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

На правах рукописи
УДК 519.2, 621.391.15

ЩУКИН Владислав Юрьевич

Дизъюнктивные коды со списочным декодированием

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

Актуальность и история вопроса

Тематика данной диссертации лежит на стыке теории вероятностей, теории информации и комбинаторной теории кодирования. Основным объектом изучения являются семейства кодов, обслуживающие канал множественного доступа.

Математическая модель *канала множественного доступа* (КМД) [8] представляет из себя дискретный канал без памяти, имеющий s входов и один выход. На входы поступают q-ичные символы $x_1, x_2, \ldots, x_s$ из алфавита $\{0, 1, \ldots, q-1\}$, а на выходе воспроизводится символ $y = f(x_1, x_2, \ldots, x_s)$. Возникает задача построения кодов для передачи сообщений через КМД и методов для их восстановления. Через КМД посимвольно передаются последовательности q-ичных символов длины N, представляющие из себя закодированные сообщения. Требуется возможность восстанавливать передаваемые сообщения по последовательности длины N на выходе. Причем для фиксированного количества всех различных сообщений t длина кодовых слов N должна быть минимальной.

Особое место занимает модель *дизъюнктивного канала множественного доступа* [3], в которой $q = 2$, а функция f представляет из себя дизъюнктивную сумму аргументов, т.е. принимает значение 0, если все (двоичные) сигналы на входе равны 0, и принимает значение 1 иначе. Благодаря значительному разнообразию приложений (групповое тестирование [24], поиск файлов в системах хранения [35], совокупные цифровые подписи [34] и другие) коды для дизъюнктивного КМД достаточно хорошо изучены.

В наиболее актуальной для приложений ситуации некоторые отправители могут молчать, т.е. число передаваемых сообщений $\leq s$. Для того, чтобы восстановить исходные кодовые слова по их дизъюнктивной сумме, необходимо и достаточно, чтобы дизъюнктивные суммы всех различных подмножеств кодовых слов мощности $\leq s$ отличались. Восстановление передаваемых кодовых слов путем перебора всех подмножеств мощности $\leq s$ и отысканием подмножества с дизъюнктивной суммой, совпадающей с выходом канала, будем называть *переборным декодированием* [7], а удовлетворяющие данному свойству коды – *дизъюнктивными s-планами* [35, 25].

Будем говорить, что двоичный столбец $\boldsymbol{u}$ *покрывает* двоичный столбец $\boldsymbol{v}$, если дизъюнктивная сумма $\boldsymbol{u}$ и $\boldsymbol{v}$ не отличается от $\boldsymbol{u}$, т.е. $\boldsymbol{u} \bigvee \boldsymbol{v} = \boldsymbol{u}$. Так называемое *пофакторное декодирование* [7], требующее немного большей длины кодовых слов при том же количестве всех различных сообщений, однако имеющее более простой и быстрый алгоритм восстановления сообщений, основано на *дизъюнктивных s-кодах* [35]. По определению, дизъюнктивная сумма любых s кодовых слов дизъюнктивного s-кода не покрывает постороннего кодового слова. Таким образом, пофакторное декодирование заключается в поиске тех кодовых слов, которые покрываются выходом КМД.

Дизъюнктивные s-коды и s-планы были введены У. Каутсом и Р. Синглетоном в 1964 году в основополагающей статье [35], где также получены первые нетривиальные свойства

и описан ряд прикладных задач. *Асимптотической скоростью* дизъюнктивных s-кодов (s-планов) будем называть величину

$$R(s) = \lim_{N\to\infty} \frac{\log_2 t(s,N)}{N} \quad \left(R(\le s) = \lim_{N\to\infty} \frac{\log_2 \tilde{t}(s,N)}{N} \right),$$

где $t(s,N)$ ($\tilde{t}(s,N)$) означает максимальный объем дизъюнктивных s-кодов (s-планов) длины N. В частности, в работе [35] показано

$$R(s) \le R(\le s) \le R(s-1), \quad R(\le s) \le \frac{1}{s}.$$

В случае $s = 2$ в 1982 году П. Эрдеш и др. [29] доказали оценки, из которых следуют неравенства

$$0.182 \le R(2) \le 0.322. \tag{1}$$

Эти неравенства представляют из себя наилучшие известные нижнюю и верхнюю границы для $R(2)$ и в настоящее время. В том же 1982 году А.Г. Дьячков и В.В. Рыков [4] иным методом вывели верхнюю границу, которая в случае $s = 2$ совпадает с правой частью (1), а при $s \to \infty$ асимптотически эквивалентна неравенству

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

Нижняя граница скорости $R(s)$ была получена в 1983 году А.Г. Дьячковым и В.В. Рыковым в работе [25], из которой следует асимптотическое неравенство

$$R(s) \ge \frac{\log_2 e}{es^2}(1 + o(1)) = \frac{0.5307}{s^2}(1 + o(1)), \quad s \to \infty. \tag{2}$$

Немного позже, в 1985 году, П. Эрдешем и др. [30] независимо от [25] выведена нижняя граница, которая для больших значений параметра s ведет себя следующим образом:

$$R(s) \ge \frac{\log_2 e}{4s^2}(1 + o(1)) = \frac{0.3607}{s^2}(1 + o(1)), \quad s \to \infty.$$

А.Г. Дьячков и др. [26] впоследствие улучшили результат 1983 года [25] и в 1989 году новым методом доказали нижнюю границу для скорости $R(s)$, из которой при $s = 2$ следует левая часть неравенства (1), а при $s \to \infty$ асимптотическое неравенство:

$$R(s) \ge \frac{1}{s^2 \log_2 e}(1 + o(1)) = \frac{0.6931}{s^2}(1 + o(1)), \quad s \to \infty. \tag{3}$$

Для многих приложений достаточно более слабого свойства кода. Двоичный код называется *дизъюнктивным кодом со списочным декодированием силы s с объемом списка L* (СД s_L-кодом), если дизъюнктивная сумма любых s кодовых слов покрывает не более $L-1$ других кодовых слов. Таким образом, если кодировать сообщения с помощью СД s_L-кода, при пофакторном декодировании получим список кодовых слов, среди которых будут присутствовать все $\le s$ переданных и $\le L-1$ лишних кодовых слов. СД s_L-коды были введены в 1981 году А.Г. Дьячковым и В.В. Рыковым в работе [3], где рассматривалось использование таких кодов при передаче информации через дизъюнктивный КМД в системе связи АЛОХА. В работе П.А. Виленкина 1998 года [42] приведены некоторые конструкции СД s_L-кодов, а также рассмотрено их применение при построении двухступенчатых процедур групповых проверок.

Аналогичным образом введем *асимптотическую скорость* СД s_L-кодов:

$$R_L(s) = \lim_{N\to\infty} \frac{\log_2 t(s, L, N)}{N},$$

где через $t(s, L, N)$ обозначен максимальный объем СД s_L-кодов длины N. В 1983 году А.Г. Дьячков и В.В. Рыков [25] получили нижнюю и верхние границы скорости $R_L(s)$, из которых, в частности, следуют неравенства:

$$R_L(s) \le \frac{1}{s}, \quad \text{при любых натуральных } s \text{ и } L;$$
$$\frac{L\log_2 e}{es^2}(1+o(1)) \le R_L(s) \le \frac{2L^2\log_2 s}{s^2}(1+o(1)), \quad \text{при } s\to\infty.$$

Отметим, что (2) является частным случаем данной нижней границы для $R_L(s)$. Позднее, в 2003 году А.Г. Дьяков [28] получил новую нижнюю границу на скорость $R_L(s)$, из которой следует асимптотическое неравенство

$$R(s) \ge \frac{L}{s^2\log_2 e}(1+o(1)), \quad s\to\infty,$$

обобщающее (3). А в 2005 году А. Де Бонис и др. [23] улучшили верхнюю границу на скорость $R_L(s)$ для достаточно больших значений параметра L и получили асимптотическое неравенство:

$$R_L(s) \le \frac{8L\log_2 s}{s^2}(1+o(1)), \quad s\to\infty.$$

Также для приложений допустимо использование алгоритмов, которые предполагают незначительную ошибку при восстановлении кодовых слов, переданных через КМД. В связи с этим, Э. Макула и др. [36] ввели понятие *почти дизъюнктивных* (s, ε)*-кодов*. По определению, у такого кода доля множеств из s кодовых слов, дизъюнктивная сумма которых покрывает хотя бы одно другое кодовое слово, не превосходит ε. Таким образом, при использовании почти дизъюнктивных (s, ε)-кодов для кодирования сообщений, передаваемых через дизъюнктивный КМД, пофакторное декодирование не восстанавливает переданные кодовые слова с вероятностью $\le \varepsilon$.

В работе [27] приведены конструкции почти дизъюнктивных (s, ε)-кодов, основанные на укороченных кодах Рида-Соломона. Асимптотическое поведение ошибки ε для данных конструкций посчитано в 2013 году Л.А. Бассалыго и В.В. Рыковым [1], откуда следует существование почти дизъюнктивных (s, ε)-кодов длины N и объема t, таких что:

$$\frac{\log_2 t}{N} = \frac{\ln 2}{s}(1+o(1)), \quad s^2 = \Theta(N), \quad \varepsilon\to 0, \quad \text{при } N\to\infty. \tag{4}$$

Следует отметить, что если число $\ln 2$ в (4) заменить на произвольную меньшую положительную константу, то ошибка ε убывает к нулю экспоненциально.

Обобщением почти дизъюнктивных (s, ε)-кодов, а также СД s_L-кодов, выступают *почти дизъюнктивные* (s_L, ε)*-коды со списочным декодированием* (СД (s_L, ε)-коды), для которых доля множеств из s кодовых слов, дизъюнктивная сумма которых покрывает $\ge L$ других кодовых слов, не превосходит ε. Под *экспонентой ошибки* $\mathbf{E}_L(s, R)$ будем подразумевать максимальный показатель экспоненциального убывания ошибки ε для последовательности СД (s_L, ε)-кодов возрастающей длины и фиксированной скорости R, а под

пропускной способностью $C_L(s)$ – верхнюю грань значений скорости R, для которых экспонента ошибки $\mathbf{E}_L(s,R)$ положительна. В недавней работе [45] И.В. Воробьевым доказана нижняя граница для пропускной способности:

$$C_L(s) \geq \frac{\ln 2}{s}, \quad s \to \infty.$$

Вызывает интерес, что данная нижняя граница для фиксированного значения параметра s совпадает со скоростью конструкций (4), где, однако, параметр s зависит от длины кода.

Введем аналогичное вероятностное обобщение для дизъюнктивных s-планов. Двоичный код называется *почти дизъюнктивным* (s,ε)*-планом*, если доля множеств из s кодовых слов, для которых существует другое множество из s кодовых слов с такой же дизъюнктивной суммой, не превосходит ε. *Пропускной способностью* $C(\leq s)$ почти дизъюнктивных s-планов будем называть верхнюю грань скорости почти дизъюнктивных (s,ε)-планов, для которых $\varepsilon \to 0$ при росте длины кода. Фундаментальным результатом является следующее точное равенство, доказанное В.Л. Фрейдлиной [7] и М.Б. Малютовым [6]:

$$C(\leq s) = \frac{1}{s}, \quad s \geq 1.$$

Рассмотрим теперь ситуацию, когда число кодовых слов поступивших на входы дизъюнктивного КМД неизвестно (и не удовлетворяет условию $\leq s$). Наиболее наглядно такой случай представляется на примере модели группового тестирования с неизвестным числом дефектов. Предположим, что задано множество из t элементов, среди которых присутствует неизвестное число s_{un}, $0 \leq s_{un} \leq t$, дефектных элементов. Требуется найти все дефекты за минимальное число групповых тестов, где под групповым тестом подразумевается некоторое подмножество элементов, а результат теста равен 1, если хотя бы один дефектный элемент попал в тестируемое множество, и 0 – иначе. Процедуру группового тестирования называют адаптивной, если каждый следующий тест строится, исходя из результатов предыдущих, и неадаптивной, если все тесты формируются изначально и могут проводиться одновременно. Различают также k-ступенчатые процедуры групповых проверок, для которых формирование тестов на l-й ступени, $1 \leq l \leq k$, основывается на результатах тестов на ступенях $1, 2, \ldots, l-1$. В случае неадаптивного алгоритма N тестов представляют в виде двоичной матрицы из N строк и t столбцов, в которой каждая строка сопоставляется некоторому тесту, каждый столбец – некоторому элементу, а на пересечении i-й строки и j-го столбца стоит 1 тогда и только тогда, когда j-й элемент включен в i-й тест. Очевидно, что столбец результатов тестов равен дизъюнктивной сумме столбцов, соответствующих дефектным элементам.

Большинство разработанных неадаптивных алгоритмов группового тестирования предполагают ограничение на количество дефектов: $s_{un} \leq s$, однако в случае отсутствия такого предположения возникает необходимость прибегнуть к k-ступенчатым процедурам групповых проверок. В 2002 году Т. Бергер и В.И. Левенштейн [14] рассматривали применение *двухступенчатых процедур восстановления* в модели группового тестирования, в которой каждый элемент является дефектным с вероятностью p. В такой процедуре на первом этапе применяется некоторое количество неадаптивных тестов, а на второй ступени по одиночке проверяется каждый элемент из числа тех, что остались подозрительными после первой ступени. Для некоторых случаев зависимости вероятности p от общего количества элементов t в работе [14] получены как верхние, так и нижние границы для асимптотики математического ожидания общего количества тестов N. Например,

$$\frac{\log_2 e}{4}\frac{(\ln t)^2}{\ln\ln t}(1+o(1)) \leq E[N] \leq \frac{(\ln t)^2}{\ln\ln t}(1+o(1)), \quad p(t) = \frac{1}{t}(1+o(1)), \quad t \to \infty.$$

Отметим, что для случая $p = 1/t^{-\beta}$, $0 < \beta < 1$, верхние и нижние границы для $E[N]$ были улучшены в работе [37].

Другой подход к задаче группового тестирования с неизвестным числом дефектных элементов был предложен в 2010 году П. Дамашке и А.Ш. Мухаммадом [21]. Для начала с помощью групповых тестов производится оценивание количества дефектов, а затем, на основе полученной оценки, применяется один из известных алгоритмов для поиска ограниченного числа дефектов. В статье [21] авторы построили случайную конструкцию неадаптивной процедуры групповых проверок, с помощью которой за $G(\varepsilon, c)\log_2 t$ тестов определяется статистика $\hat{s}$, удовлетворяющая следующим условиям: вероятность $\Pr\{\hat{s} < s_{un}\}$ ограничена сверху параметром $\varepsilon \ll 1$, а математическое ожидание величины $\hat{s}/s_{un}$ ограничено сверху параметром $c > 1$. Отметим, что указанный результат является *универсальным*, то есть не зависит от распределения множества дефектных элементов. Адаптивные алгоритмы для получения похожей оценки для количества дефектных элементов описаны в статьях [19, 31].

Рассмотрим теперь другую модель КМД. КМД называется q-ичным *гиперканалом множественного доступа* [1, 16] (ГМД), если при поступлении на его s входов q-ичных символов $x_1, x_2, \ldots, x_s$, на выходе получим *гиперсумму* этих символов, т.е. множество всех поступивших на входы символов:

$$\bigcup_{k=1}^{s}\{x_k\}.$$

Отметим, что данная модель КМД имеет различные названия в научной литературе, причем, зачастую, наблюдается отсутствие ссылок на раннее вышедшие работы. Так, в статье [16] ГМД называют A channel.

Последовательности, символами которых являются подмножества, будем называть *гиперсловами*. По аналогии с дизъюнктивной моделью КМД введем следующие понятия. Гиперслово $\boldsymbol{u}$ *подчиняет* гиперслово $\boldsymbol{v}$, если гиперсумма $\boldsymbol{u}$ и $\boldsymbol{v}$ не отличается от $\boldsymbol{u}$. q-ичный код называется *s-гиперкодом*, если гиперсумма произвольных s кодовых слов не подчиняет другого кодового слова; *s-гиперпланом*, если гиперсумма произвольных $\leq s$ кодовых слов отличается от гиперсуммы любого другого набора из $\leq s$ кодовых слов. В англоязычной литературе s-гиперкод и s-гиперплан обычно называют s-frameproof code и s-separable code, соответственно. *Асимптотической скоростью* q-ичных s-гиперкодов (q-ичных s-гиперпланов) будем называть величину

$$R^{(q)}(s) = \lim_{N\to\infty}\frac{\log_q t^{(q)}(s,N)}{N} \quad \left(R^{(q)}(\leq s) = \lim_{N\to\infty}\frac{\log_2 \tilde{t}^{(q)}(s,N)}{N}\right),$$

где $t^{(q)}(s,N)$ ($\tilde{t}^{(q)}(s,N)$) означает максимальный объем q-ичных s-гиперкодов (q-ичных s-гиперпланов) длины N.

Мотивированные возможностью использования для защиты авторских прав на цифровую продукцию от недобросовестного распространения, q-ичные s-гиперкоды были введены Д. Боне и Д. Шоу в 1998 году [15]. Отметим, что двоичные s-гиперкоды, или *симметричные дизъюнктивные s-коды*, рассматривались и ранее [3]. А. Хан Винк и С. Мартиросян в 2000 году [43] и С. Блэкберн в 2003 году [12] независимо построили некоторые конструкции s-гиперкодов, основанные на укороченных кодах Рида-Соломона. Примечательно, что в недавних статьях [11, 41] Т. Ван Чунг и М. Базрафшан доказали оптимальность данных конструкций.

Также в работах [43, 12, 20] независимо получена верхняя граница на скорость s-

гиперкодов:

$$R^{(q)}(s) \leq \frac{1}{s}. \tag{5}$$

В недавней работе [39] 2014 года Ч. Шенгуэн и др. построили новую верхнюю границу, которая улучшает (5) для больших значений параметра s и порождает асимптотическое неравенство

$$R^{(q)}(s) \leq \frac{4(q-1)\log_q s}{s^2}(1+o(1)), \quad s \to \infty.$$

В 2008 году Д. Стинсон и др. [40] вероятностным методом построили нижнюю границу на скорость $R^{(q)}(s)$:

$$R^{(q)}(s) \geq \frac{1}{s}\log_q\left[\frac{q^s}{q^s-(q-1)^s}\right], \quad q \geq 2, \quad s \geq 2, \tag{6}$$

асимптотическое поведение которой при $s \to \infty$ описывается выражением $O\left(\frac{1}{s}\left(1-\frac{1}{q}\right)^s\right)$. Оптимизируя метод случайного кодирования из [40], авторы уже упоминаемой работы [39] улучшили данную нижнюю границу (6) для больших значений параметра s и получили асимптотическое неравенство

$$R^{(q)}(s) \geq \frac{q-1}{s^2 e \ln q}(1+o(1)), \quad s \to \infty.$$

Отметим, что нижняя граница (6) достигает верхнюю границу (5) при росте q, откуда следует

$$\lim_{q\to\infty} R^{(q)}(s) = \frac{1}{s}.$$

Доказательство этого результата получено и ранее [20] и опирается на конструкциях q-ичных s-гиперкодов, основанных на алгебро-геометрических кодах.

В 2011 году М. Ченг и Ин Мяо [17] ввели s-гиперпланы в контексте защиты авторских прав на цифровую продукцию и идентификации недобросовестных пользователей, а также установили следующие соотношения между скоростями s-гиперкодов и s-гиперпланов:

$$R^{(q)}(s) \leq R^{(q)}(\leq s) \leq R^{(q)}(s-1). \tag{7}$$

Границы для скорости s-гиперпланов, вытекающие из предыдущего неравенства (7) и известных границ для $R^{(q)}(s)$, были улучшены в недавних работах [33, 13] для частного случая $s = 2$, где получено неравенство $R^{(q)}(2) \leq 2/3$.

Наряду с СД s_L-кодами, описанными выше, рассматривают *q-ичные гиперкоды со списочным декодированием силы s с объемом списка L* (кратко, q-ичные СД s_L-гиперкоды). По определению, гиперсумма произвольных s кодовых слов q-ичного СД s_L-гиперкода подчиняет не более $L-1$ других кодовых слов. По аналогии с рассмотренными ранее семействами кодов, вводится *асимптотическая скорость* СД s_L-гиперкодов, обозначим ее через $R_L^{(q)}(s)$. Для двоичного случая в 1989 году А. Рашад [38] построил нижнюю границу случайного кодирования для скорости $R_L^{(2)}(s)$, используя ансамбль кодов с независимыми одинаково распределенными двоичными компонентами кодовых слов. Асимптотическое поведение данной границы при $s \to \infty$ описывается неравенством:

$$R_L^{(2)}(s) \geq \frac{L\log_2 e}{es^2}(1+o(1)), \quad s \to \infty.$$

Цели работы

Целями диссертационной работы являются:

- Построение более точных нижних границ для асимптотической скорости дизъюнктивных кодов со списочным декодированием;
- Построение нижних и верхних границ для пропускной способности и экспоненты ошибки почти дизъюнктивных кодов со списочным декодированием;
- Исследование алгоритмов для определения количества дефектных элементов в дизъюнктивной модели группового тестирования;
- Построение более точных нижних и верхних границ для асимптотической скорости гиперкодов со списочным декодированием.

Научная новизна работы

Все результаты, представленные в диссертации, являются новыми. В работе впервые исследуется задача сравнения количества дефектных элементов с заданной константой в дизъюнктивной модели группового тестирования. Также в работе впервые рассматриваются q-ичные СД s_L-гиперкоды с мощностью алфавита $q > 2$ и объемом списка $L > 1$.

Основные результаты работы

Основные результаты, полученные в диссертации, перечислены ниже.

1. Установлена новая нижняя граница для асимптотической скорости $R_L(s)$ дизъюнктивных кодов со списочным декодированием, которая является наилучшей и в случае $L > 1$ превосходит наилучшую ранее известную нижнюю границу, полученную А.Г. Дьячковым [28]. См. ниже теорему 1.2.2 и таблицу 1.2.1.
2. Впервые получена нижняя граница для экспоненты ошибки $\mathbf{E}_L(s, R)$ почти дизъюнктивных кодов со списочным декодированием. См. ниже теорему 2.2.2.
3. Впервые получена верхняя граница для пропускной способности $C_L(s)$ почти дизъюнктивных кодов со списочным декодированием. См. ниже теорему 2.3.1.
4. Предложен нестандартный алгоритм декодирования результатов дизъюнктивных групповых тестов в задаче сравнения количества дефектных элементов с заданной константой, который по сравнению со стандартными алгоритмами позволяет использовать меньшее количество тестов для получения ответа с малой вероятностью ошибки. Для нового алгоритма получена нижняя граница на экспоненту вероятности ошибки. См. ниже теорему 3.2.1.
5. Доказаны новые нижние границы для асимптотической скорости $R_L^{(q)}(s)$ гиперкодов со списочным декодированием, которые улучшают ранее известные нижние границы, полученные Д. Стинсоном и др. [40], Ч. Шенгуэном и др. [39], А. Рашадом [38]. См. ниже теоремы 4.2.1 и 4.2.2, а также таблицы 4.4.1 и 4.4.2.

6. Выведена новая верхняя граница на асимптотическую скорость $R_L^{(q)}(s)$ гиперкодов со списочным декодированием, которая является наилучшей для достаточно больших значений параметра s и улучшает ранее известную верхнюю границу, доказанную Ч. Шэнгуэном и др. [39]. См. ниже теорему 4.3.1 и таблицу 4.4.1.

Методы исследования

В работе используются вероятностные методы, в частности метод случайного кодирования для ансамбля равновесных кодов. Для вычисления логарифмических асимптотик вероятностей больших уклонений применяются классические методы выпуклого анализа и аналитические методы. В работе также используются методы комбинаторной теории кодирования.

Теоретическая и практическая значимость работы

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

Апробация диссертации

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

1. Спецсеминар "Экстремальная комбинаторика и случайные структуры" в 2016 г., кафедра теории вероятностей, мехмат, МГУ.
2. Спецсеминар "Проблемы современной теории информации" в 2013–2016 гг., кафедра теории вероятностей, мехмат, МГУ.
3. Семинар по теории кодирования под рук. Л.А. Бассалыго в 2013–2016 гг., ИППИ РАН.
4. Семинар по дискретной математики под рук. М.В Вялого и С.П. Тарасова в 2016 г., ВЦ РАН.

Результаты диссертации докладывались автором на следующих конференциях.

1. Конференция "*Ломоносов–2013*", Москва, 2013.
2. 14th International Workshop "*Algebraic and Combinatorial Coding Theory*", Svetlogorsk, Russia, 2014.
3. Ninth International Workshop on Coding and Cryptography, Paris, France, 2015.
4. IEEE International Symposium on Information Theory, Hong Kong, China, 2015.
5. Конференция "*Ломоносов–2016*", Москва, 2016.
6. 15th International Workshop "*Algebraic and Combinatorial Coding Theory*", Albena, Bulgaria, 2016.

Публикации

Основные результаты настоящей диссертации опубликованы в работах [44]-[56], представленных в конце списка литературы. Среди них 6 работ [44]-[49] в журналах из перечня ВАК и 7 работ [50]-[56] в рецензируемых трудах международных конференций.

Краткое содержание диссертации

Настоящая диссертация состоит из введения, четырех глав, заключения и списка литературы. Нумерация утверждений, перечисленных ниже, совпадает с их нумерацией в соответствующих главах.

Во **введении** определены основные объекты исследования, представлен краткий исторический обзор результатов, а также приведено краткое содержание данной диссертации.

В **главе 1** рассматриваются коды для дизъюнктивного канала множественного доступа.

В разделе 1.1 введены используемые в главе 1 обозначения и определения.

Следующий раздел 1.2 посвящен нижним границам скорости дизъюнктивных СД s_L-кодов. С помощью метода случайного кодирования получена следующая теорема, устанавливающая наилучшие нижние границы для скорости СД s_L-кодов.

Теорема 1.2.2 (Граница случайного кодирования $\underline{R}_L(s)$)**.** *Имеют место следующие три утверждения.*
1. *Для скорости СД s_L-кодов справедливо неравенство*

$$R_L(s) \geq \underline{R}_L(s) \triangleq \frac{1}{s+L-1} \max_{0<Q<1} A_L(s,Q),$$

$$A_L(s,Q) \triangleq \log_2 \frac{Q}{1-y} - sK(Q,1-y) - L\,K\left(Q, \frac{1-y}{1-y^s}\right), \quad s \geq 2,\ L \geq 1,$$

где используется обозначение расстояния Кульбака:

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

а параметр y, $1-Q \leq y < 1$, определяется как единственный корень уравнения

$$y = 1 - Q + Qy^s \left[1 - \left(\frac{y-y^s}{1-y^s}\right)^L\right], \quad 1-Q \leq y < 1.$$

2. *При фиксированном $L = 1, 2, \ldots$ и $s \to \infty$ асимптотика границы случайного кодирования имеет вид*

$$\underline{R}_L(s) = \frac{L}{s^2 \log_2 e}(1 + o(1)), \quad s \to \infty.$$

3. *При фиксированном $s = 2, 3, \ldots$ и $L \to \infty$ существует предел*

$$\underline{R}_\infty(s) \triangleq \lim_{L\to\infty} \underline{R}_L(s) = \log_2 \left[\frac{(s-1)^{s-1}}{s^s} + 1\right].$$

Если $s \to \infty$, то данный предел $\underline{R}_\infty(s) = \frac{\log_2 e}{e \cdot s}(1 + o(1)) = \frac{0{,}5307}{s}(1 + o(1))$.

При доказательстве используется ансамбль $E(N,t,Q)$, $0<Q<1$, равновесных двоичных кодов длины N и объема t, для которых кодовые слова выбираются независимо и равновероятно из множества всех двоичных кодовых слов фиксированных длины N и веса $\lfloor QN \rfloor$. При фиксированном объеме кода t рассматривается вероятность $P(s,L,Q,N)$ *плохого события*: дизъюнктивная сумма фиксированного множества из s кодовых слов покрывает дизъюнктивную сумму фиксированного множества из L кодовых слов. Далее, через $P(s,L,Q,N)$ оценивается математическое ожидание количества кодовых слов, после удаления которых код становится СД s_L-кодом. Данная оценка приводит к нижней границе на скорость СД s_L-кодов:

$$R_L(s) \geq \underline{R}_L(s) \triangleq \frac{1}{s+L-1} \max_{0<Q<1} \varlimsup_{N\to\infty} \frac{-\log_2 P(s,L,Q,N)}{N}.$$

Используя терминологию типов последовательностей, задача нахождения логарифмической асимптотики вероятности $P(s,L,Q,N)$ сводится к поиску минимума функционала

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

в области с линейными ограничениями на распределение $\{\tau(\boldsymbol{a})\}$, $\boldsymbol{a}\in\{0,1\}^s$. Экстремальная задача решается стандартным методом множителей Лагранжа.

В разделе 1.3 сформулированы наилучшие верхние границы на скорость СД s_L-кодов.

В следующей **главе 2** рассматриваются почти дизъюнктивные коды со списочным декодированием. Основные определения вводятся в разделе 2.1. Под ошибкой $\varepsilon_L(s,R,N)$ будем подразумевать минимизированную по всем кодам X длины N и объема $t=\lfloor 2^{RN} \rfloor$ долю s-множеств кодовых слов, дизъюнктивная сумма которых покрывает $\geq L$ посторонних слов кода X. Экспонентой ошибки $\mathbf{E}_L(s,R)$ почти дизъюнктивных СД s_L-кодов и пропускной способностью $C_L(s)$ почти дизъюнктивных СД s_L-кодов назовем

$$\mathbf{E}_L(s,R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \varepsilon_L(s,R,N)}{N}, \quad R>0, \text{ и}$$

$$C_L(s) \triangleq \sup\{\, R \,:\, \mathbf{E}_L(s,R)>0\},$$

соответственно.

В разделе 2.2 с помощью метода случайного кодирования на ансамбле $E(N,t,Q)$, $0<Q<1$, равновесных двоичных кодов выведена нижняя граница на экспоненту ошибки почти дизъюнктивных СД s_L-кодов. Для начала, определим положительную часть функции:

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

а через $\underline{C}(s)$ обозначим нижнюю границу на пропускную способность $C_L(s)$, полученную И. Воробьевым в работе [45]:

$$C_L(s) \geq \underline{C}(s) \triangleq \max_{0<Q<1} \left\{ h(Q) - [1-(1-Q)^s]\, h\left(\frac{Q}{1-(1-Q)^s}\right)\right\}.$$

Теорема 2.2.2 (Нижняя граница для $\mathbf{E}_L(s,R)$)**.** *Справедливы три утверждения.*
1. *Величина* $\mathbf{E}_L(s,R)$ *удовлетворяет неравенству:*

$$\mathbf{E}_L(s,R) \geq \underline{\mathbf{E}}_L(s,R) \triangleq \max_{0<Q<1} E_L(s,R,Q), \quad s \geq 2,\ L \geq 1,\ R > 0,$$

$$E_L(s,R,Q) \triangleq \min_{Q \leq q \leq \min\{1,sQ\}} \left\{ \mathcal{A}(s,Q,q) + L \cdot [h(Q) - q \cdot h(Q/q) - R]^+ \right\},$$

где функция $\mathcal{A}(s,Q,q)$, $Q < q < \min\{1, sQ\}$, *определена следующим образом:*

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

а число y *в определении* $\mathcal{A}(s,Q,q)$ *является единственным решением уравнения*

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

2. *Для любых* $s \geq 2$ *и* $L \geq 1$ *нижняя граница* $\underline{\mathbf{E}}_L(s,R)$, *является* $\cup$*-выпуклой функцией параметра* $R > 0$. *При* $0 < R < \underline{C}(s)$ *справедливо неравенство* $\underline{\mathbf{E}}_L(s,R) > 0$. *Если* $R \geq \underline{C}(s)$, *то* $\underline{\mathbf{E}}_L(s,R) = 0$. *Кроме того, существует такое число* $\underline{R}_L^{(cr)}(s)$, $0 \leq \underline{R}_L^{(cr)}(s) < \underline{C}(s)$, *что*

$$\underline{\mathbf{E}}_L(s,R) = (s+L-1)\underline{R}_L(s) - LR, \quad \textit{при} \quad 0 \leq R \leq \underline{R}_L^{(cr)}(s), \tag{8}$$

и

$$\underline{\mathbf{E}}_L(s,R) > (s+L-1)\underline{R}_L(s) - LR, \quad \textit{при} \quad R > \underline{R}_L^{(cr)}(s),$$

где граница случайного кодирования $\underline{R}_L(s)$ *определена в теореме 1.2.2. Причем, прямая, задаваемая* (8), *является касательной к функции* $\underline{\mathbf{E}}_L(s,R)$ *в точке* $R = \underline{R}_L^{(cr)}(s)$.
3. *При любых* $s \geq 2$, $L \geq 1$ *и* $R \geq R_L^{(cr)}(s)$ *справедливо равенство* $\underline{\mathbf{E}}_L(s,R) = \underline{\mathbf{E}}_{L+1}(s,R)$, *а последовательности скорости* $R_L^{(cr)}(s)$ *и соответствующего значения нижней границы экспоненты ошибки имеют пределы:*

$$\lim_{L\to\infty} \underline{R}_L^{(cr)}(s) = \underline{R}_\infty(s),$$
$$\lim_{L\to\infty} \underline{\mathbf{E}}_L(s, \underline{R}_L^{(cr)}(s)) = (s-1)\underline{R}_\infty(s),$$

где скорость $\underline{R}_\infty(s)$ *определена в теореме 1.2.2.*

При доказательстве теоремы 2.2.2 рассматривается случайный код X длины N и объема t, распределение компонент которого подчиняется ансамблю $E(N,t,Q)$. Очевидные соображения, приводят к нижней границе на экспоненту ошибки почти дизъюнктивных СД s_L-кодов:

$$\mathbf{E}_L(s,R) \geq \overline{\lim_{N\to\infty}} \frac{-\log_2 P(s,L,Q,N,t)}{N},$$

где $P(s,L,Q,N,t)$ – вероятность того, что дизъюнктивная сумма фиксированного s-множества кодовых слов покрывает L других кодовых слов кода X. Затем, вероятность $P(s,L,Q,N,t)$ выражается по формуле полной вероятности для следующей группы несовместных событий: $B_k \triangleq \{\text{вес дизъюнктивной суммы } s \text{ данных кодовых слов равен } k\}, 0 \leq k \leq N$. Логарифмическая асимптотика вероятности события $B_{\lfloor qN \rfloor}$, $0 < q < 1$, вычисляется по аналогии с доказательством теоремы 1.2.2, использованием терминологии типов последовательностей и решением экстремальной задачи.

Следующий раздел 2.3 содержит теорему о верхней границе для пропускной способности почти дизъюнктивных СД s_L-кодов, доказательство которой основано на комбинаторных соображениях.

Теорема 2.3.1 (Верхняя граница для $C_L(s)$)**.** *Справедливо неравенство*

$$C_L(s) \le 1/s, \qquad s \ge 1, \quad L \ge 1.$$

В **главе 3** рассматривается задача проверки гипотез о количестве отправителей сообщений через дизъюнктивный канал множественного доступа. Пусть объем кода, а соответственно и количество всех различных сообщений, равен t. Через $\mathcal{S}_{un}$, $\mathcal{S}_{un} \subset [t]$, обозначим неизвестное множество передаваемых сообщений. Рассматривается задача проверки гипотезы $\{H_0 : |\mathcal{S}_{un}| \le s\}$ против альтернативы $\{H_1 : |\mathcal{S}_{un}| \ge s+1\}$ для некоторой фиксированной константы s.

В разделе 3.1 приведены основные определения, причем описанная выше задача формулируется для дизъюнктивной модели группового тестирования и мотивируется построением систем технической диагностики [5]. В такой постановке исследуемая величина $|\mathcal{S}_{un}|$ обозначает количество дефектов среди множества из t элементов, а альтернатива H_1 является событием превышения количества дефектных элементов заданного порога s. В этом же разделе задача безошибочной проверки гипотезы H_0 против H_1 с помощью неадаптивных групповых тестов сведена к исследованию дизъюнктивных кодов и применению пофакторного декодирования для проверки гипотез:

Предложение 3.1.1. *Результаты неадаптивных групповых тестов, заданных кодом X, позволяют безошибочно проверить гипотезу H_0 против альтернативы H_1 в том и только том случае, если код X является СД s_1-кодом.*

Далее рассматривается вероятностная постановка задачи, в которой для любого закона распределения с равновероятными множествами дефектов одинакового объема допустима лишь незначительная ошибка при проверке гипотез. Введен важный алгоритм, называемый *пороговым декодированием*:

$$\begin{cases} \text{принять } \{H_0 : |\mathcal{S}_{un}| \le s\}, & \text{если } |\boldsymbol{x}(\mathcal{S}_{un})| \le \lfloor \tau N \rfloor, \\ \text{принять } \{H_1 : |\mathcal{S}_{un}| \ge s+1\}, & \text{если } |\boldsymbol{x}(\mathcal{S}_{un})| \ge \lfloor \tau N \rfloor + 1, \end{cases}$$

где через $|\boldsymbol{x}(\mathcal{S}_{un})|$ обозначено количество тестов с положительным результатом, N – общее количество тестов, а τ, $0 < \tau < 1$, – заданная константа. *Экспонентой ошибки* $\mathbf{E}_s(\tau, R)$ для порогового декодирования называется максимальный показатель экспоненциального убывания ошибок первого и второго рода при росте длины кодов N и при фиксированной скорости кодов R.

В разделе 3.2 с помощью метода случайного кодирования на ансамбле равновесных двоичных кодов доказана следующая теорема.

Теорема 3.2.1 (Нижняя граница для $\mathbf{E}_s(\tau, R)$)**.** *Справедливы два утверждения.*
1. *Экспонента ошибки порогового критерия удовлетворяет неравенству $\mathbf{E}_s(\tau, R) \ge \underline{\mathbf{E}}_s(\tau)$ где функция $\underline{\mathbf{E}}_s(\tau)$ не зависит от параметра R и определяется как*

$$\underline{\mathbf{E}}_s(\tau) \triangleq \max_{1-(1-\tau)^{1/(s+1)} < Q < 1-(1-\tau)^{1/s}} \min\{\mathcal{A}'(s, Q, \tau), \mathcal{A}(s+1, Q, \tau)\} > 0,$$

$$\mathcal{A}'(s, Q, \tau) \triangleq \begin{cases} \mathcal{A}(s, Q, \tau), & \textit{если } Q \le \tau \le sQ, \\ \infty, & \textit{иначе}, \end{cases}$$

а функция $\mathcal{A}(s, Q, \tau)$ задана в формулировке теоремы 2.2.2.
2. *При $s \to \infty$ оптимальное значение $\underline{\mathbf{E}}_s(\tau)$ удовлетворяет неравенству:*

$$\underline{\mathbf{E}}_{\mathrm{Thr}}(s) \triangleq \max_{0<\tau<1} \underline{\mathbf{E}}_s(\tau) \ge \frac{\log_2 e}{4s^2}(1 + o(1)), \quad s \to \infty.$$

Доказанная ранее теорема 2.3.1 фактически означает, что экспонента ошибки при проверке гипотез с помощью традиционного пофакторного декодирования обращается в нуль, как только скорость кодов превышает $1/s$. Поэтому нижняя граница для экспоненты ошибки $\mathbf{E}_s(\tau, R)$ из теоремы 3.2.1 устанавливает превосходство порогового декодирования над традиционным пофакторным декодированием в задаче проверки гипотезы H_0 против альтернативы H_1 для больших значений скорости кода R.

В разделе 3.3 приведены результаты моделирования проверки гипотез, которые также показывают, что для большой скорости кодов пороговое декодирование имеет преимущество перед пофакторным декодированием.

Заключительная **глава 4** посвящена кодам для гиперканала множественного доступа.

В разделе 4.1 введены основные обозначения и определения.

Раздел 4.2 посвящен разработке нижних границ скорости СД s_L-гиперкодов. Первая теорема устанавливает нижнюю границу в общем случае $q \geq 2$, которая улучшает ранее известные нижние границы для скорости $R_L^{(q)}(s)$.

Теорема 4.2.1 (Нижняя граница для $R_L^{(q)}(s)$)**.** *Справедливы четыре утверждения.*
1. *При любых фиксированных $q \geq 2$, $s \geq 2$ и $L \geq 1$ справедлива нижняя граница:*

$$R_L^{(q)}(s) \geq \underline{R}_L^{(q)}(s) \triangleq \max_{q' \geq q} \frac{-\log_q P(q', s, L)}{(s + L - 1)k(q, q')}, \quad \textit{где}$$

$$P(q, s, L) \triangleq \sum_{m=1}^{\min\{q,s\}} \binom{q}{m} \left(\frac{m}{q}\right)^L \sum_{k=0}^{m} (-1)^k \binom{m}{k} \left(\frac{m-k}{q}\right)^s,$$

$$k(q, q') \triangleq \begin{cases} 1, & \textit{при} \quad q = q', \\ \lceil \frac{q'}{q-1} \rceil, & \textit{иначе.} \end{cases}$$

2. *При любых фиксированных $q \geq 2$ и $L \geq 1$ выполнено асимптотическое равенство*

$$\underline{R}_L^{(q)}(s) = \frac{L(q-1)\log_q e}{s^2 (\log_2 e)^2}(1 + o(1)), \quad s \to \infty.$$

3. *При любых фиксированных $q \geq 2$ и $s \geq 2$ существует предел $\underline{R}_\infty^{(q)}(s) \triangleq \lim_{L\to\infty} \underline{R}_L^{(q)}(s)$, причем при $s \to \infty$ выполнено асимптотическое равенство*

$$\underline{R}_\infty^{(q)}(s) = \frac{(q-1)\log_q e}{es}, \quad s \to \infty.$$

4. *При любых фиксированных $s \geq 2$ и $L \geq 1$ существует предел*

$$\lim_{q\to\infty} \underline{R}_L^{(q)}(s) = \frac{L}{s + L - 1}.$$

Первая часть доказательства теоремы 4.2.1 основана на методе случайного кодирования на ансамбле q-ичных кодов длины N и объема t, каждая q-ичная компонента которых выбирается независимо и равновероятно из множества всех q-ичных символов $\{0, 1, \ldots, q-1\}$. Рассуждения, аналогичные проведенным при доказательстве теоремы 1.2.2, приводят к следующей нижней границе на скорость q-ичных СД s_L-гиперкодов:

$$R_L^{(q)}(s) \geq \frac{-\log_q P(q, s, L)}{s + L - 1}, \tag{9}$$

где $P(q,s,L)$ – это вероятность события $\bigl\{\{\xi_1,\xi_2,\ldots,\xi_L\}\subset\{\xi_{L+1},\xi_{L+2},\ldots,\xi_{L+s}\}\bigr\}$ для независимых и равномерно распределенных на множестве $\{0,1,\ldots,q-1\}$ случайный величин $\xi_1,\xi_2,\ldots,\xi_{L+s}$.

Вторая и наиболее значимая часть доказательства теоремы 4.2.1 заключается в построении q-ичного СД s_L-гиперкода из q'-ичного СД s_L-гиперкода, $q'>q$, и оптимизации нижней границы (9) по всем $q'\geq q$. Связь между скоростями $R_L^{(q)}(s)$ для различных объемов алфавита q описывает предложение 4.1.2, доказанное в разделе 4.1.

Предложение 4.1.2. *Для любых целых чисел $q'>q\geq 2$, $s\geq 2$ и $L\geq 1$ выполнено неравенство*

$$R_L^{(q)}(s)\geq\frac{R_L^{(q')}(s)}{\lceil q'/(q-1)\rceil\log_{q'}q}.$$

Вторая теорема из раздела 4.2 служит уточнением нижних границ из теоремы 4.2.1 для случая $q=2$.

Теорема 4.2.2 (Нижняя граница для $R_L^{(2)}(s)$)**.** *Имеют место следующие* 3 *утверждения.*
1. *При любых фиксированных $s\geq 2$ и $L\geq 1$ выполнено неравенство*

$$\begin{aligned}
R_L^{(2)}(s)\geq\underline{R}_L^*(s)&\triangleq\max_{0<Q\leq 1/2}\left(h(Q)+\frac{B_L(s,Q)}{s+L-1}\right),\\
B_L(s,Q)&\triangleq Q\log_2\left[\frac{p(1-z)}{p(1-z)+q(1-z)}\right]+(1-Q)\log_2\left[\frac{p(z)}{p(z)+q(z)}\right],\\
p(z)&\triangleq p_L(s,z)=z^s(z-z^s)^L,\\
q(z)&\triangleq q_L(s,z)=(z-z^s)(1-z^s-(1-z)^s)^L,
\end{aligned}$$

где параметр $z\in(0,1)$ в формуле для $B_L(s,Q)$ определяется как единственный корень уравнения

$$Q(p(z)+q(z))=(1-Q)(p(1-z)+q(1-z)).$$

2. *При фиксированном $L=1,2,\ldots$ и $s\to\infty$ справедливо асимптотическое неравенство*

$$\underline{R}_L^*(s)\geq\frac{L}{s^2\log_2 e}(1+o(1)),\quad s\to\infty.$$

3. *При фиксированном $s=2,3,\ldots$ существует предел*

$$\underline{R}_\infty^*(s)\triangleq\lim_{L\to\infty}\underline{R}_L^*(s)=\log_2\left[\frac{(s-1)^{s-1}}{s^s}+1\right].$$

Если $s\to\infty$, то

$$\underline{R}_\infty^*(s)=\frac{\log_2 e}{es}(1+o(1))=\frac{0,5307\ldots}{s}(1+o(1)).$$

Нижняя граница в теореме 4.2.2 получена с помощью метода случайного кодирования на ансамбле $E(N,t,Q)$ равновесных двоичных кодов. Ход доказательства теоремы 4.2.2 аналогичен доказательству нижней границы для скорости СД s_L-кодов в теореме 1.2.2.

В разделе 4.3 установлены соотношения между скоростями q-ичных СД s_L-гиперкодов и СД s_L-кодов. Подстановка верхних границ для $R_L(s)$ из раздела 1.3 позволяет получить верхнюю границу для скорости $R_L^{(q)}(s)$, улучшающую ранее известные верхние границы для больших значений параметра s.

Теорема 4.3.1 (Соотношения между скоростями $R_L^{(q)}(s)$ и $R_L(s)$)**.** *Справедливы два утверждения.*
1. *Для фиксированных параметров $q \geq 2$, $s \geq 2$ и $L \geq 1$ скорости $R_L^{(q)}(s)$ и $R_L(s)$ удовлетворяют соотношению*

$$R_L^{(q)}(s) \leq \min\left\{ \frac{q}{\log_2 q} R_L(s),\ \frac{q-1}{\log_2 q} R_L(s-1) \right\}.$$

2. *При любых фиксированных $q \geq 2$, $L \geq 1$ и $s \to \infty$ скорость q-ичных СД s_L-гиперкодов удовлетворяет неравенству*

$$R_L^{(q)}(s) \leq \frac{2L(q-1)\log_q s}{s^2}(1 + o(1)), \quad s \to \infty.$$

Принимая во внимание очевидное неравенство $R_L(s) \leq R_L^{(2)}(s)$, получаем довольно важное следствие из теоремы 4.3.1, означающее, что при больших значениях параметра s преимущество по скорости двоичных СД s_L-гиперкодов над СД s_L-кодами исчезает.

Следствие 4.3.1. *При фиксированном $L \geq 1$ и $s \to \infty$ имеет место асимптотическое равенство*

$$R_L^{(2)}(s) = R_L(s)(1 + o(1)), \quad s \to \infty.$$

В разделе 4.4 приведено детальное сравнение полученных в данной диссертации границ для скорости $R_L^{(q)}(s)$ с ранее известными, а также представлены таблицы численных значений наилучших границ скорости $R_L^{(q)}(s)$ для некоторых наборов параметров q, s и L.

В разделе 4.5 рассматривается приложение q-ичных СД s_L-гиперкодов (а также СД s_L-кодов), связанное с кодированием недоопределенных данных. Оригинальный метод кодирования, полученный в работе [9], расширен на общий случай $q \geq 2$ и, что наиболее важно, на случай $L \geq 1$. Использование кодов при $L > 1$ позволяет построить более компактный метод кодирования, не увеличивая при этом асимптотические расходы на память и временную сложность алгоритма декодирования.

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

Благодарности

Автор выражает глубокую благодарность своему научному руководителю Дьячкову Аркадию Георгиевичу за постановку интересных задач, обсуждение результатов и постоянное внимание к работе. Автор благодарен Воробьеву Илье Викторовичу и Полянскому Никите Андреевичу за ценные замечания и многочисленные детальные обсуждения, а также слушателям и докладчикам семинара по теории кодирования в ИППИ РАН за полезные замечания и проявленную заинтересованность в результатах работы.

Глава 1

Дизъюнктивные коды со списочным декодированием

В данной главе будет введено определение дизъюнктивных кодов со списочным декодированием. Методом случайного кодирования на ансамбле двоичных равновесных кодов будет установлена нижняя граница для асимптотической скорости дизъюнктивных кодов со списочным декодированием. Также будут сформулированы наилучшие известные верхние границы для этой скорости.

1.1 Основные определения

Для начала введем основные обозначения. Пусть N, t, s и L – целые числа, $2 \le s < t$, $1 \le L \le t - s$, символ $\triangleq$ обозначает равенство по определению, $[N] \triangleq \{1, 2, \ldots, N\}$ – множество целых чисел от 1 до N, $|A|$ – объем множества A, n-множество – множество объема n, и $\lfloor a \rfloor$ ($\lceil a \rceil$) – наибольшее (наименьшее) целое число $\le a$ ($\ge a$). Введем двоичную $(N \times t)$-матрицу

$$X \triangleq \|x_i(j)\|, \quad x_i(j) \in \{0,1\}, \quad \boldsymbol{x}_i \triangleq (x_i(1), \ldots, x_i(t)), \quad \boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j)), \quad (1.1.1)$$

$i \in [N]$, $j \in [t]$, с N строками $\boldsymbol{x}_i$, $\boldsymbol{x}_i \in \{0,1\}^t$, $i \in [N]$, и t столбцами (кодовыми словами) $\boldsymbol{x}(j)$, $\boldsymbol{x}(j) \in \{0,1\}^N$, $j \in [t]$, которую назовем *(двоичным) кодом длины N и объема $t = \lfloor 2^{RN} \rfloor$*, где фиксированный параметр $R > 0$ есть *скорость* кода X. Число единиц в кодовом слове $\boldsymbol{x}(j), j \in [t]$, т.е. $|\boldsymbol{x}(j)| \triangleq \sum_{i=1}^{N} x_i(j)$, будем называть *весом* кодового слова $\boldsymbol{x}(j)$. Код X называется *равновесным*, если вес каждого его кодового слова равен $w, 1 \le w < N$, т.е. $|\boldsymbol{x}(j)| = w$ для любого $j \in [t]$. Стандартное обозначение $\bigvee$ означает *дизъюнктивную сумму* символов или покомпонентную дизъюнктивную сумму столбцов (кодовых слов), т.е. $0 \bigvee 0 \triangleq 0$, $1 \bigvee 1 = 0 \bigvee 1 = 1 \bigvee 0 \triangleq 0$. Будем говорить, что столбец $\boldsymbol{u}$, *покрывает* двоичный столбец $\boldsymbol{v}$ ($\boldsymbol{u} \succeq \boldsymbol{v}$), если $\boldsymbol{u} \bigvee \boldsymbol{v} = \boldsymbol{u}$.

Определение 1.1.1 ([25, 44])**.** Двоичный код X называется *дизъюнктивным кодом со списочным декодированием силы s с объемом списка L* (кратко, СД s_L-кодом), если дизъюнктивная сумма любых s кодовых слов кода X покрывает не более $L-1$ других кодовых слов кода X, не входящих в эту сумму.

Обозначим через $t(N, s, L)$ максимальный объем СД s_L-кодов длины N, и определим *скорость* СД s_L-кодов:

$$R_L(s) \triangleq \varlimsup_{N \to \infty} \frac{\log_2 t(N, s, L)}{N}.$$

В работе [42] некоторые конструкции СД s_L-кодов рассматривались при построении двухступенчатых процедур групповых проверок для поиска $\leq s$ дефектов. Проводя групповые тесты согласно СД s_L-коду и применяя пофакторное декодирование, получим список из $\leq s + L - 1$ элементов, среди которых присутствуют все $\leq s$ дефектов. Элементы из данного списка поодиночке проверяются на второй ступени. Таким образом, предел скорости

$$R_\infty(s) \triangleq \lim_{L\to\infty} R_L(s), \tag{1.1.2}$$

можно интерпретировать как нижнюю границу на скорость двухступенчатых процедур групповых проверок в дизъюнктивной модели поиска $\leq s$ дефектов.

1.2 Нижние границы скорости

В частном случае $L = 1$ наилучшая к настоящему времени нижняя граница скорости $R_1(s)$ была получена в 1989 году в работе [26], в которой с помощью метода случайного кодирования на ансамбле двоичных равновесных кодов доказана следующая теорема.

Теорема 1.2.1 ([26]). *Справедливы два утверждения.*
1. *Скорость $R_1(s)$ удовлетворяет неравенству:*

$$R_1(s) \geq \underline{R}_1(s) \triangleq \frac{1}{s} \max_{0<Q<1} A(s,Q), \quad s = 1, 2, \ldots, \tag{1.2.1}$$

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

где используется стандартное обозначение расстояния Кульбака

$$K(a,b) \triangleq a \cdot \log_2 \frac{a}{b} + (1-a) \cdot \log_2 \frac{1-a}{1-b}, \quad 0 < a, b < 1, \tag{1.2.2}$$

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

$$y = 1 - Q + Qy^s \cdot \frac{1-y}{1-y^s}, \quad 1 - Q \leq y < 1. \tag{1.2.3}$$

2. *Если $s \to \infty$, то асимптотика нижней границы $\underline{R}_1(s)$ имеет вид*

$$\underline{R}_1(s) = \frac{1}{s^2 \log_2 e}(1 + o(1)) = \frac{0,693}{s^2}(1 + o(1)). \tag{1.2.4}$$

Следующая теорема также основывается на методе случайного кодирования на ансамбле двоичных равновесных кодов и обобщает нижнюю границу в теореме 1.2.1 на случай СД s_L-кодов при $L \geq 1$.

Теорема 1.2.2 (Граница случайного кодирования $\underline{R}_L(s)$). *Имеют место следующие три утверждения.*
1. *Для скорости СД s_L-кодов справедливо неравенство*

$$R_L(s) \geq \underline{R}_L(s) \triangleq \frac{1}{s+L-1} \max_{0<Q<1} A_L(s,Q), \tag{1.2.5}$$

$$A_L(s,Q) \triangleq \log_2 \frac{Q}{1-y} - sK(Q, 1-y) - L\,K\left(Q, \frac{1-y}{1-y^s}\right), \quad s \geq 2,\ L \geq 1, \tag{1.2.6}$$

где используется обозначение расстояния Кульбака (1.2.2), *а параметр* y, $1-Q \le y < 1$, *определяется как единственный корень уравнения*

$$y = 1 - Q + Qy^s \left[1 - \left(\frac{y - y^s}{1 - y^s} \right)^L \right], \quad 1 - Q \le y < 1. \tag{1.2.7}$$

2. *При фиксированном* $L = 1, 2, \ldots$ *и* $s \to \infty$ *асимптотика границы случайного кодирования имеет вид*

$$\underline{R}_L(s) = \frac{L}{s^2 \log_2 e}(1 + o(1)), \quad s \to \infty. \tag{1.2.8}$$

3. *При фиксированном* $s = 2, 3, \ldots$ *и* $L \to \infty$ *существует предел*

$$\underline{R}_\infty(s) \triangleq \lim_{L \to \infty} \underline{R}_L(s) = \log_2 \left[\frac{(s-1)^{s-1}}{s^s} + 1 \right]. \tag{1.2.9}$$

Если $s \to \infty$, *то данный предел* $\underline{R}_\infty(s) = \frac{\log_2 e}{e \cdot s}(1 + o(1)) = \frac{0{,}5307}{s}(1 + o(1))$.

В частном случае дизъюнктных кодов со списочным декодированием при объеме списка $L = 1$ нижняя граница (1.2.5)-(1.2.7) и асимптотика (1.2.8) совпадают с нижней границей (1.2.1)-(1.2.3) и асимптотикой (1.2.4), соответственно. В таблице 1.2.1 представлены численные значения нижней границы скорости СД s_L-кодов при малых значениях параметров s и L и указана соответствующая доля $Q_L(s)$ оптимального веса кодовых слов для ансамбля равновесных двоичных кодов в границе случайного кодирования $\underline{R}_L(s)$. При доказательстве утверждений 2 и 3 теоремы 1.2.2 для $Q_L(s)$ будут установлены асимптотические равенства:

$$Q_L(s) = \frac{\ln 2}{s} + \frac{L \ln^2 2}{s^2} + o\left(\frac{1}{s^2} \right), \quad s \to \infty, \quad L = 1, 2, \ldots, \tag{1.2.10}$$

$$Q_L(s) = \left[\frac{s^s}{(s-1)^{s-1}} + 1 \right]^{-1} + o(1), \quad L \to \infty, \quad s = 2, 3, \ldots. \tag{1.2.11}$$

В таблице 1.2.1 также представлены численные значения предела (1.2.9). При $s \ge 3$ правая часть (1.2.9) дает наилучшую известную к настоящему времени нижнюю границу для максимальной скорости двухступенчатых процедур групповых проверок, основанную на (1.1.2). При $s = 2$ в работе [22] получена более сильная нижняя граница, равная 0.4103. Отметим, что в работе [18] приводится основанная, к сожалению, на ошибочных рассуждениях более сильная, чем правая часть (1.2.9), нижняя граница для скорости двухступенчатых процедур групповых проверок.

Доказательство теоремы 1.2.2

Доказательство утверждения 1. Зафиксируем целочисленные параметры $s \ge 2$ и $L \ge 1$, где $s + L < t$, а также параметр Q, $0 < Q < 1$. Как уже отмечалось, границу (1.2.5)-(1.2.7) будем выводить методом случайного кодирования на ансамбле двоичных равновесных кодов [26]. Применяя обозначения (1.1.1), введем ансамбль $E(N, t, Q)$ двоичных кодов X длины N и объема t, для которых кодовые слова выбираются независимо и равновероятно из множества, состоящего из всех $\binom{N}{\lfloor QN \rfloor}$ двоичных кодовых слов веса $\lfloor QN \rfloor$. Пара множеств $(\mathcal{S}, \mathcal{L})$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и $\mathcal{L} \subset [t] \setminus \mathcal{S}$, $|\mathcal{L}| = L$, называется s_L-*плохой*, если $\bigvee_{j \in \mathcal{S}} \boldsymbol{x}(i) \succeq \bigvee_{j \in \mathcal{L}} \boldsymbol{x}(j)$. Индекс $j \in [t]$ будем называть s_L-*плохим*, если существует

Таблица 1.2.1: Численные значения нижней границы $\underline{R}_L(s)$

s_L	2_1	3_1	4_1	5_1	6_1
$\underline{R}_L(s)$	0.1825	0.0787	0.0439	0.0279	0.0194
$Q_L(s)$	0.2605	0.1870	0.1466	0.1208	0.1027
s_L	2_2	3_2	4_2	5_2	6_2
$\underline{R}_L(s)$	0.2358	0.1147	0.0684	0.0456	0.0325
$Q_L(s)$	0.2442	0.1758	0.1388	0.1150	0.0984
s_L	2_3	3_3	4_3	5_3	6_3
$\underline{R}_L(s)$	0.2597	0.1346	0.0838	0.0575	0.0420
$Q_L(s)$	0.2334	0.1674	0.1326	0.1103	0.0947
s_L	2_4	3_4	4_4	5_4	6_4
$\underline{R}_L(s)$	0.2729	0.1469	0.0941	0.0660	0.0490
$Q_L(s)$	0.2262	0.1610	0.1275	0.1064	0.0915
s_L	2_5	3_5	4_5	5_5	6_5
$\underline{R}_L(s)$	0.2813	0.1552	0.1014	0.0723	0.0544
$Q_L(s)$	0.2211	0.1560	0.1235	0.1031	0.0888
s_L	2_6	3_6	4_6	5_6	6_6
$\underline{R}_L(s)$	0.2871	0.1611	0.1068	0.0771	0.0587
$Q_L(s)$	0.2175	0.1522	0.1201	0.1002	0.0865
s	2	3	4	5	6
$\underline{R}_\infty(s)$	0.3219	0.1993	0.1447	0.1136	0.0935

s_L-плохая пара $(\mathcal{S}, \mathcal{L})$ такая, что $j \in \mathcal{L}$. Для ансамбля $E(N, t, Q)$ вероятность события "фиксированная пара $(\mathcal{S}, \mathcal{L})$ является s_L-плохой" обозначим через $P(s, L, Q, N)$.

Нетрудно заметить, что математическое ожидание количества s_L-плохих индексов не превосходит

$$t \cdot \binom{t}{s+L-1}\binom{s+L-1}{s} P(s, L, Q, N) \le E(s, L, Q, N, t) \triangleq \frac{t^{s+L}}{s!(L-1)!} P(s, L, Q, N).$$

Очевидно, что если $E(s, L, Q, N, 2t) \le t$, то существует СД s_L-код длины N и объема t, а потому справедлива следующая нижняя граница для скорости СД s_L-кодов:

$$R_L(s) \ge \underline{R}_L(s) \triangleq \frac{1}{s+L-1} \max_{0<Q<1} A_L(s, Q),$$

$$A_L(s, Q) \triangleq \overline{\lim_{N\to\infty}} \frac{-\log_2 P(s, L, Q, N)}{N}. \tag{1.2.12}$$

Далее мы показываем, что функция $A_L(s, Q)$ описывается соотношениями (1.2.6)-(1.2.7), приведенными в формулировке утверждения 1 теоремы 1.2.2.

Будем использовать терминологию *типов* последовательностей [8]. Рассмотрим произвольное множество из s кодовых слов длины N и одинакового веса $\lfloor QN \rfloor$: $(\boldsymbol{x}(1), \ldots, \boldsymbol{x}(s))$, где $\boldsymbol{x}(i) \in \{0,1\}^N$, $\forall i \in [s]$. Это множество образует $(N \times s)$-матрицу X^s. Пусть $\boldsymbol{a} \triangleq (a_1, \ldots, a_s) \in \{0,1\}^s$ обозначает некоторую строку объема s. Определим *тип* матрицы X^s как множество $\{n(\boldsymbol{a}), \forall \boldsymbol{a} \in \{0,1\}^s\}$, где $n(\boldsymbol{a})$, $0 \le n(\boldsymbol{a}) \le N$, равно числу строк $\boldsymbol{a}$ в матрице X^s. Через $n(\boldsymbol{0})$ $(n(\boldsymbol{1}))$ обозначим число строк в матрице X^s, составленных только из нулей (единиц). При таких обозначениях вероятность появления s_L-плохой пары наборов

представим в виде:

$$P(s,L,Q,N)=\sum_{\{n(\boldsymbol{a})\}}\frac{N!}{\prod_{\boldsymbol{a}}n(\boldsymbol{a})!}\binom{N-n(\boldsymbol{0})}{\lfloor QN\rfloor}^{L}\binom{N}{\lfloor QN\rfloor}^{-s-L}, \tag{1.2.13}$$

где суммирование идет по всевозможным типам $\{n(\boldsymbol{a}),\boldsymbol{a}\in\{0,1\}^s\}$, обладающим свойствами:

$$0\le n(\boldsymbol{a})\le N,\quad \sum_{\boldsymbol{a}}n(\boldsymbol{a})=N,\quad \sum_{\boldsymbol{a}\colon a_i=1}n(\boldsymbol{a})=\lfloor QN\rfloor\quad\text{для любого } i\in[s]. \tag{1.2.14}$$

Пусть $N\to\infty$ и $n(\boldsymbol{a})\triangleq N[\tau(\boldsymbol{a})+o(1)]$, где фиксированное распределение вероятностей $\tau\triangleq\{\tau(\boldsymbol{a}),\boldsymbol{a}\in\{0,1\}^s\}$, обладает свойствами, индуцированными условиями (1.2.14), т.е.

$$0\le\tau(\boldsymbol{a})\le 1,\quad \sum_{\boldsymbol{a}\in\{0,1\}^s}\tau(\boldsymbol{a})=1,\quad \sum_{\boldsymbol{a}\colon a_i=1}\tau(\boldsymbol{a})=Q\quad\text{для любого } i\in[s]. \tag{1.2.15}$$

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

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

где

$$F(\tau,Q)\triangleq\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})\log_2[\tau(\boldsymbol{a})]-(1-\tau(\boldsymbol{0}))\,L\cdot h\left(\frac{Q}{1-\tau(\boldsymbol{0})}\right)+(s+L)h(Q). \tag{1.2.16}$$

Пусть при $\tau_Q=\{\tau_Q(\boldsymbol{a})\}$ достигается минимум функции $F\triangleq F(\tau,Q)$ для данного Q. Тогда главный член логарифмической асимптотики суммы слагаемых (1.2.13) есть

$$A_L(s,Q)\triangleq\varlimsup_{N\to\infty}\frac{-\log_2 P(s,L,Q,N)}{N}=\min_{\tau\in(1.2.15)}F(\tau,Q)=F(\tau_Q,Q). \tag{1.2.17}$$

Запишем соответствующую задачу минимизации: $F\to\min$.

$$\begin{aligned}&\text{Основная функция:}\qquad F(\tau,Q):\mathbb{Y}\to\mathbb{R}.\\ &\text{Ограничения:}\quad\begin{cases}\sum\limits_{\boldsymbol{a}\in\{0,1\}^s}\tau(\boldsymbol{a})=1;\\ \sum\limits_{\boldsymbol{a}\colon a_i=1}\tau(\boldsymbol{a})=Q\quad\text{для любого } i\in[s].\end{cases}\\ &\text{Область поиска } \mathbb{Y}:\quad 0<\tau(\boldsymbol{a})<1,\quad \boldsymbol{a}\in\{0,1\}^s.\end{aligned} \tag{1.2.18}$$

Поиск точки минимума τ_Q будем вести стандартным методом множителей Лагранжа. Рассмотрим лагранжиан

$$\Lambda\triangleq F(\tau,Q)+\lambda_0\left(\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})-1\right)+\sum_{i=1}^{s}\lambda_i\left(\sum_{\boldsymbol{a}\colon a_i=1}\tau(\boldsymbol{a})-Q\right).$$

Тогда необходимые условия экстремального распределения имеют вид:

$$\begin{cases}\frac{\partial\Lambda}{\partial(\tau(\boldsymbol{a}))}=\log_2[\tau(\boldsymbol{a})]+\log_2 e+\lambda_0+\sum_{i=1}^{s}a_i\lambda_i=0\quad\text{при }\boldsymbol{a}\ne\boldsymbol{0};\\ \frac{\partial\Lambda}{\partial(\tau(\boldsymbol{0}))}=\log_2[\tau(\boldsymbol{0})]+\log_2 e+\lambda_0+L\log_2\left[\frac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-Q}\right]=0.\end{cases} \tag{1.2.19}$$

Матрица $\frac{\partial^2 \Lambda}{\partial \tau^2}$ производных второго порядка лагранжиана является диагональной и имеет только положительные элементы на главной диагонали, т.е. положительно определена. Отметим, что матрица вторых производных функции $F(\tau, Q)$ совпадает с данной матрицей. Следовательно [2], F является строго $\cup$-выпуклой в области $\mathbb{Y}$. А значит, локальный минимум F в $\mathbb{Y}$ является глобальным и единственным. Воспользуемся теоремой Каруша-Куна-Таккера [2], согласно которой, если существует решение, удовлетворяющее необходимым условиям (1.2.19) и ограничениям (1.2.18), то оно дает локальный минимум функции F, а следовательно, является искомым минимальным распределением τ_Q.

Покажем, что из симметрии задачи вытекает равенство: $\nu \triangleq \lambda_1 = \lambda_2 = \cdots = \lambda_s$. Для доказательства достаточно убедиться, что $\lambda_i = \lambda_j$ для произвольных $i \in [s], j \in [s], i \neq j$. Пусть $\bar{\boldsymbol{a}}_i \triangleq (0, \ldots, 1, \ldots, 0)$ – строка длины s, на i-ой позиции которой стоит 1, а в остальных позициях стоят 0. Перестановка индексов i и j приводит к равносильной задаче. Следовательно, если τ_Q^1 является решением, то и τ_Q^2 будет решением, где $\tau_Q^2(\boldsymbol{a}) \triangleq \tau_Q^1(\tilde{\boldsymbol{a}})$, а $\tilde{\boldsymbol{a}}$ обозначает строку, полученную из строки $\boldsymbol{a}$ перестановкой индексов i и j. Единственность решения τ_Q означает, что распределение τ_Q^1 совпадает с распределением τ_Q^2. В частности, $\tau_Q^1(\bar{\boldsymbol{a}}_i) = \tau_Q^2(\bar{\boldsymbol{a}}_i) = \tau_Q^1(\bar{\boldsymbol{a}}_j)$. Подставив $\bar{\boldsymbol{a}}_i$ и $\bar{\boldsymbol{a}}_j$ в первое уравнение (1.2.19), заключаем, что $\lambda_i = \lambda_j$.

Таким образом, экстремальное распределение $\tau_Q = \{\tau_Q(\boldsymbol{a})\}$ удовлетворяет условиям:

$$\begin{cases} \mu + \nu \sum_{i=1}^{s} a_i + \log_2 \tau(\boldsymbol{a}) = 0 \quad \text{при } \boldsymbol{a} \neq \boldsymbol{0}; \\ \mu + \log_2 \tau(\boldsymbol{0}) + L \log_2 \left[\frac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-Q} \right] = 0, \end{cases} \tag{1.2.20}$$

где

$$\nu \triangleq \lambda_1 = \lambda_2 = \cdots = \lambda_s, \quad \mu \triangleq \log_2 e + \lambda_0.$$

После замены параметра $y \triangleq \frac{1}{1+2^{-\nu}}$, $0 < y < 1$, первое уравнения системы (1.2.20) дает

$$\tau(\boldsymbol{a}) = \frac{2^{-\nu \sum a_i}}{2^{\mu}} = \frac{1}{2^{\mu} y^s} (1-y)^{\sum a_i} y^{s - \sum a_i} \quad \text{при} \quad \boldsymbol{a} \neq \boldsymbol{0}. \tag{1.2.21}$$

Ограничение в задаче (1.2.18) на распределение вероятностей (1.2.21) приводит к равенству

$$\begin{aligned} Q &= \sum_{\boldsymbol{a}:\, a_i = 1} \tau_Q(\boldsymbol{a}) = \frac{1}{2^{\mu} y^s} \sum_{\boldsymbol{a}:\, a_i = 1} (1-y)^{\sum a_j} y^{s - \sum a_j} \\ &= \frac{1}{2^{\mu} y^s} \sum_{k=0}^{s-1} \binom{s-1}{k} y^{s-k-1} (1-y)^{k+1} = \frac{1-y}{2^{\mu} y^s}, \quad \text{для любого } i \in [s]. \end{aligned}$$

При фиксированном Q, $0 < Q < 1$, данное равенство представляет собой уравнение связи между параметрами μ и y, описывающими экстремальное распределение $\tau_Q = \{\tau_Q(\boldsymbol{a})\}$:

$$\frac{1}{2^{\mu} y^s} = \frac{Q}{1-y} \qquad \Leftrightarrow \qquad \mu = \log_2 \left[\frac{1-y}{Q y^s} \right]. \tag{1.2.22}$$

Применяя (1.2.22), для распределения вероятностей (1.2.21) вычислим

$$1 - \tau(\boldsymbol{0}) = \sum_{\boldsymbol{a} \neq \boldsymbol{0}} \tau(\boldsymbol{a}) = \frac{1}{2^{\mu} y^s} \sum_{k=1}^{s} \binom{s}{k} y^{s-k} (1-y)^k = \frac{Q(1-y^s)}{1-y}.$$

Таким образом, после исключения параметра μ компоненты экстремального распределения (1.2.21) принимают вид функций одной и той же независимой переменной y, $0 < y < 1$:

$$\tau_Q(\boldsymbol{a}) = \frac{Q}{1-y}\, y^{[s-\sum a_i]}(1-y)^{\sum a_i} \quad \text{при } \boldsymbol{a} \neq \boldsymbol{0}; \quad \tau_Q(\boldsymbol{0}) = 1 - \frac{Q(1-y^s)}{1-y}. \tag{1.2.23}$$

Подставляя (1.2.23) во второе уравнение системы (1.2.20) и учитывая (1.2.22), приходим к равенству

$$\log_2\left[\frac{1-y-Q(1-y^s)}{Qy^s}\right] + L\log_2\left[\frac{1-y^s}{y-y^s}\right] = 0. \tag{1.2.24}$$

которое равносильно уравнению (1.2.7) для параметра y, $1-Q < y < 1$, из формулировки утверждения 1 теоремы 1.2.2. Уравнение (1.2.24) имеет единственное решение $y = y(s,Q)$, поскольку для рассматриваемой нами выпуклой задачи Лагранжа существует единственное экстремальное распределение (1.2.23), задаваемое параметром y, $0 < y < 1$.

Чтобы найти значение $F(\tau_Q, Q)$ для искомого минимума в (1.2.17), подставим вероятности (1.2.23) в определение (1.2.16) функции $F(\tau, Q)$. Затем группируя слагаемые в (1.2.16) по s и L, вычисляем $F(\tau_Q, Q)$ как функцию независимой переменной y, $0 < y < 1$. Используя символ расстояния Кульбака (1.2.2), результат можно записать в виде:

$$F(\tau_Q, Q) = \log_2\left[\frac{Q}{1-y}\right] - sK\left(Q, 1-y\right) - LK\left(Q, \frac{1-y}{1-y^s}\right). \tag{1.2.25}$$

Из (1.2.12), (1.2.17), (1.2.24) и (1.2.25) вытекает приведенная в утверждении 1 теоремы 1.2.2 нижняя оценка (1.2.5)-(1.2.7) для скорости СД s_L-кодов. Утверждение 1 доказано.

Доказательство утверждения 2. При фиксированных $s \geq 2$ и $L \geq 1$ уравнение (1.2.7) будем интерпретировать как функцию $Q = Q_L(y,s)$ аргумента y, $0 < y < 1$, т.е.

$$Q = Q_L(y,s) \triangleq \frac{1-y}{1-r_L(y,s)}, \quad r_L(y,s) \triangleq y^s\left[1 - \left(\frac{y-y^s}{1-y^s}\right)^L\right], \qquad 0 < y < 1. \tag{1.2.26}$$

Тогда, применяя явную формулу (1.2.2) для расстояния Кульбака, определение границы случайного кодирования (1.2.5)-(1.2.7) можно переписать в виде

$$\underline{R}_L(s) \triangleq \frac{1}{s+L-1}\max_{0<y<1} T_L(y,s), \tag{1.2.27}$$

где

$$\begin{aligned} T_L(y,s) \triangleq{}& (1-sQ-LQ)\log_2\left[\frac{Q}{1-y}\right] \\ &- (s+L)(1-Q)\log_2\left[\frac{1-Q}{y}\right] - L\log_2\left[1-y^s\right] + L(1-Q)\log_2\left[1-y^{s-1}\right] \end{aligned} \tag{1.2.28}$$

и параметр Q в правой части (1.2.28) определяется (1.2.26).

Пусть $L \geq 1$ фиксировано и $s \to \infty$. Если в определениях (1.2.26) и (1.2.28) положить $y = 1 - c/s$, где параметр $c = c_L > 0$ не зависит от s, то (1.2.27) означает, что граница случайного кодирования

$$\underline{R}_L(s) \geq \frac{1}{s+L-1} T_L\left(1 - \frac{c}{s}, s\right), \quad c < s. \tag{1.2.29}$$

Вычисление главных членов асимптотических разложений в формулах (1.2.26) и (1.2.28), когда $y = 1 - c/s$ и $s \to \infty$, приводят к асимптотическим равенствам

$$Q = Q_L\left(1 - \frac{c}{s}, s\right) = \frac{c}{s}(1 + o(1)), \quad T_L\left(1 - \frac{c}{s}, s\right) = -\frac{L}{s}\, c \cdot \log_2[1 - e^{-c}](1 + o(1)).$$

Несложно проверить, что при $c = \ln 2 = \frac{1}{\log_2 e}$ достигается

$$\max_{c>0}\{-c \cdot \log_2[1 - e^{-c}]\} = \frac{1}{\log_2 e}. \tag{1.2.30}$$

Поэтому из (1.2.29)-(1.2.30) для границы случайного кодирования (1.2.26)-(1.2.28) вытекает асимптотическое неравенство

$$\underline{R}_L(s) \geq \frac{L}{s^2 \cdot \log_2 e}(1 + o(1)), \quad s \to \infty,\ L = 1, 2, \ldots. \tag{1.2.31}$$

Подстановка значения $y = 1 - \ln 2/s$ в (1.2.26) и вычисление соответствующего значения параметра Q приводит к асимптотической формуле (1.2.10) для доли веса $Q_L(s)$ кодовых слов в равновесном ансамбле кодов, на котором достигается асимптотика скорости, описываемая правой частью (1.2.31).

Далее мы доказываем знак равенства в (1.2.31) и завершаем вывод утверждения 2. Обозначим через $y_L(s)$, $0 < y_L(s) < 1$, $s = 1, 2, \ldots$, произвольную последовательность, на которой достигается

$$\max_{0<y<1} T_L(y, s) = T_L(y_L(s), s). \tag{1.2.32}$$

Из определения (1.2.26) функции $r_L(y, s)$, $0 < y < 1$, следует, что для любой последовательности $y = y_L(s)$, предел

$$\lim_{s\to\infty} r_L(y_L(s), s) = 0. \tag{1.2.33}$$

Тогда определение (1.2.26) функции $Q_L(y, s)$, $0 < y < 1$, дает последовательность

$$Q_L(y_L(s), s) = \frac{1 - y_L(s)}{1 - r_L(y_L(s), s)} = (1 - y_L(s))(1 + o(1)), \quad s \to \infty. \tag{1.2.34}$$

С помощью (1.2.33)-(1.2.34) несложно проверить, что

$$\log_2\left[\frac{Q_L(s)}{1 - y_L(s)}\right] = \log_2 e \cdot r_L(y_L(s), s)(1 + o(1)),$$
$$\log_2\left[\frac{1 - Q_L(s)}{y_L(s)}\right] = \log_2 e \cdot r_L(y_L(s), s)\left(1 - \frac{1}{y_L(s)}\right)(1 + o(1)), \quad s \to \infty.$$

Подставляя эти соотношения в (1.2.28), для максимального значения (1.2.32) вычисляем главный член асимптотики:

$$T_L(y_L(s), s) = \log_2 e\Bigg((1 - (s + L)(1 - y))\, r - y(s + L)\left(1 - \frac{1}{y}\right) r - \\ - L \ln\left[1 - y^s\right] + Ly \ln\left[1 - y^{s-1}\right] \Bigg)(1 + o(1)), \tag{1.2.35}$$

где в правой части (1.2.35) и последующих асимптотических формулах для сокращения записи приняли обозначения $y = y_L(s)$ и $r = r_L(y_L(s), s)$. Очевидно, что

$$\ln\left[1 - y^{s-1}\right] = \left(\ln\left[1 - y^s\right] - \frac{y^{s-1}(1-y)}{1-y^s}\right)(1 + o(1)), \quad s \to \infty. \tag{1.2.36}$$

Приведя подобные члены в (1.2.35) и используя разложение (1.2.36), имеем

$$T_L(y_L(s), s) = \log_2 e\left(r - L(1-y)\ln\left[1-y^s\right] - L(1-y)\frac{y^s}{1-y^s}\right)(1 + o(1)). \tag{1.2.37}$$

Без ограничения общности можем рассматривать случай $y_L(s) \to 1$. Если это условие не выполнено, то в силу (1.2.26) главный член асимптотики (1.2.37) является экспоненциально убывающим. Используя разложение

$$\left(1 - \frac{1-y}{1-y^s}\right)^L = 1 - L\frac{1-y}{1-y^s} + o(L(1-y)) \quad \text{при} \quad y \to 1$$

нетрудно убедиться, что имеет место асимптотика

$$r - L(1-y)\frac{y^s}{1-y^s} = o(L(1-y)).$$

Следовательно, $T_L(y_L(s), s) = -L(1-y)\log_2\left[1-y^s\right](1+o(1))$ и с помощью (1.2.30) несложно убедиться, что максимум главного члена асимптотики величины $T_L(y_L(s), s)$ получается в случае $1 - y = \ln 2/s\,(1 + o(1))$. Тогда

$$T_L(y_L(s), s) = \frac{L}{s\log_2 e}(1 + o(1)).$$

Поэтому из определения (1.2.27) и равенства (1.2.32) следует, что

$$\underline{R}_L(s) = \frac{1}{s + L - 1}\max_{0<y<1} T_L(y, s) = \frac{L}{s^2\log_2 e}(1 + o(1)).$$

Утверждение 2 доказано.

Доказательство утверждения 3. При фиксированных $s \geq 2$, $L \geq 1$ и параметре $c > 0$, не зависящем от L, рассмотрим уравнение

$$\left(\frac{y - y^s}{1-y^s}\right)^L = c(1-y), \quad 0 < y < 1. \tag{1.2.38}$$

В силу свойств возрастания левой части и убывания правой части по y, уравнение (1.2.38) имеет ровно один корень на интервале $y \in (0, 1)$. Обозначим этот корень через $y_L(s, c)$. Подставив его в (1.2.26), введем величины $Q = Q_L(s, c)$ и $r = r_L(s, c)$, которые вместе с $y = y_L(s, c)$ будем интерпретировать как последовательности аргумента $L = 1, 2, \ldots$.

Пусть $s \geq 2$ фиксировано и $L \to \infty$. Очевидны следующие асимптотические свойства данных последовательностей:

$$\begin{aligned} &y = y_L(s, c) = 1 + o(1), \\ &r_L(s, c) = 1 - (s + c)(1 - y) + o(1 - y), \\ &Q_L(s, c) = \frac{1}{s + c}(1 + o(1)), \quad L \to \infty, \quad s = 2, 3, \ldots, \quad c > 0. \end{aligned} \tag{1.2.39}$$

Определение (1.2.26)-(1.2.28) означает, что для любого $c > 0$ граница случайного кодирования

$$\underline{R}_L(s) \geq \frac{1}{s+L-1} T_L\left(y_L(s,c), s\right), \quad c > 0, \tag{1.2.40}$$

где величина $T_L\left(y_L(s,c), s\right)$ задается формулой (1.2.28), в которой $y = y_L(s,c)$, а $Q = Q_L(s,c)$. Применяя определение (1.2.38) и свойства (1.2.39), можно вычислить главный член асимптотики в правой части (1.2.28) при $y = y_L(s,c)$ и $Q = Q_L(s,c)$, а затем получить асимптотическое равенство:

$$\frac{T_L\left(y_L(s,c), s\right)}{L} = \left(\log_2 \left[\frac{s+c}{s}\right] - \frac{s+c-1}{s+c} \log_2 \left[\frac{s+c-1}{s-1}\right] - \frac{c}{s+c} \log_2 \left[\frac{s-1}{s}\right] \right)(1+o(1)), \quad L \to \infty. \tag{1.2.41}$$

С помощью взятия производной по c нетрудно убедиться, что максимум правой части равенства (1.2.41) достигается при значении $c = c(s) \triangleq \frac{s^s-(s-1)^s}{(s-1)^{s-1}}$. Если теперь данное $c = c(s)$ подставить в (1.2.41), то пользуясь неравенством (1.2.40), для границы случайного кодирования (1.2.26)-(1.2.28) устанавливаем неравенство:

$$\underline{R}_\infty(s) \triangleq \lim_{L\to\infty} \underline{R}_L(s) \geq \log_2 \left[\frac{(s-1)^{s-1}}{s^s} + 1\right], \quad s = 2, 3, \ldots. \tag{1.2.42}$$

Если же $c = c(s)$ подставить в формулу для Q из (1.2.39), то придем к асимптотической формуле (1.2.11) для доли веса $Q_L(s)$ кодовых слов в равновесном ансамбле, на котором достигается асимптотика скорости, описываемая правой частью (1.2.42).

Докажем теперь знак равенства в (1.2.42), что завершит доказательство утверждения 3. Обозначим через $y_L(s)$, $0 < y_L(s) < 1$, $L = 1, 2, \ldots$, произвольную последовательность, на которой достигается

$$\max_{0<Q<1} T_L(y,s) = T_L(y_L(s), s).$$

Далее для краткости будем писать y и Q вместо $y_L(s)$ и $Q_L(y_L(s), s)$.

Введем следующее обозначение

$$u = u_L(y_L(s), s) \triangleq \left(\frac{y-y^s}{1-y^s}\right)^L.$$

Очевидно, что $\lim\limits_{L\to\infty} u_L(y_L(s), s) = 0$, независимо от того, какая именно последовательность $y_L(s)$.

Из уравнения (1.2.7), связывающего Q и y, находим, что

$$Q = \frac{1-y}{1-y^s\,(1-u)}, \tag{1.2.43}$$

тогда заменой Q внутри логарифмов выражения (1.2.28) по формуле (1.2.43) получаем

$$T_L(y,s) = (s+L-1)\log_2\left[1-y^s\,(1-u)\right] - L\log_2\left[1-y^s\right] - (s+L)(1-Q)\log_2\left[1-y^{s-1}\,(1-u)\right] + L(1-Q)\log_2\left[1-y^{s-1}\right]. \tag{1.2.44}$$

Без ограничения общности можем рассматривать случай

$$y = y_L(s) \to 1, \tag{1.2.45}$$

иначе несложно убедиться, что асимптотика нижней границы $\underline{R}_L(s)$ получится меньше, чем в (1.2.42). Тогда, обозначив

$$v = v_L(y_L(s), s), s) \triangleq 1 - y_L(s), \tag{1.2.46}$$

имеем

$$y^s = (1 - sv)(1 + o(1)), \quad L \to \infty. \tag{1.2.47}$$

Достаточно рассмотреть случай $\frac{u}{v} \to c$ для некоторой константы $0 \le c < \infty$. Если данное условие не выполнено, придем к асимптотике нижней границы, которая хуже указанной в (1.2.42).

После подстановки (1.2.47) и $u = cv(1 + o(1))$ в (1.2.44) имеем

$$T_L(y, s) = \Big((s + L - 1)\log_2[(s + c)v] - L\log_2[sv] \\ - (s + L)(1 - Q)\log_2[(s - 1 + c)v] + L(1 - Q)\log_2[(s - 1)v]\Big)(1 + o(1)).$$

Нетрудно заметить, что при $c = 0$ асимптотика нижней границы оказывается меньше (1.2.42). Так что будем считать, что $c > 0$. А тогда

$$v = \frac{1}{c}u(1 + o(1)) = \frac{1}{c}\left(\frac{s - 1}{s}\right)^L (1 + o(1)). \tag{1.2.48}$$

Заметим, что из (1.2.43), (1.2.46) и (1.2.48) вытекает асимптотическое равенство для Q:

$$Q = \frac{v}{1 - (1 - v)^s(1 - u)} = \frac{1}{s + c}(1 + o(1)). \tag{1.2.49}$$

Таким образом, последовательности $y_L(s)$ и $Q_L(y_L(s), s)$ удовлетворяют асимптотическим соотношениям (1.2.49) и (1.2.45) соответственно, эквивалентным (1.2.39). Но как было показано выше, для любых таких последовательностей со свойствами (1.2.39) выполняется (1.2.42).

Утверждение 3 доказано.

Теорема 1.2.2 доказана. $\square$

1.3 Верхние границы скорости

Наилучшая к настоящему времени нижняя граница скорости для СД s_1-кодов (или дизъюнктивных s-кодов) была получена в 1982 году в работе [4]. Для описания этой границы, обозначаемой в данной работе символом $\overline{R}_1(s)$, $s = 1, 2, \ldots$, и называемой *рекуррентной границей*, введем стандартное обозначение двоичной энтропии

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

и функцию

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

аргумента v, $0 < v < 1$. В [4] показано, что функция $f_s(v) > 0$, выпукла вверх и принимает максимальное значение:

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

Теорема 1.3.1 ([4]). *Справедливы следующие 3 утверждения.*
1. *При любом целом $s \geq 1$ для скорости СД s_1-кодов выполнено неравенство $R_1(s) \leq \overline{R}_1(s)$, где последовательность $\overline{R}_1(1) = 1, \overline{R}_1(2), \overline{R}_1(3), \ldots$ задается рекуррентным образом:*

$$\overline{R}_1(s) \triangleq \max_{0<v<1-\overline{R}_1(s)/\overline{R}_1(s-1)} f_s(v), \quad s \geq 2. \tag{1.3.3}$$

2. *В случае $s = 2$ выполнено соотношение*

$$\overline{R}_1(2) \triangleq \max_{0<v<1} f_2(v) = f_2(v_2),$$

а при $s \geq 3$ справедливо рекуррентное уравнение

$$\overline{R}_1(s) = f_s\left(1 - \frac{\overline{R}_1(s)}{\overline{R}_1(s-1)}\right), \quad s \geq 3. \tag{1.3.4}$$

3. *Рекуррентная граница $\overline{R}_1(s)$ удовлетворяет асимптотическому соотношению*

$$\overline{R}_1(s) \leq \frac{2\log_2 s}{s^2}(1 + o(1)), \quad s \to \infty. \tag{1.3.5}$$

Отметим, что в недавней работе [44] И.В. Воробьев доказал знак равенства в асимптотическом соотношении (1.3.5).

Рассмотрим теперь общий случай $L \geq 1$. В статье [25] установлена верхняя граница

$$R_L(s) \leq \frac{1}{s},$$

которая и до настоящего времени является наилучшей для некоторых наборов параметров s и L. Также в [25] получена иная верхняя граница, являющаяся следствием неравенства

$$R_L(s) \leq R_1\left(\left\lfloor \frac{s}{L} \right\rfloor\right)$$

и верхней границы из теоремы 1.3.1. Наилучшая известная верхняя граница скорости $R_L(s)$ приведена в следующей теореме, доказанной И.В. Воробьевым в работе [44].

Теорема 1.3.2 ([44]). *Имеют место следующие три утверждения.*
1. *Для любого фиксированного $L \geq 1$ скорость СД s_L-кодов удовлетворяет неравенству $R_L(s) \leq \overline{R}_L(s)$, $s = 1, 2, \ldots$, в правой части которого последовательность $\overline{R}_L(s)$, $s = 1, 2, \ldots$, определяется рекуррентно:*

- *если $1 \leq s \leq L$, то*

$$\overline{R}_L(s) \triangleq 1/s, \quad s = 1, 2, \ldots, L; \tag{1.3.6}$$

- *если $s \geq L + 1$, то*

$$\overline{R}_L(s) \triangleq \min\{1/s;\, r_L(s)\}, \quad s = L+1, L+2, \ldots,$$

где $r_L(s)$ является единственным решением уравнения

$$r_L(s) \triangleq \max_{(1.3.8)} f_{\lfloor s/L \rfloor}(v), \quad s = L+1, L+2, \ldots, \tag{1.3.7}$$

в котором при $n = 1, 2, \ldots$ функция $f_n(v)$ параметра v, $0 < v < 1$, определена (1.3.1) – (1.3.2) и максимум берется по всем v, удовлетворяющим условию

$$0 < v < 1 - \frac{r_L(s)}{\overline{R}_L(s-1)}; \tag{1.3.8}$$

- *если* $s > 2L$ *то уравнение* (1.3.7) *можно записать в виде равенства*

$$r_L(s) = f_{\lfloor s/L \rfloor}\left(1 - \frac{r_L(s)}{\overline{R}_L(s-1)}\right), \quad L \geq 1, \quad s > 2L. \tag{1.3.9}$$

2. *Для любого* $L \geq 1$ *существует целое число* $s(L) \geq 2$*, такое, что*

$$\overline{R}_L(s) = \begin{cases} 1/s, & \text{если } s = s(L) - 1, \\ < 1/s, & \text{если } s \geq s(L), \end{cases}$$

и $s(L) = L \log_2 L(1 + o(1))$ *при* $L \to \infty$.
3. *Если* $L \geq 1$ *фиксировано и* $s \to \infty$*, то*

$$\overline{R}_L(s) = \frac{2L \log_2 s}{s^2}(1 + o(1)). \tag{1.3.10}$$

Определение рекуррентной границы (1.3.6)-(1.3.9) и асимптотика (1.3.10) представляют собой обобщения рекуррентной границы (1.3.3)-(1.3.4) и асимптотики (1.3.5).

Глава 2

Почти дизъюнктивные коды со списочным декодированием

В данной главе будет рассмотрено определение почти дизъюнктивных кодов со списочным декодированием. Методом случайного кодирования на ансамбле двоичных равновесных кодов будет установлена нижняя граница для экспоненты ошибки почти дизъюнктивных кодов со списочным декодированием. Также будет приведена наилучшая известная нижняя граница для пропускной способности почти дизъюнктивных кодов со списочным декодированием и будет доказана верхняя граница для этой пропускной способности.

2.1 Основные определения

Будем пользоваться обозначениями и определениями, введенными в главе 1 настоящей диссертации.

Определение 2.1.1 ([45]). Множество $\mathcal{S}$, $\mathcal{S} \subset [t]$, объема $|\mathcal{S}| = s$ назовем *s_L-плохим* для кода X если существует множество $\mathcal{L}$, $\mathcal{L} \subset [t] \setminus \mathcal{S}$, которое имеет объем $|\mathcal{L}| = L$, и дизъюнктивная сумма кодовых слов с номерами из $\mathcal{S}$ покрывает дизъюнктивную сумму кодовых слов с номерами из $\mathcal{L}$, т.е.

$$\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) \succeq \bigvee_{j \in \mathcal{L}} \boldsymbol{x}(j), \quad \mathcal{L} \subset [t] \setminus \mathcal{S}, \quad |\mathcal{L}| = L. \tag{2.1.1}$$

В противном случае множество $\mathcal{S}$ будем называть *s_L-хорошим* для кода X. Другими словами, дизъюнктивная сумма любого набора столбцов кода X, номера которых образуют s_L-хорошее множество $\mathcal{S}$, покрывает не более $L-1$ столбцов кода X, номера которых не входят в $\mathcal{S}$.

Пусть символ $\mathbf{B}_L(s, X)$ ($\mathbf{G}_L(s, X)$) обозначает совокупность всех s_L-плохих (s_L-хороших) множеств $\mathcal{S}$ для кода X, а $|\mathbf{B}_L(s, X)|$ ($|\mathbf{G}_L(s, X)|$) – объем соответствующей совокупности. Заметим, что

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

Определение 2.1.2 ([45]). Зафиксируем параметр ε, $0 \le \varepsilon < 1$. Код X длины N и объема t назовем *дизъюнктивным* кодом *силы* s со *списочным декодированием* (СД) при *объеме списка* L и с *вероятностью ошибки* ε (кратко, *СД* (s_L, ε)-*кодом*), если

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

Заметим, что концепция СД (s_L, ε)-кодов является естественным обобщением СД s_L-кодов, введенных в определении 1.1.1. Действительно, СД s_L-код является СД $(s_L, 0)$-кодом.

Используя традиционную теоретико-информационную терминологию, принятую в вероятностной теории кодирования [32, 8], введем

Определение 2.1.3 ([45])**.** Зафиксируем параметр R, $R > 0$, и учитывая первое неравенство в (2.1.2), определим *ошибку почти дизъюнктивных СД s_L-кодов*:

$$\varepsilon_L(s, R, N) \triangleq \min_{X: t=\lfloor 2^{RN} \rfloor} \left\{ \frac{|\mathbf{B}_L(s, X)|}{\binom{t}{s}} \right\}, \quad R > 0, \tag{2.1.3}$$

где минимум взят по всем кодам X длины N и объема $t = \lfloor 2^{RN} \rfloor$. Функцию

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

назовем *экспонентой ошибки почти дизъюнктивных СД s_L-кодов*, число

$$C_L(s) \triangleq \sup\{ R : \mathbf{E}_L(s, R) > 0\} - \tag{2.1.5}$$

пропускной способностью почти дизъюнктивных СД s_L-кодов.

Напомним, что скорость $R_L(s)$ дизъюнктивных кодов со списочным декодированием является нижней границей на скорость двухступенчатых процедур групповых проверок в дизъюнктивной модели поиска s дефектов. Пропускная способность $C_L(s)$ является нижней границей на скорость двухступенчатых процедур групповых проверок с *ошибкой*, стремящийся к 0 при росте количества элементов t, где под ошибкой подразумевается доля s-подмножеств элементов среди всех различных $\binom{t}{s}$ подмножеств, появление которых в качестве множества дефектных элементов приводит к отказу от решения. При $R_L(s) < R < C_L(s)$ существуют двухступенчатые процедуры со скоростью R и ошибкой, не превосходящей величину

$$2^{-N(\mathbf{E}_L(s,R)+o(1))}, \quad N \to \infty.$$

2.2 Нижние границы пропускной способности и экспоненты ошибки

Следующая теорема о нижней границе пропускной способности $C_L(s)$ получена И.В. Воробъевым в работе [45] с помощью метода случайного кодирования на ансамбле двоичных равновесных кодов

Теорема 2.2.1 ([45])**.** *Справедливы два утверждения.*
1. *Величина $C_L(s)$ удовлетворяет неравенству:*

$$C_L(s) \geq \underline{C}(s) \triangleq \max_{0<Q<1} C(s, Q) = C(s, Q(s)), \quad s \geq 2,\ L \geq 1, \tag{2.2.1}$$

$$C(s, Q) \triangleq h(Q) - [1 - (1 - Q)^s]\, h\left(\frac{Q}{1 - (1 - Q)^s} \right), \quad s \geq 2, \quad 0 < Q < 1. \tag{2.2.2}$$

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

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

Метод случайного кодирования на ансамбле двоичных равновесных кодов развивается в следующей теореме, в которой получена нижняя граница экспоненты ошибки $\mathbf{E}_L(s,R)$. Через

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

будем обозначать положительную часть функции.

Теорема 2.2.2 (Нижняя граница для $\mathbf{E}_L(s,R)$)**.** *Справедливы три утверждения.*
1. *Величина $\mathbf{E}_L(s,R)$ удовлетворяет неравенству:*

$$\mathbf{E}_L(s,R) \geq \underline{\mathbf{E}}_L(s,R) \triangleq \max_{0<Q<1} E_L(s,R,Q), \quad s \geq 2,\ L \geq 1,\ R > 0, \tag{2.2.4}$$

$$E_L(s,R,Q) \triangleq \min_{Q \leq q \leq \min\{1,sQ\}} \left\{ \mathcal{A}(s,Q,q) + L \cdot [h(Q) - q \cdot h(Q/q) - R]^+ \right\}, \tag{2.2.5}$$

где функция $\mathcal{A}(s,Q,q)$, $Q < q < \min\{1, sQ\}$, определена следующим образом:

$$\mathcal{A}(s,Q,q) \triangleq (1-q)\log_2(1-q) + q\log_2\left[\frac{Qy^s}{1-y}\right] + sQ\log_2\frac{1-y}{y} + sh(Q), \tag{2.2.6}$$

а число y в правой части (2.2.6) *является единственным решением уравнения*

$$q = Q\frac{1-y^s}{1-y}, \quad 0 < y < 1. \tag{2.2.7}$$

2. *Для любых $s \geq 2$ и $L \geq 1$ нижняя граница $\underline{\mathbf{E}}_L(s,R)$, определенная* (2.2.4)-(2.2.7)*, является $\cup$-выпуклой функцией параметра $R > 0$. При $0 < R < \underline{C}(s)$ справедливо неравенство $\underline{\mathbf{E}}_L(s,R) > 0$. Если $R \geq \underline{C}(s)$, то $\underline{\mathbf{E}}_L(s,R) = 0$. Кроме того, существует такое число $\underline{R}_L^{(cr)}(s)$ (критическая скорость), $0 \leq \underline{R}_L^{(cr)}(s) < \underline{C}(s)$, что*

$$\underline{\mathbf{E}}_L(s,R) = (s+L-1)\underline{R}_L(s) - LR, \quad \textit{при} \quad 0 \leq R \leq \underline{R}_L^{(cr)}(s), \tag{2.2.8}$$

и

$$\underline{\mathbf{E}}_L(s,R) > (s+L-1)\underline{R}_L(s) - LR, \quad \textit{при} \quad R > \underline{R}_L^{(cr)}(s), \tag{2.2.9}$$

где граница случайного кодирования $\underline{R}_L(s)$ определяется формулами (1.2.5)-(1.2.7) *в теореме 1.2.2. Причем, прямая, задаваемая* (2.2.8)*, является касательной к функции $\underline{\mathbf{E}}_L(s,R)$ в точке $R = \underline{R}_L^{(cr)}(s)$.*
3. *При любых $s \geq 2$, $L \geq 1$ и $R \geq R_L^{(cr)}(s)$ справедливо равенство $\underline{\mathbf{E}}_L(s,R) = \underline{\mathbf{E}}_{L+1}(s,R)$, а последовательности критической скорости и соответствующего значения нижней границы экспоненты ошибки имеют пределы:*

$$\lim_{L\to\infty} \underline{R}_L^{(cr)}(s) = \underline{R}_\infty(s), \tag{2.2.10}$$

$$\lim_{L\to\infty} \underline{\mathbf{E}}_L(s, \underline{R}_L^{(cr)}(s)) = (s-1)\underline{R}_\infty(s), \tag{2.2.11}$$

где скорость $\underline{R}_\infty(s)$ определена (1.2.9) *в теореме 1.2.2.*

В таблице 2.2.1 приведены численные значения нижней границы пропускной способности $\underline{C}(s)$, задаваемой (2.2.1)-(2.2.2), вместе с оптимальным весом $Q(s)$, а также численные значения верхней границы СД s_1-кодов $\overline{R}_1(s)$, задаваемой (1.3.3)-(1.3.4). Сравнение

значений $\underline{C}(s)$ и $\overline{R}_1(s)$ приводит к неравенству $R_1(s) < C(s)$, т.е. скорость СД s_1-кодов строго меньше пропускной способности почти дизъюнктивных СД s_1-кодов. К тому же, из асимптотических формул (1.3.5) и (2.2.3) вытекает строгое неравенство $R_1(s) < C(s)$ для больших значений параметра s. Кроме того, в таблице 2.2.1 представлены некоторые численные значения *критической скорости* $\underline{R}_L^{(cr)}(s)$.

На рисунке 2.2.1 при некоторых значениях параметров s и L изображены описываемые соотношениями (2.2.4)-(2.2.7) графики экспоненты $\underline{\mathbf{E}}_L(s, R)$ для ансамбля равновесных кодов.

Отметим, что из аналитических свойств функции $\underline{\mathbf{E}}_L(s, R)$ следует существование при фиксированных параметре $s \geq 2$ и скорости R, $\underline{R}_\infty(s) < R < \underline{C}(s)$, максимального значения экспоненты ошибки $\underline{\mathbf{E}}_L(s, R)$ и минимального значения параметра L, при котором оно принимается.

Таблица 2.2.1: Численные значения $\underline{C}(s)$ и $\underline{R}_L^{(cr)}(s)$

s	2	3	4	5	6
$\underline{C}(s)$	0.3832	0.2455	0.1810	0.1434	0.1188
$\underline{Q}(s)$	0.2864	0.2028	0.1569	0.1280	0.1080
$\overline{R}_1(s)$	0.3219	0.1993	0.1405	0.1056	0.0830
$\underline{R}_1^{(cr)}(s)$	0.3510	0.2284	0.1705	0.1364	0.1137
s_L	2_2	3_2	4_2	5_2	6_2
$\underline{R}_L^{(cr)}(s)$	0.3355	0.2177	0.1632	0.1311	0.1098
s_L	2_3	3_3	4_3	5_3	6_3
$\underline{R}_L^{(cr)}(s)$	0.3279	0.2109	0.1580	0.1271	0.1067
s_L	2_4	3_4	4_4	5_4	6_4
$\underline{R}_L^{(cr)}(s)$	0.3242	0.2065	0.1542	0.1240	0.1041
s_L	2_5	3_5	4_5	5_5	6_5
$\underline{R}_L^{(cr)}(s)$	0.3226	0.2036	0.1514	0.1216	0.1021
s_L	2_6	3_6	4_6	5_6	6_6
$\underline{R}_L^{(cr)}(s)$	0.3218	0.2017	0.1494	0.1197	0.1004

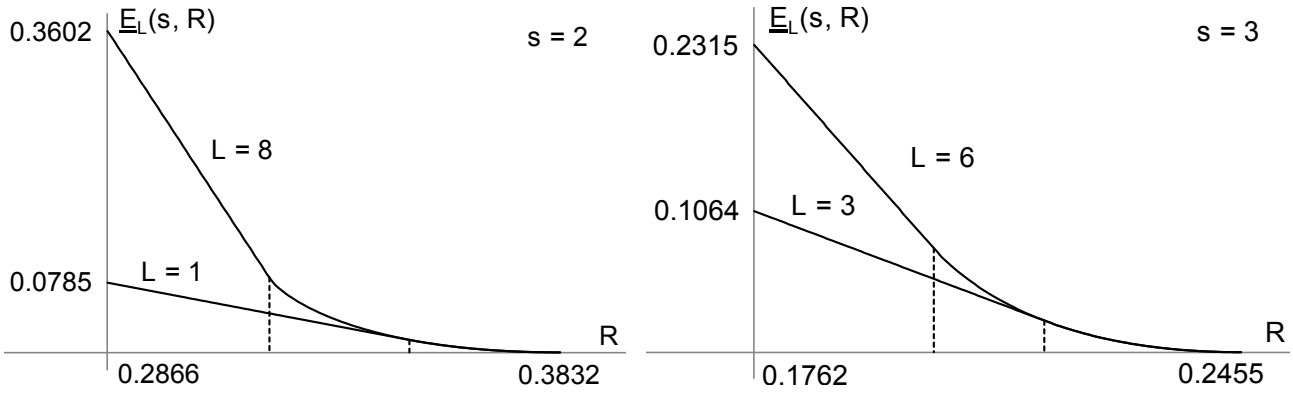

Рис. 2.2.1: Экспонента $\underline{\mathbf{E}}_L(s, R)$

Доказательство теоремы 2.2.2

Доказательство утверждения 1. Число $|\mathbf{B}_L(s,X)|$ всех s_L-плохих множеств $\mathcal{S}$, $\mathcal{S}\subset[t]$, $|\mathcal{S}|=s$, для кода X можно представить в следующем виде:

$$|\mathbf{B}_L(s,X)| \triangleq \sum_{\mathcal{S}\subset[t],|\mathcal{S}|=s} \psi_L(X,\mathcal{S}), \tag{2.2.12}$$

где

$$\psi_L(X,\mathcal{S}) \triangleq \begin{cases} 1, & \text{если множество } \mathcal{S}\in\mathbf{B}_L(s,X),\\ 0, & \text{в остальных случаях.}\end{cases}$$

Зафиксируем параметры Q, $0<Q<1$, и $R>0$. Также, как и при доказательстве теореме 1.2.2, определим ансамбль $E(N,t,Q)$ двоичных матриц X с N строками и $t\triangleq\lfloor 2^{RN}\rfloor$ столбцами, где столбцы выбираются независимо и равновероятно из множества, состоящего из $\binom{N}{w}$ столбцов фиксированного веса $w\triangleq\lfloor QN\rfloor$. Непосредственно из (2.2.12) следует, что для ансамбля $E(N,t,Q)$ математическое ожидание $\overline{|\mathbf{B}_L(s,X)|}$ числа $|\mathbf{B}_L(s,X)|$ равно

$$\overline{|\mathbf{B}_L(s,X)|} = \binom{t}{s}\Pr\{\mathcal{S}\in\mathbf{B}_L(s,X)\}$$

где для любого s-множества $\mathcal{S}$ вероятность в правой части зависит лишь от параметров s, L, R, Q и N и не зависит от выбора самого множества $\mathcal{S}$. Следовательно, математическое ожидание доли числа всех s_L-плохих множеств $\mathcal{S}$, $\mathcal{S}\subset[t]$, $|\mathcal{S}|=s$, равно

$$\mathcal{E}_L^{(N)}(s,R,Q) \triangleq \binom{t}{s}^{-1}\overline{|\mathbf{B}_L(s,X)|} = \Pr\{\mathcal{S}\in\mathbf{B}_L(s,X)\}. \tag{2.2.13}$$

Поэтому очевидную верхнюю *границу случайного кодирования* для ошибки (2.1.3) почти дизъюнктивных s_L-кодов можно представить следующим образом:

$$\varepsilon_L(s,R,N) \triangleq \min_{X\,:\,t=\lfloor 2^{RN}\rfloor}\left\{\frac{|\mathbf{B}_L(s,X)|}{\binom{t}{s}}\right\} \le \mathcal{E}_L^{(N)}(s,R,Q), \quad 0<Q<1. \tag{2.2.14}$$

Перепишем функцию $\mathcal{E}_L^{(N)}(s,R,Q)$, определенную (2.2.13), в виде:

$$\mathcal{E}_L^{(N)}(s,R,Q) = \sum_{k=\lfloor QN\rfloor}^{\min\{N,s\lfloor QN\rfloor\}} \Pr\left\{\mathcal{S}\in\mathbf{B}_L(s,X)\;\middle/\;\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}\mathcal{P}^{(N)}(s,Q,k). \tag{2.2.15}$$

Здесь мы применили формулу полной вероятности и воспользовались обозначением:

$$\mathcal{P}^{(N)}(s,Q,k) \triangleq \Pr\left\{\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}, \quad \lfloor QN\rfloor\le k\le\min\{N,s\lfloor QN\rfloor\}. \tag{2.2.16}$$

Для ансамбля $E(N,t,Q)$ и произвольного k, $\lfloor QN\rfloor\le k\le\min\{N,s\lfloor QN\rfloor\}$, условная вероятность события (2.1.1) равна

$$\Pr\left\{\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\succeq\bigvee_{j\in\mathcal{L}}\boldsymbol{x}(j)\;\middle/\;\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\} = \left[\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}\right]^L. \tag{2.2.17}$$

Кроме того, используя терминологию типов (как и при доказательстве теоремы 1.2.2):

$$\{n(\boldsymbol{u}),\ \boldsymbol{u} \triangleq (u_1, u_2, \ldots, u_s) \in \{0,1\}^s\}, \quad 0 \le n(\boldsymbol{u}) \le N, \quad \sum_{\boldsymbol{u}} n(\boldsymbol{u}) = N,$$

можем записать вероятность события (2.2.16) в ансамбле $E(N,t,Q)$ в виде:

$$\mathcal{P}^{(N)}(s,Q,k) = \binom{N}{\lfloor QN \rfloor}^{-s} \cdot \sum_{(2.2.19)} \frac{N!}{\prod_{\boldsymbol{u}} n(\boldsymbol{u})!}, \quad \lfloor QN \rfloor \le k \le \min\{N, s\lfloor QN \rfloor\}, \qquad (2.2.18)$$

где сумма в правой части (2.2.18) взята по всем типам $\{n(\boldsymbol{u})\}$, удовлетворяющим условию

$$n(\boldsymbol{0}) = N - k, \qquad \sum_{\boldsymbol{u}:\, u_i = 1} n(\boldsymbol{u}) = \lfloor QN \rfloor \quad \text{для любого } i \in [s]. \qquad (2.2.19)$$

Пусть функция

$$\mathcal{A}(s,Q,q) \triangleq \lim_{N\to\infty} \frac{-\log_2 \mathcal{P}^{(N)}(s,Q,\lfloor qN \rfloor)}{N}, \quad Q \le q \le \min\{1, sQ\}, \qquad (2.2.20)$$

обозначает главный член логарифмической асимптотики вероятности (2.2.16), вычисляемый с помощью формул (2.2.18)-(2.2.19).

Далее воспользовавшись представлением (2.2.15), условной вероятностью (2.2.17) и стандартной оценкой

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

получим верхнюю границу

$$\mathcal{E}_L^{(N)}(s,R,Q) \le \sum_{k=\lfloor QN \rfloor}^{\min\{N, s\lfloor QN \rfloor\}} \mathcal{P}^{(N)}(s,Q,k) \cdot \min\left\{1\,;\, \binom{t-s}{L}\left[\frac{\binom{k}{\lfloor QN \rfloor}}{\binom{N}{\lfloor QN \rfloor}}\right]^L\right\}, \qquad (2.2.21)$$

где объем кода $t \triangleq \lfloor 2^{RN} \rfloor$. Из неравенства (2.2.21) и границы случайного кодирования (2.2.14) вытекает *нижняя граница* для экспоненты ошибки (2.1.4), задаваемая (2.2.4)-(2.2.5).

Аналитические свойства функции (2.2.20) сформулированы в качестве лемм 2.2.1-2.2.3, которые будут доказаны ниже.

Лемма 2.2.1. *Функцию $\mathcal{A}(s,Q,q)$ параметра q, $Q < q < \min\{1, sQ\}$, определенную в* (2.2.20)*, можно записать в параметрическом виде* (2.2.6)-(2.2.7)*. Кроме того, эта функция является $\cup$-выпуклой, монотонно убывающей на интервале $(Q, 1-(1-Q)^s)$ и монотонно возрастающей на интервале $(1-(1-Q)^s, \min\{1, sQ\})$, причем минимум, равный* 0*, функция $\mathcal{A}(s,Q,q)$ достигает в точке $q = 1-(1-Q)^s$, т.е.*

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

Лемма 2.2.2. *Для любого фиксированного Q, $0 < Q < 1$, функция*

$$f(Q,q) \triangleq q \cdot h(Q/q), \quad Q < q < \min\{1, sQ\},$$

является $\cap$-выпуклой и монотонно возрастающей.

Лемма 2.2.3. *Для любого фиксированного Q, $0 < Q < 1$, функция*

$$\mathcal{A}(s,Q,q) + L \cdot [h(Q) - q \cdot h(Q/q)], \quad Q < q < \min\{1, sQ\}, \tag{2.2.22}$$

является $\cup$-выпуклой. Минимум этой функции достигается в точке $q = q_L^{(2)}(s,Q) > 1-(1-Q)^s$ и равен величине $A_L(s,Q)$, определенной формулами (1.2.6)-(1.2.7)*, т.е.*

$$\min_{Q<q<\min\{1,sQ\}} \{\mathcal{A}(s,Q,q) + L \cdot [h(Q) - q \cdot h(Q/q)]\} \;=\; A_L(s,Q),$$

$$q_L^{(2)}(s,Q) \triangleq \operatorname*{argmin}_{Q<q<\min\{1,sQ\}} \{\mathcal{A}(s,Q,q) + L \cdot [h(Q) - q \cdot h(Q/q)]\}.$$

Следуя утверждению леммы 2.2.1, а также формулам (2.2.2) и (2.2.5), несложно проверить, что при $0 < R < C(s,Q)$ функция $E_L(s,Q) > 0$.

Утверждение 1 доказано.

Доказательство утверждения 2. Нетрудно видеть, что если функция $E_L(s,R,Q)$ является $\cup$-выпуклой функцией параметра R при $0 < Q < 1$, то $\cup$-выпуклой функцией параметра R будет и $\underline{\mathbf{E}}_L(s,R)$. Докажем, что функция $E_L(s,R,Q)$ обладает свойством $\cup$-выпуклости.

Зафиксируем параметры Q и R, $0 < Q < 1$, $0 < R < 1$. Пусть $q^{(0)}(s,Q) \triangleq 1-(1-Q)^s$. Из лемм 2.2.1-2.2.3 вытекает, что минимум в (2.2.5) достигается в некоторой точке из интервала $[q^{(0)}(s,Q),\, q_L^{(2)}(s,Q)]$. Рассмотрим функцию

$$\mathcal{B}(R,Q,q) = h(Q) - qh(Q/q) - R.$$

Пусть существует решение $q = q^{(1)}(R,Q)$ уравнения $\mathcal{B}(R,Q,q) = 0$, $0 < q < 1$. Тогда заметим, что минимум в (2.2.5) достигается при $q = q_L^{(min)}(s,R,Q)$, где

$$q_L^{(min)}(s,R,Q) = \begin{cases} q_L^{(2)}(s,Q) & \text{при } \mathcal{B}(R,Q,q^{(2)}) >= 0, \\ q^{(1)}(R,Q) & \text{при } \mathcal{B}(R,Q,q^{(0)}) > 0 \text{ и } \mathcal{B}(R,Q,q^{(2)}) < 0, \\ q^{(0)}(s,Q) & \text{при } \mathcal{B}(R,Q,q^{(0)}) <= 0. \end{cases}$$

При подстановке $q = q_L^{(min)}(s,R,Q)$ в (2.2.5) имеем

$$E_L(s,R,Q) = \begin{cases} A_L(s,Q) - LR & \text{при } 0 \le R \le \underline{R}_L^{(cr)}(s,Q), \\ \mathcal{A}(s,Q,q^{(1)}) & \text{при } \underline{R}_L^{(cr)}(s,Q) \le R \le C(s,Q), \\ 0 & \text{при } C(s,Q) \le R, \end{cases} \tag{2.2.23}$$

где $A_L(s,Q)$ определена в (1.2.6)-(1.2.7), $\mathcal{A}(s,Q,q)$ – в (2.2.6)-(2.2.7), $C(s,Q)$ – в (2.2.2), а скорость

$$\underline{R}_L^{(cr)}(s,Q) \triangleq h(Q) - q^{(2)}h(Q/q^{(2)}).$$

Поскольку функция $q^{(1)}(R,Q)$ является неявной функцией параметра R, определяемой уравнением $\mathcal{B}(R,Q,q) = 0$, то несложно посчитать ее производную:

$$\left(q^{(1)}(R,Q)\right)'_R = \left(\log_2 \frac{q-Q}{q}\right)^{-1}. \tag{2.2.24}$$

Тогда воспользуемся (2.2.23) и (2.2.24), чтобы записать производную $E_L(s,R,Q)$ по переменной R:

$$(E_L(s,R,Q))'_R = \begin{cases} -L & \text{при } 0 \le R \le \underline{R}_L^{(cr)}(s,Q), \\ \log_2 \frac{Qy^s}{1-Q-y+Qy^s} \left(\log_2 \frac{q-Q}{q}\right)^{-1} & \text{при } \underline{R}_L^{(cr)}(s,Q) \le R \le C(s,Q), \\ 0 & \text{при } C(s,Q) \le R, \end{cases}$$

где в записи выражения во второй строке для краткости обозначено $q = q^{(1)}(R,Q)$, и y определяется с помощью (2.2.7). Очевидно, что функция во второй строке является неубывающей функцией параметра R. Кроме того, при $R = \underline{R}_L^{(cr)}(s,Q)$ эта функция равна $-L$, а при $R = C(s,Q)$ она равна 0. Таким образом, производная $E_L(s,R,Q)$ по переменной R существует, является непрерывной и неубывающей функцией, т.е. $E_L(s,R,Q)$ является $\cup$-выпуклой.

Если $R = 0$, то для любого $0 < Q < 1$ будет выполнено неравенство $h(Q) - qh(Q/q) \ge 0$. Следовательно, в случае $R = 0$ имеет место (2.2.8).

Если $R = \underline{C}(s)$, то $\underline{\mathbf{E}}_L(s,R) = 0$. Значит, при $R = \underline{C}(s)$ выполнено (2.2.9).

Итак, поскольку функция $\underline{\mathbf{E}}_L(s,R)$ обладает свойством $\cup$-выпуклости, то найдется такое $\underline{R}_L^{(cr)}(s)$, что равенство (2.2.8) будет выполнено при $0 \le R \le \underline{R}_L^{(cr)}(s)$, а при $R > \underline{R}_L^{(cr)}(s)$ будет иметь место неравенство (2.2.9).

Утверждение 2 доказано.

Доказательство утверждения 3. При $R \ge \max\{\underline{R}_L^{(cr)}(s), \underline{R}_{L+1}^{(cr)}(s)\}$ функции $\underline{\mathbf{E}}_L(s,R)$ и $\underline{\mathbf{E}}_{L+1}(s,R)$ совпадают, так как заданы вторым и третьим выражениями системы (2.2.23), которые не зависят от L. Так как угол наклона касательной (2.2.8) при $L+1$ больше, чем при L, то в силу $\cup$-выпуклости функции $\underline{\mathbf{E}}_L(s,R)$ выполнено неравенство $\underline{R}_L^{(cr)}(s) \ge \underline{R}_{L+1}^{(cr)}(s)$.

Покажем теперь существование пределов (2.2.10) и (2.2.11). Нетрудно заметить, что точка пересечения $R = R_0$ касательных (2.2.8) при $L+1$ и L удовлетворяет двойному неравенству $\underline{R}_{L+1}^{(cr)}(s) \le R_0 \le \underline{R}_L^{(cr)}(s)$. В то же время из (2.2.8) следует

$$R_0 = (s+L)\underline{R}_{L+1}(s) - (s+L-1)\underline{R}_L(s).$$

Перейдем к пределу при $L \to \infty$. Из двух упомянутых выше фактов вытекает неравенство

$$\underline{R}_\infty(s) \le \lim_{L\to\infty} \underline{R}_L^{(cr)}(s) \le \underline{R}_\infty(s),$$

где $\underline{R}_\infty(s) \triangleq \lim_{L\to\infty} \underline{R}_L(s)$ определено в (1.2.9). Таким образом, предел критической скорости существует и равен (2.2.10). Для вывода (2.2.11) достаточно перейти к пределу при $L \to \infty$ в (2.2.8) и подставить значения (1.2.9) и (2.2.11).

Утверждение 3 доказано. $\square$.

Доказательство лемм 2.2.1-2.2.3

Доказательство леммы 2.2.1. Зафиксируем $s \ge 2$, 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 $\{n(\boldsymbol{u})\}$ рассмотрим соответствующее распределение $\tau : \tau(\boldsymbol{u}) = \frac{n(\boldsymbol{u})}{N}, \quad \forall\ \boldsymbol{u} \in \{0,1\}^s$.

С помощью формулы Стирлинга для типов, соответствующих этим распределениям, находим логарифмическую асимптотику слагаемого в (2.2.18):

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

$$F(\tau, Q, q) = \sum_{\boldsymbol{u}} \tau(\boldsymbol{u}) \log_2 \tau(\boldsymbol{u}) + s \cdot h(Q). \tag{2.2.25}$$

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

$$\mathcal{A}(s, Q, q) = \min_{\tau \in (2.2.27):(2.2.28)} F(\tau, Q, q), \tag{2.2.26}$$

$$\{\tau : \ \forall\ \boldsymbol{u} = (u_1, \ldots, u_s) \in \{0,1\}^s \quad 0 < \tau(\boldsymbol{u}) < 1\}, \tag{2.2.27}$$

$$\sum_{\boldsymbol{u}} \tau(\boldsymbol{u}) = 1, \qquad \tau(\boldsymbol{0}) = 1 - q, \qquad \sum_{\boldsymbol{u}:u_i=1} \tau(\boldsymbol{u}) = Q \quad \forall\ i \in [s], \tag{2.2.28}$$

причем ограничения (2.2.28) индуцированы свойствами (2.2.19), а также условиями, налагаемыми на типы.

Для вычисления точки минимума применим стандартный метод множителей Лагранжа. Рассмотрим лагранжиан

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

Необходимые условия экстремального распределения имееют вид

$$\begin{cases} \frac{\partial \Lambda}{\partial \tau(\boldsymbol{0})} = \log_2 \tau(\boldsymbol{0}) + \log_2 e + \lambda_0 + \lambda_{s+1} = 0, \\ \frac{\partial \Lambda}{\partial \tau(\boldsymbol{u})} = \log_2 \tau(\boldsymbol{u}) + \log_2 e + \lambda_{s+1} + \sum_{i=1}^{s} u_i \lambda_i = 0 \quad \text{для любого } \boldsymbol{u} \neq \boldsymbol{0}. \end{cases} \tag{2.2.29}$$

Легко видеть, что матрица вторых производных лагранжиана является диагональной. Также можем заключить, что эта матрица является положительно определенной в области (2.2.27). Следовательно, функция $F(\tau, Q)$ является строго $\cup$-выпуклой в области (2.2.27).

Далее воспользуемся теоремой Каруша-Куна-Таккера [2], утверждающей, что всякое решение $\tau \in (2.2.27)$, удовлетворяющее системе (2.2.29), ограничениям (2.2.28) и имеющее положительно определенную матрицу вторых производных лагранжиана в этой точке, является локальным минимумом функции $F(\tau, Q)$. Таким образом, если есть решение системы (2.2.29), (2.2.28) в области (2.2.27), то оно единственно, и эта точка является решением в задаче минимизации (2.2.26)-(2.2.28).

Заметим, что из симметрии задачи следует равенство $\eta \triangleq \lambda_1 = \lambda_2 = \cdots = \lambda_s$. Для краткости введем параметры $\mu \triangleq \log_2 e + \lambda_{s+1}$ и $\nu \triangleq \lambda_0$. Тогда уравнения (2.2.28) и (2.2.29) принимают вид

$$\begin{cases} 1)\ \log_2 \tau(\boldsymbol{u}) + \mu + \eta \sum_{i=1}^{s} u_i = 0 \quad \text{при } \boldsymbol{u} \neq \boldsymbol{0}, \\ 2)\ \log_2 \tau(\boldsymbol{0}) + \mu + \nu = 0, \\ 3)\ \tau(\boldsymbol{0}) = 1 - q, \\ 4)\ \sum_{\boldsymbol{u}} \tau(\boldsymbol{u}) = 1, \\ 5)\ \sum_{\boldsymbol{u}:u_i=1} \tau(\boldsymbol{u}) = Q \quad \text{при } i \in [s]. \end{cases} \tag{2.2.30}$$

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

$$\tau(\boldsymbol{u}) = \frac{1}{2^{\mu} y^{s}} (1-y)^{\sum u_j} y^{s-\sum u_j} \quad \text{при } \boldsymbol{u} \neq \boldsymbol{0}. \tag{2.2.31}$$

Подставив (2.2.31) в пятое уравнение системы (2.2.30), получаем

$$\sum_{\boldsymbol{u}: u_i = 1} \frac{1}{2^{\mu} y^{s}} (1-y)^{\sum u_j} y^{s-\sum u_j} = \frac{1-y}{2^{\mu} y^{s}}.$$

Отсюда находим

$$\mu = \log_2 \frac{1-y}{Q y^{s}}. \tag{2.2.32}$$

Подстановка (2.2.31), (2.2.32) и третьего уравнения системы (2.2.30) в четвертое уравнение системы (2.2.30) дает

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

т.е. в точности уравнение (2.2.7). Таким образом, ограничения (2.2.28) и условия (2.2.29) дают единственное решение τ в области (2.2.27):

$$\tau(\boldsymbol{0}) = 1 - q, \qquad \tau(\boldsymbol{u}) = \frac{Q}{1-y} (1-y)^{\sum u_j} y^{s-\sum u_j} \quad \text{при } \boldsymbol{u} \neq \boldsymbol{0}, \tag{2.2.33}$$

где параметры q и y связаны соотношением (2.2.7). Для того чтобы получить точную формулу (2.2.6), достаточно подставить (2.2.33) в (2.2.25).

Теперь докажем свойства функции $A(s, Q, q)$. Прежде всего заметим, что функция $q(y)$ монотонно убывает по y на интервале $y \in (0, 1)$ и принимает значения Q и sQ на концах этого интервала. Поэтому вместо (2.2.6) можно рассмотреть функцию $\mathcal{T}(s, Q, y) = \mathcal{A}(s, Q, q(y))$ параметра y на интервале $y \in (0, y_1)$, причем $q(y_1) = \min\{1, sQ\}$. Посчитаем производную функции $\mathcal{T}(s, Q, y)$ по переменной y

$$\frac{\partial \mathcal{T}(s, Q, y)}{\partial y} = q'(y) \log_2 \left[\frac{Q y^{s}}{1 - Q - y + Q y^{s}} \right]. \tag{2.2.34}$$

Таким образом, функция $\mathcal{T}(s, Q, y)$ убывает по y при $y \in (0, 1-Q)$, возрастает при $y \in (1-Q, y_1)$, а также является $\cup$-выпуклой. Свой минимум, равный 0, она достигает в точке $y_0 = 1 - Q$.

Лемма 2.2.1 доказана. $\square$

Доказательство леммы 2.2.2. Зафиксируем параметр $0 < Q < 1$. Посчитаем производную функции $f(Q, q) \triangleq q \cdot h(Q/q)$ по переменной q:

$$\frac{\partial f(Q, q)}{\partial q} = -\log_2 \left[\frac{q - Q}{q} \right], \qquad Q < q < 1. \tag{2.2.35}$$

Следовательно, функция $f(Q, q)$ возрастает на интервале $q \in (Q, 1)$, а также является $\cap$-выпуклой и на любом полуинтервале $q \in (Q, a]$, $Q < a < 1$, достигает свой единственный максимум в точке $q = a$.

Лемма 2.2.2 доказана. $\square$

Доказательство леммы 2.2.3. Зафиксируем параметр $0 < Q < 1$. В силу свойств (2.2.7) вместо (2.2.22) можно рассмотреть следующую функцию

$$\mathcal{F}(s, L, Q, y) \triangleq \mathcal{A}(s, Q, q(y)) + L[h(Q) - q(y) \cdot h(Q/q(y))]$$

параметра $0 < y < y_1$, причем $q(y_1) = \min\{1, sQ\}$. Пользуясь (2.2.34) и (2.2.35), вычислим производную $\mathcal{F}(s, L, Q, y)$ по переменной y:

$$\frac{\partial \mathcal{F}(s, L, Q, y)}{\partial y} = \mathcal{T}'(s, Q, y) - Lq'(y) f'_q(Q, y) = q'(y) \cdot \log_2 \left[\frac{Qy^s}{1 - Q - y + Qy^s} \left(\frac{y - y^s}{1 - y^s} \right)^L \right].$$

Таким образом, уравнение $\mathcal{F}'(s, L, Q, y) = 0$ верно в том и только том случае, если выполняется

$$y = 1 - Q + Qy^s \left[1 - \left(\frac{y - y^s}{1 - y^s} \right)^L \right],$$

т.е. имеет место (1.2.7). Очевидно, что функция (2.2.22) является $\cap$-выпуклой и достигает свой минимум в точке $q = q(y_2)$, где с помощью y_2 обозначено решение уравнения (1.2.7).

Заметим, что выполняется

$$1 - q(y_2) = 1 - \frac{Q(1 - y_2^s)}{1 - y_2} = \frac{Qy_2^s}{1 - y_2} \left(\frac{y_2 - y_2^s}{1 - y_2^s} \right)^L.$$

Следовательно

$$\begin{aligned} \mathcal{F}(s, L, Q, y_2) = \left(1 - Q \frac{1 - y_2^s}{1 - y_2} \right) \log_2 \left[\frac{Qy_2^s}{1 - y_2} \left(\frac{y_2 - y_2^s}{1 - y_2^s} \right)^L \right] + Q \frac{1 - y_2^s}{1 - y_2} \log_2 \frac{Qy_2^s}{1 - y_2} \\ + sQ \log_2 \frac{1 - y_2}{y_2} + sh(Q) + Lh(Q) + LQ \log_2 \frac{1 - y_2}{1 - y_2^s} + LQ \frac{y_2 - y_2^s}{1 - y_2} \log_2 \frac{y_2 - y_2^s}{1 - y_2^s}. \end{aligned}$$

Упрощением предыдущего равенства получаем

$$\min_{0 < y < y_1} \mathcal{F}(s, L, Q, y) = A_L(s, Q),$$

где функция $A_L(s, Q)$ определена в (1.2.6)-(1.2.7).

Лемма 2.2.3 доказана. $\square$

2.3 Верхняя граница пропускной способности

Тривиальная верхняя граница $R_1(s) \le 1/s$ для скорости СД s_1-кодов была получена в 1964 году [35]. Позднее [25] было показано, что точно такая же верхняя граница справедлива и в общем случае $L \ge 1$, т.е. $R_L(s) \le 1/s$. Данное неравенство для пропускной способности почти дизъюнктивных СД s_L-кодов устанавливается в следующей теореме.

Теорема 2.3.1 (Верхняя граница для $C_L(s)$)**.** *Справедливо неравенство*

$$C_L(s) \le 1/s, \qquad s \ge 1, \quad L \ge 1.$$

Доказательство теоремы 2.3.1. Зафиксируем параметры R, $R > 0$, и ε, $0 \le \varepsilon < 1$. Пусть X – произвольный СД (s_L, ε)-код длины N и объема $t \triangleq \lfloor 2^{RN} \rfloor$. Для каждой двоичной последовательности $\boldsymbol{u} \in \{0, 1\}^N$ рассмотрим множество

$$\mathbf{G}_L(s, \boldsymbol{u}, X) \triangleq \left\{ \mathcal{S} \,:\, \mathcal{S} \in \mathbf{G}_L(s, X),\ \bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) = \boldsymbol{u} \right\} \subset \mathbf{G}_L(s, X), \tag{2.3.1}$$

состоящее из всех s_L-хороших множеств $\mathcal{S}$, для которых соответствующая им дизъюнктивная сумма столбцов кода X равна $\boldsymbol{u}$. Из (2.3.1) и интерпретации s_L-хорошего множества в определении 1 непосредственно следует, что

$$\mathbf{G}_L(s,\boldsymbol{u},X)\cap\mathbf{G}_L(s,\boldsymbol{v},X)=\emptyset,\quad \boldsymbol{u}\neq\boldsymbol{v},\qquad \sum_{\boldsymbol{u}\in\{0,1\}^N}\mathbf{G}_L(s,\boldsymbol{u},X)=\mathbf{G}_L(s,X). \tag{2.3.2}$$

и, кроме того, для любого $\boldsymbol{u}\in\{0,1\}^N$ объем

$$|\mathbf{G}_L(s,\boldsymbol{u},X)|\le\binom{s+L-1}{s},\quad \boldsymbol{u}\in\{0,1\}^N,\quad s\ge 1,\quad L\ge 1. \tag{2.3.3}$$

Второе неравенство в (2.1.2) из определения 2.1.2 и свойства (2.3.2)-(2.3.3) означают, что

$$(1-\varepsilon)\binom{t}{s}\le\sum_{\boldsymbol{u}\in\{0,1\}^N}|\mathbf{G}_L(s,\boldsymbol{u},X)|\le\binom{s+L-1}{s}2^N,\quad t=\left\lfloor 2^{RN}\right\rfloor. \tag{2.3.4}$$

Сравнение левой и правой части (2.3.4) приводит к нижней асимптотической ($N\to\infty$) границе для ошибки (2.1.3) почти дизъюнктивных СД s_L-кодов:

$$\varepsilon_L(s,R,N)\ge 1-\binom{s+L-1}{s}2^N\binom{t}{s}^{-1}=1-2^{-N[(sR-1)+o(1)]},\quad N\to\infty. \tag{2.3.5}$$

Из неравенства (2.3.5) и определения (2.1.4) следует, что неравенство $R<1/s$ является необходимым условием положительности экспоненты ошибки $\mathbf{E}_L(s,R)$ как функции параметра R. Поэтому из определения (2.1.5) вытекает, что пропускная способность $C_L(s)\le 1/s$. $\square$

Замечание 1. Задача улучшения границы теоремы 2.3.1 остается открытой. Отметим, что верхняя граница для $R_L(s)$, сформулированная в теореме 1.3.2 и доказанная в [44], показывает, что для скорости СД s_L-кодов улучшение верхней границы $R_L(s)\le 1/s$ возможно.

Глава 3

Пороговое декодирование в дизъюнктивной модели канала множественного доступа

В данной главе будет рассматриваться модель дизъюнктивного канала множественного доступа, в которой неизвестно число отправителей сообщений. Исследуемая задача сравнения количества отправителей с заданным порогом будет описана применительно к групповому тестированию. Для эффективного решения этой задачи будет введено понятие порогового декодирования отклика канала множественного доступа. Для такого декодирования будет доказана нижняя граница для экспоненты ошибки, где под ошибкой подразумевается вероятность получения неправильного ответа при сравнении количества отправителей с порогом. В последнем разделе будут приведены результаты компьютерного моделирования решения рассматриваемой задачи.

3.1 Основные определения

Будем пользоваться обозначениями и определениями, введенными в главе 1 настоящей диссертации.

Электронную схему из t элементов будем называть *s-активной*, $s \ll t$, если она содержит не более s *дефектных* элементов. В противном случае схема не может работать правильно и подлежит замене на новую аналогичную s-активную схему. Для проверки s-активности схемы проводится N *неадаптивных групповых тестов*. Как обычно, под групповым тестом подразумевается некоторое подмножество элементов, а результат теста равен 1, если хотя бы один дефектный элемент попал в тестируемое множество, и 0 – иначе. Неадаптивная процедура группового тестирования предполагает, что все тесты построены изначально и могут проводиться одновременно. Мы не рассматриваем формирование новых тестов на основании результатов предыдущих, так как это требует большего времени на проверку s-активности и может привести к длительным сбоям в работе электронной схемы. Подобные системы технической диагностики электронных схем, основанные на неадаптивном групповом тестировании, строились в работе [5].

Будем представлять N неадаптивных групповых тестов в виде двоичной $(N \times t)$-матрицы $X = \|x_i(j)\|$, в которой строка $\boldsymbol{x}_i$ соответствует i-ому тесту, а столбец $\boldsymbol{x}(j)$ – j-ому элементу, причем $x_i(j) \triangleq 1$ тогда и только тогда, когда j-й элемент входит в i-е тестируемое множество. Для произвольного кода X и множества $\mathcal{S} \subset [t]$, двоичный столбец

длины N

$$\boldsymbol{x}(\mathcal{S}) \triangleq \bigvee_{j\in\mathcal{S}} \boldsymbol{x}(j), \quad \text{если} \quad \mathcal{S}\neq\emptyset \quad \text{и} \quad \boldsymbol{x}(\mathcal{S}) \triangleq (0,0,\ldots,0), \quad \text{если} \quad \mathcal{S}=\emptyset,$$

будем называть *откликом*. Таким образом, после проведения групповых тестов получим отклик для множества дефектных элементов.

Определение 1.1.1 СД s_1-кода является важным достаточным условием для поиска всех дефектных элементов $\mathcal{S}\subset[t]$ в предположении $|\mathcal{S}|\leq s$. Алгоритм нахождения дефектов в таком случае заключается в отыскании всех кодовых слов кода X, покрываемых откликом $\boldsymbol{x}(\mathcal{S})$, и называется *пофакторным декодированием* отклика. Заметим, что для СД s_1-кода X данный алгоритм также позволяет проверять s-активность электронной схемы. Действительно, если $|\mathcal{S}|\leq s$, то после пофакторного декодирования получим множество $\mathcal{S}$ объема $\leq s$. Если же количество дефектов превышает s, то получаемое после декодирования множество имеет объем $> s$. Кроме того, рассуждениями от противного нетрудно заключить, что произвольный код X, для которого существует возможность проверить s-активность схемы без ошибок, является СД s_1-кодом. Если код X не является СД s_1-кодом, то существуют множество $\mathcal{S}\subset[t]$, $|\mathcal{S}|=s$, и индекс $j\in[t]\setminus\mathcal{S}$, такие что

$$\boldsymbol{x}(\mathcal{S}) = \boldsymbol{x}(\mathcal{S}\bigcup\{j\}),$$

т.е. пофакторное декодирование не сможет отличить множество потенциальных дефектов $\mathcal{S}$ объема $\leq s$ от множества потенциальных дефектов $\mathcal{S}\bigcup\{j\}$ объема $> s$.

Предложение 3.1.1. *Результаты неадаптивных групповых тестов, заданных кодом X, позволяют определить s-активность электронной схемы в том и только том случае, если код X является СД s_1-кодом.*

Далее рассмотрим вероятностную постановку задачи, в которой разрешена незначительная ошибка при определении s-активности схемы. Пусть совокупность из t элементов содержит неизвестное подмножество дефектных элементов $\mathcal{S}_{un}$, $\mathcal{S}_{un}\subset[t]$, неизвестного объема $|\mathcal{S}_{un}|$, и X – произвольный двоичный код (1.1.1) длины N и объема t. Введем *нулевую гипотезу* $\{H_0 : |\mathcal{S}_{un}|\leq s\}$ (схема s-активна) и *альтернативную гипотезу* $\{H_1 : |\mathcal{S}_{un}|\geq s+1\}$ (схема не s-активна). Результаты данной главы связаны с проверкой гипотезы H_0 против альтернативы H_1.

Мы будем полагать, что все различные подмножества дефектных элементов одинакового объема равновероятны, другими словами, *распределение вероятностей* случайного множества $\mathcal{S}_{un}$, $\mathcal{S}_{un}\subset[t]$, задано фиксированным вектором (параметром распределения) $\boldsymbol{p}\triangleq(p_0,p_1,\ldots,p_t)$, $p_k\geq 0$, $k=0,1,\ldots,t$, $\sum_{k=0}^{t}p_k=1$, таким образом:

$$\Pr\{\mathcal{S}_{un}=\mathcal{S}\} \triangleq \frac{p_{|\mathcal{S}|}}{\binom{t}{|S|}} \quad \text{для любого подмножества} \quad \mathcal{S}\subseteq[t]. \tag{3.1.1}$$

Для фиксированных параметров s, $1\leq s<t$, и T, $1\leq T<N$, рассмотрим *пороговый критерий*:

$$\begin{cases} \text{принять } \{H_0 : |\mathcal{S}_{un}|\leq s\}, & \text{если } |\boldsymbol{x}(\mathcal{S}_{un})|\leq T, \\ \text{принять } \{H_1 : |\mathcal{S}_{un}|\geq s+1\}, & \text{если } |\boldsymbol{x}(\mathcal{S}_{un})|\geq T+1. \end{cases} \tag{3.1.2}$$

Алгоритм, по которому каждый отклик $\boldsymbol{x}(\mathcal{S}_{un})$ сопоставляется одной из гипотез H_0 или H_1 согласно критерию (3.1.2), будет также называть *пороговым декодированием*. Далее, введем *максимальную вероятность ошибки* порогового критерия (3.1.2) :

$$\varepsilon_s(T,\boldsymbol{p},X) \triangleq \max\left\{\Pr\{\text{принять } H_1\big|H_0\}\,,\,\Pr\{\text{принять } H_0\big|H_1\}\right\}. \tag{3.1.3}$$

Условные вероятности в правой части (3.1.3) однозначно определяются по (3.1.1)-(3.1.2).

Определение 3.1.1. Зафиксируем параметры τ, $0 < \tau < 1$, и R, $R > 0$. Для максимальной вероятности ошибки $\varepsilon_s(T, \boldsymbol{p}, X)$, определенной (3.1.1)-(3.1.3), рассмотрим функцию

$$\varepsilon_s^N(\tau, R) \triangleq \max_{\boldsymbol{p}} \left\{ \min_X \varepsilon_s(\lfloor \tau N \rfloor, \boldsymbol{p}, X) \right\}, \tag{3.1.4}$$

где минимум берется по всем кодам X длины N и объема $t = \lfloor 2^{RN} \rfloor$. Величина $\varepsilon_s^N(\tau, R) \geq 0$ не зависит от параметра распределения $\boldsymbol{p}$ и может интерпретироваться как *универсальная* вероятность ошибки критерия (3.1.2). Соответствующая *экспонента ошибки*

$$\mathbf{E}_s(\tau, R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \varepsilon_s^N(\tau, R)}{N}, \quad s \geq 1, \quad 0 < \tau < 1, \quad R > 0, \tag{3.1.5}$$

задает максимальную вероятность ошибок первого и второго рода для критерия (3.1.2):

$$\exp_2\{-N\left[\mathbf{E}_s(\tau, R) + o(1)\right]\}, \quad N \to \infty, \quad \text{если} \quad \mathbf{E}_s(\tau, R) > 0.$$

Также будем рассматривать *дизъюнктивный критерий*, основанный на традиционном пофакторном декодировании:

$$\begin{cases} \text{принять } H_0, & \text{если } \boldsymbol{x}(\mathcal{S}_{un}) \text{ покрывает} \leq s \text{ кодовых слов кода } X, \\ \text{принять } H_1, & \text{если } \boldsymbol{x}(\mathcal{S}_{un}) \text{ покрывает} \geq s+1 \text{ кодовых слов кода } X. \end{cases} \tag{3.1.6}$$

Для фиксированного параметра R, $R > 0$, экспонента ошибки дизъюнктивного критерия (3.1.6) $\mathbf{E}_s(R)$ определяется по аналогии с (3.1.3)-(3.1.5). А именно, вводим

$$\varepsilon_s(\boldsymbol{p}, X) \triangleq \max\left\{ \Pr\{\text{принять } H_1 \big| H_0\}, \Pr\{\text{принять } H_0 \big| H_1\} \right\}, \tag{3.1.7}$$

$$\varepsilon_s^N(R) \triangleq \max_{\boldsymbol{p}} \left\{ \min_{X\,:\,t=\lfloor RN \rfloor} \varepsilon_s(\boldsymbol{p}, X) \right\}, \tag{3.1.8}$$

$$\mathbf{E}_s(R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \varepsilon_s^N(R)}{N}, \quad s \geq 1, \quad R > 0. \tag{3.1.9}$$

Предложение 3.1.2. *Определение* (3.1.7)-(3.1.9) *экспоненты ошибки* $\mathbf{E}_s(R)$ *эквивалентно определению 2.1.3 экспоненты ошибки* $\mathbf{E}_1(s, R)$.

Доказательство предложения 3.1.2. Для начала заметим, что для критерия (3.1.6) вероятность $\Pr\{\text{принять } H_0 \big| H_1\} = 0$. Для фиксированного кода X и параметра s введем семейства $B_k(X)$, $k = 0, 1, \ldots, s$, подмножеств $\mathcal{S}$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = k$, следующим образом:

$$B_k(X) \triangleq \{\, \mathcal{S} \,:\, \mathcal{S} \subset [t],\ |\mathcal{S}| = k,\ \exists\, j \in [t] \setminus \mathcal{S},\ \boldsymbol{x}(\mathcal{S}) \succeq \boldsymbol{x}(j) \}, \tag{3.1.10}$$

Тогда вероятность (3.1.7) представима в виде

$$\varepsilon_s(\boldsymbol{p}, X) \triangleq \max \sum_{k=0}^{s} \frac{p_k}{\sum\limits_{l=0}^{s} p_l} \frac{|B_k(X)|}{\binom{t}{k}}, \tag{3.1.11}$$

Нетрудно проверить, что для множеств (3.1.10) и любого целого числа k, $0 \leq k < s$, справедливо неравенство:

$$|B_{k+1}(X)| \geq \frac{t-k}{k+1} |B_k(X)|$$

Следовательно, из представления (3.1.11) вытекает, что максимум $\max_{\boldsymbol{p}} \varepsilon_s(\boldsymbol{p}, X)$ принимается при таком $\boldsymbol{p} = (p_0, p_1, \ldots, p_t)$, что $p_s = 1$ и $p_j = 0$, $j \neq s$. Таким образом, определение (3.1.8) ошибки $\varepsilon_s^N(R)$ эквивалентно определению (2.1.3) ошибки $\varepsilon_1(s, R, N)$. $\square$

3.2 Проверка гипотез о количестве отправителей

Нижняя граница для экспоненты ошибки $\mathbf{E}_s(R)$ сформулирована в теореме 2.2.2. Кроме того, из предложения 3.1.2 и теоремы 2.3.1 следует, что при $R \geq 1/s$ экспонента $\mathbf{E}_s(R) = 0$. В следующей теореме представлена нижняя граница для экспоненты ошибки $\mathbf{E}_s(\tau, R)$, которая, в частности, устанавливает, что при $N \to \infty$ и больших значениях скорости кодов R, пороговый критерий (3.1.2) имеет преимущество перед дизъюнктивным критерием (3.1.6). Данная граница получена с помощью метода случайного кодирования на ансамбле равновесных двоичных кодов. Параметр Q в формулировках теоремы 3.2.1 имеет смысл относительного веса кодовых слов. Также в формулировке используются обозначение функции $\mathcal{A}(s, Q, q)$, определенной (2.2.6)-(2.2.7) в разделе 2.2.

Теорема 3.2.1 (Нижняя граница для $\mathbf{E}_s(\tau, R)$)**.** *Справедливы два утверждения.*
1. *Экспонента ошибки порогового критерия удовлетворяет неравенству* $\mathbf{E}_s(\tau, R) \geq \underline{\mathbf{E}}_s(\tau)$ *где функция* $\underline{\mathbf{E}}_s(\tau)$ *не зависит от параметра* R *и определяется как*

$$\underline{\mathbf{E}}_s(\tau) \triangleq \max_{1-(1-\tau)^{1/(s+1)} < Q < 1-(1-\tau)^{1/s}} \min\left\{\mathcal{A}'(s, Q, \tau), \mathcal{A}(s+1, Q, \tau)\right\} > 0, \tag{3.2.1}$$

$$\mathcal{A}'(s, Q, \tau) \triangleq \begin{cases} \mathcal{A}(s, Q, \tau), & \text{если } Q \leq \tau \leq sQ, \\ \infty, & \text{иначе,} \end{cases} \tag{3.2.2}$$

а функция $\mathcal{A}(s, Q, \tau)$ *задана* (2.2.6)-(2.2.7).
2. *При* $s \to \infty$ *оптимальное значение* $\underline{\mathbf{E}}_s(\tau)$ *удовлетворяет неравенству:*

$$\underline{\mathbf{E}}_{\mathrm{Thr}}(s) \triangleq \max_{0<\tau<1} \underline{\mathbf{E}}_s(\tau) \geq \frac{\log_2 e}{4s^2}(1 + o(1)), \quad s \to \infty.$$

Для рассматриваемой задачи проверки гипотез параметр T порогового критерия (3.1.2) может быть оптимизирован для получения минимальной вероятности ошибки. Численные значения оптимальной экспоненты ошибки $\underline{\mathbf{E}}_{\mathrm{Thr}}(s)$, а также соответствующий оптимальный параметр порога $\tau = \tau(s)$ и оптимальный параметр ансамбля равновесных кодов $Q = Q(s)$, представлены в таблице 3.2.1. Таблица 3.2.1 также содержит величины $\underline{\mathbf{E}}_s(0) \triangleq \lim_{R\to 0} \underline{\mathbf{E}}_s(R)$ и $R_{\mathrm{Thr}}(s) \triangleq \sup\{R : \underline{\mathbf{E}}_s(R) > \underline{\mathbf{E}}_{\mathrm{Thr}}(s)\}$.

Таблица 3.2.1: Численные значения $\underline{\mathbf{E}}_{\mathrm{Thr}}(s)$ и $R_{\mathrm{Thr}}(s)$

s	2	3	4	5	6	7	8
$\underline{\mathbf{E}}_{\mathrm{Thr}}(s)$	0.1380	0.0570	0.0311	0.0196	0.0135	0.0098	0.0075
$\tau(s)$	0.2065	0.1365	0.1021	0.0816	0.0679	0.0582	0.0509
$Q(s)$	0.1033	0.0455	0.0255	0.0163	0.0113	0.0083	0.0064
$\underline{\mathbf{E}}_s(0)$	0.3651	0.2362	0.1754	0.1397	0.1161	0.0994	0.0869
$R_{\mathrm{Thr}}(s)$	0.2271	0.1792	0.1443	0.1201	0.1027	0.0896	0.0794

Доказательство теоремы 3.2.1

Доказательство утверждения 1. Для фиксированного кода X, параметров s и T определим семейства $B_k^i(T, X)$, $i = 1, 2$, $k = 0, 1, \ldots, t$, подмножеств $\mathcal{S}$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = k$,

следующим образом:

$$\begin{aligned} B_k^1(T,X) &\triangleq \{\,\mathcal{S} : \mathcal{S}\subset[t],\ |\mathcal{S}|=k,\ |\boldsymbol{x}(\mathcal{S})|\geq T+1\}\,,\\ B_k^2(T,X) &\triangleq \{\,\mathcal{S} : \mathcal{S}\subset[t],\ |\mathcal{S}|=k,\ |\boldsymbol{x}(\mathcal{S})|\leq T\}\,. \end{aligned} \tag{3.2.3}$$

Тогда вероятность (3.1.3) представима в виде

$$\varepsilon_s(T,\boldsymbol{p},X)\triangleq\max\left\{\sum_{k=0}^{s}\frac{p_k}{\sum\limits_{l=0}^{s}p_l}\frac{|B_k^1(T,X)|}{\binom{t}{k}},\sum_{k=s+1}^{t}\frac{p_k}{\sum\limits_{l=s+1}^{t}p_l}\frac{|B_k^2(T,X)|}{\binom{t}{k}}\right\}, \tag{3.2.4}$$

Нетрудно проверить, что для множеств (3.2.3) и любого целого числа k, $0\leq k<t$, справедливы неравенства:

$$|B_{k+1}^1(T,X)|\geq\frac{t-k}{k+1}|B_k^1(T,X)|\quad\text{и}\quad|B_k^2(T,X)|\geq\frac{k+1}{t-k}|B_{k+1}^2(T,X)|$$

Следовательно, из представления (3.2.4) вытекает, что максимум $\max_{\boldsymbol{p}}\varepsilon_s(T,\boldsymbol{p},X)$ принимается при таком $\boldsymbol{p}=(p_0,p_1,\ldots,p_t)$, что $p_s=p_{s+1}=1/2$ и $p_j=0$, $j\notin\{s,s+1\}$. Таким образом, определение (3.1.4) универсальной ошибки $\varepsilon_s^N(\tau,R)$ порогового критерия эквивалентно следующему:

$$\varepsilon_s^N(\tau,R)\triangleq\min_{X:\,t=\lfloor2^{RN}\rfloor}\varepsilon_s(\lfloor\tau N\rfloor,X),\quad R>0,\quad\text{где} \tag{3.2.5}$$

$$\varepsilon_s(T,X)\triangleq\max\left\{\frac{|B_s^1(T,X)|}{\binom{t}{s}},\frac{\left|B_{s+1}^2(T,X)\right|}{\binom{t}{s+1}}\right\}. \tag{3.2.6}$$

Зафиксируем параметры $s\geq2$, $0<\tau<1$, $R>0$ и Q, $0<Q<1$. Нижнюю границу (3.2.1) будем выводить методом случайного кодирования на ансамбле равновесных кодов [26], который определим как ансамбль $E(N,t,Q)$ двоичных кодов X длины N и объема $t=\lfloor2^{RN}\rfloor$, для которого кодовые слова выбираются независимо и равновероятно из множества всех $\binom{N}{\lfloor QN\rfloor}$ кодовых слов веса $\lfloor QN\rfloor$.

Для ансамбля $E(N,t,Q)$ обозначим математическое ожидание вероятности (3.2.6) через

$$\mathcal{E}_s^N(\tau,Q,R)\triangleq\mathbb{E}\Big[\varepsilon_s(\lfloor\tau N\rfloor,X)\Big]. \tag{3.2.7}$$

Заметим, что существует такой код X длины N и объема $t=\lfloor2^{RN}\rfloor$, что его максимальная вероятность ошибки (3.2.6) ограничена сверху значением $\mathcal{E}_s^N(\tau,Q,R)$, и в силу определения (3.2.5) справедлива следующая нижняя граница для экспоненты ошибки (3.1.5) порогового критерия (3.1.2):

$$\mathbf{E}_s(\tau,R)\geq\max_{0<Q<1}\lim_{N\to\infty}\frac{-\log_2\mathcal{E}_s^N(\tau,Q,R)}{N}. \tag{3.2.8}$$

Далее мы покажем, что предел в правой части (3.2.8) существует и его максимум по Q, $0<Q<1$ совпадает с (3.2.1).

Выразим объем множества $B_s^1(\lfloor\tau N\rfloor,X)$ через сумму индикаторных функций:

$$\left|B_s^1(\lfloor\tau N\rfloor,X)\right|=\sum_{\mathcal{S}\in[t],\,|S|=s}\mathbb{1}\big\{\mathcal{S}\in B_s^1(\lfloor\tau N\rfloor,X)\big\}.$$

Из такого представления нетрудно заключить, что математическое ожидание величины $|B_s^1(\lfloor \tau N \rfloor, X)|$ (и, аналогично, $\left|B_{s+1}^2(\lfloor \tau N \rfloor, X)\right|$) равно

$$\begin{gathered}\mathbb{E}\Big[\,\big|B_s^1(\lfloor \tau N \rfloor, X)\big|\,\Big] = \binom{t}{s} \Pr\big\{\mathcal{S} \in B_s^1(\lfloor \tau N \rfloor, X)\big\} \\ \left(\mathbb{E}\Big[\,\big|B_{s+1}^2(\lfloor \tau N \rfloor, X)\big|\,\Big] = \binom{t}{s+1} \Pr\big\{\mathcal{S} \in B_{s+1}^2(\lfloor \tau N \rfloor, X)\big\}\right).\end{gathered} \tag{3.2.9}$$

Для ансамбля $E(N,t,Q)$ через $P_s^1(\tau,Q,N)$ и $P_{s+1}^2(\tau,Q,N)$, соответственно, обозначим вероятности $\Pr\big\{\mathcal{S} \in B_s^1(\lfloor \tau N \rfloor, X)\big\}$ и $\Pr\big\{\mathcal{S} \in B_{s+1}^2(\lfloor \tau N \rfloor, X)\big\}$. Очевидно, что эти вероятности зависят только от s, τ, Q, N и не зависят от R. Из формул (3.2.9) вытекает, что математическое ожидание (3.2.7) удовлетворяет неравенствам:

$$\max\big\{P_s^1(\tau,Q,N), P_{s+1}^2(\tau,Q,N)\big\} \le \mathcal{E}_s^N(\tau,Q,R) \le P_s^1(\tau,Q,N) + P_{s+1}^2(\tau,Q,N). \tag{3.2.10}$$

Для ансамбля $E(N,t,Q)$, фиксированного множества $\mathcal{S} \subset [t]$, $|\mathcal{S}| = k$, объема k и фиксированного целого w рассмотрим вероятность

$$P_k^N(Q,w) \triangleq \Pr\left\{\left|\bigvee_{j\in\mathcal{S}} \boldsymbol{x}(j)\right| = w\right\}.$$

Заметим, что данная вероятность $P_k^N(Q,w)$ не зависит от выбора множества $\mathcal{S}$, а зависит только от параметров k, w, N и Q. Чтобы вычислить логарифмические асимптотики вероятностей в (3.2.10), представим их в следующем виде:

$$\begin{aligned} P_s^1(\tau,Q,N) &= \sum_{w=\lfloor \max\{\tau,Q\}N \rfloor+1}^{\min\{N,s\lfloor QN \rfloor\}} P_s^N(Q,w), \\ P_{s+1}^2(\tau,Q,N) &= \sum_{w=\lfloor QN \rfloor}^{\min\{\lfloor \tau N \rfloor,(s+1)\lfloor QN \rfloor\}} P_{s+1}^N(Q,w). \end{aligned} \tag{3.2.11}$$

Логарифмическая асимптотика вероятности $P_k^N(Q,w)$ уже вычислена в лемме 2.2.1, и равна

$$\lim_{N\to\infty} \frac{-\log_2 P_k^N(Q,\lfloor qN \rfloor)}{N} = \mathcal{A}(k,Q,q), \tag{3.2.12}$$

где функция $\mathcal{A}(k,Q,q)$ задана (2.2.6)-(2.2.7). Заметим, что $P_s^1(\tau,Q,N) = 0$, если $\tau > sQ$, и $P_{s+1}^2(\tau,Q,N) = 0$, если $\tau < Q$. Из данного замечания, а также (3.2.11) и (3.2.12), заключаем, что

$$\begin{aligned} \lim_{N\to\infty} \frac{-\log_2 P_s^1(\tau,Q,N)}{N} &= \min_{\max\{\tau,Q\}\le q\le 1} \mathcal{A}'(s,Q,q), \\ \lim_{N\to\infty} \frac{-\log_2 P_{s+1}^2(\tau,Q,N)}{N} &= \min_{0\le q\le \min\{\tau,(s+1)Q\}} \mathcal{A}'(s+1,Q,q), \end{aligned} \tag{3.2.13}$$

где функция $\mathcal{A}'(k,Q,q)$ определена с помощью (3.2.2).

Следовательно, (3.2.10) и (3.2.13) влекут существование предела

$$\lim_{N\to\infty} \frac{-\log_2 \mathcal{E}_s^N(\tau,Q,R)}{N} = \min\left\{\min_{\max\{\tau,Q\}\le q\le 1} \mathcal{A}'(s,Q,q), \min_{0\le q\le \min\{\tau,(s+1)Q\}} \mathcal{A}'(s+1,Q,q)\right\}. \tag{3.2.14}$$

Из аналитических свойств функции $\mathcal{A}(k,Q,q)$, сформулированных в лемме 2.2.1 вытекает справедливость утверждений

$$\min_{\max\{\tau,Q\}\le q\le 1} \mathcal{A}'(s,Q,q) = 0, \qquad \text{если } \tau \le 1-(1-Q)^s,$$
$$\min_{0\le q\le \min\{\tau,(s+1)Q\}} \mathcal{A}'(s+1,Q,q) = 0, \qquad \text{если } \tau \ge 1-(1-Q)^{s+1},$$

что, наконец, устанавливает эквивалентность нижней границы (3.2.8)-(3.2.14) и нижней границы (3.2.1) в формулировке теоремы 3.2.1. Утверждение 1 доказано.

Доказательство утверждения 2. Для доказательства утверждения 2 необходимо привести нижнюю границу на асимптотику при $s\to\infty$ выражения

$$\underline{\mathbf{E}}_{\mathrm{Thr}}(s) \triangleq \max_{0<\tau<1} \max_{1-(1-\tau)^{1/(s+1)}<Q<1-(1-\tau)^{1/s}} \min\left\{\mathcal{A}'(s,Q,\tau), \mathcal{A}(s+1,Q,\tau)\right\}. \tag{3.2.15}$$

Для произвольных фиксированных τ, $0<\tau<1$, и Q, $1-(1-\tau)^{1/(s+1)} < Q < 1-(1-\tau)^{1/s}$, обозначим через $y_1(Q,\tau)$ и $y_2(Q,\tau)$ корни уравнений (2.2.7), соответствующих функциям $\mathcal{A}(s,Q,\tau)$ и $\mathcal{A}(s+1,Q,\tau)$. Заметим, что значение y_1 может превышать 1. Из (2.2.7) следует, что параметр τ можно выразить двумя способами:

$$\tau = Q\frac{1-y_1^s}{1-y_1} = Q\frac{1-y_2^{s+1}}{1-y_2}.$$

Поэтому неравенство $1-(1-\tau)^{1/(s+1)} < Q \Leftrightarrow \tau < 1-(1-Q)^{s+1}$ эквивалентно неравенству

$$\frac{1-y_2^{s+1}}{1-y_2} < \frac{1-(1-Q)^{s+1}}{1-(1-Q)}.$$

Отметим, что для любого целого $n\ge 2$ функция $f(x) = \frac{1-x^n}{1-x}$ возрастает на интервале $x\in(0,+\infty)$, поэтому

$$1-(1-\tau)^{1/(s+1)} < Q \quad \Leftrightarrow \quad Q < 1-y_2,$$
и аналогично
$$Q < 1-(1-\tau)^{1/s} \quad \Leftrightarrow \quad Q > 1-y_1.$$

Добавим, что пара параметров (y_1,Q), $y_1>0$, $0<Q<1$, однозначно определяет значения параметров τ и y_2. Кроме того, если выполнены неравенства

$$0<\tau<1, \quad Q<1-y_2, \quad Q>1-y_1, \tag{3.2.16}$$

то параметры τ и Q лежат в той же области, в которой происходит поиск максимума в (3.2.15). Приведенные выше рассуждения позволяют в формуле (3.2.15) перейти от максимизации по (τ,Q) к максимизации по (y_1,Q).

Зафиксируем некоторую константу $c>0$. Пусть $s\to\infty$ и $y_1 \triangleq 1-c/s^2+o(1/s^3)$. Тогда асимптотика выражения τ/Q равна

$$\frac{1-y_2^{s+1}}{1-y_2} = \frac{\tau}{Q} = \frac{1-y_1^s}{1-y_1} = s-\frac{c}{2}+o(1),$$

и, следовательно,

$$y_2 = 1-\frac{c+2}{(s+1)^2}+o\left(\frac{1}{s^3}\right) = 1-\frac{c+2}{s^2}+\frac{2}{s^3}+o\left(\frac{1}{s^3}\right).$$

Необходимым условием для выполнения неравенств (3.2.16) является попадание значения параметра Q в интервал

$$\frac{c}{s^2}+o\left(\frac{1}{s^3}\right)=1-y_1<Q<1-y_2=\frac{c+2}{s^2}-\frac{2}{s^3}+o\left(\frac{1}{s^3}\right).$$

Зададим теперь параметр Q в виде $Q\triangleq d/s^2$, где d, $c<d<c+2$, – некоторая положительная константа. Очевидно, что для достаточно больших значений s параметр Q удовлетворяет предыдущему двустороннему неравенству.

Резюмируя выбор параметров y_1 и Q, приведем список выполненных асимптотических равенств:

$$\begin{aligned}
\tau &= \frac{d}{s}-\frac{cd}{2s^2}+o\left(\frac{1}{s^2}\right),\\
Q &= \frac{d}{s^2},\\
y_1 &= 1-\frac{c}{s^2}+o\left(\frac{1}{s^2}\right),\\
y_2 &= 1-\frac{c+2}{s^2}+o\left(\frac{1}{s^2}\right), \quad s\to\infty,
\end{aligned} \tag{3.2.17}$$

где c и d – произвольные действительные числа с соотношениями $c>0$, $c<d<c+2$. Параметры, определенные (3.2.17), удовлетворяют неравенствам (3.2.16), следовательно, подстановка асимптотик (3.2.17) в выражение (3.2.15) приведет к некоторой нижней границе на $\underline{\mathbf{E}}_{\mathrm{Thr}}(s)$.

Для начала вычислим асимптотику при $s\to\infty$ выражения

$$\frac{\mathcal{A}(s,Q,\tau)}{\log_2 e}=(1-\tau)\ln(1-\tau)+(sQ-\tau)\ln\left[\frac{1-y_1}{Q}\right]+s(\tau-Q)\ln y_1-s(1-Q)\ln(1-Q).$$

Выпишем разложения слагаемых в ряд Тейлора с точностью до $o(1/s^2)$:

$$\begin{aligned}
(1-\tau)\ln_2(1-\tau) &= -\frac{d}{s}+\frac{cd}{2s^2}+\frac{d^2}{2s^2}+o\left(\frac{1}{s^2}\right),\\
(sQ-\tau)\ln\left[\frac{1-y_1}{Q}\right] &= \frac{cd}{2s^2}\ln\left[\frac{c}{d}\right]+o\left(\frac{1}{s^2}\right),\\
s(\tau-Q)\ln y_1 &= -\frac{cd}{s^2}+o\left(\frac{1}{s^2}\right),\\
s(1-Q)\ln(1-Q) &= \frac{d}{s}+o\left(\frac{1}{s^2}\right).
\end{aligned}$$

Следовательно,

$$\frac{\mathcal{A}(s,Q,\tau)}{\log_2 e}=\frac{d(d-c+c\ln[c/d])}{2s^2}+o\left(\frac{1}{s^2}\right).$$

Теперь вычислим асимптотику выражения

$$\begin{aligned}
\frac{\mathcal{A}(s+1,Q,\tau)}{\log_2 e} &= (1-\tau)\ln(1-\tau)+(sQ-\tau)\ln\left[\frac{1-y_2}{Q}\right]+s(\tau-Q)\ln y_2-s(1-Q)\ln(1-Q)\\
&\quad+Q\ln\left[\frac{1-y_2}{Q}\right]+(\tau-Q)\ln y_2-(1-Q)\ln(1-Q).
\end{aligned}$$

Разложения новых слагаемых в ряд Тейлора с точностью до $o(1/s^2)$ представлены ниже:

$$(sQ-\tau)\ln\left[\frac{1-y_2}{Q}\right]=\frac{cd}{2s^2}\ln\left[\frac{c+2}{d}\right]+o\left(\frac{1}{s^2}\right),$$
$$s(\tau-Q)\ln y_2=-\frac{(c+2)d}{s^2}+o\left(\frac{1}{s^2}\right),$$
$$Q\ln\left[\frac{1-y_2}{Q}\right]=\frac{d}{s^2}\ln\left[\frac{c+2}{d}\right]+o\left(\frac{1}{s^2}\right),$$
$$(\tau-Q)\ln y_2=o\left(\frac{1}{s^2}\right).$$

Откуда следует, что

$$\frac{\mathcal{A}(s+1,Q,\tau)}{\log_2 e}=\frac{d(d-c-2+(c+2)\ln[(c+2)/d])}{2s^2}+o\left(\frac{1}{s^2}\right).$$

Наконец, максимум выражения

$$\max_{c>0}\max_{c<d<c+2}\min\left\{d\left(d-c+c\ln\left[\frac{c}{d}\right]\right),d\left(d-c-2+(c+2)\ln\left[\frac{c+2}{d}\right]\right)\right\}.$$

ограничен снизу значением $\frac{1}{2}$, которое принимается при $c\to\infty$ и $d=c+1$. Утверждение 2 доказано. $\square$

3.3 Моделирование кодов конечных длины и объема

Для некоторых конечных параметров s, N и t, проведено компьютерное моделирование следующим образом. Параметр $\boldsymbol{p}$ распределения вероятностей (3.1.1) определен по формуле

$$p_s=p_{s+1}=1/2,\quad p_j=0, j\notin\{s,s+1\},$$

т.е. распределение выбрано таким образом, чтобы принимался максимум в правых частях (3.1.4) и (3.1.8). Код X случайным образом выбирается из семейства равновесных кодов, а именно для некоторого фиксированного веса w каждое кодовое слово кода X выбирается независимо и равновероятно из множества всех $\binom{N}{w}$ кодовых слов длины N и веса w. Для каждого возможного веса w и обоих критериев была произведена генерация кода 1000 раз, и выбран код с наилучшей максимальной вероятностью ошибки. Заметим, что для дизъюнктивного критерия (3.1.6) выполнено $\Pr\{\text{принять } H_0|H_1\}=0$. В таблице 3.3.1 представлены параметры наилучших найденных кодов для каждого критерия, наилучшие значения максимальной вероятности ошибки для фиксированных параметров s, t и N выделены жирным шрифтом.

Таблица 3.3.1: Результаты моделирования

	Пороговый критерий				Дизъюнктивный критерий	
N	Pr{пр. $H_1 \mid H_0$}	Pr{пр. $H_0 \mid H_1$}	w	T	Pr{пр. $H_1 \mid H_0$}	w
			$s = 2, \quad t = 15$			
5	0.2571	**0.2571**	2	3	0.9333	2
8	**0.1619**	0.1604	3	5	0.7048	2
10	0	**0.1429**	1	2	0.4571	3
12	0	**0.0857**	1	2	0.1810	3
14	0	**0.0571**	1	2	0.0952	3
15	0	0.0462	2	4	**0.0286**	3
			$s = 2, \quad t = 20$			
5	**0.2632**	0.2588	2	3	0.9579	2
8	0.1632	**0.1649**	3	5	0.8316	2
11	0.1053	**0.1509**	4	7	0.5158	3
12	**0.1158**	0.1123	4	7	0.4158	3
14	0	**0.0842**	2	4	0.2316	3
15	0	**0.0693**	2	4	0.1526	4

Глава 4

Гиперкоды со списочным декодированием

В данной главе будет введено определение гиперкодов со списочным декодированием. Различными методами будут доказаны две новые нижние границы для асимптотической скорости гиперкодов со списочным декодированием, а также будет установлена новая верхняя граница для этой скорости. В четвертом разделе будет проведен детальный анализ существующих нижних и верхних границ для асимптотической скорости гиперкодов со списочным декодированием и будет дана сводная таблица наилучших значений границ для некоторых наборов параметров. В последнем разделе будет описано важное приложение гиперкодов (и дизъюнктивных кодов) со списочным декодированием, связанное с кодированием недоопределенных данных. Это приложение будет обобщено на общий случай с объемом списка $L > 1$.

4.1 Основные определения

Будем пользоваться обозначениями и определениями, введенными в главе 1 настоящей диссертации. Пусть q, $q \geq 2$, – целое число. Через $\mathcal{A}_q \triangleq \{0, 1, \ldots, q-1\}$ обозначим стандартный q-ичный алфавит, и, обобщая определение (1.1.1), введем q-ичную $(N \times t)$-матрицу

$$X_q \triangleq \|x_i(j)\|, \quad x_i(j) \in \mathcal{A}_q, \quad \boldsymbol{x}_i \triangleq (x_i(1), \ldots, x_i(t)), \quad \boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j)), \qquad (4.1.1)$$

$i \in [N]$, $j \in [t]$, с N строками $\boldsymbol{x}_i$, $\boldsymbol{x}_i \in \mathcal{A}_q^t$, $i \in [N]$, и t столбцами (кодовыми словами) $\boldsymbol{x}(j)$, $\boldsymbol{x}(j) \in \mathcal{A}_q^N$, $j \in [t]$, которую назовем *q-ичным кодом длины N и объема t*.

Вектор $\mathcal{Q} = (\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_N)$, $\mathcal{Q}_i \subseteq \mathcal{A}_q$ из N подмножеств алфавита $\mathcal{A}_q$ будем называть *гиперсловом* [1]. *Гиперсуммой* s q-ичных кодовых слов $\boldsymbol{x}(j_k)$, $\boldsymbol{x}(j_k) \in \mathcal{A}_q^t$, $k \in [s]$ назовем вектор

$$\left\langle \boldsymbol{x}(j_k),\, k \in [s] \right\rangle \triangleq \left(\bigcup_{k=1}^{s} x_1(j_k),\, \bigcup_{k=1}^{s} x_2(j_k),\, \ldots,\, \bigcup_{k=1}^{s} x_N(j_k) \right), \quad \bigcup_{k=1}^{s} x_i(j_k) \subseteq \mathcal{A}_q,\ i \in [N],$$

т.е. гиперслово длины N, на i-ой, $i \in [N]$, позиции которого стоит $\bigcup_{k=1}^{s} x_i(j_k)$ – подмножество символов алфавита $\mathcal{A}_q$, встречающихся на i-ой позиции *хотя бы одного* из слов $\boldsymbol{x}(j_k)$, $k \in [s]$. Будем говорить, что слово $\boldsymbol{a} = (a_1, a_2, \ldots, a_N)$, $a_i \in \mathcal{A}_q$, *подчиняется* [1] *гиперслову*

$\mathcal{Q} = (\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_N)$, $\mathcal{Q}_i \subseteq \mathcal{A}_q$, (или гиперслово $\mathcal{Q}$ *подчиняет* слово $\boldsymbol{a}$), если $a_i \in \mathcal{Q}_i$ для любого i, $i \in [N]$.

Описанное ниже определение гиперкода является аналогом определения 1.1.1 СД s_L-кода.

Определение 4.1.1. Код X_q называется *q-ичным гиперкодом со списочным декодированием силы s с объемом списка L* (кратко, *q-ичным СД s_L-гиперкодом*), если для любого множества номеров $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, гиперсумма $\langle \boldsymbol{x}(j), j \in \mathcal{S} \rangle$ подчиняет не более $L-1$ других слов кода X_q, номера которых не принадлежат множеству $\mathcal{S}$. В наиболее важном частном случае $L = 1$ это означает, что для любого множества номеров $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и любого номера $k \notin \mathcal{S}$ кодовое слово $\boldsymbol{x}(k)$ не подчиняется гиперсумме $\langle \boldsymbol{x}(j), j \in \mathcal{S} \rangle$.

Обозначим через $t^{(q)}(N, s, L)$ максимальный объем q-ичных СД s_L-гиперкодов длины N, и определим *скорость* q-ичных СД s_L-гиперкодов:

$$R_L^{(q)}(s) \triangleq \varlimsup_{N\to\infty} \frac{\log_q t^{(q)}(N, s, L)}{N}.$$

Следующее утверждение для q-ичных СД s_L-гиперкодов дает очевидный аналог свойства СД s_L-кодов, связанного с понижением параметра L до 1 [44].

Предложение 4.1.1. *Если $L \le s < t$, то любой q-ичный СД s_L-гиперкод объема t и длины N содержит не менее $t-(L-1)$ кодовых слов, образующих q-ичный СД $\lfloor s/L \rfloor$-гиперкод длины N. Поэтому для максимального объема $t^{(q)}(N, s, L)$ и скорости $R_L^{(q)}(s)$ справедливы верхние границы*

$$t^{(q)}(N, s, L) \le t^{(q)}\left(N, \lfloor s/L \rfloor, 1\right) + L - 1 \quad \Longrightarrow \quad R_L^{(q)}(s) \le R_1^{(q)}\left(\lfloor s/L \rfloor\right), \quad L \le s.$$

Доказательство предложения 4.1.1. Пусть X_q – q-ичный СД s_L-гиперкод объема t и длины N. Предположим, что любые $t-(L-1)$ кодовых слов не образуют q-ичный СД $\lfloor s/L \rfloor$-гиперкод. Выберем произвольное множество из $t-(L-1)$ кодовых слов кода X_q, тогда существует $\lfloor s/L \rfloor$ слов, гиперсумма которых подчиняет постороннее кодовое слово $\boldsymbol{x}_{j_1}$. Теперь для каждого целого k от 1 до $L-1$ выберем произвольные $t-(L-1)$ кодовых слов из $t-k$ кодовых слов кода X_q, исключающих $\boldsymbol{x}_{j_1}, \boldsymbol{x}_{j_2}, \ldots, \boldsymbol{x}_{j_k}$. Среди выбранных существуют $\lfloor s/L \rfloor$ слов, гиперсумма которых подчиняет постороннее кодовое слово $\boldsymbol{x}_{j_{k+1}}$. В итоге получим $L \cdot \lfloor s/L \rfloor$ кодовых слов, которые подчиняют L других слов. $\square$

Для фиксированных значений параметров $s \ge 2$ и $L \ge 1$ рекуррентное неравенство для скорости $R_L^{(q)}(s)$ при изменении объема кодового алфавита q устанавливает

Предложение 4.1.2. *Для любых целых чисел $q' > q \ge 2$, $s \ge 2$ и $L \ge 1$ выполнено неравенство*

$$R_L^{(q)}(s) \ge \frac{R_L^{(q')}(s)}{\lceil q'/(q-1) \rceil \log_{q'} q}. \tag{4.1.2}$$

Доказательство предложения 4.1.2. Предположим, что существует q'-ичный СД s_L-гиперкод $X'_{q'}$ длины N и объема t. Пусть $l \triangleq \lceil q'/(q-1) \rceil$ и рассмотрим q-ичный код C_q длины l и объема $l(q-1) \ge q'$, составленный из всех кодовых слов с одной ненулевой компонентой:

$$\left|\begin{array}{cccccccccccc}
1 & 0 & \ldots & 0 & 2 & 0 & \ldots & 0 & \ldots & q-1 & 0 & \ldots & 0 \\
0 & 1 & \ldots & 0 & 0 & 2 & \ldots & 0 & \ldots & 0 & q-1 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ldots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 2 & \ldots & 0 & 0 & \ldots & q-1
\end{array}\right|$$

Очевидно, что C_q является q-ичным s_1-гиперкодом. Каждому q'-ичному символу q'_0 инъективно сопоставим кодовое слово $c(q'_0)$ кода C_q. Тогда нетрудно установить рассуждениями от противного, что q-ичный код X_q длины $l \cdot N$ и объема t, полученный из кода $X'_{q'}$ заменой каждой компоненты q'_0 на q-ичный столбец $c(q'_0)$, является q-ичным СД s_L-гиперкодом, откуда и следует неравенство (4.1.2). $\square$

4.2 Нижние границы скорости

Нижняя граница на скорость q-ичных СД s_L-гиперкодов, сформулированная в следующей теореме 4.2.1, основана на методе случайного кодирования на ансамбле кодов с независимыми одинаково распределенными q-ичными компонентами, который также использовался при выводе нижних границ на скорость q-ичных СД s_1-гиперкодов в работах [39, 40], и на последовательном применении предложения 4.1.2, которое дает возможность при больших s получить границу, улучшающую границы из [39, 40]. Отметим, что коды, существование которых показано при доказательстве теоремы 4.2.1, имеют кодовые слова с одинаковым числом нулевых символов.

Теорема 4.2.1 (Нижняя граница для $R_L^{(q)}(s)$)**.** *Справедливы четыре утверждения.*
1. *При любых фиксированных $q \geq 2$, $s \geq 2$ и $L \geq 1$ справедлива нижняя граница:*

$$R_L^{(q)}(s) \geq \underline{R}_L^{(q)}(s) \triangleq \max_{q' \geq q} \frac{-\log_q P(q', s, L)}{(s + L - 1)k(q, q')}, \quad \textit{где} \tag{4.2.1}$$

$$P(q, s, L) \triangleq \sum_{m=1}^{\min\{q,s\}} \binom{q}{m} \left(\frac{m}{q}\right)^L \sum_{k=0}^{m} (-1)^k \binom{m}{k} \left(\frac{m-k}{q}\right)^s, \tag{4.2.2}$$

$$k(q, q') \triangleq \begin{cases} 1, & \textit{при} \quad q = q', \\ \lceil \frac{q'}{q-1} \rceil, & \textit{иначе.} \end{cases} \tag{4.2.3}$$

2. *При любых фиксированных $q \geq 2$ и $L \geq 1$ выполнено асимптотическое равенство*

$$\underline{R}_L^{(q)}(s) = \frac{L(q-1)\log_q e}{s^2 (\log_2 e)^2}(1 + o(1)), \quad s \to \infty. \tag{4.2.4}$$

3. *При любых фиксированных $q \geq 2$ и $s \geq 2$ существует предел $\underline{R}_\infty^{(q)}(s) \triangleq \lim_{L\to\infty} \underline{R}_L^{(q)}(s)$, причем при $s \to \infty$ выполнено асимптотическое равенство*

$$\underline{R}_\infty^{(q)}(s) = \frac{(q-1)\log_q e}{es}, \quad s \to \infty. \tag{4.2.5}$$

4. *При любых фиксированных $s \geq 2$ и $L \geq 1$ существует предел*

$$\lim_{q\to\infty} \underline{R}_L^{(q)}(s) = \frac{L}{s + L - 1}. \tag{4.2.6}$$

Уточнением нижних границ из теоремы 4.2.1 для случая $q = 2$ служит следующая теорема 4.2.2, в которой представлены нижние границы для скорости двоичных СД s_L-гиперкодов, полученные с помощью метода случайного кодирования на ансамбле равновесных двоичных кодов. Ход доказательства теоремы 4.2.2 аналогичен доказательству нижней границы для скорости СД s_L-кодов в теореме 1.2.2.

Пусть $h(z) \triangleq -z\log_2 z - (1-z)\log_2[1-z]$, $0 < z < 1$, – стандартное обозначение двоичной энтропии. Для фиксированных $s \geq 2$, $L \geq 1$ и переменной z, $0 < z < 1$, введем функции:

$$\begin{aligned} p(z) &\triangleq p_L(s,z) = z^s(z-z^s)^L, \\ q(z) &\triangleq q_L(s,z) = (z-z^s)(1-z^s-(1-z)^s)^L, \quad 0 < z < 1, \end{aligned} \tag{4.2.7}$$

аналитические свойства которых устанавливает сформулированная ниже лемма 4.2.1.

Лемма 4.2.1. *Функция*

$$\psi(z) \triangleq \frac{p(z)+q(z)}{p(1-z)+q(1-z)}, \quad 0 < z < 1, \tag{4.2.8}$$

где $p(z)$ и $q(z)$ определены (4.2.7)*, строго возрастает на интервале $(0,1)$, а также непрерывно отображает $(0,1)$ на интервал $(0,+\infty)$.*

Теорема 4.2.2 (Нижняя граница для $R_L^{(2)}(s)$)**.** *Имеют место следующие* 3 *утверждения.*
1. *При любых фиксированных $s \geq 2$ и $L \geq 1$ выполнено неравенство*

$$\begin{aligned} R_L^{(2)}(s) \geq \underline{R}_L^*(s) &\triangleq \max_{0<Q\leq 1/2}\left(h(Q) + \frac{B_L(s,Q)}{s+L-1}\right), \\ B_L(s,Q) &\triangleq Q\log_2\left[\frac{p(1-z)}{p(1-z)+q(1-z)}\right] + (1-Q)\log_2\left[\frac{p(z)}{p(z)+q(z)}\right], \end{aligned} \tag{4.2.9}$$

где параметр $z \in (0,1)$ определяется как единственный корень уравнения

$$Q(p(z)+q(z)) = (1-Q)(p(1-z)+q(1-z)). \tag{4.2.10}$$

2. *При фиксированном $L = 1, 2, \ldots$ и $s \to \infty$ справедливо асимптотическое неравенство*

$$\underline{R}_L^*(s) \geq \frac{L}{s^2\log_2 e}(1+o(1)), \quad s \to \infty. \tag{4.2.11}$$

3. *При фиксированном $s = 2, 3, \ldots$ существует предел*

$$\underline{R}_\infty^*(s) \triangleq \lim_{L\to\infty} \underline{R}_L^*(s) = \log_2\left[\frac{(s-1)^{s-1}}{s^s} + 1\right]. \tag{4.2.12}$$

Если $s \to \infty$, то

$$\underline{R}_\infty^*(s) = \frac{\log_2 e}{es}(1+o(1)) = \frac{0,5307\ldots}{s}(1+o(1)). \tag{4.2.13}$$

Отметим, что лемма 4.2.1 влечет существование и единственность корня уравнения (4.2.10).

Доказательство теоремы 4.2.1

Доказательство утверждения 1. Для произвольного q-ичного кода X_q (4.1.1) пару множеств $(\mathcal{S},\mathcal{L})$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и $\mathcal{L} \subset [t]\setminus\mathcal{S}$, $|\mathcal{L}| = L$, будем называть s_L-*плохой*, если гиперсумма $\langle \boldsymbol{x}(j), j \in \mathcal{S}\rangle$ подчиняет все кодовые слова $\{\boldsymbol{x}(j), j \in \mathcal{L}\}$. Рассмотрим ансамбль

q-ичных кодов длины N и объема t ($t \geq s + L$), q-ичные символы которого выбираются независимо и равновероятно:

$$\Pr\{x_i(j) = q_0\} = \frac{1}{q}, \quad \forall\, q_0 \in \mathcal{A}_q,\ i \in [N],\ j \in [t].$$

Обозначим вероятность события "фиксированная пара $(\mathcal{S}, \mathcal{L})$ является s_L-плохой" через $P(q, s, L, N)$. Очевидно, что такая вероятность не зависит от выбора множеств $\mathcal{S}$, $\mathcal{L}$, и $P(q, s, L, N) = (P(q, s, L, 1))^N$.

Рассуждения, аналогичные сделанным при доказательстве теоремы 1.2.2, приводят к следующей нижней границе на скорость q-ичных СД s_L-гиперкодов:

$$R_L^{(q)}(s) \geq \frac{-\log_q P(q, s, L, 1)}{s + L - 1}. \tag{4.2.14}$$

В [28] при выводе нижних границ на скорость СД s_L-кодов было показано, что вероятность $P(q, s, L, 1)$ можно вычислять по формуле (4.2.2). Неравенство (4.2.14) и предложение 4.1.2 означают, что утверждение 1 теоремы 4.2.1 полностью доказано.

Доказательство утверждения 2. Асимптотика вероятности (4.2.2) при $s \to \infty$ уже была вычислена в [28] и согласуется с утверждением 2. Здесь мы лишь приведем более простое доказательство наиболее важного факта, что асимптотика нижней границы (4.2.1)-(4.2.3) не меньше, чем правая часть (4.2.4).

Пусть $q \geq L$. Покажем, что справедлива оценка сверху

$$P(q, s, L, 1) \leq P_1(q, s, L) \triangleq \frac{\dfrac{q!}{(q-L)!}\displaystyle\sum_{k=0}^{L}(-1)^k\binom{L}{k}\left(1 - \frac{k}{q}\right)^s + q^L - \dfrac{q!}{(q-L)!}}{q^L}. \tag{4.2.15}$$

С помощью формулы полной вероятности, представим $P(q, s, L, 1)$ в следующем виде:

$$\begin{aligned} P(q, s, L, 1) &\triangleq \Pr\left\{\{x_1(s+1), x_1(s+2), \ldots, x_1(s+L)\} \subset \{x_1(1), x_1(2), \ldots, x_1(s)\}\right\} \\ &= \sum_{q_1, \ldots, q_L} \frac{1}{q^L} \Pr\left\{\{q_1, \ldots, q_L\} \subset \{x_1(1), \ldots, x_1(s)\}\right\}, \end{aligned} \tag{4.2.16}$$

где сумма взята по всем q^L различным наборам из L q-ичных символов $q_1, \ldots, q_L$. Для объема алфавита $q \geq L$ рассмотрим набор *без повторений* $\{q_1, \ldots, q_L\}$, где все L q-ичных символов различны, и введем обозначения для событий

$$B_j \triangleq \{q_j \in \{x_1(1), \ldots, x_1(s)\}\}, \quad \forall j \in [L].$$

Соответствующая набору без повторений вероятность в слагаемом (4.2.16) равна

$$\begin{aligned} &\Pr\left\{\{q_1, \ldots, q_L\} \subset \{x_1(1), \ldots, x_1(s)\}\right\} = \Pr\left\{\bigcap_{j=1}^{L} B_j\right\} = 1 - \Pr\left\{\bigcup_{j=1}^{L} \overline{B_j}\right\} \\ &= 1 - \sum_{k=1}^{L}(-1)^{k-1}\binom{L}{k} \Pr\left\{\bigcap_{j=1}^{k} \overline{B_j}\right\} = \sum_{k=0}^{L}(-1)^k\binom{L}{k}\left(1 - \frac{k}{q}\right)^s. \end{aligned}$$

Заметим, что при $q \geq L$ в сумме (4.2.16) ровно $\frac{q!}{(q-L)!}$ членов, соответствующих наборам без повторений, что завершает доказательство неравенства (4.2.15). Неравенство (4.2.15) означает, что

$$\underline{R}_L^{(q)}(s) \geq \max_{q' \geq q} \frac{-\log_q P_1(q', s, L)}{(s + L - 1)k(q, q')}. \tag{4.2.17}$$

Пусть $q \geq 2$, $L \geq 1$ фиксированы и $s \to \infty$. Заметим, что при $q' = q'(s) = \lceil s/\lambda \rceil$, где $\lambda > 0$ – произвольная константа, не зависящая от s, предел (4.2.15) равен

$$\lim_{s\to\infty} P_1(q'(s), s, L) = (1 - e^{-\lambda})^L.$$

Следовательно, после подстановки $q'(s) = \lceil s/\lambda \rceil$ в формулу (4.2.17) получим асимптотическое неравенство:

$$\underline{R}_L^{(q)}(s) \geq \frac{-L(q-1)\lambda \log_q[1 - e^{-\lambda}]}{s^2}(1 + o(1)), \quad s \to \infty. \tag{4.2.18}$$

Взятие производной по λ приводит к тому, что в точке $\lambda = \ln 2$ достигается максимум

$$\max_{\lambda>0} \left\{-\lambda \ln[1 - e^{-\lambda}]\right\} = (\ln 2)^2. \tag{4.2.19}$$

Подставляя оптимальное значение $\lambda = \ln 2$ в (4.2.18) получим

$$\underline{R}_L^{(q)}(s) \geq \frac{L(q-1)\log_q e}{s^2(\log_2 e)^2}(1 + o(1)), \quad s \to \infty.$$

Доказательство утверждения 3. Асимптотика вероятности (4.2.2) при $L \to \infty$ была исследована в [28] и согласуется с утверждением 3. Здесь мы более простым путем докажем, что предел $\underline{R}_\infty^{(q)}(s) \triangleq \lim_{L\to\infty} \underline{R}_L^{(q)}(s)$ нижней границы (4.2.1)-(4.2.3) неотрицателен, а также что при $s \to \infty$ асимптотика $\underline{R}_\infty^{(q)}(s)$ не меньше, чем правая часть (4.2.5).

Для начала покажем, что при $q \geq s$ вероятность $P(q, s, L, 1)$ удовлетворяет неравенству

$$P(q, s, L, 1) \leq P_2(q, s, L) \triangleq \left(\frac{s}{q}\right)^L. \tag{4.2.20}$$

Используя формулу полной вероятности, представим $P(q, s, L, 1)$ в такой форме:

$$P(q, s, L, 1) = \sum_{q_1,\ldots,q_s} \frac{1}{q^s} \left(\Pr\left\{x_1(1) \in \{q_1, \ldots, q_s\}\right\}\right)^L, \tag{4.2.21}$$

где сумма взята по всем различным наборам из s q-ичных символов $q_1, \ldots, q_s$. Очевидно, что $\Pr\left\{x_1(1) \in \{q_1, \ldots, q_s\}\right\} \leq \frac{s}{q}$, откуда и следует (4.2.20).

Пусть $q \geq 2$, $s \geq 2$ фиксированы и $L \to \infty$. Заметим, что существует предел

$$\lim_{L\to\infty} \frac{-\log_q P_2(q, s, L)}{s + L - 1} = \log_q \frac{q}{s},$$

Поэтому справедливо следующее асимптотическое неравенство для нижней границы (4.2.1)-(4.2.3):

$$\underline{R}_L^{(q)}(s) \geq \max_{q'\geq q} \frac{\log_q \frac{q'}{s}}{k(q, q')}(1 + o(1)), \quad L \to \infty. \tag{4.2.22}$$

Подставляя $q' = q'(s) = \lceil s/\lambda \rceil$ в правую часть (4.2.22) приходим к неравенству

$$\underline{R}_\infty^{(q)}(s) \geq \frac{-(q-1)\lambda \log_q \lambda}{s}(1 + o(1)), \quad s \to \infty,$$

максимум правой части которого достигается при $\lambda = 1/e$ и совпадает с правой частью (4.2.5).

Доказательство утверждения 4. Пусть $s \geq 2$, $L \geq 1$ фиксированы и $q \to \infty$. В силу неравенства (4.2.20) выполнено следующее соотношение для нижней границы (4.2.1)-(4.2.3):

$$\underline{R}_L^{(q)}(s) \geq \frac{L}{s+L-1} \max_{q' \geq q} \frac{\log_q [q'/s]}{k(q,q')}(1+o(1)), \quad q \to \infty, \tag{4.2.23}$$

где функция $k(q,q')$ задана (4.2.3). Заметим, что максимум в правой части (4.2.23) достигается при $q' = q$, поэтому

$$\underline{R}_L^{(q)}(s) \geq \frac{L}{s+L-1}(1+o(1)), \quad q \to \infty. \tag{4.2.24}$$

В то же время, из представления (4.2.21) и очевидного неравенства

$$\Pr\left\{x_1(1) \in \{q_1, \ldots, q_s\}\right\} \geq \frac{1}{q}$$

следует:

$$P(q,s,L,1) \geq \left(\frac{1}{q}\right)^L. \tag{4.2.25}$$

По аналогии с выводом (4.2.24) нетрудно вывести из (4.2.25) обратное неравенство:

$$\underline{R}_L^{(q)}(s) \leq \frac{L}{s+L-1}(1+o(1)), \quad q \to \infty.$$

Утверждение 4 теоремы 4.2.1 доказано. $\square$

Доказательство леммы 4.2.1

При фиксированных $s \geq 2$ и $L \geq 1$ введем следующую функцию

$$g(z) \triangleq g(s,z) = \frac{z - z^s}{1 - z - (1-z)^s}, \quad 0 < z < 1. \tag{4.2.26}$$

Перепишем формулу (4.2.8), используя обозначение неубывающей функции $g(z)$ (4.2.26):

$$\psi(z) = \frac{z^s (g(z))^L + (z - z^s)(1+g(z))^L}{(1-z)^s + (1 - z - (1-z)^s)(1+g(z))^L}. \tag{4.2.27}$$

Поделим числитель и знаменатель в выражении (4.2.27) на $(z - z^s)(1+g(z))^L$:

$$\psi(z) = \frac{\left(\frac{g(z)}{1+g(z)}\right)^L \cdot \frac{z^s}{z-z^s} + 1}{\frac{(1-z)^s}{z-z^s} \cdot \frac{1}{(1+g(z))^L} + \frac{1}{g(z)}},$$

где функция $\frac{z^s}{z-z^s}$ является строго возрастающей, а функция $\frac{(1-z)^s}{z-z^s}$ – строго убывающей. Таким образом, функция $\psi(z)$ является строго возрастающей.

Заметим, что $g(z) \to \frac{1}{s-1}$ при $z \to 0$ и $g(z) \to s-1$ при $z \to 1$. Следовательно, для выражения (4.2.27) справедливы пределы

$$\lim_{z \to 0+0} \psi(z) = 0,$$
$$\lim_{z \to 1-0} \psi(z) = +\infty.$$

Лемма 4.2.1 доказана. $\square$

Доказательство теоремы 4.2.2

Доказательство утверждения 1. Для произвольного двоичного кода X_2 (4.1.1) пару множеств $(\mathcal{S}, \mathcal{L})$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и $\mathcal{L} \subset [t] \setminus \mathcal{S}$, $|\mathcal{L}| = L$, будем называть s_L-*плохой*, если гиперсумма $\langle \boldsymbol{x}(j), j \in \mathcal{S} \rangle$ подчиняет все кодовые слова $\{\boldsymbol{x}(j), j \in \mathcal{L}\}$ (так же, как и при доказательстве теоремы 4.2.1). Зафиксируем $L \geq 1$, $s \geq 2$, а также параметр Q, $0 < Q < 1$. Как уже отмечалось, границу (4.2.9) будем выводить методом случайного кодирования на ансамбле двоичных равновесных кодов [26], применяя при этом методы из доказательства теоремы 1.2.2. Обозначим через $E(N, t, Q)$ ансамбль двоичных кодов X_2 длины N и объема t, для которых кодовые слова выбираются независимо и равновероятно из множества, состоящего из всех $\binom{N}{\lfloor QN \rfloor}$ двоичных кодовых слов веса $\lfloor QN \rfloor$. Зафиксируем пару множеств $(\mathcal{S}, \mathcal{L})$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и $\mathcal{L} \in [t] \setminus \mathcal{S}$, $|\mathcal{L}| = L$, и для ансамбля $E(N, t, Q)$ обозначим через $P(N, Q, s, L)$ вероятность события "пара $(\mathcal{S}, \mathcal{L})$ является s_L-плохой".

Рассуждения, аналогичные сделанным при доказательстве теоремы 1.2.2, приводят к неравенству:

$$\begin{gathered} R_L^{(2)}(s) \geq \underline{R}_L^*(s) \triangleq \frac{1}{s + L - 1} \max_{0<Q<1} A_L^*(s, Q), \\ A_L^*(s, Q) \triangleq \varlimsup_{N \to \infty} \frac{-\log_2 P(N, Q, s, L)}{N}. \end{gathered} \tag{4.2.28}$$

Заметим, что множество всех s_L-плохих пар является инвариантом относительно операции логического отрицания всех компонент двоичного кода X_2 (т.е. замены нулей на единицы, а единиц на нули), откуда следует равенство $P(N, Q, s, L) = P(N, 1 - Q, s, L)$. Таким образом, при поиске максимума в (4.2.28) достаточно ограничиться значениями параметра $0 < Q \leq 1/2$.

Для доказательства утверждения 1 теоремы 4.2.2 осталось вычислить функцию $A_L^*(s, Q)$.

Повторяя доказательство теоремы 1.2.2, будем использовать терминологию типов последовательностей. Рассмотрим произвольное множество из s кодовых слов длины N и одинакового веса $\lfloor QN \rfloor$: $(\boldsymbol{x}(1), \ldots, \boldsymbol{x}(s))$, где $\boldsymbol{x}(i) \in \{0,1\}^N$, $\forall i \in [s]$. Это множество образует $(N \times s)$-матрицу X^s. Пусть $\boldsymbol{a} \triangleq (a_1, \ldots, a_s) \in \{0,1\}^s$ обозначает некоторую строку объема s. Определим *mun* матрицы X^s как множество $\{n(\boldsymbol{a}), \forall \boldsymbol{a} \in \{0,1\}^s\}$, где $n(\boldsymbol{a})$, $0 \leq n(\boldsymbol{a}) \leq N$, равно числу строк $\boldsymbol{a}$ в матрице X^s.

Через $n(\boldsymbol{0})$ ($n(\boldsymbol{1})$) обозначим число строк в матрице X^s, составленных только из нулей (единиц). При таких обозначениях вероятность s_L-плохой пары выражается

$$P(N, Q, s, L) = \sum_{\{n(\boldsymbol{a})\} \in \mathcal{N}} \frac{N!}{\prod_{\boldsymbol{a}} n(\boldsymbol{a})!} \binom{N - n(\boldsymbol{0}) - n(\boldsymbol{1})}{\lfloor QN \rfloor - n(\boldsymbol{1})}^L \binom{N}{\lfloor QN \rfloor}^{-s-L}, \tag{4.2.29}$$

где множество $\mathcal{N}$ состоит из всех возможных типов $\{n(\boldsymbol{a})\}$, удовлетворяющих условиям:

$$\begin{gathered} 0 \leq n(\boldsymbol{a}) \leq N \quad \forall\, \boldsymbol{a} \in \{0,1\}^s, \quad n(\boldsymbol{0}) \leq N - \lfloor QN \rfloor, \quad n(\boldsymbol{1}) \leq \lfloor QN \rfloor, \\ \sum_{\boldsymbol{a}} n(\boldsymbol{a}) = N, \quad \sum_{\boldsymbol{a}:\, a_i = 1} n(\boldsymbol{a}) = \lfloor QN \rfloor \quad \forall\, i \in [s]. \end{gathered} \tag{4.2.30}$$

Перейдем к пределу $N \to \infty$. Каждому типу $\{n(\boldsymbol{a})\}$ поставим в соответствие распределение $\tau \triangleq \{\tau(\boldsymbol{a})\} : \tau(\boldsymbol{a}) = \frac{n(\boldsymbol{a})}{N}$. Таким образом, при $N \to \infty$ множество $\mathcal{N}$ соответствует множеству $\mathcal{T}$, содержащим все распределения со следующими свойствами, индуцирован-

ными (4.2.30):

$$\tau \in \mathcal{T} \Longleftrightarrow \left\{ \begin{array}{c} 0 \le \tau(\boldsymbol{a}) \le 1 \quad \forall\, \boldsymbol{a} \in \{0,1\}^s, \quad \tau(\boldsymbol{0}) \le 1-Q, \quad \tau(\boldsymbol{1}) \le Q, \\ \sum\limits_{\boldsymbol{a}\in\{0,1\}^s} \tau(\boldsymbol{a}) = 1, \quad \sum\limits_{\boldsymbol{a}:\ a_i=1} \tau(\boldsymbol{a}) = Q \quad \forall\, i \in [s]. \end{array} \right\} \tag{4.2.31}$$

С помощью формулы Стирлинга находим логарифмическую асимптотику слагаемого в сумме (4.2.29):

$$\begin{aligned} -\log_2 \sum_{\{n(\boldsymbol{a})\}\in\mathcal{N}} \frac{N!}{\prod_{\boldsymbol{a}} n(\boldsymbol{a})!} \binom{N-n(\boldsymbol{0})-n(\boldsymbol{1})}{\lfloor QN \rfloor - n(\boldsymbol{1})}^{L} \binom{N}{\lfloor QN \rfloor}^{-s-L} \\ = NF(\tau,Q)(1+o(1)), \quad \text{где,} \\ F(\tau,Q) \triangleq \sum_{\boldsymbol{a}} \tau(\boldsymbol{a}) \log_2[\tau(\boldsymbol{a})] - (1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1}))Lh\left(\frac{Q-\tau(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}\right) \\ +(s+L)h(Q). \end{aligned} \tag{4.2.32}$$

Пусть минимум функции $F(\tau,Q)$ достигается на распределении $\tau_Q = \{\tau_Q(\boldsymbol{a})\}$, тогда

$$A_L^*(s,Q) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 P(s,L,Q,N)}{N} = F(\tau_Q,Q) = \min_{\tau\in\mathcal{T}} F(\tau,Q). \tag{4.2.33}$$

Так как F непрерывна на компактном множестве $\mathcal{T}$ допустимых значений, то для вычисления (4.2.33) достаточно найти минимум F на множестве (4.2.31) с исключенными границами. Запишем соответствующую задачу минимизации: $F \to \min$,

$$\text{Область поиска } \mathbb{T}: \qquad 0 < \tau(\boldsymbol{a}) < 1 \quad \forall\, \boldsymbol{a} \in \{0,1\}^s, \quad \tau(\boldsymbol{1}) < Q, \quad \tau(\boldsymbol{0}) < 1-Q, \tag{4.2.34}$$

$$\text{Ограничения:} \qquad \left\{ \begin{array}{l} \sum\limits_{\boldsymbol{a}\in\{0,1\}^s} \tau(\boldsymbol{a}) = 1, \\ \sum\limits_{\boldsymbol{a}:\ a_i=1} \tau(\boldsymbol{a}) = Q \quad \forall\, i \in [s], \end{array} \right. \tag{4.2.35}$$

$$\text{Основная функция:} \qquad F(\tau,Q) = (4.2.32) :\ \mathbb{T} \to \mathbb{R}, \tag{4.2.36}$$

где ограничения (4.2.34)-(4.2.35) естественным образом получены из (4.2.30).

Для поиска точки экстремума τ_Q применим стандартный метод множителей Лагранжа. Рассмотрим лагранжиан:

$$\Lambda \triangleq F(\tau,Q) + \lambda_0 \left(\sum_{\boldsymbol{a}\in\{0,1\}^s} \tau(\boldsymbol{a}) - 1 \right) + \sum_{i=1}^{s} \lambda_i \left(\sum_{\boldsymbol{a}:a_i=1} \tau(\boldsymbol{a}) - Q \right).$$

Необходимые условия экстремального распределения τ_Q принимают вид:

$$\left\{ \begin{array}{ll} \frac{\partial\Lambda}{\partial(\tau(\boldsymbol{a}))} & = \log_2[\tau(a)] + \log_2 e + \lambda_0 + \sum_{i=1}^s \lambda_i a_i = 0, \quad \forall\, \boldsymbol{a} \in \{0,1\}^s \setminus \{\boldsymbol{0},\boldsymbol{1}\}, \\ \frac{\partial\Lambda}{\partial(\tau(\boldsymbol{0}))} & = \log_2[\tau(\boldsymbol{0})] + \log_2 e + \lambda_0 + L\log_2\left[\frac{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}{1-Q-\tau(0)}\right] = 0, \\ \frac{\partial\Lambda}{\partial(\tau(\boldsymbol{1}))} & = \log_2[\tau(\boldsymbol{1})] + \log_2 e + \lambda_0 + \sum_{i=1}^s \lambda_i + L\log_2\left[\frac{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}{Q-\tau(\boldsymbol{1})}\right] = 0. \end{array} \right. \tag{4.2.37}$$

Покажем, что матрица производных второго порядка лагранжиана является положительно определенной. Действительно, для элементов матрицы справедливы выражения:

$$\begin{aligned}
\frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{a}))^2} &= \frac{\log_2 e}{\tau(\boldsymbol{a})} > 0, \quad \forall\ \boldsymbol{a} \in \{0,1\}^s \setminus \{\boldsymbol{0}, \boldsymbol{1}\},\\
\frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{0}))^2} &= \frac{\log_2 e}{\tau(\boldsymbol{0})} + L\log_2 e\frac{Q-\tau(\boldsymbol{1})}{(1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1}))(1-Q-\tau(\boldsymbol{0}))} > 0,\\
\frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{1}))^2} &= \frac{\log_2 e}{\tau(\boldsymbol{1})} + L\log_2 e\frac{1-Q-\tau(\boldsymbol{0})}{(1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1}))(Q-\tau(\boldsymbol{1}))} > 0,\\
\frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{0}))\partial(\tau(\boldsymbol{1}))} &= -L\log_2 e\frac{1}{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})} < 0,
\end{aligned}$$

а все остальные элементы матрицы равны нулю. Таким образом, данная матрица положительно определена.

Аналогичная задача минимизации была решена при доказательстве утверждения 1 теоремы 1.2.2. Используя приведенные в этом доказательстве рассуждения, получаем, что необходимые и достаточные условия для минимального распределения τ в задаче (4.2.34)-(4.2.36) состоят из (4.2.34)-(4.2.35), а также:

$$\begin{cases}
\log_2\mu + \log_2[\tau(\boldsymbol{a})] + \nu\sum_{i=1}^s a_i = 0,\\
\log_2\mu + \log_2[\tau(\boldsymbol{0})] + L\log_2\left[\frac{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}{1-Q-\tau(\boldsymbol{0})}\right] = 0,\\
\log_2\mu + \log_2[\tau(\boldsymbol{1})] + L\log_2\left[\frac{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}{Q-\tau(\boldsymbol{1})}\right] + s\nu = 0,
\end{cases} \tag{4.2.38}$$

где $\mu \triangleq e2^{\lambda_0}$ и $\nu \triangleq \lambda_1 = \lambda_2 = \cdots = \lambda_s$

Введем параметр $z \triangleq \frac{1}{1+2^{-\nu}}, 0 < z < 1$, тогда из первого уравнения (4.2.38) следует, что

$$\tau(\boldsymbol{a}) = \frac{2^{-\nu\sum a_i}}{\mu} = \frac{1}{\mu z^s}(1-z)^{\sum a_i} z^{s-\sum a_i} \quad \forall\ \boldsymbol{a} \in \{0,1\}^s \setminus \{\boldsymbol{0}, \boldsymbol{1}\}. \tag{4.2.39}$$

Далее, подставим (4.2.39) в первое и второе уравнения (4.2.35):

$$1 = \frac{1}{\mu z^s}\sum_{i=1}^{s-1}\binom{s}{i} z^i(1-z)^{s-i} + \tau(\boldsymbol{0}) + \tau(\boldsymbol{1}) = \frac{1-z^s-(1-z)^s}{\mu z^s} + \tau(\boldsymbol{0}) + \tau(\boldsymbol{1}), \tag{4.2.40}$$

$$Q = \frac{1}{\mu z^s}\sum_{i=1}^{s-1}\binom{s-1}{i} z^i(1-z)^{s-i} + \tau(\boldsymbol{1}) = \frac{1-z-(1-z)^s}{\mu z^s} + \tau(\boldsymbol{1}). \tag{4.2.41}$$

Вычитая (4.2.41) из (4.2.40), выводим:

$$1 - Q = \frac{z-z^s}{\mu z^s} + \tau(\boldsymbol{0}). \tag{4.2.42}$$

В силу равенств (4.2.40)-(4.2.42) второе и третье уравнения (4.2.38) равносильны следующим:

$$\begin{aligned}
\mu\left(1-Q-\frac{z-z^s}{\mu z^s}\right)\left(\frac{1-z^s-(1-z)^s}{z-z^s}\right)^L &= 1,\\
\mu\left(Q-\frac{1-z-(1-z)^s}{\mu z^s}\right)\left(\frac{1-z^s-(1-z)^s}{1-z-(1-z)^s}\right)^L\left(\frac{z}{1-z}\right)^s &= 1.
\end{aligned} \tag{4.2.43}$$

Для краткости введем функции $p(z), q(z)$ (4.2.7) параметров s, L и z, а также $r(z)$:

$$r(z) \triangleq r_L(s,z) = z^s(1-z^s-(1-z)^s)^L.$$

С использованием данных обозначений получаем следующие два выражения для параметра μ, полученные из (4.2.43):

$$\mu = \frac{1}{1-Q}\frac{p(z)+q(z)}{r(z)}, \tag{4.2.44}$$

$$\mu = \frac{1}{Q}\frac{p(1-z)+q(1-z)}{r(z)}. \tag{4.2.45}$$

Приравнивая правую часть равенства (4.2.44) и правую часть равенства (4.2.45), заключаем, что параметр z удовлетворяет уравнению

$$Q(p(z)+q(z)) = (1-Q)(p(1-z)+q(1-z)),$$

которое в точности совпадает с уравнением (4.2.10) из условия теоремы 4.2.2.

Подстановки выражения для μ (4.2.44) в уравнение (4.2.42), а также (4.2.45) в (4.2.41) приводят к следующим равенствам:

$$\begin{aligned}\tau(\boldsymbol{0}) &= (1-Q)\frac{p(z)}{p(z)+q(z)},\\ \tau(\boldsymbol{1}) &= Q\frac{p(1-z)}{p(1-z)+q(1-z)}.\end{aligned} \tag{4.2.46}$$

Согласно лемме 4.2.1 существует единственное решение уравнения (4.2.10). Поэтому существует единственное решение системы (4.2.37), а минимум $F(\tau,Q)$ (4.2.32) принимается на распределении τ, определенном формулами (4.2.39) и (4.2.46). Итак, вычислим минимум выражения $F(\tau,Q)$ путем подстановки (4.2.39) и (4.2.46). Для начала, считаем следующую сумму:

$$\begin{aligned}&\sum_{\boldsymbol{a}:\,\boldsymbol{a}\neq\boldsymbol{0},\boldsymbol{1}} \tau(\boldsymbol{a})\log_2[\tau(\boldsymbol{a})] = \{\text{по (4.2.39)}\}\\ &= \sum_{i=1}^{s-1}\binom{s}{i}\frac{1}{\mu z^s}(1-z)^{s-i}z^i\left(\log_2\left[\frac{1}{\mu z^s}\right]+i\log_2 z+(s-i)\log_2[1-z]\right)\\ &= \frac{1-z^s-(1-z)^s}{\mu z^s}\log_2\left[\frac{1}{\mu z^s}\right]+\frac{z-z^s}{\mu z^s}\log_2\left[z^s\right]+\frac{1-z-(1-z)^s}{\mu z^s}\log_2\left[(1-z)^s\right]\\ &= \{\text{по (4.2.40), (4.2.42) и (4.2.41)}\}\\ &= (1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1}))\log_2\left[\frac{1}{\mu z^s}\right]+(1-Q-\tau(\boldsymbol{0}))\log_2\left[z^s\right]+(Q-\tau(\boldsymbol{1}))\log_2\left[(1-z)^s\right]\\ &= (1-Q-\tau(\boldsymbol{0}))\log_2\left[\frac{1}{\mu}\right]+(Q-\tau(\boldsymbol{1}))\log_2\left[\frac{(1-z)^s}{\mu z^s}\right].\end{aligned} \tag{4.2.47}$$

Затем, используя (4.2.47), вычисляем

$$\begin{aligned}
&\sum_{\boldsymbol{a}:\,\boldsymbol{a}\neq\boldsymbol{0},\boldsymbol{1}} \tau(\boldsymbol{a})\log_2[\tau(\boldsymbol{a})] - (1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1}))Lh\left(\frac{Q-\tau(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}\right)\\
&\qquad = (1-Q-\tau(\boldsymbol{0}))\left(-\log_2\mu - L\log_2\left[\frac{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}{1-Q-\tau(\boldsymbol{0})}\right]\right)\\
&\qquad + (Q-\tau(\boldsymbol{1}))\left(-\log_2\mu - \log_2\left[\frac{z^s}{(1-z)^s}\right] - L\log_2\left[\frac{1-\tau(\boldsymbol{0})-\tau(\boldsymbol{1})}{Q-\tau(\boldsymbol{1})}\right]\right)\\
&\qquad = \{\text{по (4.2.38)}\}\\
&\qquad = (1-Q-\tau(\boldsymbol{0}))\log_2[\tau(\boldsymbol{0})] + (Q-\tau(\boldsymbol{1}))\log_2\tau(\boldsymbol{1}).
\end{aligned} \tag{4.2.48}$$

Наконец, пользуясь (4.2.32), (4.2.48) и (4.2.46), находим

$$\begin{aligned}
F(\tau,Q) &= (s+L)h(Q) + (1-Q)\log_2[\tau(\boldsymbol{0})] + Q\log_2[\tau(\boldsymbol{1})]\\
&= (s+L-1)h(Q) + (1-Q)\log_2\left[\frac{p(z)}{p(z)+q(z)}\right] + Q\log_2\left[\frac{p(1-z)}{p(1-z)+q(1-z)}\right],
\end{aligned}$$

что завершает доказательство утверждения 1 теоремы 4.2.2.

Доказательство утверждения 2. При фиксированных $s \geq 2$ и $L \geq 1$, будем интерпретировать уравнение (4.2.10) как функцию $Q = Q_L(s,z)$ от аргумента $z, 0 < z < 1$, т.е.

$$Q = Q_L(s,z) \triangleq \frac{p(1-z)+q(1-z)}{p(1-z)+q(1-z)+p(z)+q(z)}, \tag{4.2.49}$$

где функции $p(z)$ и $q(z)$ определены в (4.2.7).

В силу существования и единственности корня уравнения (4.2.10), непрерывности и монотонности функции $Q_L(s,z)$ (4.2.49) (по лемме 4.2.1), определение границы случайного кодирования (4.2.9) можно переписать в виде

$$\underline{R}^*_L(s) \triangleq \max_{1/2\leq z<1} T_L(s,z), \qquad T_L(s,z) \triangleq h(Q_L(s,z)) + \frac{B_L(s,Q_L(s,z))}{s+L-1}. \tag{4.2.50}$$

Пусть $L \geq 1$ фиксировано и $s \to \infty$. Если в $T_L(s,z)$ подставить $z = 1-\lambda/s$, где параметр $\lambda = \lambda_L$ не зависит от s, то из (4.2.50) вытекает неравенство

$$\underline{R}^*_L(s) \geq T_L\left(s, 1-\frac{\lambda}{s}\right). \tag{4.2.51}$$

Далее, используя разложение в ряд Тейлора, мы покажем, что,

$$T_L\left(s,1-\frac{\lambda}{s}\right) = \frac{L}{s^2}\left(-\lambda\log_2[1-e^{-\lambda}]\right)(1+o(1)). \tag{4.2.52}$$

Для краткости введем следующие обозначения:

$$\begin{aligned}
U_L(s,z) &\triangleq \frac{p(1-z)}{p(1-z)+q(1-z)},\\
V_L(s,z) &\triangleq \frac{p(z)}{p(z)+q(z)}.
\end{aligned} \tag{4.2.53}$$

С их помощью функция $T_L(s,z)$ может быть представлена в виде

$$T_L(s,z) = -Q\log_2 Q - (1-Q)\log_2[1-Q] + \frac{1}{s+L-1}\left(Q\log_2 U + (1-Q)\log_2 V\right), \quad (4.2.54)$$

где для краткости опущены параметры s, L и z, а именно $Q = Q_L(s,z)$, $U = U_L(s,z)$ и $V = V_L(s,z)$.

Вычисляя первые два члена асимптотического разложения $p(z), q(z)$, $p(1-z), q(1-z)$ (4.2.7) при $z = 1-\lambda/s$ и $s \to \infty$, приходим к следующим асимптотическим формулам:

$$\begin{aligned}
p(1-z) &= p\left(\frac{\lambda}{s}\right) = \left(\frac{\lambda}{s}\right)^{s+L} + o\left(\frac{1}{s^{s+L}}\right),\\
q(1-z) &= q\left(\frac{\lambda}{s}\right) = \frac{\lambda(1-e^{-\lambda})^L}{s} + \frac{L\lambda^3 e^{-\lambda}(1-e^{-\lambda})^{L-1}}{2s^2} + o\left(\frac{1}{s^2}\right),\\
p(z) &= p\left(1-\frac{\lambda}{s}\right) = e^{-\lambda}(1-e^{-\lambda})^L + \frac{\lambda e^{-\lambda}(1-e^{-\lambda})^L(\lambda + L\lambda - 2Le^{\lambda} - \lambda e^{\lambda})}{2(e^{\lambda}-1)s} + o\left(\frac{1}{s}\right),\\
q(z) &= q\left(1-\frac{\lambda}{s}\right) = (1-e^{-\lambda})^{L+1} + \frac{\lambda e^{-\lambda}(1-e^{-\lambda})^L(\lambda + L\lambda - 2e^{\lambda})}{2s} + o\left(\frac{1}{s}\right).
\end{aligned} \quad (4.2.55)$$

Теперь, используя данные разложения (4.2.55), несложно получить асимптотические разложения для выражений (4.2.49),(4.2.53):

$$\begin{aligned}
Q_L\left(s, 1-\frac{\lambda}{s}\right) &= \frac{\lambda}{s} + \frac{L\lambda^2}{(e^{\lambda}-1)s^2} + o\left(\frac{1}{s^2}\right),\\
U_L\left(s, 1-\frac{\lambda}{s}\right) &= \left(\frac{\lambda}{s}\right)^{s+L-1}(1-e^{-\lambda})^{-L}(1+o(1)),\\
V_L\left(s, 1-\frac{\lambda}{s}\right) &= e^{-\lambda}\left(1 + \frac{\lambda - L\lambda - \lambda^2/2}{s} + o\left(\frac{1}{s}\right)\right).
\end{aligned} \quad (4.2.56)$$

Наконец, после подстановки равенств (4.2.56) в формулу (4.2.54) приходим к выводу, что асимптотика (4.2.54) совпадает с (4.2.52).

(4.2.51), (4.2.52) и (4.2.19) влекут за собой асимптотическое неравенство (4.2.11).

Доказательство утверждения 3. Пусть $s \geq 2$ и $L \geq 1$. Нетрудно заметить, что функция $g(z)$ (4.2.26) не убывает на полуинтервале $[1/2, 1)$, принимает 1 в точке $z = \frac{1}{2}$ и имеет левый предел $s-1$ при $z \to 1-0$. Поэтому при достаточно больших значениях параметра L и некотором фиксированном параметре $c > 0$, независящим от L, корень уравнения

$$\left(\frac{g(z)}{1+g(z)}\right)^L = c(1-z), \quad \frac{1}{2} \leq z < 1, \quad (4.2.57)$$

существует и единственен, действительно, левая часть (4.2.57) не убывает, а правая часть (4.2.57) строго убывает. Обозначим этот корень через $z_L(s,c)$.

Пусть $s \geq 2$ фиксировано, а $L \to \infty$. В соответствии с определением (4.2.50), выполнено неравенство

$$\underline{R}^*_L(s) \geq T_L(s, z_L(s,c))(1+o(1)), \quad L \to \infty, \quad \forall\, c = c(s) > 0. \quad (4.2.58)$$

Далее мы покажем, что

$$T_L(s, z_L(s,c)) \cdot (1 + o(1)) = \log_2[s+c] - \frac{s+c-1}{s+c}\log_2[s+c-1] + \\ + \frac{1}{s+c}\log_2\left[\frac{(s-1)^{s-1}}{s^s}\right], \quad L \to \infty. \quad (4.2.59)$$

Очевидно, что при $L \to \infty$ выполнено асимптотическое равенство

$$\begin{aligned} z_L(s,c) &= 1 + o(1), \quad \text{и следовательно,} \\ g(z_L(s,c)) &= (s-1)(1+o(1)). \end{aligned} \quad (4.2.60)$$

Далее, в выражения (4.2.49) и (4.2.53) подставим обозначения (4.2.7), поделим числитель и знаменатель на $(1 - z - (1-z)^s)$ и примем сокращение (4.2.26), тогда формулы для Q, U и V (4.2.49),(4.2.53) переписываются в более удобной форме:

$$\begin{aligned} Q_L(s,z) &= \frac{(1-z)^s + (1-z-(1-z)^s)(1+g(z))^L}{(1-z)^s + (1-z^s-(1-z)^s)(1+g(z))^L + z^s(g(z))^L}, \\ U_L(s,z) &= \frac{(1-z)^s}{(1-z)^s + (1-z-(1-z)^s)(1+g(z))^L}, \\ V_L(s,z) &= \frac{z^s(g(z))^L}{z^s(g(z))^L(z-z^s)(1+g(z))^L}. \end{aligned} \quad (4.2.61)$$

В силу (4.2.60)-(4.2.61) справедливы асимптотические разложения:

$$\begin{aligned} Q_L(s, z_L(s,c)) &= \frac{1}{s+c}(1+o(1)), \\ U_L(s, z_L(s,c)) &= \left(\frac{(s-1)^{s-1}}{s^s}\right)^L (1+o(1)), \\ V_L(s, z_L(s,c)) &= \frac{1}{1+\frac{s}{c}}(1+o(1)). \end{aligned} \quad (4.2.62)$$

Наконец, подставляя (4.2.62) в выражение (4.2.54) получаем (4.2.59).

Взятием производной по параметру c нетрудно убедиться, что максимум правой части (4.2.59) принимается в точке $c = c(s) = \frac{s^s-(s-1)^s}{(s-1)^{s-1}}$. Подставим полученное значение $c = c(s)$ в (4.2.59), тогда из (4.2.58) вытекает следующее неравенство для случайной границы (4.2.9):

$$\underline{R}^*_L(s) \geq \log_2\left[\frac{(s-1)^{s-1}}{s^s} + 1\right](1+o(1)), \quad L \to \infty. \quad (4.2.63)$$

Чтобы доказать знак равенства в (4.2.63), обозначим через $z = z_L(s)$ произвольную последовательность параметров z, при которых достигается максимум (4.2.50). По ходу доказательства мы будем рассматривать некоторые случаи и находить противоречие с неравенством (4.2.63). Для начала предположим, что последовательность $z_L(s)$ ограничена некоторой константой, скажем $d < 1$, то есть $1/2 \leq z_L(s) \leq d < 1$. Тогда для выражений (4.2.61) выполнены следующие асимптотические равенства:

$$\begin{aligned} Q_L(s, z_L(s)) &= \frac{1}{1+g(z)}(1+o(1)), \\ U_L(s, z_L(s)) &= \frac{(1-z)^s}{1-z-(1-z)^s}\frac{1}{(1+g(z))^L}(1+o(1)), \\ V_L(s, z_L(s)) &= \frac{z^s}{z-z^s}\left(\frac{g(z)}{1+g(z)}\right)^L (1+o(1)), \quad L \to \infty, \end{aligned} \quad (4.2.64)$$

Однако, вычисляя асимптотическое поведение $T_L(s, z_L(s))$ (4.2.54) при (4.2.64), заключаем $\underline{R}^*_L(s) = T_L(s, z_L(s)) \to 0$ при $L \to \infty$. Получено противоречие с (4.2.63). Следовательно, без ограничения общности можно считать, что $z_L(s) \to 1$. Как уже было показано, в таком случае выполнено (4.2.60).

Далее, предположим, что

$$\left(\frac{g(z)}{1+g(z)}\right)^L \frac{1}{1-z} \to 0, \quad L \to \infty. \tag{4.2.65}$$

Пользуясь свойствами (4.2.60) и (4.2.65), нетрудно вывести асимптотики выражений (4.2.61):

$$\begin{aligned} Q_L(s, z_L(s)) &= \frac{1}{s}(1+o(1)), \\ U_L(s, z_L(s)) &= \frac{(1-z)^{s-1}}{(1+g(z))^L}(1+o(1)), \\ V_L(s, z_L(s)) &= \frac{1}{s}\left(\frac{g(z)}{1+g(z)}\right)^L \frac{1}{1-z}(1+o(1)), \quad L \to \infty. \end{aligned} \tag{4.2.66}$$

Тем не менее, асимптотики (4.2.60) и (4.2.66) означают, что $\underline{R}^*_L(s) = T_L(s, z_L(s)) \to 0$ при $L \to \infty$. Поэтому и в данном случае получаем противоречие с (4.2.63).

Теперь предположим, что

$$\left(\frac{g(z)}{1+g(z)}\right)^L \frac{1}{1-z} \to \infty, \quad L \to \infty. \tag{4.2.67}$$

В силу свойств (4.2.60) и (4.2.67) справедливы следующие асимптотические формулы для выражений (4.2.61):

$$\begin{aligned} Q_L(s, z_L(s)) &= \left(\frac{1+g(z)}{g(z)}\right)^L (1-z)(1+o(1)), \\ U_L(s, z_L(s)) &= \frac{(1-z)^{s-1}}{(1+(z))^L}(1+o(1)), \\ V_L(s, z_L(s)) &= 1+o(1), \quad L \to \infty. \end{aligned} \tag{4.2.68}$$

Очевидно, что (4.2.60) и (4.2.68) приводят к выражению

$$T_L(s, z_L(s)) = \frac{Q(s-1)}{s+L-1}\log_2[1-z] + o(1). \tag{4.2.69}$$

Однако зависимость между параметрами Q и z, обозначенная первым равенством в (4.2.68), предполагает

$$Q = O(1-z).$$

Тогда, из (4.2.69) следует, что $\underline{R}^*_L(s) = T_L(s, z_L(s)) \to 0$ при $L \to \infty$. Снова получено противоречие с (4.2.63).

Без ограничения общности заключаем, что

$$\left(\frac{g(z)}{1+g(z)}\right)^L = c(1-z)(1+o(1)), \tag{4.2.70}$$

для некоторого положительного параметра c. Заметим, что равенство (4.2.70) отличается от (4.2.57) лишь умножением правой, либо левой части на функцию, стремящуюся к 1 при $L \to \infty$. По аналогии с проведенным выше выводом асимптотики (4.2.59) при $z = z_L(s, c)$ нетрудно вывести такую же асимптотику (4.2.59) при $z = z_L(s)$, удовлетворяющем свойствам (4.2.60) и (4.2.70).

Утверждение 3 теоремы 4.2.2 доказано. □

4.3 Верхние границы скорости

Верхние границы скорости $R_L^{(q)}(s)$, приводимые в теореме 4.3.1, основаны на результатах работы [44] по исследованию границ скорости $R_L(s)$ СД s_L-кодов. Идея использования границ скорости СД s_L-кодов применялась в [38], где было получено неравенство $R_L(s) \le R_L^{(2)}(s) \le R_L(s)/2$, и существенно развита в теореме 4.3.1, а верхние границы скорости $R_1^{(q)}(s)$ в работах [20, 43, 12, 39], с которыми мы сравним наши границы в следующем разделе 4.4, получены иными методами.

Теорема 4.3.1 (Соотношения между скоростями $R_L^{(q)}(s)$ и $R_L(s)$)**.** *Справедливы два утверждения.*
1. *Для фиксированных параметров $q \ge 2$, $s \ge 2$ и $L \ge 1$ скорости $R_L^{(q)}(s)$ и $R_L(s)$ удовлетворяют соотношению*

$$R_L^{(q)}(s) \le \min\left\{ \frac{q}{\log_2 q} R_L(s),\ \frac{q-1}{\log_2 q} R_L(s-1) \right\}. \tag{4.3.1}$$

2. *При любых фиксированных $q \ge 2$, $L \ge 1$ и $s \to \infty$ скорость q-ичных СД s_L-гиперкодов удовлетворяет неравенству*

$$R_L^{(q)}(s) \le \frac{2L(q-1)\log_q s}{s^2}(1 + o(1)), \quad s \to \infty. \tag{4.3.2}$$

Принимая во внимание очевидное неравенство $R_L(s) \le R_L^{(2)}(s)$, получаем довольно важное следствие из теоремы 4.3.1, означающее, что при больших значениях параметра s преимущество по скорости двоичных СД s_L-гиперкодов над СД s_L-кодами исчезает.

Следствие 4.3.1. *При фиксированном $L \ge 1$ и $s \to \infty$ имеет место асимптотическое равенство*

$$R_L^{(2)}(s) = R_L(s)(1 + o(1)), \quad s \to \infty.$$

Доказательство теоремы 4.3.1

Вывод границ в теореме 4.3.1 основан на следующей лемме 4.3.1, которая очевидным образом доказывается от противного.

Лемма 4.3.1. *Пусть X_q – q-ичный СД s_L-гиперкод длины N и объема t. Тогда двоичный код X_2', полученный из кода X_q с помощью стандартной замены* [35] *каждого q-ичного символа a, $a \in \mathcal{A}_q$, в коде X_q на двоичный столбец длины q, имеющий вес 1 и содержащий свой единственный символ 1 на позиции с номером $a + 1$, является равновесным СД s_L-кодом длины qN, объема t и веса N.*

Доказательство утверждения 1. Неравенство $R_L^{(q)}(s) \le \frac{q}{\log_2 q} R_L(s)$ является прямым следствием из леммы 4.3.1. Докажем теперь, что $R_L^{(q)}(s) \le \frac{q-1}{\log_2 q} R_L(s-1)$. Рассмотрим произвольный q-ичный СД s_L-гиперкод X_q, и пусть X_2' – равновесный СД s_L-код длины qN, объема t и веса N, построенный в формулировке леммы 4.3.1. Тогда двоичный код X_2'' длины $(q-1)N$ и объема $t-1$, построенный путем удаления из X_2' кодового слова $\boldsymbol{x}(1)$ и всех строк x_i, $i \in [N]$, где двоичный символ $x_i(1) = 1$, является СД $(s-1)_L$-кодом. Таким образом, (4.3.1) доказано.

Доказательство утверждения 2. Воспользуемся разработанной в [44] и приведенной в теореме 1.3.2 верхней границей на скорость СД s_L-кодов $\overline{R}_L(s)$, асимптотическое поведение которой при $s \to \infty$ для любого фиксированного $L \ge 1$ исследовано:

$$\overline{R}_L(s) = \frac{2L \log_2 s}{s^2}(1 + o(1)).$$

Перейдем в неравенстве (4.3.1) к пределу $s \to \infty$ и подставим приведенную выше асимптотику в качестве верхней границы для $R_L(s)$. В результате получим (4.3.2). $\square$

4.4 Сравнение границ и таблицы наилучших значений

Результаты сравнения всех известных границ скорости q-ичных СД s_1-гиперкодов в случаях $q = 2$ и $q = 3$ представлены в таблице 4.4.1. Как видно, теорема 4.3.1 дает лучший результат среди верхних границ для достаточно больших значений параметра s. Что касается нижних границ, то в двоичном случае большая часть наилучших значений получена с помощью теоремы 4.2.2, а при $q = 3$ – с помощью теоремы 4.2.1.

Для произвольного фиксированного $q \ge 2$ и $s \to \infty$ нижние границы, полученные в работах [39, 40] для q-ичных СД s_1-гиперкодов имеют асимптотики

$$\frac{q-1}{s^2 e \ln q}(1 + o(1)) \quad \text{и} \quad O\left(\frac{1}{s}\left(1 - \frac{1}{q}\right)^s\right),$$

соответственно. Как видим, граница (4.2.4) в теореме 4.2.1 превосходит приведенные выше значения. Наилучший результат среди верхних границ при $s \to \infty$ дает граница (4.3.2) из теоремы 4.3.1, действительно, большинство верхних границ имеют асимптотику $O(1/s)$ [20, 43, 12], а асимптотика верхней границы, полученной в [39], превышает (4.3.2) в 2 раза.

Замечание 4.4.1. При $s \to \infty$ между наилучшими известными асимптотиками среди верних границ (4.3.2) и среди нижних границ (4.2.4) есть существенный разрыв:

$$\frac{(4.3.2)}{(4.2.4)} = 2(\log_2 e)(\log_2 s)(1 + o(1)), \quad s \to \infty.$$

В случае $L > 1$ численные значения нижних границ (4.2.9)-(4.2.10) для $q = 2$ и (4.2.1)-(4.2.3) для $q = 3$ представлены в таблице 4.4.2, в которой через $Q_L(s)$ обозначен аргумент максимума в (4.2.9), а через $q'_L(s)$ – оптимальный объем алфавита в (4.2.1). Отметим, что найденная нижняя граница (4.2.9)-(4.2.10) улучшает границу случайного кодирования, полученную на ансамбле кодов с независимыми одинаково распределенными двоичными компонентами кодовых слов [38]. Более того, при малых $s \ge 2$ и $L \ge 1$ значения нижней границы (4.2.9)-(4.2.10) превышают соответствующие значения нижней границы случайного кодирования $\underline{R}_L(s)$ на скорость СД s_L-кодов (см. таблицу 1.2.1), а также значения

границы $\underline{R}_L^{(2)}(s)$ (4.2.1)-(4.2.3) из теоремы 4.2.1. Однако, при больших значениях параметров s и L указанные различия с $\underline{R}_L(s)$ и $\underline{R}_L^{(2)}(s)$ несущественны, это объясняется и тем, что при $L \to \infty$ предел $\underline{R}_L^*(s)$ (4.2.12) равен пределу $\underline{R}_L(s)$ [44], асимптотика (4.2.13) совпадает с (4.2.5), и при $s \to \infty$ асимптотика $\underline{R}_L^*(s)$ ограничена снизу выражением (4.2.11), совпадающим с асимптотиками $\underline{R}_L(s)$ [44] и $\underline{R}_L^{(2)}(s)$ (4.2.4). Мы полагаем, что знак неравенства в (4.2.11) можно заменить на знак равенства.

Замечание 4.4.2. Напомним [20], что при фиксированном s и $q \to \infty$ предел скорости q-ичных СД s_1-гиперкодов в точности равен $\lim_{q\to\infty} R_1^{(q)}(s) = 1/s$. Формула (4.2.6) в теореме 4.2.1 обобщает нижнюю границу $(1 + o(1))/s$ на случай $L \geq 1$. Однако верхняя граница из теоремы 4.3.1, основанная на (4.3.1), стремится к ∞ при $q \to \infty$ и фиксированных s, L. Нашей гипотезой является справедливость неравенства $R_L^{(q)}(s) \leq L/(s + L - 1)$. Ниже мы приводим численные значения верхней границы, полученной из (4.3.1), только при $L = 1$, так как считаем, что при фиксированном s и $L > 1$ верхняя граница (4.3.1) может быть значительно улучшена.

Таблица 4.4.1: Наилучшие границы скорости двоичных и троичных СД s_1-гиперкодов

s_1	2_1	3_1	4_1	5_1	6_1
$q = 2$					
Нижняя граница	$0.2075^{2,3,4,6}$	0.0800^{3}	0.0439^{3}	0.0279^{3}	0.0194^{3}
Верхняя граница	0.5^{4}	0.3219^{1}	0.1993^{1}	0.1405^{1}	0.1057^{1}
$q = 3$					
Нижняя граница	$0.2675^{2,5,6}$	$0.1066^{2,6}$	0.0502^{2}	0.0327^{2}	0.0230^{2}
Верхняя граница	0.5^{4}	0.3333^{4}	0.25^{4}	0.1772^{1}	0.1333^{1}

[1] Теорема 4.3.1 [2] Теорема 4.2.1 [3] Теорема 4.2.2 [4] [20] [5] [39] [6] [40]

Таблица 4.4.2: Численные значения нижних границ $\underline{R}_L^*(s)$ и $\underline{R}_L^{(3)}(s)$

s_L	2_2	3_2	4_2	5_2	6_2
$\underline{R}_L^*(s)$ $(Q_L(s))$	0.2457 (0.28)	0.1153 (0.18)	0.0684 (0.14)	0.0456 (0.12)	0.0325 (0.10)
$\underline{R}_L^{(3)}(s)$ $(q'_L(s))$	0.3333 (3)	0.1441 (3)	0.0786 (8)	0.0532 (10)	0.0387 (10)
s_L	2_3	3_3	4_3	5_3	6_3
$\underline{R}_L^*(s)$ $(Q_L(s))$	0.2635 (0.24)	0.1348 (0.17)	0.0838 (0.13)	0.0575 (0.11)	0.0420 (0.09)
$\underline{R}_L^{(3)}(s)$ $(q'_L(s))$	0.3553 (3)	0.1563 (3)	0.0964 (8)	0.0674 (10)	0.0498 (10)
s_L	2_4	3_4	4_4	5_4	6_4
$\underline{R}_L^*(s)$ $(Q_L(s))$	0.2744 (0.23)	0.1470 (0.16)	0.0941 (0.13)	0.0660 (0.11)	0.0490 (0.09)
$\underline{R}_L^{(3)}(s)$ $(q'_L(s))$	0.3635 (3)	0.1629 (6)	0.1083 (8)	0.0774 (10)	0.0582 (12)
s_L	2_5	3_5	4_5	5_5	6_5
$\underline{R}_L^*(s)$ $(Q_L(s))$	0.2819 (0.22)	0.1552 (0.16)	0.1014 (0.12)	0.0723 (0.10)	0.0544 (0.09)
$\underline{R}_L^{(3)}(s)$ $(q'_L(s))$	0.3667 (3)	0.1716 (6)	0.1166 (8)	0.0849 (10)	0.0647 (12)
s_L	2_6	3_6	4_6	5_6	6_6
$\underline{R}_L^*(s)$ $(Q_L(s))$	0.2874 (0.22)	0.1611 (0.15)	0.1068 (0.12)	0.0771 (0.10)	0.0587 (0.09)
$\underline{R}_L^{(3)}(s)$ $(q'_L(s))$	0.3681 (3)	0.1782 (8)	0.1227 (8)	0.0905 (10)	0.0698 (12)

4.5 Кодирование недоопределенных данных

Согласно терминологии в работе [9], будем различать *полностью определенные* символы – элементы множества $[t] = \{1, 2, \ldots, t\}$, и *недоопределенные* символы – непустые множества, состоящие из полностью определенных символов. *Недоопределенными данными* будем называть последовательность недоопределенных символов. Другими словами, понятие последовательности недоопределенных символов эквивалентно нашему определению гиперслова.

Рассмотрим задачу *архивации* недоопределенных данных [9], которую можно сформулировать как задачу экономного кодирования гиперслова $U \triangleq (U_1, U_2, \ldots, U_n)$, $U_k \subseteq [t]$, $U_k \neq \emptyset$, $k \in [n]$, при котором имеется возможность полностью восстановить исходное гиперслово U по кодовой последовательности. К такой постановке приводит задача хранения недоопределенных данных. Один из достаточно компактных методов такого кодирования основывается на следующем *посимвольном* кодировании гиперслова U с помощью q-ичного СД s_1-гиперкода (в работе [9] рассматривается частный случай применения двоичного гиперкода). Зафиксируем некоторый q-ичный СД s_1-гиперкод X_q (4.1.1) объема t и длины N. Если на k-той позиции, $k \in [n]$, гиперслова U стоит либо подмножество $U_k \subseteq [t]$ мощности $|U_k|$, $1 \leq |U_k| \leq s$, либо само множество $[t]$, то в качестве кодового слова для символа U_k примем гиперсумму $\langle \boldsymbol{x}(j), j \in U_k \rangle$. Таким образом, впоследствии для восстановления символа U_k достаточно найти кодовые слова из X_q, которые подчинены данной гиперсумме. Такой метод архивации, основанный на посимвольном кодировании-декодировании имеет ряд достоинств. Во-первых, для посимвольного декодирования последовательности гиперсумм

$$\langle \boldsymbol{x}(j), j \in U_1 \rangle, \langle \boldsymbol{x}(j), j \in U_2 \rangle, \ldots, \langle \boldsymbol{x}(j), j \in U_n \rangle \tag{4.5.1}$$

не требуется много памяти, достаточно располагать лишь матрицей X_q с t столбцами, в то время как при каждом $k \in [n]$, число различных подмножеств $U_k \subseteq [t]$ мощности $|U_k|$, $1 \leq |U_k| \leq s$, с учетом самого множества $[t]$, которые можно закодировать гиперсуммами $\langle \boldsymbol{x}(j), j \in U_k \rangle$, достигает $\sum\limits_{i=1}^{\min(s,q)} \binom{t}{i} + 1 \gg t$. Во-вторых, время декодирования каждой гиперсуммы (4.5.1) линейно по t, и декодеру не требуется перебирать всевозможные s-подмножества множества $[t]$. Отметим [9], что для решения задачи посимвольного кодирования-декодирования можно также применять аналогичные дизъюнктивные СД s_1-коды. Более компактный метод, обобщающий алгоритм кодирования-декодирования на случай $L \geq 1$ и приведенный ниже, также очевидно работает и в случае СД s_L-кодов. Причем способ, основанный на СД s_L-кодах более целесообразен, так как приводит к двоичному представлению гиперслова, а различие по скорости двоичных СД s_L-гиперкодов и СД s_L-кодов при больших значениях параметра s несущественно по следствию 4.3.1. Факт о целесообразности использования СД s_1-кодов в силу следствия 4.3.1 также отмечен Л.А. Шоломовым, автором оригинального метода, в недавнем докладе [10].

Пусть $L > 1$ и существует q-ичный СД s_L-гиперкод

$$X_q = \left\{ \boldsymbol{x}(j) \,:\, \boldsymbol{x}(j) \in \mathcal{A}_q^{N_L} = \{0, 1, \ldots, q-1\}^{N_L},\, j \in [t] \right\}, \tag{4.5.2}$$

имеющий объем t и длину N_L, $N_L < N - (s + L - 1)$, где N – минимальная длина s_1-гиперкода объема t. Тогда можно применить следующее улучшение изложенного выше метода посимвольного кодирования-декодирования гиперслова $U = (U_1, U_2, \ldots, U_n)$, $U_k \subseteq [t]$, $|U_k| \leq s$, $k \in [n]$. Заметим, что в данном случае гиперсумма $\langle \boldsymbol{x}(j), j \in U_k \rangle$, $k \in [n]$,

получаемая с помощью СД s_L-гиперкода (4.5.2) для символа U_k, подчиняет не более $s + L - 1$ кодовых слов кода X. Обозначим эти кодовые слова через $\boldsymbol{x}(d_1), \boldsymbol{x}(d_2), \ldots, \boldsymbol{x}(d_l)$, $l \le s + L - 1$, считая для определенности, что $d_1 < d_2 < \cdots < d_l$. Подмножество $U_k \subseteq [t]$ будем кодировать составной последовательностью

$$Z(k) \triangleq \big(\langle \boldsymbol{x}(j), j \in U_k\rangle\,;\, (y_1, y_2, \ldots, y_{s+L-1})\big)$$

длины $N_L + s + L - 1 < N$, где

$$\forall j \in [s + L - 1] \quad y_j \triangleq \begin{cases} 1, & \text{если } j < l \text{ и } d_j \in U_k, \\ 0, & \text{иначе.} \end{cases}$$

Другими словами, к гиперсумме $\langle \boldsymbol{x}(j), j \in U_k\rangle$ длины N_L добавим двоичный вектор индикаторов длины $(s + L - 1)$, определяющий какие кодовые слова из списка декодирования являются искомыми. Очевидно, что символ U_k однозначно восстанавливается по гиперслову $Z(k)$, которое имеет длину $N_L + s + L - 1 < N$, т.е. длину меньшую, чем длина s_1-гиперкода в предыдущем методе. При этом асимптотические расходы на память и временная сложность алгоритма декодирования не увеличиваются.

Заключение

В настоящей диссертационной работе доказаны новые границы для асимптотической скорости некоторых семейств комбинаторных кодов. В частности, доказана новая нижняя граница асимптотической скорости $R_L(s)$ дизъюнктивных кодов со списочным декодированием, которая улучшает ранее известные нижние границы при $L > 1$. Также получены новые нижние и верхние границы асимптотической скорости $R_L^{(q)}(s)$ гиперкодов со списочным декодированием, превосходящие ранее известные границы для широкого набора параметров. Тем не менее, между наилучшими нижними и верхними границами как скорости $R_L(s)$, так и скорости $R_L^{(q)}(s)$, остался существенный разрыв в асимптотике при $s \to \infty$. Асимптотика наилучших нижних границ равна $O(1/s^2)$, а верхних – $O(\ln s/s^2)$. Нахождение главного члена асимптотики скорости $R_L(s)$ (и $R_L^{(q)}(s)$) представляет из себя интересную задачу для дальнейших исследований.

В работе также получена и исследована нижняя граница для экспоненты ошибки почти дизъюнктивных кодов со списочным декодированием, которая обосновывает существование двухступенчатой процедуры групповых проверок в дизъюнктивной модели поиска дефектов с заданным значением экспоненциального убывания ошибки при росте числа элементов. Для почти дизъюнктивных кодов со списочным декодированием доказана верхняя граница на пропускную способность.

Разработан новый алгоритм для проверки, что количество дефектных элементов превышает заданный порог в дизъюнктивной модели группового тестирования. Этот алгоритм, в отличие от ранее известных, обеспечивает меньшую ошибку проверки при проведении неадаптивных групповых тестов для достаточно большого количества элементов. Остается открытой задача построения нижней границы на минимальное количество тестов при заданной ошибке.

Литература

[1] *Бассалыго Л.А.*, *Рыков В.В.*, Гиперканал множественного доступа, *Пробл. передачи информ.*, Т. 49, № 4, С. 3-12, 2013.

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

[3] *Дьячков А.Г.*, *Рыков В.В.*, Применение кодов для канала с множественным доступом в системе связи АЛОХА, *Тр. VI Всесоюзной школы-семинара по вычислительным сетям. Москва - Винница.*, Т. 4, С. 18-24, 1981.

[4] *Дьячков А.Г.*, *Рыков В.В.*, Границы длины дизъюнктивных кодов, *Пробл. передачи информ.*, Т. 18, № 3, С. 7-13, 1982.

[5] *Зубашич В.Ф.*, *Лысянский А.В.*, *Малютов М.Б.*, Блочно рандомизированный метод построения распределительных систем технической диагностики, *Изв. АН СССР, Техн. киб.*, т. 6, 1976.

[6] *Малютов М.Б.*, Разделяющее свойство случайных матриц, *Матем. заметки*, Т. 23, № 1, С. 155-167, 1978.

[7] *Фрейдлина В.Л.*, Об одной задаче планирования отсеивающих экспериментов, *Теор. вер. и ее приложения*, Т. 20, № 1, С. 100-114, 1975.

[8] *Чисар И.*, *Кернер Я.*, Теория информации. Теоремы кодирования для дискретных систем без памяти. Мир, Москва, 1985.

[9] *Шоломов Л.А.*, Двоичные представления недоопределенных данных и дизъюнктивные коды, *Прикладная дискретная математика*, № 1, С. 17-33, 2013.

[10] *Шоломов Л.А.*, Две постановки задачи кодирования недоопределенных данных, *Мат. XII Межд. семинара "Дискретная математика и ее приложения" имени академика О.Б. Лупанова, Москва*, С. 35-45, 2016.

[11] *Bazrafshan M.*, *van Trung T.*, Improved bounds for separating hash families, *Des. Codes Cryptogr.*, vol. 69, no. 3, pp. 369-382, 2013.

[12] *Blackburn S.R.*, Frameproof codes, *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499-510, 2003.

[13] *Blackburn S.R.*, Probabilistic Existence Results for Separable Codes, *IEEE Trans. Inform. Theory*, vol. 61, no. 11, pp. 5822-5827, 2015.

[14] *Berger T.*, *Levenshtein V.I.*, Asymptotic Efficiency of Two-Stage Disjunctive Testing, *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 1741-1749, 2002.

[15] *Boneh D.*, *Shaw J.*, Collusion-secure fingerprinting for digital data, *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897-1905, 1998.

[16] *Chang S.-C.*, *Wolf J.*, On the T-user M-frequency noiseless multiple-access channel with and without intensity information, *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 41-48, 1981.

[17] *Cheng M.*, *Miao Y.*, On Anti-Collusion Codes and Detection Algorithms for Multimedia Fingerprinting, *IEEE Trans. Inform. Theory*, vol. 57, no. 7, pp. 4843-4851, 2011.

[18] *Cheng Y.X.*, *Du D.Z.*, New Constructions of One- and Two-Stage Pooling Designs, *J. Comput. Biology*, vol. 15, no. 2, pp. 195-205, 2008.

[19] *Cheng Y.*, *Xu Y.*, An efficient FPRAS type group testing procedure to approximate the number of defectives, *J. Combin. Optim.*, vol. 27, no. 2, pp. 302-314, 2014.

[20] *Cohen G.D.*, *Schaathun H.G.*, Asymptotic overview on separating codes, *Tech. Report 248*, Department of Informatics, University of Bergen, Bergen, Norway, 2003.

[21] *Damaschke P.*, *Muhammad A.S.*, Competitive group testing and learning hidden vertex covers with minimum adaptivity, *Discrete Math. Algorithm. Appl.*, vol. 2, no. 3, pp. 291-311, 2010.

[22] *Damaschke P.*, *Muhammad A.S.*, *Wiener G.*, Strict group testing and the set basis problem, *J. Combin. Theory, Ser. A*, vol. 126, pp. 70-91, 2014.

[23] *De Bonis A.*, *Gasieniec L.*, *Vaccaro U.*, Optimal Two-Stage Algorithms for Group Testing Problems, *SIAM J. Comput.*, vol. 34, no. 5, pp. 1253-1270, 2005.

[24] *Dorfman R.*, The Detection of Defective Members of Large Populations, *Ann. Math. Statist.*, vol. 14, no. 4, pp. 436-440, 1943.

[25] *D'yachkov A.G.*, *Rykov V.V.*, A Survey of Superimposed Code Theory, *Problems of Control and Inform. Theory*, vol. 12, no. 4, pp. 229-242, 1983.

[26] *D'yachkov A.G.*, *Rykov V.V.*, *Rashad A.M.* Superimposed Distance Codes, *Problems of Control and Inform. Theory*, vol. 18, no. 4, pp. 237-250, 1989.

[27] *D'yachkov A.G.*, *Macula A.J.*, *Rykov V.V.*, New constructions of superimposed codes, *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 284-290, 2000.

[28] *D'yachkov A.G.* Lectures on Designing Screening Experiments, *Lecture Note Series 10*, Combinatorial and Computational Mathematics Center, Pohang University of Science and Technology (POSTECH), Korea Republic, Feb. 2003 (survey, 112 pages). http://arxiv.org/pdf/1401.7505

[29] *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*, vol. 33, no. 2, pp. 158-166, 1982.

[30] *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.*, vol. 51, no. 1, pp. 79-89, 1985.

[31] *Falahatgar M.*, *Jafarpour A.*, *Orlitsky A.*, *Pichapati V.*, *Suresh A.T.*, Estimating the Number of Defectives with Group Testing, *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, pp. 1376-1380, 2016.

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

[33] *Gao F.*, *Ge G.*, New Bounds on Separable Codes for Multimedia Fingerprinting, *IEEE Trans. Inform. Theory*, vol. 60, no. 9, pp. 5257-5262, 2014.

[34] *Hartung G.*, *Kaidel B.*, *Koch A.*, *Koch J.*, *Rupp A.*, Fault-Tolerant Aggregate Signatures, *Public-Key Cryptography – PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, Proceedings, Part I*, 2016.

[35] *Kautz W.H.*, *Singleton R.C.*, Nonrandom Binary Superimposed Codes, *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 363-377, 1964.

[36] *Macula A.J.*, *Rykov V.V.*, *Yekhanin S.*, Trivial two-stage group testing for complexes using almost disjunct matrices, *Discret. Appl. Math.*, vol. 137, no. 1, pp. 97-107, 2004.

[37] *Mezard M.*, *Toninelli C.*, Group Testing With Random Pools: Optimal Two-Stage Algorithms, *IEEE Trans. Inform. Theory*, vol. 57, no. 3, pp. 1736-1745, 2011.

[38] *Rashad A.M.*, On Symmetrical Superimposed Codes, *J. Inf. Process. Cybern EIK 29*, vol. 7, pp. 337-341, 1989.

[39] *Shangguan C.*, *Wang X.*, *Ge G.*, *Miao Y.*, New Bounds For Frameproof Codes, Preprint, 2014. http://arxiv.org/pdf/1411.5782v1.

[40] *Stinson D.R.*, *Wei R.*, *Chen K.*, On generalized separating hash families, *J. Combin. Theory, Ser. A*, vol. 115, no. 1, pp. 105-120, 2008.

[41] *van Trung T.*, A tight bound for frameproof codes viewed in terms of separating hash families, *Des. Codes Cryptogr.*, vol. 72, no. 3, pp. 713-718, 2014.

[42] *Vilenkin P.A.*, On Constructions of List-Decoding Superimposed Codes, *Proc. 6th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-6), Pskov, Russia*, pp. 228-231, 1998.

[43] *Vinck A.J. Han*, *Martirossian S.*, On Superimposed Codes, Numbers, Information and Complexity, Springer US, pp. 325-331, 2000.

Публикации автора

[44] *Дьячков А.Г.*, *Воробьев И.В.*, *Полянский Н.А.*, *Щукин В.Ю.*, Границы скорости дизъюнктивных кодов, *Пробл. передачи информ.*, Т. 50, № 1, С. 31-63, 2014.

[45] *Дьячков А.Г.*, *Воробьев И.В.*, *Полянский Н.А.*, *Щукин В.Ю*, Почти дизъюнктивные коды со списочным декодированием, *Пробл. передачи информ.*, Т. 51, № 2, С. 27-49, 2015.

[46] *Щукин В.Ю*, Списочное декодирование для гиперканала множественного доступа, *Пробл. передачи информ.*, Т. 52, № 4, С. 14-30, 2016.

[47] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Symmetric Disjunctive List-Decoding Codes, *Des. Codes Cryptogr.*, http://dx.doi.org/10.1007/s10623-016-0278-4, pp. 1-19, 2016.

[48] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Almost Cover-Free Codes and Designs, *Des. Codes Cryptogr.*, http://dx.doi.org/10.1007/s10623-016-0279-3, pp. 1-17, 2016.

[49] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Cover-Free Codes and Separating System Codes, *Des. Codes Cryptogr.*, http://dx.doi.org/10.1007/s10623-016-0265-9, pp. 1-13, 2016.

[50] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Bounds on the Rate of Superimposed Codes, *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, pp. 2341-2345, 2014.

[51] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Symmetric Disjunctive List-Decoding Codes, *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, pp. 2236-2240, 2015.

[52] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Almost Cover-Free Codes and Designs, *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, pp. 2899-2903, 2015.

[53] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Cover-Free Codes and Separating System Codes, *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, pp. 2894-2898, 2015.

[54] *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. Symp. Inf. Theory*, Barcelona, pp. 1183-1187, 2016.

[55] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, On Multistage Learning a Hidden Hypergraph, *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, pp. 1178-1182, 2016.

[56] *D'yachkov A.G.*, *Vorobyev I.V.*, *Polyanskii N.A.*, *Shchukin V.Yu.*, Threshold Decoding for Disjunctive Group Testing, *Proc. 15th Int. Workshop on Algebraic and Combinatorial Coding Theory*, Albena, pp. 151-156, 2016.