ФГБОУ ВО
Московский государственный университет имени М. В. Ломоносова
Механико–математический факультет

На правах рукописи
УДК 519.2, 621.391.15

ПОЛЯНСКИЙ Никита Андреевич

Коды, свободные от перекрытий

01.01.05 — теория вероятностей и математическая статистика

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико–математических наук

Научный руководитель:
доктор физико–математических наук,
профессор Дьячков Аркадий Георгиевич

Москва — 2016

Оглавление

Введение

Настоящая диссертация посвящена вопросам теории дизъюнктивных кодов. В ней рассматриваются задачи, лежащие на стыке теории вероятностей, теории информации и комбинаторной теории кодирования.

Актуальность и история вопроса

Пусть $\mathcal{X}$ — множество из N элементов, $|\mathcal{X}| = N$, а $\mathcal{F}$ — некоторое множество его подмножеств (семейство множеств), $|\mathcal{F}| = t$. Матрица инцидентности семейства множеств — это двоичная матрица, в которой строки соответствуют элементам множества $\mathcal{X}$, а столбцы — подмножествам из $\mathcal{F}$, причем единицы стоят на пересечении со строками, помеченными элементами подмножества, соответствующего столбцу.

Двоичный код называется ***дизъюнктивным*** s***-кодом****, если он является матрицей инцидентности семейства множеств, для которого никакое множество не содержится в объединении s любых других множеств данного семейства.*

Число N назовем *длиной* кода, а мощность t такого семейства — *объемом* кода. Определим *скорость* кода $R = \log_2 t/N$. Столбцы соответствующей матрицы инцидентности будем называть *кодовыми словами.*

Дизъюнктивные коды были введены У. Каутсом и Р. Синглтоном в 1964 году в основополагающей статье [28], где был описан ряд прикладных задач и построены некоторые важные конструкции таких кодов. Отметим, что многие авторы изучали вопросы, относящиеся к дизъюнктивным кодам, с принципиально разных точек зрения и зачастую проводили свои исследования независимо от других ученых. Именно поэтому многие результаты были сперва найдены в теории информации, а позднее были переоткрыты в комбинаторике или в теории группового тестирования, и наоборот. В подтверждение вышесказанного можно выделить статью [23], написанную в 1982 году П. Эрдешем и др., в которой вводится определение дизъюнктивного 2-кода, а в 1985 году в своей следующей работе [24] авторы обобщили его уже для произвольного значения s.

Определим *асимптотическую скорость* дизъюнктивных s-кодов:

$$R(s,1) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,s,1)}, \tag{1}$$

где число $N(t,s,1)$ равно минимальной длине дизъюнктивного s-кода объема t. Использованная в обозначении асимптотической скорости пара чисел $(s,1)$ соответствует тому, что никакое отдельное множество семейства не содержится в объединении s других. Из определения сразу следует (см. [28]) теоретико-информационная верхняя граница скорости $R(s,1) \leqslant 1/s$. В 1982 году П. Эрдеш доказал [23] оценки, из которых следует, что

$$0.183 \leqslant R(2,1) \leqslant 0.322. \tag{2}$$

В том же году А.Г. Дьячковым и В.В. Рыковым независимо была построена [3] верхняя граница скорости $R(s,1)$, которая к настоящему моменту является наилучшей. Следует сказать, что они использовали собственную технику при выводе оценки. Эта граница при $s = 2$ совпадает с (2), а в случае произвольного s ими было доказано, что верна следующая граница

$$R(s,1) \leqslant \frac{2\log_2[e(s+1)/2]}{s^2}. \tag{3}$$

Отметим, что в 1994 году М. Ружинко сумел привести [35] более простое доказательство этого факта, но уже в ослабленной форме

$$R(s,1) \leqslant \frac{8\log_2 s}{s^2}. \tag{4}$$

Нижняя граница скорости $R(s,1)$ была получена А.Г. Дьячковым и В.В. Рыковым в 1983 году в работе [15], в которой с помощью метода случайного кодирования на ансамбле двоичных кодов с независимыми компонентами было показано, что асимптотика границы имеет вид

$$R(s,1) \geqslant \frac{\log_2 e}{s^2 e}(1+o(1)) = \frac{0.531}{s^2}(1+o(1)), \quad s\to\infty. \tag{5}$$

Определенный интерес представляют собой работы, написанные независимо П. Эрдешом [24] в 1985 году и Ф. Хуонгом [27] в 1987 году, которые, в частности, содержат следующую оценку

$$R(s,1) \geqslant \frac{\log_2 e}{4s^2}(1+o(1)) = \frac{0.361}{s^2}(1+o(1)), \quad s\to\infty. \tag{6}$$

В дальнейшем была построена более точная граница снизу для $R(s,1)$. В 1989 году в работе [16] методом случайного кодирования на ансамбле двоичных

равновесных кодов А.Г. Дьячков и др. показали, что асимптотика нижней границы имеет вид

$$R(s,1) \geqslant \frac{1}{s^2 \log_2 e}(1+o(1)) = \frac{0.693}{s^2}(1+o(1)), \quad s \to \infty. \tag{7}$$

В частности, при $s = 2$ полученная авторами оценка совпадает с (2).

Одним из естественных и важных обобщений понятия дизъюнктивного кода является следующее определение.

Двоичный код называется ***свободным от перекрытий*** (s,ℓ)***-кодом*** *(СП (s,ℓ)-кодом), если он является матрицей инцидентности семейства множеств, для которого пересечение любых ℓ множеств не покрывается объединением s любых других множеств данного семейства.*

Очевидно, что данное определение симметрично относительно s и ℓ в том смысле, что любому свободному от перекрытий (s,ℓ)-коду соответствует свободный от перекрытий (ℓ,s)-код того же объема и длины. Для этого вместо семейства множеств $\mathcal{F}$ достаточно рассмотреть семейство $\overline{\mathcal{F}}$, состоящее из дополнений множеств: $\overline{\mathcal{F}} = \{A:\ A = \mathcal{X} \setminus B,\ B \in \mathcal{F}\}$.

Свободные от перекрытий коды были введены К. Митчеллом и Ф. Пайпером в 1988 году в работе [33] в связи с криптографической задачей распределения ключей, описание которой можно также найти в [5, 8]. Основные конструкции свободных от перекрытий кодов, построенные на укороченных кодах Рида-Соломона, были описаны А.Г. Дьячковым и др. в [19]. Для малых значений параметров s и ℓ Ш.Х. Ким и В.С. Лебедев в работах [4, 29, 30] привели некоторые оптимальные конструкции свободных от перекрытий (s,ℓ)-кодов. В 2009 году была найдена [8] скорость конструкций свободных от перекрытий кодов, основанных на алгебро-геометрических кодах.

Аналогичным образом определим асимптотическую скорость свободных от перекрытий (s,ℓ)-кодов:

$$R(s,\ell) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,s,\ell)}, \tag{8}$$

где число $N(t,s,\ell)$ равно минимальной длине дизъюнктивного свободного от перекрытий (s,ℓ)-кода объема t. Первые результаты исследования верхних границ скорости $R(s,\ell)$ для СП (s,ℓ)-кодов, $2 \leqslant \ell \leqslant s$, были получены в 2000 году в работе [36] Д. Стинсона и др., а также в 2002 году в работе [19] А.Г. Дьячкова и др. В [36] авторы показали, что выполнена оценка

$$R(s,\ell) \leqslant \frac{20 \log_2 \binom{s+\ell}{s}}{7\binom{s+\ell}{s}(s+\ell)},$$

а также верно рекуррентное неравенство

$$\frac{1}{R(s,\ell)} \geqslant \frac{1}{R(s,\ell-1)} + \frac{1}{R(s-1,\ell)}. \tag{9}$$

В 2003 году В.С. Лебедев доказал [5] неравенство

$$R(s,\ell) \leqslant \frac{R(s-i,\ell-j)}{R(s-i,\ell-j)+\frac{(i+j)^{i+j}}{i^i\cdot j^j}}, \quad i\in[s-1],\ j\in[\ell-1], \tag{10}$$

которое представляет собой уточнение неравенства

$$R(s,\ell) \leqslant R(s-i,\ell-j)\frac{i^i\cdot j^j}{(i+j)^{i+j}}, \quad i\in[s-1],\ j\in[\ell-1], \tag{11}$$

ранее установленного [22] П. Энгелом в 1996 году. Рекуррентное неравенство (10) и верхняя граница (3) для $R(s,1)$ дают [20] для скорости $R(s,\ell)$, $2\leqslant\ell\leqslant s$, наилучшую известную верхнюю границу для $R(s,\ell)$, асимптотическое поведение которой при фиксированном $\ell\geqslant 2$ и $s\to\infty$ описывается следующим неравенством

$$R(s,\ell) \leqslant \frac{(\ell+1)^{\ell+1}}{2\,e^{\ell-1}}\frac{\log_2 s}{s^{\ell+1}}(1+o(1)). \tag{12}$$

Нижняя граница скорости $R(s,\ell)$, $2\leqslant\ell\leqslant s$, была получена в 2002 году в уже упомянутой статье [19] с помощью метода случайного кодирования на ансамбле с независимыми двоичными компонентами кодовых слов и на некотором специальном ансамбле с независимыми двоичными равновесными словами, предложенном [34] ранее Н. Куонгом и Т. Зейселем. При фиксированном $\ell\geqslant 2$ и $s\to\infty$ асимптотика этой границы имеет вид

$$R(s,\ell) \geqslant \frac{\ell^\ell\log_2 e}{e^\ell}\frac{1}{s^{\ell+1}}(1+o(1)). \tag{13}$$

Одним из следующих важных понятий в теории дизъюнктивных кодов стало определение почти дизъюнктивного кода. Впервые термин почти дизъюнктивного кода был использован в 2004 году в работе [32] Э. Макула и др. В недавней статье [38] было дано формальное определение почти дизъюнктивного кода со списочным декодированием, а также были получены первые теоретические результаты. Дадим основное определение.

Под плохим событием будем понимать следующее: «дизъюнктивная сумма некоторых s кодовых слов покрывает некоторое другое кодовое слово» (подмножество из s кодовых слов выбирается равновероятно). Тогда *пропускной способностью* $C(s,1)$ почти дизъюнктивных кодов будем называть точную верхнюю грань для скорости кодов, для которых вероятность плохого события убывает экспоненциально с ростом длины кода. Для пропускной способности почти дизъюнктивных кодов И. Воробьевым была доказана [38]

следующая граница

$$C(s,1) \geqslant \frac{\ln 2}{s}(1+o(1)), \quad s \to \infty. \tag{14}$$

Отметим, что еще в 2000 году для некоторых конструкций [18] дизъюнктивных s-кодов, основанных на укороченных кодах Рида-Соломона, была подсчитана вероятность плохого события (конструкции рассматривались как почти дизъюнктивные s'-коды, причем параметр s' брался больше s). В недавней работе [1] было найдено асимптотическое поведение параметров соответствующих кодовых конструкций.

Дадим определение почти свободного от перекрытий (s,ℓ)-кода. В данном случае под плохим событием будем подразумевать следующее: «дизъюнктивная сумма некоторых s кодовых слов покрывает конъюнкцию некоторых других ℓ кодовых слов» (подмножество из s кодовых слов выбирается равновероятно). Тогда аналогичным образом (см. случай $\ell = 1$) определим пропускную способность $C(s,\ell)$ почти свободных от перекрытий кодов. Отметим, что всякий код X является почти свободным от перекрытий (s,ℓ,ε)-кодом (ПСП (s,ℓ,ε)-кодом), где параметр $\varepsilon = \varepsilon(X)$ равен вероятности плохого события.

Одним из важных приложений свободных от перекрытий кодов является [11] задача поиска скрытого гиперграфа из семейства локализованных гиперграфов. Предположим, что задан скрытый гиперграф $H_{un} = (V,E)$. При этом известно, что этот гиперграф H_{un} принадлежит некоторому семейству гиперграфов, имеющих особую структуру. Например, в качестве такого семейства можно рассмотреть всевозможные гамильтоновы циклы на множестве вершин V. Наша цель — обнаружить ребра E этого гиперграфа H_{un}, задав N вопросов $Q(S)$, где множество S — это некоторое подмножество V. Ответ на вопрос положительный, т.е. $Q(S) = 1$, в случае, если множество S содержит полностью хотя бы одно ребро из E. В остальных случаях ответ на вопрос отрицательный, т.е. $Q(S) = 0$. Будем называть поиск неадаптивным, если все вопросы определяются заранее и не меняются в зависимости от результатов уже заданных к этому моменту вопросов. Таким образом, можно считать, что все вопросы при неадаптивном поиске задаются одновременно. Если же вопросы задаются последовательно, и последующие вопросы зависят от ответов на предыдущие, то поиск называют адаптивным. Рассмотрим семейство гиперграфов $\mathcal{F}(t,s,\ell)$, которое будет состоять из таких гиперграфов $H = (V,E)$, что множество вершин $V = \{1,2,\ldots,t\}$, множество ребер $E = \{\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_{s'}\}$, $1 \leqslant s' \leqslant s$, и размер каждого ребра $1 \leqslant |\mathbf{e}_i| \leqslant \ell$, причем никакое ребро не содержится ни в каком другом. Итак, пусть задан скрытый гиперграф $H_{un} = (V,E)$, и известно, что $H_{un} \in \mathcal{F}(t,s,\ell)$. Будем говорить, что алгоритм $\mathcal{A}$ является алгоритмом поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$, если он находит H_{un}, т.е. существует ровно один гиперграф из семейства $\mathcal{F}(t,s,\ell)$, который удовлетворяет всем заданным вопросам.

Обозначим через $N(\mathcal{A})$ максимальное количество вопросов алгоритма $\mathcal{A}$, необходимых для поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$. Определим асимптотическую скорость алгоритмов поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$:

$$R_h(s,\ell) = \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N_h(t,s,\ell)}, \tag{15}$$

где число $N_h(t,s,\ell)$ равно минимальному числу вопросов $N(\mathcal{A})$ среди всех алгоритмов $\mathcal{A}$ поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$. Будем приписывать к величине $R_h(s,\ell)$ верхний индекс a и na в зависимости от адаптивности или неадаптивности алгоритма поиска.

В 2002 году в работе [19] А.Г. Дьячков и др. показали, что задача неадаптивного поиска скрытого гиперграфа и свободные от перекрытия коды сильно связаны между собой. В частности, выполнены следующие неравенства

$$R_h^{na}(s,\ell) \leqslant R(s,\ell) \leqslant \min\left(R_h^{na}(s-1,\ell), R_h^{na}(s,\ell-1)\right). \tag{16}$$

Естественной теоретико-информационной границей для скорости адаптивного поиска служит следующее неравенство

$$R_h^{a}(s,\ell) \leqslant \frac{1}{s\ell}.$$

Отметим, что при $\ell = 1$ данная задача вырождается в довольно известную задачу поиска дефектов. Известно [14], что адаптивный поиск дефектов достигает теоретико-информационной границы, т.е.

$$R_h^{a}(s,1) = \frac{1}{s}. \tag{17}$$

Для задачи поиска скрытого графа, т.е. при $\ell = 2$, в 2008 году Д. Англуин и Ж. Чен привели [12] близкий к оптимальному алгоритм поиска скрытого графа, из которого следует, что

$$R_h^{a}(s,2) \geqslant 1/(12s).$$

Для произвольных значений s и ℓ в 2014 году Х. Абаси и др. показали [10], что

$$R_h^{a}(s,\ell) \geqslant 1/(2s\ell).$$

Рассмотрим следующее вероятностное обобщение. Под плохим событием будем понимать следующее: «алгоритм поиска скрытого гиперграфа не находит скрытый гиперграф» (скрытый гиперграф выбирается равновероятно в семействе $\mathcal{F}(t,s,\ell)$). Тогда пропускной способностью $C_h(s,\ell)$ будем называть

точную верхнюю грань для скорости алгоритмов поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$, для которых вероятность плохого события стремиться к нулю с ростом числа вершин t. Также будем приписывать к величине $C_h(s, \ell)$ верхний индекс a и na в зависимости от адаптивности или неадаптивности алгоритма поиска.

Классическим результатом для теории планирования экспериментов является следующее равенство, доказанное [6] М.Б. Малютовым и В.Л Фрейдлиной

$$C_h^a(s, 1) = C_h^{na}(s, 1) = \frac{1}{s}.$$

Цели работы

Целью диссертационной работы являются:

- построение более точных оценок снизу для асимптотической скорости свободных от перекрытий кодов,
- построение оценок снизу и сверху для пропускной способности почти свободных от перекрытий кодов,
- исследование алгоритмов поиска скрытого гиперграфа из семейства локализованных гиперграфов.

Научная новизна

Все результаты работы являются новыми. В работе впервые рассматривается понятие почти свободного от перекрытий кода, определение которого дано по аналогии с уже общепринятым в литературе определением почти дизъюнктивного кода. Также в диссертации впервые рассматриваются многошаговые алгоритмы поиска скрытого гиперграфа с вероятностью ошибки.

Основные результаты работы

В диссертации получены следующие основные результаты.

1. Доказаны новые границы снизу для асимптотической скорости $R(s, \ell)$ свободных от перекрытий кодов при $\ell \geqslant 2$, улучшающие наилучшие ранее известные границы, установленные [19] А.Г. Дьячковым и др. См. ниже теорему 1.2.2 и таблицу 1.1.

2. Предложена конструкция свободных от перекрытия кодов, обобщающая ранее известную конструкцию дизъюнктивных кодов, полученную Э. Макулой в работе [31]. См. ниже раздел 1.5.

3. Впервые получены границы снизу для пропускной способности $C(s, \ell)$ почти свободных от перекрытий кодов при $\ell \geqslant 2$. См. ниже теорему 2.2.2 и таблицу 2.1.

4. Впервые получены границы сверху для пропускной способности $C(s, \ell)$ почти свободных от перекрытий кодов при $\ell \geqslant 2$. См. ниже теорему 2.3.1 и таблицу 2.1.

5. Найдена в точности асимптотическая скорость $R_h^a(s, \ell)$ адаптивного поиска скрытого гиперграфа. Полученное равенство улучшает результат работы Х. Абаси и др. [10]. См. ниже теорему 3.2.2.

6. Найдена в точности пропускная способность $C_h^{2\text{-st}}(s, \ell)$ двухступенчатой процедуры поиска скрытого гиперграфа. См. ниже теорему 3.3.3.

Методы исследования

В работе используются классические теоретико-вероятностные методы для вычисления асимптотики важных теоретико-информационных характеристик, в частности, при оценивании вероятностей больших уклонений в методе случайного кодирования для ансамбля равновесных кодов. Также применяются методы выпуклого анализа, аналитические методы и методы комбинаторной теории кодирования.

Теоретическая и практическая ценность работы

Результаты диссертации носят теоретический характер. Они могут быть полезны специалистам, работающим в теории информации и комбинаторной теории кодирования.

Содержание диссертации

Диссертация состоит из введения, трех глав, заключения и списка литературы. Далее нумерация утверждений совпадает с их нумерацией в соответствующих главах.

Во **введении** сформулированы основные объекты исследования, дан краткий исторический обзор предыдущих результатов, а также приведено основное содержание работы и ее апробация.

Первая глава состоит из пяти разделов, посвященных вопросам свободных от перекрытий кодов.

В первом разделе первой главы даны основные определения, используемые в следующих разделах.

Во втором разделе первой главы для доказательства нижних границ скорости $R(s,\ell)$ рассматривается ансамбль $E(N,t,Q)$ двоичных $(N\times t)$-матриц X с N строками и t столбцами, где столбцы выбираются независимо и равновероятно из множества столбцов фиксированного веса $\lfloor QN\rfloor$, $0\leqslant Q\leqslant 1$. Исследуется вероятность $P_0(N,Q,s,\ell)$ плохого события: «пара $(\boldsymbol{x}(\mathcal{S}),\boldsymbol{x}(\mathcal{L}))$ является (s,ℓ)-плохой», т.е. для непересекающихся наборов столбцов с номерами $\mathcal{S}$ и $\mathcal{L}$ не выполнено условие: существует строка $i\in[N]$ такая, что $x_i(j)=0$ для $j\in\mathcal{S}$ и $x_i(j)=1$ для $j\in\mathcal{L}$. Далее показано, что

$$R(s,\ell)\geqslant \underline{R}(s,\ell)\triangleq\frac{1}{s+\ell-1}\max_{0<Q<1}A(s,\ell,Q),\qquad 2\leqslant\ell\leqslant s,$$

где

$$A(s,\ell,Q)\triangleq\varliminf_{N\to\infty}\frac{-\log_2 P_0(N,Q,s,\ell)}{N},\quad 0<Q<1.$$

После этого исследуется величина $A(s,\ell,Q)$. Используя терминологию типов последовательностей, удается свести задачу к поиску минимума функционала

$$F=F(\tau,\upsilon,Q)\triangleq\sum_{\mathbf{a}\in\{0,1\}^s}\tau(\mathbf{a})\log_2[\tau(\mathbf{a})]+\sum_{\mathbf{b}\in\{0,1\}^\ell}\upsilon(\mathbf{b})\log_2[\upsilon(\mathbf{b})]$$
$$-(1-\tau(\boldsymbol{0}))h\left(\frac{\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})}\right)+(s+\ell)h(Q)+h(\upsilon(\boldsymbol{1}))$$

в области с линейными ограничениями на распределения τ и υ. Применяя стандартный метод множителей Лагранжа и используя выпуклость функции F в рассматриваемой задаче с ограничениями, можно представить распределения τ и υ, на которых достигается минимум в задаче, как функции переменных z и u. Используя полученные результаты, доказывается следующая теорема.

Теорема 1.2.2. (Граница случайного кодирования $\underline{R}(s,\ell)$.) *Имеют место следующие три утверждения.*

1. *Пусть $2\leqslant\ell\leqslant s$. Тогда скорость СП (s,ℓ)-кодов удовлетворяет неравенству*

$$R(s,\ell)\geqslant\underline{R}(s,\ell)\triangleq\frac{1}{s+\ell-1}\max_{\substack{(20)\\0<z,u<1}}T(z,u,s,\ell),\tag{18}$$

где функция $T(z,u,s,\ell)$ *определена следующим образом*

$$T(z,u,s,\ell) \triangleq \frac{su}{1-(z-u)}\log_2\left[\frac{z}{u}\right] + \frac{\ell(1-z)}{1-(z-u)}\log_2\left[\frac{1-u}{1-z}\right] + (s+\ell-1)\log_2\left[1-(z-u)\right], \quad (19)$$

а параметры z *и* u, $0 < z,\, u < 1$, *связаны между собой посредством следующего равенства*

$$z - u = z^s(1-u)^\ell. \quad (20)$$

2. *Если* $s \to \infty$ *и* $\ell \geqslant 2$ *фиксировано, то для нижней границы* $\underline{R}(s,\ell)$ *справедливо асимптотическое равенство*

$$R(s,\ell) \geqslant \underline{R}(s,\ell) = \frac{e^{-\ell}\ell^\ell \log_2 e}{s^{\ell+1}}(1+o(1)), \quad \ell = 2,3,\ldots, \quad s \to \infty. \quad (21)$$

3. *Если* $s \to \infty$, *то для скорости* $R(s,s)$ *справедливо асимптотическое неравенство*

$$R(s,s) \geqslant \frac{\log_2 e}{s2^{2s+1}}(1+o(1)), \quad s \to \infty. \quad (22)$$

В третьем разделе первой главы описаны наилучшие на сегодняшний день верхние границы скорости $R(s,\ell)$.

В четвертом разделе первой главы приведена сводная таблица с численными значениями для полученных нижних границ скорости $R(s,\ell)$, а также ранее известных верхних границ.

В пятом разделе первой главы предложена новая конструкция свободных от перекрытий кодов, которая описана как матрица инцидентности некоторой системы множеств. Данное семейство свободных от перекрытий кодов является обобщением ранее известной конструкции дизъюнктивных кодов из работы [31] Э. Макулы. Также в этом разделе можно ознакомиться с ранее известной конструкцией свободных от перекрытий кодов, основанной на укороченных кодах Рида-Соломона. В конце раздела для некоторых малых значений s и ℓ приведены таблицы с конструктивными верхними оценками для $N(t,s,\ell)$.

Вторая глава состоит из пяти разделов, посвященных вопросам почти свободных от перекрытий кодов.

В первом разделе второй главы даны основные определения, используемые в следующих разделах.

Во втором разделе второй главы для доказательства нижних границ пропускной способности $C(s,\ell)$ рассматривается ансамбль $E(N,t,Q)$ двоичных $(N \times t)$-матриц X с N строками и t столбцами, где столбцы выбираются независимо и равновероятно из множества столбцов фиксированного веса $\lfloor QN \rfloor$, $0 \leqslant Q \leqslant 1$. Рассматриваются вероятности двух событий.

1. Условная вероятность события «дизъюнктивная сумма s кодовых слов покрывает конъюнкцию некоторых других ℓ кодовых слов» при условии, что «вес дизъюнктивной суммы s кодовых слов равен k»

$$\mathcal{P}_1^{(N)}(\ell, Q, k) \triangleq \Pr\left\{ \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succcurlyeq \bigwedge_{j\in\mathcal{L}} \boldsymbol{x}(j) \;\Big/\; \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\}.$$

2. Вероятность события «вес дизъюнктивной суммы s кодовых слов равен k»

$$\mathcal{P}_2^{(N)}(s, Q, k) \triangleq \Pr\left\{ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\}, \quad \lfloor QN \rfloor \leqslant k \leqslant \min\{N, s\lfloor QN \rfloor\}.$$

Далее показано, что пропускная способность $C(s, \ell)$ удовлетворяет неравенству

$$C(s, \ell) \geqslant \underline{C}(s, \ell) \triangleq \sup_{\substack{(24),\\ 0\leqslant Q\leqslant 1}} R, \tag{23}$$

где точная верхняя грань взята по таким R, что

$$\min_{Q<q<\min\{1,sQ\}} \left\{\mathcal{A}(s, Q, q) + [\mathcal{D}(\ell, Q, q) - \ell\, R]^+\right\} > 0, \tag{24}$$

а функции $\mathcal{A}(s, Q, q)$ и $\mathcal{D}(\ell, Q, q)$ являются логарифмическими асимптотиками соответствующих вероятностей

$$\mathcal{D}(\ell, Q, q) \triangleq \lim_{N\to\infty} \frac{-\log_2\left[\mathcal{P}_1^{(N)}(\ell, Q, k)\right]}{N}, \qquad k = \lfloor qN \rfloor,$$

и

$$\mathcal{A}(s, Q, q) \triangleq \lim_{N\to\infty} \frac{-\log_2\left[\mathcal{P}_2^{(N)}(s, Q, k)\right]}{N}, \qquad k = \lfloor qN \rfloor.$$

Будем говорить, что функция $f(x)$ является $\cup$-выпуклой, если для любых двух значений аргумента x, y и для любого числа $t \in [0, 1]$ выполняется неравенство

$$f(tx + (1-t)y) \leqslant tf(x) + (1-t)f(y).$$

Пусть $\hat{q} \triangleq 1-(1-Q)^s$. Используя аналогичные соображения, что и при выводе нижней границы скорости $R(s, \ell)$ в главе 1, доказываются следующие леммы.

Лемма 2.2.1. *Функция $\mathcal{A}(s, Q, q)$ параметра q, $Q < q < \min\{1, sQ\}$, может быть записана в параметрической форме*

$$\mathcal{A}(s, Q, q) \triangleq (1-q)\log_2(1-q) + q\log_2\left[\frac{Qy^s}{1-y}\right] + sQ\log_2\frac{1-y}{y} + sh(Q),$$

$$q = Q\frac{1-y^s}{1-y}, \qquad 0 < y < 1.$$

Более того, функция $\mathcal{A}(s, Q, q)$ является $\cup$-выпуклой, монотонно убывающей в интервале $(Q, 1-(1-Q)^s)$, монотонно возрастающей в интервале $(1-(1-Q)^s, \min\{1, sQ\})$ и свой единственный минимум, равный 0, достигает в точке $q = \hat{q}$, т.е.

$$\min_{Q<q<\min\{1,sQ\}} \mathcal{A}(s, Q, q) \;=\; \mathcal{A}(s, Q, \hat{q}) = 0, \quad 0 < Q < 1.$$

Лемма 2.2.2. *Для $\ell \geqslant 2$ значение функции $\mathcal{D}(\ell, Q, q)$ в точке $q = \hat{q}$ равно*

$$\mathcal{D}(\ell, Q, \hat{q}) \triangleq (1-Q)\ell \log_2 z - (1-\hat{q}) \log_2[1-(1-z)^\ell] \tag{25}$$
$$+\ell \left(\frac{(1-Q)}{z}(1-z) - \left(\frac{(1-Q)}{z} - \hat{q} \right) (1-z)^\ell \right) \log_2[1-z] + \ell h(Q),$$

где z единственным образом определяется из следующего уравнения

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\hat{q})z(1-z)^\ell}{1-(1-z)^\ell},$$

а $h(x)$ является функцией двоичной энтропии.

Используя утверждения лемм 2.2.1 и 2.2.2, а также установленное равенство (23), доказывается следующая теорема.

Теорема 2.2.2. (Граница случайного кодирования $\underline{C}(s, \ell)$). *Имеют место следующие два утверждения.*

1. *Для $\ell \geqslant 2$ пропускная способность $C(s, \ell)$ ПСП (s, ℓ)-кодов удовлетворяет неравенству*

$$C(s, \ell) \geqslant \underline{C}(s, \ell) \triangleq \frac{1}{\ell} \max_{0 \leqslant Q \leqslant 1} \mathcal{D}(\ell, Q, \hat{q}), \tag{26}$$

где функция $\mathcal{D}(\ell, Q, \hat{q})$ задана посредством (25).

2. *Для фиксированного параметра $\ell \geqslant 2$ и при $s \to \infty$ нижняя асимптотическая граница для $C(s, \ell)$ имеет вид*

$$C(s, \ell) \;\geqslant\; \frac{\ell^{\ell-1}}{e^\ell} \frac{\log_2 e}{s^\ell} (1 + o(1)). \tag{27}$$

В третьем разделе второй главы для вывода верхней границы пропускной способности $C(s, \ell)$ сначала получена граница типа Плоткина. Пусть X — произвольный код объема t и длины N, а $\mathcal{U}$, $|\mathcal{U}| = u$, и $\mathcal{V}$, $|\mathcal{V}| = v$, — два непересекающихся подмножества множества $[t]$. Для X, $\mathcal{U}$ и $\mathcal{V}$ определим

множество строк кода, для которых выполнено следующее условие: $x_i(j) = 0$ для любого $j \in \mathcal{U}$ и $x_i(k) = 1$ для любого $k \in \mathcal{V}$. Через $D_{u,v}(\mathcal{U}, \mathcal{V}, X) \subset [N]$ обозначим это множество. Далее рассматривается средняя (по всевозможным выборам упорядоченной пары $\mathcal{U}$ и $\mathcal{V}$) мощность величины $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$ и исследуется максимальная средняя мощность по всем кодам X объема t и длины N

$$\overline{D}_{u,v}(t, N) \triangleq \max_{X} \sum_{\substack{\mathcal{U}\in\mathcal{P}_u(t),\, \mathcal{V}\in\mathcal{P}_v(t),\\ \mathcal{U}\cap\mathcal{V}=\varnothing}} \frac{|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|}{\binom{t}{u+v} \cdot \binom{u+v}{u}}.$$

Лемма 2.3.1. (Граница Плоткина). *Выполнено следующее асимптотическое неравенство*

$$\overline{\lim_{t\to\infty}} \frac{\overline{D}_{u,v}(t, N(t))}{N(t)} \leqslant \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v\} = \frac{u^u v^v}{(u+v)^{u+v}},$$

где $N(t)$ — произвольная целочисленная функция.

Определим минимальную длину почти свободных от перекрытий (s, ℓ, ε)-кодов, имеющих объем t, и обозначим ее через $N_\varepsilon(s, \ell, t)$. Далее доказывается вспомогательная лемма.

Лемма 2.3.2. *Для любого фиксированного $\delta > 0$ и $t \geqslant t(\delta)$ длина ПСП (s, ℓ, ε)-кода*

$$N_{\varepsilon'}(s-u, \ell-v, t-u-v) \leqslant (1+\delta) \cdot N_\varepsilon(s, \ell, t) \cdot \frac{u^u v^v}{(u+v)^{u+v}},$$

где $\varepsilon' < C(\delta) \cdot \varepsilon$.

Верхняя теоретико-информационная граница пропускной способности $C(s, 1)$ представлена в следующей лемме.

Лемма 2.3.3. *Для любого фиксированного s выполнено неравенство*

$$C(s, 1) \leqslant \frac{1}{s}. \tag{28}$$

Используя леммы 2.3.1, 2.3.2 и 2.3.3, устанавливается справедливость следующей теоремы.

Теорема 2.3.1. (Верхняя граница $\overline{C}(s, \ell)$). *Имеют место следующие два утверждения.*

1. *Для любого s и ℓ пропускная способность $C(s, \ell)$ ПСП (s, ℓ)-кодов удовлетворяет неравенству*

$$C(s, \ell) \leqslant \overline{C}(s, \ell), \tag{29}$$

где $\overline{C}(s, \ell)$ определяется из начального условия

$$\overline{C}(s, 1) \triangleq \frac{1}{s} \tag{30}$$

и рекуррентного уравнения

$$\overline{C}(s,\ell) = \min_{\substack{i\in[s-1]\\ j\in[\ell-1]}} \left\{ \overline{C}(s-i,\ell-j)\frac{i^i j^j}{(i+j)^{i+j}} \right\}. \tag{31}$$

2. *Для фиксированного параметра $\ell \geqslant 1$ и при $s \to \infty$ верхняя асимптотическая граница для $C(s,\ell)$ имеет вид*

$$C(s,\ell) \leqslant \frac{\ell^\ell}{e^{\ell-1}} \cdot \frac{1}{s^\ell}(1+o(1)). \tag{32}$$

В четвертом разделе второй главы приведена сводная таблица с численными значениями для полученных нижних и верхних границ границ $C(s,\ell)$.

В пятом разделе второй главы приводится сравнительный анализ асимптотической скорости $R(s,\ell)$ свободных от перекрытий кодов и пропускной способности $C(s,\ell)$ почти свободных от перекрытий кодов.

Третья глава состоит из трех разделов, посвященных алгоритмам поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$.

В первом разделе третьей главы даны основные определения, используемые в следующих разделах.

Во втором разделе третьей главы приведен детерминированный алгоритм адаптивного поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$. Приведенный алгоритм использует три следующих алгоритма.

1. Бинарный поиск новой вершины, входящей в какое-либо ребро скрытого гиперграфа.

2. Исчерпывающий поиск ребер по вершинам, входящим в какие-либо ребра скрытого гиперграфа.

3. Исчерпывающий поиск вопроса по найденным ребрам скрытого гиперграфа.

Используя полученные результаты, устанавливается справедливость следующей теоремы.

Теорема 3.2.2. *Для скорости адаптивного поиска скрытого гиперграфа выполнено следующее равенство*

$$R_h^a(s,\ell) = \frac{1}{s\ell}.$$

В третьем разделе третьей главы доказывается существование двухступенчатой процедуры поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$, являющейся оптимальной в терминах пропускной способности. В качестве первого шага предложенной стратегии используется такой неадаптивный алгоритм (матрица поиска), с помощью которого для почти всех гиперграфов $H = (V, E)$ из семейства $\mathcal{F}(t, s, \ell)$ можно получить разбиение множества вершин V на непересекающиеся доли $V_1, \ldots, V_s$ такие, что $\mathbf{e}_i \in V_i$, $i \in [s]$. При этом число вопросов (число строк в соответствующей матрице поиска) на первом шаге является незначительным по сравнению с $\log_2 t$. Несложно проверить, что существует двойственность между задачами поиска скрытого гиперграфа из семейств $\mathcal{F}(t, s, 1)$ и $\mathcal{F}(t, 1, s)$. Пользуясь этим фактом и классическим результатом $C_h^{na}(s, 1) = 1/s$, на втором шаге предложенного алгоритма производится поиск скрытого ребра $\mathbf{e}_i$ в каждой доле V_i. Используя полученные результаты, устанавливается справедливость следующей теоремы.

Теорема 3.3.3. *Для пропускной способности двухступенчатой процедуры поиска скрытого гиперграфа выполнено следующее равенство*

$$C_h^{2\text{-}st}(s, \ell) = \frac{1}{s\ell}.$$

В **заключении** сформулированы основные результаты диссертационной работы и возможные направления дальнейших исследований.

Апробация диссертации

Результаты диссертации неоднократно докладывались автором на следующих научно-исследовательских семинарах.

1. В 2011–2016 гг. на семинаре по теории кодирования под рук. Л.А. Бассалыго, Институт проблем передачи информации им. А.А. Харкевича РАН.

2. В 2010–2016 гг. на семинаре «Проблемы современной теории информации» под рук. А.Г. Дьячкова, кафедра теории вероятностей, механико-математический факультет, Московский государственный университет им. М.В. Ломоносова.

3. В 2016 г. на семинаре по дискретной математике под рук. М.В. Вялого и С.П. Тарасова, Вычислительный центр им. А.А. Дородницына РАН.

Результаты диссертации докладывались автором на следующих конференциях.

1. International Workshop «*Search Methodologies III*», Bielefeld, Germany, 2012.

2. Международная научная конференция студентов, аспирантов и молодых учёных «*Ломоносов-2013*», Москва, Россия, 2013.

3. Fourteenth International Workshop «*Algebraic and Combinatorial Coding Theory*» (ACCT-XIV), Svetlogorsk, Russia, 2014.

4. IEEE International Symposium on Information Theory (ISIT 2014), Honolulu, USA, 2014.

5. Ninth International Workshop on Coding and Cryptography (WCC), Paris, France, 2015.

6. IEEE International Symposium on Information Theory (ISIT 2015), Hong Kong, China, 2015.

7. Международная научная конференция студентов, аспирантов и молодых учёных «*Ломоносов-2016*», Москва, Россия, 2016.

8. Fifteenth International Workshop «*Algebraic and Combinatorial Coding Theory*» (ACCT-XV), Albena, Bulgaria, 2016.

9. IEEE International Symposium on Information Theory (ISIT 2016), Barcelona, Spain, 2016.

Публикации

Основные результаты настоящей диссертации опубликованы в работах [37] – [46], представленных в конце списка литературы. Среди них 3 работы в журналах из перечня ВАК и 7 работ в рецензируемых трудах международных конференций.

Благодарности

Автор глубоко благодарен и признателен своему научному руководителю профессору Аркадию Георгиевичу Дьячкову за постановку интересных задач, обсуждение результатов и постоянное внимание к работе, а также слушателям и докладчикам семинара по теории кодирования в ИППИ РАН за полезные замечания и предложения.

Глава 1

Свободные от перекрытий коды

В этой главе будет рассмотрено определение свободных от перекрытий кодов. Используя метод случайного кодирования на ансамбле двоичных равновесных кодов, будет установлена нижняя граница для асимптотической скорости свободных от перекрытий кодов. Также будут приведены ранее известная верхняя граница и сводная таблица наилучших на сегодняшний день оценок для асимптотической скорости. В последнем разделе данной главы будут рассмотрены некоторые конструкции свободных от перекрытий кодов. Далее перейдем к формальному описанию задачи.

1.1 Основные определения

Пусть N, t, s и ℓ — целые числа, $1 \leqslant s < t$, $1 \leqslant \ell \leqslant t-s$, символ $\triangleq$ обозначает равенство по определению, $|A|$ — объем множества A, а $[N] \triangleq \{1, 2, \ldots, N\}$ — множество целых чисел от 1 до N. Введем двоичную $(N \times t)$-матрицу с N строками $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$ и t столбцами $\boldsymbol{x}(1), \ldots, \boldsymbol{x}(t)$ (*кодовыми словами*)

$$X = \|x_i(j)\|,\ x_i(j) = 0, 1,$$

$$\boldsymbol{x}_i \triangleq (x_i(1), \ldots, x_i(t)),\ \boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j)),\ i \in [N],\ j \in [t], \qquad (1.1.1)$$

которую далее будем называть *кодом длины N и объема t*. Число единиц в столбце $x(j)$, т.е. $|\boldsymbol{x}(j)| \triangleq \sum\limits_{i=1}^{N} x_i(j)$, будем называть *весом* столбца $\boldsymbol{x}(j)$, $j \in [t]$. Будем говорить, что код X является *равновесным*, если каждое его кодовое слово содержит одинаковое число w, $1 \leqslant w < N$, единиц, т.е. вес $|\boldsymbol{x}(j)| = w$ для любого $j \in [t]$. Символ $\bigvee$ обозначает операцию дизъюнктивной (булевой) суммы двух двоичных чисел

$$0 \bigvee 0 = 0, \quad 0 \bigvee 1 = 1 \bigvee 0 = 1 \bigvee 1 = 1,$$

а также покомпонентную дизъюнктивную сумму двух двоичных столбцов. Будем говорить, что столбец $\mathbf{u}$ покрывает столбец $\mathbf{v}$ ($\mathbf{u} \succcurlyeq \mathbf{v}$), если $\mathbf{u} \bigvee \mathbf{v} =$

u. Через $\lfloor a \rfloor$ ($\lceil a \rceil$) будем обозначать наибольшее (наименьшее) целое число $\leqslant a$ ($\geqslant a$).

Определение 1.1.1. [33]. Код X называется *дизъюнктивным свободным от перекрытий* (s,ℓ)*-кодом* (кратко, *СП* (s,ℓ)*-кодом*), если для любых двух непересекающихся множеств $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, существует строка $\boldsymbol{x}_i$, $i \in [N]$, для которой выполнено

$$x_i(j) = 0 \quad \text{для любого } j \in \mathcal{S}, \quad \text{и} \quad x_i(k) = 1 \quad \text{для любого} \quad k \in \mathcal{L}.$$

Учитывая очевидную симметрию по s и ℓ, обозначим через $t(N,s,\ell) = t(N,\ell,s)$ максимальный объем СП (s,ℓ)-кодов длины N, а через $N(t,s,\ell) = N(t,\ell,s)$ обозначим минимальное число строк СП (s,ℓ)-кодов объема t и определим *скорость* СП (s,ℓ)-кодов:

$$R(s,\ell) = R(\ell,s) \triangleq \varlimsup_{N\to\infty} \frac{\log_2 t(N,s,\ell)}{N} = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,s,\ell)}. \tag{1.1.2}$$

Пример 1.1.1. Пусть E_n — единичная $(n \times n)$-матрица

$$E_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Тогда несложно проверить, что для любого s, $2 \leqslant s \leqslant n-1$, двоичный код E_n является СП $(s,1)$-кодом (дизъюнктивным s-кодом), но при этом для любого ℓ, $\ell \geqslant 2$, E_n не является СП (s,ℓ)-кодом.

Пример 1.1.2. Пусть X — двоичная матрица, заданная следующим образом

$$X = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Очевидно, что двоичный код X является СП $(2,2)$-кодом.

1.2 Нижние оценки $R(s,\ell)$

Наилучшая к настоящему времени нижняя граница скорости $R(s,1)$ была получена в работе [16], в которой с помощью метода случайного кодирования на ансамбле двоичных равновесных кодов доказана следующая теорема.

Теорема 1.2.1. [16]. *Имеют место следующие два утверждения.*
1. *Скорость СП $(s,1)$-кодов удовлетворяет неравенству*

$$R(s,1) \geqslant \underline{R}(s,1) \triangleq s^{-1} \cdot \max_{0<Q<1} A(s,Q), \qquad s = 1,2,\ldots, \tag{1.2.1}$$

$$A(s,Q) \triangleq \log_2 \frac{Q}{1-y} - sK(Q,1-y) - K\left(Q, \frac{1-y}{1-y^s}\right), \tag{1.2.2}$$

где используется стандартное обозначение расстояния Кульбака

$$K(a,b) \triangleq a \cdot \log_2 \frac{a}{b} + (1-a) \cdot \log_2 \frac{1-a}{1-b}, \quad 0 < a,b < 1, \tag{1.2.3}$$

а $y = y(s,Q)$, $1-Q \leqslant y < 1$, — единственный корень уравнения

$$y = 1 - Q + Q\,y^s \cdot \frac{1-y}{1-y^s}, \qquad 1-Q \leqslant y < 1. \tag{1.2.4}$$

2. *Если $s \to \infty$, то асимптотика границы (1.2.1)-(1.2.4) имеет вид*

$$R(s,1) \geqslant \underline{R}(s,1) = \frac{1}{s^2 \log_2 e}(1+o(1)) = \frac{0.693}{s^2}(1+o(1)). \tag{1.2.5}$$

При доказательстве следующей теоремы будет развит метод, ранее используемый в [16]. Будем получена граница случайного кодирования для $R(s,\ell)$ при $\ell \geqslant 2$, численные значения которой при малых значениях параметров s и ℓ указаны в таблице 1.4 и улучшают ранее известные границы. Также в теореме произведен анализ асимптотики полученной границы при фиксированном ℓ и $s \to \infty$, а также $s = \ell$ и $s \to \infty$.

Теорема 1.2.2. (Граница случайного кодирования $\underline{R}(s,\ell)$.) *Имеют место следующие три утверждения.*
1. *Пусть $2 \leqslant \ell \leqslant s$. Тогда скорость СП (s,ℓ)-кодов удовлетворяет неравенству*

$$R(s,\ell) \geqslant \underline{R}(s,\ell) \triangleq \frac{1}{s+\ell-1} \max_{\substack{(1.2.8)\\ 0<z,\,u<1}} T(z,u,s,\ell), \tag{1.2.6}$$

где функция $T(z,u,s,\ell)$ определена следующим образом

$$T(z,u,s,\ell) \triangleq \frac{su}{1-(z-u)} \log_2 \left[\frac{z}{u}\right] + \frac{\ell(1-z)}{1-(z-u)} \log_2 \left[\frac{1-u}{1-z}\right] + (s+\ell-1)\log_2 \left[1-(z-u)\right], \tag{1.2.7}$$

а параметры z и u, $0 < z,\, u < 1$, связаны между собой посредством следующего равенства

$$z - u = z^s (1-u)^\ell. \tag{1.2.8}$$

2. *Если $s \to \infty$ и $\ell \geqslant 2$ фиксировано, то для нижней границы $\underline{R}(s,\ell)$ справедливо асимптотическое равенство*

$$R(s,\ell) \geqslant \underline{R}(s,\ell) = \frac{e^{-\ell}\ell^{\ell}\log_2 e}{s^{\ell+1}}(1+o(1)), \quad \ell = 2,3,\ldots, \quad s \to \infty. \qquad (1.2.9)$$

3. *Если $s \to \infty$, то для скорости $R(s,s)$ справедливо асимптотическое неравенство*

$$R(s,s) \geqslant \frac{\log_2 e}{s2^{2s+1}}(1+o(1)), \quad s \to \infty. \qquad (1.2.10)$$

Обозначим через $Q(s,\ell)$ долю оптимального веса кодовых слов для ансамбля равновесных двоичных кодов в границе случайного кодирования из теоремы 1.2.2. При доказательстве утверждения 2 теоремы 1.2.2 для $Q(s,\ell)$ будет установлено асимптотическое равенство

$$Q(s,\ell) = \frac{\ell}{s}(1+o(1)), \quad s \to \infty, \quad \ell = 2,3,\ldots. \qquad (1.2.11)$$

Доказательство. Сначала докажем утверждение 1. При выводе теоремы 1.2.2 будет использован метод случайного кодирования для ансамбля двоичных равновесных кодов, который является обобщением метода, разработанного в [16] для классического случая дизъюнктивных s-кодов. Зафиксируем параметр Q, $0 < Q < 1$. Будем использовать обозначения (1.1.1)-(1.1.2), введенные для определения СП (s,ℓ)-кода X длины N и объема t. Для произвольного кода X и произвольного множества $\mathcal{S} \subset [t]$ через $\boldsymbol{x}(\mathcal{S}) \triangleq \{\, \boldsymbol{x}(j) : j \in \mathcal{S}\}$ обозначим соответствующее подмножество кодовых слов кода X. Для любых непересекающихся множеств $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, соответствующую пару $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ подмножеств кодовых слов кода X будем называть (s,ℓ)-*хорошей парой*, если существует строка $\boldsymbol{x}_i$, $i \in [N]$, в которой выполнено

$$x_i(j) = 0 \quad \text{для любого} \quad j \in \mathcal{S}, \quad \text{и} \quad x_i(k) = 1 \quad \text{для любого} \quad k \in \mathcal{L}.$$

В противном случае пару $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ будем называть (s,ℓ)-*плохой парой*. Столбец $\boldsymbol{x}(j)$ назовем (s,ℓ)-*плохим столбцом в коде* X, если в X найдется (s,ℓ)-плохая пара $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ и столбец $\boldsymbol{x}(j) \in \boldsymbol{x}(\mathcal{L})$.

Определим $E(N,t,Q)$ — ансамбль двоичных $(N \times t)$-матриц X с N строками и t столбцами, где столбцы выбираются независимо и равновероятно из множества, состоящего из $\binom{N}{\lfloor QN \rfloor}$ столбцов фиксированного веса $\lfloor QN \rfloor$. Пусть множества $\mathcal{S}$ и $\mathcal{L}$ зафиксированы. Для ансамбля $E(N,t,Q)$ через $P_0(N,Q,s,\ell)$ обозначим вероятность события «пара $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ является (s,ℓ)-плохой». Очевидно, что $P_0(N,Q,s,\ell)$ не зависит от выбора $\mathcal{S}$ и $\mathcal{L}$. Для ансамбля $E(N,t,Q)$ через $P_1(N,t,Q,s,\ell)$ обозначим не зависящую от $j \in [t]$

вероятность события: «столбец $\boldsymbol{x}(j)$ является (s,ℓ)-плохим в коде X». Нетрудно видеть, что

$$P_1(N,t,Q,s,\ell) \leqslant \binom{t-1}{s+\ell-1}\binom{s+\ell-1}{s} P_0(N,Q,s,\ell)$$

$$\leqslant \frac{t^{s+\ell-1}}{s!(\ell-1)!}\, P_0(N,Q,s,\ell).$$

Отсюда вытекает, что математическое ожидание случайной величины, определяемой как: «число (s,ℓ)-плохих столбцов в коде X», не превосходит

$$t\cdot\, P_1(N,t,Q,s,\ell) \,<\, t\,\frac{t^{s+\ell-1}}{s!(\ell-1)!}\, P_0(N,Q,s,\ell).$$

Поэтому при

$$t \,<\, \left[\frac{s!(\ell-1)!}{2\,P_0(N,Q,s,\ell)}\right]^{1/(s+\ell-1)}$$

существует $(N\times t/2)$-матрица X, которая является СП (s,ℓ)-кодом. Следовательно, для любого Q, $0<Q<1$, максимальный объем СП (s,ℓ)-кодов

$$t_{cf}(N,s,\ell) \,\geqslant\, \left\lfloor \frac{1}{2}\,\left[\frac{s!(\ell-1)!}{2\,P_0(N,Q,s,\ell)}\right]^{1/(s+\ell-1)}\right\rfloor, \quad 0<Q<1.$$

Тогда, согласно определению (1.1.2) скорости $R(s,\ell)$, приходим к неравенству

$$R(s,\ell)\geqslant \underline{R}(s,\ell)\triangleq \frac{1}{s+\ell-1}\,\max_{0<Q<1} A(s,\ell,Q), \qquad 2\leqslant \ell\leqslant s,$$

$$A(s,\ell,Q)\triangleq \varlimsup_{N\to\infty}\frac{-\log_2 P_0(N,Q,s,\ell)}{N}, \quad 0<Q<1. \tag{1.2.12}$$

Для завершения вывода утверждения 1 остается вычислить в явном виде функцию $A(s,\ell,Q)$ и показать, что правая часть (1.2.12) задается (1.2.6).

Будем использовать терминологию *типов* последовательностей из [9]. Рассмотрим 2 фиксированных набора, состоящих из двоичных равновесных столбцов длины N:

$$\{\boldsymbol{x}(1),\boldsymbol{x}(2),\ldots,\boldsymbol{x}(s)\} \quad \text{и} \quad \{\boldsymbol{y}(1),\boldsymbol{y}(2),\ldots,\boldsymbol{y}(\ell)\}, \quad \text{где} \quad \boldsymbol{x}(i),\,\boldsymbol{y}(j)\in\{0,1\}^N,$$

и вес столбца $|\boldsymbol{x}(i)| = |\boldsymbol{y}(j)| = \lfloor QN\rfloor$ для любых $i\in[s]$, $j\in[\ell]$. Первый набор образует двоичную $(N\times s)$-матрицу X_s, а второй набор — $(N\times\ell)$-матрицу Y_ℓ. Сопоставим данным матрицам их *типы*, т.е. наборы целых чисел $\{n(\mathbf{a})\}$, $\mathbf{a}\triangleq(a_1,a_2,\ldots,a_s)\in\{0,1\}^s$, и $\{m(\mathbf{b})\}$, $\mathbf{b}\triangleq(b_1,b_2,\ldots,b_\ell)\in\{0,1\}^\ell$,

где элемент набора $n(\mathbf{a})$, $0 \leqslant n(\mathbf{a}) \leqslant N$, ($m(\mathbf{b})$, $0 \leqslant m(\mathbf{b}) \leqslant N$) определяется как *количество строк в матрице* X_s (Y_ℓ), *совпадающих с* $\mathbf{a}$ ($\mathbf{b}$). Очевидно, что для любых двоичных матриц X_s и Y_ℓ выполнено

$$\sum_{\mathbf{a}} n(\mathbf{a}) \,=\, \sum_{\mathbf{b}} m(\mathbf{b}) \,=\, N.$$

Через $n\,(\boldsymbol{0})$ ($m\,(\boldsymbol{1})$) будем обозначать число нулевых (единичных) строк в X_s (Y_ℓ). Заметим, что если $N - n(\boldsymbol{0}) < m(\boldsymbol{1})$, то соответствующая пара (X_s, Y_ℓ) является (s,ℓ)-хорошей. В остальных случаях, число различных пар матриц (X_s, Y_ℓ), которым сопоставлены фиксированные типы $(\{n(\mathbf{a})\}, \{m(\mathbf{b})\})$, равно $\frac{N!}{\prod_{\mathbf{a}} n(\mathbf{a})!}\frac{N!}{\prod_{\mathbf{b}} m(\mathbf{b})!}$, а доля (s,ℓ)-плохих пар из общего числа составляет $\frac{\binom{N-n(\boldsymbol{0})}{m(\boldsymbol{1})}}{\binom{N}{m(\boldsymbol{1})}}$. Таким образом,

$$P_0(N, Q, s, \ell) \,=\, \sum_{\{n(\mathbf{a})\}} \sum_{\{m(\mathbf{b})\}} \frac{N!}{\prod_{\mathbf{a}} n(\mathbf{a})!}\frac{N!}{\prod_{\mathbf{b}} m(\mathbf{b})!}\frac{\binom{N-n(\boldsymbol{0})}{m(\boldsymbol{1})}}{\binom{N}{m(\boldsymbol{1})}}\binom{N}{\lfloor QN\rfloor}^{-s-\ell}, \tag{1.2.13}$$

где суммирование идет по всевозможным типам $\{n(\mathbf{a})\}$ и $\{m(\mathbf{b})\}$, для которых

$$\begin{cases} n(\boldsymbol{0}) + m(\boldsymbol{1}) \leqslant N; \\ 0 \leqslant n(\mathbf{a}) \leqslant N; \quad 0 \leqslant m(\mathbf{b}) \leqslant N; \\ \sum\limits_{\mathbf{a}} n(\mathbf{a}) = \sum\limits_{\mathbf{b}} m(\mathbf{b}) = N; \\ |\boldsymbol{x}(i)| = \sum\limits_{\mathbf{a}:\, a_i=1} n(\mathbf{a}) = |\boldsymbol{y}(j)| = \sum\limits_{\mathbf{b}:\, y_j=1} m(\mathbf{b}) = \lfloor QN\rfloor, \quad i \in [s],\, j \in [\ell]. \end{cases} \tag{1.2.14}$$

Пусть $N \to \infty$ и $n(\mathbf{a}) \triangleq N[\tau(\mathbf{a}) + o(1)]$, $m(\mathbf{b}) \triangleq N[\upsilon(\mathbf{b}) + o(1)]$, где фиксированные распределения вероятностей $\tau \triangleq \{\tau(\mathbf{a})\}$, $\mathbf{a} \in \{0,1\}^s$ и $\upsilon \triangleq \{\upsilon(\mathbf{b})\}$, $\boldsymbol{y} \in \{0,1\}^\ell$, обладают свойствами, индуцированными условиями (1.2.14), т.е.

$$\begin{cases} \sum\limits_{\mathbf{a}\in\{0,1\}^s} \tau(\mathbf{a}) = 1, \quad \sum\limits_{\mathbf{b}\in\{0,1\}^\ell} \upsilon(\mathbf{b}) = 1, \quad \tau(\boldsymbol{0}) + \upsilon(\boldsymbol{1}) \leqslant 1, \\ \sum\limits_{\mathbf{a}:\, a_i=1} \tau(\mathbf{a}) = Q, \quad \sum\limits_{\mathbf{b}:\, b_j=1} \upsilon(\mathbf{b}) = Q \quad \text{для любых } i \in [s],\, j \in [\ell]. \end{cases} \tag{1.2.15}$$

С помощью формулы Стирлинга для типов, соответствующих этим распределениям, находим логарифмическую асимптотику слагаемого в (1.2.13):

$$-\log_2 \left\{ \frac{N!}{\prod_{\mathbf{a}} n(\mathbf{a})!}\frac{N!}{\prod_{\mathbf{b}} m(\mathbf{b})!}\frac{\binom{N-n(\boldsymbol{0})}{m(\boldsymbol{1})}}{\binom{N}{m(\boldsymbol{1})}}\binom{N}{\lfloor QN\rfloor}^{-s-\ell} \right\} = N[F(\tau, \upsilon, Q) + o(1)],$$

где

$$F = F(\tau, \upsilon, Q) \triangleq \sum_{\mathbf{a}} \tau(\mathbf{a}) \log_2 [\tau(\mathbf{a})] + \sum_{\mathbf{b}} \upsilon(\mathbf{b}) \log_2 [\upsilon(\mathbf{b})] \\ - (1 - \tau(\boldsymbol{0}))h\left(\frac{\upsilon(\boldsymbol{1})}{1 - \tau(\boldsymbol{0})}\right) + (s + \ell)h(Q) + h(\upsilon(\boldsymbol{1})).$$

Пусть $\tau_Q \triangleq \{\tau_Q(\mathbf{a})\}$ и $\upsilon_Q \triangleq \{\upsilon_Q(\mathbf{b})\}$ — распределения со свойствами (1.2.15), на которых достигается минимум функции $F(\tau, \upsilon, Q)$ для данного Q. Тогда главным членом логарифмической асимптотики суммы слагаемых (1.2.13) является

$$A(s, \ell, Q) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 P_0(N, Q, s, \ell)}{N} = \min_{(\tau,\upsilon)\in(1.2.15)} F(\tau, \upsilon, Q) \\ = F(\tau_Q, \upsilon_Q, Q). \tag{1.2.16}$$

Будем искать минимум функции $F \triangleq F(\tau, \upsilon, Q)$ при ограничениях (1.2.15). Поскольку функция F непрерывна в рассматриваемой области допустимых значений аргумента (τ, υ), в том числе и на ее границе, то достаточно найти минимум F при условиях (1.2.15) с исключенными границами. Запишем соответствующую задачу минимизации: $F \to \min$.

Основная функция: $F(\tau, \upsilon, Q) : \mathbb{X} \to \mathbb{R}$.

$$\text{Ограничения: } \begin{cases} \sum\limits_{\mathbf{a}\in\{0,1\}^s} \tau(\mathbf{a}) = 1, \\ \sum\limits_{\mathbf{b}\in\{0,1\}^\ell} \upsilon(\mathbf{b}) = 1, \\ \sum\limits_{\mathbf{a}:\, a_i=1} \tau(\mathbf{a}) = Q \quad \text{для любого } i \in [s], \\ \sum\limits_{\mathbf{b}:\, b_j=1} \upsilon(\mathbf{b}) = Q \quad \text{для любого } j \in [\ell]; \end{cases} \tag{1.2.17}$$

$$\text{Область поиска } \mathbb{X}: \begin{cases} 0 < \tau(\mathbf{a}) < 1 \quad \text{для любого } \mathbf{a} \in \{0,1\}^s, \\ 0 < \upsilon(\mathbf{b}) < 1 \quad \text{для любого } \mathbf{b} \in \{0,1\}^\ell, \\ \tau(\boldsymbol{0}) + \upsilon(\boldsymbol{1}) < 1. \end{cases}$$

Для вычисления точки минимума (τ_Q, υ_Q) применим стандартный метод множителей Лагранжа. Рассмотрим лагранжиан

$$\Lambda \triangleq F(\tau, \upsilon, Q) + \lambda_0 \left(\sum_{\mathbf{a}} \tau(\mathbf{a}) - 1\right) + \lambda_1 \left(\sum_{\mathbf{b}} \upsilon(\mathbf{b}) - 1\right) \\ + \sum_{i=1}^{s} \mu_i \left(\sum_{\mathbf{a}:\, a_i=1} \tau(\mathbf{a}) - Q\right) + \sum_{i=1}^{\ell} \nu_i \left(\sum_{\mathbf{b}:\, b_i=1} \upsilon(\mathbf{b}) - Q\right).$$

Необходимые условия экстремального распределения (τ_Q, υ_Q) имеют вид

$$\begin{cases} \frac{\partial\Lambda}{\partial(\tau(\mathbf{a}))} = \log_2[\tau(\mathbf{a})] + \log_2 e + \lambda_0 + \sum\limits_{i:\, a_i=1} \mu_i \;=\; 0 \quad \text{для любого } \mathbf{a} \neq \boldsymbol{0}, \\ \frac{\partial\Lambda}{\partial(\tau(\boldsymbol{0}))} = \log_2[\tau(\boldsymbol{0})] + \log_2 e + \lambda_0 + \log_2\left[\frac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\right] = 0, \\ \frac{\partial\Lambda}{\partial(\upsilon(\mathbf{b}))} = \log_2[\upsilon(\mathbf{b})] + \log_2 e + \lambda_1 + \sum\limits_{i:\, b_i=1} \nu_i \;=\; 0 \quad \text{для любого } \mathbf{b} \neq \boldsymbol{1}, \\ \frac{\partial\Lambda}{\partial(\upsilon(\boldsymbol{1}))} = \log_2[\upsilon(\boldsymbol{1})] + \log_2 e + \lambda_1 + \sum\limits_{i=1}^{\ell} \nu_i + \log_2\left[\frac{1-\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\right] \;=\; 0. \end{cases} \tag{1.2.18}$$

Покажем, что матрица, составленная из вторых производных лагранжиана, является положительно определенной. Действительно, опишем эту матрицу:

$$\begin{aligned} &\frac{\partial^2\Lambda}{\partial^2(\tau(\mathbf{a}))} = \frac{\log_2 e}{\tau(\mathbf{a})} > 0 \quad \text{для любого } \mathbf{a} \neq \boldsymbol{0}, \\ &\frac{\partial^2\Lambda}{\partial^2(\upsilon(\mathbf{b}))} = \frac{\log_2 e}{\upsilon(\mathbf{b})} > 0 \quad \text{для любого } \mathbf{b} \neq \boldsymbol{1}, \\ &a' \triangleq \frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{0}))^2} = \frac{\log_2 e}{\tau(\boldsymbol{0})} + \frac{\log_2 e \cdot \upsilon(\boldsymbol{1})}{(1-\tau(\boldsymbol{0}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} > 0, \\ &b' \triangleq \frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{0}))\partial(\upsilon(\boldsymbol{1}))} = \frac{\log_2 e}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})} > 0, \\ &c' \triangleq \frac{\partial^2\Lambda}{\partial(\upsilon(\boldsymbol{1}))^2} = \frac{\log_2 e}{\upsilon(\boldsymbol{1})} + \frac{\log_2 e \cdot \tau(\boldsymbol{0})}{(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} > 0, \end{aligned}$$

а остальные элементы нулевые. Поэтому, достаточно проверить, что $a'c' - b'^2 > 0$. Имеем

$$\begin{aligned} &\frac{a'c' - b'^2}{(\log_2 e)^2} \\ &= \frac{1}{\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})} + \frac{1}{(1-\tau(\boldsymbol{0}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} + \frac{1}{(1-\upsilon((\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} \\ &\quad + \frac{\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})}{(1-\tau(\boldsymbol{0}))(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))^2} - \frac{1}{(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))^2} \\ &= \frac{1}{\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})} + \frac{1}{(1-\tau(\boldsymbol{0}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} + \frac{1}{(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} \\ &\quad - \frac{1}{(1-\tau(\boldsymbol{0}))(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} \geqslant \frac{1-\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})} > 0. \end{aligned}$$

Матрица вторых производных функции F совпадает с вышеописанной матрицей, и следовательно [2], функция F строго выпукла в области $\mathbb{X}$.

Заметим, что уравнения ограничений (1.2.17) образуют аффинное подпространство $\mathbb{G}$ в $\mathbb{R}^{2^s+2^\ell}$ размерности $\left(2^s+2^\ell-(s+\ell+2)\right)$. Откуда вытекает, что функция F строго выпукла и в $\mathbb{G}\cap\mathbb{X}$, что в свою очередь означает, что в $\mathbb{G}\cap\mathbb{X}$ локальный минимум функции F является глобальным и единственным. Далее воспользуемся теоремой Каруша-Куна-Таккера [2], утверждающей, что всякое решение, удовлетворяющее системе (1.2.18), ограничениям (1.2.17) и имеющее положительно определенную матрицу вторых производных лагранжиана в этой точке, является локальным минимумом функции F. Таким образом, если есть решение системы (1.2.18) и (1.2.17) в области $\mathbb{X}$, то оно единственно, и эта точка является минимумом функции F на $\mathbb{X}$.

Докажем, что из симметрии задачи следует равенство: $\mu \triangleq \mu_1 = \mu_2 = \ldots = \mu_s$. Достаточно показать, что $\mu_i = \mu_j$ для $i \neq j$. Пусть $\bar{\mathbf{a}}_i \triangleq (0,\ldots,1,\ldots,0)$ обозначает s-строку, в которой на i-м месте стоит 1. При перестановке индексов i и j получается задача минимизации, эквивалентная исходной. Следовательно, если (τ_Q^1, υ_Q) — решение, то решением будет также и (τ_Q^2, υ_Q), для которого вероятнорсть $\tau_Q^2(\mathbf{a}) = \tau_Q^1(\tilde{\mathbf{a}})$, где $\tilde{\mathbf{a}}$ — строка, полученная перестановкой индексов i и j из строки $\mathbf{a}$. Из единственности решения τ_Q следует, что распределения (τ_Q^1, υ_Q) и (τ_Q^2, υ_Q) совпадают. В частности, вероятность $\tau_Q^1(\bar{\mathbf{a}}_i) = \tau_Q^1(\bar{\mathbf{a}}_j)$. Равенство множителей Лагранжа вытекает из первого уравнения в системе (1.2.18). Используя те же рассуждения, можно доказать, что $\nu \triangleq \nu_1 = \nu_2 = \ldots = \nu_\ell$.

Для краткости введем параметры $\hat{\mu} \triangleq \log_2 e + \lambda_0$, $\hat{\nu} \triangleq \log_2 e + \lambda_1$. Тогда уравнения (1.2.18) принимают вид

$$\begin{cases} \hat{\mu} + \mu \sum_{i=1}^{s} a_i + \log_2 [\tau(\mathbf{a})] = 0 \quad \text{при } \mathbf{a} \neq \boldsymbol{0}, \\ \hat{\mu} + \log_2 [\tau(\boldsymbol{0})] + \log_2 \left[\frac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\right] = 0, \\ \hat{\nu} + \nu \sum_{i=1}^{\ell} b_i + \log_2 [\upsilon(\mathbf{b})] = 0 \quad \text{при } \mathbf{b} \neq \boldsymbol{1}, \\ \hat{\nu} + \nu\ell + \log_2 [\upsilon(\boldsymbol{1})] + \log_2 \left[\frac{1-\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\right] = 0. \end{cases} \tag{1.2.19}$$

Из первого уравнения системы (1.2.19) следует, что

$$\tau(\mathbf{a}) = 2^{-\hat{\mu}} 2^{-\mu \sum a_i} = \frac{2^{-\hat{\mu}}}{z^s} \prod_{i=1}^{s} \tilde{P}_1(a_i) \quad \text{при } \mathbf{a} \neq \boldsymbol{0},$$

где

$$\tilde{P}_1(0) \triangleq \frac{1}{1+2^{-\mu}} \triangleq z, \quad \tilde{P}_1(1) \triangleq \frac{2^{-\mu}}{1+2^{-\mu}} \triangleq 1-z.$$

Из условий (1.2.17) получаем

$$Q = \frac{2^{-\hat{\mu}}}{z^s} \sum_{k=0}^{s-1} \binom{s-1}{k} z^{s-k-1}(1-z)^{k+1} = \frac{1-z}{2^{\hat{\mu}} z^s} \quad \Leftrightarrow \quad \hat{\mu} = \log_2 \left[\frac{1-z}{Q z^s}\right].$$

Далее, так как $\tau = \{\tau(\mathbf{a})\}$, $\mathbf{a} \in \{0,1\}^s$, является распределением вероятностей, то

$$1 - \tau\left(\boldsymbol{0}\right) = \sum_{\mathbf{a}>\boldsymbol{0}} \tau(\mathbf{a}) = \frac{2^{-\hat{\mu}}}{z^s} \sum_{k=1}^{s} \binom{s}{k} z^{s-k}(1-z)^k = \frac{Q(1-z^s)}{1-z}.$$

Поэтому все вероятности экстремального распределения $\tau_Q = \{\tau_Q(\mathbf{a})\}$ могут быть представлены как функции независимой переменной z, $0 < z < 1$:

$$\tau_Q(\mathbf{a}) = \frac{Q}{1-z} z^{s-\sum_{i=1}^{s} a_i} (1-z)^{\sum_{i=1}^{s} a_i} \quad \text{при } \mathbf{a} \neq \boldsymbol{0};$$

$$\tau_Q\left(\boldsymbol{0}\right) = 1 - \frac{Q(1-z^s)}{1-z}. \tag{1.2.20}$$

Аналогичным образом, из третьего уравнения системы (1.2.19) следует, что вероятность

$$\upsilon(\mathbf{b}) = 2^{-\hat{\nu}} 2^{-\nu \sum b_i} = \frac{2^{-\hat{\nu}}}{u^\ell} \prod_{i=1}^{\ell} \tilde{P}_2(b_i) \quad \text{при } \mathbf{b} \neq \boldsymbol{1}\,,$$

где

$$\tilde{P}_2(0) \triangleq \frac{1}{1+2^{-\nu}} \triangleq u, \quad \tilde{P}_2(1) \triangleq \frac{2^{-\nu}}{1+2^{-\nu}} \triangleq 1-u.$$

Далее, так как $\upsilon = \{\upsilon(\mathbf{b})\}$, $\mathbf{b} \in \{0,1\}^\ell$, является распределением вероятностей, то

$$1 - \upsilon\left(\boldsymbol{1}\right) = \sum_{\mathbf{b}<\boldsymbol{1}} \upsilon(\mathbf{b}) = \frac{2^{-\hat{\nu}}}{u^\ell} \sum_{k=0}^{\ell-1} \binom{\ell}{k} u^{\ell-k}(1-u)^k = \frac{2^{-\hat{\nu}}}{u^\ell}(1-(1-u)^\ell).$$

Из условий (1.2.17) и предыдущего уравнения получаем

$$\begin{aligned} Q &= \frac{2^{-\hat{\nu}}}{u^\ell} \sum_{k=0}^{\ell-2} \binom{\ell-1}{k} u^{\ell-k-1}(1-u)^{k+1} + \upsilon(\boldsymbol{1}) \\ &= 1 + \frac{2^{-\hat{\nu}}}{u^\ell} \left((1-u)(1-(1-u)^{\ell-1}) - (1-(1-u)^\ell)\right). \end{aligned}$$

Откуда имеем

$$\frac{2^{-\hat{\nu}}}{u^\ell} = \frac{1-Q}{u} \quad \Leftrightarrow \quad \hat{\nu} = \log_2 \left[\frac{u}{(1-Q)u^\ell}\right].$$

Тогда вероятности экстремального распределения $\upsilon_Q = \{\upsilon_Q(\mathbf{b})\}$, $\mathbf{b} \in \{0,1\}^\ell$, можно представить в виде функций независимой переменной u, $0 < u < 1$:

$$\upsilon_Q(\mathbf{b}) = \frac{1-Q}{u} u^{\ell - \sum_{j=1}^{\ell} b_j} (1-u)^{\sum_{j=1}^{\ell} b_j} \quad \text{при } \mathbf{b} \neq \boldsymbol{1};$$

$$\upsilon_Q(\boldsymbol{1}) = 1 - \frac{(1-Q)(1-(1-u)^\ell)}{u}. \tag{1.2.21}$$

Подставив найденные выражения для μ, $\hat{\mu}$, ν, $\hat{\nu}$, $\tau_Q(\boldsymbol{0})$ и $\upsilon_Q(\boldsymbol{1})$ во второе уравнения системы (1.2.19), имеем

$$\log_2\left[\frac{1-z}{Qz^s}\right] + \log_2\left[1 - \frac{Q(1-z^s)}{1-z}\right] + \log_2\left[\frac{Q(1-z^s)}{1-z}\right]$$
$$= \log_2\left[\frac{Q(1-z^s)}{1-z} - 1 + \frac{(1-Q)(1-(1-u)^\ell)}{u}\right].$$

Откуда получаем

$$\frac{(1-z-Q(1-z^s))(1-z^s)}{z^s}$$
$$= \frac{Q(1-z^s)u - (1-z)u + (1-Q)(1-z)(1-(1-u)^\ell)}{u},$$

$$(1-z)(1-z^s)u + (1-z)uz^s - (1-z)(1-(1-u)^\ell)z^s$$
$$= Q(u(1-z^s)^2 + (1-z^s)uz^s - (1-z)(1-(1-u)^\ell)z^s),$$

$$Q = \frac{(1-z)(u - z^s(1-(1-u)^\ell))}{((1-z^s)u - z^s(1-z)(1-(1-u)^\ell))}. \tag{1.2.22}$$

Подставив найденные выражения для μ, $\hat{\mu}$, ν, $\hat{\nu}$, $\tau_Q(\boldsymbol{0})$ и $\upsilon_Q(\boldsymbol{1})$ в четвертое уравнения системы (1.2.19), имеем

$$\log_2\left[\frac{(1-Q)(1-(1-u)^\ell)}{u}\right] - \ell\log_2\left[\frac{1-u}{u}\right]$$
$$+ \log_2\left[1 - \frac{(1-Q)(1-(1-u)^\ell)}{u}\right] + \log_2\left[\frac{u}{(1-Q)u^\ell}\right]$$
$$= \log_2\left[\frac{Q(1-z^s)}{1-z} - 1 + \frac{(1-Q)(1-(1-u)^\ell)}{u}\right].$$

Откуда получаем

$$\frac{(u-(1-Q)(1-(1-u)^\ell))(1-(1-u)^\ell)}{(1-u)^\ell}$$
$$= \frac{Q(1-z^s)u - (1-z)u + (1-Q)(1-z)(1-(1-u)^\ell)}{1-z},$$

$$(1-z)(u-1+(1-u)^\ell)(1-(1-u)^\ell)+u(1-z)(1-u)^\ell-(1-z)(1-u)^\ell(1-(1-u)^\ell)$$
$$= Q((1-u)^\ell(1-z^s)u-(1-u)^\ell(1-z)(1-(1-u)^\ell)-(1-z)(1-(1-u)^\ell)^2),$$

$$Q=\frac{(1-z)((1-u-(1-u)^\ell)}{((1-z)(1-(1-u)^\ell)-u(1-u)^\ell(1-z^s))} \tag{1.2.23}$$

Из уравнений (1.2.22) и (1.2.23) следует, что

$$((1-u-(1-u)^\ell)((1-z^s)u-z^s(1-z)(1-(1-u)^\ell))$$
$$=(u-z^s(1-(1-u)^\ell))((1-z)(1-(1-u)^\ell)-u(1-u)^\ell(1-z^s)).$$

Далее элементарными преобразованиями можно получить

$$z-u=z^s(1-u)^\ell. \tag{1.2.24}$$

Используя последнее уравнение, можно упростить выражение (1.2.22)

$$Q=\frac{1-z}{1-(z-u)} \quad \Leftrightarrow \quad 1-Q=\frac{u}{1-(z-u)}. \tag{1.2.25}$$

Перепишем (1.2.20), используя последнее равенство

$$\tau_Q(\mathbf{a})=\frac{z^{s-\sum_{i=1}^s a_i}(1-z)^{\sum_{i=1}^s a_i}}{1-(z-u)} \quad \text{при } \mathbf{a}\neq \boldsymbol{0},$$

$$\tau_Q(\boldsymbol{0})=1-\frac{(1-z^s)}{1-(z-u)}=\frac{z^s-(z-u)}{1-(z-u)}. \tag{1.2.26}$$

Также перепишем (1.2.21), применяя (1.2.25)

$$\upsilon_Q(\mathbf{b})=\frac{u^{\ell-\sum_{j=1}^\ell b_j}(1-u)^{\sum_{j=1}^\ell b_j}}{1-(z-u)} \quad \text{при } \mathbf{b}\neq \boldsymbol{1},$$

$$\upsilon_Q(\boldsymbol{1})=1-\frac{(1-(1-u)^\ell)}{1-(z-u)}=\frac{(1-u)^\ell-(z-u)}{1-(z-u)}. \tag{1.2.27}$$

Заметим, что любое решение $0<z,u<1$ уравнения (1.2.24) задает распределения τ_Q и υ_Q. В силу единственности такого решения для фиксированного Q, то для вычисления максимума в (1.2.16) по параметру Q, $0<Q<1$, можно применять равенства:

$$\max_{0<Q<1} A(s,\ell,Q) = \max_{0<Q<1} F(\tau_Q,\upsilon_Q,Q)=\max_{\substack{(1.2.24)\\0<z,u<1}} F\left(\tau_{Q(z,u)},\upsilon_{Q(z,u)},Q(z,u)\right), \tag{1.2.28}$$

где

$$F\left(\tau_Q, \upsilon_Q\, Q\right) = \sum_{\mathbf{a}} \tau_Q(\mathbf{a}) \log_2\left[\tau_Q(\mathbf{a})\right] + \sum_{\mathbf{b}} \upsilon_Q(\mathbf{b}) \log_2\left[\upsilon_Q(\mathbf{b})\right]$$
$$- \left(1 - \tau_Q\left(\boldsymbol{0}\right)\right) h\left(\frac{\upsilon_Q\left(\boldsymbol{1}\right)}{1 - \tau_Q\left(\boldsymbol{0}\right)}\right) + (s+\ell) h(Q) + h(\upsilon_Q\left(\boldsymbol{1}\right)). \quad (1.2.29)$$

Используя (1.2.26)-(1.2.27), представим все пять слагаемых суммы в правой части (1.2.29) в виде функций переменных z и u, связанных между собой посредством (1.2.24). Запишем в таком виде первое слагаемое

$$\sum_{\mathbf{a}} \tau_Q(\mathbf{a}) \log_2\left[\tau_Q(\mathbf{a})\right] = \left\{ \sum_{k=1}^{s} \binom{s}{k} \frac{z^{s-k}(1-z)^k}{1-(z-u)} \log_2\left[\frac{z^{s-k}(1-z)^k}{1-(z-u)}\right] \right\}$$
$$+ \frac{z^s - (z-u)}{1-(z-u)} \log_2\left[\frac{z^s-(z-u)}{1-(z-u)}\right] = \left\{ \frac{s(z-z^s)}{1-(z-u)} \log_2 z \right.$$
$$\left. + \frac{s(1-z)}{1-(z-u)} \log_2[1-z] - \frac{1-z^s}{1-(z-u)} \log_2\left[1-(z-u)\right] \right\}$$
$$+ \frac{z^s-(z-u)}{1-(z-u)} \log_2\left[z^s-(z-u)\right] - \frac{z^s-(z-u)}{1-(z-u)} \log_2\left[1-(z-u)\right]$$
$$= \frac{s(z-z^s)}{1-(z-u)} \log_2 z + \frac{s(1-z)}{1-(z-u)} \log_2[1-z]$$
$$+ \frac{z^s-(z-u)}{1-(z-u)} \log_2\left[z^s-(z-u)\right] - \log_2\left[1-(z-u)\right]$$
$$= \frac{su}{1-(z-u)} \log_2 z + \frac{z^s-(z-u)}{1-(z-u)} \log_2\left[1-(1-u)^\ell\right]$$
$$+ \frac{s(1-z)}{1-(z-u)} \log_2[1-z] - \log_2\left[1-(z-u)\right]. \quad (1.2.30)$$

Четвертое слагаемое

$$(s+\ell) h(Q) = -\frac{(s+\ell)(1-z)}{1-(z-u)} \log_2\left[\frac{1-z}{1-(z-u)}\right] - \frac{(s+\ell)u}{1-(z-u)}$$
$$\times \log_2\left[\frac{u}{1-(z-u)}\right] = (s+\ell)\log_2\left[1-(z-u)\right] - \frac{(s+\ell)(1-z)}{1-(z-u)} \log_2\left[1-z\right]$$
$$- \frac{(s+\ell)u}{1-(z-u)} \log_2 u. \quad (1.2.31)$$

Второе слагаемое

$$\sum_{\mathbf{b}} \upsilon_Q(\mathbf{b}) \log_2 [\upsilon_Q(\mathbf{b})] = \sum_{k=0}^{\ell-1} \binom{\ell}{k} \frac{u^{\ell-k}(1-u)^k}{1-(z-u)} \log_2 \left[\frac{u^{\ell-k}(1-u)^k}{1-(z-u)} \right]$$
$$+ \frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[\frac{(1-u)^\ell - (z-u)}{1-(z-u)} \right]$$
$$= \frac{\ell u}{1-(z-u)} \log_2 u + \frac{\ell \left((1-u) - (1-u)^\ell \right)}{1-(z-u)} \log_2[1-u]$$
$$+ \frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[(1-u)^\ell - (z-u) \right] - \log_2 \left[1-(z-u) \right]$$
$$= \frac{\ell u}{1-(z-u)} \log_2 u + \frac{\ell(1-z)}{1-(z-u)} \log_2[1-u]$$
$$+ \frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[1-z^s \right] - \log_2 \left[1-(z-u) \right]. \quad (1.2.32)$$

Третье слагаемое

$$-(1-\tau_Q(\boldsymbol{0}))h\left(\frac{\upsilon_Q(\boldsymbol{1})}{1-\tau_Q(\boldsymbol{0})} \right) = -(1-\tau_Q(\boldsymbol{0})) \log_2 [1-\tau_Q(\boldsymbol{0})]$$
$$+ \upsilon_Q(\boldsymbol{1}) \log_2 [\upsilon_Q(\boldsymbol{1})] + (1-\tau_Q(\boldsymbol{0}) - \upsilon_Q(\boldsymbol{1})) \log_2 [1-\tau_Q(\boldsymbol{0}) - \upsilon_Q(\boldsymbol{1})]$$
$$= \frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[\frac{(1-u)^\ell - (z-u)}{1-(z-u)} \right] - \frac{(1-z^s)}{1-(z-u)} \log_2 \left[\frac{(1-z^s)}{1-(z-u)} \right]$$
$$+ \frac{1+(z-u)-z^s-(1-u)^\ell}{1-(z-u)} \log_2 \left[\frac{1+(z-u)-z^s-(1-u)^\ell}{1-(z-u)} \right]$$
$$= -\frac{(1-z^s)}{1-(z-u)} \log_2 [1-z^s] + \frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[(1-u)^\ell - (z-u) \right]$$
$$+ \frac{1+(z-u)-z^s-(1-u)^\ell}{1-(z-u)} \log_2 \left[1+(z-u)-z^s-(1-u)^\ell \right]$$
$$= \frac{1+(z-u)-z^s-(1-u)^\ell}{1-(z-u)} \log_2 \left[1-(1-u)^\ell \right]$$
$$+ \frac{\ell((1-u)^\ell - (z-u))}{1-(z-u)} \log_2 [1-u]. \quad (1.2.33)$$

Пятое слагаемое

$$h(\upsilon_Q(\mathbf{1})) = -\frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[\frac{(1-u)^\ell - (z-u)}{1-(z-u)}\right] - \frac{(1-(1-u)^\ell)}{1-(z-u)} \log_2 \left[\frac{(1-(1-u)^\ell)}{1-(z-u)}\right]$$

$$= -\frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 \left[(1-u)^\ell - (z-u)\right] + \log_2 [1-(z-u)]$$

$$- \frac{(1-(1-u)^\ell)}{1-(z-u)} \log_2 \left[1-(1-u)^\ell\right] = -\frac{\ell((1-u)^\ell - (z-u))}{1-(z-u)} \log_2 [1-u]$$

$$- \frac{(1-u)^\ell - (z-u)}{1-(z-u)} \log_2 [1-z^s] + \log_2 [1-(z-u)]$$

$$- \frac{(1-(1-u)^\ell)}{1-(z-u)} \log_2 \left[1-(1-u)^\ell\right]. \quad (1.2.34)$$

Подстановка (1.2.30)-(1.2.34) в (1.2.29) и группировка подобных слагаемых дает

$$F\left(\tau_{Q(z,u)}, \upsilon_{Q(z,u)}, Q(z,u)\right) = T(z,u,s,\ell), \quad 0 < z,u < 1, \quad 2 \leqslant \ell \leqslant s, \quad (1.2.35)$$

где функция $T(z,u,s,\ell)$ определена следующим образом:

$$T(z,u,s,\ell) \triangleq \frac{su}{1-(z-u)} \log_2 z - \frac{\ell(1-z)}{1-(z-u)} \log_2 [1-z]$$

$$- \frac{su}{1-(z-u)} \log_2 u + \frac{\ell(1-z)}{1-(z-u)} \log_2[1-u] + (s+\ell-1) \log_2 [1-(z-u)]$$

$$= \frac{su}{1-(z-u)} \log_2 \left[\frac{z}{u}\right] + \frac{\ell(1-z)}{1-(z-u)} \log_2 \left[\frac{1-u}{1-z}\right] + (s+\ell-1) \log_2 [1-(z-u)]. \quad (1.2.36)$$

Поэтому из построения (1.2.12) границы случайного кодирования $\underline{R}(s,\ell)$, равенств (1.2.28) и формулы (1.2.35) следует, что скорость СП (s,ℓ)-кодов

$$R(s,\ell) \geqslant \underline{R}(s,\ell) \triangleq \frac{1}{s+\ell-1} \max_{\substack{(1.2.24) \\ 0<z,u<1}} T(z,u,s,\ell). \quad (1.2.37)$$

Утверждение 1 теоремы 1.2.2 доказано.

Перейдем к доказательству утверждения 2. Пусть $\ell \geqslant 2$ фиксировано и $s \to \infty$. Заменим в правой части (1.2.37) максимум по $\{z,u\}$, $0 < z,u < 1$, функции (1.2.7) на ее значение при $z = z' \triangleq 1 - \frac{c}{s}$, где c – некоторая константа. Значение $u = u'$ возьмем из уравнения

$$z - u = z^s (1-u)^\ell. \quad (1.2.38)$$

Далее для простоты вместо z' и u' будем писать z и u. Легко проверить, что

$$u = 1 - \frac{c}{s} - \frac{e^{-c}c^{\ell}}{s^{\ell}}\left(1 - \frac{c^2}{2s} + o\left(\frac{1}{s}\right)\right), \tag{1.2.39}$$

$$z - u = \frac{e^{-c}c^{\ell}}{s^{\ell}}\left(1 - \frac{c^2}{2s} + o\left(\frac{1}{s}\right)\right), \tag{1.2.40}$$

$$\frac{z}{u} = 1 + \frac{e^{-c}c^{\ell}}{s^{\ell}}\left(1 - \frac{c^2 - 2c}{2s} + o\left(\frac{1}{s}\right)\right), \tag{1.2.41}$$

$$\frac{1-u}{1-z} = 1 + \frac{e^{-c}c^{\ell-1}}{s^{\ell-1}}(1 + o(1)). \tag{1.2.42}$$

Непосредственно из определения (1.2.36) будем искать асимптотику каждого из слагаемого с точностью до $o(1/s^{\ell})$. В процессе приведения будем использовать (1.2.38)-(1.2.42). Итак,

$$T(z,u,s,\ell) = \log_2 e\left(s\left(1 - \frac{c}{s}\right)\frac{e^{-c}c^{\ell}}{s^{\ell}}\left(1 - \frac{c^2-2c}{2s}\right) + \frac{\ell e^{-c}c^{\ell}}{s^{\ell}}\right.$$
$$\left. -s\left(1 + \frac{\ell-1}{s}\right)\frac{e^{-c}c^{\ell}}{s^{\ell}}\left(1 - \frac{c^2}{2s}\right)\right) + o\left(\frac{1}{s^{\ell+1}}\right) = \frac{\log_2 e}{e^c}\frac{c^{\ell}}{s^{\ell}}(1 + o(1)).$$

Легко видеть, что максимум по x функции x^{ℓ}/e^x достигается при $x = \ell$. Откуда получаем

$$T(z',u',s,\ell) = \frac{\log_2 e}{e^{\ell}}\frac{\ell^{\ell}}{s^{\ell}}(1 + o(1)),$$

и

$$\underline{R}(s,\ell) \geqslant \frac{1}{s+\ell-1}T(z',u',s,\ell) = \frac{\log_2 e}{e^{\ell}}\frac{\ell^{\ell}}{s^{\ell}}(1 + o(1)), \quad s \to \infty,\ \ell \geqslant 2. \tag{1.2.43}$$

Для вычисления асимптотики (1.2.11) доли оптимального веса $Q(s,\ell)$ подставим в формулу (1.2.25) значение $z = 1 - \frac{\ell}{s}$ и получим

$$Q(s,\ell) = \frac{1-z}{1 - z^s(1-z)^{\ell}} = \frac{\ell}{s}(1 + o(1)), \quad s \to \infty.$$

Утверждение 2 теоремы 1.2.2 доказано.

Наконец, докажем утверждение 3. Пусть $\ell = s$ и $s \to \infty$. Заменим в правой части (1.2.37) максимум по z, $0 < z < 1$, и u, $0 < u < 1$, функции (1.2.7) на ее значение при $z' = 1 - u'$. Из уравнения

$$z - u = z^s(1-u)^{\ell}$$

получаем

$$z' = \frac{1}{2} + \left(\frac{1}{2}\right)^{2s+1}(1+o(1)), \qquad u' = \frac{1}{2} - \left(\frac{1}{2}\right)^{2s+1}(1+o(1)).$$

Непосредственно с помощью определения (1.2.7) выведем нижнюю границу

$$R(s,s) \geqslant \frac{1}{2s-1}T(z',u',s,s) = \frac{1}{2s-1}\Big(\frac{2su'}{1-(z'-u')}\log_2\left[\frac{z'}{u'}\right] + (2s-1)\log_2\left[1-(z'-u')\right]\Big) = \frac{\log_2 e}{2s}(z'-u')(1+o(1)) = \frac{\log_2 e}{s2^{2s+1}}(1+o(1)).$$

Утверждение 3 теоремы 1.2.2 доказано. □

1.3 Верхние оценки $R(s,\ell)$

Очевидно [28], что $R(s,1) \leqslant 1/s$, $s = 1,2,\ldots$, а нетривиальная верхняя граница скорости $R(s,1)$, которая до настоящего времени является наилучшей, была построена в 1982 году в работе [3]. Для описания этой границы, обозначаемой в данной работе символом $\overline{R}(s,1)$, $s = 1,2,\ldots$, и называемой *рекуррентной границей*, введем стандартное обозначение двоичной энтропии

$$h(v) \triangleq -v\,\log_2 v - (1-v)\log_2(1-v), \qquad 0 < v < 1, \tag{1.3.1}$$

и функцию

$$f_s(v) \triangleq h(v/s) - v\,h(1/s), \quad 0 < v < 1, \quad s = 1,2,\ldots, \tag{1.3.2}$$

аргумента v, $0 < v < 1$. В [3] показано (см. также [19]), что функция $f_s(v) > 0$, выпукла вверх и принимает максимальное значение:

$$\max_{0<v<1} f_s(v) = f_s(v_s) \quad \text{при} \quad v_s \triangleq \frac{s}{1+2^{s\cdot h\left(\frac{1}{s}\right)}}, \quad s = 1,2,\ldots. \tag{1.3.3}$$

Положим

$$\overline{R}(1,1) \triangleq 1, \quad \overline{R}(2,1) \triangleq \max_{0<v<1} f_2(v) = f_2(v_2) = 0322, \tag{1.3.4}$$

а далее последовательность $\overline{R}(s,1)$, $s = 3,4,\ldots$, определяется [3] как единственное решение рекуррентного уравнения

$$\overline{R}(s,1) = f_s\left(1 - \frac{\overline{R}(s,1)}{\overline{R}(s-1,1)}\right), \quad s = 3,4,\ldots. \tag{1.3.5}$$

В [3] была доказана следующая теорема.

Теорема 1.3.1. [3]. *Имеют место следующие два утверждения.*
1. *Скорость дизъюнктивных s-кодов $R(s,1)$ удовлетворяет неравенству*

$$R(s,1) \leqslant \overline{R}(s,1) \leqslant \frac{2\log_2[e(s+1)/2]}{s^2}, \qquad s = 2,3,\ldots, \tag{1.3.6}$$

где рекуррентная последовательность $\overline{R}(s,1)$ описывается с помощью (1.3.4)-(1.3.5).
2. *Если $s \to \infty$, то для верхней границы $\overline{R}(s,1)$ справедливо асимптотическое неравенство*

$$R(s,1) \leqslant \frac{2\log_2 s}{s^2}(1+o(1)). \tag{1.3.7}$$

Первые результаты исследования верхних границ скорости $R(s,\ell)$ для СП (s,ℓ)-кодов, $2 \leqslant \ell \leqslant s$, были получены в [19] и [36]. Одной из первых оценок для скорости $R(s,\ell)$ служит следующее неравенство

$$\frac{1}{R(s,\ell)} \geqslant \frac{1}{R(s,\ell-1)} + \frac{1}{R(s-1,\ell)}.$$

Отметим, что на сегодняшний момент в некоторых случаях, используя именно это неравенство, можно получить наиболее точную верхнюю границу $R(s,\ell)$.

В работе [5] для $R(s,\ell)$ было доказано неравенство

$$R(s,\ell) \leqslant \frac{R(s-i,\ell-j)}{R(s-i,\ell-j) + \frac{(i+j)^{i+j}}{i^i \cdot j^j}}, \quad i \in [s-1],\ j \in [\ell-1], \tag{1.3.8}$$

которое представляет собой уточнение неравенства

$$R(s,\ell) \leqslant R(s-i,\ell-j) \cdot \frac{i^i \cdot j^j}{(i+j)^{i+j}}, \quad i \in [s-1],\ j \in [\ell-1], \tag{1.3.9}$$

ранее установленного в [22]. Рекуррентное неравенство (1.3.8) и рекуррентная верхняя граница $\overline{R}(s,1)$, $s \geqslant 1$, определяемая (1.3.2)-(1.3.5), дают для скорости $R(s,\ell)$, $2 \leqslant \ell \leqslant s$ наилучшую известную верхнюю рекуррентную границу.

Теорема 1.3.2. *Имеют место следующие три утверждения.*
1. [5]. *Пусть $2 \leqslant \ell \leqslant s$. Тогда скорость СП (s,ℓ)-кодов удовлетворяет неравенству*

$$R(s,\ell) \leqslant \overline{R}(s,\ell) \triangleq \min_{\substack{i\in[s-1]\\ j\in[\ell-1]}} \frac{\overline{R}(s-i,\ell-j)}{\overline{R}(s-i,\ell-j) + \frac{(i+j)^{i+j}}{i^i \cdot j^j}}. \tag{1.3.10}$$

2. *Если $s \to \infty$ и $\ell \geqslant 2$ фиксировано, то для верхней границы $\overline{R}(s,\ell)$ справедливо асимптотическое неравенство*

$$R(s,\ell) \leqslant \overline{R}(s,\ell) \leqslant \frac{(\ell+1)^{\ell+1}}{2\,e^{\ell-1}} \cdot \frac{\log_2 s}{s^{\ell+1}} \cdot (1+o(1)). \tag{1.3.11}$$

3. *Для скорости $R(s,s)$ справедливо неравенство*

$$R(s,s) \leqslant \frac{1}{1+2^{2s-2}}. \tag{1.3.12}$$

Доказательство. Пусть $s \geqslant \ell \geqslant 2$. Если для фиксированного p, $0 < p < 1$, произведение sp – целое число, то положив в правой части неравенства (1.3.9) параметр $j \triangleq \ell - 1$, получим

$$R(s,\ell) \leqslant R(s(1-p),1) \cdot \frac{(ps)^{ps} \cdot (\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}}.$$

Если $s \to \infty$ и $\ell \geqslant 2$ фиксировано, то применяя для скорости $R(s(1-p),1)$ асимптотическое равенство (1.3.7), можем написать

$$R(s,\ell) \leqslant \min_{0<p<1} \left\{ \frac{2\log_2[s(1-p)]}{s^2(1-p)^2} \cdot \frac{(ps)^{ps}(\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}} \right\} (1+o(1))$$
$$= \frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}} \frac{\log_2 s}{s^{\ell+1}} (1+o(1)),$$

где учли, что

$$\max_{0<p<1} \left\{ (1-p)^2\, p^{\ell-1} \right\} = (\ell-1)^{\ell-1} \frac{4}{(\ell+1)^{\ell+1}},$$

и максимальное значение достигается при $p = \frac{\ell-1}{\ell+1}$.

Утверждение 2 теоремы 1.3.2 доказано.

Для получения верхней границы (1.3.12) воспользуемся рекуррентным неравенством (1.3.8). Подставив $i = j = s-1$, имеем

$$R(s,s) \leqslant \frac{R(1,1)}{R(1,1) + \frac{(2s-2)^{2s-2}}{(s-1)^{s-1} \cdot (s-1)^{s-1}}} = \frac{1}{1+2^{2s-2}}.$$

Утверждение 3 теоремы 1.3.2 доказано. □

1.4 Таблица наилучших границ $R(s,\ell)$

В таблице 1.1 при $\ell = 1$ и $2 \leqslant s \leqslant 10$ даны числовые значения верхней границы (1.3.5), а также нижней границы (1.2.1) скорости $R(s,1)$ вместе с долей

$Q(s)$ оптимального веса кодовых слов для ансамбля равновесных двоичных кодов. При $1 \leqslant \ell \leqslant s \leqslant 10$, в сводной таблице 1.1 также указаны верхняя граница $\overline{R}(s,\ell)$, определяемая правой частью (1.3.10), нижняя граница $\underline{R}(s,\ell)$ и соответствующая доля $Q(s,\ell)$ оптимального веса кодовых слов для ансамбля равновесных двоичных кодов в границе случайного кодирования из теоремы 1.2.2.

Таблица 1.1: Таблица значений для $\overline{R}(s,\ell)$ и $\underline{R}(s,\ell)$

(s,ℓ)	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$	$(7,1)$
$\overline{R}(s,\ell)$	$3.22\cdot10^{-1}$	$1.99\cdot10^{-1}$	$1.40\cdot10^{-1}$	$1.06\cdot10^{-1}$	$8.3\cdot10^{-2}$	$6.7\cdot10^{-2}$
$\underline{R}(s,\ell)$	$1.83\cdot10^{-1}$	$7.87\cdot10^{-2}$	$4.39\cdot10^{-2}$	$2.79\cdot10^{-2}$	$1.9\cdot10^{-2}$	$1.4\cdot10^{-2}$
$Q(s,\ell)$	0.26	0.19	0.15	0.12	0.10	0.09
(s,ℓ)	$(8,1)$	$(9,1)$	$(10,1)$	$(2,2)$	$(3,2)$	$(4,2)$
$\overline{R}(s,\ell)$	$5.59\cdot10^{-2}$	$4.73\cdot10^{-2}$	$4.07\cdot10^{-2}$	$1.61\cdot10^{-1}$	$7.5\cdot10^{-2}$	$4.6\cdot10^{-2}$
$\underline{R}(s,\ell)$	$1.09\cdot10^{-2}$	$8.58\cdot10^{-3}$	$6.94\cdot10^{-3}$	$3.66\cdot10^{-2}$	$1.4\cdot10^{-2}$	$6.9\cdot10^{-3}$
$Q(s,\ell)$	0.08	0.07	0.06	0.50	0.40	0.33
(s,ℓ)	$(5,2)$	$(6,2)$	$(7,2)$	$(8,2)$	$(9,2)$	$(10,2)$
$\overline{R}(s,\ell)$	$2.87\cdot10^{-2}$	$2.04\cdot10^{-2}$	$1.46\cdot10^{-2}$	$1.10\cdot10^{-2}$	$8.6\cdot10^{-3}$	$6.8\cdot10^{-3}$
$\underline{R}(s,\ell)$	$3.90\cdot10^{-3}$	$2.42\cdot10^{-3}$	$1.60\cdot10^{-3}$	$1.12\cdot10^{-3}$	$8.1\cdot10^{-4}$	$6.1\cdot10^{-4}$
$Q(s,\ell)$	0.28	0.24	0.22	0.20	0.18	0.16
(s,ℓ)	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$	$(7,3)$	$(8,3)$
$\overline{R}(s,\ell)$	$3.72\cdot10^{-2}$	$1.83\cdot10^{-2}$	$1.09\cdot10^{-2}$	$6.70\cdot10^{-3}$	$4.2\cdot10^{-3}$	$3.0\cdot10^{-3}$
$\underline{R}(s,\ell)$	$4.78\cdot10^{-3}$	$2.09\cdot10^{-3}$	$1.06\cdot10^{-3}$	$5.96\cdot10^{-4}$	$3.6\cdot10^{-4}$	$2.3\cdot10^{-4}$
$Q(s,\ell)$	0.50	0.42	0.37	0.33	0.30	0.27
(s,ℓ)	$(9,3)$	$(10,3)$	$(4,4)$	$(5,4)$	$(6,4)$	$(7,4)$
$\overline{R}(s,\ell)$	$2.13\cdot10^{-3}$	$1.54\cdot10^{-3}$	$9.14\cdot10^{-3}$	$4.55\cdot10^{-3}$	$2.6\cdot10^{-3}$	$1.6\cdot10^{-3}$
$\underline{R}(s,\ell)$	$1.55\cdot10^{-4}$	$1.08\cdot10^{-4}$	$8.20\cdot10^{-4}$	$3.76\cdot10^{-4}$	$1.9\cdot10^{-4}$	$1.1\cdot10^{-4}$
$Q(s,\ell)$	0.25	0.23	0.50	0.44	0.40	0.36
(s,ℓ)	$(8,4)$	$(9,4)$	$(10,4)$	$(5,5)$	$(6,5)$	$(7,5)$
$\overline{R}(s,\ell)$	$9.90\cdot10^{-4}$	$6.26\cdot10^{-4}$	$4.35\cdot10^{-4}$	$2.27\cdot10^{-3}$	$1.1\cdot10^{-3}$	$6.6\cdot10^{-4}$
$\underline{R}(s,\ell)$	$6.34\cdot10^{-5}$	$3.95\cdot10^{-5}$	$2.56\cdot10^{-5}$	$1.57\cdot10^{-4}$	$7.4\cdot10^{-5}$	$3.8\cdot10^{-5}$
$Q(s,\ell)$	0.33	0.31	0.29	0.50	0.45	0.42
(s,ℓ)	$(8,5)$	$(9,5)$	$(10,5)$	$(6,6)$	$(7,6)$	$(8,6)$
$\overline{R}(s,\ell)$	$3.74\cdot10^{-4}$	$2.29\cdot10^{-4}$	$1.44\cdot10^{-4}$	$5.68\cdot10^{-4}$	$2.8\cdot10^{-4}$	$1.5\cdot10^{-4}$
$\underline{R}(s,\ell)$	$2.08\cdot10^{-5}$	$1.21\cdot10^{-5}$	$7.36\cdot10^{-6}$	$3.21\cdot10^{-5}$	$1.5\cdot10^{-5}$	$7.8\cdot10^{-6}$
$Q(s,\ell)$	0.38	0.36	0.33	0.50	0.46	0.43
(s,ℓ)	$(9,6)$	$(10,6)$	$(7,7)$	$(8,7)$	$(9,7)$	$(10,7)$
$\overline{R}(s,\ell)$	$8.87\cdot10^{-5}$	$5.43\cdot10^{-5}$	$1.42\cdot10^{-4}$	$7.10\cdot10^{-5}$	$3.8\cdot10^{-5}$	$2.2\cdot10^{-5}$
$\underline{R}(s,\ell)$	$4.26\cdot10^{-6}$	$2.43\cdot10^{-6}$	$6.78\cdot10^{-6}$	$3.25\cdot10^{-6}$	$1.7\cdot10^{-6}$	$9.0\cdot10^{-7}$
$Q(s,\ell)$	0.40	0.37	0.50	0.47	0.44	0.41
(s,ℓ)	$(8,8)$	$(9,8)$	$(10,8)$	$(9,9)$	$(10,9)$	$(10,10)$
$\overline{R}(s,\ell)$	$3.55\cdot10^{-5}$	$1.77\cdot10^{-5}$	$9.34\cdot10^{-6}$	$8.87\cdot10^{-6}$	$4.4\cdot10^{-6}$	$2.2\cdot10^{-6}$
$\underline{R}(s,\ell)$	$1.47\cdot10^{-6}$	$7.09\cdot10^{-7}$	$3.62\cdot10^{-7}$	$3.24\cdot10^{-7}$	$1.6\cdot10^{-7}$	$7.2\cdot10^{-8}$
$Q(s,\ell)$	0.50	0.47	0.44	0.50	0.47	0.50

1.5 Конструкции СП (s, ℓ)-кодов

Тривиальный СП (s, ℓ)-код

Рассмотрим тривиальную конструкцию СП (s, ℓ)-кода. Пусть код X имеет t, $t \geqslant s + \ell$, столбцов и $\binom{t}{s}$ строк, каждая из которых уникальна и содержит в точности s нулей. Несложно проверить, что этот код является СП (s, ℓ)-кодом. В частности, при $t = (s+\ell)$ такая конструкция является оптимальной, т.е. имеет минимально возможное количество строк. Аналогичным образом можно показать, что код, который содержит всевозможные строки веса ℓ, является СП (s, ℓ)-кодом. Таким образом,

$$N(t, s, \ell) \leqslant \binom{t}{\min(s, \ell)}.$$

Матрицы инцидентности некоторых систем множеств

Следующая конструкция СП (s, ℓ)-кодов, которая будет описана, является обобщением конструкции, полученной Э. Макулой в [31].

Обозначим через $\mathcal{M}(n, k)$ множество всевозможных подмножеств мощности k множества $[n] = \{1, 2, \dots n\}$, а через $\mathcal{M}(n, s, \ell)$ – множество, состоящее из неупорядоченных наборов ℓ различных элементов множества $\mathcal{M}(n, s)$. Занумеруем элементы множеств $\mathcal{M}(n, s)$ и $\mathcal{M}(n, s, \ell)$. Пусть $s < k < n$. Через $X(k, s, \ell, n)$ обозначим двоичную матрицу с $N = |\mathcal{M}(n, s, \ell)|$ строками и $N = |\mathcal{M}(n, k)|$ столбцами, при этом (i, j)-й элемент двоичной матрицы положим равным 1 в том случае, если i-й набор из множества $\mathcal{M}(n, s, \ell)$ содержит хотя бы одно множество, полностью содержащееся в j-м элементе множества $\mathcal{M}(n, k)$.

Теорема 1.5.1. *Матрица $X(k, s, \ell, n)$ является СП (s, ℓ)-кодом с фиксированным весом столбцов.*

Доказательство. Рассмотрим произвольные множества $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и $\mathcal{L} \subset [t]$, $|\mathcal{L}| = \ell$, причем $\mathcal{S} \cap \mathcal{L} = \varnothing$. Рассмотрим соответствующие $\mathcal{S}$ и $\mathcal{L}$ элементы множества $\mathcal{M}(n, k)$: $K_1, \dots, K_s$ и $K'_1, \dots, K'_\ell$. Поскольку все элементы множества $\mathcal{M}(n, k)$ различны и одной мощности, то можно найти множества $\mathcal{S}_1, \dots, \mathcal{S}_\ell$ мощности s такие, что $\mathcal{S}_i \subset K'_i$ и $\mathcal{S}_i \subset K_j$ для всех $i \in [\ell]$ и $j \in [s]$. Тогда рассмотрим строчку матрицы $X(k, s, \ell, n)$, соответствующую набору $\{\mathcal{S}_1, \dots, \mathcal{S}_\ell\}$. В ее пересечении со столбцами с номерами из $\mathcal{S}$ стоят 0, а в ее пересечении с столбцами с номерами из $\mathcal{L}$ стоят 1. Несложно проверить, что число единиц в столбце не зависит от того, какому именно элементу $\mathcal{M}(n, k)$ он соответствует. □

Для того чтобы максимизировать объем кода $X(k, s, \ell, n)$, необходимо взять $k = \lfloor \frac{n}{2} \rfloor$. Таким образом,

$$N\left(\binom{n}{\lfloor n/2 \rfloor}, s, \ell\right) \leqslant \binom{\binom{n}{s}}{\ell}.$$

При $n \to \infty$ параметры кода $X(\lfloor n/2 \rfloor, s, \ell, n)$ принимают вид

$$t = 2^{n(1+o(1))}, \quad N = \frac{n^{s\ell}}{(s!)^{\ell}\ell!}(1 + o(1)). \tag{1.5.1}$$

В частности, легко видеть, что асимптотическая скорость такого семейства СП (s, ℓ)-кодов равна 0.

Коды, построенные с помощью МДР кодов

Следующим семейством конструкций СП (s, ℓ)-кодов будут коды, построенные [19] из q-ичных кодов с максимальным достижимым расстоянием. Также будут рассмотрена каскадные конструкции и для некоторых значений t будут найдены оптимальные значения N длин кодов, построенных таким образом.

Пусть q — целое числа, $q \geqslant 2$, $\mathbf{q} \triangleq \{0, 1, \ldots, q-1\}$ — стандартный q-ичный алфавит. Введем q-ичную матрицу X с t столбцами $\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(t)$ (кодовыми словами) и N строками:

$$X \triangleq \|x_i(j)\|, \; x_i(j) \in \mathbf{q},$$

$$\boldsymbol{x}(j) \triangleq (x_1(j), x_2(j), \ldots, x_N(j)) \in \mathbf{q}^N, \quad i \in [N], \; j \in [t]. \tag{1.5.2}$$

Далее матрицу X будем называть *q-ичным кодом длины N и объема t.*

Для любого фиксированного множества индексов $\mathcal{S}$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, *выпуклой оболочкой* $\langle \{\boldsymbol{x}(j), j \in \mathcal{S}\} \rangle$ соответствующего набора $\{\boldsymbol{x}(j), j \in \mathcal{S}\}$ из s кодовых слов будем называть множество всевозможных q-ичных слов длины N, у которых i-ый символ для любого i, $i \in [N]$, совпадает с i-ым символом какого-нибудь кодового слова из набора $\{\boldsymbol{x}(j), j \in \mathcal{S}\}$. Очевидно, что набор $\{\boldsymbol{x}(j), j \in \mathcal{S}\} \subseteq \langle \{\boldsymbol{x}(j), j \in \mathcal{S}\} \rangle$. Например, при $q = N = 3$ выпуклая оболочка двух слов $(0, 1, 2)$ и $(0, 0, 2)$ состоит из этих же слов, а выпуклая оболочка двух слов $(0, 1, 2)$ и $(0, 2, 1)$ состоит из четырех слов: $(0, 1, 2)$, $(0, 2, 1)$, $(0, 1, 1)$ и $(0, 2, 2)$.

Определение 1.5.1. [25]. Код X называется q-ичным разделяющим (s, ℓ)-кодом, если для любых двух непересекающихся множеств $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, их выпуклые оболочки не пересекаются. Другими словами, существует такой индекс $i \in [N]$, что координатные множества $\{x_i(j),\, j \in \mathcal{S}\} \subseteq \mathbf{q}$ и $\{x_i(j),\, j \in \mathcal{L}\} \subseteq \mathbf{q}$ не пересекаются.

Следующее утверждение является классическим для теории кодировании, и оно позволяет рассматривать каскадные конструкции.

Предложение 1.5.1. *Пусть $s \geqslant 1$, $\ell \geqslant 1$, $t \geqslant s+\ell$ и $q \geqslant s+\ell$ – целые числа. Предположим, что существует q-ичный разделяющий (s,ℓ)-код Y объема t и длины N_1. Пусть также существует СП (s,ℓ)-код Y' объема $t_2 \geqslant q$ и длины N_2. Тогда существует СП (s,ℓ)-код X объема t и длины $N = N_1 N_2$.*

Доказательство. Рассмотрим некоторое подмножество $\overline{Y}$ из q, $q \leqslant t_2$, кодовых слов СП (s,ℓ)-кода Y': $\overline{Y} = \{y'(1), \ldots, y'(q)\}$. Тогда зададим двоичную матрицу X объема t и длины $N_1 N_2$ следующим образом: заменим каждый q-ичный элемент матрицы Y соответствующим кодовым словом из множества $\overline{Y}$. Несложно проверить, что получившийся код X является СП (s,ℓ)-кодом. □

Определение 1.5.2. Линейный (q,k,n) код называется кодом с максимально достижимым расстоянием (МДР кодом), если объем этого кода $t = q^k$, длина равна n и минимальное расстояние Хэмминга равно $d = n - k + 1$.

Предложение 1.5.2. [7]. *Если $q^k \geqslant s + \ell$ и $n \geqslant s\ell(k-1)+1$, тогда любой МДР код с параметрами (q,k,n) является q-ичным разделяющим (s,ℓ)-кодом.*

Из предложений 1.5.1, 1.5.2 и существования q-ичного МДР кода, а именно кода Рида-Соломона с параметрами (q,n,k), где $n \leqslant (q+1)$, следует

Предложение 1.5.3. [19]. *Пусть $s \geqslant 1$, $\ell \geqslant 1$ и $\lambda \geqslant 1$ — целые числа, а $q \geqslant s\ell\lambda$ — степень простого числа. Тогда*

$$N(q^{\lambda+1}, s, \ell) \leqslant N(q, s, \ell)(s\ell\lambda + 1).$$

Отметим, что семейство свободных от перекрытий кодов, полученное посредством итерационного применения предложения (1.5.3) с $\lambda = \lfloor \frac{q}{s\ell} \rfloor$ имеет лучшее асимптотическое поведение параметров кода, чем было получено в (1.5.1). В частности, для любого фиксированного $\varepsilon > 0$ и $n \to \infty$ асимптотическое поведение объема t и длины N кодовых конструкций данного семейства удовлетворяет следующим соотношениям

$$t = 2^{n(1+o(1))}, \quad N \geqslant n^{(1+\varepsilon)}(1+o(1)).$$

Тем не менее несложно проверить, что асимптотическая скорость такого семейства СП (s,ℓ)-кодов равна 0.

Таблицу со значениями объема и длины конструкций классических дизъюнктивных кодов, построенных на укороченных кодах Рида-Соломона, можно найти в [17]. Исследование некоторых оптимальных конструкций и методов построения СП (s,ℓ)-кодов ($(s,\ell) = (2,2)$, $(s,\ell) = (2,3)$ и $(s,\ell) = (3,3)$) было проведено в [4, 29].

Предложение 1.5.4. [19, 29]. *Минимальная длина $N(t, s, \ell)$ для некоторых малых значениях s и ℓ имеет вид*

$$N(4,2,2) = 6, \quad N(5,2,2) = 10, \quad N(6,2,2) = N(8,2,2) = 14,$$

$$N(9,2,2) = 18, \quad N(10,2,3) = 30, \quad N(11,3,3) = 66,$$

а также для $N(t, s, \ell)$ верны следующие границы

$$N(12,2,3) \leqslant 45, \quad N(16,2,3) \leqslant 48, \quad N(21,2,3) \leqslant 56, \quad N(24,2,3) \leqslant 76.$$

Далее приведены таблицы, содержащие верхние оценки для $N(t, s, \ell)$, которые выводятся с помощью предложений 1.5.3 и 1.5.4 и конструкций тривиальных кодов.

Таблица 1.2: Таблица верхних границ для $N(t, 2, 2)$

$t =$	2^2	5	2^3	3^2	2^4	5^2	2^6	3^4	2^9
$N(t,2,2) \leqslant$	6	10	14	18	30	50	70	90	126
$t =$	3^6	2^{12}	2^{16}	2^{20}	5^{10}	2^{24}	5^{12}		
$N(t,2,2) \leqslant$	162	270	390	510	850	910	1050		

Таблица 1.3: Таблица верхних границ для $N(t, 3, 2)$

$t =$	5	6	7	2^3	10	12	2^4	21	24
$N(t,3,2) \leqslant$	10	15	21	28	30	45	48	56	76
$t =$	7^2	2^6	3^4	2^8	2^{12}	3^8	7^6		
$N(t,3,2) \leqslant$	147	196	252	336	624	1764	1911		

Таблица 1.4: Таблица верхних границ для $N(t, 3, 3)$

$t =$	6	7	2^3	11	12	13	14	15	2^4
$N(t,3,3) \leqslant$	20	35	56	66	220	286	364	455	560
$t =$	11^2	13^2	2^8	11^4	11^6	11^8	47^5		
$N(t,3,3) \leqslant$	660	2860	5600	6600	12540	18480	24420		

Таблица 1.5: Таблица верхних границ для $N(t, 4, 2)$

$t =$	6	2^3	3^2	11	13	17	19	2^6	3^4
$N(t, 3, 2) \leqslant$	15	28	36	55	78	136	171	252	324
$t =$	11^2	13^2	2^8	17^2	19^2	2^{12}	17^3		
$N(t, 3, 2) \leqslant$	495	702	1080	1224	1539	2040	2312		

Глава 2

Почти свободные от перекрытий коды

В этой главе будет рассмотрено определение почти свободных от перекрытий (s, ℓ)-кодов. Используя метод случайного кодирования на ансамбле двоичных равновесных кодов, будет установлена нижняя граница для пропускной способности почти свободных от перекрытий кодов. Развивая технику доказательства обобщенной границы Плоткина, будет доказана верхняя граница для пропускной способности почти свободных от перекрытий кодов. Полученные границы при малых значениях параметров s и ℓ будут приведены в сводной таблице. В последнем разделе данной главы будет произведен сравнительный анализ асимптотической скорости свободных от перекрытия кодов и пропускной способности почти свободных от перекрытий кодов. Далее перейдем к формальному описанию задачи.

2.1 Основные определения

Будем пользоваться терминологией и обозначениями, ранее введенными в 1 главе настоящей диссертации. Двоичный код X объема t и длины N будем также называть (N, R)-кодом, где параметр $R = \log_2 t/N$. Пусть

$$[x]^+ \triangleq \begin{cases} x & \text{при } x \geqslant 0, \\ 0 & \text{при } x < 0, \end{cases}$$

и

$$h(x) \triangleq -x \log_2 x - (1-x)\log_2(1-x), \quad 0 < x < 1,$$

обозначают положительную часть функции x и двоичную энтропию. Зафиксируем два натуральных числа s и ℓ такие, что $s + \ell \leqslant t$. Определим множество всевозможных s-подмножеств множества $[t]$:

$$\mathcal{P}_s(t) = \{\mathcal{S} : \quad \mathcal{S} \subset [t],\ |\mathcal{S}| = s\}.$$

Определение 2.1.1. Пусть $X = (\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(t))$ произвольный двоичный код длины N и объема t. Множество $\mathcal{S} \in \mathcal{P}_s(t)$ будем называть (s,ℓ)-*плохим* для кода X, если существует такое множество $\mathcal{L}$, $\mathcal{L} \subset [t] \backslash \mathcal{S}$, мощности $|\mathcal{L}| = \ell$, что

$$\bigvee_{j \in \mathcal{S}} \boldsymbol{x}(j) \succcurlyeq \bigwedge_{j \in \mathcal{L}} \boldsymbol{x}(j). \tag{2.1.1}$$

В остальных случаях будем говорить, что $\mathcal{S}$ является (s,ℓ)-*хорошим* множеством для кода X. Через $\mathbf{B}(s,\ell,X)$ ($\mathbf{G}(s,\ell,X)$) будем обозначать все (s,ℓ)-плохие ((s,ℓ)-хорошие) множества для кода X.

Тогда выполнены следующие неравенства на мощность соответствующих множеств

$$0 \leqslant |\mathbf{B}(s,\ell,X)| \leqslant \binom{t}{s}, \quad 0 \leqslant |\mathbf{G}(s,\ell,X)| \leqslant \binom{t}{s},$$
$$|\mathbf{B}(s,\ell,X)| + |\mathbf{G}(s,\ell,X)| = \binom{t}{s}.$$

Предложение 2.1.1. *Любое $(s,\ell+1)$-хорошее ((s,ℓ)-плохое) множество для кода X является (s,ℓ)-хорошим ($(s,\ell+1)$-плохим) для кода X. Таким образом, верны следующие включения:* $\mathbf{B}(s,\ell,X) \subset \mathbf{B}(s,\ell+1,X)$ *и* $\mathbf{G}(s,\ell+1,X) \subset \mathbf{G}(s,\ell,X)$.

Определение 2.1.2. Зафиксируем параметр ε, $0 \leqslant \varepsilon \leqslant 1$. Двоичный код X будем называть *почти свободным от перекрытий (s,ℓ)-кодом* с *вероятностью ошибки ε* (*ПСП (s,ℓ,ε)-кодом*), если

$$\frac{|\mathbf{B}(s,\ell,X)|}{\binom{t}{s}} \leqslant \varepsilon \quad \Longleftrightarrow \quad |\mathbf{G}(s,\ell,X)| \geqslant (1-\varepsilon)\binom{t}{s}. \tag{2.1.2}$$

Непосредственно из определений следует

Предложение 2.1.2. *Любой ПСП $(s,\ell+1,\varepsilon)$-код является ПСП (s,ℓ,ε)-кодом.*

Более того верно аналогичное свойство монотонности по параметру s, которое может быть записано в следующем виде.

Предложение 2.1.3. *Если X является ПСП (s,ℓ,ε)-кодом объема t и длины N, тогда существует ПСП $(s-1,\ell,\varepsilon)$-код X' объема $t-1$ и длины N.*

Доказательство. Пусть $\mathbf{B}(s,\ell,X,i) \triangleq \{\mathcal{S} : i \in S \in \mathbf{B}(s,\ell,X)\}$ обозначает совокупность всех (s,ℓ)-плохих множеств $\mathcal{S}$ для кода X, содержащих элемент

$i \in [t]$. Заметим, что тогда для мощностей $|\mathbf{B}(s,\ell,X,i)|$, $0 \leqslant |\mathbf{B}(s,\ell,X,i)| \leqslant \binom{t-1}{s-1}$, $i \in [t]$, выполнено

$$\sum_{i=1}^{t} |\mathbf{B}(s,\ell,X,i)| = s \cdot |\mathbf{B}(s,\ell,X)| \leqslant s \binom{t}{s} \varepsilon,$$

причем в неравенстве воспользовались определением 2.1.2. Отсюда следует, что существует такое $j \in [t]$, для которого

$$|\mathbf{B}(s,\ell,X,j)| \leqslant \frac{1}{t}\, s \binom{t}{s} \varepsilon = \binom{t-1}{s-1} \varepsilon.$$

Тогда несложно видеть, что X', полученный из X удалением столбца $\boldsymbol{x}(j)$, является ПСП $(s-1,\ell,\varepsilon)$-кодом объема $t-1$ и длины N. □

Пользуясь классической терминологией [9, 26], дадим следующее определение.

Определение 2.1.3. Зафиксируем параметр R, $R > 0$. Ввиду неравенства (2.1.2) определим *ошибку* для ПСП (s,ℓ,ε)-кодов:

$$\varepsilon(s,\ell,R,N) \triangleq \min_{X\,:\,t=\lceil 2^{RN}\rceil} \left\{ \frac{|\mathbf{B}(s,\ell,X)|}{\binom{t}{s}} \right\}, \quad R > 0, \tag{2.1.3}$$

где минимум взят по всем (N,R)-кодам X. Функцию

$$\mathbf{E}(s,\ell,R) \triangleq \varliminf_{N\to\infty} \frac{-\log_2 \varepsilon(s,\ell,R,N)}{N}, \quad R > 0, \tag{2.1.4}$$

назовем *экспонентой ошибки* для ПСП (s,ℓ)-кодов, а число

$$C(s,\ell) \triangleq \sup\{R :\ \mathbf{E}(s,\ell,R) > 0\} \tag{2.1.5}$$

будем называть *пропускной способностью* ПСП (s,ℓ)-кодов.

Из определений 2.1.1 - 2.1.3 и предложений 2.1.1-2.1.3 вытекает

Теорема 2.1.1. *Имеют место следующие неравенства*

$$C(s+1,\ell) \leqslant C(s,\ell) \leqslant C(s,\ell-1). \tag{2.1.6}$$

2.2 Нижние оценки $C(s,\ell)$

Из доказанных ранее оценок выделим границу случайного кодирования для величины $C(s,1)$, полученную в работе [38].

Теорема 2.2.1. [38]. *Имеют место следующие два утверждения.*
1. *Пропускная способность $C(s,1)$ для ПСП $(s,1)$-кодов удовлетворяет неравенству*

$$C(s,1) \geqslant \underline{C}(s,1) \triangleq \max_{0<Q<1} C(s,1,Q) = C(s,1,Q(s)), \qquad s \geqslant 1, \tag{2.2.1}$$

$$C(s,1,Q) \triangleq h(Q) - [1-(1-Q)^s]\, h\left(\frac{Q}{1-(1-Q)^s}\right), \quad s \geqslant 1, \quad 0<Q<1, \tag{2.2.2}$$

2. *При $s \to \infty$ асимптотика границы случайного кодирования $\underline{C}(s,1)$, задаваемой (2.2.1) – (2.2.2), и асимптотика оптимального значения $Q(s)$ в (2.2.1) имеют вид:*

$$\underline{C}(s,1) = \frac{\ln 2}{s}(1+o(1)), \quad Q(s) = \frac{\ln 2}{s}(1+o(1)). \tag{2.2.3}$$

Одним из центральным результатов настоящей работы является следующая теорема, при доказательстве которой развивается метод, ранее используемый в [16]. Будет получена граница случайного кодирования для $C(s,\ell)$ при $\ell \geqslant 2$, численные значения которой при малых значениях параметров s и ℓ указаны в таблице 2.1. Также в теореме произведен анализ асимптотики полученной границы при фиксированном ℓ и $s \to \infty$.

Теорема 2.2.2. (Граница случайного кодирования $\underline{C}(s,\ell)$). *Имеют место следующие два утверждения.*
1. *Для $\ell \geqslant 2$ пропускная способность $C(s,\ell)$ ПСП (s,ℓ)-кодов удовлетворяет неравенству*

$$C(s,\ell) \geqslant \underline{C}(s,\ell) \triangleq \frac{1}{\ell} \max_{0 \leqslant Q \leqslant 1} \mathcal{D}(\ell,Q,\hat{q}), \tag{2.2.4}$$

где функция $\mathcal{D}(\ell,Q,\hat{q})$ задана следующим образом

$$\mathcal{D}(\ell,Q,\hat{q}) \triangleq (1-Q)\ell \log_2 z - (1-\hat{q}) \log_2[1-(1-z)^\ell] \tag{2.2.5}$$
$$+\ell\left(\frac{(1-Q)}{z}(1-z) - \left(\frac{(1-Q)}{z} - \hat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q),$$

а параметры z и $\hat{q}$ задаются как решения следующих уравнений

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\hat{q})z(1-z)^\ell}{1-(1-z)^\ell}, \qquad \hat{q} = 1-(1-Q)^s. \tag{2.2.6}$$

2. *Для фиксированного параметра $\ell \geqslant 2$ и при $s \to \infty$ нижняя асимптотическая граница для $C(s,\ell)$ имеет вид*

$$C(s,\ell) \;\geqslant\; \frac{\ell^{\ell-1}}{e^{\ell}} \frac{\log_2 e}{s^{\ell}} \,(1+o(1)). \tag{2.2.7}$$

Доказательство. Сначала докажем утверждения 1. Для произвольного кода X число (s,ℓ)-плохих множеств для кода X может быть представлено в виде

$$|\mathbf{B}(s,\ell,X)| \triangleq \sum_{\mathcal{S}\in\mathcal{P}_s(t)} \psi(X,\mathcal{S}),$$

$$\text{где индикатор } \psi(X,\mathcal{S}) \;\triangleq\; \begin{cases} 1 & \text{если множество } \mathcal{S}\in\mathbf{B}(s,\ell,X), \\ 0 & \text{в противном случае.} \end{cases} \tag{2.2.8}$$

Зафиксируем параметры Q, $0<Q<1$, и R, $0<R<1$. Определим ансамбль $E(N,t,Q)$, состоящий из двоичных $(N\times t)$-матриц $X=(\boldsymbol{x}(1),\boldsymbol{x}(2),\ldots\boldsymbol{x}(t))$, где столбцы $\boldsymbol{x}(i)$, $i\in[t]$, $t\triangleq\lfloor 2^{RN}\rfloor$, выбираются независимо и равновероятно из множества $\binom{N}{\lfloor QN\rfloor}$ столбцов фиксированного веса $\lfloor QN\rfloor$. Зафиксируем также два множества $\mathcal{S},\mathcal{L}\subset[t]$, таких что $|\mathcal{S}|=s$, $|\mathcal{L}|=\ell$ и $\mathcal{S}\cap\mathcal{L}=\varnothing$. Из (2.2.8) вытекает, что в ансамбле $E(N,t,Q)$ математическое ожидание $\overline{|\mathbf{B}(s,\ell,X)|}$ числа $|\mathbf{B}(s,\ell,X)|$ равно

$$\overline{|\mathbf{B}(s,\ell,X)|} \;=\; |\mathcal{P}_s(t)|\,\Pr\{\mathcal{S}\in\mathbf{B}(s,\ell,X)\}\,.$$

Таким образом, математическое ожидание вероятности ошибки для ПСП (s,ℓ)-кодов равно

$$\mathcal{E}^{(N)}(s,\ell,R,Q) \triangleq\; |\mathcal{P}_s(t)|^{-1}\,\overline{|\mathbf{B}(s,\ell,X)|} =\; \Pr\{\mathcal{S}\in\mathbf{B}(s,\ell,X)\}\,, \tag{2.2.9}$$

где число $t=\lfloor 2^{RN}\rfloor$. Тогда очевидная *случайная верхняя граница* для вероятности ошибки (2.1.3) для ПСП (s,ℓ)-кодов может быть записана следующим образом:

$$\varepsilon(s,\ell,R,N) \triangleq \min_{X\,:\,t=\lfloor 2^{RN}\rfloor} \left\{\frac{|\mathbf{B}(s,\ell,X)|}{|\mathcal{P}_s(t)|}\right\} \leqslant \mathcal{E}^{(N)}(s,\ell,R,Q) \quad \text{для } 0<Q<1. \tag{2.2.10}$$

Математическое ожидание $\mathcal{E}^{(N)}(s,\ell,R,Q)$, определяемое в (2.2.9), может быть представлено в виде

$$\mathcal{E}^{(N)}(s,\ell,R,Q) \;=\; \sum_{k=\lfloor QN\rfloor}^{\min\{N,\,s\lfloor QN\rfloor\}} \Pr\left\{\mathcal{S}\in\mathbf{B}(s,\ell,X) \,\middle/\, \left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right| = k\right\}$$

$$\times\mathcal{P}_2^{(N)}(s,Q,k) \leqslant \sum_{k=\lfloor QN\rfloor}^{\min\{N,\,s\lfloor QN\rfloor\}} \mathcal{P}_2^{(N)}(s,Q,k)\cdot\min\left\{1,\,\binom{t-s}{\ell}\mathcal{P}_1^{(N)}(\ell,Q,k)\right\}, \tag{2.2.11}$$

где мы воспользовались формулой полной вероятности и стандартной оценкой

$$\Pr\left\{\bigcup_i C_i\ /C\right\} \leqslant \min\left\{1,\,\sum_i \Pr\{C_i/C\}\right\},$$

а также ввели следующие обозначения

$$\mathcal{P}_1^{(N)}(\ell,Q,k) \triangleq \Pr\left\{\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i) \succcurlyeq \bigwedge_{j\in\mathcal{L}}\boldsymbol{x}(j)\ \Big/\ \left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right| = k\right\} \tag{2.2.12}$$

и

$$\mathcal{P}_2^{(N)}(s,Q,k) \triangleq \Pr\left\{\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right| = k\right\}, \quad \lfloor QN\rfloor \leqslant k \leqslant \min\{N, s\lfloor QN\rfloor\}. \tag{2.2.13}$$

Пусть $k \triangleq \lfloor qN\rfloor$. Определим функции

$$\mathcal{D}(\ell,Q,q) \triangleq \lim_{N\to\infty}\frac{-\log_2\left[\mathcal{P}_1^{(N)}(\ell,Q,k)\right]}{N} \tag{2.2.14}$$

и

$$\mathcal{A}(s,Q,q) \triangleq \lim_{N\to\infty}\frac{-\log_2\left[\mathcal{P}_2^{(N)}(s,Q,k)\right]}{N} \tag{2.2.15}$$

как экспоненты логарифмической асимптотики вероятности событий (2.2.12) и (2.2.13) в ансамбле $E(N,t,Q)$. Обозначим $\hat{q} \triangleq 1-(1-Q)^s$.

Лемма 2.2.1. *Функция $\mathcal{A}(s,Q,q)$ параметра q, $Q<q<\min\{1,sQ\}$, определяемая в* (2.2.15)*, может быть записана в параметрической форме*

$$\mathcal{A}(s,Q,q) \triangleq (1-q)\log_2(1-q)+q\log_2\left[\frac{Qy^s}{1-y}\right]+sQ\log_2\frac{1-y}{y}+sh(Q), \tag{2.2.16}$$

$$q = Q\frac{1-y^s}{1-y}, \qquad 0<y<1. \tag{2.2.17}$$

Более того, функция $\mathcal{A}(s,Q,q)$ является $\cup$-выпуклой, монотонно убывающей в интервале $(Q,1-(1-Q)^s)$, монотонно возрастающей в интервале $(1-(1-Q)^s,\min\{1,sQ\})$ и свой единственный минимум, равный 0, достигает в точке $q=\hat{q}\triangleq 1-(1-Q)^s$, т.е.

$$\min_{Q<q<\min\{1,sQ\}}\mathcal{A}(s,Q,q) = \mathcal{A}(s,Q,\hat{q}) = 0, \quad 0<Q<1.$$

Доказательство этой леммы будет проведено в следующем разделе.

Лемма 2.2.2. *Для $\ell \geqslant 2$ значение функции $\mathcal{D}(\ell, Q, q)$, определяемой в (2.2.14), в точке $q = \hat{q}$ равно*

$$\mathcal{D}(\ell, Q, \hat{q}) = (1-Q)\,\ell\,\log_2 z - (1-\hat{q})\log_2[1-(1-z)^\ell] +$$

$$+\ell\left(\frac{(1-Q)}{z}(1-z) - \left(\frac{(1-Q)}{z} - \hat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q),$$

где z единственным образом определяется из следующего уравнения

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\hat{q})z(1-z)^\ell}{1-(1-z)^\ell}.$$

Доказательство этой леммы будет проведено в следующем разделе.

Неравенство (2.2.11) и граница случайного кодирования (2.2.10) дают оценку для экспоненты вероятности ошибки (2.1.4)

$$\mathbf{E}(s, \ell, R) \geqslant \underline{\mathbf{E}}(s, \ell, R) \triangleq \max_{0 \leqslant Q \leqslant 1} E(s, \ell, R, Q), \tag{2.2.18}$$

$$E(s, \ell, R, Q) \triangleq \min_{Q < q < \min\{1, sQ\}} \left\{\mathcal{A}(s, Q, q) + [\mathcal{D}(\ell, Q, q) - \ell\, R]^+\right\}. \tag{2.2.19}$$

Из леммы 2.2.1 следует, что $\mathcal{A}(s, Q, q) > 0$ при $q \neq \hat{q}$. В частности, условие $q \neq \hat{q}$ влечет $E(s, \ell, R, Q) > 0$. Откуда имеем, что при $\ell\, R < \mathcal{D}(\ell, Q, \hat{q})$ выполнено $E(s, \ell, R, Q) > 0$, что в свою очередь означает (см. (2.1.5) и (2.2.18)), что

$$C(s, \ell) \geqslant \underline{C}(s, \ell) \triangleq \frac{1}{\ell} \max_{0 \leqslant Q \leqslant 1} \mathcal{D}(\ell, Q, \hat{q}), \quad \text{где } \hat{q} = 1 - (1-Q)^s.$$

Утверждение 1 теоремы 2.2.2 доказано.

Теперь докажем утверждение 2. Пусть параметр $\ell \geqslant 2$ зафиксирован, а $s \to \infty$. Подставляя $z = s/(s+\ell)$ в (2.2.4)-(2.2.6), получаем

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\hat{q})z(1-z)^\ell}{1-(1-z)^\ell} = \frac{\ell}{s+\ell} - \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\left(\frac{1}{s^{\ell+1}}\right),$$

$$\hat{q} = 1 - (1-Q)^s = 1 - e^{-\frac{s\ell}{s+\ell} + O\left(\frac{1}{s}\right)} = 1 - e^{-\ell} + O\left(\frac{1}{s}\right)$$

и

$$C(s, \ell) \geqslant \frac{1}{\ell} \max_{0 \leqslant Q \leqslant 1} \mathcal{D}(\ell, Q, \hat{q}) = \frac{1}{\ell} \max_{0 \leqslant z \leqslant 1} \mathcal{D}(\ell, Q(z), \hat{q}(z))$$

$$\geqslant \frac{1}{\ell}\mathcal{D}(\ell, Q(s/(s+\ell)), \hat{q}(s/(s+\ell))),$$

где

$$\mathcal{D}(\ell, Q, \hat{q}) \triangleq (1-Q)\,\ell\,\log_2 z - (1-\hat{q})\log_2[1-(1-z)^\ell] + \ell\left(\frac{(1-Q)}{z}(1-z) - \left(\frac{(1-Q)}{z} - \hat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q).$$

Тогда можно записать

$$C(s,\ell) \geqslant \left(\frac{s}{s+\ell} + \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\left(\frac{1}{s^{\ell+1}}\right)\right)\log_2\left[\frac{s}{s+\ell}\right] - \left(\frac{e^{-\ell}}{\ell} + O\left(\frac{1}{s}\right)\right)$$
$$\times \log_2\left[1-\left(\frac{\ell}{s+\ell}\right)^\ell\right] + \left(1+O\left(\frac{1}{s^\ell}\right)\right)\frac{\ell}{s+\ell}\log_2\left[\frac{\ell}{s+\ell}\right] - \left(e^{-\ell} + O\left(\frac{1}{s}\right)\right)$$
$$\times\left(\frac{\ell}{s+\ell}\right)^\ell \log_2\left[\frac{\ell}{s+\ell}\right] - \left(\frac{\ell}{s+\ell} - \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\left(\frac{1}{s^{\ell+1}}\right)\right)$$
$$\times \log_2\left[\frac{\ell}{s+\ell} - \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\left(\frac{1}{s^{\ell+1}}\right)\right] - \left(\frac{s}{s+\ell} + \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\left(\frac{1}{s^{\ell+1}}\right)\right)$$
$$\times \log_2\left[\frac{s}{s+\ell} + \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\left(\frac{1}{s^{\ell+1}}\right)\right] = \frac{\ell^{\ell-1}\log_2 e}{e^\ell\, s^\ell} + O\left(\frac{\log_2 s}{s^{\ell+1}}\right),$$

Утверждение 2 теоремы 2.2.2 доказано. □

Доказательство вспомогательных лемм

Доказательство леммы 2.2.1. Посчитаем вероятность

$$\mathcal{P}_2^{(N)}(s,Q,k) \triangleq \Pr\left\{\left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}, \quad \lfloor QN\rfloor \leqslant k \leqslant \min\{N, s\lfloor QN\rfloor\}.$$

Зафиксируем $s \geqslant 2$, а также параметры Q и q, $0 < Q < 1$, $Q < q < \min\{1, sQ\}$. Положим $k = \lfloor qN\rfloor$ и устремим $N \to \infty$. Для каждого типа $\{n(\mathbf{a})\}$ рассмотрим соответствующее распределение $\tau : \tau(\mathbf{a}) = \frac{n(\mathbf{a})}{N}, \quad \forall\ \mathbf{a} \in \{0,1\}^s$.

Воспользовавшись формулой Стирлинга, получим следующую логарифмическую асимптотику вероятности (2.2.13)

$$-\log_2 \frac{N!}{\prod_{\mathbf{a}} n(\mathbf{a})!}\binom{N}{\lfloor QN\rfloor}^{-s} = NF(\tau,Q,q)(1+o(1)),$$

где

$$F(\tau,Q,q) = \sum_{\mathbf{a}} \tau(\mathbf{a})\log_2\tau(\mathbf{a}) + sH(Q). \tag{2.2.20}$$

Таким образом, для подсчета величины $\mathcal{A}(s,Q,q)$ необходимо найти следующий минимум

$$\mathcal{A}(s,Q,q) = \min_{\tau\in\ (2.2.22)-(2.2.23)} F(\tau,Q,q), \tag{2.2.21}$$

$$\tau:\ 0<\tau(\mathbf{a})<1 \quad \forall\ \mathbf{a}=(a_1,\ldots,a_s)\in\{0,1\}^s, \tag{2.2.22}$$

$$\sum_{\mathbf{a}}\tau(\mathbf{a})=1, \qquad \tau(\boldsymbol{0})=1-q,$$

$$\sum_{\mathbf{a}:a_i=1}\tau(\mathbf{a})=Q \quad \forall\ i\in[s], \tag{2.2.23}$$

причем ограничения (2.2.23) индуцированы условиями, налагаемыми на типы, а также следующим свойством: дизъюнктивная сумма s столбцов имеет вес $\lfloor qN\rfloor$.

Для нахождения минимума и экстремального вероятностного распределения будем использовать метод множителей Лагранжа. Запишем Лагранжиан

$$\Lambda \triangleq \sum_{\tau(\mathbf{a})}\tau(\mathbf{a})\log_2\tau(\mathbf{a}) + sh(Q) + \lambda_0\left(\tau(\boldsymbol{0})+q-1\right) + \sum_{i=1}^{s}\lambda_i\left(\sum_{\mathbf{a}:a_i=1}\tau(\mathbf{a})-Q\right)+\lambda_{s+1}\left(\sum_{\mathbf{a}}\tau(\mathbf{a})-1\right).$$

Тогда выпишем необходимые условия для экстремального распределения

$$\begin{cases}\frac{\partial\Lambda}{\partial\tau(\boldsymbol{0})}=\log_2\tau(\boldsymbol{0})+\log_2 e+\lambda_0+\lambda_{s+1}=0,\\ \frac{\partial\Lambda}{\partial\tau(\mathbf{a})}=\log_2\tau(\mathbf{a})+\log_2 e+\lambda_{s+1}+\sum_{i=1}^{s}a_i\lambda_i=0 \quad \text{для любого } \mathbf{a}\neq\boldsymbol{0}.\end{cases} \tag{2.2.24}$$

Несложно проверить, что матрица из вторых производных Лагранжиана является диагональной и положительно определенной в области (2.2.22). Следовательно, функция $F(\tau,Q)$ является строго $\cup$-выпуклой в области (2.2.22).

Далее воспользуемся теоремой Каруша-Куна-Таккера [2], утверждающей, что всякое решение $\tau\in$ (2.2.35), удовлетворяющее системе (2.2.24), ограничениям (2.2.23) и имеющее положительно определенную матрицу вторых производных лагранжиана в этой точке, является локальным минимумов функции $F(\tau,Q)$. Таким образом, если есть решение системы (2.2.24), (2.2.23) в области (2.2.22), то оно единственно, и эта точка является решением в задаче минимизации (2.2.21)–(2.2.23).

Также заметим, что из симметрии задачи вытекают равенства $v\triangleq\lambda_1=\lambda_2=\cdots=\lambda_s$. Для краткости введем параметры $u\triangleq\log_2 e+\lambda_{s+1}$ и $w\triangleq\lambda_0$.

Тогда уравнения (2.2.23) и (2.2.24) принимают вид

$$\begin{cases} 1)\ \log_2 \tau(\mathbf{a}) + u + v\sum_{i=1}^{s} a_i = 0 \quad \text{при } \mathbf{a} \neq \boldsymbol{0}, \\ 2)\ \log_2 \tau(\boldsymbol{0}) + u + w = 0, \\ 3)\ \tau(\boldsymbol{0}) = 1 - q, \\ 4)\ \sum_{\mathbf{a}} \tau(\mathbf{a}) = 1, \\ 5)\ \sum_{\mathbf{a}:a_i=1} \tau(\mathbf{a}) = Q \quad \text{при } i \in [s]. \end{cases} \tag{2.2.25}$$

Используя обозначение $y \triangleq \frac{1}{1+2^{-v}}$, перепишем первое уравнение

$$\tau(\mathbf{a}) = \frac{1}{2^u y^s}(1-y)^{\sum a_j} y^{s-\sum a_j} \quad \text{при } \mathbf{a} \neq \boldsymbol{0}. \tag{2.2.26}$$

Подставив (2.2.26) в пятое уравнение системы (2.2.25), получаем

$$\sum_{\mathbf{a}:a_i=1} \frac{1}{2^u y^s}(1-y)^{\sum a_j} y^{s-\sum a_j} = \frac{1-y}{2^u y^s}.$$

Откуда находим

$$u = \log_2 \frac{1-y}{Qy^s}. \tag{2.2.27}$$

Подстановка (2.2.26), (2.2.27) и третьего уравнения системы (2.2.25) в четвертое уравнение системы (2.2.25) дает

$$q(y) = \sum_{\mathbf{a}\neq 0} \tau(\mathbf{a}) = \frac{Q(1-y^s)}{1-y},$$

т.е. в точности уравнение (2.2.17). Таким образом, ограничения (2.2.23) и условия (2.2.24) дают единственное решение τ в области (2.2.22):

$$\tau(\boldsymbol{0}) = 1 - q, \qquad \tau(\mathbf{a}) = \frac{Q}{1-y}(1-y)^{\sum a_j} y^{s-\sum a_j} \quad \text{при } \mathbf{a} \neq \boldsymbol{0}, \tag{2.2.28}$$

где параметры q и y связаны соотношением (2.2.17). Для того чтобы получить точную формулу (2.2.16), достаточно подставить (2.2.28) в (2.2.20).

Теперь докажем, что верны некоторые свойства функции $A(s,Q,q)$, указанные в лемме. Легко видеть, что функция $q(y)$ является убывающей по y при $y \in (0,1)$ и принимает значения Q и sQ на концах этого интервала. Поэтому вместо (2.2.16) можно рассмотреть функцию $\mathcal{T}(s,Q,y) = \mathcal{A}(s,Q,q(y))$ параметра y на интервале $y \in (0,y_1)$, причем $q(y_1) = \min\{1, sQ\}$. Найдем производную функции $\mathcal{T}(s,Q,y)$ по переменной y

$$\frac{\partial \mathcal{T}(s,Q,y)}{\partial y} = q'(y)\log_2\left[\frac{Qy^s}{1-Q-y+Qy^s}\right]. \tag{2.2.29}$$

Откуда получаем, что функция $\mathcal{T}(s,Q,y)$ является убывающей по y при $y \in (0, 1-Q)$, возрастающей при $y \in (1-Q, y_1)$, а также $\cup$-выпуклой. Несложно проверить, что в точке точке $y_0 = 1-Q$ функция достигает свой минимум, равный нулю.

Лемма 2.2.1 доказана. $\square$

Доказательство леммы 2.2.2. Посчитаем условную вероятность

$$\mathcal{P}_1^{(N)}(\ell,Q,k) \triangleq \Pr\left\{ \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succcurlyeq \bigwedge_{j\in\mathcal{L}} \boldsymbol{x}(j) \;\Big/\; \left| \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \right| = k \right\}$$

Зафиксируем q, $Q \leqslant q \leqslant \min\{1, sQ\}$, а также определим $k \triangleq \lfloor qN \rfloor$, $\lfloor QN \rfloor \leqslant k \leqslant s\lfloor QN \rfloor$. Используя терминологию типов из [9]

$$\{n(\mathbf{a})\}, \quad \mathbf{a} \triangleq (a_1, a_2, \ldots, a_s) \in \{0,1\}^s, \quad 0 \leqslant n(\mathbf{a}) \leqslant N, \quad \sum_{\mathbf{a}} n(\mathbf{a}) = N, \tag{2.2.30}$$

запишем вероятность $\mathcal{P}_1^{(N)}(\ell,Q,k)$ в ансамбле $E(N,t,Q)$ в виде суммы

$$\mathcal{P}_1^{(N)}(\ell,Q,k) = \sum_{(2.2.32)} \frac{N!}{\prod\limits_{\mathbf{a}\in\{0,1\}^\ell} n(\mathbf{a})!} \frac{\binom{k}{n(\boldsymbol{1})}}{\binom{N}{n(\boldsymbol{1})}} \binom{N}{\lfloor QN \rfloor}^{-\ell}, \tag{2.2.31}$$

где в правой части (2.2.31) сумма взята по всем таким типам $\{n(\mathbf{a})\}$, что

$$\sum_{\mathbf{a}\colon a_i = 1} n(\mathbf{a}) = \lfloor QN \rfloor \quad \text{для всех } i \in [\ell]. \tag{2.2.32}$$

Воспользовавшись формулой Стирлинга, получим следующую логарифмическую асимптотику слагаемого в (2.2.31)

$$\log_2 \left[\frac{N!}{\prod\limits_{\mathbf{a}\in\{0,1\}^\ell} n(\mathbf{a})!} \frac{\binom{k}{n(\boldsymbol{1})}}{\binom{N}{n(\boldsymbol{1})}} \binom{N}{\lfloor QN \rfloor}^{-\ell} \right] = 2^{-NF(\tau,Q,q)(1+o(1))},$$

где

$$F(\tau,Q,q) \triangleq \sum_{\mathbf{a}\in\{0,1\}^\ell} \tau(\mathbf{a}) \log_2 \tau(\mathbf{a}) - q \cdot h\left(\frac{\tau(\boldsymbol{1})}{q}\right) + h(\tau(\boldsymbol{1})) + \ell \cdot h(Q). \tag{2.2.33}$$

Здесь *вероятностное распределение* $\{\tau(\mathbf{a})\}$, $a \in \{0,1\}^\ell$ определено следующим образом

$$\tau(\mathbf{a}) \triangleq \frac{n(\mathbf{a})}{N} \quad \text{для всех } \mathbf{a} \in \{0,1\}^\ell.$$

Таким образом, для вычисления $\mathcal{D}(\ell, Q, q)$, определяемого как

$$\mathcal{D}(\ell, Q, q) = \lim_{N\to\infty} -\frac{\log_2\left[P_1^{(N)}(\ell, Q, k)\right]}{N},$$

необходимо решить задачу минимизации

$$\mathcal{D}(\ell, Q, q) = \min_{\tau\in\ (2.2.35):\ (2.2.36)} F(\tau, Q, q) \triangleq F(\hat{\tau}, Q, q), \tag{2.2.34}$$

$$\left\{\tau:\ \forall\ \mathbf{a} = (a_1, \ldots, a_\ell) \in \{0,1\}^\ell \quad 0 < \tau(\mathbf{a}) < 1\right\}, \tag{2.2.35}$$

$$\sum_{\mathbf{a}} \tau(\mathbf{a}) = 1, \qquad \sum_{\mathbf{a}:\, a_i=1} \tau(\mathbf{a}) = Q \quad \text{для всех } i \in [\ell], \tag{2.2.36}$$

где ограничения (2.2.36) естественным образом получены из условий (2.2.30) и (2.2.32).

Для нахождения минимума и экстремального вероятностного распределения $\{\hat{\tau}(\mathbf{a})\}$ будем использовать метод множителей Лагранжа. Запишем Лагранжиан

$$\Lambda \triangleq \sum_{\mathbf{a}\in\{0,1\}^\ell} \tau(\mathbf{a}) \log_2 \tau(\mathbf{a}) - q \cdot h\left(\frac{\tau(\boldsymbol{1})}{q}\right) + h(\tau(\boldsymbol{1})) + \ell \cdot h(Q)$$
$$+ \mu_0 \cdot \left(\sum_{\mathbf{a}} \tau(\mathbf{a}) - 1\right) + \sum_{i=1}^{\ell} \mu_i \cdot \left(\sum_{\mathbf{a}:\, a_i=1} \tau(\mathbf{a}) - Q\right). \tag{2.2.37}$$

Тогда выпишем необходимые условия для экстремального распределения $\{\hat{\tau}(\mathbf{a})\}$

$$\begin{cases} \frac{\partial\Lambda}{\partial\tau(\mathbf{a})} = \log_2 \hat{\tau}(\mathbf{a}) + \log_2 e + \mu_0 + \sum\limits_{i:\, a_i=1} \mu_i = 0 \quad \text{для } \mathbf{a} \neq \boldsymbol{1}, \\ \frac{\partial\Lambda}{\partial\tau(\boldsymbol{1})} = \log_2 \hat{\tau}(\boldsymbol{1}) + \log_2 e + \sum\limits_{i=0}^{\ell} \mu_i + \log_2\left[\frac{1-\hat{\tau}(\boldsymbol{1})}{q-\hat{\tau}(\boldsymbol{1})}\right] = 0. \end{cases} \tag{2.2.38}$$

Несложно проверить, что матрица из вторых производных Лагранжиана является диагональной и положительно определенной в области (2.2.35), а функция $F(\tau, Q, q)$, определяемая в (2.2.33), — строго выпуклой в области (2.2.33). Теорема Каруша-Куна-Таккера утверждает, что всякое решение $\{\hat{\tau}(\mathbf{a})\}$), удовлетворяющее системе (2.2.38) и ограничениям (2.2.36) дает локаль- ный минимум для функции $F(\tau, Q, q)$. Таким образом, если существует решение системы (2.2.38)и (2.2.36) в области (2.2.35), то оно единственно и дает минимум в задаче минимизации (2.2.34)-(2.2.36).

Также заметим, что из симметрии задачи вытекают равенства $\mu \triangleq \mu_1 = \mu_2 = \cdots = \mu_\ell$. Пусть $\hat{\mu} \triangleq \log_2 e + \mu_0$. Тогда перепишем (2.2.38) в следующем виде

$$\begin{cases} \hat{\mu} + \mu \sum_{i=1}^{\ell} a_i + \log_2[\hat{\tau}(\mathbf{a})] = 0 \quad \text{для } \mathbf{a} \neq \boldsymbol{1}; \\ \hat{\mu} + \mu\ell + \log_2[\hat{\tau}(\boldsymbol{1})] + \log_2\left[\frac{1-\hat{\tau}(\boldsymbol{1})}{q-\hat{\tau}(\boldsymbol{1})}\right] = 0; \end{cases} \tag{2.2.39}$$

Из первого уравнения системы (2.2.39) вытекает, что

$$\hat{\tau}(\mathbf{a}) = \frac{2^{-\hat{\mu}}}{z^\ell} \prod P(a_i) \quad \text{для } \mathbf{a} \neq \boldsymbol{1},$$

где использовали следующее распределение

$$P(a) \triangleq \begin{cases} z \triangleq \frac{1}{1+2^{-\mu}} \quad \text{для } a = 0; \\ 1 - z \triangleq \frac{2^{-\mu}}{1+2^{-\mu}} \quad \text{для } a = 1; \end{cases}$$

В частности, отсюда следует

$$\mu = \log_2\left[\frac{z}{1-z}\right]. \tag{2.2.40}$$

Поскольку согласно (2.2.36) сумма всех вероятностей равна 1, то получаем

$$\hat{\tau}(\boldsymbol{1}) = 1 - \sum_{k=0}^{\ell-1} \binom{\ell}{k} \frac{2^{-\hat{\mu}}}{z^\ell} z^{\ell-k}(1-z)^k = 1 - \frac{2^{-\hat{\mu}}}{z^\ell}\left(1 - (1-z)^\ell\right). \tag{2.2.41}$$

Из второго условия в (2.2.36) следует, что

$$Q = \frac{2^{-\hat{\mu}}}{z^\ell} \sum_{k=0}^{\ell-2} \binom{\ell-1}{k} z^{\ell-k-1}(1-z)^{k+1} + 1 - \frac{2^{-\hat{\mu}}}{z^\ell}\left(1 - (1-z)^\ell\right) = 1 - \frac{2^{-\hat{\mu}}}{z^{\ell-1}}.$$

Таким образом, можем записать уравнение связи между параметрами $\hat{\mu}$, Q и z

$$\hat{\mu} = -\log_2\left[(1-Q)z^{\ell-1}\right]. \tag{2.2.42}$$

Наконец, подставляя (2.2.40)-(2.2.42) во второе уравнение системы (2.2.39), находим

$$\begin{aligned} &-\log_2\left[(1-Q)z^{\ell-1}\right] + \ell\log_2\left[\frac{z}{1-z}\right] + \log_2\left[1 - \frac{(1-Q)}{z}\left(1-(1-z)^\ell\right)\right] \\ &+ \log_2\left[\frac{(1-Q)}{z}\left(1-(1-z)^\ell\right)\right] - \log\left[q + \frac{(1-Q)}{z}\left(1-(1-z)^\ell\right) - 1\right] = 0 \end{aligned}$$

Перепишем в эквивалентной форме

$$\log_2\left[\frac{\left(1-(1-z)^\ell\right)}{(1-z)^\ell}\right]+\log_2\left[\frac{z-(1-Q)\left(1-(1-z)^\ell\right)}{(q-1)z+(1-Q)\left(1-(1-z)^\ell\right)}\right]=0.$$

Отсюда в явном виде найдем, как Q вычисляется через параметры z, q, s и ℓ

$$Q=\frac{(1-z)(1-(1-z)^\ell)-(1-q)z(1-z)^\ell}{1-(1-z)^\ell}. \tag{2.2.43}$$

Отметим, что для фиксированных параметров q, s и ℓ существует биекция между $Q\in[0,1]$ и $z\in[0,1]$. Из (2.2.42) и (2.2.43) следует, что

$$\frac{2^{-\hat\mu}}{z^\ell}=\frac{1-Q}{z}=\frac{1-q(1-z)^\ell}{1-(1-z)^\ell}. \tag{2.2.44}$$

Подставим $q=\hat q=1-(1-Q)^s$. Тогда

$$\hat\tau(\boldsymbol{1})=\hat q(1-z)^\ell. \tag{2.2.45}$$

Напомним (2.2.34), что

$$F(\hat\tau,Q,\hat q)=\sum_{\mathbf{a}\in\{0,1\}^\ell}\hat\tau(\mathbf{a})\log_2\hat\tau(\mathbf{a})-\hat q\cdot h\left(\frac{\hat\tau(\boldsymbol{1})}{\hat q}\right)+h(\hat\tau(\boldsymbol{1}))+\ell\cdot h(Q). \tag{2.2.46}$$

Тогда, воспользовавшись (2.2.44)), перепишем первую сумму в (2.2.46):

$$\begin{aligned}
\sum_{\mathbf{a}\in\{0,1\}^\ell}\hat\tau(\mathbf{a})\log_2\hat\tau(\mathbf{a})&=\sum_{i=0}^{\ell-1}\binom{\ell}{i}\frac{2^{-\hat\mu}}{z^\ell}(1-z)^iz^{\ell-i}\log_2\left[\frac{2^{-\hat\mu}}{z^\ell}(1-z)^iz^{\ell-i}\right]\\
&+\hat\tau(\boldsymbol{1})\log_2\hat\tau(\boldsymbol{1})=\sum_{i=0}^{\ell-1}\binom{\ell}{i}\frac{2^{-\hat\mu}}{z^\ell}(1-z)^iz^{\ell-i}\log_2\left[\frac{2^{-\hat\mu}}{z^\ell}\right]\\
&+\sum_{i=0}^{\ell-1}\binom{\ell}{i}\frac{2^{-\hat\mu}}{z^\ell}(1-z)^iz^{\ell-i}\log_2\left[z^{\ell-i}\right]+\\
&+\sum_{i=0}^{\ell-1}\binom{\ell}{i}\frac{2^{-\hat\mu}}{z^\ell}(1-z)^iz^{\ell-i}\log_2\left[(1-z)^i\right]+\hat\tau(\boldsymbol{1})\log_2\hat\tau(\boldsymbol{1})\\
&=\left(1-\hat q(1-z)^\ell\right)\log_2\left[\frac{1-\hat q(1-z)^\ell}{1-(1-z)^\ell}\right]+(1-Q)\,\ell\,\log_2 z\\
&+\frac{(1-Q)}{z}\ell\left((1-z)-(1-z)^\ell\right)\log_2[1-z]+\hat\tau(\boldsymbol{1})\log_2\hat\tau(\boldsymbol{1}).
\end{aligned}$$

Учитывая (2.2.45), второй член в (2.2.46) представляется в виде

$$-\hat{q}h\left(\frac{\hat{\tau}(\boldsymbol{1})}{\hat{q}}\right) = \tau(\boldsymbol{1})\log_2\left[\frac{\hat{\tau}(\boldsymbol{1})}{q}\right] + (q-\hat{\tau}(\boldsymbol{1}))\log_2\left[\frac{q-\hat{\tau}(\boldsymbol{1})}{q}\right]$$
$$= \ell\hat{q}(1-z)^{\ell}\log_2[1-z] + \hat{q}(1-(1-z)^{\ell})\log_2[1-(1-z)^{\ell}].$$

Третий член в (2.2.46) есть

$$h(\hat{\tau}(\boldsymbol{1})) = -\hat{\tau}(\boldsymbol{1})\log_2\hat{\tau}(\boldsymbol{1}) - (1-\hat{\tau}(\boldsymbol{1}))\log_2[1-\hat{\tau}(\boldsymbol{1})].$$

Наконец, последнее слагаемое в (2.2.46) равно $\ell h(Q)$. Таким образом, значение $\mathcal{D}(\ell, Q, \hat{q}) = F(\hat{\tau}, Q, \hat{q})$ можно записать

$$\mathcal{D}(\ell, Q, \hat{q}) = (1-Q)\,\ell\,\log_2 z + \ell\left(\frac{(1-Q)}{z}(1-z) - \left(\frac{(1-Q)}{z} - \hat{q}\right)(1-z)^{\ell}\right)$$
$$\times \log_2[1-z] - (1-\hat{q})\log_2[1-(1-z)^{\ell}] + \ell h(Q).$$

Лемма 2.2.2 доказана. □

2.3 Верхние оценки $C(s, \ell)$

Следующая теорема является аналогом неравенств (1.3.8)-(1.3.9), полученных для классических свободных от перекрытия кодов в [5,22], но для определения почти свободных от перекрытия кодов доказательство является более искусным.

Теорема 2.3.1. *(Верхняя граница $\overline{C}(s, \ell)$). Имеют место следующие два утверждения.*

1. *Для любого s и ℓ пропускная способность $C(s, \ell)$ ПСП (s, ℓ)-кодов удовлетворяет неравенству*

$$C(s, \ell) \leqslant \overline{C}(s, \ell), \tag{2.3.1}$$

где $\overline{C}(s, \ell)$ определяется из начального условия

$$\overline{C}(s, 1) \triangleq \frac{1}{s} \tag{2.3.2}$$

и рекуррентного уравнения

$$\overline{C}(s, \ell) = \min_{\substack{i\in[s-1]\\ j\in[\ell-1]}}\left\{\overline{C}(s-i, \ell-j)\frac{i^i j^j}{(i+j)^{i+j}}\right\}. \tag{2.3.3}$$

2. *Для фиксированного параметра $\ell \geqslant 1$ и при $s \to \infty$ верхняя асимптотическая граница для $C(s, \ell)$ имеет вид*

$$C(s, \ell) \leqslant \frac{\ell^{\ell}}{e^{\ell-1}} \cdot \frac{1}{s^{\ell}}(1+o(1)). \tag{2.3.4}$$

Доказательство. Начнем доказательство с утверждения 1. Напомним обозначение

$$\mathcal{P}_s(t) \triangleq \{\mathcal{S} : \mathcal{S} \subset [t],\, |\mathcal{S}| = s\}.$$

Пусть X — произвольный двоичный код объема t и длины N, а $\mathcal{U}$ и $\mathcal{V}$ — два непересекающихся подмножества множества $[t]$ мощности u и v соответственно. Множество строк кода X, для которых выполнено следующее условие

$$x_i(j) = 0 \text{ для любого } j \in \mathcal{U} \quad \text{и} \quad x_i(k) = 1 \text{ для любого } k \in \mathcal{V},$$

обозначим за $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$. Определим среднюю по всем возможным выборам упорядоченной пары множеств $\mathcal{U}$ и $\mathcal{V}$ мощность $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$:

$$\overline{D}_{u,v}(X) \triangleq \sum_{\substack{\mathcal{U}\in\mathcal{P}_u(t),\, \mathcal{V}\in\mathcal{P}_v(t),\\ \mathcal{U}\cap\mathcal{V}=\varnothing}} \frac{|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|}{\binom{t}{u+v} \cdot \binom{u+v}{u}},$$

и максимальную среднюю мощность

$$\overline{D}_{u,v}(t, N) = \max_X \overline{D}_{u,v}(X)$$

по всем кодам X фиксированного объема t и длины N.

Лемма 2.3.1. *Выполнено следующее асимптотическое неравенство*

$$\overline{\lim_{t\to\infty}} \frac{\overline{D}_{u,v}(t, N(t))}{N(t)} \leqslant \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v\} = \frac{u^u v^v}{(u+v)^{u+v}}, \tag{2.3.5}$$

где $N(t)$ – произвольная целочисленная функция.

Доказательство этой вспомогательной леммы приведено в следующем разделе.

Определим функцию

$$b(u, v, N) \triangleq \frac{u^u v^v}{(u+v)^{u+v}} N.$$

Для всякого $\hat{\varepsilon} > 0$ определим такое $t(\hat{\varepsilon})$, что любого $t \geqslant t(\hat{\varepsilon})$ верно

$$\overline{D}_{u,v}(t, N) \leqslant b(u, v, N) \cdot (1 + \hat{\varepsilon}). \tag{2.3.6}$$

Множество $\mathcal{U} \subset [t]$, $|\mathcal{U}| = u$, будем называть *δ-хорошим* для кода X объема $t > t(\hat{\varepsilon})$, если существует множество $\mathcal{V}$ такое. что

$$|D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \leqslant (1 + \delta) \cdot b(u, v, N).$$

Через $J_u(X,\delta) \subseteq \mathcal{P}_u(t)$ обозначим совокупность всех δ-хороших множеств в коде X. Тогда, очевидно, выполнено следующее неравенство

$$|J_u(X,\delta)| \geqslant \left(1 - \frac{1+\hat{\varepsilon}}{1+\delta}\right)\binom{t}{u}. \tag{2.3.7}$$

Для любого фиксированного параметра ε, $0 < \varepsilon < 1$, рассмотрим произвольный ПСП (s,ℓ,ε)-код X объема $t > t(\hat{\varepsilon})$ и длины N. Введем обозначение

$$B(\mathcal{U},X) \triangleq \{\,\mathcal{S} : \mathcal{S} \in \mathcal{P}_s(t),\ \text{причем}\ \mathcal{S} \in \mathbf{B}(s,\ell,X)\ \text{и}\ \mathcal{U} \subset \mathcal{S}\}.$$

Очевидно, что средняя мощность таких множеств

$$\overline{B}_u(X) \triangleq \sum_{\mathcal{U}\in\mathcal{P}_u(t)} \frac{|B(\mathcal{U},X)|}{\binom{t}{u}} \leqslant \frac{\varepsilon\binom{s}{u}\binom{t}{s}}{\binom{t}{u}} \triangleq d(t,s,u,\varepsilon). \tag{2.3.8}$$

Для произвольного фиксированного параметра $c > 0$ определим следующую совокупность

$$G_u(X,c) \triangleq \{\mathcal{U} : \mathcal{U} \in \mathcal{P}_u(t),\ \text{причем}\ |B(\mathcal{U},X)| \leqslant c\cdot d(t,s,u,\varepsilon)\} \subset \mathcal{P}_u(t).$$

Легко видеть, что мощность такого множества

$$|G_u(X,c)| \geqslant \left(1 - \frac{1}{c}\right)\binom{t}{u}. \tag{2.3.9}$$

Пусть число T таково, что при $t > T$ выполнено

$$\frac{\binom{s}{u}\binom{t}{s}}{\binom{t}{u}\binom{t-(u+v)}{s-u}} < 2.$$

Из неравенств (2.3.7) и (2.3.9) следует, что

$$|J_u(X,\delta) \cap G_u(X,c)| \geqslant \left(1 - \frac{1}{c} - \frac{1+\hat{\varepsilon}}{1+\delta}\right)\binom{t}{u}.$$

Очевидно, что для всякого $\delta > 0$ существуют такие $c(\delta)$ и $\hat{\varepsilon}(\delta)$, что

$$1 - \frac{1}{c} - \frac{1+\hat{\varepsilon}}{1+\delta} > 0 \quad \text{для всякого } c > c(\delta) \text{ и } \hat{\varepsilon} \leqslant \hat{\varepsilon}(\delta). \tag{2.3.10}$$

Следуя (2.3.6) и (2.3.10), обозначим $t(\delta) \triangleq t(\hat{\varepsilon}(\delta))$.

Определим минимальную длину ПСП (s,ℓ,ε)-кода объема t и обозначим ее через $N_\varepsilon(s,\ell,t)$.

Лемма 2.3.2. *Для любого фиксированного $\delta > 0$ и $t > \max\{t(\delta), T\}$ длина ПСП (s, ℓ, ε)-кода удовлетворяет неравенству*

$$N_{\varepsilon'}(s-u, \ell-v, t-u-v) \leqslant (1+\delta) \cdot N_{\varepsilon}(s, \ell, t) \cdot \frac{u^u v^v}{(u+v)^{u+v}}, \qquad (2.3.11)$$

где $\varepsilon' < C(\delta) \cdot \varepsilon$.

Доказательство этой вспомогательной леммы приведено в следующем разделе.

Обозначим через

$$C'(s, \ell) \triangleq \overline{\lim_{\varepsilon \to 0}} \, \overline{\lim_{t \to \infty}} \, \frac{\log_2 t}{N_{\varepsilon}(t, s, \ell)}. \qquad (2.3.12)$$

Из леммы 2.3.2, в частности, следует, что $\varepsilon' \to 0$ при $\varepsilon \to 0$ и фиксированном параметре $\delta > 0$. Легко видеть, что

$$C'(s, \ell) \cdot (1+\delta) \leqslant C'(s-u, \ell-v) \cdot \frac{u^u v^v}{(u+v)^{u+v}}.$$

В силу того, что это неравенство выполнено для произвольного параметра $\delta > 0$, это означает, что равенство (2.3.3) доказано. Далее воспользуемся очевидной леммой, в которой описана теоретико-информационная граница для $C'(s, 1)$.

Лемма 2.3.3. *Для любого фиксированного s выполнено неравенство*

$$C'(s, 1) \leqslant \frac{1}{s}.$$

Доказательство этой вспомогательной леммы приведено в следующем разделе.

Неравенство $C'(s, \ell) \geqslant C(s, \ell)$ очевидно, т.к. условие экспоненциального убывания вероятности ошибки с ростом длины более строгое, чем условие, используемое в определении (2.3.12) числа $C'(s, \ell)$.

Утверждение 1 теоремы 2.3.1 доказано.

Перейдем к доказательству утверждения 2. Пусть $s \geqslant \ell \geqslant 2$. Будем считать, что параметр p, $0 < p < 1$, выбран так, что число sp является натуральным. В правую часть (2.3.3) подставим $j \triangleq \ell - 1$, $i \triangleq ps$. Тогда для неравенства (2.3.1) получим

$$C(s, \ell) \leqslant \overline{C}(s(1-p), 1) \cdot \frac{(ps)^{ps} \cdot (\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}}.$$

Пусть $s \to \infty$ и параметр $\ell \geqslant 2$ фиксирован. Используя начальное условие (2.3.2) для $\overline{C}(s(1-p),1) = 1/(s(1-p))$, можем написать

$$C(s,\ell) \leqslant \inf_{0<p<1}\left\{\frac{(ps)^{ps}\cdot(\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}}\frac{1}{s(1-p)}\right\} = \frac{(\ell-1)^{\ell-1}}{e^{\ell-1}s^{\ell}} \times \min_{0<p<1}\left\{\frac{1}{p^{\ell-1}(1-p)}\right\}(1+o(1)) = \frac{\ell^{\ell}}{e^{\ell-1}s^{\ell}}(1+o(1)),$$

где воспользовались тем, что

$$\max_{0<p<1}\left\{(1-p)\,p^{\ell-1}\right\} = \frac{(\ell-1)^{\ell-1}}{\ell^{\ell}},$$

и последний максимум достигается при $p = \frac{\ell-1}{\ell}$.

Утверждение 2 теоремы 2.3.1 доказано. □

Доказательство вспомогательных лемм

Доказательство леммы 2.3.1. Пусть $\mathcal{K}$ — подмножество $[t]$ мощности $u+v$. Обозначим через $\boldsymbol{x}_i(\mathcal{K})$ подматрицу кода X размера $1\times(u+v)$, состоящую из элементов, стоящих на пересечении i-ой строки и столбцов с номерами из $\mathcal{K}$. Введем величину

$$I(X,\mathcal{K},i) \triangleq \begin{cases} 1, & \text{если } \boldsymbol{x}_i(\mathcal{K}) \text{ содержит ровно } u \text{ нулей},\\ 0, & \text{иначе.}\end{cases}$$

Обозначим через $M_{u,v}(X)$ число подматриц кода X размера $1\times(u+v)$, в которых ровно u нулей, т.е.

$$M_{u,v}(X) \triangleq \sum_{i\in[N],\,\mathcal{K}\in\mathcal{P}_{u+v}(t)} I(X,\mathcal{K},i).$$

Пусть количество нулей в i-ой строке кода X равно a_i, тогда

$$M_{u,v}(X) = \sum_{i=1}^{N}\binom{a_i}{u}\cdot\binom{t-a_i}{v}.$$

С другой стороны,

$$M_{u,v}(X) = \overline{D}_{u,v}(X)\cdot\binom{t}{u+v}\binom{u+v}{u}.$$

Используя два предыдущих равенства, получаем

$$\binom{t}{u+v}\binom{u+v}{u}\cdot\overline{D}_{u,v}(X) \leqslant N\cdot\max_{a\in[t]}\left\{\binom{a}{u}\cdot\binom{t-a}{v}\right\}.$$

При $t \to \infty$ последнее неравенство превращается в (2.3.5).

Лемма 2.3.1 доказана. □

Доказательство леммы 2.3.2. Выберем $c > c(\delta)$ и предположим, что ПСП (s, ℓ, ε)-код X имеет объем $t > \max\{t(\delta), T\}$ и длину N. Выберем и зафиксируем произвольное множество $\mathcal{U} \in \{J_u(X, \delta) \cap G_u(X, c)\}$. Поскольку $\mathcal{U}$ является δ-хорошим, то найдем соответствующее ему множество $\mathcal{V}$, т.е.

$$|D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \leqslant (1 + \delta) \cdot b(u, v, N).$$

Определим код X' объема $t' = t - (u + v)$ и длины $N' = |D_{u,v}(\mathcal{U}, \mathcal{V}, X)|$ как подкод кода X, состоящий из строк $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$ и столбцов с номерами $[t] \setminus \{\mathcal{U} \cup \mathcal{V}\}$. Покажем, что X' является ПСП $(s - u, \ell - v, \varepsilon')$-кодом, причем параметр ε' удовлетворяет неравенству

$$\varepsilon' \leqslant \frac{d(t, s, u, \varepsilon) \cdot c}{\binom{t-(u+v)}{s-u}} = 2 \cdot c \cdot \varepsilon. \tag{2.3.13}$$

Действительно, поскольку $\mathcal{U} \in G_u(X, c)$, то $|B(\mathcal{U}, X)| \leqslant c \cdot d(t, s, u, \varepsilon)$. Это означает, что число $(s - u, \ell - v)$-плохих множеств для кода X' не превосходит $c \cdot d(t, s, u, \varepsilon)$. А поскольку общее число подмножеств мощности $(s - u)$ множества $[t - (u + v)]$ равно $\binom{t-(u+v)}{s-u}$, то неравенство (2.3.13) в самом деле верно. Заметим, что длина кода X'

$$N' = |D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \leqslant (1 + \delta) \cdot N \cdot \frac{u^u v^v}{(u + v)^{u+v}}.$$

В частности, отсюда следует (2.3.11).

Лемма 2.3.2 доказана. □

Доказательство леммы 2.3.3. Зафиксируем параметр ε, $0 \leqslant \varepsilon < 1$. Пусть X — произвольный ПСП $(s, 1, \varepsilon)$-код длины N и объема t Тогда

$$|\mathbf{G}(s, 1, X)| \geqslant (1 - \varepsilon)\binom{t}{s}. \tag{2.3.14}$$

Отметим, что для всякого $\mathcal{S} \in \mathbf{G}(s, 1, X)$ дизъюнктивная сумма столбцов кода X с номерами из $\mathcal{S}$ не покрывает посторонний. Тогда из леммы Шпернера и неравенства (2.3.14) следует

$$\binom{N}{\lfloor N/2 \rfloor} \geqslant (1 - \varepsilon)\binom{t}{s}.$$

Поэтому из определения (2.3.12) вытекает, что $C'(s) \leqslant 1/s$.

Лемма 2.3.3 доказана. □

2.4 Таблица наилучших границ $C(s, \ell)$

В таблице 2.1 при $\ell = 1$ и $2 \leqslant s \leqslant 10$ даны значения нижней границы (2.2.1) пропускной способности $C(s, 1)$ вместе с долей $Q(s)$ оптимального веса кодовых слов для ансамбля равновесных двоичных кодов. При $1 \leqslant \ell \leqslant s \leqslant 10$ в сводной таблице 2.1 также указаны верхняя граница $\overline{C}(s, \ell)$, определяемая (2.3.1), нижняя граница $\underline{C}(s, \ell)$ и соответствующая доля $Q(s, \ell)$ оптимального веса кодовых слов для ансамбля равновесных двоичных кодов в границе случайного кодирования из теоремы 2.2.2.

2.5 Сравнение $R(s, \ell)$ и $C(s, \ell)$

Прежде всего, отметим, что скорость $R(s, \ell)$ и пропускная способность $C(s, \ell)$ связаны между собой очевидным соотношением: $R(s, \ell) \leqslant C(s, \ell)$. Так, сравнивая значения из таблицы 1.1 со значениями из таблицы 2.1, можно увидеть, что в некоторых случаях верхняя граница скорости $R(s, \ell)$ не превосходит нижнюю границу пропускной способности $C(s, \ell)$. Например, при $s = 3$ и $\ell = 1$ выполнена следующая цепочка соотношений

$$R(3, 1) \leqslant \overline{R}(3, 1) = 1.99 \cdot 10^{-1} \leqslant 2.45 \cdot 10^{-1} = \underline{C}(3, 1) \leqslant C(3, 1).$$

На текущий момент порядок главного члена асимптотики скорости $R(s, \ell)$ при $s \to \infty$ и фиксированном значении ℓ не определен однозначно. Из нижней (1.2.9) и верхней границы (1.3.11) скорости $R(s, \ell)$ следует, что данный порядок находится в пределах от $1/s^{\ell+1}$ до $\ln s/s^{\ell+1}$.

Из сравнения нижней границы (2.2.7) с верхней границей (2.3.4) пропускной способности $C(s, \ell)$ следует, что их отношение при $s \to \infty$ и любом фиксированным значении параметра $\ell \geqslant 2$ сходится к пределу $\log_2 e/(\ell e)$. Отметим, что при $\ell = 1$ аналогичное отношение нижней границы (2.2.7) к верхней (2.3.1) сходится к пределу, равному $\ln 2$. Таким образом, порядок главного члена асимптотики $C(s, \ell)$ определен однозначно и равен $1/s^{\ell}$.

Таблица 2.1: Таблица значений для $\overline{C}(s,\ell)$ и $\underline{C}(s,\ell)$

(s,ℓ)	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$	$(7,1)$
$\overline{C}(s,\ell)$	$5.00 \cdot 10^{-1}$	$3.33 \cdot 10^{-1}$	$2.50 \cdot 10^{-1}$	$2.00 \cdot 10^{-1}$	$1.7 \cdot 10^{-1}$	$1.4 \cdot 10^{-1}$
$\underline{C}(s,\ell)$	$3.83 \cdot 10^{-1}$	$2.45 \cdot 10^{-1}$	$1.81 \cdot 10^{-1}$	$1.43 \cdot 10^{-1}$	$1.2 \cdot 10^{-1}$	$1.0 \cdot 10^{-1}$
$\overline{Q}(s,\ell)$	0.29	0.20	0.16	0.13	0.11	0.09
(s,ℓ)	$(8,1)$	$(9,1)$	$(10,1)$	$(2,2)$	$(3,2)$	$(4,2)$
$\overline{C}(s,\ell)$	$1.25 \cdot 10^{-1}$	$1.11 \cdot 10^{-1}$	$1.00 \cdot 10^{-1}$	$2.50 \cdot 10^{-1}$	$1.3 \cdot 10^{-1}$	$7.4 \cdot 10^{-2}$
$\underline{C}(s,\ell)$	$8.84 \cdot 10^{-2}$	$7.84 \cdot 10^{-2}$	$7.04 \cdot 10^{-2}$	$5.80 \cdot 10^{-2}$	$2.9 \cdot 10^{-2}$	$1.8 \cdot 10^{-2}$
$\overline{Q}(s,\ell)$	0.08	0.07	0.07	0.53	0.41	0.34
(s,ℓ)	$(5,2)$	$(6,2)$	$(7,2)$	$(8,2)$	$(9,2)$	$(10,2)$
$\overline{C}(s,\ell)$	$4.94 \cdot 10^{-2}$	$3.52 \cdot 10^{-2}$	$2.64 \cdot 10^{-2}$	$2.05 \cdot 10^{-2}$	$1.6 \cdot 10^{-2}$	$1.3 \cdot 10^{-2}$
$\underline{C}(s,\ell)$	$1.20 \cdot 10^{-2}$	$8.61 \cdot 10^{-3}$	$6.50 \cdot 10^{-3}$	$5.09 \cdot 10^{-3}$	$4.1 \cdot 10^{-3}$	$3.4 \cdot 10^{-3}$
$\overline{Q}(s,\ell)$	0.29	0.25	0.22	0.20	0.18	0.17
(s,ℓ)	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$	$(7,3)$	$(8,3)$
$\overline{C}(s,\ell)$	$6.25 \cdot 10^{-2}$	$3.13 \cdot 10^{-2}$	$1.73 \cdot 10^{-2}$	$1.10 \cdot 10^{-2}$	$7.3 \cdot 10^{-3}$	$5.1 \cdot 10^{-3}$
$\underline{C}(s,\ell)$	$8.29 \cdot 10^{-3}$	$4.29 \cdot 10^{-3}$	$2.52 \cdot 10^{-3}$	$1.61 \cdot 10^{-3}$	$1.1 \cdot 10^{-3}$	$7.8 \cdot 10^{-4}$
$\overline{Q}(s,\ell)$	0.52	0.44	0.38	0.34	0.30	0.27
(s,ℓ)	$(9,3)$	$(10,3)$	$(4,4)$	$(5,4)$	$(6,4)$	$(7,4)$
$\overline{C}(s,\ell)$	$3.71 \cdot 10^{-3}$	$2.78 \cdot 10^{-3}$	$1.56 \cdot 10^{-2}$	$7.81 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$2.5 \cdot 10^{-3}$
$\underline{C}(s,\ell)$	$5.72 \cdot 10^{-4}$	$4.33 \cdot 10^{-4}$	$1.47 \cdot 10^{-3}$	$7.64 \cdot 10^{-4}$	$4.4 \cdot 10^{-4}$	$2.7 \cdot 10^{-4}$
$\overline{Q}(s,\ell)$	0.25	0.23	0.51	0.45	0.40	0.37
(s,ℓ)	$(8,4)$	$(9,4)$	$(10,4)$	$(5,5)$	$(6,5)$	$(7,5)$
$\overline{C}(s,\ell)$	$1.63 \cdot 10^{-3}$	$1.08 \cdot 10^{-3}$	$7.41 \cdot 10^{-4}$	$3.91 \cdot 10^{-3}$	$2.0 \cdot 10^{-3}$	$1.0 \cdot 10^{-3}$
$\underline{C}(s,\ell)$	$1.75 \cdot 10^{-4}$	$1.19 \cdot 10^{-4}$	$8.34 \cdot 10^{-5}$	$2.87 \cdot 10^{-4}$	$1.5 \cdot 10^{-4}$	$8.4 \cdot 10^{-5}$
$\overline{Q}(s,\ell)$	0.33	0.31	0.29	0.50	0.46	0.42
(s,ℓ)	$(8,5)$	$(9,5)$	$(10,5)$	$(6,6)$	$(7,6)$	$(8,6)$
$\overline{C}(s,\ell)$	$5.97 \cdot 10^{-4}$	$3.69 \cdot 10^{-4}$	$2.41 \cdot 10^{-4}$	$9.77 \cdot 10^{-4}$	$4.9 \cdot 10^{-4}$	$2.6 \cdot 10^{-4}$
$\underline{C}(s,\ell)$	$5.02 \cdot 10^{-5}$	$3.15 \cdot 10^{-5}$	$2.06 \cdot 10^{-5}$	$5.92 \cdot 10^{-5}$	$3.1 \cdot 10^{-5}$	$1.7 \cdot 10^{-5}$
$\overline{Q}(s,\ell)$	0.39	0.36	0.33	0.50	0.46	0.43
(s,ℓ)	$(9,6)$	$(10,6)$	$(7,7)$	$(8,7)$	$(9,7)$	$(10,7)$
$\overline{C}(s,\ell)$	$1.44 \cdot 10^{-4}$	$8.66 \cdot 10^{-5}$	$2.44 \cdot 10^{-4}$	$1.22 \cdot 10^{-4}$	$6.3 \cdot 10^{-5}$	$3.5 \cdot 10^{-5}$
$\underline{C}(s,\ell)$	$9.95 \cdot 10^{-6}$	$6.09 \cdot 10^{-6}$	$1.26 \cdot 10^{-5}$	$6.52 \cdot 10^{-6}$	$3.8 \cdot 10^{-6}$	$2.1 \cdot 10^{-6}$
$\overline{Q}(s,\ell)$	0.40	0.38	0.50	0.47	0.44	0.41
(s,ℓ)	$(8,8)$	$(9,8)$	$(10,8)$	$(9,9)$	$(10,9)$	$(10,10)$
$\overline{C}(s,\ell)$	$6.10 \cdot 10^{-5}$	$3.05 \cdot 10^{-5}$	$1.58 \cdot 10^{-5}$	$1.53 \cdot 10^{-5}$	$7.6 \cdot 10^{-6}$	$3.8 \cdot 10^{-6}$
$\underline{C}(s,\ell)$	$2.76 \cdot 10^{-6}$	$1.42 \cdot 10^{-6}$	$7.69 \cdot 10^{-7}$	$6.12 \cdot 10^{-7}$	$3.1 \cdot 10^{-7}$	$1.4 \cdot 10^{-7}$
$\overline{Q}(s,\ell)$	0.50	0.47	0.44	0.50	0.47	0.50

Глава 3

Задача поиска скрытого гиперграфа

В этой главе будут рассмотрены комбинаторные и вероятностные постановки задачи поиска скрытого гиперграфа из семейства локализованных гиперграфов. Будет предложен детерминированный алгоритм адаптивного поиска скрытого гиперграфа, который является асимптотически оптимальным. В последнем разделе данной главы, используя вероятностный метод, будет установлена пропускная способность двухступенчатой процедуры поиска скрытого гиперграфа. Далее перейдем к формальному описанию задачи.

3.1 Основные определения

Рассмотрим семейство $\mathcal{F}(t, s, \ell)$, которое будет состоять из таких гиперграфов $H = (V, E)$, что множество вершин $V = \{1, 2, \ldots, t\}$, множество ребер $E = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{s'}\}$, $s' \leqslant s$, и размер каждого ребра $1 \leqslant |\mathbf{e}_i| \leqslant \ell$, причем никакое ребро не содержится ни в каком другом, т.е.

$$\mathcal{F}(t, s, \ell) \triangleq \left\{ \begin{array}{c} H = (V, E): \quad V = \{1, 2, \ldots, t\} \\ E = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{s'}), \quad s' \leqslant s, \\ |\mathbf{e}_i| \leqslant \ell, \quad \mathbf{e}_i \not\subset \mathbf{e}_j \text{ для } i \neq j \end{array} \right\}.$$

Предположим, что задан *скрытый* гиперграф $H_{un} = (V, E)$. При этом известно, что $H_{un} \in \mathcal{F}(t, s, \ell)$. Наша цель — обнаружить ребра E этого гиперграфа, спросив N *вопросов (тестов)* $Q(S)$, где множество S — это некоторое подмножество V, а ответ на вопрос *положительный*, т.е. $Q(S) = 1$, в случае, если множество S содержит полностью хотя бы одно ребро из E. В остальных случаях ответ на вопрос *отрицательный*, т.е. $Q(S) = 0$. Будем называть поиск *неадаптивным*, если все вопросы определяются заранее и не меняются в зависимости от результатов уже заданных к этому моменту вопросов. Таким образом, можно считать, что все вопросы при неадаптивном поиске задаются одновременно. Если же вопросы задаются последовательно, и последующие вопросы зависят от ответов на предыдущие, то поиск называют *адаптивным*. Промежуточным видом между адаптивным и неадаптивным

поиском является *многошаговый алгоритм*. Прежде чем дать формальное определение, введем несколько вспомогательных.

Вершины $V' \subset V$, входящие в какие-либо ребра из E, будем называть *активными*. Вершины $V \setminus V'$ будем называть *изолированными*.

Заметим, что N тестов неадаптивного алгоритма поиска можно записать в виде $N \times t$ матрицы поиска X. Столбцу $\boldsymbol{x}(j)$ поставим в соответствие j-ю вершину V, строчке $\boldsymbol{x}_i$ поставим в соответствие i-й тест. Пусть $\mathbf{u} \bigvee \mathbf{v}$ обозначает дизъюнктивную сумму двух столбцов $\mathbf{u}, \mathbf{v} \in \{0,1\}^N$. Для произвольного гиперграфа $H = (V, E)$ определим *вектор-ответ*:

$$\mathbf{r}(X, H) = \bigvee_{e_i \in E} \bigwedge_{j \in e_i} \boldsymbol{x}(j).$$

Очевидно, что i-я координата вектора $\mathbf{r}(X, H)$ может быть записана в следующем виде

$$r_i = \begin{cases} 1, & \text{если } \exists\, \mathbf{e}_i \in E, \text{ такое что } x_i(j) = 1 \text{ для всех } j \in \mathbf{e}_i, \\ 0, & \text{в остальных случаях.} \end{cases} \tag{3.1.1}$$

Тогда можно сказать, что код X, соответствующий неадаптивному алгоритму поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$, обладает следующим свойством:

$$\mathbf{r}(X, H) \neq \mathbf{r}(X, H'), \quad \text{при } H \neq H'.$$

Определение 3.1.1. Пусть задан скрытый гиперграф $H_{un} \in \mathcal{F}(t, s, \ell)$. Будем говорить, что $\mathcal{A}$ является *p-шаговым алгоритмом* поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$, если выполнено следующее:

1. задан код $X_1 = X_1^{\mathcal{A}}$, соответствующий первому шагу поиска (можно считать, что вопросы внутри одного шага тестирования задаются одновременно),

2. код X_i, соответствующий i-му шагу поиска, определяется как

$$X_i = X_i^{\mathcal{A}}(\mathbf{r}(X_1, H_{un}), \ldots, \mathbf{r}(X_{i-1}, H_{un})),$$

3. можно точно определить H_{un}, используя векторы-ответы

$$\mathbf{r}(X_1, H_{un}),\, \mathbf{r}(X_2, H_{un}), \ldots, \mathbf{r}(X_p, H_{un}).$$

Таким образом, можно считать, что p-шаговый алгоритм поиска имеет $p-1$ ступень адаптации. В частности, при $p = 1$ алгоритм поиска называют

неадаптивным. Пусть $N_i^{\mathcal{A}}(H_{un})$ равно числу тестов на i-м шаге при поиске H_{un} с помощью алгоритма $\mathcal{A}$. Тогда определим число тестов в *худшем случае*:

$$N^{\mathcal{A}} = \max_{H_{un} \in \mathcal{F}(t,s,\ell)} \sum_{i=1}^{p} N_i^{\mathcal{A}}(H_{un}).$$

Символом $N_h^{p\text{-st}}(t, s, \ell)$ обозначим минимальное число тестов $N^{\mathcal{A}}$ среди всевозможных p-шаговых алгоритмов $\mathcal{A}$ поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$.

Определим асимптотическую скорость p-шаговых алгоритмов поиска скрытого гиперграфа как

$$R_h^{p\text{-st}}(s, \ell) = \varlimsup_{t \to \infty} \frac{\log_2 t}{N_h^{p\text{-st}}(t, s, \ell)}. \tag{3.1.2}$$

Тогда асимптотическую скорость неадаптивного поиска можно понимать как $R_h^{1\text{-st}}(s, \ell)$. Очевидно, что выполнена цепочка неравенств

$$R_h^{na}(s, \ell) = R_h^{1\text{-st}}(s, \ell) \leqslant R_h^{2\text{-st}}(s, \ell) \leqslant \ldots \leqslant R_h^{a}(s, \ell).$$

Наиболее важными границами для скорости являются оценки для крайних величин, но и оценки для промежуточных величин также представляют определенный интерес.

Далее определим, что будем понимать под пропускной способностью $C_h^{p\text{-st}}(s, \ell)$ для p-шагового алгоритма поиска скрытого гиперграфа.

Определение 3.1.2. Будем говорить, что $\mathcal{A}$ является *p-шаговым алгоритмом* поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$ *с вероятностью ошибки* ε, если выполнено следующее: существует такое подмножество $\mathcal{F}' \subset \mathcal{F}(t, s, \ell)$ мощности $|\mathcal{F}'| \geqslant (1 - \varepsilon)|\mathcal{F}(t, s, \ell)|$, что для всякого $H_{un} \in \mathcal{F}'$ алгоритм $\mathcal{A}$ позволяет (в смысле ранее указанных условий 1-3 в определении 3.1.1) точно определить H_{un}.

Заметим, что ранее введенное определение 3.1.1 можно понимать как алгоритм поиска с вероятностью ошибки 0.

Пусть $N_i^{\mathcal{A}}(H_{un})$ число тестов на i-м шаге при поиске H_{un} с помощью алгоритма поиска $\mathcal{A}$. Тогда определим число тестов в худшем случае:

$$N^{\mathcal{A}} = \max_{H_{un} \in \mathcal{F}(t,s,\ell)} \sum_{i=1}^{p} N_i^{\mathcal{A}}(H_{un}).$$

Символом $N_h^{p\text{-st}}(t, s, \ell, \varepsilon)$ обозначим минимальное число тестов $N^{\mathcal{A}}$ среди всевозможных p-шаговых алгоритмов $\mathcal{A}$ поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$ с вероятностью ошибки ε.

Определим пропускную способность p-шаговых алгоритмов поиска скрытого гиперграфа как

$$C_h^{p\text{-st}}(s,\ell) = \varlimsup_{\substack{t\to\infty\\ \varepsilon\to 0}} \frac{\log_2 t}{N_h^{p\text{-st}}(t,s,\ell,\varepsilon)}. \tag{3.1.3}$$

Отметим, что выполнена очевидная цепочка неравенств

$$C_h^{1\text{-st}}(s,\ell) \leqslant C_h^{2\text{-st}}(s,\ell) \leqslant \ldots \leqslant C_h^{a}(s,\ell).$$

Напомним, что для p-шагового алгоритма поиска существует не более $p-1$ ступени адаптации. В частности, при $p=1$ алгоритм поиска называют неадаптивным, и пропускную способность $C_h^{1\text{-st}}(s,\ell)$ будем также обозначать через $C_h^{na}(s,\ell)$. Нас также будет интересовать случай $p=2$, как наиболее близкий к неадаптивному поиску.

3.2 Оценки $R_h(s,\ell)$

В работе [19] было показано, что задача неадаптивного поиска скрытого гиперграфа и свободные от перекрытия коды сильно связаны между собой. В частности, верна следующая теорема.

Теорема 3.2.1. [19]. *Для скорости неадаптивного поиска скрытого гиперграфа $R_h^{na}(s,\ell)$ и скорости СП кодов $R(s,\ell)$ верна цепочка неравенств*

$$R_h^{na}(s,\ell) \leqslant R(s,\ell) \leqslant \min\left(R_h^{na}(s-1,\ell), R_h^{na}(s,\ell-1)\right). \tag{3.2.1}$$

Отметим, что при $\ell=1$ задача поиска скрытого гиперграфа вырождается в довольно известную задачу *поиска дефектов*. Известно [14], что адаптивный поиск дефектов достигает теоретико-информационную границу, т.е.

$$R_h^{a}(s,1) = \frac{1}{s}. \tag{3.2.2}$$

Для произвольных значений s и ℓ недавно было показано [10], что

$$R_h^{a}(s,\ell) \geqslant \frac{1}{2s\ell}. \tag{3.2.3}$$

Естественная теоретико-информационная граница для скорости $R_h^{a}(s,\ell)$ представлена в следующем утверждении.

Лемма 3.2.1. *Скорость $R_h^{a}(s,\ell)$ удовлетворяет неравенству*

$$R_h^{a}(s,\ell) \leqslant \frac{1}{s\ell}.$$

Следующая лемма улучшает константу в нижней границе (3.2.3) для скорости $R_h^a(s,\ell)$.

Лемма 3.2.2. *Скорость $R_h^a(s,\ell)$ удовлетворяет неравенству*

$$R_h^a(s,\ell) \geqslant \frac{1}{s\ell}.$$

Таким образом, леммы 3.2.1 и 3.2.2 устанавливают точное равенство для скорости $R_h^a(s,\ell)$, которое представлено в виде следующего утверждения.

Теорема 3.2.2. *Для скорости адаптивного поиска скрытого гиперграфа выполнено следующее равенство*

$$R_h^a(s,\ell) = \frac{1}{s\ell}.$$

Доказательство леммы 3.2.1. Пусть $N = N_h^a(t,s,\ell)$ — минимальное число тестов в худшем случае среди всевозможных адаптивных алгоритмов $\mathcal{A}$ поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$. Тогда должно быть выполнено следующее неравенство

$$2^N \geqslant |\mathcal{F}(t,s,\ell)|,$$

из которого сразу следует утверждение теоремы, поскольку при $t \to \infty$

$$|\mathcal{F}(t,s,\ell)| = \frac{t^{s\ell}}{(\ell!)^s s!}(1+o(1)).$$

Лемма 3.2.1 доказана. □

Доказательство леммы 3.2.2. Пусть $H_{un} = (V,E)$ является скрытым гиперграфом из семейства $\mathcal{F}(t,s,\ell)$. Напомним, что вершина $v \in V$ называется активной, если существует по крайней мере одно ребро $\mathbf{e} \in E$, такое что $v \in \mathbf{e}$. Символом F, $F \subset V$, обозначим множество найденных к текущему моменту активных вершин. Символом E, $E' \subset E$, обозначим множество найденных к текущему моменту ребер гиперграфа H_{un}, т.е. если $\mathbf{e} \in E$ и $\mathbf{e} \subset F$, то $\mathbf{e} \in E'$. Заметим, что пара (V,E') задает частичный гиперграф H_{un}. Пусть S, $S \subset V$, — это вопрос, который будем задавать в текущий момент. Прежде чем применим предложенный алгоритм, зададим $F = \varnothing$, $E' = \varnothing$ и $S = V$.

Во-первых, опишем алгоритм, отмеченный как алгоритм 2, который позволяет находить новые активные вершины v, т.е. $v \notin F$. Входными параметрами данного алгоритма являются множество F, а также вопрос S, который содержит по крайней мере одно ребро $\mathbf{e} \in E$ и $\mathbf{e} \notin E'$. Зададим множества $S' = S \setminus F$ и $S'' = S \setminus S'$. На каждом шаге множество S' будет содержать по

крайней мере одну активную вершину. Пока мощность $|S'| > 1$, будем использовать следующую процедуру. Делим множество S' на примерно равные по размеру множества S_1 и S_2, т.е. $S' = S_1 \sqcup S_2$, $|S_1| = \lceil |S'|/2 \rceil$ и $|S_2| = \lfloor |S'|/2 \rfloor$. Далее задаем вопрос $S_1 \sqcup S''$. Если $Q(S_1 \sqcup S'') = 1$, то это означает, что S_1 содержит по крайней мере одну новую активную вершину, т.к. из предыдущих шагов, очевидно, выполнено, что $Q(S'') = 0$. Далее положим $S' = S_1$ и повторим процедуру. Если $Q(S_1 \sqcup S'') = 0$, то это означает, что по крайней мере одна активная вершина содержится в множестве S_2, т.к. из предыдущих шагов, очевидно, выполнено, что $Q(S_1 \sqcup S_2 \sqcup S'') = 1$. Далее положим $S' = S_2$, $S'' = S_1 \sqcup S''$ и повторим процедуру. По окончании процедуры ($|S'| = 1$) получим, что единственная вершина v множества S' является активной вершиной гиперграфа H_{un} и $v \notin F$. Отметим, что алгоритм 2 является вариацией бинарного поиска вершины.

Во-вторых, опишем алгоритм, отмеченный как алгоритм 3, который позволяет находить все ребра E', которые можно составить из уже найденных активных вершин F. Единственным входным параметром является множество F. После того, как найдем новую вершину v, можно обновить множество ребер E'. Например, если будем искать только ребра, содержащие v. Но поскольку $|F| \leqslant s\ell \ll t$ (число вопросов данного алгоритма будет невелико), то зададим $E' = \varnothing$ и запустим следующую процедуру по всем множествам S, таким что $S \subset F$ и $|S| \leqslant \ell$. Если не существует такого ребра $\mathbf{e}$, что $\mathbf{e} \in E'$ и $\mathbf{e} \subset S$, то задаем вопрос S. Если $Q(S) = 1$, то удаляем все ребра $\mathbf{e} \in E'$, такие что $S \subset \mathbf{e}$, и добавляем ребро $\mathbf{e} = S$ к множеству ребер E'. Отметим, что алгоритм 3 является исчерпывающим поиском ребер.

В-третьих, опишем алгоритм, отмеченный как алгоритм 4, который позволяет находить множество (вопрос) S, $S \subset V$, такое что S содержит по крайней мере одно ребро $\mathbf{e}$, такое что $\mathbf{e} \in E$ и $\mathbf{e} \notin E'$ (и, как следствие, множество S содержит по крайней мере одну активную вершину $v \notin F$). Единственным входным параметром является множество E'. Зададим множество A как множество вершин, входящих в по крайней мере одно ребро $\mathbf{e} \in E'$, множество $B = V \setminus A$ и $S = \varnothing$. Очевидно, что $|A| \leqslant s\ell \ll t$. Запустим следующую процедуру по всем множествам C, $C \subset V$, таким что $B \subset C$, и $\nexists\, \mathbf{e} \in E'$, $\mathbf{e} \subset C$. Если $Q(C) = 1$, то установим множество $S = C$ и выходим из процедуры. Если $Q(C) = 0$, то рассматриваем следующее множество C. Если завершили указанную процедуру и имеем $S = \varnothing$, то это означает, что найдены все ребра гиперграфа H_{un}, т.е. $E' = E$. Отметим, что алгоритм 4 является исчерпывающим поиском вопроса.

Таким образом, основной алгоритм адаптивного поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$ разбит на несколько частей. Полное описание стратегии поиска скрытого гиперграфа представлено алгоритмом 1, и он основывается на алгоритмах 2, 3 и 4. В начале поиска полагаем $F = \varnothing$, $E' = \varnothing$ и $S = V$. Пока выходом алгоритма 3 является непустой вопрос $S \neq \varnothing$, запус-

каем следующую процедуру. С помощью алгоритма 2 находим вершину v и добавляем ее к F. Далее используем алгоритм 3, чтобы обновить множество ребер E', составленных из уже найденных активных вершин F. После этого запускаем алгоритм 4 для того, чтобы найти подходящий вопрос S, который далее будет использоваться алгоритмом 2.

Пусть $|V| = t$. Несложно проверить, что алгоритм 2 использует не более $\lceil \log_2 |S| \rceil \leqslant \lceil \log_2 t \rceil$ тестов. Легко видеть, что общее число активных вершин в графе из семейства $\mathcal{F}(t, s, \ell)$ не превосходит $s\ell$. Алгоритм 4 использует не более $F_4(s, \ell)$ тестов, а алгоритм 3 — не более $F_3(s, \ell)$ тестов, где функции F_4 и F_3 не зависят от t. Также можно оценить число циклов в алгоритме 1 максимальным количеством активных вершин, т.е. $s\ell$. Таким образом, общее число тестов для данного адаптивного алгоритма поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$ не превосходит $s\ell(\log_2 t + F_3(s, \ell) + F_4(s, \ell) + 1)$.

Исходные параметры: множество вершин V гиперграфа
$$H_{un} \in \mathcal{F}(t, s, \ell)$$
Результат: множество ребер E гиперграфа H_{un}
инициализация $E' := \varnothing$; $F := \varnothing$; $S := V$;
до тех пор, пока $S \neq \varnothing$ **выполнять**
  выполняем алгоритм 2, находим вершину $v \notin F$ и $F := F \sqcup v$;
  выполняем алгоритм 3 и находим подмножество ребер E';
  выполняем алгоритм 4, и находим вопрос S;
конец

Алгоритм 1: Поиск скрытого гиперграфа

Исходные параметры: вопрос $S \subseteq V$, $Q(S) = 1$, и множество $F \subset V$
Результат: вершина $v \in V$, $v \notin F$, и $\exists\, \mathbf{e} \in E$, $v \in \mathbf{e}$
инициализация $S' := S \setminus F$; $S'' := S \setminus S'$;
до тех пор, пока $|S'| > 1$ **выполнять**
  делим пополам множество S': $S' = S_1 \sqcup S_2$;
  если $Q(S_1 \sqcup S'') = 1$ **тогда**
    $S' := S_1$;
  иначе
    $S' := S_2$, $S'' := S'' \sqcup S_1$;
  конец
конец

Алгоритм 2: Поиск новой активной вершины

Лемма 3.2.1 доказана. □

Исходные параметры: множество $F \subset V$
Результат: подмножество ребер $E' \subset E$
инициализация $E' := \varnothing$;
цикл $\forall S \subset F$: $1 \leqslant |S| \leqslant \ell$ **выполнять**
  если $\nexists\, \mathbf{e} \in E' : \mathbf{e} \subset S$ **тогда**
    если *Q(S) = 1* **тогда**
      цикл $\forall \mathbf{e} \in E' : S \subset \mathbf{e}$ **выполнять**
        удаляем ребро $\mathbf{e}$ из E';
      конец
      добавляем ребро $\mathbf{e} = S$ к E';
    конец
  конец
конец

Алгоритм 3: Поиск ребер

Исходные параметры: подмножество ребер $E' \subset E$
Результат: вопрос S
инициализация $A := \{v : \ v \in \mathbf{e} \in E'\}$; $B := V \setminus A$; $S := \varnothing$;
цикл $\forall C \subset V$: $B \subset C$ u $\nexists\, \mathbf{e} \in E'$, $\mathbf{e} \subset C$ **выполнять**
  если *Q(C) = 1* **тогда**
    $S := C$ и остановить цикл;
  конец
конец

Алгоритм 4: Поиск вопроса

3.3 Оценки $C_h(s, \ell)$

Классическим результатом для теории планирования экспериментов является следующее теорема, доказанная [6] М.Б. Малютовым и В.Л Фрейдлиной.

Теорема 3.3.1. [6]. *Для* $C_h^{na}(s, 1)$ *выполнено равенство*

$$C_h^{na}(s, 1) = \frac{1}{s}.$$

Естественная теоретико-информационная граница для пропускной способности $C_h^a(s, \ell)$ представлена в следующей лемме.

Лемма 3.3.1. *Скорость* $C_h^a(s, \ell)$ *удовлетворяет неравенству*

$$C_h^{na}(s, \ell) \leqslant C_h^a(s, \ell) \leqslant \frac{1}{s\ell}.$$

Опустим доказательство этой леммы, поскольку оно практически в точности совпадает с доказательством леммы 3.2.1.

В [42] авторы частично доказали аналог теоремы 3.2.1. Они показали, что ПСП (s, ℓ, ε)-коду длины N и объема t соответствует неадаптивный поиск скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$ с вероятностью ошибки не более $\varepsilon\ell^s$, состоящий из N групповых проверок. Более формально запишем это утверждение в виде следующей теоремы.

Теорема 3.3.2. [42]. *Для $C_h^{na}(s, \ell)$ и $C(s, \ell)$ выполнено неравенство*

$$C_h^{na}(s, \ell) \geqslant C(s, \ell).$$

Отметим, что нижняя оценка $C_h^{na}(s, \ell)$, представленная теоремой 3.3.2, довольно далека от верхней границы $C_h^{na}(s, \ell)$ в теореме 3.3.1. Чтобы это увидеть, зафиксируем ℓ, устремим $s \to \infty$ и воспользуемся теоремами 2.2.2 и 2.3.1. Легко проверить, что порядок главного члена асимптотики $C(s, \ell)$ равен $1/s^\ell$, в то время как порядок главного члена для верхней границы $C_h^{na}(s, \ell)$ имеет порядок $1/s$. Мы считаем, что более точной границей является верхняя, и имеем следующую гипотезу, доказанную на сегодняшний момент лишь для случая $\ell = 1$.

Гипотеза 3.3.1. *Для $C_h^{na}(s, \ell)$ выполнено равенство*

$$C_h^{na}(s, \ell) = \frac{1}{s\ell}. \tag{3.3.1}$$

В следующем утверждении будет показано, что для достижения теоретико-информационной границы алгоритму достаточно иметь лишь одну ступень адаптации.

Лемма 3.3.2. *Пропускная способность $C_h^{2\text{-}st}(s, \ell)$ двухступенчатой процедуры поиска скрытого гиперграфа удовлетворяет неравенству*

$$C_h^{2\text{-}st}(s, \ell) \geqslant \frac{1}{s\ell}.$$

Таким образом, леммы 3.3.1 и 3.3.2 устанавливают точное равенство для пропускной способности $C_h^{2\text{-st}}(s, \ell)$ двухступенчатой процедуры поиска скрытого гиперграфа, которое представлено в виде следующего утверждения.

Теорема 3.3.3. *Для пропускной способности двухступенчатой процедуры поиска скрытого гиперграфа выполнено следующее равенство*

$$C_h^{2\text{-}st}(s, \ell) = \frac{1}{s\ell}.$$

Доказательство леммы 3.3.2. Рассмотрим подмножество семейства гиперграфов $\mathcal{F}(t,s,\ell)$, в которое войдут все гиперграфы, состоящие из s попарно непересекающихся ребер размера ℓ, т.е.

$$\mathcal{F}^{=}(t,s,\ell)=\left\{\begin{array}{l} H: \quad H\in\mathcal{F}(t,s,\ell),\ E=(\mathbf{e}_1,\ldots,\mathbf{e}_s),\\ |\mathbf{e}_i|=\ell,\ \mathbf{e}_i\cap\mathbf{e}_j=\varnothing \text{ для любого } i\neq j\end{array}\right\}.$$

Легко видеть, что при $t\to\infty$ выполнено

$$\mathcal{F}^{=}(t,s,\ell)=|\mathcal{F}(t,s,\ell)|(1+o(1)).$$

Таким образом, для доказательства утверждения теоремы будет достаточно рассматривать только гиперграфы из семейства $\mathcal{F}^{=}(t,s,\ell)$. Определим ансамбль $E(N_1,t,s)$, состоящий из двоичных $(N_1\times t)$-матриц $X=||x_i(j)||$, в котором каждый элемент $x_i(j)$ матрицы выбирается независимо и равновероятно из множества $\{1,2,\ldots,s\}$. Далее заменим каждый s-ичный символ x в матрице X на двоичный столбец высоты s, который будет иметь ровно одну единицу на x-й позиции. Другими словами, в ходе этой процедуры s-ичная $(N_1\times t)$-матрица X заменяется на двоичную $(N_1 s\times t)$-матрицу X_1. Также можно сказать, что матрица X_1 состоит из N_1 слоев, таких что каждый слой (представленный двоичной $(s\times t)$-матрицей, которой соответствуют s тестов) состоит из t столбцов веса 1. Определим событие $A(s,\ell)$: «для данного гиперграфа $H\in\mathcal{F}^{=}(s,\ell,t)$ существует слой в X_1, такой что ответы на все s вопросов, соответствующих данному слою, являются положительными». Если это событие выполняется, то это означает, что по данному слою можно построить разбиение множества вершин V на непересекающиеся доли:

$$V_1\sqcup V_2\sqcup\ldots\sqcup V_s=V=\{1,2,\ldots,t\},$$

такое что $\mathbf{e}_1\in V_1$, $\mathbf{e}_2\in V_2,\ldots,\mathbf{e}_s\in V_s$, причем V_1 можно определить как множество, содержащее номера столбцов, у которых стоит единица в 1-й строчке данного слоя, V_2 – множество, содержащее номера столбцов, у которых стоит единица во 2-й строчке данного слоя, и т.д. Обозначим объем множества V_i с помощью символа $t_i=|V_i|$. Далее оценим вероятность противоположного события к $A(s,\ell)$:

$$\Pr\left(\overline{A(s,\ell)}\right)=\left(1-\frac{s!}{s^{s\ell}}\right)^{N_1}.$$

Пусть $t\to\infty$ и $N_1=o(\log_2 t)$. Тогда для любого $\varepsilon'>0$ существует $N'(\varepsilon')$, такое что для любого $N_1\geqslant N'(\varepsilon')$ вероятность $\Pr\left(\overline{A(s,\ell)}\right)\leqslant\varepsilon$. Это означает, что существует $(N_1 s\times t)$-матрица X_1, которая может быть использована на первом шаге (двухшагового алгоритма) поиска скрытого гиперграфа, и для некоторых $(1-\varepsilon')|\mathcal{F}^{=}(s,\ell,t)|$ гиперграфов существует s вопросов, ответы на

которые положительны, и при этом вопросы попарно не пересекаются между собой как множества. Итак, те гиперграфы, для которых существует такое разбиение, будем называть *хорошими*. Обозначим через $\mathbf{G}(X_1)$ множество всех хороших гиперграфов для кода X_1.

Далее воспользуемся леммой, ранее установленной в [6].

Лемма 3.3.3. [6]. *Для любого ε существует неадаптивный алгоритм поиска скрытого гиперграфа из семейства $\mathcal{F}^{=}(t,\ell,1)$ с вероятностью ошибки ε, который состоит из не более $\ell\log_2 t(1+o(1))$ вопросов. Иными словами, пропускная способность $C_h^{na}(\ell,1)=1/\ell$.*

Заметим, следующий очевидный факт. Если в коде Y, представляющем неадаптивный поиск скрытого гиперграфа из семейства $\mathcal{F}^{=}(t,\ell,1)$ (другими словами, поиск ℓ дефектов) с вероятностью ошибки ε, заменить каждый элемент по правилу: $0\to 1$, $1\to 0$, тогда получим код Y', который является матрицей неадаптивного поиска скрытого гиперграфа из семейства $\mathcal{F}^{=}(t,1,\ell)$ (другими словами, он будет соответствовать поиску одного ребра размера ℓ) с вероятностью ошибки ε.

Грубо говоря, для хорошего гиперграфа на втором шаге поиска будет достаточно использовать s неадаптивных алгоритмов поиска ребра, состоящего из ℓ вершин, с вероятностью ошибки ε для того, чтобы с большой вероятностью найти s ребер в каждой из долей V_i. Докажем, что так можно сделать. Для этого воспользуемся леммой 3.3.3. Определим ансамбль $E(N_2,t)$, состоящий из двоичных $(N_2\times t)$-матриц, которые получены с помощью перестановки столбцов матрицы Y, которая представляет неадаптивный поиск ребра размера ℓ с вероятностью ошибки ε, причем каждая копия матрицы Y выбирается независимо и равновероятно с вероятностью $1/t!$. Пусть для хорошего гиперграфа H после первого шага алгоритма поиска скрытого гиперграфа имеется разбиение на непересекающиеся множества $V_1\sqcup V_2\sqcup\ldots\sqcup V_s=V=[t]$, так что $\mathbf{e}_1\in V_1$, $\mathbf{e}_2\in V_2,\ldots,\mathbf{e}_s\in V_s$. На втором шаге данного алгоритма для вершин V_1 воспользуемся N_2 тестами матрицы Y, при этом не используя вершины $V\setminus V_1$, для вершин V_2 — N_2 тестами матрицы Y, при этом не будем использовать вершины $V\setminus V_2$, и т.д. Определим событие $B(s,\ell)$: «все ребра хорошего гиперграфа H могут быть найдены, после использования sN_2 тестов». Оценим вероятность противоположного события к $B(s,\ell)$

$$\Pr\left(\overline{B(s,\ell)}\right)\leqslant s\varepsilon.$$

Это означает, что существует такой код X_2, полученный перестановкой столбцов из Y, что для $(1-s\varepsilon)\cdot|\mathbf{G}(X_1)|$ хороших гиперграфов можно обнаружить все ребра после второго шага алгоритма поиска.

Наконец, для любого $\varepsilon>0$ существует возрастающая последовательность $\{t_n\}$, $n=1,2,\ldots$, такая что для $(1-\varepsilon)|\mathcal{F}(t_n,s,\ell)|$ гиперграфов найдется

код X_1, который может быть использован на первом шаге алгоритма поиска из семейства $\mathcal{F}(t_n, s, \ell)$, и код X_2, который может быть использована на втором шаге алгоритма поиска, так что общее число тестов не превосходит $s\ell \log_2 t_n(1 + o(1))$, $n \to \infty$.

Лемма 3.3.2 доказана. □

Заключение

В настоящей диссертационной работе были доказаны новые нижние границы для асимптотической скорости $R(s, \ell)$ свободных от перекрытий кодов и впервые получены оценки сверху и снизу для пропускной способности $C(s, \ell)$ почти свободных от перекрытий кодов. Также были исследованы некоторые алгоритмы поиска скрытого гиперграфа из семейства локализованных гиперграфов. В частности, была найдена асимптотическая скорость $R_h^a(s, \ell)$ адаптивного алгоритма поиска скрытого гиперграфа и пропускная способность $C_h^{2\text{-st}}(s, \ell)$ двухступенчатой процедуры поиска скрытого гиперграфа.

Дальнейшее исследование темы диссертации может быть связано с доказательством (или опровержением) гипотезы, что пропускная способность неадаптивного поиска скрытого гиперграфа из семейства локализованных гиперграфов достигает теоретико-информационной границы. Кроме того, большой интерес представляет порядок главного члена асимптотики скорости $R(s, 1)$ при $s \to \infty$. На текущий момент существуют две гипотезы, которые следуют из доказанных верхней и нижней границ: $1/s^2$ и $\ln s/s^2$.

Литература

[1] Бассалыго Л. А., Рыков В. В., Гиперканал множественного доступа // *Пробл. передачи информ.*, **49**:4 (2013), 3–12.

[2] Галеев Э. М., Тихомиров В. М., Оптимизация: теория, примеры, задачи. *М.: Эдиториал УРСС*, 2000.

[3] Дьячков А. Г., Рыков В. В., Границы длины дизъюнктивных кодов // *Пробл. передачи информ.*, **18**:3 (1982), 7–13.

[4] Ким Ш. Х., Лебедев В. С., Об оптимальности тривиальных кодов, свободных от (w, r)-перекрытий // *Пробл. передачи информ.*, **40**:3 (2004), 13–20.

[5] Лебедев В. С., Асимптотическая верхняя граница скорости кодов, свободных от (w, r)-перекрытий // *Пробл. передачи информ.*, **39**:4 (2003), 3–9.

[6] Малютов М. Б., Фрейдлина В. Л., О применении теории информации к одной задаче выделения значимых факторов // *Теория вероятностей и ее применения*, **18**:2 (1973), 432—444.

[7] Сагалович Ю. Л., Разделяющие системы // *Пробл. передачи информ.*, **30**:2 (1994), 14–35.

[8] Сидельников В. М., Приходов О. Ю., О построении кодов, свободных от (w, r)-перекрытий // *Пробл. передачи информ.*, **45**:1 (2009), 36–40.

[9] Чисар И., Кернер Я., Теория информации. Теоремы кодирования для дискретных систем без памяти // *М.: Мир*, 1985.

[10] Abasi H., Bshouty N. H., Mazzawi H., On Exact Learning Monotone DBF from Membership Queries // *Lecture Notes in Artificial Intelligence*, (2014), 111–124.

[11] Angluin D., Chen J., Learning a hidden hypergraph // *Journal of Machine Learning Research*, **7** (2006), 2215–2236.

[12] Angluin D., Chen J., Learning a hidden graph using $O(\log n)$ queries per edge // *J. Comput. Syst. Sci.*, **74** (2008), 546–556.

[13] Chen H-B., Fu H-L., Nonadaptive Algorithms for Threshold Group Testing // *Discrete Applied Mathematics*, **157** (2009), 1581–1585.

[14] Du D. Z., Hwang F. K., Combinatorial Group Testing and Its Applications, 2nd ed., *Series on Applied Mathematics*, **12** (2000).

[15] D'yachkov A. G., Rykov V. V., A Survey of Superimposed Code Theory // *Prob. of Control and Inform. Theory*, **12**:4 (1983), 229–242.

[16] D'yachkov A. G., Rykov V. V., Rashad A. M., Superimposed Distance Codes // *Problems of Control and Inform. Theory*, **18**:4 (1989), 237–250.

[17] D'yachkov A. G., Macula A. J., Rykov V. V., New Constructions of Superimposed Codes // *IEEE Trans. Inform. Theory*, **46**:1 (2000), 284–290.

[18] D'yachkov A. G., Macula A. J., Rykov V. V., New Applications and Results of Superimposed Code Theory Arising from the Potentialities of Molecular Biology // In the book «Numbers, Information and Complexit», *Kluwer Academic Publishers*, (2000), 265–282.

[19] D'yachkov A., Vilenkin P., Macula A., Torney D., Families of Finite Sets in Which No Intersection of ℓ Sets Is Covered by the Union of s Others // *J. Combin. Theory*, Ser. A, **99** (2002), 195–218.

[20] D'yachkov A. G., Vilenkin P. A., Yekhanin S. M., Upper Bounds on the Rate of Superimposed (s, ℓ)-Codes Based on Engel's Inequality // *Proc. Eighth Int. Workshop «Algebraic and Combinatorial Coding Theory»*, Tsarskoe Selo, (2002), 95–99.

[21] D'yachkov A. G., Rykov V. V., Deppe C., Lebedev V. S., Superimposed Codes and Threshold Group Testing // Information Theory, Combinatorics, and Search Theory, *Lecture Notes in Computer Science*, **7777** (2013), 509–533.

[22] Engel K., Interval Packing and Covering in the Boolean Lattice // *Combinatorics Prob. and Computing*, **5** (1996), 373–384.

[23] Erdos P., Frankl P., Furedi Z., Families of Finite Sets in Which No Set Is Covered by the Union of two Others // *J. Combin. Theory*, Ser. A, **33** (1982), 158–166.

[24] Erdos P., Frankl P., Furedi Z., Families of Finite Sets in Which No Set Is Covered by the Union of r Others // *Israel J. Math.*, **51** (1985), 79–89.

[25] Friedman A. D., Graham R. L., Ullman J. D., Universal single transition time asynchronous state assignments // *IEEE Trans. Comput.*, **18**:6 (1969), 541–547.

[26] Gallager R. G., Information Theory and Reliable Communication, *J. Wiley*, New York, 1968.

[27] Hwang F. K., Sos V. Z., Non adaptive hypergeometric group testing // *Studia Sci. Math. Hungarica*, **22** (1987), 257–263.

[28] Kautz W. H., Singleton R. C., Nonrandom Binary Superimposed Codes // *IEEE Trans. Inform. Theory*, **10**:4 (1964), 363–377.

[29] Kim H., Lebedev V. S., On Optimal Superimposed Codes // *J. Combin. Des.*, **12**:2 (2004), 79–91.

[30] Kim H., Lebedev V., Oh D., Some new results on superimposed codes, *J. Combin. Des.*, **13**:4 (2005), 276—285.

[31] Macula A. J., A simple construction of d-disjunct matrices with certain constant weights // *Discrete Math.*, Ser. A, **162**:1-3 (1996), 311–312.

[32] Macula A. J., Rykov V. V., Yekhanin S., Trivial two-stage group testing for complexes using almost disjunct matrices // *Discrete Applied Mathematics*, **137**:1 (2004), 97—107.

[33] Mitchell C. J., Piper F. C., Key storage in Secure Networks // *Discrete Applied Mathematics*, **21** (1988), 215–228.

[34] Quang A. N., Zeisel T., Bounds on Constant Weight Binary Superimposed Codes // *Problems of Control and Inform. Theory*, **17**:4 (1988), 223–230.

[35] Ruszinko M., On the upper bound of the size of the r-cover-free families // *J. Combin. Theory*, Ser. A., **66** (1994), 302–310.

[36] Stinson D. R., Wei R., Zhu L., Some New Bounds for Cover-Free Families // *J. Combin. Theory*, Ser. A, **90** (2000), 224–234.

Публикации автора

[37] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю., Границы скорости дизъюнктивных кодов // *Пробл. передачи информ.*, **50**:1 (2014), 31–63.

[38] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю., Почти дизъюнктивные коды со списочным декодированием // *Пробл. передачи информ.*, **51**:2 (2015), 27–49.

[39] Полянский Н. А., Почти свободные от перекрытий коды // *Пробл. передачи информ.*, **52**:2 (2016), 46–60.

[40] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Almost Disjunctive List-Decoding Codes // *Proc. 14th Int'l Workshop «Algebraic and Combinatorial Coding Theory»*, Svetlogorsk, (2014), 115–126.

[41] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Bounds on the Rate of Superimposed Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Honolulu, (2014), 2341–2345.

[42] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Almost Cover-Free Codes and Designs // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2899–2903.

[43] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Cover-Free Codes and Separating System Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2894–2898.

[44] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Symmetric Disjunctive List-Decoding Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2236–2240.

[45] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., On Multistage Learning a Hidden Hypergraph // *Proc. IEEE Int'l Symp. Inf. Theory*, Barcelona, 2016.

[46] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., On a Hypergraph Approach to Multistage Group Testing Problems // *Proc. IEEE Int'l Symp. Inf. Theory*, Barcelona, 2016.