}$:

$$d_{\mathrm{ML}}(\mathbf{y}) = \arg\max \left\{ f^{(N)}_{\mathrm{ch}}(\mathbf{y}|\mathbf{x}) \colon \mathbf{x} \in \mathcal{X}_{M,N} \right\}. \tag{4.1.11}$$

Случай, когда максимум не один, трактуется как ошибочный.

Другой полезный пример — это декодер совместной типичности (с. т.) $d_{\mathrm{JT}} = d_{\mathrm{JT}}^{(N),\varepsilon}$ (см. ниже); он ищет такое кодовое слово $\mathbf{x}$, что $\mathbf{x}$ и $\mathbf{y}$ попадают в ε-типичное множество T_ε^N:

$$d_{\mathrm{JT}}(\mathbf{y}) = \mathbf{x}, \text{ если } \mathbf{x} \in \mathcal{X}_{M,N} \text{ и } (\mathbf{x}, \mathbf{y}) \in T_\varepsilon^N. \tag{4.1.12}$$

Декодер с. т. проектируется — через множества T_ε^N специального вида — для кодов, генерируемых как выборки *случайного* кода $\mathcal{X}_{M,N}$. Следовательно, для данного выходного вектора $\mathbf{y}^{(N)}$ и кода $\mathcal{X}_{M,N}$ декодирующее слово $d_{\mathrm{JT}}(\mathbf{y}) \in \mathcal{X}_{M,N}$ может быть не однозначно определено (или не определено вовсе), что тоже ведёт к ошибке. Общий декодер нужно представлять себе как инъективное отображение, заданное на множестве $\mathbb{K}^{(N)} \subseteq \mathbb{R}^N$, переводящее точку $\mathbf{y}^{(N)} \in \mathbb{K}^{(N)}$ в точку $\mathbf{x} \in \mathcal{X}_{M,N}$; вне множества $\mathbb{K}^{(N)}$ оно может быть не определено корректно. Декодируемая область $\mathbb{K}^{(N)}$ — это часть спецификаций декодера $d^{(N)}$. В любом случае нам хотелось бы достичь, чтобы декодер удовлетворял условию

$$\mathbf{P}_{\mathrm{ch}}^{(N)}(d^{(N)}(\mathbf{Y}) \neq \mathbf{x} | \mathbf{x} \text{ послано }) = \mathbf{P}_{\mathrm{ch}}^{(N)}(\mathbf{Y} \notin \mathbb{K}^{(N)} | \mathbf{x} \text{ послано }) + \\ + \mathbf{P}_{\mathrm{ch}}^{(N)}(\mathbf{Y} \in \mathbb{K}^{(N)},\ d^{(N)}(\mathbf{Y}) \neq \mathbf{x} | \mathbf{x} \text{ послано }) \to 0$$

при $N \to \infty$. В случае г. к. б. п. для любого кода $\mathcal{X}_{M,N}$ декодер м. п. из формулы (4.1.6) определяется однозначно почти всюду на $\mathbb{R}^N$ (но не обязательно даёт верный ответ).

Мы также требуем, чтобы входной вектор удовлетворял условию $\mathbf{x}^{(N)} \in \mathbb{D}^{(N)} \subset \mathbb{R}^N$, и когда $\mathbf{x}^{(N)} \notin \mathbb{D}^{(N)}$, результат передачи объявляется не декодируемым (невзирая на качество применяемого декодера). Тогда средняя вероятность ошибки при использовании кодовой книги $\mathcal{X}_{M,N}$ и декодера $d^{(N)}$ определяется по формуле

$$e^{\mathrm{av}}(\mathcal{X}_{M,N},\ d^{(N)},\ \mathbb{D}^{(N)}) = \frac{1}{N} \sum_{\mathbf{x} \in \mathcal{X}_{M,N}} e(\mathbf{x},\ d^{(N)},\ \mathbb{D}^{(N)}), \tag{4.1.13а}$$

а максимальная вероятность ошибки — по формуле

$$e^{\max}(\mathcal{X}_{M,N},\ d^{(N)},\ \mathbb{D}^{(N)}) = \max\{e(\mathbf{x},\ d^{(N)},\ \mathbb{D}^{(N)}) : \mathbf{x} \in \mathcal{X}_{M,N}\}. \tag{4.1.13б}$$

Здесь $e(\mathbf{x},\ d^{(N)},\ \mathbb{D}^{(N)})$ — вероятность ошибки, когда было послано слово $\mathbf{x}$:

$$e(\mathbf{x},\ d^{(N)},\ \mathbb{D}^{(N)}) = \begin{cases} 1, & \mathbf{x} \notin \mathbb{D}^{(N)}, \\ \mathbf{P}_{\mathrm{ch}}^{(N)}(d^{(N)}(\mathbf{Y}) \neq \mathbf{x} | \mathbf{x}), & \mathbf{x} \in \mathbb{D}^{(N)}. \end{cases} \tag{4.1.14}$$

В формуле (4.1.14) порядок кодовых слов в кодовой книге $\mathcal{X}_{M,N}$ не имеет значения; поэтому $\mathcal{X}_{M,N}$ можно рассматривать просто как M-точечное множество в евклидовом пространстве $\mathbb{R}^N$.

Геометрически мы хотим, чтобы точки $\mathcal{X}_{M,N}$ были расположены так, чтобы максимально повысить вероятность правильного м. п. -декодирования, и лежали, как правило, в области $\mathbb{D}^{(N)}$ (что опять-таки приводит к задаче плотной упаковки сфер).

Итак, предположим, что зафиксировано число $R > 0$, тогда размер кодовой книги $\mathcal{X}_{M,N}$ составляет $M = \lceil 2^{NR} \rceil$. Ниже мы определим скорость надёжной передачи при $N \to \infty$ по аналогии с тем, как это было сделано в § 1.4.

Определение 4.1.2. Число $R > 0$ называется *скоростью надёжной передачи* с областью доступной передачи $\mathbb{D}^{(N)}$, если при $M = \lceil 2^{NR} \rceil$ существует такая последовательность $\{\mathcal{X}_{M,N}\}$ кодовых книг $\mathcal{X}_{M,N} \subset \mathbb{R}^N$ и такая последовательность $\{d^{(N)}\}$ декодеров $d^{(N)} \colon \mathbb{R}^N \to \mathbb{R}^N$, что

$$\lim_{N\to\infty} e^{\mathrm{av}}(\mathcal{X}_{M,N},\, d^{(N)},\, \mathbb{D}^{(N)}) = 0. \tag{4.1.15}$$

□

Замечание 4.1.3. Легко проверить, что скорость надёжной передачи R в смысле средней вероятности ошибки $e^{\mathrm{av}}(\mathcal{X}_{M,N},\, d^{(N)},\, \mathbb{D}^{(N)})$ является таковой и для максимальной вероятности ошибки $e^{\max}(\mathcal{X}_{M,N},\, d^{(N)},\, \mathbb{D}^{(N)})$. В самом деле, предположим, что R — надёжная скорость в смысле определения 4.1.2, т. е. в смысле средней вероятности ошибки. Возьмём последовательность $\{\mathcal{X}_{M,N}\}$ соответствующей кодовой книги с $M = \lceil 2^{RN} \rceil$ и последовательность соответствующих декодеров $\{d^{(N)}\}$. Разделим каждый код $\mathcal{X}_N$ на две половины $\mathcal{X}_N^{(0)}$ и $\mathcal{X}_N^{(1)}$ кодовых слов, упорядоченных в неубывающем порядке по вероятностям их ошибочного декодирования, где первые $M^{(0)} = \lceil M/2 \rceil$ кодовых слова лежат в множестве $\mathcal{X}_N^{(0)}$, а остальные $M^{(1)} = M \setminus M^{(0)}$ слов — в $\mathcal{X}_N^{(0)}$. Тогда для последовательности кодов $\{\mathcal{X}_{M,N}^{(0)}\}$

а) скорость передачи информации приближается к R при $N \to \infty$, так как

$$\frac{1}{N} \log M^{(0)} \geqslant R + O(N^{-1});$$

б) максимальная вероятность ошибки при использовании декодера d_N имеет вид

$$P_{\mathrm{e}}^{\max}(\mathcal{X}_N^{(0)},\, d_N) \leqslant \frac{1}{M^{(1)}} \sum_{\mathbf{x}^{(N)} \in \mathcal{X}_N^{(1)}} P_{\mathrm{e}}(\mathbf{x}^{(N)},\, d_N) \leqslant \frac{M}{M^{(1)}} P_{\mathrm{e}}^{\mathrm{av}}(\mathcal{X}_N,\, d_N).$$

Поскольку $M/M^{(1)} \leqslant 2$, п. ч. стремится к 0 при $N \to \infty$. Мы заключаем, что R — скорость надёжной передачи для максимальной вероятности ошибки. Обратное утверждение о том, что скорость надёжной передачи R в смысле

максимальной вероятности ошибки остаётся таковой и в смысле средней вероятности ошибки, очевидно. □

Пропускная способность канала определяется как супремум скоростей надёжной передачи:

$$C = \sup\{R > 0\colon R \text{ — скорость надёжной передачи}\}; \tag{4.1.16}$$

она зависит от канала и формы области ограничения.

Оказывается (см. теорему 4.1.9 ниже), для г. к. б. п. со средним ограничением по мощности α (см. формулу (4.1.7)), пропускная способность канала $C(\alpha, \sigma^2)$ задаётся следующим красивым выражением

$$C(\alpha, \sigma^2) = \frac{1}{2}\log_2\left(1 + \frac{\alpha}{\sigma^2}\right). \tag{4.1.17}$$

Более того, как и в § 1.4 пропускная способность $C(\alpha, \sigma^2)$ реализуется последовательностью случайных кодирований, где компоненты кодового слова $\mathbf{x}(i) = (X_1(i), \ldots, X_N(i))$ — н. о. р. с. в. $X_j(i) \sim \mathrm{N}(0, \alpha - \varepsilon_N)$, $j = 1, \ldots, N$, $i = 1, \ldots, M$, а $\lim\limits_{N\to\infty} \varepsilon_N = 0$. Хотя такие случайные кодирования формально не подчиняются ограничению (4.1.7) при конечном N, оно нарушается с исчезающе малой вероятностью при $N \to \infty$ (так как

$$\limsup_{N\to\infty} \mathsf{P}\left(\max\left\{\frac{1}{N}\sum_{j=1}^{N} X_j(i)^2\colon 1 \leqslant i \leqslant M\right\} \leqslant \alpha\right) = 1$$

при подходящем выборе ε_N). Следовательно, средняя вероятность ошибки (4.1.13а) стремится к нулю (конечно, при случайном кодировании и вероятность ошибки случайна).

Пример 4.1.4. Теперь обсудим а. г. к. с *«цветным» гауссовским шумом*. Пусть кодовое слово $\mathbf{x} = (x_1, \ldots, x_N)^{\mathrm{T}}$ имеет многомерные компоненты $x_j = \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_k} \end{pmatrix} \in \mathbb{R}^k$, $1 \leqslant j \leqslant N$, причём компоненты Z_j вектора шума $\mathbf{Z} = \begin{pmatrix} Z_1 \\ \vdots \\ Z_N \end{pmatrix}$ — случайные k-мерные векторы $Z_j = \begin{pmatrix} Z_{j_1} \\ \vdots \\ Z_{j_k} \end{pmatrix}$. Например, $Z_1, \ldots, Z_N$ могут быть н. о. р. с. в. $\mathrm{N}(0, \Sigma)$ (k-мерные нормальные с. в.), где Σ — данная $(k \times k)$-матрица ковариаций.

Модель «цветного» шума возникает при параллельном использовании k скалярных гауссовских каналов. Здесь скалярный сигнал x_{j1} посылается по каналу 1, x_{j2} — по каналу 2 и т. д. Разумно предполагать, что каждый скалярный гауссовский канал вносит свой гауссовский шум; разные каналы могут быть независимыми (с диагональной $k \times k$-матрицей Σ) или

зависимыми (с общей положительно определённой матрицей Σ размера $k \times k$).

При этом кодовая книга, как и раньше, состоит из (упорядоченного или нет) набора кодовых слов $\mathcal{X}_{M,N} = \{\mathbf{x}(1), \ldots, \mathbf{x}(M)\}$, где каждое кодовое слово $\mathbf{x}(i)$ — «мультивектор» $(x_1(i), \ldots, x_N(i))^{\mathrm{T}} \in \mathbb{R}^{k\times N} := \mathbb{R}^k \times \ldots \times \mathbb{R}^k$. Пусть Q — положительно определённая $k \times k$-матрица, коммутирующая с Σ: $Q\Sigma = \Sigma Q$. Тогда ограничение по мощности принимает вид

$$\frac{1}{N}\sum_{j=1}^{N}\langle x_j,\, Qx_j\rangle \leqslant \alpha. \tag{4.1.18}$$

□

Не удивительно, что формула пропускной способности а. г. к. с «цветным» шумом оказывается более сложной. Поскольку $\Sigma Q = Q\Sigma$, матрицы Σ и Q могут быть одновременно диагонализируемыми. Пусть λ_i и γ_i $(i = 1, \ldots, k)$ — собственные значения матриц Σ и Q соответственно (отвечающие одинаковым собственным векторам). Тогда

$$C(\alpha,\, Q,\, \Sigma) = \frac{1}{2}\sum_{l=1}^{k}\log_2\left(1 + \frac{(\nu\gamma_l^{-1} - \lambda_l)_+}{\lambda_l}\right), \tag{4.1.19}$$

где $(\nu\gamma_l^{-1} - \lambda_l)_+ = \max\{\nu\gamma_l^{-1} - \lambda_l,\, 0\}$. Иначе говоря, $(\nu\gamma_l^{-1} - \lambda_l)_+$ — собственные числа матрицы $(\nu Q^{-1} - \Sigma)_+$, представляющей собой положительно определённую часть эрмитовой матрицы $\nu Q^{-1} - \Sigma$. Далее $\nu = \nu(\alpha) > 0$ определяется из условия

$$\mathrm{trace}[(\nu\mathbf{1} - Q\Sigma)_+] = \alpha. \tag{4.1.20}$$

Положительно-определённая часть $(\nu\mathbf{1} - Q\Sigma)_+$, в свою очередь, определяется как

$$(\nu\mathbf{1} - Q\Sigma)_+ = \Pi_+(\nu\mathbf{1} - Q\Sigma)\Pi_+,$$

где Π_+ — ортогональная проекция (в $\mathbb{R}^k$) на подпространство, натянутое на собственные векторы матрицы $Q\Sigma$ с собственными значениями $\gamma_l\lambda_l < \nu$. В формуле (4.1.20) имеем $\mathrm{trace}[(\nu\mathbf{1} - Q\Sigma)_+] \geqslant 0$ (так как $\mathrm{trace}[AB] > 0$ для любой пары положительно определённых матриц), причём равенство достигается при $\nu = 0$ (поскольку $(-Q\Sigma)_+ = \mathbf{0}$) и $\mathrm{trace}[(\nu\mathbf{1} - Q\Sigma)_+]$ монотонно возрастает до $+\infty$ по ν. Следовательно, по любому $\alpha > 0$ формула (4.1.20) однозначно определяет значение $\nu = \nu(\alpha)$.

Хотя формула (4.1.19) выглядит гораздо более сложно, чем (4.1.17), оба выражения являются следствием двух фактов: а) пропускную способность можно определить как максимум взаимной энтропия между (случайными) входным и выходным сигналами, так же как в дискретном случае, см. § 1.3 и 1.4, и б) взаимная информация в случае гауссовского шума (белого или

«цветного») достигается, когда входной сигнал сам является гауссовским, причём матрица ковариаций решает вспомогательную задачу оптимизации. В случае уравнения (4.1.17) эта задача оптимизации довольно проста, в то время как в формуле (4.1.19) она более сложная (но по-прежнему имеет прозрачный смысл).

Соответственно случайное кодирование, на котором достигается пропускная способность $C(\alpha; Q; \Sigma)$, таково, что сигналы $X_j(i)$, $1 \leqslant j \leqslant N$, $i = 1, \ldots, M$, независимы и одинаково распределены, и $X_j(i) \sim \mathrm{N}(0, A - \varepsilon_N \mathbf{1})$, где A — положительно определённая $k \times k$-матрица, максимизирующая определитель $\det(A + \Sigma)$ при условии постоянного следа $\mathrm{trace}[QA] = \alpha$; такая матрица имеет вид $(\nu Q^{-1} - \Sigma)_+$. Случайное кодирование предоставляет удобный инструмент для расчёта пропускной способности в разных моделях. Мы обсудим ряд таких моделей на примерах. □

Заметное отличие каналов с непрерывно распределённым шумом состоит в том, что энтропия меняется при необходимости на дифференциальную энтропию. Напомним, что понятие дифференциальной энтропии было введено в § 1.5, одним из его основных свойств является неравенство обработки данных $I(X : Y) \geqslant I(X : \varphi(Y))$. Взаимная энтропия между двумя с. в. X и Y с совместной ф. в. $f_{X,Y}(x, y)$ относительно опорной меры $\mu \times \nu$ и маргинальными ф. в. $f_X(x) = \int f_{X,Y}(x, y)\nu(dy)$ и $f_Y(y) = \int f_{X,Y}(x, y)\mu(dx)$) равна

$$I(X : Y) = \mathsf{E} \log \frac{f_{X,Y}(X, Y)}{f_X(X) f_Y(Y)} = \int f_{X,Y}(x, y) \log \frac{f_{X,Y}(x, y)}{f_X(x) f_Y(y)} \mu(dx)\nu(dy). \quad (4.1.21)$$

Аналогичное определение работает при замене X и Y на случайные векторы $\mathbf{X} = (X_1, \ldots, X_N)$ и $\mathbf{Y} = (Y_1, \ldots, Y_{N'})$ (или даже мультивекторы, как в примере 4.1.4, с векторными компонентами X_j и Y_j):

$$I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N')}) = \mathsf{E} \log \frac{f_{\mathbf{X}^{(N)}, \mathbf{Y}^{(N')}}(\mathbf{X}^{(N)}, \mathbf{Y}^{(N')})}{f_{\mathbf{X}^{(N)}}(\mathbf{X}^{(N)}) f_{\mathbf{Y}^{(N')}}(\mathbf{Y}^{(N')})}. \quad (4.1.22a)$$

Здесь $f_{\mathbf{X}^{(N)}}(\mathbf{X}^{(N)})$ и $f_{\mathbf{Y}^{(N')}}(\mathbf{Y}^{(N')})$ — маргинальные ф. в. для $\mathbf{X}^{(N)}$ и $\mathbf{Y}^{(N')}$ (т. е. совместные ф. в. для компонент этих векторов).

А именно, если $N = N'$, то $\mathbf{X}^{(N)}$ представляет собой случайный вход, а $\mathbf{Y}^{(N)} = \mathbf{X}^{(N)} + \mathbf{Z}^{(N)}$ — соответствующий случайный выход канала со (случайной) вероятностью ошибки

$$E(\mathbf{x}^{(N)}, \mathbb{D}^{(N)}) = \begin{cases} 1, & \mathbf{x} \notin \mathbb{D}^{(N)}, \\ \mathbf{P}^{(N)}_{\mathrm{ch}}(d_{\mathrm{ML}}(\mathbf{Y}^{(N)}) \neq \mathbf{x}^{(N)} | \mathbf{x}^{(N)}), & \mathbf{x} \in \mathbb{D}^{(N)}, \end{cases}$$

см. формулу (4.1.4). Более того, нас интересует математическое ожидание

$$\mathcal{E}(P_{\mathbf{x}^{(N)}};\, \mathbb{D}^{(N)}) = \mathsf{E}[E(\mathbf{x}^{(N)},\, \mathbb{D}^{(N)})]. \tag{4.1.22б}$$

Далее, при данном $\varepsilon > 0$ можно определить супремум взаимной информации на сигнал (т. е. на одно использование канала) по всем входным распределениям вероятности $P_{\mathbf{x}^{(N)}}$ с $\mathcal{E}(P_{\mathbf{x}^{(N)}},\, \mathbb{D}^{(N)}) \leqslant \varepsilon$:

$$\bar{C}_{\varepsilon,N} = \frac{1}{N} \sup[I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \colon \mathcal{E}(P_{\mathbf{x}^{(N)}},\, \mathbb{D}^{(N)}) \leqslant \varepsilon], \tag{4.1.23}$$

$$\bar{C}_{\varepsilon} = \limsup_{N\to\infty} \bar{C}_{\varepsilon,N}, \quad \bar{C} = \liminf_{\varepsilon\to 0} \bar{C}_{\varepsilon}. \tag{4.1.24}$$

Подчеркнём, что супремум в формуле (4.1.23) следует брать по *всем* распределениям вероятности $P_{\mathbf{x}^{(N)}}$ входного слова $\mathbf{X}^{(N)}$ с тем свойством, что математическое ожидание не превосходит ε, вне зависимости от того, дискретное это распределение, непрерывное или смешанное (содержащее обе компоненты). Это сильно усложняет правильную оценку значения $\bar{C}_{N,\varepsilon}$. Однако предельное значение $\bar{C}$ более доступно, по крайней мере в некоторых важных примерах.

Теперь мы готовы доказать обратную часть второй теоремы Шеннона о кодировании

Теорема 4.1.5 (см. теорему 1.4.12). *Рассмотрим канал, заданный последовательностью распределений вероятности* $\mathbf{P}_{\mathrm{ch}}(\,\cdot\,|\mathbf{x}^{(N)}$ *послано*) *случайных выходных слов* $\mathbf{Y}^{(N)}$ *и декодируемых областей* $\mathbb{D}^{(N)}$. *Тогда число* $\bar{C}$ *из формулы* (4.1.24) *даёт верхнюю границу пропускной способности*:

$$C \leqslant \bar{C}. \tag{4.1.25}$$

Доказательство. Пусть R — скорость надёжной передачи и $\{\mathcal{X}_{M,N}\}$, где $M = \#\mathcal{X}_{M,N} \sim 2^{NR}$, — последовательность кодовых книг, для которой $\lim\limits_{N\to\infty} e^{\mathrm{av}}(\mathcal{X}_{M,N},\, \mathbb{D}^{(N)}) = 0$. Рассмотрим пару $(\mathbf{x},\, d_{\mathrm{ML}}(\mathbf{y}))$, где а) $\mathbf{x} = \mathbf{x}_{\mathrm{eq}}^{(N)}$ — случайное входное слово, равномерно распределённое на $\mathcal{X}_{M,N}$, б) $\mathbf{Y} = \mathbf{Y}^{(N)}$ — полученное слово и в) $d_{\mathrm{ML}}(\mathbf{Y})$ — гипотетическое кодовое слово, предлагаемое декодером м. п. d_{ML} после передачи. Слова $\mathbf{x}$ и $d_{\mathrm{ML}}(\mathbf{Y})$ совместно пробегают множество $\mathcal{X}_{M,N}$, т. е. обладают совместным распределением дискретного типа. Тогда согласно обобщённому неравенству

Фано (1.2.25) имеем

$$h_{\mathrm{discr}}(\mathbf{X}|d(\mathbf{Y})) \leqslant 1 + \log(M-1) \sum_{\mathbf{x}\in\mathcal{X}_{M,N}} \mathsf{P}(\mathbf{X}=\mathbf{x},\, d_{\mathrm{ML}}(\mathbf{Y}) \neq \mathbf{x}) \leqslant$$

$$\leqslant 1 + \frac{NR}{M} \sum_{\mathbf{x}\in\mathcal{X}_{M,N}} \mathbf{P}_{\mathrm{ch}}(d_{\mathrm{ML}}(\mathbf{Y}) \neq \mathbf{x} | \mathbf{x} \text{ послано}) =$$

$$= 1 + NRe^{\mathrm{av}}(\mathcal{X}_{M,N}, \mathbb{D}^{(N)}) := N\theta_N,$$

где $\lim\limits_{N\to\infty} \theta_N = 0$. Далее, приравняв $h(\mathbf{x}_{\mathrm{eq}}^{(N)}) = \log M$, получим, что $NR - 1 \leqslant h(\mathbf{x}_{\mathrm{eq}}^{(N)})$. Следовательно,

$$R \leqslant \frac{1 + h(\mathbf{x}_{\mathrm{eq}}^{(N)})}{N} = \frac{1}{N} I(\mathbf{x}_{\mathrm{eq}}^{(N)} : d(\mathbf{Y}^{(N)})) + \frac{1}{N} h(\mathbf{x}_{\mathrm{eq}}^{(N)} | d(\mathbf{Y}^{(N)})) +$$

$$+ \frac{1}{N} \leqslant \frac{1}{N} I(\mathbf{x}_{\mathrm{eq}}^{(N)} : \mathbf{Y}^{(N)}) + \theta_N.$$

При любом заданном $\varepsilon > 0$ средняя вероятность ошибки $e^{\mathrm{av}}(\mathcal{X}_{M,N}, \mathbb{D}^{(N)})$ за счёт выбора достаточно большого N может быть сделана меньше ε. Значит, $R \leqslant \bar{C}_{N,\varepsilon}$ при достаточно больших N (потому что равномерное распределение на кодовой книге $\mathcal{X}_{M,N}$, $e^{\mathrm{av}}(\mathcal{X}_{M,N}, \mathbb{D}^{(N)})$ доставляет специальный пример входного распределения $P_{\mathbf{x}^{(N)}}$, для которого $\mathcal{E}(P_{\mathbf{x}^{(N)}}, \mathbb{D}^{(N)}) \leqslant \varepsilon$). Таким образом, $R \leqslant \bar{C}_\varepsilon$ при любом положительном ε, откуда следует неравенство $R \leqslant \bar{C}$ на скорость передачи, как и утверждалось. □

Неравенство $C \leqslant \bar{C}$ в формуле (4.1.25) становится равенством $C = \bar{C}$ во многих интересных ситуациях. Более того, выражение, описывающее $\bar{C}$, упрощается в некоторых любопытных случаях. Например, для а. г. к. вместо максимизации взаимной информации $I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})$ по различным N возможно ограничится поиском максимума $I(X : Y)$ — взаимной информации между отдельными входным и выходным сигналами при некотором подходящем ограничении. А именно, для а. г. к. имеем

$$C = \bar{C} = \sup[I(X : Y) \colon \mathsf{E}X^2 < \alpha]. \tag{4.1.26а}$$

Величину $\sup[I(X : Y) \colon \mathsf{E}X^2 < \alpha]$ часто называют информационной пропускной способностью а. г. к. при квадратичном ограничении α. Более того, для общего а. г. к. имеет место равенство

$$C = \bar{C} = \lim_{N\to\infty} \frac{1}{N} \sup \left[I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \colon \frac{1}{N} \sum_{j=1}^{N} \mathsf{E}X_j^2 < \alpha \right]. \tag{4.1.26б}$$

Когда специалист по теории информации делает это, он часто бывает неинформированным и страдает отсутствием памяти.

(Из серии «Как они делают это».)

Неинформативный источник канала без памяти

(Из серии «Фильмы, которые не вышли на большой экран».)

Пример 4.1.6. Здесь мы найдём $\bar{C}(\alpha, \sigma^2)$ а. г. к. б. п. с аддитивным белым гауссовским шумом дисперсии σ^2 при ограничении по средней мощности ($\mathbb{D}^{(N)} = \mathbb{B}^{(N)}(\sqrt{N\alpha})$), см. пример 4.1.1, т. е. границу п. ч. формулы (4.1.26б). При данном распределении $P_{\mathbf{X}^{(N)}}$ запишем

$$I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) = h(\mathbf{Y}^{(N)}) - h(\mathbf{Y}^{(N)}|\mathbf{X}^{(N)}) = h(\mathbf{Y}^{(N)}) - h(\mathbf{Z}^{(N)}) \leqslant$$
$$\leqslant \sum_{j=1}^{n} h(Y_j) - h(\mathbf{Z}^{(n)}) = \sum_{j=1}^{N} (h(Y_j) - h(Z_j)). \quad (4.1.26в)$$

Обозначим через $\alpha_j^2 = \mathsf{E}X_j^2$ второй момент с. в. одномоментного входа X_j, j-й компоненты случайного входного вектора $\mathbf{X}^{(N)}$. Тогда для соответствующей выходной с. в. Y_j вычисляем второй момент:

$$\mathsf{E}Y_j^2 = \mathsf{E}(X_j + Z_j)^2 = \mathsf{E}X_j^2 + 2\,\mathsf{E}X_jZ_j + \mathsf{E}Z_j^2 = \alpha_j^2 + \sigma^2,$$

поскольку X_j и Z_j независимы и $\mathsf{E}Z_j = 0$.

Заметим, что при гауссовском канале распределение с. в. Y_j непрерывно (с п. р. $f_{Y_j}(y)$, определяемой свёрткой $\int \varphi_{\sigma^2}(x - y)dF_{X_j}(x)$, где φ_{σ^2} — п. р. с. в. $Z_j \sim \mathrm{N}(0, \sigma^2)$). Следовательно, энтропия $h(Y_j)$, фигурирующая в формуле (4.1.26а), — это дифференциальная энтропия. Напомним, что для с. в. Y_j с п. р. f_{Y_j} при ограничении $\mathsf{E}Y_j^2 \leqslant \alpha_j^2 + \sigma^2$ максимум дифференциальной энтропии удовлетворяет неравенству $h(Y_j) \leqslant \frac{1}{2}\log_2[2\pi e(\alpha_j^2 + \sigma^2)]$. Действительно, по неравенству Гиббса имеем

$$h(Y_j) = -\int f_{Y_j}(y)\log_2 f_{Y_j}(y)dy \leqslant -\int f_{Y_j}(y)\log_2 \varphi_{\alpha_j^2+\sigma^2}(y)dy =$$
$$= \frac{1}{2}\log_2[2\pi(\alpha_j^2 + \sigma^2)] + \frac{\log_2 e}{2(\alpha_j^2 + \sigma^2)}\,\mathsf{E}Y_j^2 \leqslant \frac{1}{2}\log_2[2\pi e(\alpha_j^2 + \sigma^2)],$$

и, следовательно,

$$I(X_j : Y_j) = h(Y_j) - h(Z_j) \leqslant \log_2[2\pi e(\alpha_j^2 + \sigma^2)] - \log_2(2\pi e\sigma^2) = \log_2\left(1 + \frac{\alpha_j^2}{\sigma^2}\right),$$

причём равенство достигается тогда и только тогда, когда $Y_j \sim \mathrm{N}(0, \alpha_j^2 + \sigma^2)$.

Из границы $\sum_{j=1}^{N} \mathsf{E}X_j^2 = \sum_{j=1}^{N} \alpha_j^2 < N\alpha$ в формуле (4.1.26б) по закону больших чисел следует, что $\lim_{N\to\infty} P_{\mathbf{X}^{(N)}}(\mathbb{B}^{(N)}(\sqrt{N\alpha}) = 1$. Более того, для любого такого входного распределения вероятностей $P_{\mathbf{X}^{(N)}}$, что $\mathsf{E}X_j^2 < \alpha^2$, $1 \leqslant j \leqslant N$, мы имеем

$$\frac{1}{N} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \leqslant \frac{1}{2N} \sum_{j=1}^{N} \log_2 \left(1 + \frac{\alpha_j^2}{\sigma^2}\right).$$

Из неравенства Йенсена, применённого к вогнутой функции $x \mapsto \log_2(1+x)$, получаем, что

$$\frac{1}{2N} \sum_{j=1}^{N} \log_2 \left(1 + \frac{\alpha_j^2}{\sigma^2}\right) \leqslant \frac{1}{2} \log_2 \left(1 + \frac{1}{2} \sum_{j=1}^{N} \frac{\alpha_j^2}{\sigma^2}\right) \leqslant \frac{1}{2} \log_2 \left(1 + \frac{\alpha}{\sigma^2}\right).$$

Значит, в этом примере информационная пропускная способность $\bar{C}$, определенная в п. ч. формулы (4.1.26б), подчиняется неравенству

$$\bar{C} \leqslant \frac{1}{2} \log_2 \left(1 + \frac{\alpha}{\sigma^2}\right). \tag{4.1.27}$$

В примере 4.1.10 мы проверим, что пропускная способность $C(\alpha, \sigma^2)$ совпадает с п. ч., подтверждая ответ в формуле (4.1.17). □

Пример 4.1.7. Оценку (4.1.26в) можно повторить для «цветного» гауссовского шума:

$$I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \leqslant \sum_{j=1}^{N} [h(Y_j) - h(Z_j)].$$

Здесь мы работаем со смешанными моментами второго порядка случайных векторов входного и выходного сигналов X_j и $Y_j = X_j + Z_j$:

$$\alpha_j^2 = \mathsf{E}\langle X_j, QX_j\rangle, \quad \mathsf{E}\langle Y_j, QY_j\rangle = \alpha_j^2 + \operatorname{trace}(Q\Sigma), \quad \frac{1}{N} \sum_{j=1}^{N} \alpha_j^2 \leqslant \alpha;$$

мы снова воспользовались тем фактом, что X_j и Z_j независимы и $\mathsf{E}Z_j = 0$.

Далее, как и в скалярном случае, величина $I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)})/N$ не превышает разности $h(Y) - h(Z)$, где $Z \sim \mathrm{N}(0, \Sigma)$ — вектор «цветного» шума и $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$ распределён по многомерному нормальному закону, максимизирующему дифференциальную энтропию при ограничении следа. Формально,

$$\frac{1}{N} I(\mathbf{X}^{(N)} : \mathbf{Y}^{(N)}) \leqslant \bar{h}(\alpha, Q, \Sigma) - h(Z),$$

где K — матрица ковариаций сигнала и

$$\bar{h}(\alpha,\, Q,\, \Sigma) = \frac{1}{2}\max\Big\{\log[(2\pi)^k e\det(K+\Sigma)]:\ \text{матрица } K \text{ положительно определена, имеет размер } k\times k \text{ и } \operatorname{trace}(QK)\leqslant\alpha\Big\}.$$

Представим Σ в диагональном виде: $\Sigma = C\Lambda C^{\mathrm{T}}$, где C — ортогональная, а Λ — диагональная матрица размера $k\times k$, составленная из собственных значений матрицы Σ:

$$\Lambda = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & \lambda_k \end{pmatrix}.$$

Обозначим $C^{\mathrm{T}}KC = B$ и максимизируем $\det(B+\Lambda)$, соблюдая ограничение:

матрица B положительно определена, и $\operatorname{trace}(\Gamma B)\leqslant\alpha$, где $\Gamma = C^{\mathrm{T}}QC$.

Ввиду неравенства Адамара из примера 1.5.10 имеем $\det(B+\Lambda)\leqslant \prod_{i=1}^{k}(B_{ii}+\lambda_i)$, где равенство достигается тогда и только тогда, когда B диагональна (т. е. у матриц Σ и K одинаковые собственные векторы) и $B_{11}=\beta_1,\ \dots,\ B_{kk}=\beta_k$ — собственные числа матрицы K. Как и раньше, предположим, что $Q\Sigma = \Sigma Q$, тогда $\operatorname{trace}(\Gamma B) = \sum_{i=1}^{k}\gamma_i\beta_i$, так что нам нужно максимизировать произведение $\prod_{i=1}^{k}(\beta_i+\lambda_i)$, или, что то же самое, сумму

$$\sum_{i=1}^{k}\log(\beta_i+\lambda_i)\quad\text{при условии}\quad \beta_1,\ \dots,\ \beta_k\geqslant 0\quad\text{и}\quad \sum_{i=1}^{k}\gamma_i\beta_i\leqslant\alpha.$$

Если отбросить ограничение $\beta_1,\ \dots,\ \beta_k\geqslant 0$, то лагранжиан

$$\mathcal{L}(\beta_1,\ \dots,\ \beta_k;\ \varkappa) = \sum_{i=1}^{k}\log(\beta_i+\lambda_i) + \varkappa\left(\alpha - \sum_{i=1}^{k}\gamma_i\beta_i\right)$$

достигает максимума при

$$\frac{1}{\beta_i+\lambda_i} = \varkappa\gamma_i,\ \text{ т. е. } \beta_i = \frac{1}{\varkappa\gamma_i} - \lambda_i,\ \ i=1,\ \dots,\ k.$$

Для того чтобы выполнялись отброшенные ограничения, выберем

$$\beta_i = \left(\frac{1}{\varkappa\gamma_i} - \lambda_i\right)_+,\quad i=1,\ \dots,\ k,$$

и подправим $\varkappa > 0$ так, чтобы выполнялось равенство

$$\sum_{i=1}^{k} \left(\frac{1}{\varkappa} - \gamma_i \lambda_i \right)_+ = \alpha. \tag{4.1.28}$$

Отсюда следует, что информационная пропускная способность $\bar{C}(\alpha, Q, \Sigma)$ подчиняется неравенству

$$\bar{C}(\alpha, Q, \Sigma) \leqslant \frac{1}{2} \sum_{l=1+1}^{k-1} \log_2 \left(1 + \frac{(\nu \gamma_l^{-1} - \lambda_l)_+}{\lambda_l} \right), \tag{4.1.29}$$

где $\nu = \nu(\alpha) = 1/\varkappa(\alpha)$, см. формулу (4.1.28). И опять мы покажем, что пропускная способность $\bar{C}(\alpha, Q, \Sigma)$ равна п. ч. формулы (4.1.29), подтверждая ответ в формуле (4.1.19). □

Теперь перейдём к прямой части второй теоремы Шеннона о кодировании для общих каналов с ограничениями на доступную передаче область. Хотя её формулировка отличается от содержания теоремы 1.4.12 только предположениями об ограничениях на кодовые слова (и доказательство — не более чем повторение), полезно привести её в формальном контексте.

... through the channels of the ear
May wander like a river
The swaying sound of the sea.

Уистен Х. Оден (1907–1973), американский поэт, англичанин по происхождению.

Теорема 4.1.8. *Пусть канал задаётся последовательностью условных вероятностей* $\mathbf{P}_{\mathrm{ch}}^{(N)}(\cdot \,|\, \mathbf{x}^{(N)}$ *послано*$)$ *для полученного слова* $\mathbf{Y}^{(N)}$ *и последовательностью ограничений декодируемости* $\mathbf{x}^{(N)} \in \mathbb{D}^{(N)}$ *для входного вектора. Предположим, что вероятности* $\mathbf{P}_{\mathrm{ch}}^{(N)}(\cdot \,|\, \mathbf{x}^{(N)}$ *послано*$)$ *заданы как ф.в.* $f_{\mathrm{ch}}(\mathbf{y}^{(N)} | \mathbf{x}^{(N)}$ *послано*$)$ *относительно опорной меры* $\nu^{(N)}$. *Предположим, что при данном* $c > 0$ *существует последовательность таких входных распределений вероятности* $\mathbf{P}_{\mathbf{x}^{(N)}}$, *что а)* $\lim\limits_{N\to\infty} P_{\mathbf{x}^{(N)}}(\mathbb{D}^{(N)}) = 1$, *б) распределение* $\mathbf{P}_{\mathbf{x}^{(N)}}$ *задаётся совместной ф.р.* $f_{\mathbf{X}^{(N)}}(\mathbf{x}^{(N)})$ *относительно опорной меры* $\mu^{(N)}$, *в) выполнена следующая сходимость по вероятности*: $\forall \varepsilon > 0$

$$\begin{aligned} &\lim_{N\to\infty} \mathsf{P}_{\mathbf{x}^{(N)}, \mathbf{Y}^{(N)}}(T_\varepsilon^N) = 1, \\ &T_\varepsilon^N = \left(\left| \frac{1}{N} \log_+ \frac{f_{\mathbf{X}^{(N)}, \mathbf{Y}^{(N)}}(\mathbf{x}^{(N)}, \mathbf{Y}^{(N)})}{f_{\mathbf{X}^{(N)}}(\mathbf{x}^{(N)}) f_{\mathbf{Y}^{(N)}}(\mathbf{Y}^{(N)})} - c \right| \leqslant \varepsilon \right), \end{aligned} \tag{4.1.30a}$$

где

$$f_{\mathbf{X}^{(N)},\mathbf{Y}^{(N)}}(\mathbf{x}^{(N)},\,\mathbf{Y}^{(N)}) = f_{\mathbf{X}^{(N)}}(\mathbf{x}^{(N)})f_{\mathrm{ch}}(\mathbf{y}^{(N)}|\mathbf{x}^{(N)}\ \textit{послано}),$$
$$f_{\mathbf{Y}^{(N)}}(\mathbf{Y}^{(N)}) = \int f_{\mathbf{X}^{(N)}}(\tilde{\mathbf{x}}^{(N)})f_{\mathrm{ch}}(\mathbf{y}^{(N)}|\tilde{\mathbf{x}}^{(N)}\ \textit{послано})\mu^{\times N}(d\tilde{\mathbf{x}}^{(N)}). \tag{4.1.30б}$$

Тогда пропускная способность канала удовлетворяет оценке $C \geqslant c$.

Доказательство. Возьмём $R < c$ и рассмотрим случайную кодовую книгу $\{\mathbf{x}^{(N)}(1), \ldots, \mathbf{x}^{(N)}(M)\}$ с $M \sim 2^{NR}$, составленную из н. о. р. кодовых слов, где каждое кодовое слово $\mathbf{x}^{(N)}(i)$ случайно в соответствии с законом $P^{(N)} = P_{\mathbf{x}^{(N)}}$. Предположим, что получено (случайное) слово $\mathbf{Y}^{(N)} = \mathbf{Y}^{(N)}(j)$ с совместной ф. в. $f_{\mathbf{X}^{(N)},\mathbf{Y}^{(N)}}$, как в (4.1.30б). Мы берём $\varepsilon > 0$ и декодируем $\mathbf{Y}^{(N)}$, используя декодер совместной типичности

$$d_{\mathrm{JT}}(\mathbf{Y}^{(N)}) = \mathbf{x}^{(N)}(i) \text{ когда } \mathbf{x}^{(N)}(i) \text{ — единственный такой вектор}$$
$$\text{среди } \mathbf{x}^{(N)}(1), \ldots, \mathbf{x}^{(N)}(M), \text{ что } (\mathbf{x}^{(N)}(i),\,\mathbf{Y}^{(N)}) \in T_\varepsilon^N.$$

Множество T_ε^N определено в формуле (4.1.30а).

Предположим, что по каналу послали случайный вектор $\mathbf{x}^{(N)}(j)$. Считается, что ошибка возникает в следующих случаях: а) $\mathbf{x}^{(N)}(j) \notin \mathbb{D}^{(N)}$, б) $(\mathbf{x}^{(N)}(j),\,\mathbf{Y}^{(N)}) \notin T_\varepsilon^N$, в) $(\mathbf{x}^{(N)}(i),\,\mathbf{Y}^{(N)}) \in T_\varepsilon^N$ при некотором $i \neq j$. Ни одна из перечисленных возможностей не исключает другую, но если ничего из этого не произошло, то а) $\mathbf{x}^{(N)}(j) \in \mathbb{D}^{(N)}$ и б) $\mathbf{x}^{(N)}(j)$ — единственное такое слово из $\mathbf{x}^{(N)}(1), \ldots, \mathbf{x}^{(N)}(M)$, что $(\mathbf{x}^{(N)}(j),\,\mathbf{Y}^{(N)}) \in T_\varepsilon^N$. Следовательно, декодер совместной типичности даст верный результат. Рассмотрим среднюю вероятность ошибки

$$\mathcal{E}_M(P^N) = \frac{1}{M}\sum_{j=1}^{M} E(j,\,P^N),$$

где $E(j,\,P^N)$ — вероятность того, что произошёл один из перечисленных выше случаев а)–в):

$$E(j,\,P^N) = \mathsf{P}\big(\{\mathbf{x}^{(N)}(j) \notin \mathbb{D}^{(N)}\} \cup \{(\mathbf{x}^{(N)}(j),\,\mathbf{Y}^{(N)}) \notin T_\varepsilon^N\} \cup$$
$$\cup\,\{(\mathbf{x}^{(N)}(i),\,\mathbf{Y}^{(N)}) \in T_\varepsilon^N \text{ для некоторого } i \neq j\}\big) =$$
$$= \mathsf{E}\,\mathbf{1}\big(\mathbf{x}^{(N)}(j) \notin \mathbb{D}^{(N)}\big) + \mathsf{E}\,\mathbf{1}\big(\mathbf{x}^{(N)}(j) \in \mathbb{D}^{(N)},\ d_{\mathrm{JT}}(\mathbf{Y}^{(N)}) \neq \mathbf{x}^{(N)}(j)\big). \tag{4.1.31}$$

Символы P и E в формуле (4.1.31) относятся к 1^0) набору н. о. р. входных векторов $\mathbf{x}^{(N)}(1), \ldots, \mathbf{x}^{(N)}(M)$ и 2^0) выходному вектору $\mathbf{Y}^{(N)}$, связанному с $\mathbf{x}^{(N)}(j)$ действием канала. Значит, вектор $\mathbf{Y}^{(N)}$ не зависит от $\mathbf{x}^{(N)}(i)$ при $i \neq j$. Поучительно представить распределение вероятностей P в виде прямого произведения, например, для $j = 1$ в формуле (4.1.31) мы имеем

$$\mathsf{P} = P_{\mathbf{x}^{(N)}(1),\mathbf{Y}^{(N)}(1)} \times P_{\mathbf{x}^{(N)}(2)} \times \ldots \times P_{\mathbf{x}^{(N)}(M)},$$

где $P_{\mathbf{x}^{(N)}(1),\mathbf{Y}^{(N)}(1)}$ обозначает совместное распределение входного вектора $\mathbf{x}^{(N)}(1)$ и выходного вектора $\mathbf{Y}^{(N)}(1)$, определяемое совместной ф. р.

$$f_{\mathbf{x}^{(N)}(1),\mathbf{Y}^{(N)}(1)}(\mathbf{x}^{(N)},\, \mathbf{y}^{(N)}) = f_{\mathbf{x}^{(N)}(1)}(\mathbf{x}^{(N)}) f_{\mathrm{ch}}(\mathbf{y}^{(N)}|\mathbf{x}^{(N)} \text{ послано}).$$

Из соображений симметрии $E(j,\, P^N)$ не зависит от j, поэтому далее мы можем считать, что $j = 1$. Далее, вероятность $E(1,\, P^N)$ не превышает сумму вероятностей

$$\mathsf{P}(\mathbf{x}^{(N)}(1) \notin \mathbb{D}^{(N)}) + \mathsf{P}(\mathbf{x}^{(N)}(1),\, \mathbf{Y}^{(N)}) \notin T_\varepsilon^N) + \sum_{i=2}^{M} \mathsf{P}((\mathbf{x}^{(N)}(i),\, \mathbf{Y}^{(N)}) \in T_\varepsilon^N).$$

Ввиду того что $\lim\limits_{N\to\infty} P_{\mathbf{x}^{(N)}}(\mathbb{D}^{(N)}) = 1$ первое слагаемое обращается в нуль при $N \to \infty$. Второе слагаемое при переходе к пределу при $N \to \infty$ тоже обращается в нуль благодаря формуле (4.1.30a). Осталось оценить сумму $\sum\limits_{i=2}^{M} \mathsf{P}((\mathbf{x}^{(N)}(i),\, \mathbf{Y}^{(N)}) \in T_\varepsilon^N)$.

Заметим для начала, что из соображений симметрии все слагаемые равны

$$\sum_{i=2}^{M} \mathsf{P}\big((\mathbf{x}^{(N)}(i),\, \mathbf{Y}^{(N)}) \in T_\varepsilon^N\big) = \big(2^{\lceil NR\rceil} - 1\big)\, \mathsf{P}\big((\mathbf{x}^{(N)}(2),\, \mathbf{Y}^{(N)}) \in T_\varepsilon^N\big).$$

Далее, по теореме 4.2.4 (см. формулу (4.2.15)) имеем

$$\mathsf{P}(\mathbf{x}^{(N)}(2),\, \mathbf{Y}^{(N)}) \in T_\varepsilon^N) \leqslant 2^{-N(c-3\varepsilon)},$$

и, следовательно,

$$\sum_{i=2}^{M} \mathsf{P}((\mathbf{x}^{(N)}(i),\, \mathbf{Y}^{(N)}) \in T_\varepsilon^N) \leqslant 2^{N(R-c+3\varepsilon)},$$

что стремится к 0 при $N \to \infty$, когда $\varepsilon < (c - R)/3$.

Итак, при $R < c$ получаем, что $\lim\limits_{N\to\infty} \mathcal{E}_M(P^N) = 0$. Здесь R означает скорость надёжной передачи в смысле определения 4.1.2. Но $\mathcal{E}_M(P^N)$ допускает представление

$$\mathcal{E}_M(P^N) = \mathsf{E}_{P_{\mathbf{x}^{(N)}(1)} \times \ldots \times P_{\mathbf{x}^{(N)}(M)}} \left(\frac{1}{M} \sum_{j=1}^{M} E(j) \right),$$

где $E(j)$ представляет собой вероятность ошибки, как определено в формуле (4.1.14):

$$E(j) = \begin{cases} 1, & \mathbf{x} \notin \mathbb{D}^{(N)}, \\ \mathbf{P}_{\mathrm{ch}}\big(d_{\mathrm{JT}}^{(N),\varepsilon}(\mathbf{Y}^{(N)}) \neq \mathbf{x}^{(N)}(j) | \mathbf{x}^{(N)}(j) \text{ послано}\big), & \mathbf{x} \in \mathbb{D}^{(N)}. \end{cases}$$

Заключаем, что существует такая последовательность кодовых книг $\mathcal{X}_{M,N}$, что средняя вероятность ошибки удовлетворяет условию

$$\frac{1}{M}\sum_{\mathbf{x}\in\mathcal{X}_{M,N}} e(\mathbf{x}) \to 0,$$

где $e(\mathbf{x}) = e(\mathbf{x},\, \mathcal{X}_{M,N},\, \mathbb{D}^{(N)},\, d_{\mathrm{JT}}^{(N),\varepsilon})$ — вероятность ошибки для входного слова $\mathbf{x}$ в коде $\mathcal{X}_{M,N}$ при декодере с. т. и ограничении на доступную передаче область $\mathbb{D}^{(N)}$:

$$e(\mathbf{x}) = \begin{cases} 1, & \mathbf{x}\notin\mathbb{D}^{(N)}, \\ \mathbf{P}_{\mathrm{ch}}\bigl(d_{\mathrm{JT}}^{(N),\varepsilon}(\mathbf{Y}^{(N)}) \neq \mathbf{x} | \mathbf{x} \text{ послано}\bigr), & \mathbf{x}\in\mathbb{D}^{(N)}. \end{cases}$$

Этим завершается доказательство теоремы 4.1.8, а вместе с ним и доказательство следующей теоремы 4.1.9. □

Теорема 4.1.9. *Предположим, что выполнены условия теоремы* 4.1.5. *Тогда для любых $R < C$ существует такая последовательность кодов $\mathcal{X}_{M,N}$ длины N и размера $M \sim 2^{RN}$, что максимум вероятности ошибки стремится к* 0 *при $N\to\infty$.*

Пример 4.1.10. Теорема 4.1.8 позволяет уточнить неравенства примеров 4.1.3 и 4.1.4 для истинных значений соответствующих пропускных способностей (при декодере м. п.): для скалярного белого шума с дисперсией σ^2 при ограничении по средней мощности $\sum\limits_{i=1}^{N} x_i^2 \leqslant N\alpha$ имеем

$$C(\alpha,\, \sigma^2) = \frac{1}{2}\log\Bigl(1 + \frac{\alpha}{\sigma^2}\Bigr),$$

для вектора белого шума с дисперсией $\underline{\sigma}^2 = (\sigma_1^2,\, \ldots,\, \sigma_k^2)$ при ограничении $\sum\limits_{j=1}^{N} x_j^{\mathrm{T}} x_j \leqslant N\alpha$ получаем, что

$$C(\alpha,\, \underline{\sigma}^2) = \frac{1}{2}\sum_{i=1}^{k}\log\left(1 + \frac{(\nu - \sigma_i^2)_+}{\sigma_i^2}\right), \quad \text{где} \quad \sum_{i=1}^{k}(\nu - \sigma_i^2)_+ = \alpha^2,$$

и, наконец, для «цветного» векторного шума с матрицей ковариаций Σ при ограничении $\sum\limits_{i=1}^{N} x_i^{\mathrm{T}} Q x_i \leqslant N\alpha$ имеем

$$C(\alpha,\, Q,\, \Sigma) = \frac{1}{2}\sum_{i=1}^{k}\log\Bigl(1 + \frac{(\nu\gamma_i^{-1} - \lambda_i)_+}{\lambda_i}\Bigr),$$

где $\sum\limits_{i=1}^{k}(\nu - \gamma_i\lambda_i)_+ = \alpha$.

А именно, для скалярного белого шума мы берём случайное кодирование, в котором сигналы $X_j(i)$, $1 \leqslant j \leqslant N$, $1 \leqslant i \leqslant M = \lceil 2^{NR} \rceil$ — н. о. р. $\mathrm{N}(0, \alpha - \varepsilon)$. Нам предстоит проверить выполнение условий теоремы 4.1.8 в этом случае: при $N \to \infty$ должны выполняться условия 1) $\lim\limits_{N\to\infty} \mathsf{P}(\mathbf{x}^{(N)}(i) \in \mathbb{B}^{(N)}(\sqrt{N\alpha}) \ \ \forall i = 1, \ldots, M) = 1$ и 2) $\lim\limits_{\varepsilon\to 0} \lim\limits_{N\to\infty} \theta_N = C(\alpha, \sigma^2)$ по вероятности, где

$$\theta_N = \frac{1}{N} \sum_{j=1}^{N} \log \frac{P(X, Y)}{P_X(X) P_Y(Y)}.$$

Начнём со свойства 1): поскольку дисперсия сигнала $X_j(i) = \tilde{\sigma}^2 = \alpha - \varepsilon$, запишем

$$\mathsf{P}\left(\mathbf{x}^{(N)}(i) \notin \mathbb{B}^{(N)}(\sqrt{N\alpha}) \text{ для некоторого } i = 1, \ldots, M\right) \leqslant$$
$$\leqslant \mathsf{P}\left(\frac{1}{NM} \sum_{i=1}^{M} \sum_{j=1}^{N} X_j(i)^2 \geqslant \alpha\right) = \mathsf{P}\left(\frac{1}{NM} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_j(i)^2 - \tilde{\sigma}^2) \geqslant \varepsilon\right) \leqslant$$
$$\leqslant \mathsf{E}(X^2 - \tilde{\sigma}^2)^2 \left(\frac{1}{NM\varepsilon^2}\right) \to 0.$$

Теперь проверим условие 2: так как пары (X_j, Y_j) — н. о. р., можно применить закон больших чисел и получить, что $\theta_N \to \mathsf{E} \log \frac{P(X, Y)}{P_X(X) P_Y(Y)} = I(X_1 : Y_1)$. Но

$$I(X_1 : Y_1) = h(Y_1) - h(Y_1|X_1) = \frac{1}{2} \log[2\pi e(\alpha - \varepsilon + \sigma^2)] - \frac{1}{2} \log(2\pi e \sigma^2) =$$
$$= \frac{1}{2} \log\left(1 + \frac{\alpha - \varepsilon}{\sigma^2}\right) \to C(\alpha, \sigma^2) \ \text{ при } \ \varepsilon \to 0.$$

Следовательно, пропускная способность равна $C(\alpha, \sigma^2)$, как и утверждалось. Случай «цветного» шума исследуется аналогично. □

Замечание 4.1.11. Введение ограничений на доступную передаче область $\mathbb{D}$ не означает, что весь код $\mathcal{X}$ должен лежать в $\mathbb{D}$. Чтобы гарантировать, что вероятность ошибки $P_{\mathrm{e}}^{\mathrm{av}} \to 0$, достаточно проследить за тем, чтобы «большинство» кодовых слов $\mathbf{x}(i) \in \mathcal{X}$ попадало в $\mathbb{D}$, если длина кодового слова N достаточно велика. □

Пример 4.1.12. Здесь мы рассмотрим негауссовский аддитивный канал, когда компоненты вектора шума $\mathbf{Z} = \begin{pmatrix} Z_1 \\ \vdots \\ Z_N \end{pmatrix}$ представляют собой н. о. р. с двусторонним экспоненциальным распределением $Z_j \sim (2)\mathrm{Exp}(\lambda)$

с п. р.

$$f_{z_j}(z) = \frac{\lambda}{2} e^{-\lambda|z|}, \quad -\infty < z < \infty,$$

где $\lambda > 0$ и $\mathsf{E}|Z_j| = 1/\lambda$. Здесь мы вновь вычислим пропускную способность при декодере м. п. с ограничением на доступную передаче область $\mathbf{x}^{(N)} \in \mathbb{L}(N\alpha)$, где

$$\mathbb{L}(N\alpha) = \left\{ \mathbf{x}^{(N)} \in \mathbb{R}^N \colon \sum_{j=1}^{N} |x_j| \leqslant N\alpha \right\}.$$

Заметим сначала, что если математические ожидания с. в. X и Z подчиняются неравенствам $\mathsf{E}|X| \leqslant \alpha$, $\mathsf{E}|Z| \leqslant \zeta$, то $\mathsf{E}|X+Z| \leqslant \alpha + \zeta$. Далее воспользуемся тем, что дифференциальная энтропия с. в. Y с п. р. f_Y и $\mathsf{E}|Y| \leqslant \eta$ подчиняется неравенству

$$h(Y) \leqslant 2 + \log_2 \eta,$$

где равенство достигается тогда и только тогда, когда $Y \sim (2)\mathrm{Exp}(1/\eta)$. Действительно, как и раньше, по неравенству Гиббса имеем

$$\begin{aligned} h(Y) = -\int f_Y(y) \log f_Y(y) dy \leqslant -\int f_Y(y) \log \varphi^{(2)\mathrm{Exp}(1/\eta)}(y) dy = \\ = 1 + \frac{1}{\eta} \int f_Y(y)|y| dy + \log \eta = 1 + \log \eta \leqslant 2 + \log \eta + \frac{1}{\eta} \mathsf{E}|Y| = \\ = -\int \varphi^{(2)\mathrm{Exp}(1/\eta)}(y) \log \varphi^{(2)\mathrm{Exp}(1/\eta)}(y) dy, \end{aligned}$$

и равенство достигается, только когда $f_Y = \varphi^{(2)\mathrm{Exp}(1/\eta)}$.

Тогда по обратной части ВТШК имеем

$$\begin{aligned} \frac{1}{N} I(\mathbf{x}^{(N)} : \mathbf{Y}^{(N)}) = \frac{1}{N} \sum h(Y_j) - h(Z_j) \leqslant \\ \leqslant \frac{1}{N} \sum [2 + \log_2(\alpha_j + \lambda^{-1}) - 2 + \log_2 \lambda] = \\ = \frac{1}{N} \sum \log_2(1 + \alpha_j \lambda) \leqslant \log_2(1 + \alpha\lambda). \end{aligned}$$

Теми же рассуждениями, как и до этого, можно показать, что п. ч. даёт пропускную способность канала. □

Где мудрость, которую мы потеряли в знаниях?
Где же знания, которые мы потеряли в информации?

Томас С. Элиот (1888–1965), английский поэт
и драматург, американец по рождению

Пример 4.1.13. Теперь рассмотрим канал с аддитивным равномерным шумом, где с. в. шума $Z \sim \mathrm{U}(-b, b)$, $b > 0$, представляет предельную амплитуду шума. Выберем ограничение на доступную передаче область для входного сигнала в виде конечного множества $\mathcal{A} \subset \mathbb{R}$ (входной «алфавит») вида $\mathcal{A} = \{a, a+b, \ldots, a+(M-1)b\}$. Вычислите информационную пропускную способность канала:

$$C^{\inf} = \sup[I(X:Y)\colon p_X(\mathcal{A}) = 1,\ Y = X + Z].$$

Решение. Благодаря инвариантности относительно сдвига можно считать, что $a = -A$ и $a + Mb = A$, где $2A = Mb$ — «ширина» входного сигнального множества. Формула $I(X:Y) = h(Y) - h(Y|X)$, где $h(Y|X) = h(Z) = \ln(2b)$, показывает, что нам нужно максимизировать энтропию выходного сигнала $h(Y)$. С. в. Y меняется в пределах $-A - b \leqslant Y \leqslant A + b$, так что распределение P_Y должно быть настолько близко к равномерному $\mathrm{U}(-A-b, A+b)$, насколько возможно.

Допустим сначала, что M нечётно: $\#A = 2M + 1$,

$$\mathcal{A} = \{0, \pm A/M, \pm 2A/m, \ldots, \pm A\} \quad \text{и} \quad b = A/m,$$

т. е. есть точки множества $\mathcal{A}$ разбивают отрезок $[-A, A]$ на $2m$ интервалов длины A/m; «расширенный отрезок» $[-A-b, A+b]$ содержит $2(m+1)$ таких отрезков. Максимизирующее распределение вероятности P_X можно найти без вычислений: оно приписывает равные вероятности $1/(m+1)$ каждой из $m+1$ точек

$$-A,\ \ -A+2b,\ \ \ldots,\ \ A-2b,\ \ A.$$

Другими словами, мы «вычёркиваем» каждую вторую «букву» из $\mathcal{A}$ и используем оставшиеся буквы с равными вероятностями.

Действительно, при $P_X(-A) = P_X(-A+2b) = \ldots = P_X(A)$ п. р. выходного сигнала f_Y приписывает значение $[2b(m+1)]^{-1}$ каждой точке $y \in [-A-b, A+b]$. Другими словами, $Y \sim \mathrm{U}(-A-b, A+b)$, как и требовалось. Информационная пропускная способность в этом случае равна

$$C^{\inf} = \ln(2A + 2b) - \ln 2b = \ln(1+m). \tag{4.1.32}$$

Скажем, при $M = 3$ (три входных сигнала, в точках $-A$, 0, A и $b = A$) $C^{\inf} = \ln 2$. При $M = 5$ (пять входных сигналов в точках $= A$, $-A/2$, 0, $A/2$, A и $b = A/2$) $C^{\inf} = \ln 3$. См. рис. 4.2 для $M = 13$.

Замечание 4.1.14. Можно доказать, что формула (4.1.32) задаёт максимум взаимной информации $I(X:Y)$ между входным и выходным сигналами X и $Y = X + Z$, когда 1) с. в. шума $Z \sim \mathrm{U}(-b, b)$ не зависит от X и 2) X имеет общее распределение с носителем на отрезке $[-A, A]$, $b = A/m$.

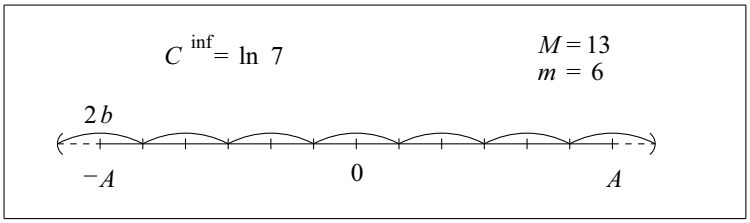


Рис. 4.2

Взаимная информация $I(X:Y)$ здесь определяется по Колмогорову:

$$I(X:Y) = \sup_{\xi,\eta} I(X_\xi : Y_\eta), \tag{4.1.33}$$

где супремум берётся по всем конечным разбиениям ξ и η отрезков $[-A, A]$ и $[-A-b, A+b]$, а X_ξ и Y_η — квантованные векторы с. в. X и Y соответственно. □

Иначе говоря, распределение P_X входного сигнала, удовлетворяющее условию

$$P_X(-A) = P_X(-A+2b) = \ldots = P_X(A-2b) = P_X(A) = \frac{1}{m+1}, \tag{4.1.34}$$

максимизирует $I(X:Y)$ при предположениях 1 и 2. Будем обозначать это распределение через $P_X^{(A,A/m)}$, или $P_X^{(bm,m)}$.

Однако при $M = 2m$, т. е. когда число $\#\mathcal{A}$ допустимых сигналов чётно, вычисления становятся более запутанными. Очевидно, что здесь равномерное распределение $\mathrm{U}(-A-b, A+b)$ не получается. Нам нужно максимизировать $h(Y) = h(X+Z)$ внутри класса кусочно постоянных п. р. f_Y на $[-A-b, A+b]$; см. ниже.

Равные промежутки на $[-A, A]$ порождаются точками $\pm A/(2m-1)$, $\pm 3A/(2m-1)$, …, $\pm A$; они описываются формулой $\pm(2k-1)A/(2m-1)$ для $k = 1, \ldots, m$. Эти точки делят отрезок $[-A, A]$ на $2m-1$ отрезков длины $2A/(2m-1)$. При $Z \sim \mathrm{U}(-b, b)$ и $A = b(m-1/2)$ мы тоже имеем п. р. $f_Y(y)$ выходного сигнала с носителем на $[-A-b, A+b]$:

$$f_Y(y) = \begin{cases} p_m/(2b), & \text{если } b(m-1)/2 \leqslant y \leqslant b(m+1)/2, \\ (p_k + p_{k+1})/(2b), & \text{если } b(k-1)/2 \leqslant y \leqslant b(k+1)/2 \\ & \text{для } k = 1, \ldots, m-1, \\ (p_{-1} + p_1)/(2b), & \text{если } -b/2 \leqslant y \leqslant b/2, \\ p_{-m}/(2b), & \text{если } -b(m+1)/2 \leqslant y \leqslant -b(m-1)/2, \end{cases}$$

где

$$p_{\pm k} = p_X\Big(\pm b\Big(k - \frac{1}{2}\Big)\Big) = \mathsf{P}\Big(X = \pm\frac{(2k-1)A}{2m-1}\Big), \quad k = 1, \ldots, m,$$

обозначает вероятности входного сигнала. Энтропия $h(Y) = h(X+Z)$ записывается как

$$-\frac{p_m}{2}\ln\frac{p_m}{2b} - \sum_{k=1}^{m-1}\frac{p_k+p_{k+1}}{2}\ln\frac{p_k+p_{k+1}}{2b} - \frac{p_{-1}+p_1}{2}\ln\frac{p_{-1}+p_1}{2b} -$$
$$-\sum_{k=1-m}^{-1}\frac{p_k+p_{k+1}}{2}\ln\frac{p_k+p_{k+1}}{2b} - \frac{p_{-m}}{2}\ln\frac{p_{-m}}{2b}.$$

Получается, что максимизирующее распределение P_X удовлетворяет условию $p_{-k} = p_k$, для $k = 1, \ldots$ Таким образом, перед нами стоит проблема оптимизации:

$$\text{максимизировать } G(\underline{p}) = -p_m\ln\frac{p_m}{2b} - \sum_{k=1}^{m-1}(p_k+p_{k+1})\ln\frac{p_k+p_{k+1}}{2b} - p_1\ln_2\frac{p_1}{b} \tag{4.1.35}$$

при условиях $p_k \geqslant 0$ и $2\sum\limits_{k=1}^{m} p_k = 1$. Лагранжиан $\mathcal{L}(P_X;\,\lambda)$ имеет вид

$$\mathcal{L}(P_X;\,\lambda) = G(\underline{p}) + \lambda(2p_1 + \ldots + 2p_m - 1)$$

и достигает максимума, когда

$$\frac{\partial}{\partial p_k}\mathcal{L}(P_X;\,\lambda) = 0, \quad k = 1, \ldots, m.$$

Итак, у нас есть m уравнений с одинаковыми п. ч.:

$$-\ln\frac{p_m(p_{m-1}+p_m)}{4b^2} - 2 + 2\lambda, \quad \text{т. е. } p_m(p_{m-1}+p_m) = 4b^2e^{2\lambda-2},$$
$$-\ln\frac{(p_{k-1}+p_k)(p_k+p_{k+1})}{4b^2} - 2 + 2\lambda = 0,$$
$$\text{т. е. } (p_{k-1}+p_k)(p_k+p_{k+1}) = 4b^2e^{2\lambda-2}, \quad 1 < k < m,$$
$$-\ln\frac{2p_1(p_1+p_2)}{4b^2} - 2 - 2\lambda = 0, \quad \text{т. е. } 2p_1(p_1+p_2) = 4b^2e^{2\lambda-2}.$$

Отсюда следует, что

$$\left.\begin{aligned} p_m &= p_{m-1} + p_{m-2} = \ldots = p_3 + p_2 = 2p_1, \\ p_m + p_{m-1} &= p_{m-2} + p_{m-3} = \ldots = p_2 + p_1 \end{aligned}\right\} \text{ для чётного } m$$

и

$$\left.\begin{aligned} &p_m = p_{m-1} + p_{m-2} = \ldots = p_2 + p_1, \\ &p_m + p_{m-1} = p_{m-2} + p_{m-3} = \ldots = p_3 + p_2 = 2p_1 \end{aligned}\right\} \text{ для нечётного } m.$$

При малых значениях $M = 2m$ решение получается легко. А именно, при $M = 2$ (два входных сигнала при $\pm A$ с $b = 2A$): $p_1 = 1/2$ и максимизирующая п. р. выходного сигнала равна

$$f_Y(y) = \begin{cases} 1/(4b), & A \leqslant y \leqslant 3A, \\ 1/(2b), & -A \leqslant y \leqslant A, \\ 1/(4b), & -3A \leqslant y \leqslant -A, \end{cases}$$

откуда $C^{\inf} = (\ln 2)/2$.

При $M = 4$ (четыре входных сигнала при $-A$, $-A/3$, $A/3$, A, где $b = 2A/3$): $p_1 = 1/6$, $p_2 = 1/3$, максимизирующая п. р. выходного сигнала имеет вид

$$f_Y(y) = \begin{cases} 1/(6b), & A \leqslant y \leqslant 5A/3 \ \text{ и } \ -5A/3 \leqslant y \leqslant -A, \\ 1/(4b), & 2A/3 \leqslant y \leqslant A \ \text{ и } \ -A \leqslant y \leqslant -2A/3, \\ 1/(6b), & -2A/3 \leqslant y \leqslant 2A/3, \end{cases}$$

что даёт $C^{\inf} = \ln(6^{1/2}4^{1/3}/2)$.

При $M = 6$ (шесть входных сигналов при $-A$, $-3A/5$, $-A/5$, $A/5$, $3A/5$, где $b = 2A/5$): $p_1 = 1/6$, $p_2 = 1/12$, $p_3 = 1/4$. Аналогично для $M = 8$ (восемь входных сигналов при $-A$, $-5A/7$, $-3A/7$ $-A/7$, $A/7$, $3A/7$, $5A/7$, A, где $b = 2A/7$): $p_1 = 1/10$, $p_2 = 3/20$, $p_3 = 1/20$, $p_4 = 1/5$.

В общей ситуации можно выразить все вероятности через p_1. А именно, для чётного m:

$$p_m = 2p_1,\ p_{m-1} = p_2 - p_1,\ p_{m-2} = 3p_1 - p_2,\ p_{m-3} = 2(p_2 - p_1),$$
$$p_{m-4} = 4p_1 - 2p_2,\ \ldots,\ p_3 = \left(\frac{m}{2} - 1\right)(p_2 - p_1),\ p_2 = \frac{m+2}{m}p_1,$$

откуда

$$\begin{aligned} &p_2 = \frac{m+2}{m}p_1,\ p_3 = \frac{m-2}{m}p_1,\ p_4 = \frac{m+4}{m}p_1,\ p_5 = \frac{m-4}{m}p_1,\ \ldots, \\ &p_{m-2} = \frac{2m-2}{m},\ p_{m-1} = \frac{2}{m},\ p_m = 2p_1, \quad p_1 = \frac{1}{2(m+1)}. \end{aligned} \tag{4.1.36}$$

Соответствующая п. р. даёт значения

$$h(Y) = -\frac{1}{2}\ln\frac{1}{4m(m+1)b^2} \ \text{ и } \ C_{\mathcal{A}}^{\inf} = -\frac{1}{2}\ln\frac{1}{4m(m+1)} - \ln 2. \tag{4.1.37}$$

С другой стороны, при нечётном m максимизирующее распределение P_X входного сигнала имеет вид

$$\begin{aligned} &p_1 = \frac{m+1}{2m(m+1)},\ \ p_2 = \frac{m-1}{2m(m+1)},\ \ p_3 = \frac{m+3}{2m(m+1)},\\ &p_4 = \frac{m-3}{2m(m+1)},\ \ \ldots,\ \ p_{m-1} = \frac{1}{2m(m+1)},\ \ p_m = \frac{m}{2m(m+1)}. \end{aligned} \tag{4.1.38}$$

Это даёт те же ответы для максимальной энтропии и ограниченной пропускной способности:

$$h(Y) = -\frac{1}{2}\ln\frac{1}{4m(m+1)b^2} \quad \text{и} \quad C_{\mathcal{A}}^{\inf} = -\frac{1}{2}\ln\frac{1}{4m(m+1)} - \ln 2. \tag{4.1.39}$$

В дальнейшем мы будем обозначать распределение входного сигнала из формул (4.1.36) и (4.1.38) через $\tilde{P}_X^{(A,2A/(2m-1))}$.

Замечание 4.1.15. Приведённые выше формулы дают максимум взаимной информации $I(X:Y)$, когда 1) с. в. шума $Z \sim \mathrm{U}(-b,\, b)$ не зависит от X и 2) распределение P_X входного сигнала задано на $[-A,\, A]$ с $b = 2A/(2m-1)$, но в любом другом отношении произвольно (здесь $I(X:Y)$ определяется в формуле (4.1.33)). Интересно найти этот максимум, когда A/b не является целым числом.

Когда b уменьшается от A/m до $A/(m+1)$ (или, что эквивалентно, A растёт от bm до $b(m+1)$), максимизирующее распределение $P_X^{(A,b)}$ трансформируется из $P_X^{(bm,b)}$ в $P_X^{(b(m+1),b)}$ при $A = b(m+1)/2$, т. е. $M = 2(m+1)$. Здесь $P_X^{(bm,b)}$ и $P_X^{(b(m+1),b)}$ заданы формулами (4.1.36) и (4.1.38).

Чтобы частично прояснить этот вопрос, рассмотрим случай, когда $A/2 \leqslant b \leqslant A$, и предположим, что распределение P_X входного сигнала имеет вид

$$P_X(-A) = P_X(A) = p \quad \text{и} \quad P_X(0) = 1 - 2p, \qquad 0 \leqslant p \leqslant \frac{1}{2}. \tag{4.1.40}$$

Тогда

$$h(Y) = -\frac{1}{b}\Big[Ap\ln\frac{p}{2b} + (2b-A)(1-p)\ln\frac{1-p}{2b} + (A-b)(1-2p)\ln\frac{1-2p}{2b}\Big],$$

и из равенства $dh(Y)/dp = 0$ следует условие

$$p^A = (1-p)^{2b-A}(1-2p)^{2(A-b)}. \tag{4.1.41}$$

При $b = A/2$ получаем $p^A = (1-2p)^A$, т. е. $p = 1-2p$, откуда $p = 1/3$. При $b = A$ имеем $p = 1/2$ в соответствии с ранее полученными результатами. При $b = 2A/3$ получаем, что

$$p^A = (1-p)^{A/3}(1-2p)^{2A/3}, \quad \text{т. е.} \quad p^3 = (1-p)(1-2p)^2. \tag{4.1.42a}$$

Нас интересуют решения, лежащие в $(0,\ 1/2)$ (на самом деле в $(1/3,\ 1/2)$). При $b = 3A/4$ уравнение (4.1.41) приобретает вид

$$p^A = (1-p)^{A/2}(1-2p)^{A/2}, \quad \text{т. е.} \quad p^2 = (1-p)(1-2p), \tag{4.1.42б}$$

откуда $p = (3-\sqrt{5})/2$. □

Пример 4.1.16. Полезно познакомиться с примером, когда с. в. шума Z состоит из двух компонент: дискретной и непрерывной, например

$$f_Z(z) = q\delta_0 + (1-q)\tilde{f}_Z(z),$$

т. е. $Z = 0$ с вероятностью q и суммарная вероятность ошибки равна $1-q$. Здесь мы рассмотрим случай

$$f_Z(z) = q\delta_0 + (1-q)\frac{1}{2b}\mathbf{1}(|z| \leqslant b)$$

и изучим ф. р. входного сигнала вида

$$P_X(-A) = p_{-1},\ \ P_X(0) = p_0,\ \ P_X(A) = p_1, \tag{4.1.43а}$$

где

$$p_{-1},\ p_0,\ p_1 \geqslant 0, \quad p_{-1} + p_0 + p_1 = 1, \tag{4.1.43б}$$

$b = A$ и $M = 3$ (три уровня сигнала на $(-A,\ A)$). Энтропия входного сигнала равна

$$h(X) = H(p_{-1},\ p_0,\ p_1) = -p_{-1}\ln p_{-1} - p_0 \ln p_0 - p_1 \ln p_1.$$

Ф. р. выходного сигнала выглядит как

$$f_Y(y) = q(p_{-1}\delta_{-A} + p_0\delta_0 + p_1\delta_A) + (1-q)\frac{1}{2b} \times$$
$$\times \left[p_{-1}\mathbf{1}(-2A \leqslant y \leqslant 0) + p_0\mathbf{1}(-A \leqslant y \leqslant A) + p_1\mathbf{1}(0 \leqslant y \leqslant 2A)\right],$$

а его энтропия $h(Y)$ (вычисленная относительно опорной меры μ на $\mathbb{R}$, абсолютно непрерывная компонента которой совпадает с мерой Лебега, а дискретная сопоставляет значение 1 точкам $-A$, 0 и A) задаётся формулой

$$h(Y) = \eta(q) - qh(p_{-1},\ p_0,\ p_1) - (1-q)A\Big[p_{-1}\ln\frac{p_{-1}}{2A} +$$
$$+ (p_{-1}+p_0)\ln\frac{p_{-1}+p_0}{2A} + (p_0+p_1)\ln\frac{p_0+p_1}{2A} + p_1\ln\frac{p_1}{2A}\Big].$$

По соображениям симметрии $h(Y)$ достигает максимума при $p_{-1} = p_1 = p$, $p_0 = 1-2h$ и нам нужно максимизировать по $p \in (0,\ 1)$ выражение

$$h(Y) = \eta(q) - qh(p,\ p,\ 1-2p) - (1-q)A\left[2p\ln\frac{p}{2A} + (1-2p)\ln\frac{1-2p}{2A}\right]$$

при данном $q \in (0, 1)$.

Дифференцируя, получаем

$$\frac{d}{dp}h(Y) = 0 \;\leftrightarrow\; \frac{p}{1-2p} = \left(\frac{p}{1-p}\right)^{-(1-q)A/q}.$$

Если $(1-q)A/q > 1$, то это уравнение даёт единственное решение, определяющее распределение P_X входного сигнала, как в формулах (4.1.43а) и (4.1.43б).

Если нас интересует значение q, доставляющее максимум $h(Y)$ (и, следовательно, максимум информационной пропускной способности), нам нужно дифференцировать по q:

$$\frac{d}{dq}h(Y) = 0 \;\leftrightarrow\; \log\frac{q}{1-q} = (A-1)h(p, p, 1-2p) - 2A\ln 2A.$$

Если мы хотим рассматривать входной сигнал с непрерывным распределением на $[-A, A]$ с п. р. $f_X(x)$, то п. р. выходной с. в. $Y = X + Z$ вычисляется через свёртку:

$$f_Y(y) = \frac{1}{2b}\int\limits_{(y-b)\vee(-A)}^{(y+b)\wedge A} f_X(x)dx.$$

Дифференциальная энтропия $h(Y) = -\int f_Y(y)\ln f_Y(y)dy$ в терминах f_X принимает вид

$$h(X+Z) = -\frac{1}{2b}\int\limits_{-A}^{A} f_X(x)\int\limits_{-b}^{b}\ln\left[\frac{1}{2b}\int\limits_{(x+z-b)\vee(-A)}^{(x+z+b)\wedge A} f_X(x')dx'\right]dzdx.$$

П. р. f_X, минимизирующая дифференциальную энтропию $h(X+Z)$ находится из вариационной задачи с ограничениями $f_X(x) \geqslant 0$, $\int\limits_{-A}^{A} f_X(x)dx = 1$.

Пример 4.1.17. Интересные задачи возникают при одновременной передаче по каналу нескольких скалярных сигналов. Предположим, что входной сигнал представляется точкой $\mathbf{x} = (x_1, x_2)$ на плоскости $\mathbb{R}^2$ и $Z \sim \mathrm{U}((-b, b)\times(-b, b))$ не зависит от входного сигнала. Тогда квадрат $S_b(\mathbf{x}) = (x_1 - b, x_1 + b)\times(x_2 - b, x_2 + b)$ с равномерной п. р. $1/(4b^2)$ изображает возможные положения выходного сигнала Y при данном $X = (x_1, x_2)$. Предположим, что нам предстоит работать с конечным алфавитом $\mathcal{A} \subset \mathbb{R}^2$, тогда область выходного сигнала представляет собой конечное объединение $\mathcal{B} = \bigcup\limits_{\mathbf{x}\in\mathcal{A}} S(\mathbf{x})$. По аналогии с примером 4.1.13, если мы сможем найти такое подмножество $\mathcal{A}' \subseteq \mathcal{A}$, что квадраты $S_b(\mathbf{x})$ с $\mathbf{x} \in \mathcal{A}'$ разбивают область $\mathcal{B}$ (т. е. покрывают $\mathcal{B}$, но не пересекаются друг

с другом), то для входной ф. р. $P_{\mathbf{x}}$, $P_{\mathbf{x}} = 1/(\#\mathcal{A}')$ (равномерное распределение над $\mathcal{A}'$), п. р. выходного вектор-сигнала f_Y будет равномерной на $\mathcal{B}$ (т. е. $f_Y(y) = 1/(\text{площадь } \mathcal{B})$). Следовательно, энтропия выходного сигнала $h(Y) = \ln(\text{площадь } \mathcal{B})$ достигает максимума среди всех ф. р. $P_{\mathbf{x}}$ входного сигнала, где $P_{\mathbf{x}}(\mathcal{A}) = 1$ (и даже достигает максимума среди всех ф. р. $P_{\mathbf{x}}$, где $P_{\mathbf{x}}(\mathcal{B}') = 1$, где $\mathcal{B}' \subset \mathcal{B}$ — произвольное подмножество с тем свойством, что $\bigcup\limits_{\mathbf{x}' \in \mathcal{B}'} S(\mathbf{x}')$ лежит внутри $\mathcal{B}$). Наконец, информационная пропускная способность рассматриваемого канала равна

$$C^{\inf}(\mathcal{B}) = \frac{1}{2} \ln \frac{\text{площадь } \mathcal{B}}{4b^2} \text{ nats/(скалярный входной сигнал)} \qquad (4.1.44)$$

(см. рис. 4.3).

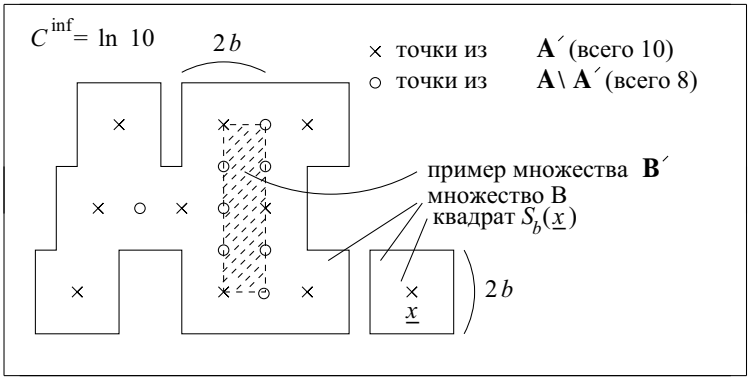


Рис. 4.3

Иначе говоря, любое ограниченное множество $\mathbb{D}_2 \subseteq \mathbb{R}^2$, которое можно разбить на непересекающиеся квадраты со стороной длины $2b$, даёт информационную пропускную способность $C^{\inf}(\mathbb{D}_2)$, ср. с формулой (4.1.44), аддитивного канала с равномерным шумом $\mathrm{U}((-b, b) \times (-b, b))$, где случайный входной вектор $\mathbf{x} = (X_1, X_2)$ удовлетворяет ограничению на доступную передаче область $\mathbf{x} \in \mathbb{D}_2$. Максимизирующая ф. р. входного вектора приписывает равные вероятности центрам квадратов, образующих разбиение.

Аналогичное заключение справедливо в $\mathbb{R}^3$, когда входной сигнал — это трёхмерный вектор $\mathbf{x} = (x_1, x_2, x_3)$, и т. д. В общей ситуации, когда мы используем K-мерный входной сигнал $\mathbf{x} = (x_1, \ldots, x_K) \in \mathbb{R}^K$ и ограничение на доступную передаче область $\mathbf{x} \in \mathbb{D}_K \subset \mathbb{R}^K$, где $\mathbb{D}_K$ — ограниченная область, которую можно разбить на непересекающиеся кубы с ребром $2b$,

информационная пропускная способность равна

$$C^{\inf}(\mathbb{D}_K) = \frac{1}{2}\ln\frac{\text{объём } \mathbb{D}_K}{(2b)^K} \text{ nats/(скалярный входной сигнал)}$$

и достигается на ф. р. $P_{\mathbf{x}}$ входного вектор-сигнала, сопоставляющей равные значения центрам кубов разбиения.

При $K \to \infty$ значение $C^{\inf}$ может сходиться к пределу $C^{\inf}_{\infty}$, дающему пропускную способность на скалярный входной сигнал при последовательности ограничений на доступные передаче области $\mathbb{D}_K$. Простейший пример такой ситуации — когда $\mathbb{D}_K = (-2bm, 2bm)^{\times K}$ — K-мерный куб. Тогда $C^{\inf}_K = \ln(1+m)$ не зависит от K (и канал не имеет памяти).

§ 4.2. А. с. р. в условиях непрерывного времени

> The errors of a wise man make your rule,
> Rather than perfections of a fool.
> Ошибки мудрого человека формируют ваши принципы,
> А не совершенство дурака.
>
> *Уильям Блейк* (1757–1821), английский поэт

В этом параграфе вы найдёте пропущенные моменты доказательства теоремы 4.1.8 и дальнейшие примеры. Начнём с серии примеров, иллюстрирующих свойство а. с. р. в различных формах. Центральные факты основаны на теореме Шеннона—Макмиллана—Бреймана (ШМБ), считающейся краеугольным камнем теории информации. Теорема ШМБ позволяет найти скорость передачи информации стационарным эргодическим процессом $\mathbf{X} = (X_n)$. Напомним, что преобразование пространства вероятностей T называется эргодичным, если каждое из множеств A, для которых $TA = A$, удовлетворяет условию $\mathsf{P}(A) = 0$ или 1. Для стационарного эргодического источника с конечным математическим ожиданием эргодическая теорема Биркгофа утверждает у. з. б. ч.:

$$\frac{1}{n}\sum_{i=1}^{n} X_i \to \mathsf{E}X. \tag{4.2.1}$$

Обычно для измеримой функции $f(X_i)$ эргодического процесса выполнено

$$\frac{1}{n}\sum_{i=1}^{n} f(X_i) \to \mathsf{E}f(X). \tag{4.2.2}$$

Теорема 4.2.1 (Шеннона—Макмиллана—Бреймана). *Для любого стационарного эргодичного процесса* $\mathbf{X}$ *с конечным математиче-*

ским ожиданием скорость передачи информации $R = h$, *т. е. предел в формуле* (4.2.3) *существует почти всюду и равен энтропии*,

$$-\lim_{n\to\infty}\frac{1}{n}\log p_{\mathbf{X}_0^{n-1}}(\mathbf{X}_0^{n-1}) = h \text{ п.в.} \tag{4.2.3}$$

Доказательство теоремы 4.2.1 основано на нескольких вспомогательных утверждениях и приводится в конце этого параграфа.

Пример 4.2.2 (общее а. с. р.). Для данной последовательности с. в. $X_1, X_2, \ldots$ для всех $N = 1, 2, \ldots$ распределение случайного вектора $\mathbf{X}_1^N = \begin{pmatrix} X_1 \\ \vdots \\ X_N \end{pmatrix}$ определяется ф. р. $f_{\mathbf{X}_1^N}(\mathbf{x}_1^N)$ относительно меры $\mu^{(N)} = \underbrace{\mu \times \ldots \times \mu}_{N}$. Допустим, что выполнено утверждение теоремы ШМБ:

$$-\frac{1}{N}\log f_{\mathbf{X}_1^N}(\mathbf{X}_1^N) \xrightarrow{\mathsf{P}} h,$$

где $h > 0$ — константа (обычно $h = \lim\limits_{i\to\infty} h(X_i)$), а $\xrightarrow{\mathsf{P}}$ — сходимость по вероятности. При данном $\varepsilon > 0$ рассмотрим типичное множество

$$T_\varepsilon^N = \left\{ \mathbf{X}_1^N = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} : -\varepsilon \leqslant \frac{1}{N}\log f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) + h \leqslant \varepsilon \right\}.$$

Объём $\mu^{(N)}(T_\varepsilon^N) = \int\limits_{T_\varepsilon^N} \mu(dx_1)\ldots\mu(dx_N)$ множества T_ε^N обладает следующим свойством:

$$\mu^{(N)}(T_\varepsilon^N) \leqslant 2^{N(h+\varepsilon)} \ \forall \varepsilon,\ N \tag{4.2.4}$$

и при $0 < \varepsilon < h$ и любого $\delta > 0$ выполнено неравенство

$$\mu^{(N)}(T_\varepsilon^N) \geqslant (1-\delta)2^{N(h-\varepsilon)} \text{ при достаточно большом } N, \text{ зависящем от } \delta. \tag{4.2.5}$$

Решение. Поскольку $\mathsf{P}(\mathbb{R}^N) = \int\limits_{\mathbb{R}^N} f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) \prod\limits_{j=1}^N \mu(dx_j) = 1$, мы получаем, что

$$1 = \int\limits_{\mathbb{R}^N} f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) \prod_{j=1}^N \mu(dx_j) \geqslant \int\limits_{T_\varepsilon^N} f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) \prod_{j=1}^N \mu(dx_j) \geqslant$$

$$\geqslant 2^{-N(h+\varepsilon)} \int\limits_{T_\varepsilon^N} \prod_{j=1}^N \mu(dx_j) = \geqslant 2^{-N(h+\varepsilon)} \mu^{(N)}(T_\varepsilon^N),$$

откуда следует верхняя граница для (4.2.4). С другой стороны, при данном $\delta > 0$ мы можем взять N столь большим, что $\mathsf{P}(T_\varepsilon^N) \geqslant 1 - \delta$. В этом случае при $0 < \varepsilon < h$ имеем

$$1 - \delta \leqslant \mathsf{P}(T_\varepsilon^N) = \int\limits_{T_\varepsilon^N} f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) \prod_{j=1}^N \mu(dx_j) \leqslant$$
$$\leqslant 2^{-N(h-\varepsilon)} \int\limits_{T_\varepsilon^N} \prod_{j=1}^N \mu(dx_j) = 2^{-N(h-\varepsilon)} \mu^{(N)}(T_\varepsilon^N).$$

Это даёт нижнюю границу в формуле (4.2.5). □

Следующим шагом мы обобщаем а. с. р. на совместное распределение пар $\mathbf{X}_1^N$, $\mathbf{Y}_1^N$ (в приложениях $\mathbf{X}_1^N$ играет роль входного, а $\mathbf{Y}_1^N$ — выходного сигналов). Пусть даны две последовательности с. в. $X_1, X_2, \ldots$ и $Y_1, Y_2, \ldots$ Для всех $N = 1, 2, \ldots$ рассмотрим совместное распределение случайных векторов $\mathbf{X}_1^N = \begin{pmatrix} X_1 \\ \vdots \\ X_N \end{pmatrix}$ и $\mathbf{Y}_1^N = \begin{pmatrix} Y_1 \\ \vdots \\ Y_N \end{pmatrix}$, определяемые (совместной) ф. в. $f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}$ относительно меры $\mu^{(N)} \times \nu^{(N)}$, где $\underbrace{\mu^{(N)} = \mu \times \ldots \times \mu}_{N}$ и $\underbrace{\nu^{(N)} = \nu \times \ldots \times \nu}_{N}$. Символами $f_{\mathbf{X}_1^N}$ и $f_{\mathbf{Y}_1^N}$ обозначим (совместные) ф. в. векторов $\mathbf{X}_1^N$ и $\mathbf{Y}_1^N$ соответственно.

Как и в примере 4.2.2, мы предполагаем, что выполнены утверждения теоремы ШМБ, на этот раз для пары $(\mathbf{X}_1^N, \mathbf{Y}_1^N)$ и каждого вектора $\mathbf{X}_1^N$ и $\mathbf{Y}_1^N$ при $N \to \infty$:

$$-\frac{1}{N} \log f_{\mathbf{X}_1^N}(\mathbf{X}_1^N) \xrightarrow{\mathsf{P}} h_1, \quad -\frac{1}{N} \log f_{\mathbf{Y}_1^N}(\mathbf{Y}_1^N) \xrightarrow{\mathsf{P}} h_2, \quad -\frac{1}{N} \log f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}(\mathbf{X}_1^N, \mathbf{Y}_1^N) \xrightarrow{\mathsf{P}} h,$$

где h, h_1, h_2 — положительные константы,

$$h_1 + h_2 \geqslant h \tag{4.2.6}$$

(как правило, $h_1 = \lim\limits_{i \to \infty} h(X_i)$, $h_2 = \lim\limits_{i \to \infty} h(Y_i)$, $h = \lim\limits_{i \to \infty} h(X_i, Y_i)$ и $h_1 + h_2 - h = \lim\limits_{i \to \infty} I(X_i : Y_i)$). Для данного $\varepsilon > 0$ рассмотрим типичное множество, образованное парами отсчётов $(\mathbf{x}_1^N, \mathbf{y}_1^N)$, где $\mathbf{x}_1^N = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$ и $\mathbf{y}_1^N = \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}$. Формально,

$$T_\varepsilon^N = \Big\{ (\mathbf{x}_1^N, \mathbf{y}_1^N) \colon -\varepsilon \leqslant \frac{1}{N} \log f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) + h_1 \leqslant \varepsilon,$$
$$-\varepsilon \leqslant \frac{1}{N} \log f_{\mathbf{Y}_1^N}(\mathbf{y}_1^N) + h_2 \leqslant \varepsilon, \; -\varepsilon \leqslant \frac{1}{N} \log f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) + h \leqslant \varepsilon \Big\}; \tag{4.2.7}$$

по предположениям имеем $\lim\limits_{N\to\infty} \mathsf{P}(T_\varepsilon^N) = 1\ \forall \varepsilon > 0$. Далее найдём объём множества T_ε^N:

$$\mu^{(N)} \times \nu^{(N)}(T_\varepsilon^N) = \int\limits_{T_\varepsilon^N} \mu^{(N)}(d\mathbf{x}_1^N)\nu^{(N)}(d\mathbf{y}_1^N).$$

Рассмотрим, наконец, независимую пару $(\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N)$, компонента которой с. в. $\tilde{\mathbf{X}}_1^N$ распределена так же, как и $\mathbf{X}_1^N$, а $\tilde{\mathbf{Y}}_1^N$ — как $\mathbf{Y}_1^N$, т. е. совместная ф. в. с. в. $\tilde{\mathbf{X}}_1^N$ и $\tilde{\mathbf{Y}}_1^N$ имеет вид

$$f_{\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) = f_{\mathbf{X}_1^N}(\tilde{\mathbf{x}}_1^N) f_{\tilde{\mathbf{Y}}_1^N}(\mathbf{y}_1^N). \tag{4.2.8}$$

Далее мы оценим объём множества T_ε^N, а затем вероятность того, что $(\tilde{\mathbf{x}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N$.

Пример 4.2.3 (общее совместное а. с. р.). 1. Объём типичного множества обладает следующими свойствами:

$$\mu^{(N)} \times \nu^{(N)}(T_\varepsilon^N) \leqslant 2^{N(h+\varepsilon)}\ \forall \varepsilon, N, \tag{4.2.9}$$

и при любом $\delta > 0$ и $0 < \varepsilon < h$ при достаточно больших N, зависящих от δ выполнено неравенство

$$\mu^{(N)} \times \nu^{(N)}(T_\varepsilon^N) \geqslant (1-\delta)2^{N(h-\varepsilon)}. \tag{4.2.10}$$

2. Для независимой пары $(\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N)$ имеем

$$\mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N) \leqslant 2^{-N(h_1+h_2-h-3\varepsilon)}\ \forall \varepsilon, N, \tag{4.2.11}$$

а для любого $\delta > 0$ при достаточно большом N, зависящем от δ, выполнено неравенство

$$\mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N) \geqslant (1-\delta)2^{-N(h_1+h_2-h+3\varepsilon)}\ \forall \varepsilon. \tag{4.2.12а}$$

Решение. Доказательство утверждения 1 полностью повторяет доказательство формул (4.2.4) и (4.2.5) с интегрированием $f_{\mathbf{X}_1^N \mathbf{Y}_1^N}$.

2. Для вероятности $\mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N)$ формула (4.2.11) получается следующим образом:

$$\text{по определению } \mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N) = \int\limits_{T_\varepsilon^N} f_{\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N}(\tilde{\mathbf{x}}_1^N, \tilde{\mathbf{y}}_1^N)\mu(d\tilde{\mathbf{x}}_1^N)\nu(d\tilde{\mathbf{y}}_1^N) =$$

$$= (\text{подставляем соотношение (4.2.8)}) \int\limits_{T_\varepsilon^N} f_{\tilde{\mathbf{X}}_1^N}(\tilde{\mathbf{x}}_1^N) f_{\tilde{\mathbf{Y}}_1^N}(\mathbf{y}_1^N)\mu(d\tilde{\mathbf{x}}_1^N)\nu(d\tilde{\mathbf{y}}_1^N) \leqslant$$

$$\leqslant (\text{согласно формуле (4.2.7)})\ 2^{-N(h_1-\varepsilon)}2^{-N(h_2-\varepsilon)} \int\limits_{T_\varepsilon^N} \mu(d\tilde{\mathbf{x}}_1^N)\nu(d\tilde{\mathbf{y}}_1^N) \leqslant$$

$$\leqslant (\text{учитываем границу (4.2.9)})\ 2^{-N(h_1-\varepsilon)}2^{-N(h_2-\varepsilon)}2^{N(h+\varepsilon)} = 2^{-N(h_1+h_2-h-3\varepsilon)}. \tag{4.2.12б}$$

Наконец, обращая неравенства в последних двух строчках, мы можем привести их к виду

$$\text{п. ч. (4.2.12б) (согласно (4.2.7))} \geqslant 2^{-N(h_1+\varepsilon)}2^{-N(h_2+\varepsilon)} \int\limits_{T_\varepsilon^N} \mu(d\tilde{\mathbf{x}}_1^N)\nu(d\tilde{\mathbf{y}}_1^N) \geqslant$$

$$\geqslant (\text{ввиду границы (4.2.10)})(1-\delta)2^{-N(h_1+\varepsilon)}2^{-N(h_2+\varepsilon)}2^{N(h-\varepsilon)} =$$

$$= (1-\delta)2^{-N(h_1+h_2-h+3\varepsilon)}.$$

Формально мы здесь предполагаем, что $0 < \varepsilon < h$ (так как это предполагалось в формуле (4.2.10)), но увеличение ε делает множитель $2^{-N(h_1+h_2-h+3\varepsilon)}$ только меньше. Это доказывает ограничение (4.2.12а). □

Более наглядно и геометрично обобщение а. с. р., где мы предполагаем, что утверждения теоремы ШМБ выполняются непосредственно для отношения $f_{\mathbf{X}_1^N,\mathbf{Y}_1^N}(\mathbf{X}_1^N, \mathbf{Y}_1^N)/(f_{\mathbf{X}_1^N}(\mathbf{X}_1^N)f_{\mathbf{Y}_1^N}(\mathbf{Y}_1^N))$, т. е.

$$\frac{1}{N}\log\frac{f_{\mathbf{X}_1^N,\mathbf{Y}_1^N}(\mathbf{X}_1^N, \mathbf{Y}_1^N)}{f_{\mathbf{X}_1^N}(\mathbf{X}_1^N)f_{\mathbf{Y}_1^N}(\mathbf{Y}_1^N)} \xrightarrow{\mathsf{P}} c, \tag{4.2.13}$$

где $c > 0$ — константа. Напомним, что $f_{\mathbf{X}_1^N,\mathbf{Y}_1^N}$ — это совместная ф. в., тогда как $f_{\mathbf{X}_1^N}$ и $f_{\mathbf{Y}_1^N}$ — индивидуальные ф. в. случайных входного и выходного векторов $\mathbf{X}^N$ и $\mathbf{Y}^N$ относительно мер $\mu^{(N)}$ и $\nu^{(N)}$:

$$f_{\mathbf{X}_1^N,\mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) = f_{\mathbf{X}_1^N}(\mathbf{x}_1^N)f_{\mathrm{ch}}(\mathbf{y}_1^N|\mathbf{x}_1^N \text{ послано}),$$

$$f_{\mathbf{Y}_1^N}(\mathbf{y}_1^N) = \int f_{\mathbf{X}_1^N,\mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N)\mu^{(N)}(d\mathbf{x}_1^N).$$

Здесь для $\varepsilon > 0$ рассматривается типичное множество вида

$$T_\varepsilon^N = \left\{(\mathbf{x}_1^N, \mathbf{y}_1^N)\colon\ -\varepsilon \leqslant \frac{1}{N}\log\frac{f_{\mathbf{X}_1^N,\mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N)}{f_{\mathbf{X}_1^N}(\mathbf{x}_1^N)f_{\mathbf{Y}_1^N}(\mathbf{y}_1^N)} - c \leqslant \varepsilon\right\}; \tag{4.2.14}$$

по предположению (4.2.13) мы получаем, что при любом $\varepsilon > 0$ выполняется равенство $\lim\limits_{N\to\infty} \mathsf{P}((\mathbf{X}_1^N, \mathbf{Y}_1^N) \in T_\varepsilon^N) = 1$.

Опять рассмотрим независимую пару $(\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N)$, где ф. в. компоненты $\tilde{\mathbf{X}}_1^N$ совпадает с ф. в. $\mathbf{X}_1^N$, а ф. в. компоненты $\tilde{\mathbf{Y}}_1^N$ — с ф. в. $\mathbf{X}_1^N$.

Теорема 4.2.4 (отклонение от совместного а. с. р.). *Предположим, что выполнено свойство* (4.2.13). *Если* $(\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N)$ *— случайная пара, то вероятность события* $(\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N$ *подчиняется неравенству*

$$\mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N) \leqslant 2^{-N(c-\varepsilon)}\ \forall\varepsilon,\ N \tag{4.2.15}$$

и для произвольного $\delta > 0$ *и достаточно большого* N, *зависящего от* δ *выполняется неравенство*

$$\mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N) \geqslant (1-\delta)2^{-N(c+\varepsilon)} \ \forall \varepsilon. \tag{4.2.16}$$

Доказательство. И вновь мы получаем неравенство (4.2.15) следующим образом:

$$\text{(по определению) } \mathsf{P}((\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N) \in T_\varepsilon^N) = \int\limits_{T_\varepsilon^N} f_{\tilde{\mathbf{X}}_1^N, \tilde{\mathbf{Y}}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) \mu^{\times N}(d\mathbf{x}_1^N) \nu^{\times N}(d\mathbf{y}_1^N) =$$

$$= \text{(подставляя (4.2.8))} \int\limits_{T_\varepsilon^N} f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) f_{\mathbf{Y}_1^N}(\mathbf{y}_1^N) \mu(d\mathbf{x}_1^N) \nu(d\mathbf{y}_1^N) =$$

$$= \text{(по прямому вычислению)} \int\limits_{T_\varepsilon^N} \exp\left[-\log \frac{f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N)}{f_{\mathbf{X}_1^N}(\mathbf{x}_1^N) f_{\mathbf{Y}_1^N}(\mathbf{y}_1^N)}\right] \times$$

$$\times f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) \mu^{\times N}(d\mathbf{x}_1^N) \nu^{\times N}(d\mathbf{y}_1^N) \leqslant$$

$$\leqslant \text{(ввиду ограничения (4.2.14))} \ 2^{-N(c-\varepsilon)} \int\limits_{T_\varepsilon^N} f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) \mu(d\mathbf{x}_1^N) \nu(d\mathbf{y}_1^N) =$$

$$= 2^{-N(c-\varepsilon)} \mathsf{P}((\mathbf{X}_1^N, \mathbf{Y}_1^N) \in T_\varepsilon^N) \leqslant 2^{-N(c-\varepsilon)}.$$

Наконец, обращая неравенства в двух последних строчках, мы получаем ограничение (4.2.16):

$$\geqslant 2^{-N(c+\varepsilon)} \int\limits_{T_\varepsilon^N} f_{\mathbf{X}_1^N, \mathbf{Y}_1^N}(\mathbf{x}_1^N, \mathbf{y}_1^N) \mu(d\mathbf{x}_1^N) \nu(d\mathbf{y}_1^N) =$$

$$= \text{(из-за (4.2.14))} \ 2^{-N(c+\varepsilon)} \mathsf{P}((\mathbf{X}_1^N, \mathbf{Y}_1^N) \in T_\varepsilon^N) \geqslant 2^{-N(c+\varepsilon)}(1-\delta). \quad \square$$

Пример 4.2.5. Пусть $\mathbf{x} = \{X(1), \ldots, X(n)\}$ — вектор (набор с. в.) и $\mathbf{x}(C)$ — поднабор $\{X(i)\colon i \in C\}$, где C — непустое подмножество индексов $\{1, \ldots, n\}$. Предположим, что совместное распределение для любого поднабора $\mathbf{x}(C)$ с $\#C = k$, $1 \leqslant k \leqslant n$ задаётся совместной ф. в. $f_{\mathbf{x}(C)}$ относительно меры $\mu \times \ldots \times \mu$ (k сомножителей, каждый из которых соответствует с. в. $X(i)$ с $i \in C$). Аналогично имея вектор $\mathbf{x} = \begin{pmatrix} x(1) \\ \vdots \\ x(n) \end{pmatrix}$, обозначим через $\mathbf{x}(C)$ подвектор, полученный из исходного выбором строчек с номерами $i \in C$. Для любого разбиения $\{C_1, \ldots, C_s\}$ множества $\{1, \ldots, n\}$ на непересекающиеся подмножества $C_1, \ldots, C_s$ (с $1 \leqslant s \leqslant n$) по неравенству Гиббса получаем, что

$$\int f_{\mathbf{x}_1^n}(\mathbf{x}) \log \frac{f_{\mathbf{x}_1^n}(\mathbf{x})}{f_{\mathbf{x}(C_1)}(\mathbf{x}(C_1)) \ldots f_{\mathbf{x}(C_s)}(\mathbf{x}(C_s))} \prod_{j=1}^n \mu(dx(j)) \geqslant 0. \tag{4.2.17}$$

При каком разбиении интеграл в (4.2.17) достигает своего максимума?

Решение. Разбиение, о котором идёт речь, состоит из $s = n$ одноточечных подмножеств. Действительно, рассмотрим разбиение множества $\{1, \ldots, n\}$ на отдельные точки. Соответствующий интеграл будет равен

$$\int f_{\mathbf{x}_1^n}(\mathbf{x}) \log \frac{f_{\mathbf{x}_1^N}(\mathbf{x})}{\prod_{i=1}^{n} f_{X_i}(x_i)} \prod_{j=1}^{n} \mu(dx(j)). \tag{4.2.18}$$

Пусть $\{C_1, \ldots, C_s\}$ — произвольное разбиение множества $\{1, \ldots, n\}$. Преобразовывая дробь, стоящую под логарифмом, в произведение совместных ф. в. $\prod_{i=1}^{s} f_{\mathbf{x}(C_i)}(\mathbf{x}(C_i))$, получим интеграл (4.2.18) в виде суммы

$$\int f_{\mathbf{x}_1^n}(\mathbf{x}) \log \frac{f_{\mathbf{x}_1^N}(\mathbf{x})}{\prod_{i=1}^{n} f_{\mathbf{x}(C_i)\mathbf{x}(C_i)}} \prod_{j=1}^{n} \mu(dx(j)) + \text{неотрицательные члены.}$$

Отсюда следует ответ. □

Пример 4.2.6. Пусть $\mathbf{x} = \{X(1), \ldots, X(n)\}$ — такой набор с. в., как в примере 4.2.5, а Y — другая с. в. Предположим, что существует совместная ф. в. $f_{\mathbf{x},Y}$ относительно меры $\mu^{(n)} \times \nu$, где $\mu^{(n)} = \underbrace{\mu \times \ldots \times \mu}_{n}$. Для подмножества $C \subseteq \{1, \ldots, n\}$ рассмотрим сумму

$$I(\mathbf{x}(C) : Y) + \mathsf{E}[I(\mathbf{x}(\bar{C} : Y)|\mathbf{x}(C)].$$

Здесь $\mathbf{x}(C) = \{X(i) \colon i \in C\}$, $\mathbf{x}(\bar{C}) = \{X(i) \colon i \notin C\}$ и $\mathsf{E}[I(\mathbf{x}(\bar{C} : Y)|\mathbf{x}(C)]$ обозначает условное среднее с. в. $I(\mathbf{x}(\bar{C} : Y)$ при условии $\mathbf{x}(C)$. Докажите, что сумма не зависит от выбора множества C.

Решение. Достаточно проверить, что интересующее нас выражение равно $I(\mathbf{x} : Y)$. □

В §4.3 нам потребуются следующие факты о параллельных каналах (или их произведении).

Пример 4.2.7 (лемма А в [W1]; см. также [W2]). Покажите, что пропускная способность r параллельных дискретных по времени гауссовских каналов с параметрами $(\alpha_j, p^{(j)}, \sigma_j^2)$ равна

$$C = \sum_{j=1}^{r} \frac{\alpha_j}{2} \ln \left(1 + \frac{p^{(j)}}{\alpha_j \sigma_j^2}\right). \tag{4.2.19}$$

Более того это равенство остаётся верным, даже когда некоторые из α_j обращаются в $+\infty$; в этом случае соответствующее слагаемое принимает вид $p^{(j)}/\sigma_j^2$. Здесь $p^{(j)}$ — ограничение по мощности j-го канала.

Решение. Допустим, что мультивекторные данные $\mathbf{x} = \{x_1, \ldots, x_r\}$ передаются по r параллельным каналам пропускных способностей $C_1, \ldots, C_r$, где каждый вектор $x_j = \begin{pmatrix} x_{j1} \\ \vdots \\ x_{jn_j} \end{pmatrix} \in \mathbb{R}^{n_j}$. Удобно положить $n_j = \lceil \alpha_j \tau \rceil$, где $\tau \to \infty$. Ясно, что пропускная способность такого произведения каналов равна сумме $\sum_{i=1}^{r} C_i$. Используя индукцию, достаточно рассмотреть случай $r = 2$. Для доказательства прямой части предположим, что $R < C_1 + C_2$ и дано $\varepsilon > 0$. При достаточно большом τ нам нужно найти код для произведения каналов с $M = e^{R\tau}$ кодовыми словами и $P_e < \varepsilon$. Положим $\eta = (C_1 + C_2 - R)/2$. Пусть $\mathcal{X}^1$ и $\mathcal{X}^2$ — коды, предназначенные каналам 1 и 2, соответственно $M_1 \sim e^{(C_1 - \eta)\tau}$ и $M_2 \sim e^{(C_2 - \eta)\tau}$, и вероятности ошибок удовлетворяют неравенству $P_e^{\mathcal{X}^1}, P_e^{\mathcal{X}^2} \leqslant \varepsilon/2$. Построим код сцепления $\mathcal{X}$ с кодовыми словами $v = x_k^1 x_l^2$, где $x_\bullet^i \in \mathcal{X}^i$, $i = 1, 2$. Тогда для рассматриваемого произведения каналов с кодами $\mathcal{X}^1$ и $\mathcal{X}^2$ вероятность ошибки $P_e^{\mathcal{X}^1, \mathcal{X}^2}$ имеет вид

$$P_e^{\mathcal{X}^1, \mathcal{X}^2} = \frac{1}{M_1 M_2} \sum_{k=1}^{M_1} \sum_{l=1}^{M_2} \mathsf{P}(\text{ошибка в канале 1 или 2} | x_k^1 x_l^2 \text{ послано}).$$

В силу независимости каналов получаем, что $P_e^{\mathcal{X}^1, \mathcal{X}^2} \leqslant P_e^{\mathcal{X}^1} + P_e^{\mathcal{X}^2} \leqslant \varepsilon$, откуда следует прямая часть.

Доказательство обратной части намного сложнее, и мы представим лишь его набросок, порекомендовав интересующемуся читателю работу [W2]. Идея состоит в применении так называемого списка декодирования: предположим, что у нас есть код $\mathcal{Y}$ размера и правило декодирования $d = d^{\mathcal{Y}}$. Далее, при получении на выходе канала вектора $\mathbf{y}$ генерируется список L возможных кодовых слов из $\mathcal{Y}$ с помощью декодера $\tilde{d} = \tilde{d}^{\mathcal{Y}}_{\text{list}}$. Декодирование (основанное на правиле $\tilde{d}$) считается удачным, если правильное слово попало в список. Тогда средняя вероятность ошибки $P_e = P_e^{\mathcal{Y}}(d)$ при использовании кода $\mathcal{Y}$ удовлетворяет следующему неравенству:

$$P_e \geqslant P_e(\tilde{d}) P_e^{\text{av}}(L, d), \tag{4.2.20}$$

где вероятность ошибки $P_e(\tilde{d}) = P^{\mathcal{Y}}(\tilde{d})$ отсылает к списку декодирования и $P_e^{\text{av}}(L, d) = P_e^{\text{av}}(\mathcal{Y}, L, d)$ обозначает вероятность ошибки при использовании декодера d, усреднённую по всем подкодам в $\mathcal{Y}$ размера L.

Возвращаясь теперь к произведению каналов пропускных способностей C_1 и C_2, выберем $R > C_1 + C_2$, положим $\eta = (R - C_1 - C_2)/2$, и пусть размер списка будет равен $L = e^{R_L \tau}$ с $R_L = C_2 + \eta$. Предположим, что мы

пользуемся кодом $\mathcal{Y}$ размера $e^{R\tau}$ с декодером d и списком декодирования $\tilde{d}$ размера L. На основе неравенства (4.2.20) запишем

$$P_e \geqslant P_e(\tilde{d})P_e^{\mathrm{av}}(e^{R_L\tau},\, d) \tag{4.2.21}$$

и воспользуемся тем фактом, что $R_L > C_2$, а величина $P_e^{\mathrm{av}}(e^{R_L\tau},\, d)$ отделена от нуля. Утверждение обратной части вытекает из следующего наблюдения, которое будет обсуждаться в примере 4.2.8: возьмём $R_2 < R - R_L$ и рассмотрим подкоды $\mathcal{L} \subset \mathcal{Y}$ размера $\#\mathcal{L} = e^{R_2\tau}$. Предположим, что мы выбираем подкод $\mathcal{L}$ случайно, с равномерной вероятностью. Пусть $M_2 = e^{R_2\tau}$ и $P_e^{\mathcal{Y},M_2}(d)$ обозначает среднее значение вероятности ошибки, усреднённой по всем подкодам $\mathcal{L} \subset \mathcal{Y}$ размера $\#\mathcal{L} = e^{R_2\tau}$. Тогда

$$P_e(\tilde{d}) \geqslant P_e^{\mathcal{Y},M_2}(d) + \varepsilon(\tau), \tag{4.2.22}$$

где $\varepsilon(\tau) \to 0$ при $\tau \to \infty$. □

Пример 4.2.8. Пусть $L = e^{R_L\tau}$ и $M = e^{R\tau}$. Мы хотим показать, что если $R_2 < R - R_L$ и $M_2 = e^{R_2\tau}$, то выполнено следующее. Для данного кода $\mathcal{X}$ размера M, декодера d и списка декодирования $\tilde{d}$ размера L рассмотрим среднюю вероятность ошибки $P_e^{\mathcal{X},M_2}(d)$, усреднённую по всем равномерно распределённым подкодам $\mathcal{S} \subset \mathcal{X}$ размера $\#\mathcal{S} = M_2$. Тогда $P_e^{\mathcal{X},M_2}(d)$ и вероятность ошибки списка $P_e^{\mathcal{X}}(\tilde{d})$ подчиняются неравенству

$$P_e^{\mathcal{X}}(\tilde{d}) \geqslant P_e^{\mathcal{X},M_2}(d) + \varepsilon(\tau), \tag{4.2.23}$$

где $\varepsilon(\tau) \to 0$ при $\tau \to \infty$.

Решение. Пусть $\mathcal{X}$, $\mathcal{S}$ и d такие, как в условии, и предположим, что используется список декодирования $\tilde{d}$ длины L.

Для подкода $\mathcal{S} \subset \mathcal{X}$ с M_2 кодовыми словами будем применять следующую процедуру декодирования. Пусть $\mathcal{L}$ — результат декодера $\tilde{d}$. Если в $\mathcal{L}$ попадает ровно один элемент $x_j \in \mathcal{S}$, то y декодируется как x_j. В противном случае сообщается об ошибке. Обозначим декодирующий элемент для $\mathcal{S}$ через $d^{\mathcal{S}}$. Таким образом, если передан элемент $x_k \in \mathcal{S}$, то результирующая вероятность ошибки при использовании только что описанного правила декодирования принимает вид

$$P_{ek} = \sum_{\mathcal{L}} p(\mathcal{L}|x_k)E_{\mathcal{S}}(\mathcal{L}|x_k),$$

где $p(\mathcal{L}|x_k)$ — вероятность получить $\mathcal{L}$ на выходе после передачи x_k при использовании правила $d^{\mathcal{X}}$, а $E_{\mathcal{S}}(\mathcal{L}|x_k)$ — вероятность ошибки для $d^{\mathcal{S}}$. Запишем далее, $E_{\mathcal{S}}(\mathcal{L}|x_k) = E_{\mathcal{S}}^1(\mathcal{L}|x_k) + E_{\mathcal{S}}^2(\mathcal{L}|x_k)$, где $E_{\mathcal{S}}^1(\mathcal{L}|x_k)$ обозначает вероятность того, что $x_k \notin \mathcal{L}$, а $E_{\mathcal{S}}^2(\mathcal{L}|x_k)$ — того, что слово $x_k \in \mathcal{L}$ было декодировано ошибочным словом из $\mathcal{L}$ (обе вероятности условные при

условии, что послано слово x_k). Далее, $E^2_{\mathcal{S}}(\mathcal{L}|x_k)$ расщепляется в сумму (условных) вероятностей $E^2_{\mathcal{S}}(\mathcal{L}, x_j|x_k)$ того, что декодер вернул слово $x_j \in \mathcal{L}$, $j \neq k$.

Пусть $P_e^{\mathcal{S}}(d) = P_e^{\mathcal{S},\mathrm{av}}(d)$ обозначает среднюю вероятность ошибки для подкода $\mathcal{S}$. Тогда из описанной конструкции получаем

$$P_e^{\mathcal{S}}(d) \leqslant \frac{1}{M_2} \sum_{k:\, x_k \in \mathcal{S}} \sum_{\mathcal{L}} p(\mathcal{L}|x_k) \left[W^1_{\mathcal{S}}(\mathcal{L}|x_k) + \sum_{j \neq k} E^2_{\mathcal{S}}(\mathcal{L}, x_j|x_k) \right]. \quad (4.2.24)$$

Неравенство (4.2.24) выполнено для любого подкода $\mathcal{S}$. Теперь будем из $\mathcal{X}$ выбирать подкод $\mathcal{S}$ размера M_2 случайным образом с равномерным распределением вероятностей. После усреднения по всем таким подкодам мы получим границу для средней вероятности ошибки $P_e^{\mathcal{X},M_2} = P_e^{\mathcal{X},M_2}(d)$:

$$P_e^{\mathcal{X},M_2} \leqslant P_e^{\mathcal{X}}(\tilde{d}) + \frac{1}{M_2} \sum_{k=1}^{M_2} \sum_{\mathcal{L}} \sum_{j \neq k} \langle p(\mathcal{L}|x_k) E^2_{\bullet}(\mathcal{L}, x_j|x_k) \rangle^{\mathcal{X},M_2}, \quad (4.2.25)$$

где $\langle \ \ \rangle^{\mathcal{X},M_2}$ означает усреднение по всем выбранным подкодам. Поскольку x_j и x_k выбираются независимо, получаем, что

$$\langle p(\mathcal{L}|x_k) E^2_{\bullet}(\mathcal{L}, x_j|x_k) \rangle^{\mathcal{X},M_2} = \langle p(\mathcal{L}|x_k) \rangle^{\mathcal{X},M_2} \langle E^2_{\bullet}(\mathcal{L}, x_j|x_k) \rangle^{\mathcal{X},M_2}.$$

Далее,

$$\langle p(\mathcal{L}|x_k) \rangle^{\mathcal{X},M_2} = \sum_{x \in \mathcal{X}} \frac{1}{M} p(\mathcal{L}|x), \quad \langle E^2_{\bullet}(\mathcal{L}, x_j|x_k) \rangle^{\mathcal{X},M_2} = \frac{L}{M},$$

и мы получаем

$$P_e^{\mathcal{X},M_2} \leqslant P_e^{\mathcal{X}}(\tilde{d}) + \frac{1}{M_2} \sum_{k=1}^{M_2} \sum_{\mathcal{L}} \left(\sum_{x \in \mathcal{X}} \frac{1}{M} p(\mathcal{L}|x) \right) \left(\sum_{j \neq k} \frac{L}{M} \right),$$

откуда

$$P_e^{\mathcal{X},M_2} \leqslant P_e^{\mathcal{X}}(\tilde{d}) + \frac{M_2 L}{M}. \quad (4.2.26)$$

Так как $\lim\limits_{\tau \to \infty} M_2 L/M = e^{R_2 \tau} e^{-(R-R_L)\tau} = 0$ при $R_2 < R - R_L$, неравенство (4.2.23) доказано. □

> A man of genius makes no mistakes. His errors are volitional and are the portals of discovery.
>
> *Джеймс Джойс* (1882–1941), ирландский писатель

Теперь мы приведем доказательство теоремы 4.2.1, следуя подходу, изложенному в монографии [CT]. Для простоты предположим, что мно-

жество состояний I процесса X конечно. Рассмотрим последовательность k-марковских аппроксимаций процесса $\mathbf{X}$. Положим

$$p^{(k)}(X_0^{n-1}) = p_{X_0^{k-1}}(X_0^{k-1}) \prod_{i=k}^{n-1} p(X_i|X_{i-k}^{i-1}). \tag{4.2.27}$$

Также положим

$$H^{(k)} = \mathbf{E}[-\log p(X_0|X_{-k}^{-1})] = h(X_0|X_{-k}^{-1}) \tag{4.2.28}$$

и

$$\bar{H} = \mathbf{E}[-\log p(X_0|X_{-\infty}^{-1})] = h(X_0|X_{-\infty}^{-1}). \tag{4.2.29}$$

Теорема 4.2.1 вытекает из следующих результатов: лемма 4.2.9 (о сэндвиче), лемма 4.2.10 (о марковской аппроксимации) и лемма 4.2.11 (об отсутствии щели).

Лемма 4.2.9. *Для любого стационарного процесса* $\mathbf{X}$ *выполнены неравенства*

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{p^{(k)}(X_0^{n-1})}{p(X_0^{n-1})} \leqslant 0 \quad п.н. \tag{4.2.30}$$

и

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{p(X_0^{n-1})}{p(X_0^{n-1}|X_{-\infty}^{-1})} \leqslant 0 \quad п.н. \tag{4.2.31}$$

Доказательство. Пусть A_n — событие полной вероятности для меры $p_{X_0^{n-1}}$, (т. е. $\mathbf{P}(X_0^{n-1} \in A_n) = 1$), запишем

$$\mathbf{E}\frac{p^{(k)}(X_0^{n-1})}{p(X_0^{n-1})} = \sum_{x_0^{n-1}\in A_n} p(x_0^{n-1}) \frac{p^{(k)}(x_0^{n-1})}{p(x_0^{n-1})} = \sum_{x_0^{n-1}\in A_n} p^{(k)}(x_0^{n-1}) = p^{(k)}(A) \leqslant 1.$$

Аналогично, если $B_n = B_n(X_{-\infty}^{-1})$, событие полной вероятности для меры $p_{X_0^{n-1}|X_{-\infty}^{-1}}$ $\mathbf{P}(X_0^{n-1} \in B_n|X_{-\infty}^{-1})$ (т. е. $= 1$), то запишем

$$\mathbf{E}\frac{p(X_0^{n-1})}{p(X_0^{n-1}|X_{-\infty}^{-1})} = \mathbf{E}_{X_{-\infty}^{-1}} \sum_{x_0^{n-1}\in B_n} p(x_0^{n-1}|X_{-\infty}^{-1}) \frac{p(x_0^{n-1})}{p(x_0^{n-1}|X_{-\infty}^{-1})} =$$

$$= \mathbf{E}_{X_{-\infty}^{-1}} \sum_{x_0^{n-1}\in B_n} p(x_0^{n-1}) = \mathbf{E}_{X_{-\infty}^{-1}} \mathbf{P}(B_n) \leqslant 1.$$

По неравенству Маркова

$$\mathbf{P}\Big(\frac{p^{(k)}(X_0^{n-1})}{p(X_0^{n-1})} \geqslant t_n\Big) = \mathbf{P}\Big(\frac{1}{n}\log\frac{p^{(k)}(X_0^{n-1})}{p(X_0^{n-1})} \geqslant \frac{1}{n}\log t_n\Big) \leqslant \frac{1}{t_n},$$

и аналогично получаем оценку для $\mathbf{P}\Big(\dfrac{p(X_0^{n-1})}{p(X_0^{n-1}|X_{-\infty}^{-1})} \geqslant t_n\Big)$.

Завершаем доказательство с помощью леммы Бореля—Кантелли, выбирая $t_n = n^2$, так что $\sum\limits_n 1/t_n < \infty$. □

Лемма 4.2.10. *Для любого стационарного эргодического процесса выполнены соотношения*

$$-\frac{1}{n}\log p^{(k)}(X_0^{n-1}) \overset{\text{п.н.}}{\Rightarrow} H^{(k)}, \tag{4.2.32}$$

$$-\frac{1}{n}\log p(X_0^{n-1}|X_{-\infty}^{-1}) \overset{\text{п.н.}}{\Rightarrow} \bar{H}. \tag{4.2.33}$$

Доказательство. Подставляя

$$f = -\log p(X_0|X_{-k}^{-1}) \quad \text{и} \quad f = -\log p(X_0|X_{-\infty}^{-1})$$

в эргодическую теорему Биркгофа, получаем, что

$$-\frac{1}{n}\log p^{(k)}(X_0^{n-1}) =$$

$$= -\frac{1}{n}\log p(X_0^{k-1}) - \frac{1}{n}\sum_{i=k}^{n-1}\log p^{(k)}(X_i|X_{i-k}^{i-1}) \Rightarrow 0 + H^{(k)} \tag{4.2.34}$$

и

$$-\frac{1}{n}\log p(X_0^{n-1}|X_{-\infty}^{-1}) = -\frac{1}{n}\sum_{i=0}^{n-1}\log p(X_i|X_{-\infty}^{i-1}) \Rightarrow \bar{H} \tag{4.2.35}$$

соответственно.

Теперь в силу лемм 4.2.9 и 4.2.10 имеем

$$\limsup_{n\to\infty}\frac{1}{n}\log\frac{1}{p(X_0^{n-1})} \leqslant \lim_{n\to\infty}\frac{1}{n}\log\frac{1}{p^{(k)}(X_0^{n-1})} = H^{(k)}, \tag{4.2.36}$$

и

$$\liminf_{n\to\infty}\frac{1}{n}\log\frac{1}{p(X_0^{n-1})} \geqslant \lim_{n\to\infty}\frac{1}{n}\log\frac{1}{p(X_0^{n-1}|X_{-\infty}^{-1})} = \bar{H},$$

что может быть переписано в виде

$$\bar{H} \leqslant \liminf_{n\to\infty}\Big[-\frac{1}{n}\log p(X_0^{n-1})\Big] \leqslant \limsup_{n\to\infty}\Big[-\frac{1}{n}\log p(X_0^{n-1}) \leqslant H^{(k)}\Big]. \tag{4.2.37}$$

□

Лемма 4.2.11. *Для любого стационарного процесса* $\mathbf{X}$ *справедливо равенство*

$$H^{(k)} \searrow \bar{H} = H.$$

Доказательство. Сходимость $H^{(k)} \searrow H$ следует из стационарности и того факта, что условная энтропия не превосходит безусловную. Остается показать, что $H^{(k)} \searrow \bar{H}$, и таким образом, $\bar{H} = H$. Из теоремы Дуба—Леви о сходимости мартингалов (см., например, [Wi]), образованных условными вероятностями, следует, что

$$p(X_0 = x_0|X_{-k}^{-1}) \overset{\text{п.н.}}{\Rightarrow} p(X_0 = x_0|X_{-\infty}^{-1}), \quad k \to \infty. \tag{4.2.38}$$

Поскольку множество I конечно, функция $p \in [0,\, 1] \mapsto -p \log p$ ограничена. Поэтому из теоремы об ограниченной сходимости следует, что

$$H^{(k)} = \mathbf{E}\left[-\sum_{x_0 \in I} p(X_0 = x_0|X_{-k}^{-1}) \log p(X_0 = x_0|X_{-k}^{-1}) \right] \Rightarrow$$

$$\Rightarrow \mathbf{E}\left[-\sum_{x_0 \in I} p(X_0 = x_0|X_{-\infty}^{-1}) \log p(X_0 = x_0|X_{-\infty}^{-1}) \right] = \bar{H} \quad \text{при } k \to \infty. \quad \square$$

§ 4.3. Формула Найквиста—Шеннона

В этом параграфе мы приводим строгий вывод знаменитой формулы Найквиста—Шеннона[1] для пропускной способности непрерывного по времени канала с ограничением по мощности и конечной полосой пропускания. Этот результат нередко считается наивысшим достижением теории информации. Наше изложение повторяет (с небольшими изменениями) работу [W1]. Поскольку оно довольно длинное, мы разделим параграф на пункты 1–18, каждый из которых посвящён своему шагу конструкции.

Гарри Найквист (1889–1976) считается пионером теории информации, он занимался вместе с Ральфом Хартли (1888–1970) разработкой понятия пропускной способности канала.

1. Отправная точка состоит в следующем: фиксируем числа τ, α, $p > 0$ и предполагаем, что каждые τ временных отсчетов кодер производит вещественное кодовое слово $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, где $n = \lceil \alpha\tau \rceil$. Каждый вектор $\mathbf{x}$, генерируемый кодером, лежит в конечном множестве $\mathcal{X} = \mathcal{X}_n \subset \mathbb{R}^n$ мощности $M \sim 2^{R_b \tau}$ (кодовая книга); иногда, как и прежде, мы будем писать $\mathcal{X}_{M,n}$, чтобы подчеркнуть роль M и n. Кроме того, удобно перенумеровать

[1] Некоторые авторы называют её теоремой Шеннона—Хартли.

кодовые слова из $\mathcal{X}$: $\mathbf{x}(1), \dots, \mathbf{x}(M)$ (в произвольном порядке), где $\mathbf{x}(i) = \begin{pmatrix} x_1(i) \\ \vdots \\ x_n(i) \end{pmatrix}$, $1 \leqslant i \leqslant M$.

2. Затем кодовое слово $\mathbf{x}$ преобразуется в непрерывный по времени сигнал

$$x(t) = \sum_{i=1}^{n} x_i \varphi_i(t), \quad 0 \leqslant t \leqslant \tau, \tag{4.3.1}$$

где $\varphi_i(t)$, $i = 1, 2, \dots$ — ортогональный базис в $\mathbb{L}_2[0, \tau]$ (с $\int_0^\tau \varphi_i(t)\overline{\varphi_j(t)}dt = \delta_{ij}$). Тогда элемент x_i можно восстановить как

$$x_i = \int_0^\tau x(t)\overline{\varphi_j(t)}dt. \tag{4.3.2}$$

Мгновенная мощность сигнала в момент t ассоциируется с $|x(t)|^2$; в этом случае квадратичная норма $\|\mathbf{x}\|^2 = \int_0^\tau |x(t)|^2 dt = \sum_{i=1}^n |x_i|^2$ представляет полную энергию сигнала на отрезке $[0, \tau]$. Ограничение по мощности для полной энергии, затраченной при передаче, выглядит следующим образом:

$$\|\mathbf{x}\|^2 \leqslant p\tau, \quad \text{или} \quad \mathbf{x} \in \mathbb{B}_n(\sqrt{p\tau}). \tag{4.3.3}$$

(В теории волноводов размерность n называется числом Найквиста, а значение $W = n/(2\tau) \sim \alpha/2$ — *полосой пропускания канала*.)

3. Кодовый вектор $\mathbf{x}(i)$ пересылается по аддитивному каналу, и на выходе получается (случайный) вектор

$$\mathbf{Y} = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}, \quad Y_k = x_k + Z_k, \ \ 1 \leqslant k \leqslant n. \tag{4.3.4}$$

Мы считаем, что $\mathbf{Z} = \begin{pmatrix} Z_1 \\ \vdots \\ Z_n \end{pmatrix}$ — вектор с н. о. р. координатами $Z_k \sim \mathrm{N}(0, \sigma^2)$.

(В приложениях инженеры используют представление $Z_i = \int_0^\tau Z(t)\varphi_i(t)dt$ в терминах процесса «белого шума» $Z(t)$.)

Для начала мы объявим, что если $\mathbf{x}(i) \in \mathcal{X} \setminus \mathbb{B}_n(\sqrt{p\tau})$, т. е. $\|\mathbf{x}(i)\|^2 > p\tau$, то выходной вектор $\mathbf{Y}$ считается «недекодируемым». Другими словами, вероятность верного декодирования вектора $\mathbf{Y} = \mathbf{x}(i) + \mathbf{Z}$, $\|\mathbf{x}(i)\|^2 > p\tau$ считается равной нулю (несмотря на то, что вектор шума $\mathbf{Z}$ может быть маленьким и выходной вектор $\mathbf{Y}$ близок к $\mathbf{x}(i)$ с положительной вероятностью).

В противном случае, т. е. когда $\|\mathbf{x}(i)\|^2 \leqslant p\tau$, получатель применяет к выходному вектору $\mathbf{Y}$ декодер $d(= d_{n,\mathcal{X}})$, т. е. отображение $\mathbf{y} \in \mathbb{K} \mapsto d(\mathbf{y}) \in \mathcal{X}$, где $\mathbb{K} \subset \mathbb{R}^n$ — «область декодируемости» (в которой определено отображение d). Итак, если $\mathbf{Y} \in \mathbb{K}$, то он декодируется как $d(\mathbf{Y}) \in \mathcal{X}$. Здесь появляется ошибка, когда либо $\mathbf{Y} \notin \mathbb{K}$, либо $d(\mathbf{Y}) \neq \neq \mathbf{x}(i)$ при посланном слове $\mathbf{x}(i)$. Это приводит к следующей формуле для вероятности ошибочного декодирования входного кодового слова $\mathbf{x}(i)$:

$$P_e(i,\, d) = \begin{cases} 1, & \|\mathbf{x}(i)\|^2 > p\tau, \\ \mathbf{P}_{\mathrm{ch}}(\mathbf{Y} \notin \mathbb{K} \text{ или } d(\mathbf{Y}) \neq \mathbf{x}(i) | \mathbf{x}(i) \text{ послано}), & \|\mathbf{x}(i)\|^2 \leqslant p\tau. \end{cases} \tag{4.3.5}$$

В этом случае средняя вероятность ошибки $P_e = P_e^{\mathcal{X},\mathrm{av}}(d)$ для кода $\mathcal{X}$ определяется как

$$P_e = \frac{1}{M} \sum_{1 \leqslant i \leqslant M} P_e(i,\, d). \tag{4.3.6}$$

Более того, будем говорить, что R_{bit} (или R_{nat}) — скорость надёжной передачи (для данных α и p), если $\forall \varepsilon > 0$ можно указать такое $\tau(\varepsilon) > 0$, что $\forall \tau > \tau(\varepsilon)$ найдутся такая кодовая книга $\mathcal{X}$ размера $\#\mathcal{X} \sim e^{R_{\mathrm{nat}}\tau}$ и такое правило декодирования d, что $P_e^{\mathcal{X},\mathrm{av}}(d) < \varepsilon$. Пропускная способность канала C тогда определяется как супремум всех скоростей надёжных передач, и применяя рассуждения из § 4.1, получаем, что

$$C = \frac{\alpha}{2} \ln \left(1 + \frac{p}{\alpha\sigma^2}\right) \quad \text{в натах;} \tag{4.3.7}$$

см. формулу (4.1.17). Заметим, что при $\alpha \to \infty$ п. ч. формулы (4.3.7) стремится к $p/(2\sigma^2)$.

4. В непрерывной по времени ситуации Шеннон (а перед ним Найквист) обсуждал приложение формулы (4.3.7) к сигналам с ограниченной полосой частот. Более точно, положим $W = \alpha/2$, тогда формула

$$C = W \ln \left(1 + \frac{p}{2\sigma_0^2 W}\right) \tag{4.3.8}$$

должна описывать пропускную способность непрерывного по времени аддитивного канала с белым шумом дисперсии $\sigma^2 = \sigma_0^2 W$ для сигнала $x(t)$ с ограниченной полосой частот, спектром на $[-W,\, W]$, энергия которого на единицу времени не превосходит p.

Эта фраза, совершенно ясная квалифицированным инженерам, стала камнем преткновения для математиков, и требуются технические усилия для того чтобы придать ей строгий математический смысл. На языке инженеров «идеальная» ортонормированная система на отрезке $[0,\, \tau]$, используемая в формуле (4.3.1), означает набор $n \sim 2W\tau$ равномерно

отстоящих друг от друга δ-функций. Иначе говоря, с его помощью очень удобно представлять кодовое слово $\mathbf{x}(i) = (x_1(i), \ldots, x_n(i))$ через функцию $f_i(t)$, зависящую от времени $t \in [0, \tau]$, заданную как сумма

$$f_i(t) = \sum_{k=1}^{n} x_k(i)\delta\left(t - \frac{k}{2W}\right), \tag{4.3.9}$$

где $n = \lceil 2W\tau \rceil$ (и $\alpha = 2W$). Здесь $\delta(t)$ — «единичный импульс», возникающий вблизи момента времени 0, график которого выглядит как «острый единичный всплеск» в окрестности точки $t = 0$. Тогда сдвинутая функция $\delta(t - k/(2W))$ представляет собой всплеск в окрестности точки $t = k/(2W)$. График функции $f_i(t)$ показан на рис. 4.4.

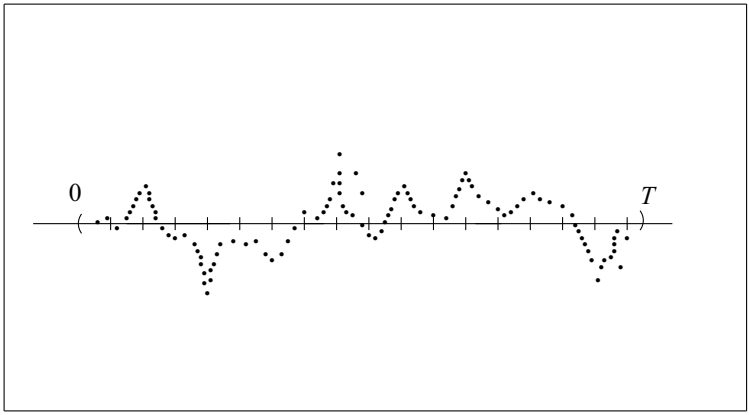


Рис. 4.4

Будем считать, что наш кодер производит функции $x_i(t)$ каждые τ секунд и каждая из этих функций — результат кодирования сообщения i. Более того, внутри каждого временно́го интервала длины τ всплески $x_k(i)\delta(t - k/(2W))$ появляются на временно́м шаге $1/(2W)$. Здесь $\delta(t - k/(2W))$ — сдвинутая по времени δ-функция Дирака.

5. Проблема в том, что $\delta(t)$ — это так называемая «обобщённая функция» и $\delta \notin \mathbb{L}_2$. Способ устранения этой трудности заключается в том, чтобы пропустить сигнал через фильтр нижних частот. Вместо функции $f_i(t)$ он генерирует функцию $\bar{f}_i(t) (= \bar{f}_{W,i}(t))$:

$$\bar{f}_i(t) = \sum_{k=1}^{n} x_k(i)\mathrm{sinc}(2Wt - k). \tag{4.3.10}$$

Здесь

$$\operatorname{sinc}(2Wt-k)=\frac{\sin(2Wt-k)}{\pi(2Wt-k)} \tag{4.3.11}$$

— значение сдвинутой и нормализованной sinc-*функции*:

$$\operatorname{sinc}(s)=\begin{cases}\dfrac{\sin(\pi s)}{\pi s}, & s\neq 0,\\ 1, & s=0,\end{cases} \tag{4.3.12}$$

график которой изображён на рис. 4.5.

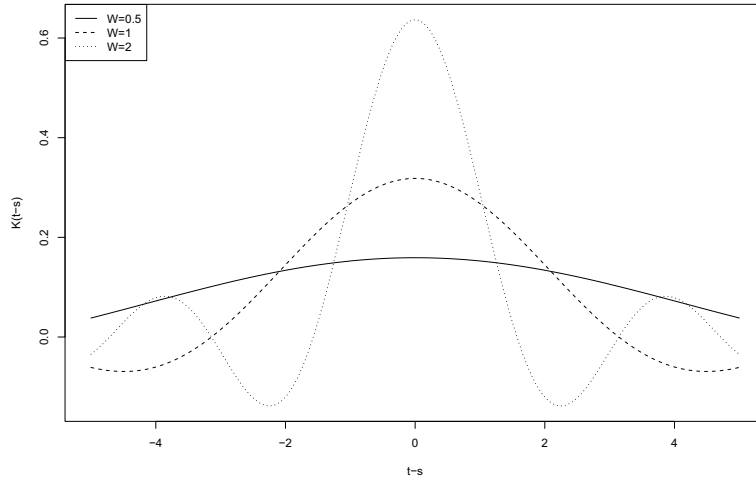


Рис. 4.5

Процедура удаления гармоник высоких частот (или, более общим образом, компонент высокого разрешения) и замещения сигнала $f_i(t)$ его (аппроксимированной) версией с низким разрешением $\bar{f}_i(t)$ широко применяется в современной компьютерной графике и других областях цифровой обработки сигналов.

Пример 4.3.1 (преобразование Фурье в $\mathbb{L}_2$). Напомним, что *преобразование Фурье* $\varphi\mapsto\mathbf{F}\varphi$ интегрируемой функции φ (т. е. функции, удовлетворяющей условию $\int|\varphi(x)|dx<\infty$) определяется как

$$[\mathbf{F}\varphi](\omega)=\int\varphi(x)e^{i\omega x}dx,\quad \omega\in\mathbb{R}. \tag{4.3.13}$$

Обратное преобразование Фурье можно записать как обратное отображение

$$[\mathbf{F}^{-1}\varphi](x) = \frac{1}{2\pi}\int \varphi(\omega)e^{-i\omega x}d\omega. \tag{4.3.14}$$

Глубокий факт заключается в том, что преобразования (4.3.13) и (4.3.14) можно обобщить на функции с интегрируемым квадратом $\varphi \in \mathbb{L}_2(\mathbb{R})$ (с $\|\varphi\|^2 = \int |\varphi(x)|^2 dx < +\infty$). У нас нет возможности излагать это подробно. Интересующемуся читателю можно порекомендовать книгу [RS]. Кроме того, методы преобразования Фурье оказываются чрезвычайно полезными в многочисленных применениях. Обозначив, например, $\mathbf{F}\varphi = \hat{\varphi}$, и записав $\mathbf{F}^{-1}\hat{\varphi} = \varphi$, из формул (4.3.13) и (4.3.14) мы получим, что

$$\varphi(x) = \frac{1}{2\pi}\int \hat{\varphi}(\omega)e^{-ix\omega}d\omega. \tag{4.3.15}$$

Кроме этого, для любых двух функций с интегрируемым квадратом φ_1, $\varphi_2 \in \mathbb{L}_2(\mathbb{R})$ имеем

$$2\pi\int \varphi_1(x)\overline{\varphi_2(x)}dx = \int \hat{\varphi}_1(\omega)\overline{\hat{\varphi}_2(\omega)}d\omega. \tag{4.3.16}$$

□

Более того, преобразование Фурье можно определить и для обобщённых функций (см. [RS]). А именно, формулы (4.3.13) и (4.3.14) для δ-функций имеет вид

$$\delta(t) = \frac{1}{2\pi}\int e^{-i\omega t}d\omega, \quad 1 = \int \delta(t)e^{it\omega}dt. \tag{4.3.17}$$

Таким образом, преобразование Фурье δ-функции Дирака равно $\hat{\delta}(\omega) \equiv 1$. Для сдвинутой δ-функции мы получаем

$$\delta\Big(t - \frac{k}{2W}\Big) = \frac{1}{2\pi}\int e^{ik\omega/(2W)}e^{-i\omega t}d\omega. \tag{4.3.18}$$

6. Формула Шеннона—Найквиста устанавливается для устройств, в которых каналу предшествует «фильтр», отсекающий гармоники $e^{\pm it\omega}$ с частотами ω, лежащими вне отрезка $[-2\pi W, 2\pi W]$. Иначе говоря, (сдвинутый) единичный импульс $\delta(t - k/(2W))$ в формуле (4.3.18) замещается его обрезанной версией, появляющейся после того, как фильтр обрежет гармоники $e^{-it\omega}$, $|\omega| > 2\pi W$.

Sinc-функция (знаменитый объект в прикладной математике) является классической функцией, возникающей при ограничении интеграла по ω в формуле (4.3.17) на отрезке $[-\pi, \pi]$:

$$\operatorname{sinc}(t) = \frac{1}{2\pi}\int\limits_{-\pi}^{\pi} e^{-i\omega t}d\omega, \quad \mathbf{1}_{[-\pi,\pi]}(\omega) = \int \operatorname{sinc}(t)e^{it\omega}dt, \quad t,\ \omega \in \mathbb{R}^1 \tag{4.3.19}$$

(в символах $\mathrm{sinc} = \mathbf{F}^{-1}\mathbf{1}_{[-\pi,\pi]}$). В нашей ситуации функцию $t \mapsto A\mathrm{sinc}(At)$ можно рассматривать для больших значений параметра $A > 0$, как удобную аппроксимацию функции $\delta(t)$. Только нужно помнить о том, что функция $\mathrm{sinc}(t)$ не интегрируется на всей числовой прямой $\mathbb{R}$ (из-за множителя $1/t$), хотя её квадрат интегрируется: $\int(\mathrm{sinc}[t])^2 dt < \infty$. В связи с этим правое уравнение из (4.3.19) нужно понимать в смысле $\mathbb{L}_2$.

Однако это не упрощает математические и физические аспекты теории (также как и инженерные аспекты). Действительно, считается, что идеальный фильтр очищает сигнал от нежелательных гармоник, что естественно «физически невозможно». Более того, если предположить, что такое совершенное устройство построено, мы получим сигнал $\bar{f}_i(t)$, который будет уже определён не только на отрезке $[0, \tau]$, но аналитически продолжается на всю временну́ю ось. Для преодоления этого препятствия необходимо ввести дополнительные технические аппроксимации.

Пример 4.3.2. Проверьте, что функции

$$t \mapsto (2\sqrt{\pi W})\mathrm{sinc}(2Wt - k), \quad k = 1, \ldots, n \tag{4.3.20}$$

ортогональны в пространстве $\mathbb{L}_2(\mathbb{R}^1)$:

$$(4\pi W)\int[\mathrm{sinc}(2Wt - k)][\mathrm{sinc}(2Wt - k')] = \delta_{kk'}.$$

Решение. Самый простой способ увидеть это заключается в выписывании преобразования Фурье (см. формулу (4.3.19)):

$$2\sqrt{\pi W}\mathrm{sinc}(2Wt - k) = \frac{1}{2\sqrt{\pi W}}\int_{-2\pi W}^{2\pi W} e^{ik\omega/(2W)}e^{-it\omega}d\omega \tag{4.3.21}$$

и проверке того, что функции, представляющие преобразование Фурье:

$$\frac{1}{2\sqrt{\pi W}}\mathbf{1}(|\omega| \leqslant 2\pi W)e^{ik\omega/(2W)}, \quad k = 1, \ldots, n,$$

ортогональны, т. е.

$$\frac{1}{4\pi W}\int_{-2\pi W}^{2\pi W} e^{i(k-k')\omega/(2W)}d\omega = \delta_{kk'}, \tag{4.3.22}$$

где $\delta_{kk'} = \begin{cases} 1, & k = k', \\ 0, & k \neq k' \end{cases}$ — символ Кронекера. Но формула (4.3.22) проверяется стандартным способом. □

7. Поскольку функции из формулы (4.3.20) ортогональны, мы получаем, что

$$\|\mathbf{x}(i)\|^2 = (4\pi W)\|\bar{f}_i\|^2, \quad \text{где} \quad \|\bar{f}_i\|^2 = \int|\bar{f}_i(t)|^2 dt, \tag{4.3.23}$$

а функции f_i^- введены в формуле (4.3.10). Таким образом, ограничение по мощности можно записать как

$$\|f_i^-\|^2 \leqslant p\tau/4\pi W = p_0. \tag{4.3.24}$$

Фактически коэффициенты $x_k(i)$ совпадают со значениями $f_i^-(k/(2W))$ функции f_i^-, вычисленными в моменты времени $k/(2W)$, $k = 1, \ldots, n$; эти точки можно называть «моментами отсчётов».

Итак, входной сигнал $f_i^-(t)$ зависит от непрерывного времени, хотя полностью определяется его значениями $f_i^-(k/(2W)) = x_k(i)$. Таким образом, если мы считаем, что различные сигналы генерируются в непересекающиеся интервалы времени $(0, \tau)$, $(\tau, 2\tau)$, $\ldots$, то, несмотря на помехи, вызванные бесконечными хвостами функции $\mathrm{sinc}(t)$, эти сигналы чётко идентифицируются по своим значениям в моменты отсчётов.

Предположения Найквиста—Шеннона заключаются в том, что сигнал $f_i^-(t)$ трансформируется каналом в

$$g(t) = f_i^-(t) + Z^-(t). \tag{4.3.25}$$

Здесь $Z^-(t)$ — стационарный непрерывный по времени гауссовский процесс с нулевым средним ($\mathsf{E}Z^-(t) \equiv 0$) и (авто)корреляционной функцией

$$\mathsf{E}[Z^-(s)Z^-(t+s)] = 2\sigma_0^2 W \mathrm{sinc}(2Wt), \quad t, s \in \mathbb{R}. \tag{4.3.26}$$

В частности, когда t кратно π/W (т. е. точка t попала на момент отсчёта), с. в. $Z^-(s)$ и $Z^-(t+s)$ будут независимы. Эквивалентный вид этого условия состоит в том, что спектральная плотность имеет вид

$$\Phi(\omega) := \int e^{it\omega}\, \mathsf{E}[Z^-(0)Z^-(t)]dt = \sigma_0^2 \mathbf{1}(|\omega| < 2\pi W). \tag{4.3.27}$$

Мы видим, что полученный непрерывный по времени сигнал $y(t)$ можно отождествить с его значениями $y_k = y\left(\dfrac{k}{2W}\right)$ через уравнения

$$y_k = x_k(i) + Z_k, \quad \text{где} \quad Z_k = Z^-\left(\frac{k}{2W}\right) \text{— н. о. р. с. в. } \mathrm{N}(0,\, 2\sigma_0^2 W).$$

Это соответствует системе, рассмотренной в § 4.1, с $p = 2Wp_0$ и $\sigma^2 = 2\sigma_0^2 W$. В инженерной среде было принято считать, что пропускная способность действующей системы определяется формулой (4.3.8), т. е. скорость передачи ниже этого значения C надёжна, а выше — нет.

8. Однако возникает ряд проблем, которые необходимо решить для строгого понимания формулы (4.3.8). Одна из них заключается в том, что, как было отмечено выше, «точный» фильтр, ограничивающий спектр сигнала на определённой частотный интервал, — идеализированное устройство. Другая состоит в том, что выходной сигнал $g(t)$ из формулы (4.3.25) является аналитическим и может быть восстановлен, после того как он

был зарегистрирован на небольшом интервале времени, потому что любая функция отсчётов вида

$$t \in \mathbb{R} \mapsto \sum_{k=1}^{n} (x_k(i) + z_k)\mathrm{sinc}(2Wt - k) \tag{4.3.28}$$

аналитична по t. Следовательно, понятие *пропускной способности* нужно, по существу, переопределить.

Простейшее решение (предложенное в работе [W1]) состоит во введении класса функций $\mathcal{A}(\tau, W, p_0)$, которые а) приблизительно ограничены по частотам до W циклов на единицу времени (скажем, секунду), б) отличны от нуля на временно́м интервале длины τ (удобно конкретизировать этот интервал как $[-\tau/2, \tau/2]$), в) обладают общей энергией ($\mathbb{L}_2(\mathbb{R})$-нормой), не превышающей $p_0\tau$. Эти условия определяют ограничения на доступные передаче области.

9. Итак, рассмотрим код $\mathcal{X}$ размера $N \sim e^{R\tau}$, т. е. набор функций $f_1^{\cdot}(t), \ldots, f_M^{\cdot}(t)$ от временно́й переменной t. Если сигнал $f_i^{\cdot} \notin \mathcal{A}(\tau, W, p_0)$, то его объявляют недекодируемым: он даёт ошибку с вероятностью один. Иначе сигнал $f_i^{\cdot} \in \mathcal{A}(\tau, W, p_0)$ подвергается воздействию аддитивного гауссовского шума $Z^{\cdot}(t)$ со средним $\mathsf{E}Z^{\cdot}(t) \equiv 0$, описанным формулой (4.3.27), и преобразуется в $g(t) = f_i^{\cdot}(t) + Z^{\cdot}(t)$ — выходной сигнал канала (см. (4.3.25)). Получатель пользуется правилом декодирования, т. е. отображением $d\colon \mathbb{K} \to \mathcal{X}$, где $\mathbb{K}$ — область определения отображения d. (Как и ранее, декодер d может варьироваться вместе с кодом, на что указывает обозначение $d = d^{\mathcal{X}}$.) И вновь если $g \notin \mathbb{K}$, то передача считается ошибочной. Если, наконец, $g \in \mathbb{K}$, то полученный сигнал g декодируется кодовой функцией $d^{\mathcal{X}}(g)(t) \in \mathcal{X}$. Вероятность ошибки для кода $\mathcal{X}$, когда кодовый сигнал, генерируемый кодером, был равное $f_i^{\cdot} \in \mathcal{X}$, имеет вид

$$P_e(i) = \begin{cases} 1, & f_i^{\cdot} \notin \mathcal{A}(\tau, W, p_0), \\ \mathbf{P}_{\mathrm{ch}}(\mathbb{K}^{\mathrm{c}} \cup \{g\colon d^{\mathcal{X}}(g) \neq f_i^{\cdot}\}), & f_i^{\cdot} \in \mathcal{A}(\tau, W, p_0). \end{cases} \tag{4.3.29}$$

Средняя вероятность ошибки $P_e = P_e^{\mathcal{X},\mathrm{av}}(d)$ для кода $\mathcal{X}$ (и декодера d) равна

$$P_e = \frac{1}{M} \sum_{i=1}^{M} P_e(i, d). \tag{4.3.30}$$

Величина $R(= R_{\mathrm{nat}})$ называется скоростью надёжной передачи, если $\forall \varepsilon > 0$ существуют такое число τ и такой код $\mathcal{X}$ размера $M \sim e^{R\tau}$, что $P_e < \varepsilon$.

10. Фиксируем, далее, число $\eta \in (0, 1)$. Класс $\mathcal{A}(\tau, W, p_0) = \mathcal{A}(\tau, W, p_0, \eta)$ определяется как класс таких функций $f^{\circ}(t)$, что

1) $f^\circ = D_\tau f$, где

$$D_\tau f(t) = f(t)\mathbf{1}(|t| \leqslant \tau/2), \quad t \in \mathbb{R}$$

и Фурье-образ $\int e^{it\omega} f(t)dt$ функции $f(t)$ равен нулю при $|\omega| > 2\pi W$;

2) справедливо неравенство

$$\frac{\|f^\circ\|^2}{\|f\|^2} \geqslant 1 - \eta;$$

3) $\|f^\circ\|^2 \leqslant p_0\tau$.

Иными словами, сигналы $f^\circ \in \mathcal{A}(\tau, W, p_0, \eta)$, которые можно передать, «резко локализованы» во времени и в точности узкополосные по частоте.

Формулу Найквиста—Шеннона можно получить как предельный случай нескольких формальных утверждений, простейшее из которых — это теорема 4.3.3, приведённая ниже. Альтернативный подход будет представлен позже, в теореме 4.3.7.

Теорема 4.3.3. *Пропускная способность $C = C(\eta)$ описанного выше канала с ограничением на доступную передаче область $\mathcal{A}(\tau, W, p_0, \eta)$, описанным выше условиями* 1)–3), *задаётся формулой*:

$$C = W \ln\left(1 + \frac{p_0}{2\sigma_0^2 W}\right) + \frac{\eta}{1-\eta}\frac{p_0}{\sigma_0^2} \tag{4.3.31}$$

и

$$\lim_{\eta \to 0} C(\eta) = W \ln\left(1 + \frac{p_0}{2\sigma_0^2 W}\right), \tag{4.3.32}$$

что даёт формулу Найквиста—Шеннона (4.3.8).

11. Перед тем как окунуться в (довольно сложные) технические детали, мы обсудим некоторые факты, имеющие отношение к произведению, или параллельному подключению r дискретных по времени гауссовских каналов. (По сути эта модель обсуждалась в конце § 4.2.) Здесь τ — единица времени, генерируемый входной сигнал является упорядоченным набором векторов

$$\{\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(r)}\}, \quad \text{где} \quad \mathbf{x}^{(j)} = \begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{n_j}^{(j)} \end{pmatrix} \in \mathbb{R}^{n_j}, \quad 1 \leqslant j \leqslant r, \tag{4.3.33}$$

и $n_j = \lceil \alpha_j \tau \rceil$, где α_j — данное число (скорость производства знаков j-м кодером). Для каждого вектора $\mathbf{x}^{(j)}$ рассмотрим ограничение по мощности

$$\|\mathbf{x}^{(j)}\|^2 \leqslant p^{(j)}\tau, \quad 1 \leqslant j \leqslant r. \tag{4.3.34}$$

Выходной сигнал представляет собой набор (случайных) векторов

$$\{\mathbf{Y}^{(1)}, \ldots, \mathbf{Y}^{(r)}\}, \quad \text{где} \quad \mathbf{Y}^{(j)} = \begin{pmatrix} Y_1^{(j)} \\ \vdots \\ Y_{n_j}^{(j)} \end{pmatrix} \in \mathbb{R}^{n_j}, \quad Y_k^{(j)} = x_k^{(j)} + Z_k^{(j)}, \quad (4.3.35)$$

$Z_k^{(j)}$ — н. о. р. с. в. $Z_k^{(j)} \sim \mathrm{N}(0, {\sigma^{(j)}}^2)$, $1 \leqslant k \leqslant n_j$, $1 \leqslant j \leqslant r$.

Кодовая книга $\mathcal{X}$ со скоростью передачи информации R для произведения каналов с ограничениями — это массив M входных сигналов

$$\{(\mathbf{x}^{(1)}(1), \ldots, \mathbf{x}^{(r)}(1)), \ (\mathbf{x}^{(1)}(2), \ldots, \mathbf{x}^{(r)}(2)), \ \ldots, \ (\mathbf{x}^{(1)}(M), \ldots, \mathbf{x}^{(r)}(M))\}, \quad (4.3.36)$$

каждый из которых имеет ту же структуру, что и в формуле (4.3.33). Как и раньше, декодер d — это отображение, действующее на множестве $\mathbb{K}$ выходных сигналов $\{\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(r)}\}$, и переводящее эти сигналы в $\mathcal{X}$.

Как и прежде, при $i = 1, \ldots, M$ мы определяем вероятность ошибки $P_e(i, d)$ для кода $\mathcal{X}$, когда посылается входной сигнал $(\mathbf{x}^{(1)}(i), \ldots, \mathbf{x}^{(r)}(i))$:

$$P_e(i, d) = 1, \quad \text{если} \quad \|\mathbf{x}^{(j)}(i)\|^2 \geqslant p^{(j)}\tau \text{ для некоторого } j = 1, \ldots, r$$

и

$$P_e(i, d) = \mathbf{P}_{\mathrm{ch}}(\{\mathbf{Y}^{(1)}, \ldots, \mathbf{Y}^{(r)}\} \notin \mathbb{K} \text{ или } d(\{\mathbf{Y}^{(1)}, \ldots, \mathbf{Y}^{(r)}\}) \neq \{\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(r)}\} \,|\, \{\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(r)}\} \text{ послано}),$$
$$\text{если} \quad \|\mathbf{x}^{(j)}(i)\|^2 < p^{(j)}\tau \ \forall j = 1, \ldots, r.$$

Средняя вероятность ошибки $P_e = P_e^{\mathcal{X},\mathrm{av}}(d)$ для кода $\mathcal{X}$ (при использовании декодера d) снова вычисляется по формуле

$$P_e = \frac{1}{M} \sum_{i=1}^{M} P_e(i, d).$$

Как обычно, говорят, что R — скорость надёжной передачи, если $\forall \varepsilon > 0$ существует такое $\tau_0 > 0$, что для всех $\tau > \tau_0$ найдутся такой код $\mathcal{X}$ мощности $M \sim e^{R\tau}$ и такое правило декодирования d, что $P_e < \varepsilon$. Пропускная способность комбинированного канала вновь определяется как супремум всех скоростей надёжной передачи. В примере 4.2.7 был установлен следующий факт (см. лемму A в [W1] и работу [W2]).

Лемма 4.3.4. *Пропускная способность произведения каналов с ограничениями равна*

$$C = \sum_{j=1}^{r} \frac{\alpha_j}{2} \ln \left(1 + \frac{p^{(j)}}{\alpha_j \sigma_j^2}\right). \quad (4.3.37)$$

Более того, это равенство справедливо даже если некоторые из α_j *обращаются в* $+\infty$: *в этом случае соответствующее слагаемое принимает вид* $p^{(j)}/2\sigma_j^2$.

12. Наш следующий шаг состоит в рассмотрении произведения дискретных по времени гауссовских каналов с совместными ограничениями по мощности. Мы обсудим следующие типы совместных ограничений.

Случай I. Возьмём $r = 2$ и предположим, что $\sigma_1^2 = \sigma_2^2 = \sigma_0^2$ и заменим условие (4.3.34) на

$$\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2 < p_0\tau. \tag{4.3.38а}$$

Кроме того, если $\alpha_1 \leqslant \alpha_2$, мы вводим $\beta \in (0, 1)$ и требуем,чтобы выполнялось неравенство

$$\|\mathbf{x}^{(2)}\|^2 \leqslant \beta(\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2). \tag{4.3.38б}$$

В противоположном случае, т. е. если $\alpha_2 \leqslant \alpha_1$, требование (4.3.38б) меняется на следующее:

$$\|\mathbf{x}^{(1)}\|^2 \leqslant \beta(\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2). \tag{4.3.38в}$$

Случай II. Здесь мы берём $r = 3$ и предполагаем, что $\sigma_1^2 = \sigma_2^2 \geqslant \sigma_3^2$, а $\alpha_3 = +\infty$. Здесь ограничение по мощности имеет вид

$$\sum_{j=1}^{3} \|\mathbf{x}^{(j)}\|^2 < p_0\tau \tag{4.3.39а}$$

и

$$\|\mathbf{x}^{(3)}\|^2 \leqslant \beta \sum_{j=1}^{3} \|\mathbf{x}^{(j)}\|^2. \tag{4.3.39б}$$

Случай III. Как и в случае I, возьмём $r = 2$ и предположим, что $\sigma_1^2 = \sigma_2^2 = \sigma_3^2$. Положим, далее, $\alpha_2 = +\infty$ и наложим такое ограничение по мощности:

$$\|\mathbf{x}^{(2)}\|^2 < p_0\tau \tag{4.3.40а}$$

и

$$\|\mathbf{x}^{(2)}\|^2 < \beta(\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2). \tag{4.3.40б}$$

Пример 4.3.5 (см. теорему 1 из [W1]). Мы хотим доказать, что пропускные способности подключенных параллельно каналов типов I–III выглядят следующим образом.

$$\text{Случай I: } \alpha_1 \leqslant \alpha_2\colon\ C = \frac{\alpha_1}{2}\ln\left(1 + \frac{(1-\zeta)p_0}{\alpha_1\sigma_0^2}\right) + \frac{\alpha_2}{2}\ln\left(1 + \frac{\zeta p_0}{\alpha_2\sigma_0^2}\right), \tag{4.3.41а}$$

где

$$\zeta = \min\left\{\beta,\ \frac{\alpha_2}{\alpha_1+\alpha_2}\right\}. \tag{4.3.41б}$$

Если $\alpha_2 \leqslant \alpha_1$, то в этих формулах нужно поменять местами индексы 1 и 2. Далее, когда $\alpha_i = +\infty$, используется предельное выражение $\lim\limits_{\alpha\to\infty} (\alpha/2)\ln(1+v/\alpha) = v/2$. В частности, если $\alpha_1 < \alpha_2 = +\infty$, то $\beta = \zeta$ и пропускная способность становится равной

$$C = \frac{\alpha_1}{2}\ln\left(1+\frac{(1-\beta)p_0}{\alpha_1\sigma_0^2}\right) + \beta\frac{p_0}{2\sigma_0^2}. \tag{4.3.41в}$$

Это означает, что лучшая скорость передачи достигается, когда на канал 2 подаётся так много «энергии», как разрешается по формуле (4.3.38б).

Случай II:
$$C = \frac{\alpha_1}{2}\ln\left(1+\frac{(1-\beta)p_0}{(\alpha_1+\alpha_2)\sigma_1^2}\right) + \frac{\alpha_2}{2}\ln\left(1+\frac{(1-\beta)p_0}{(\alpha_1+\alpha_2)\sigma_1^2}\right) + \frac{\beta p}{2\sigma_3^2}. \tag{4.3.42}$$

Случай III:
$$C = \frac{\alpha_1}{2}\ln\left(1+\frac{p_0}{\alpha_1\sigma_0^2}\right) + \frac{\beta p_0}{2(1-\beta)\sigma_0^2}. \tag{4.3.43}$$

Решение. Мы приведём доказательство только для случая I. Для определённости предположим, что $\alpha_1 < \alpha_2 \leqslant \infty$. Начнём с прямой части. При $p_1 = (1-\zeta)p_0$, $p_2 = \zeta p_0$ рассмотрим параллельную комбинацию двух каналов с индивидуальными ограничениями на мощность входных сигналов $\mathbf{x}^{(1)}$ и $\mathbf{x}^{(2)}$:

$$\|\mathbf{x}^{(1)}\|^2 \leqslant p_1\tau, \quad \|\mathbf{x}^{(2)}\|^2 \leqslant p_2\tau. \tag{4.3.44а}$$

Естественно, из условия (4.3.44а) вытекает ограничение (4.3.38а). Далее, при $\zeta \leqslant \beta$ условие (4.3.38б) тоже выполнено. Поэтому, учитывая прямую часть леммы 4.3.4, получаем, что любая скорость R, удовлетворяющая оценке $R < C_1(p_1) + C_2(p_2)$ надёжна. Здесь и далее

$$C_i(q) = \frac{\alpha_i}{2}\ln\left(1+\frac{q}{\alpha_i\sigma_0^2}\right), \quad i = 1,\ 2. \tag{4.3.44б}$$

Отсюда следует прямая часть утверждения.

Для доказательства обратного утверждения требуются более длинные рассуждения. Положим $C^* = C_1(p_1) + C_2(p_2)$. Наша цель — показать, что любая скорость $R > C^*$ не надёжна. Предположим противное: найдётся надёжная скорость $R = C^* + \varepsilon$; напомним, что это означает с формальной точки зрения. Существуют последовательность значений $\tau^{(l)} \to \infty$ и 1) последовательность кодов

$$\mathcal{X}^{(i)} = \left\{\mathbf{x}(i) = (\mathbf{x}^{(1)}(i),\ \mathbf{x}^{(2)}(i)),\ \ 1 \leqslant i \leqslant M^{(i)}\right\}$$

размера $M^{(i)} \sim e^{R\tau^{(i)}}$, состоящих из «комбинированных» кодовых векторов $\mathbf{x}(i) = \{\mathbf{x}^{(1)}(i), \mathbf{x}^{(2)}(i)\}$ с квадратом нормы $\|\mathbf{x}(i)\|^2 = \|\mathbf{x}^{(1)}(i)\|^2 + \|\mathbf{x}^{(2)}(i)\|^2$ и 2) последовательность таких декодирующих отображений $d^{(l)} : \mathbf{y} \in \mathbb{K}^{(l)} \mapsto$ $\mapsto d^{(l)}(\mathbf{y}) \in \mathcal{X}^{(l)}$, что $P_e \to 0$. Здесь, как всегда, $P_e = P_e^{\mathcal{X}^{(l)},\mathrm{av}}(d^{(l)})$ обозначает среднюю вероятность ошибки

$$P_e = \frac{1}{M^{(l)}} \sum_{i=1}^{M^{(l)}} P_e(i,\, d^{(l)}),$$

где индивидуальная вероятность ошибки равна

$$P_e(i,\, d^{(l)}) = \begin{cases} 1, & \text{если } \|\mathbf{x}(i)\|^2 > p_0\tau^{(l)} \text{ или } \|\mathbf{x}(i)\|^2 > \beta\|\mathbf{x}\|^2, \\ \mathbf{P}_{\mathrm{ch}}(\mathbf{Y} \notin \mathbb{K}^{(l)} \text{ или } d^{(l)}(\mathbf{Y}) \neq \mathbf{x}(i) | \mathbf{x}(i) \text{ послано}), \\ \text{если } \|\mathbf{x}(i)\|^2 \leqslant p_0\tau^{(l)} \text{ и } \|\mathbf{x}(i)\|^2 \leqslant \beta\|\mathbf{x}\|^2. \end{cases}$$

Компоненты векторов $\mathbf{x}^{(1)}(i) = \begin{pmatrix} x^{(1)}(i) \\ \vdots \\ x^{(1)}_{\lceil \alpha_1\tau^{(l)} \rceil}(i) \end{pmatrix} \in \mathbb{R}^{\lceil \alpha_1\tau^{(l)} \rceil}$ и $\mathbf{x}^{(2)}(i) =$ $= \begin{pmatrix} x^{(2)}(i) \\ \vdots \\ x^{(2)}_{\lceil \alpha_2\tau^{(l)} \rceil}(i) \end{pmatrix} \in \mathbb{R}^{\lceil \alpha_2\tau^{(l)} \rceil}$ пересылаются через свою часть комбинированного канала, в результате чего на выходе получаются векторы

$$\mathbf{Y}^{(1)} = \begin{pmatrix} Y^{(1)}(i) \\ \vdots \\ Y^{(1)}_{\lceil \alpha_1\tau^{(l)} \rceil}(i) \end{pmatrix} \in \mathbb{R}^{\lceil \alpha_1\tau^{(l)} \rceil}, \quad \mathbf{Y}^{(2)} = \begin{pmatrix} Y^{(2)}(i) \\ \vdots \\ Y^{(2)}_{\lceil \alpha_1\tau^{(l)} \rceil}(i) \end{pmatrix} \in \mathbb{R}^{\lceil \alpha_2\tau^{(l)} \rceil},$$

формирующие выходной сигнал $\mathbf{Y} = \{\mathbf{Y}^{(1)}, \mathbf{Y}^{(2)}\}$. Компоненты векторов $\mathbf{Y}^{(1)}$ и $\mathbf{Y}^{(2)}$ — это суммы

$$Y^{(1)}_j(i) = x^{(1)}_j(i) + Z^{(1)}_j, \quad Y^{(2)}_k(i) = x^{(2)}_k(i) + Z^{(2)}_k,$$

где $Z^{(1)}_j$ и $Z^{(2)}_k$ — н. о. р. с. в., распределённые по закону $\mathrm{N}(0, \sigma_0^2)$. Соответственно $\mathbf{P}_{\mathrm{ch}}$ обозначает совместное распределение с. в. $Y^{(1)}_j$ и $Y^{(2)}_k$, $1 \leqslant j \leqslant \lceil \alpha_1\tau^{(l)} \rceil$, $1 \leqslant k \leqslant \lceil \alpha_2\tau^{(l)} \rceil$.

Заметим, что функция $q \mapsto C_1(q)$ равномерно непрерывна по q на отрезке $[0,\, p_0]$. Значит, можно найти такие достаточно большое натуральное число J_0, что

$$\left| C_1(q) - C_1\left(q - \frac{\zeta p_0}{J_0}\right) \right| < \frac{\varepsilon}{2}, \quad \forall q \in (0,\, \zeta p_0).$$

Тогда разобьём код $\mathcal{X}^{(l)}$ на J_0 классов (подкодов) $\mathcal{X}_j^{(l)}$, $j = 1, \ldots, J_0$: кодовый вектор $(\mathbf{x}^{(1)}(i), \mathbf{x}^{(2)}(i))$ попадает в класс $\mathcal{X}_j^{(l)}$, если

$$(j-1)\frac{\zeta p_0 \tau}{J_0} < \sum_{k=1}^{\lceil \alpha_2 \tau^{(l)} \rceil} \|x_k^{(2)}\|^2 \leqslant j\frac{\zeta p_0 \tau}{J_0}. \tag{4.3.45а}$$

Поскольку компонента $\mathbf{x}^{(2)}$ передаваемого кодового вектора $\mathbf{x}$ удовлетворяет неравенству $\|\mathbf{x}^{(2)}\|^2 \leqslant \zeta \|\mathbf{x}\|^2$, каждый такой вектор $\mathbf{x}$ лежит в одном и только одном классе. (Договоримся, что нулевой кодовый вектор лежит в $\mathcal{X}_1^{(l)}$.) Класс $\mathcal{X}_j^{(l)}$, содержащий большинство кодовых векторов, обозначается через $\mathcal{X}_*^{(l)}$. Тогда, очевидно, $\#\mathcal{X}_*^{(l)} \geqslant M^{(l)}/J_0$ и скорость передачи R_* кода $\mathcal{X}_*^{(l)}$ подчиняется неравенству

$$R_* \geqslant R - \frac{1}{\tau^{(l)}} \ln J_0. \tag{4.3.45б}$$

С другой стороны, максимум вероятности ошибки для подкода $\mathcal{X}_*^{(l)}$ не больше, чем для всего кода $\mathcal{X}^{(l)}$ (при использовании одинакового декодера $d^{(l)}$); обратно, вероятность ошибки удовлетворяет соотношению $P_e^{\mathcal{X}_*^{(l)},\mathrm{av}}(d^{(l)}) \leqslant P_e^{(l)} \to 0$.

Имея фиксированное число J_0 классов разбиения $\mathcal{X}^{(l)}$, мы можем найти по крайней мере один такой $j_0 \in \{1, \ldots, J_0\}$, что для бесконечного числа l наиболее многочисленный класс $\mathcal{X}_*^{(l)}$ совпадает с $\mathcal{X}_{j_0}^{(l)}$. Ограничив наши рассуждения этими значениями l, мы можем предполагать, что $\mathcal{X}_*^{(l)} = \mathcal{X}_{j_0}^{(l)}$ $\forall l$. Тогда для всех $(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}) \in \mathcal{X}_*^{(l)}$, где $\mathbf{x}^{(i)} = \begin{pmatrix} x_1^{(i)} \\ \vdots \\ x_{n_i}^{(i)} \end{pmatrix}$, $i = 1, 2$ с помощью формул (4.3.38а) и (4.3.45а) получаем, что

$$\|\mathbf{x}^{(1)}\|^2 \leqslant \Big(1 - \frac{(j_0-1)\zeta}{J_0}\Big) p_0 \tau^{(l)}, \quad \|\mathbf{x}^{(2)}\|^2 \leqslant \Big(1 - \frac{j_0\zeta}{J_0}\Big) p_0 \tau^{(l)},$$

т. е. $\{(\mathcal{X}_*^{(l)}, d^{(l)})\}$ — последовательность кодеров/декодеров для «стандартного» параллельного подключения каналов (см. (4.3.34)), с вероятностями

$$p_1 = \left[1 - \frac{(j_0-1)\zeta}{J_0}\right] p_0 \quad \text{и} \quad p_2 = \frac{j_0\zeta}{J_0} p_0.$$

Поскольку вероятность ошибки $P_e^{\mathcal{X}_*^{(l)},\mathrm{av}}(d^{(l)}) \to 0$, скорость R^* надёжна для этой комбинации каналов. Следовательно, эта скорость не превосходит пропускную способность

$$R^* \leqslant C_1\Big(\Big(1 - \frac{(j_0-1)\zeta}{J_0}\Big) p_0\Big) + C_2\Big(\frac{j_0\zeta}{J_0} p_0\Big).$$

Здесь и далее мы имеем в виду определение $C_i(u)$ из формулы (4.3.44б), т. е.

$$R^* \leqslant C_1((1-\delta)p_0) + C_2(\delta p_0) + \frac{\varepsilon}{2}, \tag{4.3.46}$$

где $\delta = j_0\zeta/J_0$.

Заметим теперь, что для $\alpha_2 \geqslant \alpha_1$ функция

$$\delta \mapsto C_1((1-\delta)p_0) + C_2(\delta p_0)$$

возрастает по δ при $\delta < \alpha_2/(\alpha_1+\alpha_2)$ и убывает при $\delta > \alpha_2/(\alpha_1+\alpha_2)$. Значит, так как $\delta = j_0\zeta/J_0 \leqslant \zeta$, при $\zeta = \min[\beta,\ \alpha_2/(\alpha_1+\alpha_2)]$ мы получаем, что

$$C_1((1-\delta)p_0) + C_2(\delta p_0) \leqslant C_1(p_1) + C_2(p_2) = C^*. \tag{4.3.47}$$

В свою очередь, из этого соотношения совместно с формулами (4.3.45б), (4.3.46) и из формулы (4.3.47) следует, что

$$R \leqslant C^* + \frac{\varepsilon}{2} + \frac{1}{\tau^{(l)}}\ln J_0 \quad \text{или} \quad R \leqslant C^* + \frac{\varepsilon}{2}, \quad \text{где} \quad \tau^{(l)} \to \infty.$$

Противоречие с равенством $R = C^* + \varepsilon$ доказывает обратную часть. □

Пример 4.3.6. Вытянутые сфероидальные волновые функции (в. с. в. ф.) (см. [P2], [P3]). Для любых заданных $\tau,\ W > 0$ существует последовательность вещественных функций $\psi_1(t)$, $\psi_2(t)$, ... от переменной $t \in \mathbb{R}$, лежащих в гильбертовом пространстве $\mathbb{L}_2(\mathbb{R})$ (т. е. $\int \psi_n(t)^2 dt < \infty$), называемых вытянутыми сфероидальными волновыми функциями, удовлетворяющих следующим условиям.

1) Преобразования Фурье $\hat{\psi}_n(\omega) = \int \psi_n(t)e^{it\omega}dt$ равны 0 при $|\omega| > 2\pi W$; более того, функции $\psi_n(t)$ образуют ортонормированный базис в гильбертовом подпространстве в $\mathbb{L}_2(\mathbb{R})$, состоящем из функций с таким свойством.

2) Функции $\psi_n^\circ(t) := \psi_n(t)\mathbf{1}(|t| < \tau/2)$ (ограничение $\psi_n(t)$ на $(-\tau/2,\ \tau/2)$) попарно ортогональны:

$$\int \psi_n^\circ(t)\psi_{n'}^\circ(t)dt = \int\limits_{-\tau/2}^{\tau/2} \psi_n(t)\psi_{n'}(t)dt = 0, \quad \text{где} \quad n \neq n'. \tag{4.3.48а}$$

Более того, функции $\psi_n^\circ(t)$ образуют полную систему в $\mathbb{L}_2(-\tau/2,\ \tau/2)$: если $\varphi \in \mathbb{L}_2(-\tau/2,\ \tau/2)$ и $\int_{-\tau/2}^{\tau/2} \varphi(t)\psi_n(t)dt = 0\ \ \forall n \geqslant 1$, то $\varphi(t) = 0$ в $\mathbb{L}_2(-\tau/2,\ \tau/2)$.

3) При любом $n \geqslant 1$ и $t \in \mathbb{R}$ функции $\psi_n(t)$ удовлетворяют уравнениям

$$\lambda_n\psi_n(t) = 2W\int\limits_{-\tau/2}^{\tau/2} \psi_n(s)\mathrm{sinc}(2W\pi(t-s))ds, \tag{4.3.48б}$$

т. е. $\psi_n(t)$ — собственные функции с собственными значениями λ_n интегрального оператора $\varphi \mapsto \int \varphi(s)R(\cdot\,, s)\,ds$ с интегральным ядром

$$K(t, s) = \mathbf{1}(|s| < \tau/2)(2W)\mathrm{sinc}(2W(t-s)) = \\ = \mathbf{1}(|s| < \tau/2)\frac{\sin(2\pi W(t-s)}{\pi(t-s)}, \quad -\tau/2 \leqslant t,\, s \leqslant \tau/2.$$

4) Собственные числа λ_n удовлетворяют следующему свойству:

$$\lambda_n = \int\limits_{-\tau/2}^{\tau/2} \psi_n(t)^2 dt, \quad 1 > \lambda_1 > \lambda_2 > \ldots > 0.$$

Эквивалентную формулировку можно дать через преобразование Фурье $[\mathbf{F}\psi_n^\circ](\omega) = \int \psi_n^\circ(t)e^{it\omega}dt$:

$$\frac{1}{2\pi}\int\limits_{-2\pi W}^{2\pi W} \left|[\mathbf{F}\psi_n^\circ](\omega)\right|^2 d\omega \Big/ \int\limits_{-\tau/2}^{\tau/2} |\psi_n(t)|^2 dt = \lambda_n,$$

откуда следует, что λ_n даёт «концентрацию частоты» для усечённой функции ψ_n°.

5) Можно проверить, что функции $\psi_n(t)$ (а значит, и числа λ_n) зависят не от самих W и τ, а только от их произведения $W\tau$. Более того, $\forall\theta \in (0,\, 1)$ при $W\tau \to \infty$ имеем

$$\lambda_{\lceil 2W\tau(1-\theta)\rceil} \to 1 \quad \text{и} \quad \lambda_{\lceil 2W\tau(1+\theta)\rceil} \to 0. \tag{4.3.48в}$$

Иными словами, при больших τ около $2W\tau$ значений λ_n близки к 1, а остальные — к 0. □

14. Важной частью рассуждений является разложение Карунена—Лоэва. Предположим, что $Z(t)$ — гауссовский случайный процесс со спектральной плотностью $\Phi(\omega)$, заданной формулой (4.3.27). Разложение Карунена—Лоэва утверждает, что $\forall t \in (-\tau/2,\, \tau/2)$ с. в. $Z(t)$ можно записать как сходящийся (в среднеквадратичном) ряд

$$Z(t) = \sum_{n\geqslant 1} A_n\psi_n(t), \tag{4.3.49}$$

где $\psi_1(t)$, $\psi_2(t)$, ... — в. с. в. ф. из примера 4.3.6, а A_1, A_2, ... — н. о. р. с. в., $A_n \sim \mathrm{N}(0,\, \lambda_n)$, где λ_n — соответствующие собственные числа. Эквивалентно можно записать, что $Z(t) = \sum\limits_{n\geqslant 1} \sqrt{\lambda_n}\xi_n\psi_n(t)$, где $\xi_n \sim \mathrm{N}(0,\, 1)$ — н. о. р. с. в.

Доказательство этого факта выходит за рамки нашей книги, а заинтересованный читатель может ознакомиться с ним в книгах [DR] или [Lo], с. 144.

15. Идея доказательства теоремы 4.3.3 состоит в следующем. При данных W и τ входной сигнал $s^\circ(t)$ из $\mathcal{A}(\tau, W, p_0, \eta)$ представляется в виде ряда Фурье по в. с. в. ф. ψ_n. Первые $2W\tau$ слагаемых этого ряда представляют часть сигнала, заключённую между ограничивающими частотами $\pm 2\pi W$ и моментами времени $\pm\tau/2$. Представление шума $Z(t)$ тоже раскладывается в ряд по ψ_n. Тогда воздействие непрерывного по времени канала представляется в терминах параллельной комбинации дискретных по времени гауссовских каналов с совместным ограничением по мощности. Первый канал имеет дело с первыми $2W\tau$ в. с. в. ф. разложения сигнала, и для него $\alpha_1 = 2W$. Второй канал обрабатывает оставшуюся часть разложения, и для него $\alpha_2 = +\infty$. Ограничение по мощности $\|s\|^2 \leqslant p_0\tau$ приводит к совместному ограничению на каналы, как в формуле (4.3.38а). Кроме того, налагается требование, чтобы энергия, выделяющаяся за пределами ограничивающих частот $\pm 2\pi W$ или временно́го интервала, ограниченного $\pm\tau/2$, была невелика: это результат другого ограничения по мощности вида (4.3.38б). Результат примера 4.3.5 (случай I) даёт утверждение теоремы 4.3.3.

Последняя тау в Париже[2]

(Из серии «Фильмы, которые не вышли на большой экран».)

Для уточнения этой идеи мы сначала выведем теорему 4.3.7, которая предоставляет альтернативный подход к формуле Найквиста—Шеннона (более сложный по формулировке, но с несколько более простым (хотя все ещё довольно длинным) доказательством).

Теорема 4.3.7. *Рассмотрим следующую модификацию модели из теоремы* 4.3.3. *Множество допустимых сигналов* $\mathcal{A}_2(\tau, W, p_0, \eta)$ *состоит из таких функций* $t \in \mathbb{R} \mapsto s(t)$, *что* 1) $\|s\|^2 = \int |s(t)|^2 dt \leqslant p_0\tau$, 2) *преобразование Фурье* $[\mathbf{F}s](\omega) = \int s(t)e^{it\omega}dt$ *равно* 0 *при* $|\omega| > 2\pi W$, 3) $\int\limits_{-\tau/2}^{\tau/2} |s(t)|^2 dt \Big/ \|s\|^2 > 1 - \eta$. *Иначе говоря, функции* $s \in \mathcal{A}_2(\tau, W, p_0, \eta)$ *точно ограничены по частоте и почти локализованы по времени.*

Шумовой процесс является гауссовским со спектральной плотностью, равной нулю при $|\omega| > 2\pi W$ *и равной* σ_0^2 *при* $|\omega| \leqslant 2\pi W$. *Тогда пропускная способность такого канала равна*

$$C = C_\eta = W \ln\left(1 + (1-\eta)\frac{p_0}{2\sigma_0^2 W}\right) + \frac{\eta p_0}{2\sigma_0^2}. \tag{4.3.50}$$

[2] Ср. с названием фильма Бернардо Бертолуччи «Last Tango in Paris» (1972 г.).

При $\eta \to 0$ *выполняется соотношение*

$$C_\eta \to W \ln\left(1 + \frac{p_0}{2\sigma_0^2 W}\right)$$

что даёт формулу Найквиста—Шеннона (4.3.8).

Доказательство. Сначала проверим прямую часть утверждения. Возьмём

$$R < W \ln\left(1 + (1-\eta)\frac{p_0}{2\sigma_0^2 W}\right) + \frac{\eta p_0}{2\sigma_0^2} \tag{4.3.51}$$

и такие числа $\delta \in (0,\, 1)$, $\xi \in (0,\, \min[\eta,\, 1-\eta])$, что R всё ещё остаётся меньше чем

$$C^* = W(1-\delta)\ln\left(1 + \frac{(1-\eta+\xi)p_0}{2\sigma_0^2 W(1-\delta)}\right) + \frac{(\eta-\xi)p_0}{2\sigma_0^2}. \tag{4.3.52}$$

Согласно примеру 4.3.5 число C^* — пропускная способность двух параллельных дискретных по времени каналов с совместным ограничением по мощности, как в случае **??**. Положим

$$\alpha_1 = 2W(1-\delta), \quad \alpha_2 = +\infty, \quad \beta = \eta - \xi, \quad p = p_0, \quad \sigma^2 = \sigma_0^2 \tag{4.3.53}$$

(см. формулу (4.3.41a)). Мы хотим построить коды и правила декодирования для непрерывной по времени версии канала, для которого вероятность ошибки стремится к нулю при $\tau \to \infty$. Предположим, что $(\mathbf{x}^{(1)},\, \mathbf{x}^{(2)})$ — допустимый входной сигнал для параллельной пары дискретных по времени каналов, параметры которых даются в формуле (4.3.35). Тогда входной сигнал для непрерывного по времени канала — следующий ряд по $(W,\, \tau)$-в. с. в. ф.:

$$s(t) = \sum_{k=1}^{\lceil \alpha_1 \tau \rceil} x_k^{(1)} \psi_k(t) + \sum_{k=1}^{\infty} x_k^{(2)} \psi_{k+\lceil \alpha_1 \tau \rceil}(t). \tag{4.3.54}$$

Первое, что нужно проверить = это принадлежность сигнала из формулы (4.3.54) множеству $\mathcal{A}_2(\tau,\, W,\, p_0,\, \eta)$, т. е. то, что он обладает свойствами 1–3 из теоремы 4.3.7.

Для проверки первого из них запишем

$$\|s\|^2 = \sum_{k=1}^{\lceil \alpha_1 \tau \rceil} (x_k^{(1)})^2 + \sum_{k=1}^{\infty} (x_k^{(2)})^2 = \|x_k^{(1)}\|^2 + \|x_k^{(2)}\|^2 \leqslant p_0 \tau.$$

Далее, сигнал $s(t)$ ограничен по частоте, наследуя это свойство у в. с. в. ф. $\psi_k(t)$. Значит, условие 2 тоже имеет место.

Для проверки последнего свойства требуются более пространные рассуждения. Так как функции $\psi_k(t)$ ортогональны в $\mathbb{L}_2[-\tau/2,\, \tau/2]$ (см.

формулу (4.3.48а)), учитывая монотонность чисел λ_n (см. (4.3.48б)), мы получаем, что

$$1 - \int\limits_{-\tau/2}^{\tau/2} |s(t)|^2 dt \Big/ \|s\|^2 = \frac{\|(1 - D_\tau)s\|^2}{\|s\|^2} =$$

$$= \sum_{k=1}^{\lceil \alpha_1 \tau \rceil} \frac{(1 - \lambda_k)(x_k^{(1)})^2}{\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2} + \sum_{k=1}^{\infty} \frac{1 - \lambda_{k + \lceil \alpha_1 \tau \rceil})(x_k^{(2)})^2}{\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2} \leqslant$$

$$\leqslant (1 - \lambda_{\lceil \alpha_1 \tau \rceil}) \frac{\|\mathbf{x}^{(1)}\|^2}{\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2} + \frac{\|\mathbf{x}^{(2)}\|^2}{\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2}.$$

Далее, при $\tau \to \infty$ числа $\lambda_{\lceil \alpha_1 \tau \rceil} \to 1$ (см. формулу (4.3.48в)). Поскольку $\|\mathbf{x}^{(1)}\|^2 / (\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2) \leqslant 1$, мы получаем, что для достаточно больших τ выполняется неравенство

$$(1 - \lambda_{\lceil \alpha_1 \tau \rceil}) \frac{\|\mathbf{x}^{(1)}\|^2}{\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2} < \xi.$$

Кроме того, $\|\mathbf{x}^{(1)}\|^2 / (\|\mathbf{x}^{(1)}\|^2 + \|\mathbf{x}^{(2)}\|^2) \leqslant \eta - \xi$ (см. формулу (4.3.48б)), откуда, наконец, следует, что

$$1 - \int\limits_{-\tau/2}^{\tau/2} |s(t)| dt \Big/ \|s\|^2 = \frac{\|(1 - D_\tau)s\|^2}{\|s\|^2} \leqslant \xi + \eta - \xi = \eta,$$

т. е. выполняется свойство 3.

Далее, шум можно представить согласно разложению Карунена—Лоэва:

$$Z(t) = \sum_{k=1}^{\lceil \alpha_1 \tau \rceil} Z_k^{(1)} \psi_k(t) + \sum_{k=1}^{\infty} Z_k^{(2)} \psi_{k + \lceil \alpha_1 \tau \rceil}. \tag{4.3.55}$$

Здесь $\psi_k(t)$ тоже в. с. в. ф., и н. о. р. с. в. $Z_k^{(j)} \sim \mathrm{N}(0, \lambda_k)$. Выходной сигнал соответственно записывается как

$$Y(t) = \sum_{k=1}^{\lceil \alpha_1 \tau \rceil} Y_k^{(1)} \psi_k(t) + \sum_{k=1}^{\infty} Y_k^{(2)} \psi_{k + \lceil \alpha_1 \tau \rceil}, \tag{4.3.56}$$

где

$$Y_k^{(j)} = x_k^{(j)} + Z_k^{(j)}, \quad j = 1, 2, \quad k \geqslant 1. \tag{4.3.57}$$

Итак, непрерывный по времени канал эквивалентен параллельной комбинации каналов с совместным ограничением по мощности. Как мы проверили, пропускная способность, равна величине C^*, выписанной в формуле (4.3.52). Поэтому для $R < C^*$ мы можем построить такие коды скорости R и декодирующие правила, что вероятность ошибки стремится к 0.

Для доказательства противоположной части предположим, что существуют последовательность $\tau^{(l)} \to \infty$, последовательность $\mathcal{A}_2^{(l)}(\tau^{(l)},\, W,\, p_0,\, \eta^{(l)})$, заданная условиями 1–3 (и задающая допустимые для передачи сигналы), и последовательность кодов $\mathcal{X}^{(l)}$ размера $M = \lceil e^{R\tau^{(l)}} \rceil$, где

$$R > W \ln\left(1 + \frac{(1-\eta)p_0}{2W\sigma_0^2}\right) + \frac{\eta p_0}{\sigma_0^2}.$$

Как обычно, мы хотим показать, что вероятность ошибки $P_e^{\mathcal{X}^{(l)},\mathrm{av}}(d^{(l)})$ не стремится к нулю.

Как и ранее, мы берём $\delta > 0$ и $\xi \in (0,\, 1-\eta)$ для обеспечения неравенства $R > C^*$, где

$$C^* = W(1+\delta)\ln\left[1 + \frac{(1-\eta-\xi)}{(1-\xi)}\frac{p_0}{2W\sigma_0^2(1+\delta)}\right] + \frac{\eta p_0}{(1-\xi)\sigma_0^2}.$$

Тогда, как и при доказательстве прямой части, C^* — пропускная способность параллельного подключения каналов с совместным ограничением по мощности типа **??**, при этом

$$\beta = \frac{\eta}{1-\xi}, \quad \sigma^2 = \sigma_0^2, \quad p = p_0, \quad \alpha_1 = 2W(1+\delta), \quad \alpha_2 = +\infty. \quad (4.3.58)$$

Пусть $s(t) \in \mathcal{X}^{(l)} \cap \mathcal{A}_2^{(l)}(\tau^{(l)},\, W,\, p_0,\, \eta^{(l)})$ — кодовая функция, непрерывная по времени. Так как в. с. в. ф. $\psi_k(t)$ образуют ортогональный базис в $\mathbb{L}_2(\mathbb{R})$, мы можем разложить

$$s(t) = \sum_{k=1}^{\lceil \alpha_1 \tau^{(l)} \rceil} x_k^{(1)} \psi_k(t) + \sum_{k=1}^{\infty} x_k^{(2)} \psi_{k+\lceil \alpha_1 \tau^{(l)} \rceil}(t), \quad t \in \mathbb{R}. \quad (4.3.59)$$

Мы хотим показать, что дискретный по времени сигнал $\mathbf{x} = (\mathbf{x}^{(1)},\, \mathbf{x}^{(2)})$, представляет допустимый вход параллельного соединения каналов с совместным ограничением по мощности типа **??**, описанным в формуле (4.3.58). Ввиду ортогональности в. с. в. ф. $\psi_k(t)$ в $\mathbb{L}_2(\mathbb{R})$ мы можем записать

$$\|\mathbf{x}\|^2 = \|s\|^2 \leqslant p_0 \tau^{(l)},$$

что даёт уверенность в выполнении условия (4.3.38a). Далее, учитывая ортогональность функций $\psi_k(t)$ в $\mathbb{L}_2(-\tau/2,\, \tau/2)$ и тот факт, что собственные

числа λ_k монотонно убывают, мы получаем, что

$$1 - \int\limits_{-\tau^{(l)}/2}^{\tau^{(l)}/2} |s(t)|^2 dt \Big/ \|s\|^2 = \frac{\|(1 - D_{\tau^{(l)}})s\|^2}{\|s\|^2} = \sum_{k=1}^{\lceil \alpha_1 \tau^{(l)} \rceil} \frac{(1-\lambda_k)(x_k^{(1)})^2}{\|\mathbf{x}\|^2} + \\ + \sum_{k=1}^{\infty} \frac{(1-\lambda_{k+\lceil \alpha_1 \tau^{(l)} \rceil}(x_k^{(2)})^2}{\|\mathbf{x}\|^2} \geqslant (1 - \lambda_{k+\lceil \alpha_1 \tau^{(l)} \rceil}) \frac{\|\mathbf{x}^{(2)}\|^2}{\|\mathbf{x}\|^2}.$$

Согласно формуле (4.3.48в) при достаточно больших l имеем $\lambda_{\lceil \alpha_1 \tau^{(l)} \rceil} \leqslant \xi$. Более того, так как $1 - \int\limits_{-\tau^{(l)}/2}^{\tau^{(l)}/2} |s(t)|^2 dt \Big/ \|s\|^2 \leqslant \eta$, мы можем записать

$$\frac{\|\mathbf{x}^{(2)}\|^2}{\|\mathbf{x}\|^2} \leqslant \frac{\eta}{1-\xi}$$

и вывести свойство (4.3.38б).

Далее, как при доказательстве прямой части, мы вновь воспользуемся разложением Карунена—Лоэва шума $Z(t)$, чтобы вывести, что каждому коду для непрерывного по времени канала соответствует код для параллельной комбинации дискретных по времени каналов с совместным ограничением по мощности с теми же скоростью и вероятностью ошибки. Поскольку $R > C^*$, где C^* — пропускная способность дискретного по времени канала, вероятность ошибки $P_e^{\mathcal{X}^{(l)},\mathrm{av}}(d^{(l)})$ остаётся отделённой от нуля при $l \to \infty$, что приводит к противоречию. □

16. Доказательство теоремы 4.3.3 (набросок). Формальное рассуждение ведётся так же, как в теореме 4.3.7: нам нужно доказать прямую и обратную части теоремы. Напомним, что прямая часть утверждает, что пропускная способность не меньше величины C, указанной в формуле (4.3.31), в то время как обратная часть говорит, что пропускная способность не превосходит C. Для прямой части канал раскладывается в произведение двух параллельных каналов, как в случае III, при этом

$$\alpha_1 = 2W(1-\theta), \quad \alpha_2 = +\infty, \quad p = p_0, \quad \sigma^2 = \sigma_0^2, \quad \beta = \eta - \xi, \quad (4.3.60)$$

где $\theta \in (0, 1)$ (см. свойство 5 в. с. в. ф. в примере 4.3.6) и $\xi \in (0, \eta)$ — вспомогательные величины.

Для обратной части мы прибегаем к разложению на два параллельных канала, как в случае III, причём

$$\alpha_1 = 2W(1+\theta), \quad \alpha_2 = +\infty, \quad p = p_0, \quad \sigma^2 = \sigma_0^2, \quad \beta = \frac{\eta}{1-\xi}. \quad (4.3.61)$$

Здесь, как и ранее, число $\theta \in (0, 1)$ появляется из свойства 5 в. с. в. ф., а $\xi \in (0, 1)$.

17. Суммируя наши предыдущие наблюдения, мы получаем знаменитую лемму.

Лемма 4.3.8 (лемма о дискретизации Найквиста—Шеннона—Котельникова—Уиттекера). *Пусть f — функция из $\mathbb{R}$ в $\mathbb{R}$, $\int |f(t)|dt < +\infty$. Предположим, что преобразование Фурье*

$$[\mathbf{F}f](\omega) = \int e^{it\omega} f(t)dt$$

равно нулю при $|\omega| > 2\pi W$. Тогда $\forall x \in \mathbb{R}$ функцию f можно однозначно восстановить по её значениям $f(x + n/(2W))$, вычисленным в точках $x + n/(2W)$, где $n = 0, \pm 1, \pm 2$. Более точно, для любого $t \in \mathbb{R}$ выполняется равенство

$$f(t) = \sum_{n\in\mathbb{Z}^1} f\Big(\frac{n}{2W}\Big) \frac{\sin[2\pi(Wt - n)]}{2\pi(Wt - n)}. \tag{4.3.62}$$

Пример 4.3.9. По знаменитому принципу неопределённости в квантовой физике функцию и её преобразование Фурье нельзя одновременно локализовать в конечных отрезках $[-\tau, \tau]$ и $[-2\pi W, 2\pi W]$. Что можно сказать о том случае, когда и функция, и её преобразование Фурье почти локализованы? Как количественно описать принцип неопределенности в этом случае?

Решение. Рассмотрим функцию $f \in \mathbb{L}_2(\mathbb{R})$ и её преобразование Фурье $\hat{f} = \mathbf{F}f \in \mathbb{L}_2(\mathbb{R})$. (Напомним, что пространство $\mathbb{L}_2(\mathbb{R})$ состоит из функций f, для которых $\|f\|^2 = \int |f(t)|^2 dt < +\infty$, и что $\forall f, g \in \mathbb{L}_2(\mathbb{R})$ скалярное произведение $\int f(t)\bar{g}(t)dt$ конечно.) Мы увидим, что если

$$\int\limits_{t_0-\tau/2}^{t_0+\tau/2} |f(t)|^2 dt \Big/ \int\limits_{-\infty}^{+\infty} |f(t)|^2 dt = \alpha^2 \tag{4.3.63}$$

и

$$\int\limits_{-2\pi W}^{2\pi W} |\mathbf{F}f(\omega)|^2 d\omega \Big/ \int\limits_{-\infty}^{+\infty} |\mathbf{F}f(\omega)|^2 d\omega = \beta^2, \tag{4.3.64}$$

то $W\tau \geqslant \eta$, где $\eta = \eta(\alpha, \beta)$ будет найдено в явном виде. (Неравенство является точным, и функции, на которых достигается равенство, будут уточняться.)

Рассмотрим линейные операторы $f \in \mathbb{L}_2(\mathbb{R}) \mapsto Df \in \mathbb{L}_2(\mathbb{R})$ и $f \in \mathbb{L}_2(\mathbb{R}) \mapsto$ $\mapsto Bf \in \mathbb{L}_2(\mathbb{R})$, определённые формулами

$$Df(t) = f(t)\mathbf{1}(|t| \leqslant \tau/2) \tag{4.3.65}$$

и

$$Bf(t) = \frac{1}{2\pi} \int\limits_{-2\pi W}^{2\pi W} \mathbf{F}f(\omega) e^{-i\omega t} d\omega = \frac{1}{\pi} \int\limits_{-\infty}^{\infty} f(s) \frac{\sin 2\pi W(t-s)}{t-s} ds. \qquad (4.3.66)$$

Нас интересует произведение этих операторов $A = BD$:

$$Af(t) = \frac{1}{\pi} \int\limits_{-\tau/2}^{\tau/2} f(s) \frac{\sin 2\pi W(t-s)}{t-s} ds \qquad (4.3.67)$$

(см. пример 4.3.6). Собственные числа λ_n оператора A упорядочены $1 > \lambda_0 > \lambda_1 > \ldots$ и стремятся к нулю при $n \to \infty$ (см. [P3]). Нас интересует собственное число λ_0: можно показать, что λ_0 является функцией от произведения $W\tau$. Фактически, собственные функции (ψ_j) из формулы (4.3.48б) образуют ортогональный базис в $\mathbb{L}_2(\mathbb{R})$; в то же самое время эти функции образуют ортогональный базис в пространстве $\mathbb{L}_2[-\tau/2, \tau/2]$:

$$\int\limits_{-\tau/2}^{\tau/2} \psi_j(t)\psi_i(t)dt = \lambda_i \delta_{ij}.$$

Как обычно, угол между f и g в гильбертовом пространстве $\mathbb{L}_2(\mathbb{R})$ вычисляется по формуле

$$\theta(f, g) = \arccos\left(\frac{1}{\|f\|\,\|g\|} \Re \int f(t)\bar{g}(t)dt\right). \qquad (4.3.68)$$

Угол между двумя подпространствами определяется как минимальный угол между векторами этих подпространств. Мы покажем, что существует положительный угол $\theta(\mathcal{B}, \mathcal{D})$ между подпространствами $\mathcal{B}$ и $\mathcal{D}$ — образами операторов B и D, т. е. $\mathcal{B}$ — линейное подпространство всех функций с ограниченными частотами, в то время как $\mathcal{D}$ состоит из функций, ограниченных по времени. Более того,

$$\theta(\mathcal{B}, \mathcal{D}) = \arccos\sqrt{\lambda_0}, \qquad (4.3.69)$$

и минимальный угол $\theta(f, g)$ между этими подпространствами реализуется на $f = \psi_0$, $g = D\psi_0$, где ψ_0 — (единственная) собственная функция с собственным числом λ_0.

В качестве завершающего штриха мы проверим, что для любой функции $f \in \mathcal{B}$ выполняется равенство

$$\min_{g \in \mathcal{D}} \theta(f, g) = \arccos \frac{\|Df\|}{\|f\|}. \qquad (4.3.70)$$

Действительно, представим функцию f в виде $f = f - Df + Df$ и заметим, что $\int [f(t) - Df(t)]g(t)dt = 0$ (так как носители g и $f - Df$ не пересекаются).

Отсюда следует, что

$$\left|\Re \int f(t)\bar{g}(t)dt\right| \leqslant \left|\int f(t)\bar{g}(t)dt\right| = \left|\int Df(t)\bar{g}(t)dt\right|.$$

Таким образом,

$$\frac{1}{\|f\|\,\|g\|}\Re \int f(t)\bar{g}(t)dt \leqslant \frac{\|Df\|}{\|f\|},$$

откуда получаем равенство (4.3.70), положив $g = Df$.

Разложим f в ряд по собственным функциям оператора A: $f = \sum\limits_{n=0}^{\infty} a_n\psi_n$ и получим формулу

$$\arccos\frac{\|Df\|}{\|f\|} = \arccos\left(\frac{\sum_n |a_n|^2\lambda_n}{\sum_n |a_n|^2}\right)^{1/2} \tag{4.3.71}$$

Супремум правой части по f достигается, когда $a_n = 0$ при $n \geqslant 1$ и $f = \psi_0$. Можно сделать вывод, что существует минимальный угол между подпространствами $\mathcal{B}$ и $\mathcal{D}$, и достигается он на паре функций $f = \psi_0$ и $g = D\psi_0$, что и требовалось.

Далее мы докажем следующую лемму.

Лемма 4.3.10. *Существует такая функция $f \in \mathbb{L}_2$, что $\|f\| = 1$, $\|Df\| = \alpha$ и $\|Bf\| = \beta$ тогда и только тогда, когда α и β попадают в одну из следующих групп* 1)–4):

1) $\alpha = 0$ *и* $0 \leqslant \beta < 1$;

2) $0 < \alpha < \sqrt{\lambda_0} < 1$ *и* $0 \leqslant \beta \leqslant 1$;

3) $\sqrt{\lambda_0} \leqslant \alpha < 1$ *и* $\arccos\alpha + \arccos\beta \geqslant \arccos\sqrt{\lambda_0}$,

4) $\alpha = 1$ *и* $0 < \beta \leqslant \sqrt{\lambda_0}$.

Доказательство. Возьмём $\alpha \in [0, 1]$. Обозначим через $\mathcal{G}(\alpha)$ семейство функций $f \in \mathbb{L}_2$ с нормой $\|f\| = 1$ и $\|Df\| = \alpha$. Положим $\beta^*(\alpha) := \sup\limits_{f\in\mathcal{G}(\alpha)} \|Bf\|$.

1. Если $\alpha = 0$, то семейство $\mathcal{G}(0)$ может не содержать таких функций, что $\beta = \|Bf\| = 1$. Более того, если $\|Df\| = 0$ и $\|Bf\| = 1$ для $f \in \mathcal{B}$, то из условия аналитичности f и соотношения $f(t) = 0$ при $|t| < \tau/2$ следует тождество $f \equiv 0$. Чтобы показать наличие в множестве $\mathcal{G}(0)$ функций со всеми значениями $\beta \in [0, 1)$, положим $\tilde{f}_n = \dfrac{\psi_n - D\psi_n}{\sqrt{1-\lambda_n}}$. Тогда $\|B\tilde{f}_n\| = \sqrt{1-\lambda_n}$. Поскольку существуют собственные числа λ_n сколь угодно близкие к 0, то норма $\|B\tilde{f}_n\|$ может быть сколь угодно близкой к 1. Рассматривая функции

$e^{ipt}\tilde{f}(t)$, мы можем получить все значения β между точками $\sqrt{1-\lambda_n}$, так как

$$\|Be^{ipt}\tilde{f}\| = \left(\int\limits_{p-\pi W}^{-p+\pi W} |F_n(\omega)|^2 d\omega\right)^{1/2}.$$

Норма $\|Be^{ipt}\tilde{f}\|$ непрерывна по p и стремится к 0 при $p \to \infty$. Это завершает анализ первого случая.

2. Если $0 < \alpha < \sqrt{\lambda_0} < 1$, то мы положим

$$\tilde{f} = \frac{\sqrt{\alpha^2 - \lambda_n}\psi_0 - \sqrt{\lambda_0 - \alpha^2}\psi_n}{\sqrt{\lambda_0 - \lambda_n}}$$

для достаточно больших n, когда λ_n близко к 0. Мы имеем $\tilde{f} \in \mathcal{B}$, $\|\tilde{f}\| = \|B\tilde{f}\| = 1$, в то время как простые вычисления показывают, что $\|D\tilde{f}\| = \alpha$. Это включает в себя случай $\beta = 1$, так как, выбирая $e^{ipt}\tilde{f}(t)$, мы соответственно можем получить любое значение $0 < \beta < 1$.

3 и 4. Если $\sqrt{\lambda_0} \leqslant \alpha < 1$, мы разложим $f \in \mathcal{G}(\alpha)$ следующим образом:

$$f = \alpha_1 Df + \alpha_2 Bf + g, \tag{4.3.72}$$

где функция g ортогональна как Df, так и Bf. Вычисляя скалярное произведение п. ч. формулы (4.3.72) соответственно с f, Df, Bf и g, мы получим четыре уравнения:

$$\begin{aligned} 1 &= a_1\alpha^2 + a_2\beta^2 + \int g(t)\bar{f}(t)dt, \\ \alpha^2 &= a_1\alpha^2 + a_2 \int Bf(t)\overline{Dg}(t)dt, \\ \beta^2 &= a_1 \int Df(t)\overline{Bf}(t)dt + a_2\beta^2, \\ \int f(t)\bar{g}(t)dt &= \|g\|^2. \end{aligned}$$

Из уравнений следует, что

$$\alpha^2 + \beta^2 - 1 + \|g\|^2 = a_1 \int Df(t)\overline{Bf}(t)dt + a_2 \int Bf(t)\overline{Df}(t)dt.$$

Исключая $\int g(t)\bar{f}(t)dt$, a_1 и a_2, для $\alpha\beta \neq 0$ мы найдём, что

$$\beta^2 = \frac{1-\alpha^2-\|g\|^2}{\beta^2 - \int Bf(t)\overline{Df}(t)dt}\beta^2 + \\ + \left[1 - \frac{1-\alpha^2-\|g\|^2}{\alpha^2(\beta^2 - \int Bf(t)\overline{Df}(t)dt)} \int Bf(t)\overline{Df}(t)dt\right] \int Df(t)\overline{Bf}(t)dt,$$

что эквивалентно неравенству

$$\beta^2 - 2\Re \int Df(t)\overline{Bf}(t)dt \leqslant -\alpha^2 + \Big(1 - \frac{1}{\alpha^2\beta^2}\Big|\int Df(t)\overline{Bf}(t)dt\Big|^2\Big) - \\ - \|g\|^2\Big(1 - \frac{1}{\alpha^2\beta^2}\Big|\int Df(t)\overline{Bf}(t)dt\Big|^2\Big). \quad (4.3.73)$$

В терминах угла θ можно записать

$$\alpha\beta\cos\theta = \Re\int Df(t)\overline{Bf}(t)dt \leqslant \Big|\int Df(t)\overline{Bf}(t)dt\Big| \leqslant \alpha\beta.$$

Подставляя это соотношение в формулу (4.3.73) и дополняя до квадрата, получаем, что

$$(\beta - \alpha\cos\theta)^2 \leqslant (1-\alpha^2)\sin^2\theta, \quad (4.3.74)$$

где равенство достигается тогда и только тогда, когда $g = 0$ и интеграл $\int Df(t)\overline{Bf}(t)dt$ вещественен. Поскольку $\theta \geqslant \arccos\sqrt{\lambda_0}$, из формулы (4.3.74) следует, что

$$\arccos\alpha + \arccos\beta \geqslant \arccos\sqrt{\lambda_0}. \quad (4.3.75)$$

Геометрическое место точек (α, β), удовлетворяющих формуле (4.3.75), лежат правее и выше кривой, описываемой равенством

$$\arccos\alpha + \arccos\beta = \arccos\sqrt{\lambda_0} \quad (4.3.76)$$

(см. рис. 4.6).

Соотношение (4.3.76) выполняется для функции $\tilde{f} = b_1\psi_0 + b_2 D\psi_0$ с коэффициентами

$$b_1 = \sqrt{\frac{1-\alpha^2}{1-\lambda_0}} \quad \text{и} \quad b_2 = \frac{\alpha}{\sqrt{\lambda_0}} - \sqrt{\frac{1-\alpha^2}{1-\lambda_0}}.$$

Все промежуточные значения β опять получаются за счёт выбора $e^{ipt}\tilde{f}$. □

> Quantum physicists are so poor in bed because when they find the position, they can't have the momentum, and when they have the momentum, they can't find the position.
>
> (Из серии «Почему их не понимают».)

> Quantum physicists can either know how fast they do it, or where they do it, but not both.
>
> (Из серии «Как они делают это».)

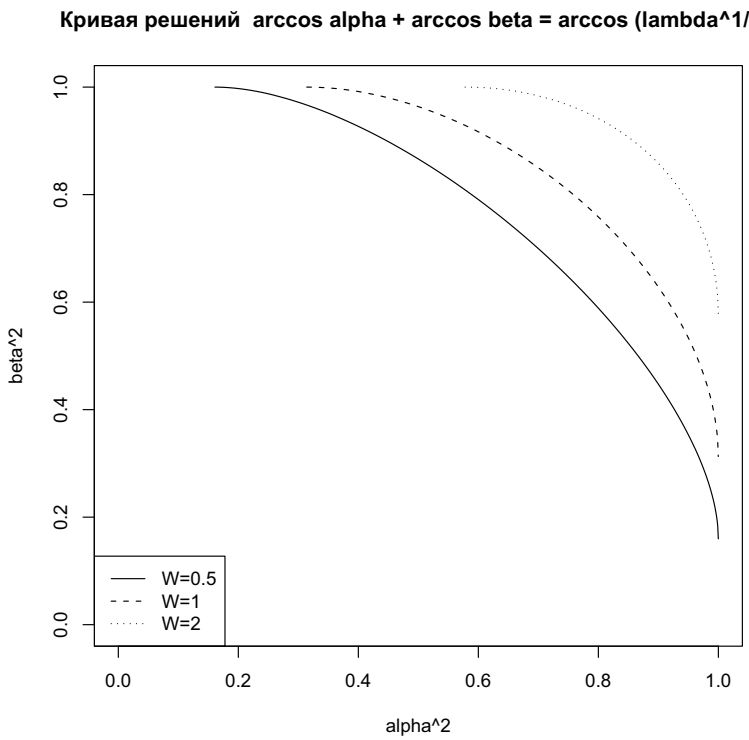


Рис. 4.6

§ 4.4. Пространственные точечные процессы и сетевая теория информации

Для обсуждения пропускной способности распределенных систем и построения случайных кодовых книг, основанных на точечных процессах, нам потребуются некоторые предварительные сведения. Здесь мы изучаем пространственные процессы Пуассона в $\mathbb{R}^d$ и вводим некоторые более сложные модели точечных процессов с хорошими кодовыми расстояниями. Этот параграф можно читать независимо от тома 2, хотя некоторые факты оттуда могут оказаться очень полезны.

Определение 4.4.1 (см. том 2, с. 211). Пусть μ — мера на $\mathbb{R}$ со значениями $\mu(A)$ на измеримых подмножествах $A \subseteq \mathbb{R}$. Предположим, что мера μ 1) *безатомная* и 2) σ-*конечная*, т. е. 1) $\mu(A) = 0$ для любого

счётного множества $A \subset \mathbb{R}$ и 2) существует разбиение $\mathbb{R} = \bigcup_j J_j$ на такие попарно непересекающиеся интервалы $J_1, J_2, \ldots,$ что $\mu(J_j) < \infty$. Будем говорить, что считающая мера M определяет *случайную меру Пуассона* (для краткости СМП) со средней мерой, или интенсивностью, μ, если для любого набора попарно непересекающихся интервалов $I_1, \ldots, I_n$ на $\mathbb{R}$ с. в. $M(I_k)$, $k = 1, \ldots, n$, независимы и $M(I_k) \sim \mathrm{Po}(\mu(I_k))$. □

Сформулируем без доказательства несколько фактов о существовании и свойствах случайных мер Пуассона, введённых в определении 4.4.1.

Теорема 4.4.2. *Для любой безатомной σ-конечной меры μ на $\mathbb{R}_+$ существует единственная СМП, удовлетворяющая определению* 4.4.1. *Если мера μ имеет вид $\mu(dt) = \lambda dt$, где $\lambda > 0$ — константа, то эта СМП является процессом Пуассона* $\mathrm{PP}(\lambda)$. *Если мера μ имеет вид $\mu(dt) = \lambda(t)dt$, где $\lambda(t)$ — данная функция, то эта СМП даёт неоднородный процесс Пуассона* $\mathrm{PP}(\lambda(t))$.

Теорема 4.4.3 (теорема об отображении). *Пусть μ — такая безатомная и σ-конечная мера на $\mathbb{R}$, что $\forall t \geqslant 0$ и $h > 0$ мера $\mu(t, t+h)$ интервала $(t, t+h)$ положительна и конечна* (*т. е. значение* $\mu(t, t+h) \in (0, \infty)$), *причём* $\lim_{h\to 0} \mu(0, h) = 0$ *и* $\mu(\mathbb{R}_+) = \lim_{u\to+\infty} \mu(0, u) = +\infty$. *Рассмотрим функцию*

$$f\colon u \in \mathbb{R}_+ \mapsto \mu(0, u),$$

и пусть f^{-1} — обратная функция к f (*она существует, поскольку функция $f(u) = \mu(0, u)$ строго монотонна по u*). *Пусть M — СМП (μ). Определим случайную меру f^*M как*

$$(f^*M)(I) = M(\mu(f^{-1}(I)) = M(\mu(f^{-1}(a), f^{-1}(b))) \tag{4.4.1}$$

для интервала $I = (a, b) \subset \mathbb{R}_+$ и продолжим её на $\mathbb{R}$. Тогда $f^*M \sim \mathrm{PP}(1)$, т. е. f^*M задаёт процесс Пуассона с единичной интенсивностью.

Проиллюстрируем сказанное выше парой примеров.

Пример 4.4.4. Пусть интенсивность процесса Пуассона $\Pi = \mathrm{PP}(\lambda(x))$ на интервале $S = (-1, 1)$ равна

$$\lambda(x) = (1 + x)^{-2}(1 - x)^{-3}.$$

Покажите, что Π с вероятностью 1 имеет бесконечно много точек на S, и что их можно обозначить по возрастанию как

$$\ldots X_{-2} < X_{-1} < X_0 < X_1 < X_2 < \ldots,$$

причём $X_0 < 0 < X_1$.

Покажите, что существует такая возрастающая функция $f\colon S \to \mathbb{R}$ с $f(0) = 0$, что точки $f(X)$ $(X \in \Pi)$ образуют процесс Пуассона с единичной

интенсивностью на $\mathbb{R}$, и, опираясь на усиленный закон больших чисел (у. з. б. ч.), покажите, что с вероятностью 1 выполняется равенство

$$\lim_{n\to\infty} (2n)^{1/2}(1 - X_n) = \frac{1}{2}. \tag{4.4.2}$$

Найдите предел при $n \to -\infty$.

Решение. Так как

$$\int_{-1}^{1} \lambda(x)dx = \infty,$$

с вероятностью 1 существует бесконечно много точек из Π на $(-1, 1)$. С другой стороны,

$$\int_{-1+\delta}^{1-\delta} \lambda(x)dx < \infty$$

для каждого $\delta > 0$, так что с. в. $\Pi(-1 + \delta, 1 - \delta)$ конечна с вероятностью 1. Этого достаточно для однозначной нумерации точек из Π в возрастающем порядке. Пусть

$$f(x) = \int_{0}^{x} \lambda(y)dy.$$

Поскольку функция $f\colon S \to \mathbb{R}$ возрастает, она отображает Π в процесс Пуассона, средняя мера которого определяется формулой

$$\mu(a, b) = \int_{f^{-1}(a)}^{f^{-1}(b)} \lambda(x)dx = b - a.$$

При таком выборе f точки $(f(X_n))$ образуют процесс Пуассона с единичной интенсивностью на $\mathbb{R}$. У. з. б. ч. показывает, что при $n \to \infty$ с вероятностью 1 выполняется соотношение

$$n^{-1}f(X_n) \to 1 \quad \text{и} \quad n^{-1}f(X_{-n}) \to -1.$$

Заметим теперь, что

$$\lambda(x) \sim \frac{1}{4}(1 - x)^{-3} \quad \text{и} \quad f(x) \sim \frac{1}{8}(1 - x)^{-2} \qquad \text{при } x \to 1.$$

Следовательно, при $n \to \infty$ с вероятностью 1 имеем, что

$$n^{-1}\frac{1}{8}(1 - X_n)^{-2} \to 1,$$

что эквивалентно условию (4.4.2). Аналогично из соотношений

$$\lambda(x) \sim \frac{1}{8}(1 + x)^{-2} \quad \text{и} \quad f(x) \sim \frac{1}{8}(1 + x)^{-1} \qquad \text{при } x \to -1$$

следует, что с вероятностью 1

$$\frac{1}{8n}(1+X_n)^{-1}\to 1 \quad \text{при } n\to\infty,$$

откуда с вероятностью 1 имеем, что

$$\lim_{n\to\infty} n(1+X_{-n})=\frac{1}{8}. \qquad \square$$

Пример 4.4.5. Покажите, что если $Y_1<Y_2<Y_3<\ldots$ — точки процесса Пуассона на $(0,\infty)$ с постоянной интенсивностью λ, то

$$\lim_{n\to\infty}\frac{Y_n}{n}=\lambda$$

с вероятностью 1. Пусть интенсивность процесса Пуассона $\Pi=\mathrm{PP}(\lambda(x))$ на $(0,1)$ равна

$$\lambda(x)=x^{-2}(1-x)^{-1}.$$

Покажите, что точки из Π можно пронумеровать как

$$\ldots<X_{-2}<X_{-1}<\frac{1}{2}<X_0<X_1<\ldots$$

и что

$$\lim_{n\to-\infty}X_n=0, \qquad \lim_{n\to\infty}X_n=1.$$

Докажите, что с вероятностью 1 выполняется соотношение

$$\lim_{n\to\infty} nX_{-n}=1$$

Что можно сказать о пределе X_n при $n\to+\infty$?

Решение. Первая часть тоже следует из у. з. б. ч. Для доказательства второй части положим

$$f(x)=\int_{1/2}^{x}\lambda(\xi)d\xi$$

и воспользуемся тем, что f отображает Π в процесс Пуассона с постоянной интенсивностью на $(f(0),f(1))$, $f(\Pi)=\mathrm{PP}(1)$. В нашем случае $f(0)=-\infty$ и $f(1)=\infty$, так что $f(\Pi)$ — ПП на $\mathbb{R}$. Точки процесса можно пронумеровать как

$$\ldots Y_{-2}<Y_{-1}<0<Y_0<Y_1<\ldots,$$
$$\lim_{n\to-\infty}Y_n=-\infty, \qquad \lim_{n\to+\infty}Y_n=+\infty.$$

Тогда $X_n=f^{-1}(Y_n)$ обладает нужными свойствами.

Применяя у. з. б. ч. к Y_{-n}, получаем, что

$$\lim_{n\to-\infty}\frac{f(X_n)}{n}=\lim_{n\to-\infty}\frac{Y_n}{n}=1 \text{ почти всюду.}$$

Далее, из того, что

$$f(x) = -\int_x^{1/2} \xi^{-2}(1-\xi)^{-1}d\xi \sim -\int_x^{1/2} \xi^{-2}d\xi \sim -x^{-1} \quad \text{при } x \to 0,$$

получаем

$$\lim_{n\to\infty} \frac{X_{-n}^{-1}}{n} = 1, \quad \text{т. е.} \quad \lim_{n\to\infty} nX_{-n} = 1 \text{ почти всюду.}$$

Аналогично

$$\lim_{n\to+\infty} \frac{f(X_n)}{n} = 1 \text{ почти всюду,}$$

и при $x \to 1$ получаем, что

$$f(x) \sim \int_{1/2}^{x} (1-\xi)^{-1}d\xi \sim -\ln(1-x).$$

Отсюда следует, что

$$\lim_{n\to\infty} -\frac{\ln(1-X_n)}{n} = 1 \text{ почти всюду.} \qquad \square$$

Далее мы обсудим понятие случайной меры Пуассона (СМП) на общем множестве E. Формально мы предполагаем, что E снабжено σ-алгеброй $\mathcal{E}$ подмножеств, а мера μ сопоставляет каждому подмножеству $A \in \mathcal{E}$ число $\mu(A)$, так что если $A_1, A_2, \ldots$ — попарно непересекающиеся подмножества из $\mathcal{E}$, то

$$\mu\Big(\bigcup_n A_n\Big) = \sum_n \mu(A_n).$$

Величина $\mu(E)$ может быть как конечной, так и бесконечной. Наша цель — определить случайную целочисленную меру $M = (M(A),\ A \in \mathcal{S})$ со следующими свойствами.

1. С. в. $M(A)$ принимает неотрицательные целые значения (включая, возможно, $+\infty$). Более того,

$$M(A) \begin{cases} \sim \text{Po}(\lambda\mu(A)), & \text{если } \mu(A) < \infty, \\ = +\infty \text{ с вероятностью 1}, & \text{если } \mu(A) = \infty. \end{cases} \tag{4.4.3}$$

2. Если $A_1, A_2, \ldots \in \mathcal{E}$ — непересекающиеся подмножества, то

$$M\Big(\bigcup_i A_i\Big) = \sum_i M(A_i). \tag{4.4.4}$$

3. С. в. $M(A_1), M(A_2), \ldots$ независимы, если множества $A_1, A_2, \ldots \in \mathcal{E}$ не пересекаются, т. е. для любого конечного набора непересекающихся

множеств $A_1, \ldots, A_n \in \mathcal{E}$ и неотрицательных целых $k_1, \ldots, k_n$ выполняется равенство

$$\mathsf{P}(M(A_i) = k_i,\ \ 1 \leqslant i \leqslant n) = \prod_{i=1}^{n} \mathsf{P}(M(A_i) = k_i). \tag{4.4.5}$$

Предположим сначала, что $\mu(E) < \infty$ (если нет, расщепим E на подмножества конечной меры). Фиксируем с. в. $M(E) \sim \mathrm{Po}(\lambda\mu(E))$. Рассмотрим последовательность $X_1, X_2, \ldots$ н. о. р. случайных точек в E, $X_i \sim \mu/\mu(E)$ независимо от $M(E)$. Это означает, что $\forall n \geqslant 1$ и любых множеств $A_1, \ldots, A_n \in \mathcal{E}$ (не обязательно непересекающихся)

$$\mathsf{P}(M(E) = n,\, X_1 \in A_1, \ldots, X_n \in A_n) = e^{-\lambda\mu(E)} \frac{(\lambda\mu(E))^n}{n!} \prod_{i=1}^{n} \frac{\mu(A_i)}{\mu(E)} \tag{4.4.6}$$

и условно

$$\mathsf{P}(X_1 \in A_1, \ldots, X_n \in A_n | M(E) = n) = \prod_{i=1}^{n} \frac{\mu(A_i)}{\mu(E)}. \tag{4.4.7}$$

Тогда положим

$$M(A) = \sum_{i=1}^{M(E)} \mathbf{1}(X_i \in A),\ \ A \in \mathcal{E}. \tag{4.4.8}$$

Теорема 4.4.6. *Если* $\mu(E) < \infty$, *то формула* (4.4.8) *определяет случайную меру* M *на* E, *удовлетворяющую перечисленным выше свойствам* 1–3.

Пример 4.4.7. Пусть M — случайная мера Пуассона интенсивности λ на плоскости $\mathbb{R}^2$. Обозначим через $C(r)$ круг $\{\mathbf{x} \in \mathbb{R}^2 \colon |\mathbf{x}| < r\}$ радиуса r на $\mathbb{R}^2$ с центром в начале координат, и пусть R_k — наибольший радиус круга $C(R_k)$, содержащего ровно k точек из M. (Так, $C(R_0)$ — наибольший круг с центром в начале координат, не содержащий точек из M; $C(R_1)$ — наибольший круг с центром в начале координат, содержащий единственную точку из M, и т. д.) Вычислите $\mathsf{E}R_0$, $\mathsf{E}R_1$ и $\mathsf{E}R_2$.

Решение. Ясно, что

$$\mathsf{P}(R_0 > r) = \mathsf{P}(C(r) \text{ не содержит точек из } M) = e^{-\lambda\pi r^2},\ \ r > 0,$$

и

$$\mathsf{P}(R_1 > r) = \mathsf{P}(C(r) \text{ содержит не более одной точки из } M) = \\ = (1 + \lambda\pi r^2) e^{-\lambda\pi r^2},\ \ r > 0.$$

Аналогично

$$\mathsf{P}(R_2 > r) = \left[1 + \lambda\pi r^2 + \frac{1}{2}(\lambda\pi r^2)^2\right] e^{-\lambda\pi r^2},\ \ r > 0.$$

Тогда

$$\mathsf{E}R_0 = \int_0^\infty \mathsf{P}(R_0 > r)dr = \frac{1}{\sqrt{2\pi\lambda}} \int_0^\infty e^{-\pi\lambda r^2} d(\sqrt{2\pi\lambda}r) = \frac{1}{2\sqrt{\lambda}},$$

$$\mathsf{E}R_1 = \int_0^\infty \mathsf{P}(R_1 > r)dr = \frac{1}{2\sqrt{\lambda}} + \int_0^\infty e^{-\pi\lambda r^2}(\lambda\pi r^2)dr =$$

$$= \frac{1}{2\sqrt{\lambda}} + \frac{1}{2\sqrt{2\pi\lambda}} \int_0^\infty (2\pi\lambda r^2) e^{-\pi\lambda t^2} d(\sqrt{2\pi\lambda}r) = \frac{3}{4\sqrt{\lambda}},$$

$$\mathsf{E}R_2 = \frac{3}{4\sqrt{\lambda}} + \int_0^\infty \frac{(\lambda\pi r^2)^2}{2} e^{-\pi\lambda r^2} dr = \frac{3}{4\sqrt{\lambda}} +$$

$$+ \frac{1}{8\sqrt{2\pi\lambda}} \int_0^\infty (2\lambda\pi r^2)^2 e^{-\pi\lambda r^2} d(\sqrt{2\lambda\pi}r) = \frac{3}{4\sqrt{\lambda}} + \frac{3}{16\sqrt{\lambda}} = \frac{15}{16\sqrt{\lambda}}. \quad \square$$

СМП M на фазовом пространстве E интенсивности μ, построенную в теореме 4.4.6, мы будем обозначать символом $\mathrm{PRM}(E, \mu)$. Далее мы обобщим определение СМП на интегральные суммы: для любой функции $g\colon E \to \mathbb{R}_+$ определим

$$M(g) = \sum_{i=1}^{M(E)} g(X_i) := \int g(y)dM(y), \tag{4.4.9}$$

где сумма берётся по всем точкам $X_i \in E$, $M(E)$ — общее число таких точек. Для общей функции $g\colon E \to \mathbb{R}$ мы положим

$$M(g) = M(g_+) - M(g_-)$$

со стандартным соглашением, что $+\infty - a = +\infty$ и $a - \infty = -\infty$ $\forall a \in (0, \infty)$ (когда и $M(g_+)$, и $M(g_-)$ равны бесконечности, будем считать, что значение $M(g)$ не определено). Тогда имеет место следующая

Теорема 4.4.8 (теорема Кэмпбелла). *Для всех $\theta \in \mathbb{R}$ и всех таких функций $g\colon E \to \mathbb{R}$, таких что $e^{\theta g(y)} - 1$ является μ-интегрируемой функцией, выполняется равенство*

$$\mathsf{E}e^{\theta M(g)} = \exp\left(\lambda \int_E (e^{\theta g(y)} - 1)d\mu(y)\right). \tag{4.4.10}$$

Доказательство. Запишем

$$\mathsf{E}e^{\theta M(g)} = \mathsf{E}\left[\mathsf{P}(e^{\theta M(g)} | M(E))\right] =$$

$$= \sum_k \mathsf{P}((M(E) = k)\, \mathsf{E}\left(\exp\left[\theta \sum_{i=1}^k g(X_i)\right] \middle| M(E) = k\right).$$

Учитывая условную независимость (4.4.7), получаем, что

$$\mathsf{E}\left(\exp\left[\theta\sum_{i=1}^{k} g(X_i)\right]\Big| M(E)=k\right)=\prod_{i=1}^{k}\mathsf{E}e^{\theta g(X_i)}=(\mathsf{E}e^{\theta g(X_1)})^k=$$

$$=\left(\frac{1}{\mu(E)}\int\limits_E e^{\theta g(x)}d\mu(x)\right)^k$$

и

$$\mathsf{E}e^{\theta M(g)}=\sum_k e^{-\lambda\mu(E)}\frac{(\lambda\mu(E))^k}{k!}\frac{1}{(\mu(E))^k}\left(\int\limits_E e^{\theta g(x)}d\mu(x)\right)^k=$$

$$=e^{-\lambda\mu(E)}\exp\left[\lambda\int\limits_E e^{\theta g(x)}d\mu(x)\right]=\exp\left[\lambda\int\limits_E(e^{\theta g(x)}-1)d\mu(x)\right]. \quad \square$$

Следствие 4.4.9. *Математическое ожидание с. в.* $M(g)$

$$\mathsf{E}M(g)=\int\limits_E g(y)d\mu(y)$$

существует тогда и только тогда, когда интеграл в правой части корректно определён.

Доказательство получается из вычисления производной производящей функции моментов (п. ф. м.) в точке $\theta=0$. $\square$

Пример 4.4.10. Предположим, что радиопередатчики расположены в точках процесса Пуассона Π на $\mathbb{R}^2$ интенсивности λ. Пусть r_i — расстояние от i-го передатчика до центрального приёмника, расположенного в нуле, а минимальное расстояние до передатчика равно r_0. Предположим, что мощность полученного сигнала $Y=\sum\limits_{X\in\Pi}\dfrac{P}{r_i^\alpha}$ для некоторого $\alpha>2$. Тогда

$$\mathsf{E}e^{\theta Y}=\exp\left[2\lambda\pi\int\limits_{r_0}^{\infty}(e^{\theta g(r)}-1)rdr\right], \tag{4.4.11}$$

где $g(r)=P/r^\alpha$, а P — мощность передачи. $\square$

Известной моделью в приложениях является так называемый маркированный точечный процесс с пространством марок D. Это просто целочисленная случайная мера на $\mathbb{R}^d\times D$ или на его подмножестве. Нам потребуется следующее свойство произведения, доказанное ниже в простейших предположениях.

Теорема 4.4.11 (теорема о произведении). *Предположим, что на* $\mathbb{R}$ *задан процесс Пуассона постоянной интенсивности* λ *и н. о. р. марками* Y_i *с распределением* ν. *Определим случайную меру* M *на*

$\mathbb{R}_+ \times D$ *по формуле*

$$M(F) = \sum_{n=1}^{\infty} \mathbf{1}((T_n,\, Y_n) \in A), \quad A \subseteq \mathbb{R}_+ \times D. \tag{4.4.12}$$

Эта мера является случайной мерой Пуассона (*СМП*) *на* $\mathbb{R}_+ \times D$ *интенсивности* $\lambda m \times \nu$, *где* m *— мера Лебега.*

Доказательство. Рассмотрим сначала множество $A \subseteq [0,\, t) \times D$, где $t > 0$. Тогда

$$M(A) = \sum_{n=1}^{N_t} \mathbf{1}((T_n,\, Y_n) \in A).$$

Рассмотрим п. ф. м. $\mathsf{E}e^{\theta M(A)}$ и воспользуемся стандартными преобразованиями:

$$\mathsf{E}e^{\theta M(A)} = \mathsf{E}\left[\,\mathsf{E}(e^{\theta M(A)}|N_t)\right] = \sum_{k=1}^{\infty} \mathsf{P}(N_t = k)\,\mathsf{E}(e^{\theta M(A)}|N_t = k).$$

Нам известно, что $N_t \sim \mathrm{Po}(\lambda t)$. Более того, если $N_t = k$, то точки скачка $T_1,\, \ldots,\, T_k$ обладают совместной плотностью распределения $f_{T_1,\ldots,T_k}(\cdot\,|N_t = k)$, приведённой в формуле (4.4.7). Тогда, учитывая при дальнейших преобразованиях, что с. в. $T_1,\, \ldots,\, T_k$ не зависят от Y_n, получаем

$$\begin{aligned}
&\mathsf{E}(e^{\theta M(A)}|N_t = k) = \mathsf{E}\left[(e^{\theta M(A)}|N_t = k;\, T_1,\, \ldots,\, T_k)\right] = \\
&= \int_0^t \ldots \int_0^t dx_k \ldots dx_1 f_{T_1,\ldots,T_k}(x_1,\, \ldots,\, x_k|N = k) \times \\
&\qquad \times \mathsf{E}\left(\exp\theta\left(\sum_{i=1}^{k} I((x_i,\, Y_i) \in A)\right) \,\middle|\, N_t = k;\, T_1 = x_1,\, \ldots,\, T_k = x_k \right) = \\
&\qquad\qquad = \frac{1}{t^k}\left(\int_0^t \int_D e^{\theta I_A(x,y)} d\nu(y) dx \right)^k.
\end{aligned}$$

Итак,

$$\begin{aligned}
\mathsf{E}e^{\theta M(A)} &= e^{-\lambda t} \sum_{k=0}^{\infty} \frac{(\lambda t)^k}{k!} \frac{1}{t^k} \left(\int_0^t \int_D e^{\theta I_A(x,y)} d\nu(y) dx \right)^k = \\
&= \exp\left[\lambda \int_0^t \int_D (e^{\theta I_A(x,y)} - 1) d\nu(y) dx \right].
\end{aligned}$$

Выражение $e^{\theta I_A(x,y)} - 1$ принимает значение $e^\theta - 1$ при $(x, y) \in A$ и 0 при $(x, y) \notin A$. Значит,

$$\mathsf{E}e^{\theta M(A)} = \exp\left[(e^\theta - 1)\lambda \int\limits_A d\nu(y)dx\right], \quad \theta \in \mathbb{R}, \tag{4.4.13}$$

Следовательно, $M(A) \sim \mathrm{Po}(\lambda m \times \nu(A))$.

Более того, если $A_1, \ldots, A_n$ — непересекающиеся подмножества в $[0, t) \times D$, то с. в. $M(A_1), \ldots, M(A_n)$ независимы. Чтобы это увидеть, заметим сначала, что по определению мера M аддитивна: $M(A) = M(A_1) + \ldots + M(A_n)$, когда $A = A_1 \cup \ldots \cup A_n$. Из формулы (4.4.13) получаем

$$\mathsf{E}e^{\theta M(A)} = \exp\left[(e^\theta - 1)\lambda \sum_{i=1}^n \int\limits_{A_i} d\nu(y)dx\right] = \prod_{i=1}^n \mathsf{E}e^{\theta M(A_i)}, \quad \theta \in \mathbb{R},$$

откуда следует независимость.

Таким образом, ограничение M на $\bar{E}_n = [0, n) \times D$ является $(\bar{E}, \lambda m_n \times \nu)$-СМП, где $m_n = m|_{[0,n)}$. Значит, благодаря теореме существования, M — $(\mathbb{R}_+ \times D, \lambda m \times \nu)$-СМП. □

Пример 4.4.12. Используя теорему о произведении и теорему Кэмпбелла, решите следующую задачу. Звезды разбросаны по трёхмерному пространству $\mathbb{R}^3$ по процессу Пуассона с плотностью $\nu(\mathbf{x})$ $(\mathbf{x} \in \mathbb{R}^3)$. Массы звёзд — н. о. р. с. в., масса $m_{\mathbf{x}}$ звезды $\mathbf{x}$ имеет плотность распределения $\rho(\mathbf{x}, dm)$. Гравитационный потенциал в начале координат задается формулой

$$F = \sum_{\mathbf{x} \in \Pi} \frac{G m_{\mathbf{x}}}{|\mathbf{x}|},$$

где G — константа. Найдите п. ф. м. $\mathsf{E}e^{\theta F}$.

Галактика занимает сферу радиуса R с центром в начале координат. Плотность распределения звёзд равна $\nu(\mathbf{x}) = 1/|\mathbf{x}|$ для точки $\mathbf{x}$ внутри сферы; масса каждой звезды имеет экспоненциальное распределение со средним M. Вычислите средний потенциал галактики в начале координат. Пусть C — положительная константа. Найдите распределение расстояний от начала координат до ближайшей звезды, вклад в потенциал F которой не меньше чем C.

Решение. Теорема Кэмпбелла говорит, что если M — случайная мера Пуассона на пространстве E интенсивности ν и $a\colon E \to \mathbb{R}$ — ограниченная измеримая функция, то

$$\mathsf{E}e^{\theta\Sigma} = \exp\left(\int\limits_E (e^{\theta a(y)} - 1)\nu(dy)\right),$$

где

$$\Sigma = \int\limits_E a(y)M(dy) = \sum_{X\in\Pi} a(X).$$

По теореме о произведении пары $(X,\, m_X)$ (положение, масса) образуют СМП на $\mathbb{R}^3 \times \mathbb{R}_+$ интенсивности $\mu(dx \times dm) = \nu(x)dx\rho(x,\, dm)$. Тогда по теореме Кэмпбелла получаем

$$\mathsf{E}e^{\theta F} = \exp\left(\int\limits_{\mathbb{R}^d}\int\limits_0^\infty \mu(dx\times dm)(e^{\theta Gm/|x|}-1)\right).$$

Средний потенциал в начале координат $\mathsf{E}F = \dfrac{d\,\mathsf{E}e^{\theta F}}{d\theta}\Big|_{\theta=0}$ равен

$$\int\limits_{\mathbb{R}^3}\nu(x)dx\int\limits_0^\infty \rho(x,\, dm)\frac{Gm}{|x|} = GM\int\limits_{\mathbb{R}^3} dx\frac{1}{|x|^2}\mathbf{1}(|x|\leqslant R).$$

В сферических координатах имеем

$$\int\limits_{\mathbb{R}^3} dx\frac{1}{|x|^2}\mathbf{1}(|x|\leqslant R) = \int\limits_0^R dr\frac{1}{r^2}r^2\int d\theta\cos\theta\int d\varphi = 4\pi R,$$

следовательно,

$$\mathsf{E}F = 4\pi GMR.$$

Обозначим, наконец, через D расстояние до ближайшей звезды, дающей вклад в F не менее C. Тогда по теореме о произведении 4.4.11 имеем

$$\mathsf{P}(D\geqslant d) = \mathsf{P}(\text{в } A \text{ нет точек}) = \exp(-\mu(A)).$$

Здесь

$$A = \left\{(x,\, m)\in\mathbb{R}^3\times\mathbb{R}_+ \colon |x|\leqslant d,\ \ \frac{Gm}{|x|}\geqslant C\right\}$$

и $\mu(A) = \int\limits_A \mu(dx\times dm)$ представляется как

$$\int\limits_0^d dr\frac{1}{r}r^2\int d\theta\cos\theta\int d\varphi\int\limits_{Cr/G}^\infty dm\frac{e^{-m/M}}{M} = 4\pi\int\limits_0^d dr\, re^{-Cr/(GM)} =$$

$$= 4\pi\left(\frac{GM}{C}\right)^2\left(1-e^{-Cd/(GM)}-\frac{Cd}{GM}e^{-Cd/(GM)}\right).$$

Это определяет распределение D на $[0,\, R]$. □

В распределенных системах передатчиков и приемников, таких как, например, беспроводные сети мобильных телефонов, допустимая скорость связи между парами узлов в беспроводной сети зависит от их случайных

положений и стратегии передачи. Как правило, передача осуществляется по цепочке передатчиков от источника к получателю. В последние годы в теории информации возникло новое интересное направление, некоторые эксперты даже предложили термин «сетевая теория информации». Это поле исследований тесно переплетается с теорией вероятностей, в частности, с фильтрацией и пространственными точечными процессами. Мы даже не пытаемся дать краткое описание этой быстро развивающейся области, но изложение современной теории информации не может полностью избежать сетевых аспектов. Здесь мы слегка коснёмся нескольких тем и предлагаем заинтересованному читателю книгу [FM] и литературу, приведенную там.

Пример 4.4.13. Предположим, что приёмник расположен в точке y, а передатчики разбросаны по плоскости $\mathbb{R}^2$ в точках $x_i \in \Pi$ процесса Пуассона интенсивности λ. Тогда простейшая модель мощности полученного в приемнике сигнала имеет вид

$$Y = \sum_{x_i \in \Pi} P(\ell |x_i - y|), \tag{4.4.14}$$

где P — мощность сигнала, а функция ℓ описывает замирание сигнала. В случае так называемого релеевского замирания $\ell(|x|) = e^{-\beta |x|}$, а в случае степенного замирания мощности $\ell(|x|) = |x|^{-\alpha}$, $\alpha > 2$. По теореме Кэмпбелла 4.4.8 имеем

$$\varphi(\theta) = \mathsf{E}[e^{\theta Y}] = \exp\left(2\lambda\pi \int\limits_0^\infty r(e^{\theta P \ell(r)} - 1)dr\right). \tag{4.4.15}$$

Более реалистичную модель беспроводных сетей можно описать следующим образом. Предположим, что приёмники расположены в точках y_j, $j = 1, \ldots, J$, а передатчики разбросаны по плоскости $\mathbb{R}^2$ в точках $x_k \in \Pi$ процесса Пуассона интенсивности λ. Запишем сигнал как

$$Y_j = \sum_{x_k \in \Pi} h_{jk} X_k + Z_j, \quad j = 1, \ldots, J. \tag{4.4.16}$$

Здесь простейшая модель функции передачи выглядит как

$$h_{jk} = \sqrt{P}\, \frac{e^{2\pi i r_{jk}/\nu}}{r_{jk}^{\alpha/2}}, \tag{4.4.17}$$

где ν — длина волны передачи, а $r_{jk} = |y_j - x_k|$. Предполагается, что с. в. шума Z_j — НОР $\mathrm{N}(0, \sigma^2)$. Аналогичную формулу можно написать для релеевского замирания. $\square$

Мы знаем, что в случае $J = 1$ и единственного передатчика $K = 1$ по теореме Найквиста—Шеннона из § 4.3 пропускная способность непрерывного по времени канала с аддитивным гауссовским белым шумом $Y(t) = X(t)\ell(x, y) + Z(t)$ с коэффициентом поглощения $\ell(x, y)$ при условии ограничения по мощности $\int\limits_{-\tau/2}^{\tau/2} X^2(t)dt < P\tau$ с шириной полосы W и спектральной плотностью шума σ_0^2 равна

$$C = W \log\left(1 + \frac{P\ell^2(x, y)}{2W\sigma_0^2}\right). \tag{4.4.18}$$

Рассмотрим далее случай конечного числа K передатчиков и J приёмников

$$y_j(t) = \sum_{i=1}^{K} \ell(x_i, y_j)x_i(t) + z_j(t), \quad j = 1, \ldots, J, \tag{4.4.19}$$

с ограничением по мощности P_k для k-го передатчика, $P_1 \geqslant P_2 \geqslant \ldots \geqslant P_K$. С помощью леммы 4.3.5 для пропускной способности параллельных каналов можно доказать (см. [FM]), что пропускная способность нашего канала равна

$$C = \sum_{k=1}^{K} W \log\left(1 + \frac{P_k^2 s_k^2}{2W\sigma_0^2}\right), \tag{4.4.20}$$

где s_k — k-е наибольшее сингулярное значение матрицы $E = (\ell(|y_j - x_k|))$. Далее предположим, что ширина полосы $W = 1$. Кроме того, любопытно описать пропускную способность распределительных систем из K передатчиков и J приёмников при ограничении средней мощности передачи $K^{-1}\sum\limits_k P_k \leqslant P$. Любознательному читателю и здесь можно рекомендовать книгу [FM], где устанавливается область пропускной способности в терминах допустимых скоростей R_{kj}:

$$\sum_{k=1}^{K}\sum_{j=1}^{J} R_{kj} \leqslant \max_{\substack{P_k \geqslant 0,\\ \sum_k P_k \leqslant KP}} \sum_{k=1}^{K} \log\left(1 + \frac{P_k s_k^2}{2\sigma_0^2}\right). \tag{4.4.21}$$

Теорема 4.4.14. *Рассмотрим произвольную конфигурацию S из $2n$ узлов, помещённых внутрь квадрата B_n площади $2n$ (т. е. размера $\sqrt{2n}$), разбитую затем на два таких непересекающихся подмножества S_1 и S_2, что $S_1 \cup S_2 = S$, $\#S_1 = \#S_2 = n$. Сумма $C_n = \sum\limits_{k=1}^{n}\sum\limits_{i=1}^{n} R_{ki}$ скоростей надёжных передач модели* (4.4.19) *от передатчика $x_k \in S_1$*

к приёмнику $y_i \in S_2$ ограничена сверху

$$C_n = \sum_{k=1}^{n}\sum_{i=1}^{n} R_{ki} \leqslant \max_{\substack{P_i \geqslant 0,\\ \sum_i P_i \leqslant nP}} \sum_{k=1}^{n} \log\Big(1 + \frac{P_k s_k^2}{2\sigma_0^2}\Big),$$

где s_k — k-е наибольшее сингулярное значение матрицы $L = (\ell(x_k, y_j))$, σ_0^2 — спектральная плотность мощности шума и ширина полосы $W = 1$.

Этот результат позволяет найти асимптотику пропускной способности при $n \to \infty$. В наиболее интересном случае экспоненциального замирания $R(n) = C_n/n \sim O\Big(\frac{(\log n)^2}{\sqrt{n}}\Big)$, в случае, когда замирание степенное и $\alpha > 2$, $R(n) \sim O\Big(\frac{n^{1/\alpha}(\log n)^2}{\sqrt{n}}\Big)$ (см. [FM]).

Далее мы обсудим сети с ограничениями на передачу, связанными с интерференцией. Пусть Π — процесс Пуассона интенсивности λ на плоскости $\mathbb{R}^2$. Предположим, что функция $\ell\colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}_+$, описывающая замирание сигнала, переданного из точки x в точку y, симметрична: $\ell(x, y) = \ell(y, x)$, $x, y \in \mathbb{R}^2$. Наиболее популярными примерами служат функции $\ell(x, y) = e^{-\beta|x-y|/2}$ и $\ell(x, y) = \frac{1}{|x-y|^{\alpha/2}}$, $\alpha > 2$. Общая теория строится на следующих предположениях:

1) $\ell(x, y) = \ell(|x - y|)$, $\int\limits_{r_0}^{\infty} r\ell(r)dr < \infty$ для некоторого $r_0 > 0$,
2) $\ell(0) > k\sigma_0^2/P$, $\ell(x) \leqslant 1$ для всех $x > 0$, где $k > 0$ — допустимый уровень интерференции,
3) функция ℓ непрерывна и строго убывает там, где она отлична от нуля.

Для каждой пары точек x_i, $x_j \in \Pi$ определим отношение сигнал/шум (ОСШ) как

$$\text{ОСШ}(x_i \to x_j) = \frac{P\ell^2(x_i, x_j)}{\sigma_0^2 + \gamma \sum_{k \neq i,j} P\ell^2(x_k, x_j)}, \tag{4.4.22}$$

где P, σ_0^2, $k > 0$ и $0 \leqslant \gamma < 1/k$. Будем говорить, что передатчик, расположенный в точке x_i, может послать сообщение приёмнику, находящемуся в точке x_j, если $\text{ОСШ}(x_i \to x_j) \geqslant k$. Для произвольных чисел $k > 0$ и $\varkappa$, $0 < \varkappa < 1$, обозначим через $A_n(k, \varkappa)$ событие, состоящее в том, что существует множество S_n из по крайней мере $\varkappa n$ точек процесса Π, образующих связный кластер, т. е. таких что любые две точки могут обмениваться сообщениями, возможно, используя ретрансляторы. Нас интересует, при

каких условиях для всех $k \in (0, 1)$ найдётся такое $\varkappa = \varkappa(k)$, что

$$\lim_{n\to\infty} \mathsf{P}(A_n(k, \varkappa(k))) = 1. \tag{4.4.23}$$

В этом случае мы будем называть сеть суперкритической на уровне интерференции $\varkappa(k)$. Это означает, что для данного передатчика (скажем, расположенного в начале координат 0) число других передатчиков, с которыми он может обмениваться сообщениями, привлекая ретрансляторы в точках интерференции, с положительной вероятностью бесконечно.

Прежде всего заметим, что любой данный передатчик можно напрямую подключить не более чем к $1 + (\gamma k)^{-1}$ приёмникам. Действительно, допустим, что n_x узлов соединено с узлом x. Обозначим через x_1 такой узел, соединённый с x, что

$$\ell(|x_1 - x|) \leqslant \ell(|x_i - x|), \quad i = 2, \ldots, n_x. \tag{4.4.24}$$

Поскольку x_1 связан с x, мы имеем

$$\frac{P\ell^2(|x_1 - x|)}{\sigma_0^2 + \gamma \sum_{i=2}^{\infty} P\ell^2(|x_i - x|)} \geqslant k,$$

откуда

$$\begin{aligned} P\ell^2(|x_1 - x|) &\geqslant k\sigma_0^2 + k\gamma \sum_{i=2}^{\infty} P\ell^2(|x_i - x|) \geqslant \\ &\geqslant k\sigma_0^2 + k\gamma(n_x - 1)P\ell^2(|x_1 - x|) + \\ &\quad + k\gamma \sum_{i=n_x+1}^{\infty} P\ell^2(|x_i - x|) \geqslant k\gamma(n_x - 1)P\ell^2(|x_1 - x|). \end{aligned} \tag{4.4.25}$$

Из формулы (4.4.25) следует, что $n_x \leqslant 1 + (k\gamma)^{-1}$. Однако при выполнении равенства (4.4.23) существует бесконечный кластер или, как говорят, сеть просачивается. Это означает, что с положительной вероятностью данный передатчик можно связать с бесконечным числом других через ретрансляторы. В частности, модель просачивается при $\gamma = 0$, если интенсивность процесса Пуассона $\lambda > \lambda_{cr}$, где λ_{cr} зависит от коэффициента замирания $\ell(x, y)$. При $\lambda > \lambda_{cr}$ модель просачивается, если значение коэффициента $\gamma \leqslant \gamma^*(\lambda)$, при этом критическое значение $\gamma^*(\lambda)$ сначала растёт с ростом λ, а затем начинает затухать, поскольку интерференция становится слишком сильной. Доказательство следующего утверждения можно прочитать в книге [FM].

Теорема 4.4.15. *Пусть λ_{cr} — критическая плотность узлов при $\gamma = 0$. Для любой плотности узлов $\lambda > \lambda_{cr}$ найдётся $\gamma^*(\lambda) > 0$, такое,*

что при $\gamma \leqslant \gamma^*(\lambda)$ *модель интерференции просачивается. При* $\lambda \to \infty$ *справедливо соотношение*

$$\gamma^*(\lambda) = O(\lambda^{-1}). \tag{4.4.26}$$

Другая интересная связь с пространственными точечными процессами в $\mathbb{R}^N$ проявляется при использовании точечных процессов для моделирования случайных кодовых книг. Альтернативный (и более эффективный) способ генерирования случайных кодов, достигающий значения $C(\alpha)$ из формулы (4.1.17), состоит в следующем. Возьмём процесс Пуассона $\Pi^{(N)}$ в $\mathbb{R}^N$ интенсивности $\lambda_N = e^{NR_N}$, где $R_N \to R$ при $N \to \infty$. Здесь $R < \frac{1}{2}\log\frac{1}{2\pi e\sigma_0^2}$, где σ_0^2 — дисперсия аддитивного гауссовского шума в канале. Включим в кодовую книгу $\mathcal{X}_{M,N}$ случайные точки $X(i)$ из процесса $\xi^{(N)}$, лежащие внутри евклидова шара $\mathbb{B}^{(N)}(\sqrt{N\alpha})$ и оставшиеся после следующей процедуры «чистки». Фиксируем $r > 0$ (минимальное расстояние случайного кода) и для любой точки x_j процесса Пуассона $\Pi^{(N)}$ генерируем н. о. р. с. в. $t_j \sim \mathrm{U}([0, 1])$ (случайная метка). Далее, для любой точки x_j исходного процесса Пуассона рассмотрим шар $\mathbb{B}^{(N)}(x_j, r)$ радиуса r с центром в точке x_j. Точка x_j останется только если её метка t_j окажется строго меньше, чем метки всех остальных точек из $\Pi^{(N)}$, лежащих в $\mathbb{B}^{(N)}(x_j, r)$. Получившийся в результате точечный процесс известен как *процесс Матерна*; он является примером более общей конструкции случайных кодовых книг, которая обсуждается в недавней статье [AB].

Главный параметр случайной кодовой книги с кодовыми словами $\mathbf{x}^{(N)}$ длины N — это индуцированное распределение расстояний между кодовыми словами. В случае кодовой книги, порождённой стационарным точечным процессом, удобно ввести такую функцию $K(t)$, что $\lambda^2 K(t)$ даёт среднее число упорядоченных пар различных точек в единичном объёме, отстоящих друг от друга на расстояние меньше чем t. Иначе говоря, $\lambda K(t)$ — среднее число дополнительных точек на расстоянии t от произвольной точки процесса. Например, для процесса Пуассона на $\mathbb{R}^2$ интенсивности λ имеем $K(t) = \pi t^2$. Нас интересуют модели кодовых книг, где $K(t)$ значительно меньше для малых и небольших t. Следовательно, случайные кодовые слова появляются на небольших расстояниях друг от друга существенно реже, чем в процессе Пуассона. Удобно ввести так называемую плотность произведения

$$\rho(t) = \frac{\lambda^2}{c(t)}\frac{dK(t)}{dt}, \tag{4.4.27}$$

где $c(t)$ зависит от пространства состояний точечного процесса. Скажем, $c(t) = 2\pi t$ на $\mathbb{R}^1$, $c(t) = 2\pi t^2$ на $\mathbb{R}^2$, $c(t) = 2\pi \sin t$ на единичной сфере, и т. д.

Некоторые удобные модели такого типа были предложены Б. Матерном. Здесь мы обсуждаем две модели точечных процессов Матерна на $\mathbb{R}^N$. Первый процесс Матерна получается прореживанием процесса Пуассона интенсивности λ и удалением всех точек, находящихся друг от друга ближе чем на расстоянии $2R$, невзирая на то, была или не была удалена ранее одна из рассматриваемых точек. Интенсивность этого процесса при $N = 2$ равна

$$\lambda_{M,1} = \lambda e^{-4\pi\lambda R^2}. \tag{4.4.28}$$

Плотность произведения $\rho(t) = 0$ при $t < 2R$ и

$$\rho(t) = \lambda^2 e^{-2U(t)}, \quad t > 2R,$$

где

$$U(t) = \mathrm{meas}[\mathbb{B}(\mathbf{0}, 2R) \cup \mathbb{B}((t, 0), 2R)]. \tag{4.4.29}$$

Здесь $\mathbb{B}(\mathbf{0}, 2R)$ — шар с центром в точке $(0, 0)$ радиуса $2R$ и $\mathbb{B}((t, 0), 2R)$ — шар с центром в точке $(t, 0)$ радиуса $2R$. При различных λ эта модель обладает максимальной интенсивностью $(4\pi e R^2)^{-1}$ и поэтому не может моделировать плотно упакованный код. Интенсивность этого процесса достигает 10 % от теоретической границы $(\sqrt{12}R^2)^{-1}$, которая достигается на треугольной решётке, см. [AB].

Вторая модель Матерна — это упомянутый выше маркированный точечный процесс. Точкам процесса Пуассона интенсивности λ независимо приписываются н. о. р. с. в. — марки (метки) с распределением $\mathrm{U}([0, 1])$. Точка удаляется, если существует другая точка процесса в пределах $2R$, которая обладает бóльшей меткой, вне зависимости от того, была или не была удалена эта точка с большей меткой ранее. Интенсивность второго процесса Матерна при $N = 2$ составляет

$$\lambda_{M,2} = (1 - e^{-\lambda c})/c, \quad c = U(0) = 4\pi R^2. \tag{4.4.30}$$

Плотность произведения $\rho(t) = 0$ при $t < 2R$ и

$$\rho(t) = \frac{2U(t)(1 - e^{-4\pi R^2\lambda}) - 2c(1 - e^{-\lambda U(t)})}{cU(t)(U(t) - c)}, \quad t > 2R. \tag{4.4.31}$$

Эквивалентное определение состоит в следующем. Для двух точек x и y исходного процесса Пуассона, находящихся на расстоянии $t = |x - y|$ друг от друга, определим вероятность $k(t) = \rho(t)/\lambda^2$ того, что обе точки останутся во втором процессе Матерна. Тогда $k(t) = 0$ при $t < 2R$ и

$$k(t) = \frac{2U(t)(1 - e^{-4\pi R^2\lambda}) - 8\pi R^2(1 - e^{-\lambda U(t)})}{4\lambda^2\pi R^2 U(t)(U(t) - 4\pi R^2)}, \quad t > 2R.$$

Пример 4.4.16 (вероятность отказа в беспроводных сетях). Предположим, что приёмник поместили в начале координат, а передатчики распределены в процессе Матерна с жёстким ядром с внутренним радиусом r_0. Мы предполагаем, что никакие два передатчика не находятся друг от друга на расстоянии ближе чем r_0, а расстояние охвата — a, т. е. рассматриваются только точки второго процесса Матерна в кольце $r_0 < r < a$. Сумма полученных центральным приёмником мощностей сигналов из всей беспроводной сети записывается как

$$X_{r_0} = \sum_{J_{r_0,a}} \frac{P}{r_i^{\alpha}}, \tag{4.4.32}$$

где $J_{r_0,a}$ обозначает множество таких радиусов интерференции, что $r_0 \leqslant r_i < a$. Пусть λ_P — интенсивность процесса Пуассона, генерирующего процесс Матерна второго типа после прореживания. Интенсивность прореженного процесса составит

$$\lambda = \frac{1 - \exp(-\lambda_P \pi r_0^2)}{\pi r_0^2}.$$

Опираясь на теорему Кэмпбелла 4.4.8, вычислим п. ф. м. X_{r_0}:

$$\varphi(s) = \mathsf{E}(e^{sX_{r_0}}) = \exp\left(\lambda_P \pi (a^2 - r_0^2) \int_0^1 q(t)dt \left[\int_{r_0}^{a} \frac{2r}{a^2 - r^2} e^{sg(r)} dr - 1\right]\right). \tag{4.4.33}$$

Здесь $g(r) = P/r^{\alpha}$ и $q(t) = \exp(-\lambda_P \pi r_0^2 t)$ — вероятность выживания точки с меткой t. Так как $\int_0^1 q(t)dt = \lambda/\lambda_P$, мы получаем

$$\varphi(s) = \exp\left(\lambda\pi(a^2 - r_0^2)\left[\int_{r_0}^{a} \frac{2r}{a^2 - r_0^2} e^{sg(r)} dr - 1\right]\right). \tag{4.4.34}$$

Теперь мы можем вычислить все абсолютные моменты интерферирующих сигналов:

$$\mu_k = \lambda\pi \int_{r_0}^{a} 2r(g(r))^k dr = \frac{2\lambda\pi}{k\alpha - 2}\left(\frac{P^k}{r_0^{k\alpha-2}} - \frac{P^k}{a^{k\alpha-2}}\right). \tag{4.4.35}$$

Инженеры говорят, что происходит отказ центрального приёмника, т. е. помехи не дают прочесть сигнал, полученный от отправителя на расстоянии r_s, если

$$\frac{P/r_s^{\alpha}}{\sigma_0^2 + \sum_{J_{r_0,a}} P/r_i^{\alpha}} \leqslant k.$$

Здесь σ_0^2 — мощность шума, r_s — расстояние до отправителя и k — минимальное ОСШ (отношение сигнал/шум), необходимое для приемлемого приёма. Обычно используются аппроксимации вероятности отказа, основанные на моментах, вычисленных в формуле (4.4.35). Как правило, распределение X_{r_0} близко к логнормальному, см., например, [MBR].

> В математике вы не понимаете вещей. Вы просто привыкаете к ним.
>
> Нет никакого смысла в том, чтобы быть точным, когда вы даже не знаете, о чем вы говорите.
>
> *Джон фон Нейман* (1903–1957), американский математик и программист, родившийся в Венгрии.

§ 4.5. Избранные примеры и задачи криптографии

> Вся математика делится на три части: криптография (оплачивается ЦРУ, КГБ и т. д.), гидродинамика (поддерживается производителями атомных подводных лодок) и небесная механика (финансируется военными и другими учреждениями, связанными с ракетами, такими, как НАСА). Криптография породила теорию чисел, алгебраическую геометрию над конечными полями, алгебру, комбинаторику и компьютеры.
>
> *Владимир Арнольд* (1937–2010), русский математик

Здесь мы представляем избранные примеры и задачи криптографии. Криптография, определяемая как «практика и исследования сокрытия информации», стала частью многих курсов и занятий по кодированию, в нашем описании мы в основном следуем традиции Кембриджского курса «Кодирование и криптография». Мы сводим теоретические объяснения к минимуму и рекомендуем обращаться к специализированным книгам за подробностями. Криптография имеет долгую и подчас захватывающую историю, где математика чередуется с другими науками (и не только науками), которая вдохновила множество художественных и полуфантастических книг, фильмов, а также телевизионных программ; этот поток, кажется, вовсе не иссякнет.

Например, знаменитый французский математик Франсуа Виет (1549–1603), которому приписывается изобретение биномиальной формулы, был также правоведом и государственным деятелем и служил королям Франции Генриху III и Генриху IV в качестве личного криптографа. Виет добился таких успехов в дешифровке секретной переписки «врагов короля» (в частности, испанцев), что обвинялся в использовании черной магии; некоторые его

достижения будет нелегко превзойти и современным криптографам. (Не вполне ясно, от кого исходили эти обвинения — от отчаявшихся заговорщиков и «врагов короля» или от столь же отчаявшихся коллег Виета по королевской службе.)

Другой пример касается Гольдбаха. Христиан Гольдбах (1690–1764) — немецкий математик (родился в Кёнигсберге, в то время Восточная Пруссия) прославился благодаря своей гипотезе, хорошо известной в теории чисел. В современном виде, гипотеза Гольдбаха гласит, что каждое чётное число $N \geqslant 4$ может быть представлено в виде суммы двух простых чисел. (Некоторые специалисты называют её «строгой», «четной» или «двоичной» формой гипотезы Гольдбаха.) Гипотеза Гольдбаха является одной из старейших нерешённых проблем в математике; он сформулировал её в своём письме к Эйлеру (1742 г.), с которым был в дружеских отношениях (так же как и с Лейбницем, и членами клана Бернулли). Первоначально гипотеза Гольдбаха утверждала, что каждое целое число $N \geqslant 5$ может быть записано в виде суммы трёх простых чисел, на что Эйлер ответил, что это следует из вышесказанного более сильного заявления. Эйлер высказал свою полную убежденность в том, что двоичная гипотеза — это правильное утверждение; современный компьютерный поиск показал, что все числа до 4×10^{18} ему удовлетворяют.

Биографы Гольдбаха указывают, что он жил в Петербурге, учил на дому молодого императора Петра II (взошедшего на престол в возрасте 11 и умершего в возрасте 15 лет) и был активным сотрудником российской императорской Академии наук и Министерства иностранных дел. (Не похоже, чтобы министерство было самым естественным местом трудоустройства для профессионального математика первого класса с глубоким интересом к теории чисел и анализу.) Биографы также отмечают, что карьера Гольдбаха смогла успешно пережить многочисленные перевороты в период истории России, наполненный заговорами и предательствами. Некоторые из них приписывают ему блестящее знание латыни, свободное владение немецким и французским языками, «[его] изысканные манеры и космополитический круг друзей», которые «обеспечили его успех в элитном российском обществе, которое старалось подражать ее западным соседям».

Однако может найтись и более практическое объяснение. По-видимому, с 1742 г. (или может быть даже и с более раннего времени) и до своей смерти Гольдбах возглавлял службу криптографии в императорском министерстве иностранных дел. Он был в состоянии расшифровать огромное количество корреспонденции между Санкт-Петербургом и другими европейскими столицами (официальный отчёт утверждал, что он взломал ключи от почти всех перехваченных зашифрованных писем, показанных ему, кроме «определённо малого числа»). В 1760 г. ему был присвоен титул «тайный советник» — самая высокая награда для членов аристократии и дворянства в Российской Империи. Даже Эйлер никогда не получил такой титул (императрица Елизавета Петровна говорила: «у меня много тайных советников, но только один Эйлер», когда её неоднократно просили даровать Эйлеру этот чин). Это, естественно, подводит к выводу, что Эйлер не был привлечён к криптографической работе (или другой деятельности, аналогичного значения). Однако один из его сыновей, Карл Иоханн, в самом деле, был занят в течение ряда лет в тайном отделении императорского министерства иностранных дел и разрабатывал шифры для российской дипломатической переписки (некоторые из этих шифров с его фамилией и подписью были найдены в архивах).

Популярный способ получения зашифрованных последовательностей знаков — это так называемая обратная связь регистра сдвига. Мы ограничимся двоичным случаем, работая с пространством строк $\mathcal{H}_{n,2} = \{0, 1\}^n = \mathbb{F}_2^{\times n}$.

Определение 4.5.1. Двоичная (общая) *обратная связь регистра сдвига* (о. с. р. с.) длины d — это отображение $\{0,1\}^d \to \{0,1\}^d$ вида

$$(x_0, \ldots, x_{d-1}) \mapsto (x_1, \ldots, x_{d-1}, f(x_0, \ldots, x_{d-1}))$$

для некоторой функции $f\colon \{0,1\}^d \to \{0,1\}$ (функция обратной связи). Исходная строка $(x_0, \ldots, x_{d-1})$ называется *начальным заполнением*: оно инициирует выходной поток $(x_n)_{n\geqslant 0}$, удовлетворяющий рекуррентному уравнению

$$x_{n+d} = f(x_n, \ldots, x_{n+d-1}) \quad \forall n \geqslant 0. \tag{4.5.1}$$

Обратная связь регистра сдвига называется *линейной* (для краткости л. о. с. р. с.), если функция f линейна и $c_0 = 1$:

$$f(x_0, \ldots, x_{d-1}) = \sum_{i=0}^{d-1} c_i x_i, \quad c_i = 0, 1, \ c_0 = 1. \tag{4.5.2}$$

В этом случае рекуррентное соотношение тоже линейно:

$$x_{n+d} = \sum_{i=0}^{d-1} c_i x_{n+i} \quad \forall n \geqslant 0. \tag{4.5.3}$$

□

Соотношение (4.5.3) удобно переписать в матричном виде:

$$\mathbf{x}_{n+1}^{n+d} = \mathbf{V}\mathbf{x}_n^{n+d-1}, \tag{4.5.4}$$

где

$$\mathbf{V} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ c_0 & c_1 & c_2 & \ldots & c_{d-2} & c_{d-1} \end{pmatrix}, \quad \mathbf{x}_n^{n+d-1} = \begin{pmatrix} x_n \\ x_{n+1} \\ \vdots \\ x_{n+d-2} \\ x_{n+d-1} \end{pmatrix}. \tag{4.5.5}$$

Раскрывая определитель по первому столбцу, можно увидеть, что $\det \mathbf{V} = 1 \bmod 2$: множитель при $(n, 1)$-элементе c_0 — это определитель матрицы $\mathbf{1}_{d-1}$. Следовательно,

$$\det \mathbf{V} = c_0 \det \mathbf{1}_{d-1} = c_0 = 1 \tag{4.5.6}$$

и матрица $\mathbf{V}$ обратима.

Полезным понятием служит вспомогательный многочлен, или многочлен обратной связи л. о. с. р. с. из формулы (4.5.3):

$$C(X) = c_0 + c_1 X + \ldots + c_{d-1} X^{d-1} + X^d. \tag{4.5.7}$$

Заметим, что общая обратная связь регистров сдвига после начального прогона становится периодичной.

Теорема 4.5.2. *Выходной поток* (x_n) *общей обратной связи регистров сдвига длины* d *обладает следующим свойством*: *существует такие целые числа* r *и* D, $0 \leqslant r < 2^d$, $1 \leqslant D < 2^d - r$, *что* $x_{k+D} = x_k$ $\forall k \geqslant r$.

Доказательство. Отрезок $x_M, \ldots, x_{M+d-1}$ однозначно определяет остаток выходного потока из формулы (4.5.1), т. е. $(x_n,\ n \geqslant M + d - 1)$. Мы видим, что если такой отрезок воспроизведётся в потоке, то он будет повторяться. Существует 2^d различных возможностей для строки d последовательных знаков. Значит, по принципу Дирихле найдутся такие $0 \leqslant r < R < 2^d$, что, начиная с позиций r и R два отрезка выходного потока длины d будут одинаковыми: $x_{r+j} = x_{R+j}$, $0 \leqslant j < d$. Тогда, как уже отмечалось, $x_{r+j} = x_{R+j}$ $\forall j \geqslant 0$ и утверждение справедливо с $D = R - r$. □

В линейном случае (л. о. с. р. с.) мы можем повторить эти рассуждения, отбросив нулевые строки, что позволит нам снизить 2^d до $2^d - 1$. Однако л. о. с. р. с. периодична в «собственном смысле».

Теорема 4.5.3. *Л. о. с. р. с.* (x_n) *периодична*, *т. е. существует такое* $D \leqslant 2^d - 1$, *что* $x_{n+D} = x_n$ *для всех* n. *Наименьшее* D *с таким свойством называется периодом л. о. с. р. с.*

Доказательство. Действительно, вектор-столбцы $\mathbf{x}_n^{n+d-1}$, $n \geqslant 0$ связаны уравнением $\mathbf{x}_{n+1} = \mathbf{V}x_n = \mathbf{V}^{n+1}\mathbf{x}_0$, $n \geqslant 0$, где матрица $\mathbf{V}$ была определена в формуле (4.5.5). Мы отметили, что $\det \mathbf{V} = c_0 \neq 0$ и поэтому матрица $\mathbf{V}$ обратима. Как было сказано раньше, мы можем отбросить нулевое начальное заполнение. Для каждого вектора $\mathbf{x}_n \in \{0, 1\}^d$ существует только $2^d - 1$ ненулевые возможности. Следовательно, как и в доказательстве теоремы 4.5.2 среди начальных $2^d - 1$ векторов $\mathbf{x}_n$ $(0 \leqslant n \leqslant 2^d - 2)$ либо встретятся повторяющиеся, либо найдётся нулевой вектор. Вторую возможность можно вновь отбросить, поскольку она ведёт к нулевому начальному заполнению. Итак, предположим, что первое повторение было для j и $D + j$: $\mathbf{x}_j = \mathbf{x}_{D+j}$, т. е. $\mathbf{V}^{j+D}\mathbf{x}_0 = \mathbf{V}^j\mathbf{x}_0$. Если $j \neq 0$, умножим на $\mathbf{V}^{-1}$ и придём к более раннему повторению. Таким образом, можно считать, что $j = 0$, $D \leqslant 2^d - 1$ и $\mathbf{V}^D\mathbf{x}_0 = \mathbf{x}_0$. Тогда, очевидно, $\mathbf{x}_{n+D} = \mathbf{V}^{n+D}\mathbf{x}_0 = \mathbf{V}^n\mathbf{x}_0 = \mathbf{x}_n$. □

Пример 4.5.4. Приведите пример регистра общей обратной связи с выходом (k_j) и таким начальным заполнением $(k_0, k_1, \ldots, k_{d-1})$, что

$$(k_n, k_{n+1}, \ldots, k_{n+d-1}) \neq (k_0, k_1, \ldots, k_{d-1}) \quad \forall n \geqslant 1.$$

Решение. Возьмём $f\colon \{0, 1\}^2 \to \{0, 1\}^2$, $f(x_1, x_2) = x_2 1$. Начальное заполнение 00 даёт выход 00111111... Здесь $k_{n+1} \neq 0 = k_1$ $\forall n \geqslant 1$. □

Пример 4.5.5. Пусть матрица $\mathbf{V}$ такая же, как в формуле (4.5.5) для линейной рекурсии (4.5.3). Определите и вычислите характеристический и минимальный многочлены матрицы $\mathbf{V}$.

Решение. Характеристический многочлен матрицы $\mathbf{V}$ — это $h_{\mathbf{V}}(X) = \det(X\mathbf{1} - V) \in \mathbb{F}_2[X]$:

$$h_{\mathbf{V}}(X) = \det \begin{pmatrix} X & 1 & 0 & \dots & 0 & 0 \\ 0 & X & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \dots & X & 1 \\ c_0 & c_1 & c_2 & \dots & c_{d-2} & (c_{d-1}+X) \end{pmatrix} \tag{4.5.8}$$

(напомним, что элементы 1 и c_i принадлежат $\mathbb{F}_2$). Раскрывая определитель по последней строке, можно представить $h_{\mathbf{V}}(X)$ как линейную комбинацию определителей размера $(d-1)\times(d-1)$ (алгебраических дополнений):

$$c_0 \det \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ X & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & X & 1 \end{pmatrix} + c_1 \det \begin{pmatrix} X & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & X & 1 \end{pmatrix} + \dots + c_{d-2} \det \begin{pmatrix} X & 1 & \dots & 0 & 0 \\ 0 & X & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} +$$

$$+ (c_{d-1}+X)X^{d-1} = c_0 + c_1 X + \dots + c_{d-2}X^{d-2} + (c_{d-1}+X)X^{d-1} = \sum_{i=0}^{d-1} c_i X^i + X^d,$$

что совпадает с характеристическим многочленом рекурсии.

По теореме Гамильтона—Кэли имеем

$$h_{\mathbf{V}}(\mathbf{V}) = c_0\mathbf{1} + c_1\mathbf{V} + \dots + c_{d-1}\mathbf{V}^{d-1} + \mathbf{V}^d = \mathbf{0}.$$

Минимальным многочленом $m_{\mathbf{V}}(X)$ матрицы $\mathbf{V}$ называется многочлен минимальной степени, для которого $m_{\mathbf{V}}(\mathbf{V}) = \mathbf{0}$. Он делит $h_{\mathbf{V}}(X)$ и каждый корень характеристического многочлена является корнем минимального. Отличие $m_{\mathbf{V}}(X)$ от $h_{\mathbf{V}}(X)$ заключается в кратности корней: кратность корня μ многочлена $m_{\mathbf{V}}(X)$ равна максимальному размеру жордановой клетки в $\mathbf{V}$ с собственным числом μ, в то время как кратность этого корня в многочлене $h_{\mathbf{V}}(X)$ равна сумме размеров всех таких жордановых клеток матрицы $\mathbf{V}$.

Чтобы вычислить $m_{\mathbf{V}}(X)$, мы 1) выберем базис $\mathbf{e}_1, \dots, \mathbf{e}_d$ (в $\mathbb{F}_2^{\times d}$), 2) для каждого вектора $\mathbf{e}_j$ найдём такое минимальное число d_j, что векторы $\mathbf{e}_j$, $\mathbf{V}\mathbf{e}_j \dots$, $\mathbf{V}^{d_j}\mathbf{e}_j$, $\mathbf{V}^{d_j+1}\mathbf{e}_j$ линейно зависимы, и 3) выпишем тождество, соответствующее линейной зависимости:

$$a_0^{(j)}\mathbf{e}_j + a_1^{(j)}\mathbf{V}\mathbf{e}_j + \dots + a_{d_j}^{(j)}\mathbf{V}^{d_j}\mathbf{e}_j + \mathbf{V}^{d_j+1}\mathbf{e}_j = \mathbf{0},$$

4) соберём соответствующий многочлен

$$m_{\mathbf{V}}^{(j)}(X) = \sum_{i=0}^{d_j} a_i^{(j)} X^i + X^{d_j+1},$$

5) тогда

$$m_{\mathbf{V}}(X) = \text{НОК}\left[m_{\mathbf{V}}^{(1)}(X), \ldots, m_{\mathbf{V}}^{(d)}(X)\right].$$

В нашем случае удобно выбрать $\mathbf{e}_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ (единица на j-м месте). Тогда $\mathbf{V}^j \mathbf{e}_1 = \mathbf{e}_j$ и мы получаем, что $d_1 = d$ и

$$m_{\mathbf{V}}^{(1)}(X) = \sum_{i=0}^{d-1} c_i X^i + X^d = h_{\mathbf{V}}(X). \qquad \square$$

Мы увидели, что многочлен обратной связи $C(X)$ рекурсии совпадает с характеристическим и минимальным многочленами для $\mathbf{V}$. Заметим, что при $X = 0$ мы получаем

$$h_{\mathbf{V}}(0) = C(0) = c_0 = 1 = \det \mathbf{V}. \tag{4.5.9}$$

Любой многочлен можно идентифицировать по его корням, такое описание может быть очень полезным. В случае л. о. с. р. с. весьма показателен следующий пример.

Теорема 4.5.6. *Рассмотрим двоичную линейную рекурсию* (4.5.3) *и соответствующий вспомогательный многочлен* (4.5.7).

1. *Предположим, что многочлен $C(X)$ имеет корень α кратности m в поле $\mathbb{K}$, содержащем $\mathbb{F}_2$. Тогда $\forall k = 0, 1, \ldots, m-1$ последовательность*

$$x_n = A(n, k)\alpha^n, \quad n = 0, 1, \ldots \tag{4.5.10}$$

является решением уравнения (4.5.3) *в поле $\mathbb{K}$, где*

$$A(n, k) = \begin{cases} 1, & k = 0, \\ \left(\prod\limits_{l=0}^{k-1} (n-l)_+\right) \bmod 2, & k > 0. \end{cases} \tag{4.5.11}$$

Здесь и далее $(a)_+$ обозначает $\max\{a, 0\}$. Иначе говоря, последовательность $\mathbf{x}^{(k)} = (x_n)$, где x_n определяется формулой (4.5.10), *— выходной поток л. о. с. р. с. со вспомогательным многочленом $C(X)$.*

2. *Пусть* $\mathbb{K}$ *— поле, содержащее* $\mathbb{F}_2$, *в котором* $C(X)$ *раскладывается на линейные множители, а* $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$ *— его различные корни кратностей* $m_1, \ldots, m_r$ *с* $\sum_{i=1}^{r} m_i = d$. *Тогда общее решение уравнения* (4.5.3) *в поле* $\mathbb{K}$ *имеет вид*

$$x_n = \sum_{i=1}^{r} \sum_{k=0}^{m_i-1} b_{i,k} A(n, k) \alpha_i^n \tag{4.5.12}$$

для некоторых $b_{u,v} \in \mathbb{K}$. *Другими словами, последовательности* $\mathbf{x}^{(i,k)} = (x_n)$, *где* $x_n = A(n, k)\alpha_i^n$ *и* $A(n, k)$ *из* (4.5.11), *порождают множество всех выходных потоков л. о. с. р. с. со вспомогательным многочленом* $C(X)$.

Доказательство. 1. Если $C(X)$ имеет корень $\alpha \in \mathbb{K}$ кратности m, то $C(X) = (X - \alpha)^m \tilde{C}(X)$, где $\tilde{C}(X)$ — многочлен степени $d - m$ (с коэффициентами из поля $\mathbb{K}' \subseteq \mathbb{K}$). Тогда $\forall k = 0, \ldots, m - 1$ и $\forall n \geqslant d$ многочлен

$$D_{k,n} := X^k \frac{d^k}{dX^k}(X^{n-d} C(X))$$

(с коэффициентами, взятыми по модулю 2) обращается в нуль при $X = \alpha$ (в поле $\mathbb{K}$):

$$D_{k,n}(\alpha) = \sum_{i=0}^{d-1} c_i A(n - d + i, k)\alpha^{n-d+i} + A(n, k)\alpha^n = 0.$$

Отсюда следует, что

$$A(n, k)\alpha^n = \sum_{i=0}^{d-1} c_i A(n - d + i, k)\alpha^{n-d+i}.$$

Итак, поток $\mathbf{x}^{(k)} = (x_n)$, где x_n определяется формулой (4.5.10), является решением рекурсии $x_n = \sum_{i=0}^{d-1} c_i x_{n-d+i}$ в поле $\mathbb{K}$. Число таких решений равно m — кратности корня α.

2. Прежде всего заметим, что множество выходных потоков образует векторное пространство $\mathbb{W}$ над $\mathbb{K}$ (в множестве всех последовательностей элементов из $\mathbb{K}$). Размерность $\mathbb{W}$ равна d, поскольку каждый поток однозначно определяется начальным заполнением $x_0, x_1, \ldots, x_{d-1} \in \mathbb{K}^d$. С другой стороны, $d = \sum_{i=1}^{r} m_i$ — число всех последовательностей $\mathbf{x}^{(i,k)} = (x_n^{(i,k)})$ с элементами

$$x_n^{(i,k)} = A(n, k)\alpha_i^n, \quad n = 0, 1, \ldots$$

Таким образом, достаточно проверить, что потоки $\mathbf{x}^{(i,k)}$, где $i = 1, \ldots, r$, $k = 0, 1, \ldots m_i - 1$, линейно независимы над $\mathbb{K}$.

Чтобы завершить доказательство, рассмотрим линейную комбинацию $\sum_{i=1}^{r} \sum_{k=0}^{m_i-1} b_{i,k}\mathbf{x}^{(i,k)}$, равную $\mathbf{0}$. Пусть $\mathbf{x}^{(i,k)} = \mathbf{0}$ при $k < 0$. Удобно ввести оператор сдвига $\mathbf{x} = (x_n) \mapsto \mathbf{S}\mathbf{x} = (x'_n)$, где $x'_n = x_{n+1}$, $n = 0, 1, \ldots$ Ключевое наблюдение состоит в следующем. Пусть $\mathbf{1}$ обозначает тождественное преобразование. Тогда $\forall \beta \in \mathbb{K}$

$$(\mathbf{S} - \beta\mathbf{1})\mathbf{x}^{(i,k)} = (\alpha_i - \beta)\mathbf{x}^{(i,k)} + k\alpha_i\mathbf{x}^{(i,k-1)}.$$

На самом деле n-й член последовательности $(\mathbf{S} - \beta\mathbf{1})\mathbf{x}^{(i,k)}$ равен

$$\begin{aligned} A(n+1,\, k)\alpha_i^{n+1} - \beta A(k,\, n)\alpha_i^n = \\ = [A(n,\, k) + kA(n,\, k-1)]\alpha_i^{n+1} - \beta A(n,\, k)\alpha_i^n = \\ = (\alpha_i - \beta)A(n,\, k)\alpha_i^n + \alpha_i kA(n,\, k-1)\alpha_i^n, \end{aligned}$$

если учитывать приведённое выше соглашение. Мы воспользовались здесь элементарным тождеством

$$A(n+1,\, k) = A(n,\, k) + kA(n,\, k-1).$$

Продолжая итерации, получим, что

$$\begin{aligned} (\mathbf{S} - \beta_1\mathbf{1})(\mathbf{S} - \beta_2\mathbf{1})\mathbf{x}^{(i,k)} = (\alpha_i - \beta_1)(\alpha_i - \beta_2)\mathbf{x}^{(i,k)} + \\ + k\alpha_i(\alpha_i - \beta_1 + \alpha_i - \beta_2)\mathbf{x}^{(i,k-1)} + k^2\alpha_i^2\mathbf{x}^{(i,k-2)} = (\mathbf{S} - \beta_2\mathbf{1})(\mathbf{S} - \beta_1\mathbf{1})\mathbf{x}^{(i,k)} \end{aligned}$$

и т. д. (все операции над коэффициентами осуществляются в поле $\mathbb{K}$). В частности, при $\beta = \alpha_i$ имеем

$$\begin{aligned} &(\mathbf{S} - \alpha_i\mathbf{1})^l\mathbf{x}^{(i,k)} = (k\alpha_i)^l\mathbf{x}^{(i,k-l)}, \quad 1 \leqslant l \leqslant k, \\ &(\mathbf{S} - \alpha_i\mathbf{1})^l\mathbf{x}^{(i,k)} = \mathbf{0}, \quad l > k. \end{aligned}$$

Теперь применим произведение операторов $\prod_{i=1}^{r-1} (\mathbf{S} - \alpha_i\mathbf{1})^{m_i}(\mathbf{S} - \alpha_r\mathbf{1})^{m_r-1}$ к нашей нулевой линейной комбинации $\sum_{i=1}^{r} \sum_{k=0}^{m_i-1} b_{i,k}\mathbf{x}^{(i,k)}$. Единственный вклад возникает из слагаемого $b_{r,m_r-1}\mathbf{x}^{(r,m_r-1)}$. Таким образом,

$$b_{r,m_r-1} \prod_{i=1}^{r-1} (\alpha_i - \alpha_r)^{m_i}[(m_r - 1)\alpha_r]^{m_r-1}\mathbf{x}^{(i,0)} = \mathbf{0}.$$

Следовательно, $b_{r,m_r-1}=0$. Далее мы применяем $\prod_{i=1}^{r-1}(\mathbf{S}-\alpha_i\mathbf{1})^{m_i}(\mathbf{S}-\alpha_r\mathbf{1})^{m_r-2}$ и получаем, что $b_{r,m_r-2}=0$. Продолжая в том же духе, мы сможем убедиться что все коэффициенты $b_{i,k}=0$. □

Изучая поток символов $(x_n)_{n\geqslant 0}$, наблюдатель, возможно, пожелает определить, был ли он генерирован л. о. с. р. с. Это можно сделать с помощью так называемого алгоритма Берлекэмпа—Мэсси (БМ) решения систем линейных уравнения. Если последовательность (x_n) появилась из л. о. с. р. с. с многочленом обратной связи $C(X)=\sum_{i=0}^{d-1}c_iX^i+X^d$, то рекуррентные соотношения $x_{n+d}=\sum_{i=0}^{d-1}c_ix_{n+i}$ для $n=0,\ldots,d$ могут быть записаны в векторно-матричном виде $\mathbf{A}_d\mathbf{c}_d=\mathbf{0}$, где

$$\mathbf{A}_d=\begin{pmatrix} x_0 & x_1 & x_2 & \ldots & x_d\\ x_1 & x_2 & x_3 & \ldots & x_{d+1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ x_d & x_{d+1} & x_{d+2} & \ldots & x_{2d}\end{pmatrix},\qquad \mathbf{c}_d=\begin{pmatrix} c_0\\ c_1\\ \vdots\\ c_{d-1}\\ 1\end{pmatrix}. \tag{4.5.13}$$

Следовательно, матрица $\mathbf{A}_d$ размера $(d+1)\times(d+1)$ должна иметь нулевой определитель, и $(d+1)$-мерный вектор $\mathbf{c}_d$ должен лежать в ядре $\ker\mathbf{A}_d$.

Алгоритм начинается с исследования матрицы $\mathbf{A}_r$ для малых значений r (известно, что $r\leqslant d$):

$$\mathbf{A}_r=\begin{pmatrix} x_0 & x_1 & x_2 & \ldots & x_r\\ x_1 & x_2 & x_3 & \ldots & x_{r+1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ x_r & x_{r+1} & x_{r+2} & \ldots & x_{2r}\end{pmatrix}.$$

Мы вычисляем $\det\mathbf{A}_r$ и если $\det\mathbf{A}_r\neq 0$, то делаем вывод, что $d\neq r$, и увеличиваем r на 1. Если $\det\mathbf{A}_r=0$, то решаем уравнение $\mathbf{A}_r\mathbf{a}_r=\mathbf{0}$, например, методом Гаусса, т. е. пробуем $d=r$:

$$\begin{pmatrix} x_0 & x_1 & x_2 & \ldots & x_d\\ x_1 & x_2 & x_3 & \ldots & x_{d+1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ x_d & x_{d+1} & x_{d+2} & \ldots & x_{2d}\end{pmatrix}\begin{pmatrix} a_0\\ a_1\\ \vdots\\ a_{d-1}\\ 1\end{pmatrix}=\mathbf{0}.$$

и тестируем последовательность (x_n) в качестве решения рекуррентного соотношения $x_{n+d}=\sum_{i=0}^{d-1}a_ix_{n+i}$. Если мы обнаруживаем противоречие, то

выбираем другой вектор $\mathbf{c}_r \in \ker \mathbf{A}_r$ или — если это не удаётся — увеличиваем r.

Алгоритм БМ можно сформулировать в красивом алгебраическом виде. Для данной последовательности (x_n) рассмотрим формальный степенной ряд $\sum\limits_{j=0}^{\infty} x_j X^j$. Тот факт, что последовательность (x_n) генерирована л. о. с. р. с. со вспомогательным многочленом $C(X)$, эквивалентен тому, что выписанный выше ряд является частным от деления $A(X) = \sum\limits_{i=0}^{d-1} a_i X^i$ на $C(X)$.

$$\sum_{j=0}^{\infty} x_j X^j = \frac{A(X)}{C(X)}. \tag{4.5.14}$$

Действительно, так как $c_0 = 1$, равенство $A(X) = C(X) \sum\limits_{j=0}^{\infty} x_j X^j$ равносильно тому, что

$$x_n = \begin{cases} a_n - \sum\limits_{i=1}^{d-1} c_i x_{n-i}, & n = 0,\ 1,\ \ldots,\ d-1, \\ -\sum\limits_{i=1}^{d-1} c_i x_{n-i}, & n \geqslant d. \end{cases} \tag{4.5.15}$$

Другими словами, $A(X)$ задает начальное заполнение, а $C(X)$ выступает в качестве многочлена обратной связи. □

Пример 4.5.7. Что такое линейная обратная связь регистра сдвига? Объясните метод Берлекэмпа—Мэсси восстановления многочлена обратной связи л. о. с. р. с. по её выходу. Проиллюстрируйте метод на таких выходах:

$$1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\ldots,$$
$$0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\ldots$$

и

$$1\,1\,0\,0\,1\,0\,1\,1\ldots$$

Решение. Начальное заполнение $x_0 \ldots x_{d-1}$ индуцирует выходной поток $(x_n)_{n\geqslant 0}$, удовлетворяющий рекуррентному соотношению

$$x_{n+d} = \sum_{i=0}^{d-1} c_i x_{n+i} \ \forall n \geqslant 0.$$

Многочлен обратной связи

$$C(X) = c_0 + c_1 X + \ldots + c_{d-1} X^{d-1} + X^d \tag{4.5.16}$$

является характеристическим многочленом для этого рекуррентного соотношения, определяющим его решения. Мы будем предполагать, что $c_0 \neq 0$; иначе значение x_n не влияет на x_{n+d} и регистр можно уменьшить на единицу до длины $d-1$.

Алгоритм Берлекэмпа—Мэсси начинается с рассмотрения матрицы

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \det \mathbf{A}_1 \neq 0,$$

но

$$\mathbf{A}_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{имеет } \det \mathbf{A}_2 = 0$$

и уравнение $\mathbf{A}_2 \begin{pmatrix} c_0 \\ c_1 \\ 1 \end{pmatrix} = 0$ обладает решением $c_0 = 1,\ c_1 = 0$. Отсюда получаем рекурсию

$$x_{n+2} = x_n,$$

что не согласуется с концом строки. Поэтому мы переходим к $\mathbf{A}_3$:

$$\mathbf{A}_3 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \det \mathbf{A}_3 \neq 0,$$

значит, берём $\mathbf{A}_4$:

$$\mathbf{A}_4 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad \det \mathbf{A}_4 = 0.$$

Решением уравнения $\mathbf{A}_4 \mathbf{c}_4 = 0$ служит столбец $\mathbf{c}_4 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. Отсюда следует соотношение

$$x_{n+4} = x_n + x_{n+3},$$

которое согласуется с последовательностью $(x_n)_{n \geqslant 0}$. Во втором примере имеем

$$\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq 0, \quad \det \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \neq 0, \quad \det \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \neq 0$$

и

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0,$$

откуда находим решение: $d = 4$, $x_{n+4} = x_n + x_{n+1}$. Линейному рекуррентному соотношению удовлетворяет каждый член данной выходной последовательности. Многочлен обратной связи равен $X^4 + X + 1$.

В третьем примере рекуррентное соотношение имеет вид $x_{n+3} = x_n + x_{n+1}$. □

> Полная безопасность никогда не была доступна для всех. Ожидать её нереально; представить, что она может существовать, — это катастрофа.
>
> *Эдвард Теллер* (1908–2003), американский физик, родившийся в Венгрии.

Л. о. с. р. с. используются для получения аддитивного шифра обратной связи. Аддитивные шифры обратной связи были изобретены в 1917 г. Гильбертом Вернамом, сотрудником AT&T Bell Labs. Здесь отправитель использует выходной поток л. о. с. р. с., (k_n), чтобы зашифровать открытый текст (p_n) как (z_n), где

$$z_n = p_n + k_n \bmod 2, \quad n \geqslant 0. \tag{4.5.17}$$

Получатель может декодировать сообщение как

$$p_n = z_n + k_n \bmod 2, \quad n \geqslant 0, \tag{4.5.18}$$

но, конечно, он должен знать начальное заполнение $k_0 \dots k_{d-1}$ и строку $c_0 \dots c_{d-1}$. Основной недостаток шифра обратной связи заключается в его периодичности. Действительно, если генерирующий л. о. с. р. с. имеет период D, то для «атакующего» достаточно иметь в своем распоряжении шифрограмму $z_0 z_1 \dots z_{2D-1}$ и соответствующий открытый текст $p_0 p_1 \dots p_{2D-1}$, длина $2D$. (Вполне выполнимые задачи для современных Шерлоков Холмсов.) Если при некоторой удаче атакующий знает величину периода D, то ему нужно только $z_0 z_1 \dots z_{D-1}$ и $p_0 p_1 \dots p_{D-1}$. Это позволит ему взломать шифр, т. е. расшифровать весь текст, хотя и за долгое время.

Ясно, что л. о. с. р. с. с коротким периодом легче взломать, когда они используются многократно. История второй мировой войны и последующей холодной войны даёт ряд впечатляющих примеров (успехи немецких криптографов во взломе кодов британского военно-морского флота, успехи британских и американских криптографов во вскрытии немецких кодов,

американский проект «Венона» по расшифровке советских кодов, полученных из интенсивного трафика сообщений). Однако даже ультрабольшой период не может гарантировать безопасность. Мы бы хотели упомянуть следующий не очень хорошо известный факт. Когда знаменитый офицер британской разведки Ким Филби, работавший как русский разведчик в 1930-х и 1940-х гг., услышал об успехах программы «Венона», он сообщил по аварийному каналу связи своим контроллерам в Москве, что американцы используют компьютер, который в один день делает столько, сколько «тысячи людей делают в тысячу дней», и что ключ к дешифровке — это многократное использование одного и того же шифра. Мы не знаем, было ли учтено его предупреждение.

Период л. о. с. р. с. можно увеличить, объединяя несколько л. о. с. р. с.

Теорема 4.5.8. *Пусть поток* (x_n) *получен с помощью л. о. с. р. с. длины* d_1 *периода* D_1 *и со вспомогательным многочленом* $C_1(X)$, *а поток* (y_n) *— с помощью л. о. с. р. с. длины* d_2 *периода* D_2 *и со вспомогательным многочленом* $C_2(X)$. *Пусть* $\alpha_1, \ldots, \alpha_{r_1}$ *и* $\beta_1, \ldots, \beta_{r_2}$ *— различные корни многочленов* $C_1(X)$ *и* $C_2(X)$ *соответственно, лежащие в некотором поле* $\mathbb{K} \supset \mathbb{F}_2$. *Пусть* m_i *— кратность корня* α_i *и* m'_j *— кратность корня* β_j *с* $d_1 = \sum\limits_{i=1}^{r_1} m_i$, $d_2 = \sum\limits_{i=1}^{r_2} m'_i$. *Тогда*

1) *поток* $(x_n + y_n)$ *получается из л. о. с. р. с. со вспомогательным многочленом* $\mathrm{НОК}\{C_1(X), C_2(X)\}$;

2) *поток* $(x_n y_n)$ *получается из л. о. с. р. с. со вспомогательным многочленом* $C(X) = \prod\limits_{i=1}^{r_1} \prod\limits_{j=1}^{r_2} (X - \alpha_i\beta_j)^{m_i + m'_j - 1}$.

В частности, период результирующего л. о. с. р. с. в обоих случаях делится на $\mathrm{НОК}\{D_1, D_2\}$.

Доказательство. Согласно теореме 4.5.6 выходные потоки (x_n) и (y_n) для л. о. с. р. с. из условия имеют следующий вид в поле $\mathbb{K}$:

$$x_n = \sum_{i=1}^{r_1} \sum_{k=0}^{m_i - 1} a_{i,k} A(n, k) \alpha_i^n, \quad y_n = \sum_{j=1}^{r_2} \sum_{l=0}^{m'_j - 1} b_{j,l} A(n, l) \beta_j^n \tag{4.5.19}$$

для некоторых $a_{i,k}, b_{j,l} \in \mathbb{K}$.

1. Представляя $x_n + y_n$ как сумму выражений из предыдущей формулы и приводя подобные члены, получим п. 1.

2. Для произведения $x_n y_n$ имеем выражение

$$\sum_{i,j} \sum_{k,l} a_{i,k} b_{j,l} A(n, k) A(n, l) (\alpha_i \beta_j)^n.$$

Произведение $a_{i,k}b_{j,l}A(n,\,k)A(n,\,l)$ можно представить в виде суммы $\sum\limits_{t=k\wedge l}^{k+l-1} A(n,\,t)u_t(a_{i,k},\,b_{j,l})$, где коэффициенты $u_t(a_{i,k},\,b_{j,l}) \in \mathbb{K}$. Отсюда получаем следующее представление произведений $x_n y_n$

$$\sum_{i=1}^{r_1}\sum_{j=1}^{r_2}\sum_{k=0}^{m_i-1}\sum_{l=0}^{m'_j-1}\sum_{t=k\wedge l}^{k+l-1} A(n,\,t)u_t(a_{i,k},\,b_{j,l})(\alpha_i\beta_j)^n,$$

что в свою очередь можно переписать как

$$x_n y_n = \sum_{i=1}^{r_1}\sum_{j=1}^{r_2}\sum_{t=0}^{m_i+m'_j-2} A(n,\,t)v_{i,j;t}(\alpha_i\beta_j)^n$$

в соответствии с общем видом выходного потока л. о. с. р. с. со вспомогательным многочленом $C(X)$ из п. 2. □

Несмотря на серьезные недостатки, л. о. с. р. с. ещё находят применение в самых разных ситуациях: они позволяют просто шифровать и дешифровать без «упреждения», а также отображать «локальное» воздействие ошибок, будь то кодирование, передача или декодирование. В более общей ситуации нелинейные о. с. р. с. часто предлагают только минимальные преимущества, но привносят серьёзные недостатки, в частности при дешифровании.

... an error by the same example.
Will rush into the state.

Вильям Шекспир (1564–1616),
английский драматург и поэт;
«Венецианский купец»

Пример 4.5.9. 1. Пусть (x_n), (y_n), (z_n) — потоки, произведённые л. о. с. р. с. Положим

$$k_n = \begin{cases} x_n, & \text{если } y_n = z_n, \\ y_n, & \text{если } y_n \neq z_n. \end{cases}$$

Покажите, что k_n тоже поток, произведённый л. о. с. р. с.

2. Шифр обратной связи генерируется с помощью л. о. с. р. с. известной длины d. Покажите, что, обладая исходным и зашифрованным текстами длины $2d$, можно восстановить шифр обратной связи.

Решение. 1. Для трёх потоков (x_n), (y_n), (z_n), сгенерированных л. о. с. р. с., положим

$$k_n = x_n + (x_n + y_n)(y_n + z_n) \quad (\text{в } \mathbb{F}_2),$$

так что достаточно заметить, что (поточечные) сумма и произведение потоков, сгенерированных л. о. с. р. с., представляют собой потоки, произведённые л. о. с. р. с.

2. Предположим, что исходный текст имеет вид $y_1, y_2, \ldots, y_{2d}$, а зашифрованный — $x_1 + y_1, x_2 + y_2, \ldots, x_{2d} + y_{2d}$. Тогда можно восстановить $x_1, \ldots, x_{2d}$. Нам известно, что $a_1, a_2, \ldots a_d$ должны удовлетворять системе d линейных уравнений

$$x_{d+j} = \sum_{i=1}^{d} a_i x_{j+i-1}, \quad j = 1, 2, \ldots, d.$$

Решая её, находим $a_1, a_2, \ldots a_d$, а значит, и весь шифр обратной связи. □

Пример 4.5.10. Двоичный нелинейный регистр обратной связи длины 4 определяется соотношением

$$x_{n+1} = x_{n-1} + x_n x_{n-2} + x_{n-3}.$$

Покажите, что пространство состояний содержит циклы длины 1, 4, 9 и 2.

Решение. Существует $2^4 = 16$ начальных двоичных строк. Простой проверкой убеждаемся, что

$$\begin{aligned}
&0000 \mapsto 0000 && \text{(цикл длины 1)},\\
&0001 \mapsto 0010 \mapsto 0100 \mapsto 1000 \mapsto 0001 && \text{(цикл длины 4)},\\
&0011 \mapsto 0111 \mapsto 1111 \mapsto 1110 \mapsto 1101 \mapsto\\
&\mapsto 1011 \mapsto 0110 \mapsto 1100 \mapsto 1001 \mapsto 0011 && \text{(цикл длины 9)},\\
&0101 \mapsto 1010 \mapsto 0101 && \text{(цикл длины 2)}.
\end{aligned}$$

Все 16 начальных заполнений присутствуют в списке, так что анализ полный. □

> ... случайные числа не должны быть сгенерированы методом, выбранным наугад.
>
> *Дональд Кнут* (род. в 1938 г.),
> американский программист, математик;
> «Искусство программирования»

Пример 4.5.11. Опишите принцип работы аддитивного шифра обратной связи. Что такое одноразовый блокнот? Коротко объясните, почему одноразовый блокнот стоек, если его применять только один раз, и теряет стойкость при многократном использовании?

При помощи одноразового блокнота посылается сообщение $x_1x_2x_3x_4x_5x_6y_7$ в виде 0101011. Из-за ошибки также передаётся сообщение $y_0x_1x_2x_3x_4x_5x_6$, в шифрованном виде — 0100010. Покажите,

что $x_1x_2x_3x_4x_5x_6$ — одно из двух возможных сообщений, и найдите обе возможности.

Решение. Одноразовый блокнот — это пример шифра, основанного на случайном ключе, предложенный Гильбертом Вернамом и Джозефом Моборном (командующий войск связи США во Второй мировой войне). Шифр использует генератор случайных чисел, производящий последовательность букв $k_1k_2k_3\ldots$ из алфавита J размера q. Более точно, каждая буква равномерно распределена по J, а разные буквы независимы. Сообщение $m = m_1m_2\ldots m_n$ зашифровывается как $c = c_1c_2\ldots c_n$, где

$$c_i = m_i + k_i \bmod q.$$

Чтобы показать, что одноразовый блокнот обеспечивает абсолютную стойкость, запишем

$$\mathsf{P}(M = m,\, C = c) = \mathsf{P}(M = m,\, K = c - m) = \\ = \mathsf{P}(M = m)\,\mathsf{P}(K = c - m) = \mathsf{P}(M = m)\frac{1}{q^n}.$$

Здесь разность $c - m$ берётся познаково и по модулю q. Следовательно, условная вероятность

$$\mathsf{P}(C = c|M = m) = \frac{\mathsf{P}(M = m,\, C = c)}{\mathsf{P}(M = m)} = \frac{1}{q^n}$$

не зависит от m. Значит, M и C не зависят друг от друга.

Работая в поле $\mathbb{F}_2$, рассмотрим поток ключей шифрования $k_1k_2k_3\ldots$ Тогда входной поток открытого текста $p_1p_2p_3\ldots$ шифруется как поток $c_1c_2c_3\ldots$, где $c_j = p_j + k_j$. Если k_j — н. о. р. случайные числа и поток ключей шифрования используется только раз (что случается на практике), то мы имеем дело с одноразовым блокнотом. (Предполагается, что поток ключей шифрования известен только отправителю и получателю.) В нашем примере мы имеем

$$x_1x_2x_3x_4x_5x_6y_7 \mapsto 0101011,$$
$$y_0x_1x_2x_3x_4x_5x_6 \mapsto 0100010.$$

Предположим, что $x_1 = 0$. Тогда

$$k_0 = 0,\ \ k_1 = 1,\ \ x_2 = 0,\ \ k_2 = 0,\ \ x_3 = 0,\ \ k_3 = 0,$$
$$x_4 = 1,\ \ k_1 = 0,\ \ x_5 = 1,\ \ k_5 = 0,\ \ x_6 = 1,\ \ k_6 = 1.$$

Таким образом,

$$k = 0100101, \quad x = 000111.$$

Если $x_1 = 1$, каждый знак изменится на противоположный, так что

$$k = 1011010, \quad x = 111000.$$

Альтернативное рассуждение: положим $x_0 = y_0$ и $x_7 = y_7$. Если первый шифр равен $q_1 q_2 \ldots$, второй — $p_1 p_2 \ldots$ и одноразовый блокнот — $k_1 k_2 \ldots$, то

$$q_j = k_{j+1} + x_{j+1}, \quad p_j = k_j + x_j.$$

Следовательно,

$$x_j + x_{j+1} = q_j + p_j,$$

и

$$x_1 + x_2 = 0, \quad x_2 + x_3 = 0,$$
$$x_3 + x_4 = 1, \quad x_4 + x_5 = 0, \quad x_5 + x_6 = 0,$$

откуда

$$x_1 = x_2 = x_3, \quad x_4 = x_5 = x_6, \quad x_4 = x_3 + 1.$$

Значит, сообщением может быть 000111 или 111000. □

Шифроблокноты были традиционным средством шифрования в первой половине XX века (до появления компьютеров, для генерирования случайных ключей использовались различные объемные тома классической литературы). В частности, советской (а до этого русской) разведкой был достигнут ряд успехов в использовании таких криптосистем. Некоторые эксперты считают, что эти успехи объясняются отчасти тем, что на протяжении десятилетий русские революционеры (особенно большевики) так преуспели в криптографической переписке. Ленин сам был дотошным криптографом (он когда-то выговаривал своему младшему брату, который использовал тот же или слегка изменённый блокнот более одного раза), но его жена Надежда Крупская (также активная большевичка) стала настоящим экспертом в криптографии. Известно, что члены Политбюро ЦК ВКП(б) регулярно обсуждали ситуации с неправильным использованием шифроблокнотов на своих заседаниях. В секретных стенограммах одного из заседаний в 1928 г. строго запрещается повторное использование тех же текстов для шифровки докладов советской внешней разведки. (В те годы разведывательная сеть пострадала от нескольких серьезных провалов.) Одной из рекомендованных мер была немедленная и всесторонняя проверка личных дел всех причастных лиц. При этом небрежность приравнивалась к саботажу — устрашающее обвинение, если вспомнить, что документ принимался с участием таких персонажей, как Сталин и Молотов, хотя Сталин в это время еще не получил полный политический контроль. С другой стороны, царская полиция и другие российские институты власти тоже имели высококвалифицированных криптографов. Когда Наполеон вторгся в Россию в 1812 г., его «депеши» (секретные приказы) регулярно перехватывались и расшифровывались; это привело к его падению. В 1815 г. состоялся знаменательный разговор российского императора Александра I с французским маршалом Макдональдом, одним из генералов Наполеона (шотландским якобитом, родившимся во Франции в 1765 г.). Император, сочувствуя покинутому всеми маршалу, указал на плачевное состояние дел Франции (Париж был тогда оккупирован Англией, Россией и Пруссией, и вся страна была в смятении) и отметил, что антифранцузская коалиции многое получила из перехваченной тайной переписки Наполеона. Макдональд выразил удивление и сказал: «Это странно... кто-то, вероятно, дал вам ключ». Александр ответил: «Вовсе нет. Я даю вам слово: мы просто все их расшифровали».

Есть ещё один известный эпизод из истории Первой мировой войны: он относится к затопленному на Балтике в 1914 г. немецкому крейсеру «Магдебург». После тщательного обыска севшего на скалы и затонувшего судна, русские получили его неповрежденные секретные кодовые книги. Уинстон Черчилль в своих мемуарах рассказывает историю (которая оспаривается некоторыми историками) о том, что русские подняли тело утонувшего немецкого офицера; его руки сжимали водонепроницаемый мешок с секретными немецкими военно-морскими документами, в том числе кодовыми книгами. На следующее утро, российский военный атташе в Лондоне сообщил Черчиллю (в то время первому лорду адмиралтейства) об этой находке, и в российский порт Архангельск был направлен британский корабль, чтобы забрать ценные кодовые книги, которые впоследствии были перевезены в Лондон. Но интересно то, что, как правило, опускают в этой истории: русские ловко обманули захваченных членов экипажа (в том числе капитана «Магдебурга»), они «случайно» обронили копию ложного сообщения, в котором говорилось, что поиски затонувшего крейсера не представляют для них какого-либо интереса. Один из пленных немецких офицеров немедленно написал об этом своей семье (в зашифрованной форме, конечно), и эта информация достигла германского адмиралтейства. В результате немецкий флот продолжал использовать тот же шифр, что и прежде...

Криптографы делают это в бесконечной случайной последовательности.

(Из серии «Как они делают это».)

Пример 4.5.12. 1. Пусть $\theta\colon \mathbb{Z}_+ \to \{0, 1\}$ определяется правилом: $\theta(n) = 1$, если n нечётное, и $\theta(n) = 0$, если n чётное. Рассмотрим следующее рекуррентное соотношение над $\mathbb{F}_2$:

$$u_{n+3} + u_{n+2} + u_{n+1} + u_n = 0. \tag{4.5.20}$$

Верно ли, что общее решение уравнения (4.5.20) выглядит как $u_n = A + B\theta(n) + C\theta(n^2)$? Если верно, то докажите это, если нет, то объясните, почему это не так, выпишите и обоснуйте правильное решение.

2. Решите рекуррентное уравнение $u_{n+2} + u_n = 1$ над $\mathbb{F}_2$ при условии, что $u_0 = 1$, $u_1 = 0$. Выразите решение через функцию $\theta(n)$.

3. Линейный регистр обратной связи генерирует четыре потока w_n, x_n, y_n, z_n. Положим

$$k_n = \begin{cases} x_n + y_n + z_n, & \text{если } z_n + w_n = 1, \\ x_n + w_n, & \text{если } z_n + w_n = 0. \end{cases}$$

Покажите, что k_n — тоже поток, сгенерированный л. о. с. р. с.

Решение. 1. Заметим, что $\theta(n^2) = \theta(n)$, так что приведённая в условии сумма содержит только две произвольные константы. Теперь рассмотрим

$g(n) = \theta(n(n-1)/2)$. Тогда

$$g(n+3) + g(n+2) + g(n+1) + g(n) =$$
$$= \theta\Big(\frac{(n+3)(n+2)}{2}\Big) + \theta\Big(\frac{(n+2)(n+1)}{2}\Big) +$$
$$+ \theta\Big(\frac{(n+1)n}{2}\Big) + \theta\Big(\frac{n(n-1)}{2}\Big) = \theta((n+2)^2 + n^2) = 0,$$

$g(0) = g(1) = 0$, $g(2) = 1$. Подставим $n = 0$ и $n = 1$ в соотношение $a\theta(n) + b + cg(n) = 0$ и заметим, что $a = b = c = 0$. Поэтому $\theta(n)$, 1, $g(n)$ независимы и $A\theta(n) + B + Cg(n)$ — общее решение разностного уравнения 3-го порядка.

2. Сначала попробуем решить уравнение $u_{n+2} + u_n = 1$ без каких-либо дополнительных условий.

$$g(n) + g(n+2) = \theta\Big(\frac{n(n-1)}{2} + \frac{(n+2)(n+1)}{2}\Big) =$$
$$= \theta\Big(\frac{n^2 - n + n^2 + 3n + 2}{2}\Big) = \theta(n^2 + n + 1) = 1.$$

Теперь подставим $n = 0$ и $n = 1$ в равенство $u_n = A + B\theta(n) + g(n)$ и получим, что $A = B = 1$, откуда $u_n = 1 + \theta(n) + g(n)$.

3. Последовательность k_n генерируется линейным регистром

$$k_n = x_n + w_n + (z_n + w_n)(y_n + z_n + w_n). \qquad \square$$

Враг знает всё.

Клод Шеннон (1916–2001),
американский электротехник и математик

В следующей части параграфа мы обсудим свойства класса современных криптосистем, которые называются *шифрами с открытым ключом*, уделив особое внимание системе РША (Райвест (Rivest), Шамир (Shamir) и Адлеман (Adelman)) и электронной подписи.

Определение 4.5.13. Будем говорить, что задана формальная криптосистема, если заданы такие

1) множество $\mathcal{P}$ *открытых текстов* — на языке гл. 1 источник сообщений;
2) множество $\mathcal{C}$ *шифротекстов* — на языке гл. 1 кодовых слов;
3) множество $\mathcal{K}$ *ключей*, которые нумеруют отображения кодирования;
4) множество $\mathcal{E}$ шифрующих функций (кодирующих отображений), где каждая функция $E_k\colon P \in \mathcal{P} \mapsto E_k(P) \in \mathcal{C}$ зависит от элемента $k \in \mathcal{K}$;

5) множество $\mathcal{D}$ дешифрующих функций (декодирующих отображений), где каждая функция $D_k\colon C \in \mathcal{C} \mapsto D_k(C) \in \mathcal{P}$ тоже зависит от элемента $k \in \mathcal{K}$;

что

6) для любого ключа $e \in \mathcal{K}$ найдётся ключ $d \in \mathcal{K}$ с тем свойством, что $D_d(E_e(P)) = P$ для любого открытого текста $P \in \mathcal{P}$. □

Пример 4.5.14. Предположим, что две стороны, Боб и Алиса, собираются устроить двустороннюю закрытую переписку. Они хотят обменяться своими ключами E_A и E_B через открытый двоичный канал. Очевидный протокол состоит в следующем. Алиса шифрует открытый текст m как $E_A(m)$ и посылает его Бобу. Тот шифрует его как $E_B(E_A(m))$ и возвращает полученное Алисе. Теперь мы воспользуемся ключевым предположением о том, что E_A и E_B коммутируют на любом открытом тексте m': $E_A \circ E_B(m') = E_B \circ E_A(m')$. В этом случае Алиса может дешифровать это сообщение как $D_A(E_A(E_B(m))) = E_B(m)$ и отослать результат Бобу, который вычислит $D_B(E_B(m)) = m$. В соответствии с этим протоколом, в течение всего обмена незашифрованное сообщение ни разу не передаётся.

Вместе с тем после некоторого размышления можно понять, что это не решает всех проблем. Действительно, предположим, что Алиса использует одноразовый блокнот k_A, а Боб — одноразовый блокнот k_B. Тогда любой однократный перехват не предоставляет информации о тексте p. Однако если все три передачи была перехвачены, то достаточно взять сумму

$$(m + k_A) + (m + k_A + k_B) + (m + k_B) = m$$

и получить открытый текст m. Поэтому нужно разработать более сложный протокол: здесь полезны криптосистемы с открытым ключом. □

Еще одним популярным примером служат применяемые сетью инвесторов и брокеров, действующих на рынке, криптосистемы открытого ключа, такие как РША. Инвестор опасается, что брокер будет покупать акции без авторизации и в случае потери станет утверждать, что у него есть письменный запрос от клиента. На самом деле брокеру несложно создать шифрованное поручение покупать акции, так как ключ шифрования находится в открытом доступе. С другой стороны, брокер может быть обеспокоен тем, что если он покупает акции по запросу вкладчика и рынок пойдет вниз, то инвестор может утверждать, что он никогда не заказывал эту сделку и что его зашифрованное поручение — это фальшивка.

Однако можно легко разработать протокол, который решает эти вопросы. Инвестор Алиса отправляет брокеру Бобу вместе с поручением p купить акции свою «электронную подпись» $f_B f_A^{-1}(p)$. После получения этого сообщения Боб посылает квитанцию r, шифруя её как $f_A f_B^{-1}(r)$.

В конфликтной ситуации обе стороны могут предоставить третьей стороне (например, суду) эти кодированные сообщения и ключи. Поскольку никто, кроме Алисы, не может шифровать сообщение функцией $f_B f_A^{-1}$ и никто, кроме Боба, не в состоянии пользоваться функцией $f_A f_B^{-1}$, сомнений не останется. В этом суть электронной подписи. □

Упоминавшаяся ранее схема РША является основным примером криптосистемы с открытым ключом. Здесь получатель (Боб, а возможно, коллективный пользователь) устанавливает

$$N = pq, \quad \text{где } p \text{ и } q \text{ — большие простые числа, хранящиеся в секрете.} \tag{4.5.21}$$

Число N часто называют модулем РША и делают открытым. Значение функции Эйлера

$$\varphi(N) = (p-1)(q-1)$$

держится в секрете. Далее, получатель выбирает (или получает из распределительного центра) такое натуральное число l, что

$$1 < l < \varphi(N) \quad \text{и} \quad \text{НОД}\,(\varphi(N),\, l) = 1. \tag{4.5.22}$$

И, наконец, вычисляется такое целое число d (опять же Бобом или от его имени), что

$$1 < d < \varphi(N) \quad \text{и} \quad ld = 1 \bmod (\varphi(N)). \tag{4.5.23}$$

(Значение d можно вычислить с помощью расширенного алгоритма Евклида.) Открытый ключ e_B, используемый для шифрования — это пара (N, l) (доступная в открытой директории). Отправитель (Алиса) при связи с Бобом понимает, что множествами открытых текстов и шифротекстов являются $\mathcal{P} = \mathcal{C} = \{1, \ldots, N-1\}$. Она шифрует свой выбранный открытый текст $m = 1, \ldots, N-1$ как шифрограмму

$$E_{N,l}(m) = c = m^l \bmod N. \tag{4.5.24}$$

Будь проклята открытость!

Уильям Г. Вандербильт (1821–1885),
американский бизнесмен

Частный ключ Боба d_B — это пара (N, d) (или просто число d): оно скрыто от общественности, но известно Бобу. Получатель дешифрует шифротекст c как

$$D_d(c) = c^d \bmod N. \tag{4.5.25}$$

В литературе l часто называют шифрующей, а d — дешифрующей экспонентами. Теорема 4.5.15, сформулированная ниже, гарантирует, что

$$D_d(c) = m^{dl} = m \bmod N, \tag{4.5.26}$$

т. е. шифротекст c дешифруется корректно.

Теорема 4.5.15. *Для всех целых чисел* $m = 0, \ldots, N-1$ *выполнено соотношение* (4.5.26), *когда числа* l *и* d *удовлетворяют условиям* (4.5.22) *и* (4.5.23), *а* N — (4.5.21).

Доказательство. Ввиду формулы (4.5.23) имеем

$$ld = 1 + b(p-1)(q-1),$$

где b — целое число. Тогда

$$(m^l)^d = m^{ld} = m^{1+b(p-1)(q-1)} = m(m^{(p-1)})^{(q-1)b}.$$

Напомним теорему Эйлера—Ферма: если НОД $(m, p) = 1$, то $m^{\varphi(p)} = 1 \bmod p$. Отсюда следует, что если m не делится на p, то

$$(m^l)^d = m \bmod p. \tag{4.5.27}$$

В противном случае, т. е. когда $p|m$, равенство (4.5.27) остаётся верным, поскольку тогда как m, так и $(m^l)^d$ равны нулю по модулю p. Аналогично

$$(m^l)^d = m \bmod q. \tag{4.5.28}$$

По китайской теореме об остатках (см. [Bu], [Mo]) из равенства (4.5.27) и (4.5.28) следует соотношение (4.5.26). □

Пример 4.5.16. Предположим, что Боб выбрал $p = 29$, $q = 31$, тогда $N = 899$ и $\varphi(N) = 840$. Наименьшее возможное l, для которого НОД $(l, \varphi(N)) = 1$, — это $l = 11$, затем 13, 17 и т. д. Расширенный алгоритм Евклида даёт $d = 611$ для $l = 11$, $d = 517$ для $l = 13$ и т. д. В первом случае шифрующий ключ $E_{899,11}$ равен

$$m \mapsto m^{11} \bmod 899, \quad \text{а именно,} \quad E_{899,11}(2) = 250.$$

Шифротекст 250 дешифруется так:

$$D_{611}(250) = 250^{611} \bmod 899 = 2.$$

(Вычисления осуществляются на компьютере. Компьютер необходим даже после упрощения с использованием китайской теоремы об остатках. В качестве примера приведём команду в программе «Математика» — это PowerMod[250,611,899].) □

Пример 4.5.17. 1. В рамках криптосистемы РША с открытым ключом (N, l) и закрытым ключом $(\varphi(N), d)$, обсудите возможные преимущества или недостатки выбора а) $l = 2^{32} + 1$ или б) $d = 2^{32} + 1$.

2. Пусть дано (большое) число N и нам известно, что оно является произведением двух разных простых чисел: $N = pq$, но сами сомножители p и q нам неизвестны. Допустим, нам дано ещё одно натуральное число m, которое делится на $\varphi(N)$. Объясните, как найти p и q.

3. Опишите, как решить проблему взаимных обязательств с помощью РША.

Решение. 1. Используя $l = 2^{32} + 1$, осуществим быстрое шифрование (потребуется только 33 умножения, опирающихся на повторяющееся возведение в квадрат). При $d = 2^{32} + 1$ можно быстро дешифровать сообщение (но атакующий может легко отгадать его).

2. Покажем, что если известно число m, кратное $\varphi(N)$, то можно «легко» разложить N на простые множители. Для натуральных чисел y, $M > 1$ обозначим через $\mathrm{ord}_M(y)$ порядок y относительно M:

$$\mathrm{ord}_M(y) = \min[s = 1, 2, \ldots : y^s = 1 \bmod M].$$

Допустим, что $m = 2^a b$, где $a \geqslant 0$ и b нечётно. Положим

$$\mathbb{X} = \{x = 1, 2, \ldots, N\colon \mathrm{ord}_p(x^b) \neq \mathrm{ord}_q(x^b)\}. \tag{4.5.29}$$

Лемма 4.5.18. 1. *Пусть $N = pq$ и m — таковы, что $\varphi(N) | m$, и определим множество $\mathbb{X}$ как в формуле* (4.5.29). *Если $x \in \mathbb{X}$, то существует такое $0 \leqslant t < a$, что* НОД $(x^{2^t b} - 1, N) > 1$ — *нетривиальный делитель числа $N = pq$.*

2. *Мощность множества $\#\mathbb{X}$ не меньше $\varphi(N)/2$.*

Доказательство. 1. Положим $y = x^b \bmod N$. Из теоремы Эйлера—Ферма следует, что $x^{\varphi(N)} = 1 \bmod N$ и поэтому $y^{2^a} = 1 \bmod N$. Тогда

$$\mathrm{ord}_p(x^b) \quad \text{и} \quad \mathrm{ord}_q(x^b) \text{ — степени числа 2.}$$

Если $x \in \mathbb{X}$, то $\mathrm{ord}_p(x^b) \neq \mathrm{ord}_q(x^b)$; скажем, $\mathrm{ord}_p(x^b) < \mathrm{ord}_q(x^b)$. Тогда существует такое $0 \leqslant t < a$, что

$$y^{2^t} = 1 \bmod p, \quad y^{2^t} \neq 1 \bmod q.$$

Таким образом, НОД $(y^{2^t} - 1, N) = p$, что и требовалось.

2. По китайской теореме об остатках существует такая биекция

$$x \in \{1, \ldots, N\} \leftrightarrow (x \bmod p, x \bmod q) \in \{1, \ldots, p\} \times \{1, \ldots, q\},$$

что $N \leftrightarrow (p, q)$. Тогда достаточно показать, что если разбить множество $\{1, \ldots, p\}$ на подмножества согласно значению $\mathrm{ord}_p(x^b)$, $x \in \mathbb{X}$, то размер каждого подмножества окажется не больше $(p-1)/2$. Проверяем это, предъявив подмножество размера $(p-1)/2$. Заметим, что

$$\varphi(N) | 2^a b \implies \text{существует такое } \gamma \in \{1, \ldots p-1\}, \text{ что } \mathrm{ord}_p(\gamma^b) \text{ — степень 2.}$$

Из последнего утверждения, в свою очередь, следует, что

$$\mathrm{ord}_p(\gamma^{\delta b}) = \mathrm{ord}_p(\gamma^b), \text{ если } \delta \text{ нечётно, и } \mathrm{ord}_p(\gamma^{\delta b}) < \mathrm{ord}_p(\gamma^b), \text{ если } \delta \text{ чётно.}$$

Следовательно, $\{\gamma^\delta \bmod p\colon \delta \text{ нечётно}\}$ — искомое подмножество. □

Теперь вернёмся к примеру 4.5.17. Для данных N, l и d положим $m = dl - 1$. Поскольку $\varphi(N) | dl - 1$, можно воспользоваться леммой 4.5.18 и разложить N на множители. Если мы выберем $x < N$ наугад, то вероятность отыскать нетривиальный делитель — не менее чем $1/2$, Поэтому вероятность неудачи при r случайных попытках выбора $x \in \mathbb{X}$ — не превосходит $1/2^r$.

3. Проблема взаимных обязательств возникает в следующем случае: Алиса шлёт сообщение Бобу таким образом, что

1) Боб не может прочесть сообщение, пока Алиса не пришлёт дальнейшую информацию,

2) Алиса не в состоянии изменить сообщение.

Решение проблемы заключается в электронной подписи: Боб не прочтёт сообщение, пока Алиса (позже) не покажет ему свой частный ключ. Это не нарушает условий 1) и 2) и создаёт условия, при которых Алиса (юридически), не может отказаться от своего авторства. □

Наш следующий пример посвящён *шифру Рабина*, или криптосистеме Рабина—Уильямса. Здесь стойкость тоже зависит от сложности разложения на простые множители. Для этой системы, была доказана тесная связь между стойкостью и проблемой разложения на множители: зная, решение проблемы разложения, можно взломать криптосистему, а способность взломать криптосистему приводит к разложению на множители. (Это не так в случае с РША: не известно, позволяет ли взлом РША решить проблема разложения.)

В системе Рабина принимающий пользователь Алиса случайно выбирает два больших простых числа p и q, так что

$$p = q = 3 \bmod 4. \tag{4.5.30}$$

Более того,

$$\begin{gathered}\text{открытый ключ Алисы} — N = pq, \text{ а её частный ключ} — \text{пара } (p, q);\\ \text{открытый и шифротекст Алисы} — \text{это числа } M = 0, 1, \ldots, N-1,\\ \text{а её шифрующая функция} — E_N(m) = c = m^2 \bmod N.\end{gathered} \tag{4.5.31}$$

Чтобы расшифровать шифротекст c, присланный ей, Алиса вычисляет

$$m_p = c^{(p+1)/4} \bmod p \quad \text{и} \quad m_q = c^{(q+1)/4} \bmod q. \tag{4.5.32}$$

Тогда

$$\pm m_p = c^{1/2} \bmod p \quad \text{и} \quad \pm m_q = c^{1/2} \bmod q,$$

т. е. $\pm m_p$ и $\pm m_q$ — квадратные корни из c по модулю p или q соответственно. Действительно,

$$(\pm m_p)^2 = c^{(p+1)/2} = c^{(p-1)/2}c = (\pm m_p)^{p-1}c = c \bmod p;$$

На последнем шаге мы воспользовались теоремой Эйлера—Ферма. Рассуждения с $\pm m_q$ аналогичны. Затем с помощью алгоритма Евклида она вычисляет такие целые числа $u(p)$ и $v(q)$, что

$$u(p)p + v(q)q = 1.$$

Наконец, Алиса вычисляет

$$\pm r = \pm[u(p)pm_q + v(q)qm_p] \bmod N$$

и

$$\pm s = \pm[u(p)pm_q - v(q)qm_p] \bmod N.$$

Существует четыре квадратных корня из c по модулю N. Открытый текст m — один из них. Для уверенности, что она сможет идентифицировать исходный открытый текст, Алиса может уменьшить пространство открытых текстов $\mathcal{P}$, накладывая на допустимые тексты дополнительные условия (например, чтобы первые 32 и последние 32 знака повторяли друг друга), чтобы было маловероятным, что более одного квадратного корня удовлетворяло этим условиям.

Однако такая мера может привести к облегчению взлома шифра, поскольку будет не всегда верно, что «редуцированная» проблема взлома эквивалентна проблеме разложения на простые множители.

> Я часто восхищался мистическим образом мыслей Пифагора и тайной магией чисел.
>
> *Томас Браун* (1605–1682)
> английский писатель, который писал о медицине, религии, науке и эзотерике

Пример 4.5.19. Алиса привлекает простые числа $p = 11$ и $q = 23$, т. е. $N = 253$. Боб шифрует сообщение числом $m = 164$:

$$c = m^2 \bmod N = 78.$$

Алиса вычисляет $m_p = 1$, $m_q = 3$, $u(p) = -2$, $v_q = 1$, после чего получает

$$r = \pm[u(p)pm_q + v(q)qm_p] \bmod N = 210 \text{ и } 43,$$
$$s = \pm[u(p)pm_q - v(q)qm_p] \bmod N = 164 \text{ и } 89$$

и отыскивает сообщение $m = 164$ среди решений: $164^2 = 78 \bmod 253$. □

Мы продолжаем знакомство с крипографией на примере схемы обмена ключами Диффи—Хеллмана. Диффи и Хеллман предложили протокол, позволяющий двум пользователям обменяться секретными ключами по незащищенным каналам. Схема Диффи—Хеллмана не является криптосистемой с открытым ключом, но её значение было широко признано, поскольку она создаёт основу для подписи Эль-Гамаля.

Протокол Диффи—Хеллмана связан с проблемой дискретных логарифмов (ПДЛ): нам даны простое число p, поле $\mathbb{F}_p$, мультипликативная циклическая группа $\mathbb{F}_p^* \simeq \mathbb{Z}_{p-1}$ и её образующая γ (т. е. примитивный элемент в $\mathbb{F}_p^*$). Тогда $\forall b \in \mathbb{F}_p^*$ существует такое единственное $\alpha \in \{0, 1, \ldots, p-2\}$, что

$$b = \gamma^\alpha \bmod p. \tag{4.5.33}$$

В этом случае α называют *дискретным логарифмом* по модулю p числа b с основанием γ; некоторые авторы пишут $\alpha = \operatorname{dlog}_\gamma b \bmod p$. Вычисление дискретных логарифмов считается трудной задачей: неизвестно эффективного (полиномиального) алгоритма их вычисления. (В аддитивной циклической группе $\mathbb{Z}/(n\mathbb{Z})$ ПДЛ сводится к уравнению $b = \gamma\alpha \bmod n$ и решается с помощью алгоритма Евклида.)

Протокол Диффи—Хеллмана позволяет Алисе и Бобу выработать общий секретный ключ, основываясь на таблицах полей $\mathbb{F}_p$ для достаточно большого количества простых чисел p. Им известен примитивный элемент γ в каждом из этих полей. Они договариваются фиксировать большое простое число p и примитивный элемент $\gamma \in \mathbb{F}_p$. Пара (p, γ) может быть всем известна: Алиса с Бобом могут договариваться о p и γ по незащищённому каналу.

Далее Алиса случайно выбирает $a \in \{0, 1, \ldots, p-2\}$, вычисляет

$$A = \gamma^a \bmod p$$

и посылает Бобу, храня a в секрете. Симметрично Боб случайно выбирает $b \in \{0, 1, \ldots, p-2\}$, вычисляет

$$B = \gamma^b \bmod p$$

и передаёт B Алисе, храня b в секрете. Затем

$$\text{Алиса вычисляет } B^a \bmod p, \text{ а Боб} — A^b \bmod p,$$

и их общий секретный ключ — это

$$K = \gamma^{ab} = B^a = A^b \bmod p.$$

Атакующий может перехватить p, γ, A и B, но ему неизвестны

$$\text{ни } a = \operatorname{dlog}_\gamma A \bmod p, \text{ ни } b = \operatorname{dlog}_\gamma B \bmod p.$$

Если атакующий сумеет найти дискретный логарифм по модулю p, он сможет взломать секретный ключ, и это единственный известный способ взлома такого ключа. Противоположный вопрос: сможет ли атакующий решить ПДЛ, взломав протокол, остаётся открытым (его считают важной задачей в криптосистемах с открытым ключом).

Однако, как и остальные обсуждавшиеся схемы, протокол Диффи—Хеллмана имеет свои слабые места: он уязвим при атаке *человек посередине*. Здесь атакующий пользуется тем, что ни Алиса, ни Боб не могут проверить, что данное сообщение действительно пришло от партнёра, а не от кого-то третьего. Предположим, что атакующий может перехватывать все сообщения переписки между Алисой и Бобом. Допустим, он может выдать себя за Боба и обменяться ключами с Алисой и в то же время притвориться Алисой и обменяться ключами с Бобом. Необходима электронная подпись, чтобы исключить эту возможность.

Мы закончим § 4.5 знакомством с криптосистемой Эль-Гамаля, основанной на *электронной подписи*. Шифр Эль-Гамаля можно рассматривать как усовершенствование протокола Диффи—Хеллмана. Обе схемы опираются на сложность решения ПДЛ. В системе Эль-Гамаля получающий пользователь Алиса выбирает простое число p и примитивный элемент $\gamma \in \mathbb{F}_p$. Затем она случайно выбирает показатель $a \in \{0, \ldots, p-2\}$, вычисляет

$$A = \gamma^a \bmod p$$

и объявляет/пересылает

$$\text{тройку } (p, \gamma, A) \text{ — её открытый ключ.}$$

В то же время она скрывает

$$\text{показатель } a \text{ — её частный ключ.}$$

Множество открытых текстов Алисы — это $\mathcal{P} = \{0, 1, \ldots, p-1\}$.

Второй участник, Боб, хочет послать сообщение Алисе и, зная тройку (p, γ, A), случайно выбирает показатель $b \in \{0, 1, \ldots, p-2\}$ и вычисляет

$$B = \gamma^b \bmod p.$$

Потом Боб позволяет Алисе узнать B (что он может сделать, переслав значение B). Величина B будет играть роль «подписи» Боба. В отличие от этого, значение показателя b Боб держит в секрете.

Далее, чтобы послать Алисе сообщение $m \in \{0, 1\ldots., p-1\}$, Боб шифрует m парой

$$E_b(m) = (B, c), \text{ где } c = A^b m \bmod p,$$

т. е. шифротекст Боба состоит из двух компонент: зашифрованного сообщения c и его *подписи* B.

Ясно, что числа A и B — части протокола Диффи—Хеллмана; в том смысле, что последний можно рассматривать как часть шифра Эль-Гамаля. Далее, зашифрованное сообщение c — это произведение m на множитель A^b, объединяющий часть открытого ключа Алисы и показатель b Боба.

Когда Алиса получает шифротекст (B, c), она пользуется своим секретным ключом a. А именно, она делит c на B^a по модулю p. Удобно вычислить $x = p - 1 - a$: поскольку $1 \leqslant a \leqslant p - 2$, значение x тоже удовлетворяет неравенству $1 \leqslant x \leqslant p - 2$. После этого Алиса дешифрует c как $B^x \bmod p$. Это даёт исходное сообщение m, поскольку

$$B^x c = \gamma^{b(p-1-a)} A^b m = (\gamma^{p-1})^b (\gamma^a)^{-b} A^b m = A^{-b} A^b m = m \bmod p. \qquad \square$$

Пример 4.5.20. При $p = 37$, $\gamma = 2$ и $a = 12$ мы имеем

$$A = \gamma^a \bmod p = 26,$$

и открытый ключ Алисы — $(p = 3, \gamma = 2, A = 26)$, множество её открытых текстов — 0,1,...,36, а частный ключ — $a = 12$. Предположим, что Боб выбрал $b = 32$, тогда

$$B = 2^{32} \bmod 37 = 4.$$

Допустим, Боб собирается послать $m = 31$. Он шифрует m как

$$c = A^b m \bmod p = (26)^{32} m \bmod 37 = 10 \times 31 \bmod 37 = 14.$$

Алиса дешифрует это сообщение как $2^{32} = 7$ и $7^{24} = 26 \bmod 37$

$$14 \times 2^{32(37-12-1)} \bmod 37 = 14 \times 7^{24} = 14 \times 26 \bmod 37 = 31. \qquad \square$$

Пример 4.5.21. Предположим, что Алиса планирует послать Бобу сообщение «today», используя шифр Эль-Гамаля. Опишите, как она может это сделать с простым числом $p = 15485863$, и примитивным элементом $\gamma = 6$ по модулю p при её выборе $b = 69$. Предположите, что частный ключ Боба — $a = 5$. Как Боб сможет прочесть сообщение с помощью программы «Математика»?

Решение. Открытый ключ Боба — это (15485863, 6, 7776), что известно Алисе. Пронумеровав английский алфавит, Алиса переведёт сообщение в числовой эквивалент 19, 14, 3, 0, 24. Так как $26^5 < p < 26^6$, она может представить открытый текст сообщения как одно пятизначное целое число в 26-ичной системе счисления:

$$m = 19 \times 26^4 + 14 \times 26^3 + 3 \times 26^2 + 0 \times 26 + 24 = 8930660.$$

Теперь она вычисляет $\gamma^b = 6^{69} = 13733130 \bmod 15485863$, затем

$$m\gamma^{ab} = 8930660 \times 7776^{69} = 4578170 \bmod 15485863.$$

Алиса посылает $c = (13733130, 4578170)$ Бобу. Тот с помощью своего частного ключа вычисляет

$$(\gamma^b)^{p-1-a} = 13733130^{15485863-1-5} = 2620662 \bmod 15485863$$

и

$$(\gamma^b)^{p-1-a} m\gamma^{ab} = 2620662 \times 4578170 = 8930660 \bmod 15485863,$$

после чего переводит число обратно в английский открытый текст. □

Пример 4.5.22. 1. Опишите схему Рабина—Уильямса шифрования сообщения x как x^2 по подходящему модулю N. Покажите, что если N выбрано произвольно, то взлом шифра эквивалентен разложению модуля в произведение двух простых.

2. Опишите систему РША, ассоциированную с открытым ключом e, частным ключом d и произведением N двух больших простых чисел.

Приведите простой пример, показывающий, что система уязвима для атаки гомоморфизма. Объясните, как разложить N на множители, если известны e, d и N.

Решение. 1. Фиксируем два больших простых числа p, $q = -1 \bmod 4$, которые составят частный ключ; открытым ключом служит произведение $N = pq$. Используются следующие свойства:

1) если p — простое число, то уравнение $a^2 = d \bmod p$ имеет не более двух решений,

2) для простого числа $p = -1 \bmod 4$, т. е. $p = 4k - 1$, если уравнение $a^2 = c \bmod p$ имеет решение, то $a = c^{(p+1)/4}$ — одно решение, а $a = -c^{(p+1)/4}$ — второе. (Действительно, если $c = a^2 \bmod p$, то по теореме Эйлера—Ферма $c^{2k} = a^{4k} = a^{(p-1)+2} = a^2 \bmod p$, откуда $c^k = \pm a$.)

Сообщение — это число $m \in \mathcal{M} = \{0, 1, \ldots, N-1\}$. Шифровальщик (Боб) посылает (открыто) $\tilde{m} = m^2 \bmod N$. Дешифратор (Алиса) использует свойство 2) для вычисления двух возможных значений $m \bmod p$ и двух возможных $m \bmod q$. После этого китайская теорема об остатках даёт четыре возможных значения для m: три из них будут неверными, а одно правильным.

Таким образом, разложив N в произведение, можно взломать шифр. Обратно, допустим, нам удалось взломать шифр. Тогда мы можем найти все четыре различные квадратных корня u_1, u_2, u_3, $u_4 \bmod N$ для общего u. (Китайская теорема об остатках плюс свойство 1) показывают, что u будет иметь 0 или 4 квадратных корня, если, конечно, u не кратно p или q.)

Тогда $u_j u^{-1}$ (что можно вычислить через алгоритм Евклида) даёт четыре квадратных корня из 1 по mod$N$: 1, -1, ε_1 и ε_2, причём

$$\varepsilon_1 = 1 \bmod p, \quad \varepsilon_1 = -1 \bmod q$$

и

$$\varepsilon_2 = -1 \bmod p, \quad \varepsilon_2 = 1 \bmod q.$$

Меняя при необходимости p и q, можно считать, что мы знаем ε_1. Поскольку $\varepsilon_1 - 1$ делится на p и не делится на q, НОД $(\varepsilon_1 - 1, N) = p$, т. е. p можно найти алгоритмом Евклида, после чего легко отыскать и q.

На практике это можно сделать следующим образом. Предполагая, что мы можем вычислять квадратные корни по модулю N, мы случайно берём x и решаем уравнение $x^2 = y^2 \bmod N$. С вероятностью $1/2$ получим, что $x \neq \pm y \bmod N$. Тогда НОД $(x - y, N)$ — нетривиальный делитель модуля N. Процедура повторяется до тех пор, пока не найдётся делитель; после k таких попыток вероятность успеха составит $1 - 2^{-k}$.

2. Чтобы определить криптосистему РША, выберем случайным образом большие простые числа p и q. По малой теореме Ферма

$$x^{p-1} = 1 \bmod p, \quad x^{q-1} = 1 \bmod q.$$

Поэтому, положив $N = pq$ и $\lambda(N) = \text{НОК}\,(p - 1, q - 1)$, получим

$$x^{\lambda(N)} = 1 \bmod N$$

для любого целого x, взаимно простого с N.

Далее мы случайно выбираем e. Либо алгоритм Евклида покажет, что e не взаимно просто с $\lambda(N)$, либо с помощью алгоритма Евклида мы отыщем такое d, что

$$de = 1 \bmod (\lambda(N)).$$

С очень большой вероятностью несколько попыток дадут подходящие d и e.

Теперь мы выложим значения e и N в качестве открытого ключа, но сохраним в секрете частный ключ d. Сообщение m, $1 \leqslant m \leqslant N - 1$, трансформируется в шифротекст c, так что

$$1 \leqslant c \leqslant N - 1 \quad \text{и} \quad c = m^e \bmod N.$$

Если m взаимно просто с N (противоположное событие имеет незначительную вероятность), мы может декодировать, поскольку

$$m = m^{de} = c^d \bmod N.$$

В качестве примера атаки гомоморфизмом предположим, что система используется для передачи числа m (долларов, которые нужно заплатить) и некто, знающий об этой операции заменяет шифротекст c на c^2. Тогда

$$(c^2)^d = m^{2de} = m^2$$

и получатель (фальшивого) сообщения считает, что должен заплатить m^2 долларов.

Предположим, что также кодируется и передаётся подпись $B(m)$, где B — сильно немонотонная функция с не простыми алгебраическими свойствами. Тогда атака, описанная выше, будет производить несоответствующие сообщения и подписи, и получатель узнает, что сообщение подменили.

Предположим, что нам известны e, d и N. Так как

$$de - 1 = 0 \bmod (\lambda(N))$$

и $\lambda(N)$ — чётно, $de - 1$ тоже чётно. Значит, $de - 1 = 2^a b$, где b нечётно и $a \geqslant 1$.

Случайным образом выберем x. Положим $z = x^b \bmod N$. По китайской теореме об остатках z является квадратным корнем из 1 по модулю $N = pq$ тогда и только тогда, когда оно является квадратным корнем из единицы по модулям p и q. Так как $\mathbb{F}_p$ — поле, имеем

$$x^2 = 1 \bmod p \leftrightarrow (x-1)(x+1) = 0 \bmod p \leftrightarrow$$
$$\leftrightarrow (x-1) = 0 \bmod p \text{ или } (x+1) = 0 \bmod p.$$

Следовательно, единица имеет 4 квадратных корня w по модулю N, удовлетворяющие условиям $w = \pm 1 \bmod p$ и $w = \pm 1 \bmod q$. Иначе говоря,

$$w = 1 \bmod N, \quad w = -1 \bmod N,$$
$$w = w_1 \bmod N, \quad w_1 = 1 \bmod p \text{ и } w_1 = -1 \bmod q,$$
или
$$w = w_2 \bmod N, \quad w_2 = -1 \bmod p \text{ и } w_2 = 1 \bmod q.$$

Пусть теперь z — квадратный корень из 1 по модулю N, не удовлетворяющий $z = 1 \bmod N$. Если $z = -1 \bmod N$, то нам не повезло и надо повторить попытку. В противном случае мы знаем, что $z + 1 \neq 0 \bmod N$, но делится на один из его простых делителей. С помощью алгоритма Евклида можно найти общий делитель. Зная его несложно найти второй делитель либо простым делением, либо глядя на $z - 1$.

Поскольку квадратные корни из единицы алгебраически неразличимы, вероятность неудачи в этом методе стремится к 0 при увеличении числа попыток. □

Тот, кто пытается генерировать случайные числа детерминированными методами, пребывает, конечно, в состоянии греха.

Джон фон Нейман (1903–1957),
американский математик и программист,
родившийся в Венгрии

§ 4.6. Дополнительные задачи к главе 4

Задача 4.6.1. 1. Пусть $(N_t)_{t\geqslant 0}$ — процесс Пуассона интенсивности λ и $p \in (0, 1)$. Предположим, что каждый скачок в (N_t) имеет тип 1 с вероятностью p и тип 2 с вероятностью $1-p$ независимо от остальных скачков и процесса Пуассона. Пусть $M_t^{(1)}$ — число скачков типа 1 и $M_t^{(2)} = N_t - N_1^{(1)}$ — число скачков типа 2 к моменту времени t. Что можно сказать о совместном распределении пары процессов: $(M_t^{(1)})_{t\geqslant 0}$ и $(M_t^{(2)})_{t\geqslant 0}$? Что произойдёт, если зафиксировав $p_1, \ldots, p_m$ с $p_1 + \ldots + p_m = 1$, мы рассмотрим не два типа, а m?

2. Человек собирает купоны, по одному на каждый момент времени скачка процесса Пуассона $(N_t)_{t\geqslant 0}$ интенсивности λ. Есть m типов купонов, и каждый раз купон типа j получается с вероятностью p_j независимо от ранее собранных купонов и процесса Пуассона. Пусть T — такой момент времени, когда впервые соберётся полный набор типов купонов. Покажите, что

$$\mathsf{P}(T < t) = \prod_{j=1}^{m} (1 - e^{-p_j \lambda t}). \tag{4.6.1}$$

Пусть $L = N_T$ — общее число купонов, собранных к тому моменту, когда получился полный набор типов купонов. Покажите, что $\lambda\,\mathsf{E}T = \mathsf{E}L$. Покажите, что $\mathsf{E}L$ не зависит от λ.

Решение. 1. Непосредственно следует из определения процесса Пуассона.

2. Пусть T_j — момент времени, когда первый раз появился купон типа j. Тогда $T_j \sim \mathrm{Exp}(p_j\lambda)$ независимо от других j. Мы имеем

$$T = \max\{T_1, \ldots, T_m\},$$

и поэтому

$$\mathsf{P}(T < t) = \mathsf{P}(\max\{T_1, \ldots, T_m\} < t) = \prod_{j=1}^{m} \mathsf{P}(T_j < t) = \prod_{j=1}^{m} (1 - e^{-p_j \lambda t}).$$

Далее, заметим, что с. в. L подсчитывает скачки в исходном процессе Пуассона (N_t) до того момента, когда соберутся купоны всех типов, т. е.

$$T = \sum_{i=1}^{L} S_i,$$

где S_1, $S_2 \ldots$ — времена пребывания процесса (N_t) с $S_j \sim \mathrm{Exp}(\lambda)$, с. в. S_j независимы при разных j. Тогда

$$\mathsf{E}(T|L=n) = n\,\mathsf{E}S_1 = n\lambda^{-1}.$$

Более того, L не зависит от с. в. S_1, S_2, … Значит,

$$\mathsf{E}T = \sum_{n \geqslant m} \mathsf{P}(L=n)\,\mathsf{E}(T|L=n) = \mathsf{E}S_1 \sum_{n \geqslant m} n\,\mathsf{P}(L=n) = \lambda^{-1}\,\mathsf{E}L.$$

Но

$$\lambda\,\mathsf{E}T = \lambda \int_0^\infty \mathsf{P}(T>t)dt = \lambda \int_0^\infty \left(1 - \prod_{j=1}^{m}(1-e^{-p_j\lambda t})\right)dt = \int_0^\infty \left(1 - \prod_{j=1}^{m}(1-e^{-p_j t})\right)dt$$

и п. ч. не зависит от λ.

Эквивалентно, L — это число наборов, необходимых для собрания полного комплекта купонов, когда попытки производятся в положительные моменты времени $t = 1, 2, \ldots$ с вероятностью p_j получения купона типа j, вне зависимости от результата предыдущих попыток. В этой конструкции λ не участвует, так что среднее $\mathsf{E}L$ от него не зависит (как, на самом деле, и всё распределение L). □

Задача 4.6.2. Системы массового обслуживания подробно обсуждались в томе 2. Мы иногда будем ссылаться на эту тему, так как она служит богатым источником примеров точечных процессов. Рассмотрим систему из k последовательных очередей, каждая из них имеет бесконечно много обслуживающих приборов. Требования, покинувшие i-ю очередь, $i = 1, \ldots, k-1$, немедленно ставятся в $(i+1)$-ю очередь. Времена прихода в первую очередь образуют процесс Пуассона интенсивности λ. Время обслуживания в i-й очереди не зависит от номера, имеет распределение F, и независимо от времени обслуживания в других очередях, для всех i. Предположим, что первоначально эта система была пустой, и обозначим через $V_i(t)$ число требований в i-й очереди в момент времени $t \geqslant 0$. Покажите, что $V_1(t), \ldots, V_k(t)$ являются независимыми с. в. Пуассона.

В случае $F(t) = 1 - e^{-\mu t}$ покажите, что

$$\mathsf{E}V_i(t) = \frac{\lambda}{\mu}\,\mathsf{P}(N_t \geqslant i), \quad t \geqslant 0, \quad i = 1, \ldots, k, \tag{4.6.2}$$

где $(N_t)_{t\geqslant 0}$ — процесс Пуассона интенсивности μ.

Теперь предположим, что прибытие в первую очередь прекратилось в момент времени T. Найдите среднее число требований в i-й очереди для каждого момента времени $t \geqslant T$.

Решение. Применим теорему о произведении к процессу Пуассона поступления требований со случайным вектором $\mathbf{Y}_n = (S_n^1, \ldots, S_n^k)$, где S_n^i — время обслуживания n-го требования в i-й очереди. Тогда

$$V_i(t) = \text{число требований в } i\text{-й очереди в момент времени } t =$$
$$= \sum_{n=1}^{\infty} \mathbf{1}(\text{в момент } J_n \text{ требование } n \text{ прибывает в первую очередь и находится в } i\text{-й очереди в момент } t) =$$
$$= \sum_{n=1}^{\infty} \mathbf{1}\big(J_n > 0, S_n^1, \ldots, S_n^k \geqslant 0, J_n + S_n^1 + \ldots + S_n^{i-1} < t < J_n + S_n^1 + \ldots + S_n^i\big) =$$
$$= \sum_{n=1}^{\infty} \mathbf{1}\big((J_n, (S_n^1, \ldots, S_m^k)) \in A_i(t)\big) = M(A_i(t)).$$

Здесь $(J_n : n \in \mathbb{N})$ — моменты скачков процесса Пуассона интенсивности λ, а меры M и ν на $(0, \infty) \times \mathbb{R}_+^k$ определяются как

$$M(A) = \sum_{n=1}^{\infty} \mathbf{1}((J_n, Y_n) \in A), \quad A \subset (0, \infty) \times \mathbb{R}_+^k, \qquad \nu((0, t] \times B) = \lambda t \mu(B).$$

Теорема о произведении утверждает, что M — случайная мера Пуассона на $(0, \infty) \times \mathbb{R}_+^k$ с интенсивностью ν. Далее, множество $A_t(T) \subset (0, \infty) \times \mathbb{R}_+^k$ определяется как

$$A_i(t) = \big\{(\tau, s^1, \ldots, s^k) : 0 < \tau < t, \ \ s^1, \ldots, s^k \geqslant 0 \text{ и } \ \tau + s^1 + \ldots + s^{i-1} \leqslant t < \tau + s^1 + \ldots + s^i\big\} =$$
$$= \left\{(\tau, s^1, \ldots, s^k) : 0 < \tau < t, \ \ s^1, \ldots, s^k \geqslant 0 \ \text{ и } \ \sum_{l=1}^{i-1} s^l \leqslant t - \tau < \sum_{l=1}^{i} s^l\right\}.$$

Множества $A_i(t)$ попарно не пересекаются при $i = 1, \ldots, k$ (так как $t - \tau$ может попасть между последовательными частичными суммами $\sum\limits_{l=1}^{i-1} s^i$ и $\sum\limits_{l=1}^{i} s^i$ только один раз). Таким образом, с. в. $V_i(t)$ независимы.

Прямая проверка осуществляется через совместную п. ф. м., а именно, $N_t \sim \mathrm{Po}(\lambda t)$ — число прибытий в первую очередь за время t. Запишем

$$M_{V_1(t),\ldots,V_k(t)}(\theta_1, \ldots, \theta_k) = \mathsf{E}\exp(\theta_1 V_1(t) + \ldots + \theta_k V_k(t)) =$$
$$= \mathsf{E}\left(\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i V_i(t)\Big| N_t; J_1, \ldots, J_{N_t}\right)\right).$$

В свою очередь, при данном $n = 1, 2, \ldots$ и при $0 < \tau_1 < \ldots < \tau_n < t$ условное ожидание равно

$$\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i V_i(t)\Big| N_t = n; J_1 = \tau_1, \ldots, J_n = \tau_n\right) =$$
$$= \mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i \sum_{j=1}^{n}\mathbf{1}\big[(\tau_j, (S_j^1, \ldots, S_j^k)) \in A_i(t)\big]\right) =$$
$$= \mathsf{E}\exp\left(\sum_{i=1}^{k}\sum_{j=1}^{n}\theta_i \mathbf{1}\big[(\tau_j, (S_j^1, \ldots, S_j^k)) \in A_i(t)\big]\right) =$$
$$= \prod_{j=1}^{n}\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i \mathbf{1}\big[(\tau_j, (S_j^1, \ldots, S_j^k)) \in A_i(t)\big]\right).$$

Далее, суммируя по n и интегрируя по $\tau_1, \ldots, \tau_n$, получаем

$$\mathsf{E}\left[\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i V_i(t)\,\Big|\,N_t; J_1, \ldots, J_{N_t}\right)\right] = \sum_{n=1}^{\infty}\lambda^n e^{-\lambda t}\int_0^t\int_0^{\tau_n}\ldots\int_0^{\tau_2}\times$$

$$\times\prod_{j=1}^{n}\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i\mathbf{1}\left[(\tau_j,\,(S_j^1,\ldots,S_j^k))\in A_i(t)\right]\right)d\tau_1\ldots d\tau_{n-1}d\tau_n =$$

$$=\sum_{n=1}^{\infty}\frac{\lambda^n}{n!}e^{-\lambda t}\left(\int_0^t\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i\mathbf{1}\left[(\tau,\,(S_j^1,\ldots,S_j^k))\in A_i(t)\right]\right)dt\right)^n =$$

$$=\exp\left(\lambda\int_0^t\left[\mathsf{E}\exp\left(\sum_{i=1}^{k}\theta_i\mathbf{1}\left[(\tau,\,(S_j^1,\ldots,S_j^k))\in A_i(t)\right]\right)-1\right]d\tau\right) =$$

$$=\exp\left[\lambda\int_0^t\sum_{i=1}^{k}\mathsf{P}((\tau,\,(S^1,\ldots,S^k))\in A_i(t))(e^{\theta_i}-1)d\tau\right] =$$

$$=\prod_{i=1}^{k}\exp\left[(e^{\theta_i}-1)\lambda\int_0^t\mathsf{P}\left(\sum_{l=1}^{i-1}S^l<t-\tau<\sum_{l=1}^{i}S^l\right)d\tau\right].$$

Из единственности с. в. с данной п. ф. м. следует, что

$$V_i(t)\sim\mathrm{Po}\left(\lambda\int_0^t\mathsf{P}\left(\sum_{l=1}^{i-1}S^l<t-\tau<\sum_{l=1}^{i}S^l\right)d\tau\right)\text{ независимо.}$$

Если $F(t)=1-e^{-\mu t}$, частичные суммы $S_1,\ S_1+S_2,\ \ldots$ отмечают последовательные точки процесса Пуассона $\tilde{N}_s$ интенсивности μ. В этом случае $\mathsf{E}V_i(t)=\nu(A_i(t))$ равно

$$\lambda\int_0^t\mathsf{P}\left(\sum_{l=1}^{i-1}S^l<t-\tau<\sum_{l=1}^{i}S^l\right)d\tau=\lambda\int_0^t\mathsf{P}(\tilde{N}_{t-\tau}=i-1)d\tau=$$

$$=\lambda\,\mathsf{E}\int_0^t\mathbf{1}(\tilde{N}_s=i-1)ds=\frac{\lambda}{\mu}\,\mathsf{P}(\tilde{N}_t\geqslant i).$$

Наконец, запишем $V_i(t,\,T)$ для числа требований в очереди i в момент времени t после закрытия входа в момент T. Имеем

$$\mathsf{E}V_i(t,\,T)=\lambda\int_0^T\mathsf{P}(\tilde{N}_{t-\tau}=i-1)d\tau=\lambda\,\mathsf{E}\int_{t-T}^{t}\mathbf{1}(\tilde{N}_s=i-1)ds=$$

$$=\frac{\lambda}{\mu}[\mathsf{P}(\tilde{N}_t\geqslant i)-\mathsf{P}(\tilde{N}_{t-T}\geqslant i)].\quad\square$$

Задача 4.6.3. Времена входа покупателей в супермаркет образуют процесс Пуассона интенсивности λ. Каждый клиент тратит случайный период времени S, набирая покупки, плотность распределения с. в. S для клиентов, прибывающих в момент времени t, — $(f(s,\, t)\colon s \geqslant 0)$. Клиенты ведут себя независимо друг от друга. Для оплаты набранных покупок в кассе нужно время $g(S)$. Политика супермаркета состоит в том, что никто не должен ждать перед кассой, так что кассовые аппараты подключаются по мере необходимости.

Найдите

1) вероятность того, что первый покупатель успеет уйти из супермаркета до того как в него войдёт второй;
2) распределение числа задействованных кассовых аппаратов в момент времени T.

Решение. 1) Если J_1 — время прибытия первого покупателя, то $J_1 + S_1$ — время его подхода к кассе и $J_1 + S_1 + g(S_1)$ — время его выхода из магазина. Пусть J_2 — время входа второго покупателя. Тогда $J_1,\, J_2 - J_1 \sim \mathrm{Exp}(\lambda)$ независимо.

Вероятность $\mathsf{P}(S_1 + g(S_1) < J_2 - J_1)$ равна

$$\int\limits_0^\infty dt_1 \lambda e^{-\lambda t_1} \int\limits_0^\infty dt_2 \lambda e^{-\lambda t_2} \int\limits_0^{t_2} ds_1 f(s_1,\, t_1) \mathbf{1}(s_1 + g(s_1) < t_2) =$$

$$= \int\limits_0^\infty dt_1 \lambda e^{-\lambda t_1} \int\limits_0^\infty ds_1 f(s_1,\, t_1) \int\limits_{s_1 + g(s_1)}^\infty dt_2 \lambda e^{-\lambda t_2} =$$

$$= \int\limits_0^\infty dt_1 \lambda e^{-\lambda t_1} \int\limits_0^\infty ds_1 f(s_1,\, t_1) e^{-\lambda(s_1 + g(s_1))}.$$

2) Пусть N_T^{ch} — число касс, задействованных в момент времени T. По теореме о произведении 4.4.11 получаем, что $N_T^{\mathrm{ch}} \sim \mathrm{Po}(\Lambda(T))$, где

$$\Lambda(T) = \lambda \int\limits_0^{\mathrm{T}} du \int\limits_0^\infty ds f(s,\, u) \mathbf{1}(u + s < T,\, u + s + g(s) > T) =$$

$$= \lambda \int\limits_0^{\mathrm{T}} du \int\limits_0^\infty ds f(s,\, u) \mathbf{1}(T - g(s) < u + s < T).$$

Действительно, если $N_T^{\mathrm{arr}} \sim \mathrm{Po}(\lambda T)$ — число вошедших покупателей к моменту T, то

$$N_T^{\mathrm{ch}} = \sum_{i=1}^{N_T^{\mathrm{arr}}} \mathbf{1}(J_i + S_i < T < J_i + S_i + g(S_i))$$

и п. ф. м. имеет вид

$$\mathsf{E}\exp(\theta N_T^{\mathrm{ch}}) = \mathsf{E}(\mathsf{E}(\theta N_T^{\mathrm{ch}}) \mid N_T^{\mathrm{arr}};\, J_1,\, \ldots,\, J_{N_T^{\mathrm{arr}}})) =$$

$$= e^{-\lambda T} \sum_{k=0}^{\infty} \lambda^k \int_0^T \int_0^{t_k} \ldots \int_0^{t_2} \prod_{i=1}^{k} \mathsf{E}\exp(\theta\, \mathbf{1}(t_i + S_i < T < t_i + S_i + g(S_i)))dt_1 \ldots dt_k =$$

$$= e^{-\lambda T} \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} \int_0^T \ldots \int_0^T \prod_{i=1}^{k} \mathsf{E}\exp(\theta\, \mathbf{1}(t_i + S_i < T < t_i + S_i + g(S_i)))dt_1 \ldots dt_k =$$

$$= e^{-\lambda T} \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} \left(\int_0^T \mathsf{E}\exp(\theta\, \mathbf{1}(t + S < T < t + S + g(S)))\right)^k =$$

$$= \exp\left(\lambda \int_0^T \mathsf{E}(\exp(\theta\, \mathbf{1}(t + S < T < t + S + g(S))) - 1)dt \right) =$$

$$= \exp\left(\lambda(e^\theta - 1) \int_0^T \mathsf{P}(u + s < T < u + s + g(s))dt \right) =$$

$$= \exp\left(\lambda(e^\theta - 1) \int_0^T \int_0^\infty f(s,\, u)\mathbf{1}(u + s < T < u + s + g(s))ds\, du \right),$$

что доказывает утверждение. □

Задача 4.6.4. Библиотека открыта с 9 утра до 5 вечера. Ни один студент не может войти туда после 5 вечера; студент, уже находящийся в библиотеке, может остаться там и после 5 вечера. Студенты приходят в библиотеку в период с 9 утра до 5 вечера в соответствии с процессом Пуассона интенсивности λ. Каждый студент проводит в библиотеке случайный промежуток времени: H часов, где $0 \leqslant H \leqslant 8$ — с. в. с п. р. h и $\mathsf{E}[H] = 1$. Периоды пребывания различных студентов в библиотеке — н. о. р. с. в.

1. Найдите распределение числа студентов, покинувших библиотеку между 3 и 4 часами.

2. Докажите, что среднее число студентов, покинувших библиотеку между 3 и 4 часами, равно $\mathsf{E}[\min[1, (7 - H)_+]]$, где w_+ обозначает $\max\{w, 0\}$.

3. Что можно сказать о числе студентов, остающихся в библиотеке после закрытия?

Решение. Библиотека открыта с 9 утра до 5 вечера. Студенты приходят туда в соответствие с законом $\mathrm{P}\,\mathrm{P}(\lambda)$. Задача эквивалентна очереди $M/GI/\infty$ (до 5 часов вечера, когда наступает запрет на вход, но для задач,

включающих более ранние времена, это неважно).

$J_n =$ время прихода n-го студента по 24-часовым часам;

$H_n =$ время пребывания n-го студента в библиотеке.

Используем вновь теорему о произведении 4.4.11 для случайной меры на $(0, 8) \times (0, 8)$ с атомами (J_n, H_n), где $(J_n : n \in \mathbb{N})$ — время прихода и $(H_n : n \in \mathbb{N})$ — время пребывания студента в библиотеке. Определим меру на $(0, \infty) \times \mathbb{R}_+$ по правилу $\mu((0, t) \times B) = \lambda t \mu(B)$, $N(A) = \sum_n \mathbf{1}_{((J_n, H_n) \in A)}$. Тогда N — случайная мера Пуассона интенсивности $\nu([0, t] \times [0, y]) = \lambda t F(y)$, где $F(y) = \int_0^y h(x)dx$ ($t = 0$ соответствует 9 часам утра).

1. Далее, число студентов, покинувших библиотеку между 3 и 4 часами (т. е. $6 \leqslant t \leqslant 7$) имеет распределение Пуассона $\mathrm{Po}(\nu(A))$, где

$$A = \{(r, s) : s \in [0, 7], r \in [6 - s, 7 - s], \text{ если } s \leqslant 6; r \in [0, 7 - s], \text{ если } s > 6\}.$$

Здесь

$$\nu(A) = \int_0^8 \lambda dF(r) \int_{(6-r)_+}^{(7-r)_+} ds = \int_0^8 \lambda [(7 - r)_+ - (6 - r)_+] dF(r).$$

Итак, число студентов, покинувших библиотеку между 3 и 4, имеет распределение Пуассона интенсивности $\lambda \int_0^7 [(7 - r)_+ - (6 - r)_+] dF(r)$.

2. Имеем

$$(7 - r)_+ - (6 - r)_+ = \begin{cases} 0, & \text{если } y \geqslant 7, \\ 7 - y, & \text{если } 6 \leqslant y \leqslant 7, \\ 1, & \text{если } y \leqslant 6. \end{cases}$$

Среднее число студентов, покинувших библиотеку между 3 и 4 часами, равно

$$\nu(A) = \int_0^8 \lambda \min[1, (7 - r)_+] dF(r) = \lambda \mathsf{E}(\min[1, (7 - H)_+]),$$

что и требовалось.

3. Для студентов, остающихся в библиотеке после закрытия, мы потребуем, чтобы выполнялось неравенство $J + H \geqslant 8$ при H, пробегающем отрезок $[0, 8]$, и J, меняющемся от $8 - H$ до 8. Пусть

$$B = \{(t, x) : t \in [0, 8], x \in [8 - t, 8]\}.$$

Тогда

$$\nu(B) = \lambda \int_0^8 dt \int_{8-t}^8 dF(x) = \lambda \int_0^8 dF(x) \int_0^{8-x} dt =$$

$$= \lambda \int_0^8 (8-x)\, dF(x) = 8\lambda \int_0^8 dF(x) - \lambda \int_0^8 x\, dF(x).$$

Но $\int_0^8 dF(x) = 1$ и $\int_0^8 x\, dF(x) = \mathsf{E}H = 1$, откуда $\lambda\, \mathsf{E}H = \lambda$. Следовательно, среднее число студентов в библиотеке после закрытия — 7λ. □

Задача 4.6.5. 1. Докажите теорему Кэмпбелла, т. е. покажите, что если M — случайная мера Пуассона интенсивности μ на пространстве состояний E и $a\colon E \to \mathbb{R}$ — ограниченная измеримая функция, то

$$\mathsf{E}[e^{\theta X}] = \exp\left(\int_E (e^{\theta a(y)} - 1)\mu(dy) \right), \tag{4.6.3}$$

где $X = \int_E a(y) M(dy)$ (предполагаем, что $\lambda = \mu(E) < \infty$).

2. Выстрелы раздаются во времена скачков $J_1, J_2, \ldots$ процесса Пуассона со интенсивностью λ. Начальные амплитуды шума выстрелов $A_1, A_2, \ldots \sim \mathrm{Exp}(2)$ — н. о. р. с. в. с экспоненциальным распределением с параметром 2, а затухают амплитуды линейно со скоростью α. Вычислите п. ф. м. полной амплитуды X в момент времени t, где

$$X_t = \sum_n A_n (1 - \alpha(t - J_n)_+) \mathbf{1}_{(J_n \leqslant t)}$$

($x_+ = x$, если $x \geqslant 0$, и 0 в противном случае).

Решение. 1. При условии $M(E) = n$ атомы M образуют случайные отсчёты $Y_1, \ldots, Y_n$ с распределением $\frac{1}{\lambda}\mu$, так что

$$\mathsf{E}[e^{\theta X} \mid M(E) = n] = \mathsf{E}\left[\exp\left(\theta \sum_{k=1}^n a(Y_k) \right) \right] = \left(\int_E e^{\theta a(y)} \mu(dy)/\lambda \right)^n.$$

Следовательно,

$$\mathsf{E}\left[e^{\theta X}\right] = \sum_n \mathsf{E}\left[e^{\theta X} \mid M(E) = n\right] \mathsf{P}(M(E) = n) =$$

$$= \sum_n \left(\int_E e^{\theta a(y)} \mu(dy)/\lambda \right)^n \frac{e^{-\lambda} \lambda^n}{n!} = \exp\left(\int_E (e^{\theta a(y)} - 1)\mu(dy) \right).$$

2. Фиксируем t, и пусть $E = [0, t] \times \mathbb{R}^+$, а ν и V таковы, что $\nu(ds, dx) = 2\lambda e^{-2x} ds dx$, $M(B) = \sum\limits_n \mathbf{1}_{\{(J_n, A_n) \in B\}}$. По теореме о произведении M — случайная мера Пуассона интенсивности ν. Положим $a_t(s, x) = x(1 - \alpha(t - s))_+$, тогда $X_t = \int_E a_t(s, x) M(ds, dx)$, так что по теореме Кэмпбелла для $\theta < 2$ получаем, что

$$\mathsf{E}\left[e^{\theta X}\right] = \exp\left(\int\limits_E (e^{\theta a_t(s,x)} - 1)\nu(ds, dx)\right) =$$

$$= e^{-\lambda t} \exp\left(2\lambda \int\limits_0^t \int\limits_0^\infty e^{-x(2-\theta(1-\alpha(t-s))_+)} dx\, ds\right) =$$

$$= e^{-\lambda t} \exp\left(2\lambda \int\limits_0^t ds \frac{1}{2 - \theta(1 - \alpha(t-s))_+}\right) =$$

$$= e^{-\lambda \min[t, 1/\alpha]} \left(\frac{2 - \theta + \theta\alpha \min[t, 1/\alpha]}{2 - \theta}\right)^{\frac{2\lambda}{\theta\alpha}},$$

используя расщепление интеграла $\int\limits_0^t = \int\limits_0^{t - \frac{1}{\alpha}} + \int\limits_{t - \frac{1}{\alpha}}^t$ в случае $t > \dfrac{1}{\alpha}$. □

Задача 4.6.6. Семена сажают в поле $S \subset \mathbb{R}^2$ случайным образом так, что они образуют процесс Пуассона на S интенсивности $\lambda(x, y)$. Из семян вырастают растения, которые позже собирают как урожай, и масса урожая, собранного в точке (x, y), имеет математическое ожидание $m(x, y)$ и дисперсию $v(x, y)$. Массы различных растений — независимые с. в. Покажите, что общий вес W всех растений является с. в. с конечным средним

$$I_1 = \iint\limits_S m(x, y)\lambda(x, y) dx\, dy$$

и дисперсией

$$I_2 = \iint\limits_S \{m(x, y)^2 + v(x, y)\}\lambda(x, y) dx\, dy,$$

если эти интегралы конечны.

Решение. Предположим сначала, что

$$\mu = \int\limits_S \lambda(x, y) dx\, dy$$

конечно. Тогда число N растений конечно и распределено по закону $\mathrm{Po}(\mu)$. Предположим, что N и положения растений — независимые с. в.

$(X_n, Y_n, n = 1, \ldots, N)$ с плотностью λ/μ на S. Тогда веса отдельных растений не зависят друг от друга,

$$\mathsf{E}\, W_n = \int\limits_S m(x, y)\lambda(x, y)\mu^{-1} dx\, dy = \mu^{-1} I_1$$

и

$$\mathsf{E}\, W_n^2 = \int\limits_S [m(x, y)^2 + v(x, y)]\lambda(x, y)\mu^{-1} dx\, dy = \mu^{-1} I_2,$$

где I_1 и I_2 конечны. Значит,

$$\mathsf{E}(W|N) = \sum_{n=1}^{N} \mu^{-1} I_1 = N\mu^{-1} I_1$$

и

$$\mathrm{Var}[W|N] = \sum_{n=1}^{N} (\mu^{-1} I_2 - \mu^{-2} I_1^2) = N(\mu^{-1} I_2 - \mu^{-2} I_1^2).$$

Тогда

$$\mathsf{E}\, W = \mathsf{E} N\mu^{-1} I_1 = I_1$$

и

$$\mathrm{Var}[W] = \mathsf{E}[\mathrm{Var}[W|N]] + \mathrm{Var}[\mathsf{E}(W|N)] =$$
$$= \mu(\mu^{-1} I_2 - \mu^{-2} I_1^2) + (\mathrm{Var}[N])\mu^{-2} I_1^2 = I_2,$$

что и требовалось.

Если $\mu = \infty$, мы разобьём S на непересекающиеся множества S_k, на которых функция λ интегрируема, и запишем $W = \sum\limits_k W_{(k)}$, где веса $W_{(k)}$ урожая на S_k независимы, и получим

$$\mathsf{E}\, W = \sum_k \mathsf{E}\, W_{(k)} = \sum_k \int\limits_{S_k} m(x, y)\lambda(x, y) dx\, dy = \int\limits_S m(x, y)\lambda(x, y) dx\, dy$$

и аналогично для $\mathrm{Var}[W]$. □

Я иду среди полей...

Джон Китс (1795–1821),
английский поэт

Задача 4.6.7. Прямую L на плоскости $\mathbb{R}^2$, не проходящую через начало координат O, можно задать, указав расстояние $p > 0$ от неё до O (по перпендикулярному направлению) и угол $\theta \in [0, 2\pi)$, который образует с осью x перпендикуляр, идущий из O к L. Аккуратно объясните, что подразумевается под процессом Пуассона таких прямых L.

Процесс Пуассона Π прямых L обладает средней мерой μ, определяемой формулой

$$\mu(B) = \iint\limits_B dpd\theta \tag{4.6.4}$$

для $B \subseteq (0, \infty) \times [0, 2\pi)$. Случайное счётное множество $\Phi \subset \mathbb{R}^2$ определяется как множество всех точек пересечения пар прямых из Π. Покажите, что вероятность того, что существует по крайней мере одна точка из Φ, лежащая внутри круга D с центром в O и радиусом r, меньше чем

$$1 - (1 + 2\pi r)e^{-2\pi r}.$$

Является ли Φ процессом Пуассона?

Решение. Пусть μ — мера на пространстве $\mathcal{L}$ прямых в $\mathbb{R}^2$, не проходящих через O. Процесс Пуассона со средней мерой μ — это такое случайное счётное подмножество $\Pi \subset \mathcal{L}$, что

1) число $N(A)$ точек из Π в измеримом подмножестве $A \subset \mathcal{L}$ имеет распределение $\mathrm{Po}(\mu(A))$ и

2) для непересекающихся подмножеств $A_1, \ldots, A_n$ с. в. $N(A_j)$ независимы.

В нашем примере число N прямых, которые пересекают круг D с центром в нуле и радиусом r, совпадает с числом прямых, для которых $p < r$. Оно имеет распределение Пуассона со средним

$$\int\limits_0^r \int\limits_0^{2\pi} dpd\theta = 2\pi r.$$

Если в пересечении $\Phi \cap D$ есть по крайней мере одна точка, то круг D должны пересекать хотя бы две прямые из Π, и вероятность такого события равна

$$\sum_{n \geqslant 2} \frac{(2\pi r)^n}{n!} e^{-2\pi r} = 1 - (1 + 2\pi r)e^{-2\pi r}.$$

Вероятность того, что точка из Φ лежит в D, строго меньше, чем эта, поскольку могут найтись две прямые, пересекающие D, общая точка которых лежит вне D.

Наконец, Φ не является процессом Пуассона, поскольку в нём с положительной вероятностью могут быть коллинеарные точки. □

Задача 4.6.8. Ниже приводится определение распределения Пуассона—Дирихле для случайной последовательности $(p_1, p_2, \ldots, p_n, \ldots)$,

$\sum_{i=1}^{\infty} p_i = 1$, $p_i \geqslant 0$. Его частный случай уже появлялся в томе 2. Покажите, что для любого многочлена φ, где $\varphi(0) = 0$, имеет место соотношение

$$\mathsf{E}\left\{\sum_{n=1}^{\infty} \varphi(p_n)\right\} = \theta \int_0^1 \varphi(x) x^{-1}(1-x)^{\theta-1} dx. \tag{4.6.5}$$

Что вам это говорит о распределении p_1?

Решение. Самый простой способ определить распределение Пуассона—Дирихле — это сказать, что (p_n) имеет то же распределение, что и ξ_n/σ, где $\{\xi_n,\ n = 1, 2, \ldots\}$ — точки процесса Пуассона на $(0, \infty)$ интенсивности $\theta x^{-1} e^{-x}$, записанные в убывающем порядке, и $\sigma = \sum_{n \geqslant 1} \xi_n$. По теореме Кэмпбелла σ почти всегда конечно, имеет распределение $\mathrm{Gam}(\theta)$ (где $\theta > 0$ может быть любым) и не зависит от вектора $\mathbf{p} = (p_1, p_2, \ldots)$ с

$$p_1 \geqslant p_2 \geqslant \ldots, \quad \sum_{n \geqslant 1} p_n = 1 \text{ с вероятностью один.}$$

Для доказательства равенства (4.6.5) мы можем взять $p_n = \xi_n/\sigma$ и воспользоваться тем, что σ и (p_n) независимы. Для $k \geqslant 1$ имеем

$$\mathsf{E}\left(\sum_{n \geqslant 1} \xi_n^k\right) = \int_0^{\infty} x^k \theta x^{-1} e^{-x} dx = \theta \Gamma(k).$$

Л. ч. равна

$$\mathsf{E}\left(\sigma^k \sum_{n \geqslant 1} p_n^k\right) = \Gamma(\theta + k)\Gamma(\theta)^{-1}\, \mathsf{E}\left(\sum_{n \geqslant 1} p_n^k\right).$$

Значит,

$$\mathsf{E}\left(\sum_{n \geqslant 1} p_n^k\right) = \frac{\theta \Gamma(k)\Gamma(\theta)}{\Gamma(k+\theta)} = \theta \int_0^1 x^{k-1}(1-x)^{\theta-1} dx.$$

Мы видим, что тождество (4.6.5) выполнено для $\varphi(x) = x^k$ $(k \geqslant 1)$ и, следовательно, по линейности для всех таких многочленов φ, что $\varphi(0) = 0$.

Аппроксимируя ступенчатые функции многочленами, получаем, что среднее число точек p_n на интервале (a, b) $(0 < a < b < 1)$ равно

$$\theta \int_a^b x^{-1}(1-x)^{\theta-1} dx.$$

Если $a > 1/2$, то может найтись не более одного такого p_n, так что п. р. у p_1 имеет вид

$$\theta x^{-1}(1-x)^{\theta-1} \quad (1/2,\ 1).$$

Но это не так на $(0,\ 1/2)$, и тождество (4.6.5) не определяет распределение p_1 на этом интервале. □

Задача 4.6.9. Положения деревьев в большом лесу можно моделировать как процесс Пуассона Π постоянной интенсивности λ на $\mathbb{R}^2$. Каждое дерево производит случайное число семян, имеющих распределение Пуассона со средним 1. Семена, падая на землю, попадают в точки, равномерно распределённые по окружности радиуса r, центр которой находится под деревом. Положения различных семян относительно их родительского дерева и количество семян, производимых данным деревом, независимыми друг от друга и от Π. Докажите, что в зависимости от Π, семена образуют процесс Пуассона Π^*, средняя мера которого зависит от Π. Является ли безусловное распределение Π^* процессом Пуассона?

Решение. Прямым вычислением убеждаемся, что семена дерева образуют процесс Пуассона интенсивности

$$\rho_X(x) = \begin{cases} \pi^{-1} r^{-2}, & |x - X| < r, \\ 0 & \text{иначе.} \end{cases}$$

Суперпозиция этих независимых процессов Пуассона даёт процесс Пуассона интенсивности

$$\Lambda_\Pi(x) = \sum_{X \in \Pi} \rho_X(x),$$

очевидно, зависит от Π. Нереалистичное предположение о круговом равномерном распределении мы выбрали, чтобы не возникало сомнений относительно этой зависимости — в этом случае процесс Π может быть реконструирован из очертаний Λ_Π.

Здесь мы впервые встретились с процессом Кокса, или дважды стохастическим процессом (Cox process), т. е. процессом Пуассона случайной интенсивности. Число семян в ограниченном множестве Λ имеет среднее

$$\mathsf{E} N(A) = \mathsf{E}\,\mathsf{E}[N(A)|\Pi] = \mathsf{E} \int\limits_A \Lambda_\Pi(x)dx$$

и дисперсию

$$\operatorname{Var}[N(A)] = \mathsf{E}(\operatorname{Var}[N(A)|\Pi]) + \operatorname{Var}[\mathsf{E}(N(A)|\Pi)] = \\ = \mathsf{E} N(A) + \operatorname{Var}\Big[\int \Lambda_\Pi(x)dx\Big] > \mathsf{E} N(A).$$

Следовательно, Π^* не является процессом Пуассона. □

Задача 4.6.10. Равномерный процесс Пуассона Π на единичном шаре в $\mathbb{R}^3$ задается тем, что его интенсивность — это мера Лебега (объём) на

$$B = \big\{(x,\ y,\ z) \in \mathbb{R}^3 \colon r^2 = x^2 + y^2 + z^2 \leqslant 1\big\}.$$

Покажите, что

$$\Pi_1 = \{r\colon (x,\, y,\, z) \in \Pi\}$$

является процессом Пуассона на $[0,\, 1]$, и найдите его среднюю меру. Покажите, что

$$\Pi_2 = \big\{(x/r,\, y/r,\, z/r)\colon (x,\, y,\, z) \in \Pi\big\}$$

является процессом Пуассона на границе множества B, средняя мера которого пропорциональна площади поверхности. Зависимы ли процессы Π_1 и Π_2?

Решение. По теореме 4.4.3 об отображении Π_1 является процессом Пуассона со средним числом точек на $(a,\, b)$ равным $\lambda\times$ (объём сферического кольца радиусов a и b), т. е.

$$\lambda\Big(\frac{4}{3}\pi b^3 - \frac{4}{3}\pi a^3\Big).$$

Таким образом, п. р. средней меры Π_1 имеет вид

$$4\lambda\pi r^2 \quad (0 < r < 1).$$

Аналогично среднее число точек процесса Π_2 в $A \subseteq \partial B$ равно

$$\lambda \times (\text{конический объём от } 0 \text{ до } A) = \frac{1}{3}\lambda \times (\text{площадь поверхности } A).$$

Наконец, Π_1 и Π_2 не являются независимыми, поскольку у них одинаковое число точек. □

Задача 4.6.11. Точки процесса Π случайно раскрасили красным и зелёным цветом. Вероятность того, что данную точку покрасили красным, равна r $(0 < r < 1)$, а цвета различных точек независимы. Покажите, что красные и зелёные точки образуют независимые процессы Пуассона.

Решение. Если $\mu(A) < \infty$ — мера множества $A \subset \mathbb{R}^d$, то запишем

$$N(A) = N_1(A) + N_2(A),$$

где N_1 и N_2 — количества красных и зелёных точек. При условии $N(A) = n$ число $N_1(A)$ имеет биномиальное распределение $\mathrm{Bin}(n,\, r)$, так что

$$\begin{aligned}\mathsf{P}(N_1(A) = k,\, N_2(A) = l) &= \mathsf{P}(N(A) = k + l)\,\mathsf{P}(N_1(A) = k \,|\, N(A) = k + l) = \\ &= \frac{\mu(A)^{k+l}e^{-\mu(A)}}{(k+l)!}C^k_{k+l}r^k(1-r)^l = \frac{[r\mu(A)]^k e^{-r\mu(A)}}{k!}\,\frac{[(1-r)\mu(A)]^l e^{-(1-r)\mu(A)}}{l!}\end{aligned}$$

Здесь $N_1(A)$ и $N_2(A)$ — независимые $\mathrm{Po}(r\mu(A))$ и $\mathrm{Po}((1-r)\mu(A))$ с. в. соответственно.

Если $A_1,\, A_2,\, \ldots$ — непересекающиеся множества, то пары

$$(N_1(A_1),\, N_2(A_1)),\ \ (N_1(A_2),\, N_2(A_2)),\, \ldots$$

независимы, и поэтому

$$(N_1(A_1),\, N_1(A_2),\, \ldots) \quad \text{и} \quad (N_2(A_1),\, N_2(A_2),\, \ldots)$$

— две независимые последовательности независимых с. в. Если $\mu(A) = \infty$, то почти всюду $N(A) = \infty$ и, поскольку $r > 0$ и $1 - r > 0$, почти наверное существует бесконечно много красных и зелёных точек в A. □

Задача 4.6.12. В модели дождя, падающего на поверхность (считаем, что на плоскость $\mathbb{R}^2$), каждая капля описывается тройкой $(X,\, T,\, V)$, где $X \in \mathbb{R}^2$ — это горизонтальное смещение центра падения, T — тот миг, когда капля попадает на плоскость, и V — объём воды в капле. Предполагается, что точки $(X,\, T,\, V)$, образуют процесс Пуассона на $\mathbb{R}^4$ с заданной плотностью $\lambda(x,\, t,\, v)$. Упавшая капля — это мокрое круглое пятно на поверхности с центром в точке X и постепенно увеличивающимся радиусом: в момент времени $T + t$ радиус — определяется функцией $r(t,\, V)$. Найдите вероятность того, что точка $\xi \in \mathbb{R}^2$ будет сухой в момент τ, и покажите, что ожидаемое общее количество осадков

$$\int\limits_{\mathbb{R}^4} v\lambda(x,\, t,\, v)dx\, dt\, dv,$$

если интеграл сходится.

Решение. Итак, точка $\xi \in \mathbb{R}^2$ мокрая тогда и только тогда, когда найдётся такая точка из $X \in \Pi$ с $t < \tau$, что

$$\|X - \xi\| < r(\tau - t,\, V).$$

(не имеет значения, строгое или нестрогое неравенство, так как разница состоит из множества нулевой вероятности). Число точек из Π, удовлетворяющих этим двум неравенствам, является пуассоновым со средним

$$\mu = \int \lambda(x,\, t,\, v)\mathbf{1}(t < \tau,\, \|x - \xi\| < r(t - \tau,\, v))dx\, dt\, dv.$$

Значит, вероятность того, что точка ξ остаётся сухой, равна $e^{-\mu}$ (или 0, если $\mu = \infty$).

Наконец, формула для ожидаемого общего числа осадков

$$\sum_{(X,T,V)\in\Pi} V$$

получается непосредственно из теоремы Кэмпбелла. □

Задача 4.6.13. Пусть M — случайная мера Пуассона на $E = \mathbb{R} \times [0,\, \pi)$ постоянной интенсивности λ. Для точки $(x,\, \theta) \in E$ обозначим через $l(x,\, \theta)$ прямую на $\mathbb{R}^2$, полученную поворотом прямой $\{(x,\, y)\colon y \in \mathbb{R}\}$ на угол θ вокруг начала координат.

Рассмотрим процесс прямых $L = M \circ l^{-1}$.

1) Какое распределение имеет число прямых, пересекающих диск $D_a = \{z \in \mathbb{R}^2 : |z| \leqslant a\}$?

2) Как распределено расстояние от начала координат до ближайшей прямой?

3) Как распределено расстояние от начала координат до k-й ближайшей прямой?

Решение. 1) Прямая пересекает диск $D_a = \{z \in \mathbb{R}^2 : |z| \leqslant a\}$ тогда и только тогда, когда представляющая её точка (x, θ) попала на $(-a, a) \times [0, \pi)$. Следовательно,

$$\text{число прямых, пересекающих } D_a \sim \mathrm{Po}(2a\pi\lambda).$$

2) Обозначим через Y расстояние от начала координат до ближайшей прямой. Тогда

$$\mathsf{P}(Y \geqslant a) = \mathsf{P}(M((-a, a) \times [0, \pi)) = 0) = \exp(-2a\lambda\pi),$$

т. е. $Y \sim \mathrm{Exp}(2\pi\lambda)$.

3) Пусть $Y_1, Y_2, \ldots$ — расстояния от начала координат до ближайшей прямой, второй ближайшей прямой и т. д. Тогда Y_i — атомы случайной меры Пуассона N на $\mathbb{R}_+$, которая получается из M проекцией $(x, \theta) \mapsto |x|$. По теореме об отображении N является процессом Пуассона на $\mathbb{R}_+$ интенсивности $2\pi\lambda$. Значит, $Y_k \sim \mathrm{Gam}(k, 2\pi\lambda)$, так как $Y_k = S_1 + \ldots + S_k$, где $S_i \sim \mathrm{Exp}(2\pi\lambda)$ независимы. □

Задача 4.6.14. Рассмотрим точечный процесс $\tilde{N}(t)$ на $\mathbf{R}_+$, образованный точками пуассоновского процесса $N(t)$ интенсивности λ с четными номерами. Вычислите среднее значение и дисперсию $\tilde{N}(t)$.

Решение. Используя тождество

$$\tilde{N}(t) = \left\lfloor \frac{N(t)}{2} \right\rfloor = \frac{N(t)}{2} - \frac{1}{2}\mathbf{1}(N(t) \text{ нечетно}),$$

получаем

$$\mathbf{E}[\tilde{N}(t)] = \frac{\lambda t}{2} - \frac{1}{4}e^{-\lambda t}(e^{\lambda t} - e^{-\lambda t}) = \frac{\lambda t}{2} - \frac{1}{4}(1 - e^{-2\lambda t}).$$

Далее,

$$\mathbf{E}[\tilde{N}(t)]^2 = \frac{1}{4}\mathbf{E}[N(t)]^2 - \frac{1}{2}\mathbf{E}[N(t)\mathbf{1}(N(t) \text{ нечетно})] + \frac{1}{4}\mathbf{E}\mathbf{1}(N(t) \text{ нечетно}).$$

Итак, мы получаем

$$\frac{1}{4}\mathbf{E}\,[N(t)]^2 = \frac{\lambda t}{4} + \frac{\lambda^2 t^2}{4},$$

$$\frac{1}{4}\mathbf{E}\mathbf{1}(N(t) \text{ нечетно}) = \frac{1}{8}(1 - e^{-2\lambda t}).$$

Далее,

$$\frac{1}{2}\mathbf{E}\left[N(t)\mathbf{1}(N(t)\text{ нечетно})\right] = \frac{1}{2}e^{-\lambda t}\sum_{n\text{ нечетно}} n\times\frac{(\lambda t)^n}{n!} = \\ = \frac{\lambda t}{2}e^{-\lambda t}\sum_{n\text{ четно}}\frac{(\lambda t)^n}{n!} = \frac{\lambda t}{4}(1+e^{-2\lambda t}).$$

Итак,

$$\mathrm{Var}\left[\tilde{N}(t)\right] = \frac{\lambda t}{4}+\frac{\lambda^2 t^2}{4}-\frac{\lambda t}{4}(1+e^{-2\lambda t})+\frac{1}{8}(1-e^{-2\lambda t})- \\ -\left(\frac{\lambda t}{2}-\frac{1}{4}(1-e^{-2\lambda t})\right)^2 = \frac{\lambda t}{4}+\frac{1}{16}-\frac{1}{16}e^{-4\lambda t}-\frac{\lambda t}{2}e^{-2\lambda t}. \quad \square$$

Задача 4.6.15. Требуется передать одно из M равновероятных различных сообщений через зашумлённый канал. Кодируем j-е сообщение последовательностью скаляров a_{jt} $(t = 1, 2, \ldots, n)$, которые после передачи принимаются как $a_{jt}+\varepsilon_t$ $(t = 1, 2, \ldots, n)$. Здесь с. в. шума ε_t независимы и нормально распределены с нулевым средним и зависящей от времени дисперсией $\mathrm{Var}[\varepsilon_t] = v_t$.

Найдите правило вывода получателя, при котором средняя вероятность того, что сообщение будет неверно определено, ограничена сверху:

$$\mathsf{P}(\text{ошибка}) \leqslant \frac{1}{M}\sum_{1\leqslant j\neq k\leqslant M}\exp(-d_{j,k}/8), \tag{4.6.6}$$

где

$$d_{jk} = \sum_{t=1}^{n}(a_{jt}-a_{kt})^2/v_t.$$

Предположим, что $M = 2$ и что форма волны передатчика подчиняется ограничению по мощности $\sum_{t=1}^{n} a_{jt}^2 \leqslant K$ $(j = 1, 2)$. Как выбрать две формы волны, минимизирующие вероятность ошибки?

Указание. Можно использовать неравенство $\mathsf{P}(Z \geqslant a) \leqslant \exp(-a^2/2)$, где Z — стандартная с. в., распределённая по закону $\mathrm{N}(0, 1)$.

Решение. Пусть $f_j = f_{\mathrm{ch}}(\mathbf{y}|X = (\mathbf{a})_j)$ — п. р. полученного вектора $\mathbf{y}$, если передавалась «форма волны» $(\mathbf{a})_j = (a_{jt})$. Тогда

$$\mathsf{P}(\text{ошибка}) \leqslant \frac{1}{M}\sum_{j}\sum_{k:\,k\neq j}\mathsf{P}(\mathbf{y}\colon f_k(\mathbf{y}) \geqslant f_j(\mathbf{y})|X = (\mathbf{a})_j).$$

В этом случае

$$f_j = C\exp\left(-\frac{1}{2}\sum_{t=1}^{n}(y_t - a_{jt})^2/v_t\right) = C\exp\left(-\frac{1}{2}(Y-(\mathbf{a})_j)^{\mathrm{T}}V^{-1}(Y-(\mathbf{a})_j)\right).$$

Тогда, если $X = (\mathbf{a})_j$ и $Y = (\mathbf{a})_j + \varepsilon$, то мы имеем

$$\log f_k - \log f_j = -\frac{1}{2}((\mathbf{a})_j - (\mathbf{a})_k + \varepsilon)^{\mathrm{T}}V^{-1}((\mathbf{a})_j - (\mathbf{a})_k + \varepsilon) + \frac{1}{2}\varepsilon^{\mathrm{T}}V^{-1}\varepsilon =$$
$$= -\frac{1}{2}d_{jk} - ((\mathbf{a})_j - (\mathbf{a})_k)^{\mathrm{T}}V^{-1}\varepsilon = -\frac{1}{2}d_{jk} + \sqrt{d_{jk}}Z,$$

где $Z \sim \mathrm{N}(0,\,1)$. Воспользовавшись указанием, из формулы (4.6.6) получаем, что

$$\mathsf{P}(f_k \geqslant f_j) = \mathsf{P}(Z > \sqrt{d_{jk}}/2) \leqslant e^{-d_{jk}/8}.$$

В случае $M = 2$ нам следует максимизировать

$$d_{12} = ((\mathbf{a})_1 - (\mathbf{a})_2)^{\mathrm{T}}V^{-1}((\mathbf{a})_1 - (\mathbf{a})_2) = \sum_{t=1}^{n}(a_{1t} - a_{2t})^2/v_t$$

при условии

$$\sum_t a_{jt}^2 \leqslant K, \quad \text{или} \quad (\mathbf{a})_j^{\mathrm{T}}(\mathbf{a})_j \leqslant K, \quad j = 1,\,2.$$

По неравенству Коши—Шварца имеем

$$((\mathbf{a})_1 - (\mathbf{a})_2)^{\mathrm{T}}V^{-1}((\mathbf{a})_1 - (\mathbf{a})_2) \leqslant \left(\sqrt{(\mathbf{a})_1^{\mathrm{T}}V^{-1}(\mathbf{a})_1} + \sqrt{(\mathbf{a})_2^{\mathrm{T}}V^{-1}(\mathbf{a})_2}\,\right)^2, \tag{4.6.7}$$

где равенство достигается при $(\mathbf{a})_1 = \mathrm{const}(\mathbf{a})_2$. В нашем случае матрица V диагональна и п. ч. неравенства (4.6.7) достигает максимума, когда $(\mathbf{a})_j^{\mathrm{T}}(\mathbf{a})_j = K$, $j = 1,\,2$. Делаем вывод, что

$$a_{1t} = -a_{2t} = b_t,$$

где $b_t \neq 0$ только для таких t, что v_t минимально и $\sum\limits_t b_t^2 = K$. □

Задача 4.6.16. Пусть с. в. Y распределена на $\mathbb{Z}_+$. Покажите, что максимум энтропии с. в. Y при условии $\mathsf{E}Y \leqslant M$, равный

$$-M\log M + (M+1)\log(M+1),$$

достигается на геометрическом распределении со средним M.

Выходной сигнал Y канала без памяти при неотрицательном целозначном входе X получается как

$$Y = X + \varepsilon,$$

где ε не зависит от X, $\mathsf{P}(\varepsilon = 1) = p$, $\mathsf{P}(\varepsilon = 0) = 1 - p = q$ и входные сигналы X подчиняются неравенству $\mathsf{E}X \leqslant q$. Покажите, что при $p \leqslant 1/3$ оптимальное распределение входного сигнала

$$\mathsf{P}(X = r) = (1 + p)^{-1}\Big(\frac{1}{2^{r+1}} - \Big(\frac{-p}{q}\Big)^{r+1}\Big), \quad r = 0,\ 1,\ 2,\ \ldots, \tag{4.6.8}$$

и определите пропускную способность канала.

Опишите очень коротко проблемы, возникающие при определении пропускной способности канала, если $p > 1/3$.

Решение. Сначала рассмотрим задачу

$$\text{максимизировать } h(Y) = -\sum_{y \geqslant 0} p_y \log p_y \text{ при условии } \begin{cases} p_y \geqslant 0, \\ \sum_y p_y = 1, \\ \sum_y y p_y = M. \end{cases}$$

Решение находим через лагранжиан.

$$p_y = (1 - \lambda)\lambda^y, \ \ y = 0,\ 1,\ \ldots, \quad M = \frac{\lambda}{1 - \lambda}, \ \text{ или } \lambda = \frac{M}{M + 1}$$

с оптимальным значением

$$h(Y) = (M + 1)\log(M + 1) - M \log M.$$

Далее, дифференцируя функцию $g(m) = \log(m + 1)\log(m + 1) - m \log m$, находим, что

$$g'(m) = \log(m + 1) - \log m > 0,$$

а значит, $h(Y)$ возрастает при росте M. Следовательно, максимум и оптимальное значение при $\mathsf{E}Y \leqslant M$ совпадают, что и требовалось.

Далее, пропускная способность равна $C = \sup\{h(Y) - h(Y|X)\} = h(Y) - h(\varepsilon)$ и $\mathsf{E}Y \leqslant q + \mathsf{E}\varepsilon = q + p = 1$. При $h(\varepsilon) = -p \log p - q \log q$ мы рассмотрим геометрическую с. в. Y с $M = 1$, $\lambda = 1/2$, для которой

$$C = 2 \log 2 + p \log p + q \log q = \log(4p^p q^q).$$

Тогда

$$\mathsf{E}z^X = \frac{\mathsf{E}z^Y}{\mathsf{E}z^\varepsilon} = \Big(\frac{1 - \lambda}{1 - \lambda z}\Big)\Big/(pz + q) = \frac{1}{(2 - z)(q + pz)} =$$
$$= \frac{(2 - z)^{-1} + p(q + pz)^{-1}}{1 + p} = \frac{1}{1 + p}\Big(\sum (1/2)^{1+r} z^r + (p/q)\sum (-p/q)^r z^r\Big).$$

Если $p > 1/3$, то $p/q > 1/2$ и вероятность в (4.6.8) получается отрицательной, что означает, что не существует распределения X, дающего максимум. $\square$

Задача 4.6.17. Предполагая, что границы пропускной способности канала устанавливается второй теоремой Шеннона о кодирования, выведите пропускную способность гауссовского канала без памяти.

Канал состоит из r независимых гауссовских каналов без памяти, причём дисперсия шума в i-м канале равна v_i, $i = 1, 2, \ldots, n$. Составной канал подчиняется ограничению суммарной мощности: $\mathsf{E}\Big(\sum\limits_i x_{it}^2\Big) \leqslant p$ для каждого t, где x_{it} — вход в i-й канал в момент времени t. Вычислите пропускную способность составного канала.

Решение. По поводу первой части см. § 4.1.

Далее, если мощность в i-м канале ограничена величиной p_i, то пропускная способность могла бы равняться

$$C' = \frac{1}{2}\sum_i \log\Big(1 + \frac{p_i}{v_i}\Big).$$

Реальная пропускная способность определяется как $C = \max C'$ при условии, что $p_1, \ldots, p_r \geqslant 0$, $\sum\limits_i p_i = p$. Итак, нам нужно максимизировать лагранжиан

$$\mathcal{L} = \frac{1}{2}\sum_i \log\Big(1 + \frac{p_i}{v_i}\Big) - \lambda\sum_i p_i,$$

т. е.

$$\frac{\partial}{\partial p_i}\mathcal{L} = \frac{1}{2}(v_i + p_i)^{-1} - \lambda, \quad i = 1, \ldots, r$$

и максимум достигается при

$$p_i = \max\Big\{\frac{1}{2\lambda} - v_i,\, 0\Big\} = \Big(\frac{1}{2\lambda} - v_i\Big)_+.$$

Чтобы найти константу, выберем $\lambda = \lambda^*$, где λ^* определяется из условия

$$\sum_i \Big(\frac{1}{2\lambda^*} - v_i\Big)_+ = p.$$

Существование и единственность λ^* следуют из того, что л. ч. монотонно убывает от $+\infty$ до $\sum\limits_j v_j$. Таким образом,

$$C = \frac{1}{2}\sum_i \log\Big(\frac{1}{2\lambda^* v_i}\Big). \qquad \square$$

Задача 4.6.18. Рассмотрим с. в., принимающие значения в данном множестве $\mathbb{A}$ (конечном, счётном или континуальном), распределение которых определяется плотностью относительно заданной меры μ. Пусть φ — вещественная функция, а β — вещественное число. Докажите, что максимум

$h^{\max}(X)$ энтропии $h(X) = -\int f_X(x)\log f_X(x)\mu(dx)$ при условии $\mathsf{E}\psi(X) = \beta$ достигается на с. в. X^* с п. р.

$$f_{X^*}(x) = \frac{1}{\Xi}\exp[-\gamma\psi(x)], \tag{4.6.9}$$

где $\Xi = \Xi(\gamma) = \int \exp[-\gamma\psi(x)]\mu(dx)$ — нормирующая константа, а вещественное число γ выбирается так, что

$$\mathsf{E}\psi(X^*) = \int \frac{\psi(x)}{\Xi}\exp[-\gamma\psi(x)]\mu(dx) = \beta. \tag{4.6.10}$$

Указание. Предположим, что существует γ со свойством

$$\int \frac{\psi(x)}{\Xi}\exp[-\gamma\psi(x)]\mu(dx) = \beta.$$

Покажите, что если функция ψ неотрицательна, то для любого $\beta > 0$ функция вероятности f_{X^*} из формул (4.6.9) и (4.6.10) максимизирует энтропию $h(X)$ при более широком ограничении $\mathsf{E}\psi(X) \leqslant \beta$.

Вычислите максимальное значение $h(X)$ при условии $\mathsf{E}\psi(X) \leqslant \beta$ в следующих случаях: 1) когда $\mathbb{A}$ — конечное множество, μ — положительная мера на $\mathbb{A}$ (с $\mu_i = \mu(\{i\}) = 1/\mu(\mathbb{A})$, где $\mu(\mathbb{A}) = \sum_{j\in\mathbb{A}}\mu_j$) и $\psi(x) \equiv 1$, $x \in \mathbb{A}$; 2) когда $\mathbb{A}$ — произвольное множество, μ — положительная мера на $\mathbb{A}$ с $\mu(\mathbb{A}) < \infty$ и $\psi(x) \equiv 1$, $x \in \mathbb{A}$; 3) когда $\mathbb{A} = \mathbb{R}$ — вещественная прямая, μ — мера Лебега и $\psi(x) = |x|$; 4) когда $\mathbb{A} = \mathbb{R}^d$, μ — d-мерная мера Лебега и $\psi(x) = \sum_{j=1}^{d} K_{ij}x_j$, где $K = (K_{ij})$ — положительно определённая вещественная матрица размера $d \times d$.

Решение. Учитывая, что $\ln f^*_X(x) = -\gamma\psi(x) - \ln\Xi$, воспользуемся неравенством Гиббса

$$h(X) = -\int f_X(x)\ln f_X(x)\mu(dx) \leqslant \int f_X(x)[\gamma\psi(x) + \ln\Xi]\mu(dx) = \\ = \int f_{X^*}(x)[\gamma\psi(x) + \ln\Xi]\mu(dx) = h(X^*),$$

где равенство достигается тогда и только тогда, когда $X \sim X^*$. Это доказывает первое утверждение.

Если $\psi \geqslant 0$, т. е. среднее значение $\mathsf{E}\psi(X) \geqslant 0$ и γ минимально, когда $\mathsf{E}\psi(X) = \beta$. □

Представьте ящики — один в другом.
Большой объём — и маленькие в нём.
И точно так внутри большого Мира —
полно других, хоть строй их по ранжиру.
Иной так мал, что лучше не тревожь,
когда Мирок своим размером — с грош.
На мелочи природа–мастерица.
Иной Мирок сквозь пальцы просочится.
Повсюду различимые едва
размером чуть не с атом существа.
Лишь четырёх довольно Миру–крошке.
А сколько же таких в любой серёжке?
Их не один, пожалуй, миллион
на шляпке у булавки размещён.
Миры малы, и, серьги вдев, подружки
несут Миры Миров на каждом ушке..

Маргарет Кавендиш (1623–1673),
герцогиня Ньюкасл; «О многих мирах»

Литература

[Д] *Добрушин Р.Л.* Предельный переход под знаком информации и энтропии // Теория вероятн. и ее прим. 1960. Т. 5, № 1. С. 29–37.

[MCh] *Маслов В.П.*, *Черный А.С.* О минимизации и максимизации энтропии в различных дисциплинах // Теория вероятностей и ее применения. 2003. Т. 48, № 3. С. 466–486.

[Хал] *Халатников И.М.* Дау, Кентавр и другие. М.: Физматлит, 2007.

[YY] *Яглом А.М.*, *Яглом И.М.* Вероятность и информация. М.: Наука, 1973.

[AB] *Anantharam V.*, *Baccelli F.* A Palm theory approach to error exponents // Proceedings of the 2008 IEEE Symposium on Information Theory (Toronto, 2008). P. 1768–1772.

[Ad] *Adámek J.* Foundations of coding: theory and applications of error-correcting codes, with an introduction to cryptography and information theory. Chichester: Wiley, 1991.

[Ap] *Applebaum D.* Probability and information: an integrated approach. Cambridge: Cambridge University Press, 1996.

[As] *Ash R.B.* Information theory. NY: Interscience, 1965.

[AK] *Assmus Jr. E.F.*, *Key J.D.* Designs and their codes. Cambridge: Cambridge University Press, 1992.

[AD] *Arwini K.A.*, *Dodson C.T.J.* Information geometry: near randomness and near independence. Berlin: Springer, 2008. (Lecture notes in mathematics; V. 1953.)

[AS] *Augot D.*, *Stepanov M.* A note on the generalisation of the Guruswami–Sudan list decoding algorithm to Reed-Muller codes // Gröbner Bases, Coding, and Cryptography. RISC Book Series. Springer, Heidelberg, 2009.

[Ay] *Ayres R.U.* Manufacturing and human labor as information processes. Laxenburg: International Institute for Applied System Analysis, 1987.

[B] *Balakrishnan A.V.* Communication theory (with contributions by J. W. Carlyle et al.). NY: McGraw-Hill, 1968.

[Ba] *Baylis J.* Error-correcting codes: a mathematical introduction. London: Chapman & Hall, 1998.

[BBF] *Betten A.* et al. Error-correcting linear codes classification by isometry and applications. Berlin: Springer, 2006.

[TB] *Berger T.* Rate distortion theory: a mathematical basis for data compression. Englewood Cliffs, NJ: Prentice-Hall, 1971.
[B1] *Berlekamp E.R.* A survey of algebraic coding theory. Wien: Springer, 1972.
[B2] *Berlekamp E.R.* Algebraic coding theory. NY: McGraw-Hill, 1968.
[BP] *Berstel J., Perrin D.* Theory of codes. Orlando: Academic Press, 1985.
[Bie] *Bierbrauer J.* Introduction to coding theory. Boca Raton, FL: Chapman & Hall/CRC, 2005.
[Bi] *Billingsley P.* Ergodic theory and information. NY: Wiley, 1965. Имеется перевод на русск. яз.: *Биллингслей П.* Эргодическая теория и информация. М.: Мир, 1969.
[Bl] *Blahut R.E.* Principles and practice of information theory. Reading, MA: Addison-Wesley, 1987.
[Bl1] *Blahut R.E.* Theory and practice of error control codes. 2nd Ed. Reading, MA: Addison-Wesley, 1983. Имеется перевод на русск. яз.: *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986; Algebraic codes for data transmission. Cambridge: Cambridge University Press, 2003.
[Bl2] *Blahut R.E.* Algebraic codes on lines, planes, and curves. Cambridge: Cambridge University Press, 2008.
[BM1] *Blake I.F., Mullin R.C.* The mathematical theory of coding. NY: Academic Press, 1975.
[BM2] *Blake I.F., Mullin R.C.* An introduction to algebraic and combinatorial coding theory. NY: Academic Press, 1976.
[Bla] *Blake I.F.* (Ed). Algebraic coding theory: history and development. Stroudsburg, PA: Dowden, Hutchinson & Ross, 1973.
[Blac] *Blachman N.* Noise and its effect on communication. NY: McGrow-Hill, 1966.
[BR] *Bose R.C., Ray-Chaudhuri D.K.* On a class of errors, correcting binary group codes // Information and Control. 1960. V. 3, № 1. P. 68–79.
[BS] *Bradley W., Suhov Y.M.* The entropy of famous reals: some empirical results // Random and Computational Dynamics. 1997. V. 5. P. 349–359.
[BF] *Bruen A.A., Forcinito M.A.* Cryptography, information theory, and error-correction: a handbook for the 21st century. Hoboken, NJ: Wiley-Interscience, 2005.
[Bu] *Buchmann J.A.* Introduction to cryptography. NY: Springer-Verlag, 2002.
[CvL] *Cameron P.J., van Lint J.H.* Designs, graphs, codes and their links. Cambridge: Cambridge University Press, 1991.
[CMF] *Castiñeira Moreira J., Farrell P.G.* Essentials of error-control coding. Chichester: Wiley, 2006.
[Cha] *Chambers W.G.* Basics of communications and coding. Oxford: Clarendon, 1985.
[Ch1] *Chaitin G.J.* The limits of mathematics: a course on information theory and the limits of formal reasoning. Singapore: Springer, 1998.
[Ch2] *Chaitin G.* Information-theoretic incompleteness. Singapore: World Scientific, 1992.

[Ch3] *Chaitin G.* Algorithmic information theory. Cambridge: Cambridge Univ. Press, 1987.

[CS] *Conway F.*, *Siegelman J.* Dark Hero of the information age: In search of Norbert Wiener, the father of Cybernetics. NY: Basic Books, 2004.

[CT] *Cover T.M.*, *Thomas J.M.* Elements of information theory. NY: Wiley, 2006.

[CK] *Csiszár I.*, *Körner J.* Information theory: coding theorems for discrete memoryless systems. NY: Academic Press, 1981; Budapest: Akadémiai Kiadó, 1981. Имеется перевод на русск. яз.: *Чисар И.*, *Кернер Я.* Теория информации. М.: Мир. 1985.

[DR] *Davenport W.*, *Root W.* Random signals and noise. NY: McGraw Hill, 1958. Имеется перевод на русск. яз.: *Давенпорт В.Б.*, *Рут В.Л.* Введение в теорию случайных сигналов и шумов. М.: ИЛ, 1960.

[DCT] *Dembo A.*, *Cover T.M.*, *Thomas J.A.* Information Theoretic Inequalities // IEEE Transactions on Information Theory. 1991. V. 37, № 6. P. 1501–1518.

[Dy] *Dyson F.* The tragic tale of a genius // NY Review of Books (July, 14), 2005.

[E] *Ebeling W.* Lattices and codes: a course partially based on lectures by F. Hirzebruch. Braunschweig/Wiesbaden: Vieweg, 1994.

[El] *Elkies N.* Excellent codes from modular curves // STOC'01. Proceedings of the 33rd Annual Symposium on Theory of Computing (Hersonissos, Crete, Greece). NY: ACM, 2001. P. 200–208.

[En] *Engelberg S.* Random signals and noise: a mathematical introduction. Boca Raton, FL: CRC/Taylor & Francis, 2007.

[F] *Fano R.M.* Transmission of information: a statistical theory of communication. NY: Wiley, 1961. Имеется перевод на русск. яз.: *Фано Р.М.* Передача информации. Статистическая теория связи. М.: Мир, 1965.

[Fe] *Feinstein A.* Foundations of information theory. NY: McGrow-Hill, 1958. Имеется перевод на русск. яз.: *Файнстейн А.* Основы теории информации. М.: Мир, 1960.

[Fo] *Forney G.D.* Concatenated codes. Cambridge, MA: M.I.T. Press, 1966.

[FM] *Franceschetti M.*, *Meester R.* Random networks for communication. From statistical physics to information science. Cambridge: Cambridge Univ. Press, 2007.

[Ga] *Gallager R.* Information theory and reliable communications. NY: Wiley, 1968. Имеется перевод на русск. яз.: *Галлагер Р.* Теория информации и надежная связь. М.: Советское радио, 1974.

[GK] *Gofman A.*, *Kelbert M.* Un upper bound for Kullback-Leiber divergence with a small number of outliers // Mathematical Communications. 2013. V. 18, № 1. P. 75–78.

[G] *Goldman S.* Information theory. Englewood Cliffs, NJ: Prentice-Hall, 1953.

[GP] *Goldie C.M.*, *Pinch R.G.E.* Communication theory. Cambridge: Cambridge Univ. Press, 1991.

[Gol] *Goldreich O.* Foundations of cryptography. V. 1, 2. Cambridge: Cambridge University Press, 2001, 2004.

[Go] *Goppa V.D.* Geometry and codes. Dordrecht: Kluwer, 1988.

[Gr] *Gravano S.* Introduction to error control codes. Oxford: Oxford University Press, 2001.
[G1] *Gray R.M.* Source coding theory. Boston: Kluwer, 1990.
[G2] *Gray R.M.* Entropy and information theory. NY: Springer-Verlag, 1990.
[GD] *Gray R.M.*, *Davisson L.D.* Eds. Ergodic and information theory. Stroudsburg, CA: Dowden, Hutchinson & Ross, 1977.
[GS] *Guruswami V.*, *Sudan M.* Improved decoding of Reed—Solomon codes and algebraic geometry codes // IEEE Trans. Inform. Theory. 1999. V. 45, № 6. P. 1757–1767.
[H] *Hamming R.W.* Coding and information theory. 2nd ed. Englewood Cliffs: Prentice-Hall, 1986.
[Ha] *Han T.S.* Information-spectrum methods in information theory. NY: Springer-Verlag, 2002.
[HHJ] *Hankerson D.R.*, *Harris G.A.*, *Johnson Jr. P.D.* Introduction to information theory and data compression. 2nd ed. Boca Raton, FL: Chapman & Hall/CRC, 2003.
[HHL] *Hankerson D.R.* et al. Coding theory and cryptography: the essentials / 2nd ed. NY: M. Dekker, 2000; previous ed.: *Hoffman D.G.* et al. Coding theory: the essentials. NY: M. Dekker 1991.
[Har] *Hartnett W.E.* Foundations of coding theory. Dordrecht: Reidel, 1974.
[Hei] *Heims S.J.* John von Neumann and Norbert Wiener: from mathematics to the technologies of life and death. Cambridge, MA: MIT Press, 1980.
[He1] *Helstrom C.* Statistical theory of signal detection / 2nd Ed. Oxford: Pergamon Press, 1968.
[He2] *Helstrom C.W.* Elements of signal detection and estimation. Englewood Cliffs, NJ: Prentice-Hall, 1995.
[Hi] *Hill R.* A first course in coding theory. Oxford: Oxford University Press, 1986.
[HL] *Ho T.*, *Lun D.S.* Network coding: an introduction. Cambridge: Cambridge University Press, 2008.
[Hoc] *Hocquenhem A.* Codes correcteurs d'erreurs // Chiffres. 1959. V. 2. P. 147–156.
[HP] *Huffman W.C.*, *Pless V.* Fundamentals of error-correcting codes. Cambridge: Cambridge University Press, 2003.
[HPr] *Humphreys J.F.*, *Prest M.Y.* Numbers, groups, and codes. 2nd ed. Cambridge: Cambridge University Press, 2004.
[I] *Ihara S.* Information theory for continuous systems. Singapore: World Scientific, 1993.
[In] *Ingels F.M.* Information and coding theory. Scranton: Intext Educational Publishers, 1971.
[Ja] *James I.* Remarkable mathematicians. From Euler to von Neumann. Spectrum Series published by The Mathematical Association of America. Cambridge: Cambridge University Press, 2009.
[Jay] *Jaynes E.T.* Papers on probability, statistics and statistical physics. Dordrecht: Reidel, 1982.

[Je] *Jelinek F.* Probabilistic information theory. NY: McGrow-Hill, 1968.

[JJ] *Jones G.A.*, *Jones J.M.* Information and coding theory. London: Springer, 2000.

[J] *Jones D.S.* Elementary information theory. Oxford: Clarendon Press, 1979.

[Jo] *Johnson O.* Information Theory and The Central Limit Theorem. London: Imperial College Press, 2004.

[Ju] *Justensen J.* A class of constructive asymptotically good algebraic codes // IEEE Transactions Information Theory. 1972. V. 18, № 5. P. 652–656.

[KS] *Kelbert M.*, *Suhov Y.* Continuity of mutual entropy in the large signal-to-noise ratio limit // Stochastic Analysis. Berlin: Springer, 2010. P. 281–299.

[Khi] *Хинчин А.Я.* Об основных теоремах теории информации // УМН. 1956. Т. 11, № 1. С. 17–75.

[Kl] *Klove T.* Codes for error detection. Singapore: World Scientific, 2007.

[Ko] *Koblitz N.* A course in number theory and cryptography, NY: Springer, 1993. Имеется перевод на русск. яз.: *Коблиц Н.* Курс теории чисел и криптографии. Москва: Научное изд-во ТВП, 2001.

[Kr] *Krishna H.* Computational complexity of bilinear forms: algebraic coding theory and applications of digital communication systems. Berlin: Springer-Verlag, 1987. (Lecture notes in control and information sciences; V. 94.)

[Ku] *Kullback S.* Information theory and statistics. NY: Wiley, 1959. Имеется перевод на русск. яз.: *Кульбак С.* Теория информации и статистика. М.: Наука, 1967.

[KKK] *Kullback S.*, *Keegel J.C.*, *Kullback J.H.* Topics in statistical information theory. Berlin: Springer, 1987.

[P2] *Landau H.J.*, *Pollak H.O.* Prolate spheroidal wave functions, Fourier analysis and uncertainty, II // Bell System Technical Journal. 1961. P. 64–84.

[P3] *Landau H.J.*, *Pollak H.O.* Prolate spheroidal wave functions, Fourier analysis and uncertainty, III. The dimension of the space of essentially time- and band-limited signals // Bell System Technical Journal. 1962. P. 1295–1336.

[LN] *Lidl R.*, *Niderreiter H.* Finite fields. Cambridge: Cambridge University Press, 1997. Имеется перевод на русск. яз.: *Лидл Р.*, *Нидеррайтер Г.* Конечные поля: В 2-х томах. М.: Мир, 1988.

[LP] *Lidl R.*, *Pilz G.* Applied abstract algebra. 2nd ed. NY: Wiley, 1999.

[L] *Lieb E.H.* Proof of entropy conjecture of Wehrl // Commun. Math. Phys. 1978. V. 62, № 1. P. 35–41.

[Li] *Lin S.* An introduction to error-correcting codes. Englewood Cliffs, NJ; London: Prentice-Hall, 1970

[LC] *Lin S.*, *Costello D.J.* Error control coding: fundamentals and applications. Englewood Cliffs, NJ: Prentice-Hall, 1983.

[LX] *Ling S.*, *Xing C.* Coding Theory, Cambridge: Cambridge University Press, 2004.

[vL] *van Lint J.H.* Introduction to coding theory. 3rd ed. Berlin: Springer, 1999.

[vLG] *van Lint J.H.*, *van der Geer G.* Introduction to coding theory and algebraic geometry. Basel: Birkhäuser, 1988.

[vLu] *van der Lubbe J.C.A.* Information theory. Cambridge: Cambridge University Press, 1997.

[Le] *Lewand R.E.* Cryptological mathematics. Washington, DC: Mathematical Association of America, 2000.

[Ll] *Llewellyn J.A.* Information and coding. Bromley: Chartwell-Bratt; Lund: Studentlitteratur, 1987.

[Lo] *Loève M.* Probability theory. Van Nostrand, Princeton, NY, 1955. Имеется перевод на русск. яз.: *Лоэв М.* Теория вероятностей. М.: ИЛ, 1962.

[Lu] *Luenberger D.G.* Information science. Princeton, NJ: Princeton University Press, 2006.

[M] *Mackay D.J.C.* Information theory, inference and learning algorithms. Cambridge: Cambridge Univ. Press, 2003.

[Ma] *Mann H.B.* (Ed.) Error-correcting codes. NY: J. Wiley, 1969.

[Mar] *Marcus M.* Dark Hero of the information age: in search of Norbert Wiener, the father of cybernetics // Notices of the AMS. 2005. V. 53, № 5. P. 574–579.

[MO] *Marshall A.*, *Olkin I.* Inequalities: theory of majorization and its applications. NY: Academic Press, 1979

[MWS] *MacWilliams F.J.*, *Sloane N.J.A.* The theory of error-correcting codes, Volumes I, II. Amsterdam: North-Holland Publish. Company, 1977

[McE1] *McEliece R.J.* The theory of information and coding. Reading, MA: Addison-Wesley, 1977

[McE2] *McEliece R.* The theory of information and coding. Student ed. Cambridge: Cambridge University Press, 2004

[McE3] *McEliece R.J.* The theory of information and coding. 2nd ed. Cambridge: Cambridge University Press, 2002

[MBR] *Menon A.*, *Buecher R.M.*, *Read J.H.* Impact of exclusion region and spreading in spectrum-sharing ad hoc networks. 2006 ACM 1-59593-510-X/06/08

[Mo] *Mollin R.A.* RSA and public-key cryptography. NY: Chapman & Hall, 2003

[MZ] *Morelos-Zaragoza R.H.* The art of error correcting coding. 2nd ed. Chichester: Wiley, 2006

[MM] *Mullen G.L.*, *Mummert C.* Finite fields and applications. Providence, RI: American Mathematical Society, 2007

[MSU] *Myasnikov A.*, *Shpilrain V.*, *Ushakov A.* Group-based cryptography. Basel: Birkhäuser, 2008.

[NRS] *Nebe G.*, *Rains E.M.*, *Sloane N.J.A.* Self-dual codes and invariant theory. NY: Springer, 2006

[NX] *Niederreiter H.*, *Xing C.* Rational points on curves over finite fields : theory and applications. Cambridge: Cambridge University Press, 2001

[Pe] *Peterson W.W.*, *Weldon E.J.* Error-correcting codes. 2nd ed. Cambridge, MA: MIT Press, 1972 (previous ed.: W.W. Peterson Error-correcting codes. Cambridge, MA: MIT Press, 1961)

[P] *Pinsker M.S.* Information and information stability of random variables and processes. San Francisco: Holden-Day, 1964

[Pl] *Pless V.* Introduction to the theory of error-correcting ccodes. 2nd ed. NY: Wiley, 1989

[PBH] *Pless V.S., Huffman W.C.* Eds. Handbook of coding theory, vols 1,2. Amsterdam: Elsevier, 1998

[Pi] *Piret P.* Convolutional codes: an algebraic approach. Cambridge, MA: MIT Press, 1988

[Pr] *Pretzel O.* Error-correcting codes and finite fields. Oxford: Clarendon Press, 1992; Student ed. 1996

[Ra] *Rao T.R.N.* Error coding for arithmetic processors. NY: Academic Press, 1974

[RS] *Reed M., Simon B.* Methods of modern mathematical physics, volume II. Fourier analysis, self-adjointness. NY: Academic Press, 1975 Имеется перевод на русск. яз.: Рид М., Саймон Б. Методы современной математической физики. Том 2. Гармонический анализ. Самосопряженность. М.: Мир, 1978.

[ReS] *Reed I.S., Solomon G.* Polynomial codes over certain finite fields // SIAM J. 1960. V. 8, № 2. P. 300–304.

[Re] *Rényi A.* A diary on information theory. Chichester: Wiley, 1987; initially published Budapest: Akad'emiai Kiadó, 1984. Имеется перевод на русск. яз. в кн.: *Реньи А.* Трилогия о математике. Диалоги о математике. Письма о вероятности. Дневник записки студента по теории информации. М.: Мир, 1980.

[Rez] *Reza F.M.* An introduction to information theory. NY: Constable, 1994

[R1] *Roman S.* Coding and information theory. NY: Springer, 1992

[R2] *Roman S.* Field theory. 2nd ed. NY: Springer, 2006.

[RU] *Richardson T., Urbanke R.* Modern coding theory / Cambridge: Cambridge University Press, 2008

[Ro] *Roth R.M.* Introduction to coding theory. Cambridge: Cambridge University Press, 2006

[RF] *Ryabko B., Fionov A.* Basics of contemporary cryptography for IT practitioners. Singapore: World Scientific, 2005. Русская версия: *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии. М.: Научный мир, 2004.

[Rya] *Ryan W.E., Lin S.* Channel codes: classical and modern. Cambridge: Cambridge University Press, 2009

[Sh] *Shannon C.E.* A mathematical theory of cryptography. Bell Lab. Tech. Memo., 1945

[SG] *Schürmann T., Grassberger P.* Entropy estimation of symbol sequences. Chaos, 6, 1996, 3, 414–427

[Se] *Seibt P.* Algorithmic information theory: mathematics of digital information processing. Berlin: Springer, 2006

[CES] Claude Elwood Shannon: collected papers. N.J.A. Sloane, A.D. Wyner, Eds. NY, NY: IEEE Press, 1993.

[S] *Shannon C.E.* A mathematical theory of communication. The Bell System Technical Journal, Vol. 27, July, October 1948, pp. 379–423, 623–658 Имеется перевод на русск. яз. в кн.: *Шеннон К.* Работы по теории информации и кибернетике. М.: Изд-во иностранной литературы, 1963.

[SW] *Shannon C.E.*, *Weaver W.* The mathematical theory of communication. Urbana, IL: University of Illinois Press, 1949.

[Sh] *Shields P.C.* The ergodic theory of discrete sample paths. Providence, RI: American Mathematical Society, 1996

[SS] *Shrikhande M.S.*, *Sane S.S.* Quasi-symmetric designs. Cambridge: Cambridge University Press, 1991

[Si] *Simic S.* Best possible global bounds for Jensen functional. AMS Proceedings, 138, 2010, 7, 2457-2462

[Sin] *Sinkov A.* Elementary cryptanalysis: a mathematical approach. 2nd ed. revised and updated by T. Feil. Washington, DC: Mathematical Association of America, 2009.

[P1] *Slepian D.*, *Pollak H.O.* Prolate spheroidal wave functions, Fourier analysis and uncertainty, I. Bell System Technical Journal, 1961, 43–64

[Sta] *Stallings W.* Cryptography and network security: principles and practice. 5th ed. Boston, MA: Prentice Hall; London: Pearson Education, 2011

[Stic] *Stichtenoth H.* Algebraic function field and codes. Berlin: Springer, 1993

[Sti] *Stinson D.R.* Cryptography: theory and practice. 2nd ed. Boca Raton, FL; London: Chapman & Hall/CRC, 2002

[St] *Stoyan D.*, *Kendall W.S.*, *Mecke J.* Stochastic geometry and its applications. Berlin: Academie-Verlag, 1987

[SP] *Schlegel C.*, *Perez L.* Trellis and turbo coding. NY: Wiley, 2004

[Su] *Šujan Š.* Ergodic theory, entropy and coding problems of information theory. Praha: Academia, 1983

[Sw] *Sweeney P.* Error control coding: an introduction. NY: Prentice Hall, 1991

[TK] *Te Sun Han*, *Kobayashi K.* Mathematics of information and coding. Providence, RI: American Mathematical Society, 2002

[T] *Thompson T.M.* From error-correcting codes through sphere packings to simple groups. Washington, DC: Mathematical Association of America, 1983

[TdS] *Togneri R.*, *deSilva C.J.S.* Fundamentals of information theory and coding design. Boca Raton, FL: Chapman & Hall/CRC, 2002

[TW] *Trappe W.*, *Washington L.C.* Introduction to cryptography: with coding theory. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2006

[TV] *Tsfasman M.A.*, *Vlădut S.G.* Algebraic-geometric codes. Dordrecht: Kluwer Academic, 1991

[TVN] *Tsfasman M.*, *Vlădut S.*, *Nogin D.* Algebraic geometric codes: basic notions. Providence, RI: American Mathematical Society, 2007; *Влэдуц С.Г.*, *Ногин Д.Ю.*, *Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003 г.

[TVZ] *Tsfasman M.*, *Vladut S.*, *Zink T.* Modular curves, Shimura curves and Goppa codes, better than Varshamov–Gilbert bound. Mathematics Nachrichten, 109, 21–28, 1982.

[U1] *Usher M.J.* Information theory for information technologists. London: Macmillan, 1984

[U2] *Usher M.J.*, *Guy C.G.* Information and communication for engineers. Basingstoke: Macmillan, 1997

[UG] *Usher M.J.*, *Guy C.G.* Information and communication for engineers. Basingstoke: Macmillan, 1997

[V] *Vajda I.* Theory of statistical inference and information. Dordrecht: Kluwer, 1989

[Ve] *Verdú S.* Multiuser detection. NY: Cambridge Univ. Press, 1998

[VG] *Verdú S.*, *Guo D.* A simple proof of the entropy–power inequality. IEEE Trans. Inform. Theory, 52, 2006, 5, 2165-2166

[Ve] *Vermani L.R.* Elements of algebraic coding theory. London: Chapman & Hall, 1996

[VY] *Vucetic B.*, *Yuan J.* Turbo codes: principles and applications. Norwell, MA: Kluwer, 2000

[Wa] *Wade G.* Coding techniques: an introduction to compression and error control. Basingstoke: Palgrave, 2000

[Wal] *Walker J.L.* Codes and curves. Providence, RI: American Mathematical Society, 2000

[We] *Welsh D.* Codes and Cryptography. Oxford, Oxford University Press, 1988

[W] *Wiener N.* Cybernetics or control and communication in animal and machine. Cambridge, MA: MIT Press, 1948; 2nd Edition: 1961, 1962. Имеется перевод на русск. яз.: *Винер Н.* Кибернетика, или Управление и связь в животном и машине. 2-е издание. М.: Наука, 1983.

[Wi] *Williams D.* Probability with Martingales. Cambridge: Cambridge Univ. Press, 1991.

[Wo] *Wolfowitz J.* Coding theorems of information theory. Berlin: Springer, 1961; 3rd Ed: 1978. Имеется перевод на русск. яз.: *Вольфовиц Дж.* Теоремы кодирования теории информации. М.: Мир, 1967.

[W1] *Wyner A.D.* The capacity of the band-limited Gaussian channel. Bell System Technical Journal, 1966, 359–395

[W2] *Wyner A.D.* The capacity of the product of channels. Information and Control, 1966, 423–433

[X] *Xing C.* Nonlinear codes from algebraic curves beating the Tsfasman–Vladut–Zink bound. IEEE Transactions Information Theory, 49, 1653–1657, 2003.

[Y1] *Yeung R.* A first course in information theory. Boston: Kluwer Academic, 1992, 2nd Ed. NY: Kluwer, 2002.

[Y2] *Yeung R.* Information theory and network coding. NY: Springer Verlag, 2008.

Список сокращений

БЧХ — коды Боуза—Чоудхури—Хоквингема, 256
ВТШК — вторая теорема Шеннона о кодировании для канала с шумом, 135
ДПФ — дискретное преобразование Фурье, 365
НОД — наибольший общий делитель
НОК — наименьшее общее кратное
ПТШК — первая теорема Шеннона о кодировании для канала с шумом, 57
РМ — код Рида—Маллера, 245
РС — код Рида—Соломона, 340
РША — Райвест, Шамир, Адлеман, 525
СМП — случайная мера Пуассона, 490
ШМБ — теорема Шеннона—Макмиллана—Бреймана, 450
а. г. к. — аддитивный гауссовский канал, 421
а. г. к. б. п. — аддитивный гауссовский канал без памяти, 420
а. с. р. — асимптотическое свойство равнораспределённости, 155
в. с. в. ф. — вытянутая сфероидальная волновая функция, 477
г. к. б. п. — гауссовский канал без памяти, 421
д. к. б. п. — двоичный канал без памяти, 75
д. с. к. б. п. — двоичный симметричный канал без памяти, 137
и. н. — идеальный наблюдатель, 81
л. о. с. р. с. — линейная обратная связь регистра сдвига, 509
л. ч. — левая часть
м. п. — максимальное правдоподобие, 81
м. д. р. — максимальное достижимое расстояние, 191
н. о. р. с. в. — независимые одинаково распределенные случайные величины, 11
н. о. р. — независимые одинаково распределенные
н. э. э. — неравенство Шеннона на экспоненты от энтропии (entropy power inequality), 110
о. с. р. с. — обратная связь регистра сдвига, 509
п. р. — плотность распределения, 104
п. ф. м. — производящая функция моментов, 496
п. ч. — правая часть
с. в. — случайная величина, 11
с. т. — совместная типичность, 426

у. д. б. — уравнения детального баланса, 70
у. з. б. ч. — усиленный закон больших чисел, 491
ф. в. — функция вероятности, 419
ф. р. — функция распределения, 436
ц. м. д. в. — цепь Маркова с дискретным временем, 11

Предметный указатель