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

На правах рукописи
УДК 519.2, 621.391.15

ВОРОБЬЕВ Илья Викторович

Разделяющие коды

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 темы и история вопроса

В настоящей диссертации рассматриваются задачи, лежащие на стыке теории вероятностей, теории информации и комбинаторной теории кодирования. Первая глава диссертации посвящена исследованию разделяющих кодов. Коду X мощности t и длины N сопоставим матрицу размера $N \times t$, столбцами которой служат кодовые слова кода X. Код X называется *разделяющим* (s, ℓ)*-кодом*, если в соответствующей ему матрице для для любых двух непересекающихся множеств столбцов $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует такая строка (координата) i, что в ней множества символов из столбцов $\mathcal{S}$ и $\mathcal{L}$ не пересекаются. Будем говорить, что такая координата i *разделяет* множества слов $\mathcal{S}$ и $\mathcal{L}$.

В случае двоичных разделяющих кодов определение может быть переформулировано следующим образом. Код X называется *двоичным разделяющим* (s, ℓ)*-кодом*, если для любых двух непересекающихся множеств $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует такая координата i, для которой выполнено одно из следующих условий

$$x_i = 0 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 1 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}$$

или

$$x_i = 1 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 0 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}.$$

Скоростью q-ичного кода X длины N и мощности t будем называть величину $R = \frac{\log_q t}{N}$. Определим *асимптотическую верхнюю и нижнюю скорости* разделяющих (s, ℓ)-кодов как

$$\overline{R}_s^{(q)}(s, \ell) = \varlimsup_{t \to \infty} \frac{\log_q t}{N^{(q)}(t, s, \ell)}, \qquad \underline{R}_s^{(q)}(s, \ell) = \varliminf_{t \to \infty} \frac{\log_q t}{N^{(q)}(t, s, \ell)}, \tag{1}$$

где число $N^{(q)}(t, s, \ell)$ равно минимальной длине q-ичного разделяющего (s, ℓ)-кода мощности t. Асимптотические скорости двоичных кодов будем обозначать просто $\overline{R}_s(s, \ell)$ и $\underline{R}_s(s, \ell)$.

Двоичные разделяющие (2, 2)-коды были впервые введены Ю.Л. Сагаловичем в 1965 году в статье [7]. Начало этим исследованиям по разделяющим кодам положили проблемы противогоночного кодирования состояний дискретных автоматов. В 1969 году в работе А. Фридмана и др. [36] понятие двоичных разделяющих (2, 2)-кодов было обобщено до двоичных разделяющих (s, ℓ)-кодов. В этой же работе была получена первая нижняя граница

$$\underline{R}_s(s, \ell) \geqslant \frac{-\log_2(1 - 2^{1-s-\ell})}{s + \ell}. \tag{2}$$

В работе [6] 1972-го года М.С. Пинскер и Ю.Л. Сагалович стали рассматривать q-ичные разделяющие коды и доказали следующую нижнюю оценку асимптотической скорости линейных разделяющих (2, 2)-кодов

$$\underline{R}_s^{(q)} \geqslant \frac{-\log_q(1 - \beta)}{3}, \quad \beta = 1 - 4/q + 6/q^2 - 3/q^3. \tag{3}$$

Позднее, в [11] Ю.Л. Сагаловичем было показано, что эта граница верна для произвольных, а не только для линейных кодов.

В статьях Ю.Л. Сагаловича [8, 9] была доказана верхняя оценка асимптотической скорости

$$\overline{R}_s(2, 2) < 0.3045. \tag{4}$$

Эта оценка опирается на верхнюю границу $\overline{R}(\delta)$ скоростей кодов с фиксированным отношением расстояния и длины. Приведенное выше значение было получено с помощью границы Элайеса. В работе [39] Дж. Кернер и Г. Симоньи повторили рассуждение Ю.Л. Сагаловича из [8, 9] и, воспользовавшись наилучшей известной границей для величины $\overline{R}(\delta)$ Р. Макэлиса и др. из [42], получили оценку

$$\overline{R}_s(2, 2) < 0.2835, \tag{5}$$

которая не улучшена до сих пор.

Новая волна интереса к разделяющим кодам возникла благодаря статье Д. Боне и Д. Шоу [17] 1998 года, посвященной задаче защиты авторских прав, где могут быть применены разделяющие $(s, 1)$-коды и (s, s)-коды.

Наилучшие границы скорости для многих значений параметров s и ℓ доказаны с помощью неравенств, связывающих скорости разделяющих, свободных от перекрытий и полностью разделяющих кодов.

Код X называется *полностью разделяющим* (s, ℓ)*-кодом*, если для любых двух непересекающихся множеств $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует две координаты i и j, для которых выполнены следующие условия

$$x_i = 0 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 1 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}$$

и

$$x_j = 1 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_j = 0 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}.$$

Двоичный код X называется *свободным от перекрытий* (s,ℓ)*-кодом*, если для любых двух непересекающихся множеств $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует координата i, для которой

$$x_i = 0 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 1 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}.$$

Полностью разделяющие коды впервые появились в 1973 году в работе Г. Маго [41]. Эти коды, как и разделяющие, используются в теории автоматов. Свободные от перекрытий коды были введены К. Митчеллом и Ф. Пайпером в 1988 году в работе [43] в связи с криптографической задачей распределения ключей, описание которой можно также найти в статье В.С. Лебедева [4] или статье В.М. Сидельникова и О.Ю. Приходова [13]. Асимптотические скорости полностью разделяющих и свободных от перекрытий кодов определяются аналогично скорости разделяющих кодов

$$\overline{R}_{cs}(s,\ell) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N_{cs}(t,s,\ell)}, \qquad \underline{R}_{cs}(s,\ell) = \varliminf_{t\to\infty} \frac{\log_2 t}{N_{cs}(t,s,\ell)},$$

$$\overline{R}_{cf}(s,\ell) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N_{cf}(t,s,\ell)}, \qquad \underline{R}_{cf}(s,\ell) = \varliminf_{t\to\infty} \frac{\log_2 t}{N_{cf}(t,s,\ell)},$$

где числа $N_{cs}(t,s,\ell)$ и $N_{cf}(t,s,\ell)$ равны соответственно минимальным длинам полностью разделяющего и свободного от перекрытий кода мощности t.

Непосредственно из определений следуют следующие неравенства

$$\begin{aligned} \overline{R}_{s}(s,\ell)/2 \leqslant \overline{R}_{cs}(s,\ell) \leqslant \overline{R}_{cf}(s,\ell) \leqslant \overline{R}_{s}(s,\ell), \\ \underline{R}_{s}(s,\ell)/2 \leqslant \underline{R}_{cs}(s,\ell) \leqslant \underline{R}_{cf}(s,\ell) \leqslant \underline{R}_{s}(s,\ell). \end{aligned} \tag{6}$$

В работе Г. Коэна и Г. Шаатуна 2003 года [19] представлены неравенства

$$\begin{aligned} \overline{R}_{cs}(s,\ell) \leqslant \overline{R}\left(\frac{2\overline{R}_{cs}(s,\ell)}{\overline{R}_{cs}(s-1,\ell-1)}\right), \\ \overline{R}_{s}(s,\ell) \leqslant \overline{R}\left(\frac{\overline{R}_{s}(s,\ell)}{\overline{R}_{cs}(s-1,\ell-1)}\right), \end{aligned} \tag{7}$$

где $\overline{R}(\delta)$ — оценка асимптотической скорости произвольного кода с фиксированным отношением кодового расстояния к длине кода из работы Р. Макэлиса и др. [42]. Рекурсивное применение этих неравенств позволило авторам получить верхние оценки скоростей двоичных разделяющих и полностью разделяющих кодов для малых значений параметров s и ℓ, многие из которых остаются наилучшими до сих пор.

Асимптотическое поведение величин $\overline{R}_s(s,\ell)$ и $\underline{R}_s(s,\ell)$ при $s\to\infty$ и фиксированном ℓ следует из границ для свободных от перекрытий кодов и неравенства (2)

$$\frac{\ell^\ell \log_2 e}{e^\ell}\frac{1}{s^{\ell+1}}(1+o(1)) \leqslant \underline{R}_{cf}(s,\ell),$$

$$\overline{R}_{cf}(s,\ell) \leqslant \frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}}\frac{\log_2 s}{s^{\ell+1}}(1+o(1)), \quad s\to\infty. \tag{8}$$

Верхняя оценка была доказана А.Г. Дьячковым и др. в [34] с помощью рекуррентных неравенств, установленных ранее В.С. Лебедевым в [4]

$$\overline{R}_{cf}(s,\ell) \leqslant \frac{\overline{R}_{cf}(s-i,\ell-j)}{\overline{R}_{cf}(s-i,\ell-j)+\frac{(i+j)^{i+j}}{i^i\cdot j^j}}, \quad i\in[s-1],\, j\in[\ell-1].$$

Нижняя оценка была получена Н. Куонгом и Т. Зейселем в 1988 году в статье [44] с помощью метода случайного кодирования на некотором специальном ансамбле с независимыми двоичными равновесными словами.

Множество результатов было получено специально для наиболее важных для задачи защиты авторских прав разделяющих $(s,1)$-кодов и (s,s)-кодов, причем зачастую авторов интересовали результаты для конечных длин, а не асимптотическая скорость. В работе Дж. Стаддон и др. [47] были установлены границы

$$t \leqslant s(q^{\lceil \frac{N(t,s,1)}{s}\rceil}-1),$$

$$t \leqslant q^{\lceil \frac{N(t,s,s)}{s}\rceil}+2s-2,$$

откуда следуют оценки для асимптотической скорости

$$\overline{R}_s^{(q)}(s,1)\leqslant\frac{1}{s}, \quad \overline{R}_s^{(q)}(s,s)\leqslant\frac{1}{s}.$$

В работе Д. Стинсона и др. [48] было показано, что

$$t \leqslant 4q^{\lceil \frac{N(t,2,2)}{3}\rceil}-3,$$

а в [49] Д. Стинсоном и Г. Заверухой этот результат был обобщен до

$$t \leqslant q^{\lceil \frac{N(t,s,s)}{2s-1}\rceil}+(s-1)(2s-1)(q^{\lceil \frac{N(t,s,s)}{2s-1}\rceil}-1).$$

Для общего случая разделяющих (s,ℓ)-кодов в [50] Д. Стинсоном и Г. Заверухой была доказана граница

$$t \leqslant (2s\ell-w)q^{\lceil \frac{N(t,s,\ell)}{s+\ell-1}\rceil}-2s\ell+s+1,$$

что дает следующую оценку для асимптотической скорости

$$\overline{R}_s^{(q)}(s,\ell) \leqslant \frac{1}{s+\ell-1}.$$

Вместе с достаточно очевидной случайной нижней границей

$$\lim_{q\to\infty} \underline{R}_s^{(q)}(s,\ell) \geqslant \frac{1}{s+\ell-1}$$

это дает нам равенство

$$\lim_{q\to\infty} \underline{R}_s^{(q)}(s,\ell) = \lim_{q\to\infty} \overline{R}_s^{(q)}(s,\ell) = \frac{1}{s+\ell-1}.$$

В недавней работе Ч. Шэнгуэн и др. [46] построили новую границу для разделяющих $(s,1)$-кодов

$$t \leqslant q^{\left\lceil \frac{N(t,s,1)(q-1)}{s(s-1)/2} \right\rceil \log_q(eqs(s-1)/(2(q-1))} + s,$$

которая дает следующую оценку для асимптотической скорости

$$\overline{R}_s^{(q)}(s,1) \leqslant \frac{4(q-1)\log_q s}{s^2}(1+o(1)), \qquad s\to\infty.$$

В этой же работе была доказана нижняя граница

$$\underline{R}_s^{(q)}(s,1) \geqslant \frac{q-1}{s^2 e \ln q}(1+o(1)), \qquad s\to\infty.$$

В следующих двух главах настоящей диссертации исследуются два обобщения классических дизъюнктивных кодов. Дизъюнктивные коды являются частным случаем свободных от перекрытий кодов при $\ell = 1$. Дизъюнктивной суммой множества двоичных слов называется двоичное слово, у которого в i-ой позиции стоит 0 в том и только в том случае, если у всех складываемых слов в этой позиции стоит 0. Говорят, что слово $\mathbf{u}$ покрывает слово $\mathbf{v}$, если их дизъюнктивная сумма совпадает со словом $\mathbf{u}$. Двоичный код X называется *дизъюнктивным кодом силы* s, если произвольная дизъюнктивная сумма s слов не покрывает никакое другое слово кода. Ключевое свойство дизъюнктивных кодов заключается в том, что, имея дизъюнктивную сумму не более чем s слов, мы можем эти слова найти.

Дизъюнктивные коды были введены У. Каутсом и Р. Синглтоном в 1964 году в статье [38]. Эти коды имеют множество приложений, обзор которых можно найти в книге Д. Ду и Ф. Хвонга [24] или монографии Ф. Чикалеза [18]. Наиболее известное приложение – это применение дизъюнктивных

кодов в задаче группового тестирования. Асимптотические нижнюю и верхнюю скорости дизъюнктивных кодов $\underline{R}_{cf}(s,1)$ и $\overline{R}_{cf}(s,1)$ будем для краткости обозначать просто $\underline{R}_{cf}(s)$ и $\overline{R}_{cf}(s)$. Из работ А.Г. Дьячкова с В.В. Рыковым [3] и с А.М. Рашадом [28] известно, что выполняются неравенства

$$\frac{\ln 2}{s^2}(1+o(1)) \leqslant \underline{R}_{cf}(s) \leqslant \overline{R}_{cf}(s) \leqslant \frac{2\log_2 s}{s^2}(1+o(1)), \quad s\to\infty.$$

Вторая глава диссертации посвящена дизъюнктивным кодам со списочным декодированием. Двоичный код называется *дизъюнктивным кодом со списочным декодированием силы s и размером списка L* (СД s_L-кодом), если дизъюнктивная сумма любых s кодовых слов покрывает не более $L-1$ других кодовых слов. СД s_L-коды были введены в 1981 году А.Г. Дьячковым и В.В. Рыковым в работе [2], где рассматривалось использование таких кодов при передаче информации через канал множественного доступа в системе связи АЛОХА. В работе П.А. Виленкина 1998 года [51] приведены некоторые конструкции СД s_L-кодов, а также рассмотрено их применение при построении двухступенчатых процедур групповых проверок.

Определим асимптотические верхнюю и нижнюю скорости СД s_L-кодов стандартным образом:

$$\overline{R}_L(s) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,s,L)}, \qquad \underline{R}_L(s) = \varliminf_{t\to\infty} \frac{\log_2 t}{N(t,s,L)},$$

где число $N(t,s,L)$ равно минимальной длине СД s_L-кода мощности t. В работе [29] А.Г. Дьячковым и В.В. Рыковым были получены границы для асимптотической скорости $R_L(s)$, из которых вытекают неравенства

$$\overline{R}_L(s) \leqslant \frac{1}{s}, \quad \text{при любых натуральных } s \text{ и } L,$$

$$\frac{L\log_2 e}{es^2}(1+o(1)) \leqslant \underline{R}_L(s) \leqslant \overline{R}_L(s) \leqslant \frac{2L^2\log_2 s}{s^2}(1+o(1)), \qquad \text{при } s\to\infty.$$

В работе 2005 года А. Де Бонис и др. [23] была улучшена верхняя граница скорости:

$$\overline{R}_L(s) \leqslant \frac{8L\log_2 s}{s^2}(1+o(1)), \qquad s\to\infty.$$

В третьей главе диссертации исследуются почти дизъюнктивные коды, которые являются вероятностным обобщением понятия дизъюнктивных кодов. Впервые они были определены в работе [40] Э. Макулой и др. в 2004-ом году. Будем называть код X *почти дизъюнктивным (s,ε)-кодом*, если доля множеств из s кодовых слов, чья дизъюнктивная сумма покрывает хотя бы одно другое слово, не превосходит ε. Параметр ε может интерпретироваться

как вероятность ошибки декодирования (восстановления s слагаемых, дающих исходную дизъюнктивную сумму).

В работе 2013-го года Л.А. Бассалыго и В.В. Рыкова [1] для некоторого семейства кодов была посчитана вероятность ошибки ε и доказано существование почти дизъюнктивных кодов с параметрами

$$\frac{\log_2 t}{N} = \frac{\ln 2}{s}(1 + o(1)), \quad s^2 = \Theta(N), \quad \varepsilon \to 0, \quad N \to \infty. \tag{9}$$

В данном исследовании нас интересует пропускная способность почти дизъюнктивных кодов при константном s и $N \to \infty$. *Пропускной способностью* $C(s)$ почти дизъюнктивных кодов будем называть точную верхнюю грань скорости кодов, для которых вероятность ошибки ε убывает экспоненциально с ростом длины кода.

Близким к понятию дизъюнктивных кодов является понятие дизъюнктивных планов поиска, которое накладывает несколько более слабые ограничения на код. Код называется *дизъюнктивным планом поиска силы* s, если нет двух разных множеств мощности s с одинаковой дизъюнктивной суммой. Дизъюнктивный план тоже позволяет восстанавливать множество слов по их дизъюнктивной сумме, но для этого нам может потребоваться перебирать все множества слов мощности s. Будем называть код X *почти дизъюнктивным* (s, ε)*-планом*, если доля множеств из s кодовых слов, чья дизъюнктивная сумма совпадает с дизъюнктивной суммой хотя бы одного другого множества мощности s, не превосходит ε. *Пропускной способностью* $C_p(s)$ почти дизъюнктивных s-планов будем называть точную верхнюю грань скорости кодов, для которых вероятность ошибки ε убывает экспоненциально с ростом длины кода. Пропускная величина $C_p(s)$ дизъюнктивных планов поиска была подсчитана М.Б. Малютовым и В.Л. Фрейдлиной в [5]:

$$C_p(s) = \frac{1}{s}.$$

Последняя часть диссертации посвящена многоступенчатому поиску дефектов с помощью групповых проверок. Имеется два основных типа алгоритмов поиска: адаптивные и неадаптивные. В неадаптивных алгоритмах все тесты определены заранее и могут проводиться одновременно, а в адаптивных алгоритмах тесты проводятся последовательно, и при планировании следующего могут быть использованы результаты предыдущих. Многоступенчатые алгоритмы являются промежуточным вариантом между адаптивными и неадаптивными. В них выделяется несколько этапов(ступеней), внутри которых тесты могут проводиться параллельно, но при планировании следующего этапа учитываются результаты предыдущих. Верхней(нижней) асимптотической скоростью поиска $\overline{R}^{(p)}(s)(\underline{R}^{(p)}(s))$ мы будем называть верхний(нижний)

предел отношения двоичного логарифма количества объектов к минимальному необходимому числу тестов для нахождения не более s дефектов за p ступеней. Очевидно, что при росте количества ступеней растет и скорость поиска, минимальную скорость имеют неадаптивные алгоритмы, а максимальную – адаптивные.

Теоретико-информационная граница дает верхнюю оценку $1/s$ на скорость поиска s дефектов для алгоритма с произвольным числом ступеней. Известно, что адаптивные алгоритмы достигают этой границы, а неадаптивные алгоритмы ее не достигают для $s = 2$ (см. работу Д. Копперсмита и Дж. Ширера [20]) и $s \geqslant 11$ (см. статью А.Г. Дьячкова и В.В. Рыкова [3]). Отметим работу П. Дамашке и др. [22], где предложен новый подход к многоступенчатым алгоритмам поиска, основанный на гиперграфах, и доказано существование двухступенчатого алгоритма поиска со скоростью $1/2.44$. Также в другой работе П. Дамашке и Ш. Мухаммада [21] был предложен явный алгоритм со скоростью 0.4.

Цели работы

Целью диссертационной работы являются:

- построение новых верхних и нижних оценок для асимптотической скорости разделяющих кодов;
- построение верхних оценок для асимптотической скорости списочных дизъюнктивных кодов;
- построение нижних оценок для пропускной способности дизъюнктивных кодов;
- исследование многоступенчатых алгоритмов поиска малого числа дефектов.

Научная новизна работы

Все результаты работы являются новыми. В диссертации получены следующие основные результаты.

1. Доказаны новые верхние и нижние границы для асимптотической скорости q-ичных разделяющих кодов.
2. Доказаны новые верхние границы асимптотической скорости списочных дизъюнктивных кодов.

3. Впервые получены границы снизу для пропускной способности $C(s)$ почти дизъюнктивных кодов.

4. Впервые построен алгоритм поиска двух дефектов с конечным числом ступеней, достигающий информационной границы.

5. Впервые явно построен алгоритм поиска произвольного числа дефектов с конечным числом ступеней и ненулевой скоростью.

Методы исследования

В работе используются классические теоретико-вероятностные методы для вычисления асимптотики важных теоретико-информационных характеристик; аналитические методы; методы комбинаторной теории кодирования.

Практическая и теоретическая значимость работы

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

Содержание диссертации

Диссертация состоит из введения, четырех глав, заключения и списка литературы.

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

Первая глава состоит из семи разделов, посвященных границам асимптотических скоростей разделяющих кодов.

В первом разделе первой главы вводятся основные обозначения и даются определения исследуемых объектов.

Во втором разделе указаны основные приложения разделяющих кодов. Подробно описано применение разделяющих $(s, 1)$ и (s, s)-кодов в задаче защиты авторских прав (в англоязычной литературе эта задача известна под названием *digital fingerprinting*).

В третьем разделе даются вспомогательные определения и формулируется первый новый результат, связывающий асимптотические скорости двоичных разделяющих кодов и свободных от перекрытий кодов.

Теорема 1.3.1 *Для скоростей двоичных разделяющих кодов и свободных от перекрытий кодов справедливы следующие неравенства*

$$\underline{R}_{cf}(s,\ell) \leqslant \underline{R}_{s}(s,\ell) \leqslant \overline{R}_{s}(s,\ell) \leqslant \overline{R}_{cf}(s-1,\ell). \tag{10}$$

Доказанные в этой теореме неравенства позволяют улучшить верхние границы скорости двоичных разделяющих кодов для многих значений параметров s и ℓ, а также получить новую верхнюю границу для случая фиксированного ℓ и $s \to \infty$, использовав известную оценку для скорости свободных от перекрытых кодов (2).

В четвертом разделе первой главы рассматриваются границы скоростей q-ичных разделяющих кодов. Следующая теорема позволяет улучшить верхние оценки скорости для многих значений параметров q, s и ℓ.

Теорема 1.4.1 *Введем обозначение* $m = \min\{\max\{q-s,1\},\ell\}$*.Для любого* $q \geqslant 2$ *скорости* q*-ичных разделяющих кодов* $\overline{R}_{s}^{(q)}(s,\ell)$ *ограничены следующим образом*

$$\overline{R}_{s}^{(q)}(s,\ell) \leqslant \frac{(2^{q-1}-1)\cdot \overline{R}_{s}(s,\ell)}{\log_2 q}, \tag{11}$$

$$\overline{R}_{s}^{(q)}(s,\ell) \leqslant \frac{\sum\limits_{k=m}^{\ell} \binom{q-1}{k} \cdot \overline{R}_{cf}(s-1,\ell)}{\log_2 q} \quad \textit{для } s \geqslant 2, \tag{12}$$

$$\overline{R}_{s}^{(q)}(s,\ell) \leqslant \frac{\sum\limits_{k=m}^{\ell} \binom{q-1}{k-1} \cdot \overline{R}_{cf}(s,\ell-1)}{\log_2 q} \quad \textit{для } \ell \geqslant 2. \tag{13}$$

Нижнюю границу дает следующая теорема:

Теорема 1.4.2 (Граница случайного кодирования). *При фиксированных* $q \geqslant 2$, $\ell \geqslant 1$ *и* $s \to \infty$ *для скоростей* $\underline{R}^{(q)}(s,\ell)$ q*-ичных разделяющих кодов справедливо следующее неравенство*

$$\underline{R}_{s}^{(q)}(s,\ell) \geqslant \frac{(q-1)^{\ell}}{e^{\ell}\ln q}\frac{1}{s^{\ell+1}}(1+o(1)). \tag{14}$$

Отметим, что отношение верхней и нижней границ, получаемых из теорем (1.4.1) и (1.4.2), ограничено не зависящей от q величиной, которая при $q > 2\ell$ и $s \to \infty$ может быть записана как

$$\frac{e(\ell+1)^{\ell+1}}{2(\ell-1)!}\ln s(1+o(1)).$$

В пятом разделе в виде теоремы 1.5.1 сформулированы рекуррентные неравенства, связывающие скорости разделяющих и полностью разделяющих кодов с разными параметрами s и ℓ.

Теорема 1.5.1 1) *Для любых* $u \in [s-1]$, $v \in [\ell-1]$

$$\overline{R}_s(s,\ell) \leqslant \overline{R}_s(s-u,\ell-v) \cdot \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v + (1-z)^u z^v\}. \qquad (15)$$

2) *Для любого* $v \in [\ell-1]$ *и* $u = v+s-\ell$, $1 \leqslant u \leqslant s-1$,

$$\overline{R}_s(s,\ell) \leqslant \overline{R}_{cs}(s-u,\ell-v) \cdot \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v + (1-z)^u z^v\}. \qquad (16)$$

3) *Для любого* $v \in [\min(s,\ell)-1]$,

$$\overline{R}_s(s,\ell)/2 \leqslant \overline{R}_{cs}(s,\ell) \leqslant \overline{R}_{cs}(s-v,\ell-v)\frac{1}{2^{2v}}. \qquad (17)$$

Теорема позволяет улучшить верхние границы скоростей $\overline{R}(s,\ell)$ для многих значений параметров s и ℓ. Утверждение 3 дает следующую оценку для скорости разделяющих кодов

$$\overline{R}_s(s,s) = O\left(\frac{1}{2^{2s}}\right),$$

что довольно близко к нижней оценке

$$\underline{R}_s(s,s) \geqslant \frac{-\log_2(1-2^{-(2s-1)})}{2s-1} \sim \frac{\log_2 e}{s2^{2s}}, \quad s\to\infty,$$

которая доказывается с помощью стандартной техники случайного кодирования.

Доказательство теоремы опирается на несколько лемм. Первая лемма является аналогом границы Плоткина для разделяющих кодов со специально введенным "расстоянием". Дадим вспомогательные определения.

Обозначим за X произвольный двоичный код мощности t и длины N. Пусть $\mathcal{U}$ и $\mathcal{V}$ два непересекающихся множества кодовых слов кода X мощности u и v соответственно. Множество координат i кода X, разделяющих $\mathcal{U}$ и $\mathcal{V}$, обозначим за $D_{u,v}(\mathcal{U},\mathcal{V},X)$. Определим среднюю по всем возможным выборам упорядоченной пары множеств $\mathcal{U}$ и $\mathcal{V}$ мощность $D_{u,v}(\mathcal{U},\mathcal{V},X)$

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

и максимальную среднюю мощность

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

по всем кодам X фиксированной мощности t и длины N.

Лемма 1.7.1 (Граница Плоткина). *Выполнено следующее асимптотическое неравенство*

$$\overline{\lim_{t\to\infty}} \frac{\overline{D}_{u,v}(t, N(t))}{N(t)} \leqslant \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v + (1-z)^u z^v\}, \tag{18}$$

где $N(t)$ - произвольная функция.

Следующие три леммы с помощью величины $\overline{D}_{u,v}$ связывают минимальные длины разделяющих и полностью разделяющих кодов с разными параметрами.

Лемма 1.7.2 *Для любых $u \in [s-1]$ и $v \in [\ell-1]$ минимальная длина разделяющего $(s-u, \ell-v)$-кода мощности $t-(u+v)$ удовлетворяет неравенству*

$$N_s(t-(u+v), s-u, \ell-v) \leqslant \overline{D}_{u,v}(t, N_s(t,s,\ell)). \tag{19}$$

Лемма 1.7.3 *Для любого $v \in [\ell-1]$ и $u = v+s-\ell$, $s-(\ell-1) \leqslant u \leqslant s-1$ минимальная длина полностью разделяющего $(s-u, \ell-v)$-кода мощности $t-(u+v)$ удовлетворяет неравенству*

$$N_{cs}(t-(u+v), s-u, \ell-v) \leqslant \overline{D}_{u,v}(t, N_s(t,s,\ell)).$$

Лемма 1.7.4 *Для любого $v \in [\ell-1]$ минимальная длина полностью разделяющего $(s-v, \ell-v)$-кода мощности $t-2v$ удовлетворяет неравенству*

$$2N_{cs}(t-2v, s-v, \ell-v) \leqslant \overline{D}_{v,v}(t, N_{cs}(t,s,\ell)).$$

В шестом разделе приведены таблицы с численными значениями верхних границ скорости двоичных и троичных разделяющих кодов. Новые оценки, полученные в представленной диссертации, сравниваются с наилучшими ранее известными.

В седьмом разделе содержатся доказательства теорем и лемм.

Вторая глава состоит из пяти разделов, посвященных верхним границам асимптотических скоростей классических дизъюнктивных кодов и дизъюнктивных кодов со списочным декодированием.

В первом разделе второй главы даются основные определения и вводятся обозначения, используемые в дальнейшем.

Во втором разделе мы напоминаем известные нижние и верхние границы асимптотических скоростей $\overline{R}_{cf}(s)$ и $\underline{R}_{cf}(s)$ классических двоичных дизъюнктивных кодов. Для доказательства верхней границы А.Г. Дьячковым и В.В. Рыковым [3] была построена рекуррентная последовательность

$\overline{R}_{DR}(s)$, ограничивающая сверху скорость дизъюнктивных кодов, и было показано, что

$$\overline{R}_{DR}(s) \leqslant \frac{2\log_2 s}{s^2}(1+o(1)), \qquad s \to \infty,$$

однако нижней границы для $\overline{R}_{DR}(s)$ получено не было. В этом разделе формулируется теорема, устанавливающая нижнюю границу для $\overline{R}_{DR}(s)$.

Теорема 2.2.1 *Если* $s \geqslant 8$, *то рекуррентная последовательности* $\overline{R}_{DR}(s)$, *определяемая* (2.2.9) – (2.2.10), *удовлетворяет неравенству*

$$\overline{R}_{DR}(s) \geqslant \frac{2\log_2[(s+1)/8]}{(s+1)^2}, \qquad s \geqslant 8. \tag{20}$$

Теорема позволяет утверждать, что

$$\overline{R}_{DR}(s) = \frac{2\log_2 s}{s^2}(1+o(1)), \qquad s \to \infty, \tag{21}$$

то есть, сделанная ранее оценка рекуррентной функции $\overline{R}_{DR}(s)$ была асимптотически оптимальна, и нельзя улучшить верхнюю границу скорости $\overline{R}_{cf}(s)$ с помощью более аккуратных оценок последовательности $\overline{R}_{DR}(s)$.

В третьем разделе речь идет о верхних границах скоростей списочных дизъюнктивных кодов, которые являются обобщением классических дизъюнктивных кодов. Формулируется следующая теорема.

Теорема 2.3.1 (Верхняя рекуррентная граница $r_L(s)$). Имеют место следующие три утверждения.

1. Для любого фиксированного $L \geqslant 1$ скорость СД s_L-кодов удовлетворяет неравенству

$$\overline{R}_L(s) \leqslant \min\left\{\frac{1}{s}, r_L(s)\right\}, \qquad s = 1, 2, \ldots,$$

в правой части которого последовательность $r_L(s)$, $s = 1, 2, \ldots$, определяется рекуррентно:

- если $1 \leqslant s \leqslant L$, то

$$r_L(s) \triangleq 1/s, \qquad s = 1, 2, \ldots, L\,; \tag{22}$$

- если $s \geqslant L+1$, то $r_L(s)$ является единственным решением уравнения

$$r_L(s) \triangleq \max_{(26)} f_{\lfloor s/L \rfloor}(v), \qquad s = L+1, L+2, \ldots, \tag{23}$$

в котором при $n = 1, 2, \ldots$ функция $f_n(v)$ параметра v, $0 < v < 1$, определена равенствами

$$h(v) \triangleq -v\,\log_2 v - (1-v)\log_2(1-v), \qquad 0 < v < 1, \tag{24}$$

и

$$f_s(v) \triangleq h(v/s) - v\,h(1/s), \quad 0 < v < 1, \quad s = 1, 2, \ldots, \tag{25}$$

а максимум берется по всем v, удовлетворяющим условию

$$0 < v < 1 - \frac{r_L(s)}{\min\left\{\frac{1}{s-1}, r_L(s-1)\right\}}; \tag{26}$$

- если $s > 2L$ то уравнение (23) можно записать в виде равенства

$$r_L(s) = f_{\lfloor s/L \rfloor}\left(1 - \frac{r_L(s)}{\min\left\{\frac{1}{s-1}, r_L(s-1)\right\}}\right), \quad L \geqslant 1, \quad s > 2L. \tag{27}$$

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

$$r_L(s) = \begin{cases} \geqslant 1/s, & \text{если} \quad s = s(L) - 1, \\ < 1/s, & \text{если} \quad s \geqslant s(L), \end{cases}$$

и $s(L) = L \log_2 L(1 + o(1))$ при $L \to \infty$.

3. Если $L \geqslant 1$ фиксировано и $s \to \infty$, то

$$r_L(s) = \frac{2L \log_2 s}{s^2}(1 + o(1)). \tag{28}$$

Рекуррентная граница $r_L(s)$, определяемая (22)-(27), а также ее асимптотика (28), являются обобщением рекуррентной границы $\overline{R}_{DR}(s)$ и асимптотики (21). Второе утверждение теоремы отвечает на вопрос, с какого момента новая оценка становится лучше тривиальной оценки $1/s$.

В четвертом разделе дается определение дизъюнктивных планов поиска и описывается их связь со списочными дизъюнктивными кодами. Приведена таблица с численными значениями верхних границ скорости дизъюнктивных планов поиска, получаемыми из теоремы 2.3.1.

В пятом разделе приводятся доказательства теорем 2.2.1 и 2.3.1.

Третья глава состоит из трех разделов, в которых исследуется пропускная способность почти дизъюнктивных кодов.

В первом разделе даны основные определения и установлены некие простые свойства, в том числе доказана верхняя граница для пропускной способности почти дизъюнктивных кодов $C(s) \leqslant 1/s$.

Во втором разделе сформулирована основная теорема главы, дающая нижнюю границу для пропускной способности почти дизъюнктивных кодов.

Теорема 3.2.1 Справедливы следующие два утверждения.

1. Величины $C(s)$ удовлетворяет неравенствам:

$$C(s) \geqslant \underline{C}(s) \triangleq \max_{0<Q<1} C(s,Q) = C(s,Q(s)), \qquad s \geqslant 1, \tag{29}$$

$$C(s,Q) \triangleq h(Q) - [1-(1-Q)^s]\; h\left(\frac{Q}{1-(1-Q)^s}\right), \quad s \geqslant 1, \quad 0 < Q < 1, \tag{30}$$

2. При $s \to \infty$ асимптотика границы случайного кодирования $\underline{C}(s)$, задаваемой (3.2.2) – (3.2.3) и асимптотика оптимального значения $Q(s)$ в (3.2.2) имеют вид:

$$\underline{C}(s) = \frac{\ln 2}{s}(1+o(1)), \quad Q(s) = \frac{\ln 2}{s}(1+o(1)). \tag{31}$$

Для доказательства теоремы рассматривается ансамбль $E(N,t,Q)$ двоичных $(N \times t)$-матриц X с N строками и t столбцами, где столбцы выбираются независимо и равновероятно из множества столбцов фиксированного веса $\lfloor QN \rfloor$, $0 \leqslant Q \leqslant 1$. Оценивается матожидание мощности множества $\mathbf{B}(s,X)$ плохих совокупностей из s столбцов, объединение которых покрывает посторонний столбец. Для оценки матожидания рассматривается условная вероятность $\Pr\left\{ \mathcal{S} \in \mathbf{B}(s,X) \;\middle|\; \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\}$ того, что некая совокупность является плохой, при условии, что вес ее объединения равен k. Далее эта вероятность оценивается сверху как минимум из произведения количества посторонних столбцов на вероятность покрыть один посторонний и единицы. Следующая лемма устанавливает, что эта оценка отличается от настоящего значения не более чем в константу раз, а это значит, что оценка пропускной способности на ансамбле точна.

Лемма 3.3.1 *Пусть* $\lfloor QN \rfloor \leqslant k \leqslant \min\{N, s\lfloor QN \rfloor\}$. *Для условной вероятности в правой части* (3.3.4) *выполнена следующая оценка*

$$\Pr\left\{ \mathcal{S} \in \mathbf{B}(s,X) \;\middle|\; \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\} \geqslant \min\left\{ 1/4;\; \frac{t-s}{2}\frac{\binom{k}{\lfloor QN \rfloor}}{\binom{N}{\lfloor QN \rfloor}} \right\}. \tag{32}$$

Также отметим, что в статье [53] доказан и более сильный результат, а именно то, что на рассматриваемом ансамбле нельзя улучшить нижнюю оценку пропускной способности из теоремы 3.2.1 и для более общего случая почти дизъюнктивных кодов со списочным декодированием, т.е. пропускная способность на ансамбле не зависит от длины списка.

Для завершения доказательства теоремы нужно разобраться с поведением вероятности $\Pr\left\{ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\}$ в зависимости от параметра k, в чем помогает следующая лемма.

Лемма 3.3.2 *Пусть X_n и Y_n две последовательности случайных величин, i-ая случайная величина принимает целые значения из отрезка $[0, i]$, причем для любого $\varepsilon > 0$ существуют $\delta_1(\varepsilon) > 0$ и $\delta_2(\varepsilon) > 0$, такие что*

$$\Pr\left(\left|\frac{X_n}{n} - q_1\right| > \varepsilon\right) < 2^{-\delta_1(\varepsilon)n}(1 + o(1)), \qquad n \to \infty,$$

$$\Pr\left(\left|\frac{Y_n}{n} - q_2\right| > \varepsilon\right) < 2^{-\delta_2(\varepsilon)n}(1 + o(1)), \qquad n \to \infty.$$

Пусть случайная величина Z_n равна весу объединения двух случайных столбцов веса X_n и Y_n соответственно. Тогда для любого $\varepsilon > 0$ существует $\delta(\varepsilon) > 0$, такая что

$$\Pr\left(\left|\frac{Z_n}{n} - (q_1 + q_2 - q_1 q_2)\right| > \varepsilon\right) < 2^{-\delta(\varepsilon)n}(1 + o(1)), \qquad n \to \infty. \qquad (33)$$

В последнем разделе содержатся доказательства теоремы 3.2.1 и лемм 3.3.1, 3.3.2.

Четвертая глава состоит из пяти разделов, в которых обсуждается задача многоступенчатого поиска дефектов.

В первом разделе формулируется рассматриваемая задача, вводятся определения и приводятся некоторые ранее известные результаты по этой теме. Задача заключается в поиске малого числа дефектов элементов среди большого числа объектов с помощью тестов специального вида.

Во втором разделе задача многоступенчатого поиска дефектов описывается на языке гиперграфов. Каждому объекту соответствует вершина, а каждому гиперребру – возможное множество дефектов. Изначально в гиперграфе проведены все гиперребра, чей размер не превосходит максимального возможного числа дефектов s. После проведения тестов, мы узнаем, что некоторые вершины уже не могут быть дефектными, поэтому гиперребра, содержащие эти вершины, стираются. Используя свойства гиперграфа, порожденного проведенными на текущий момент тестами, мы можем придумывать тесты для последующих ступеней алгоритма. Общая идея алгоритма заключается в том, что мы стараемся разбить вершины на множества, в которых будет по одному дефекту, а потом отдельно разобраться с каждым из этих множеств.

В третьем разделе описанная ранее процедура применяется для двух дефектов вместе с возможными в этом частном случае оптимизациями. Предлагается такая первая ступень поиска, после которой порожденный граф имеет небольшое хроматическое число. Хроматические классы этого графа и будут теми множествами, которые содержат не более одного дефекта. В итоге получается четырехступенчатый алгоритм, чья скорость поиска достигает теоретико-информационной границы, т.е. доказана следующая теорема:

Теорема 4.3.1 *Асимптотическая скорость поиска двух дефектов четырехступенчатым алгоритмом равна 1/2,*

$$\overline{R}^{(4)}(2) = \underline{R}^{(4)}(2) = \frac{1}{2}.$$

В четвертом разделе рассмотрен общий случай произвольного числа дефектов и доказана следующая теорема

Теорема 4.4.1 *Скорость поиска s дефектов $2s-1$-ступенчатым алгоритмом удовлетворяет неравенству*

$$\frac{1}{2s-1} \leqslant \underline{R}^{(2s-1)}(s) \leqslant \overline{R}^{(2s-1)}(s) \leqslant \frac{1}{s}.$$

В пятом разделе построены таблицы, в которых приведено минимальное количество тестов, за которое предлагаемый алгоритм находит 2 дефектных элемента. При построении таблиц были также использованы некие дополнительные оптимизации, не влияющие на асимптотическую скорость поиска, но позволяющие улучшить результат для конечного количества размера множества, в котором производится поиск.

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

Апробация диссертации

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

1. Семинар по теории кодирования под рук. Л.А. Бассалыго в 2013–2016 гг., Институт проблем передачи информации им. А.А. Харкевича РАН.

2. Семинар «Проблемы современной теории информации» в 2013–2016 гг. под рук. А.Г. Дьячкова, кафедра теории вероятностей, механико-математический факультет, Московский государственный университет им. М.В. Ломоносова.

3. Семинар «Экстремальная комбинаторика и случайные структуры» в 2016 гг. под рук. Д.А. Шабанова, кафедра теории вероятностей, механико-математический факультет, Московский государственный университет им. М.В. Ломоносова.

4. Семинар по дискретной математике под рук. М.В. Вялого и С.П. Тарасова в 2016 г., Вычислительный центр им. А.А. Дородницына РАН.

Результаты диссертации докладывались на следующих конференциях:

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

2. 14th International Workshop «*Algebraic and Combinatorial Coding Theory*», Svetlogorsk, Russia, 2014.

3. IEEE International Symposium on Information Theory, Honolulu, USA, 2014.

4. Ninth International Workshop on Coding and Cryptography, Paris, France, 2015.

5. IEEE International Symposium on Information Theory, Hong Kong, China, 2015.

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

7. 15th International Workshop «*Algebraic and Combinatorial Coding Theory*», Albena, Bulgaria, 2016.

8. IEEE International Symposium on Information Theory, Barcelona, Spain, 2016.

Публикации

Основные результаты настоящей диссертации опубликованы в работах [52] – [64], представленных в конце списка литературы. Среди них 5 работ в журналах из перечня ВАК и 8 работ в рецензируемых трудах международных конференций.

Благодарности

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

Глава 1

Разделяющие коды

В этой главе мы рассмотрим разделяющие коды, докажем неравенства, связывающие скорости двоичных разделяющих и свободных от перекрытий кодов, выведем новую нижнюю границу для скорости q-ичных разделяющих кодов, получим верхние границы скорости q-ичных разделяющих через известные верхние границы для двоичных разделяющих кодов и приведем новые рекуррентные неравенства, связывающие скорости разделяющих и полностью разделяющих кодов.

1.1 Обозначения, определения и результаты

Пусть q, N, t – целые числа, $q \geqslant 2$, символ $\triangleq$ обозначает равенство по определению, $\mathbf{q} \triangleq \{0, 1, \ldots, q-1\}$ стандартный q-ичный алфавит, $\mathbf{q}^N$ – множество всех q-ичных слов длины N, $|A|$ – мощность множества A, а $[N] \triangleq \{1, 2, \ldots, N\}$ – множество целых чисел от 1 до N. Произвольное подмножество множества $\mathbf{q}^N$ будем называть q-ичным кодом длины N.

Выпуклой оболочкой $\langle S \rangle$ множества кодовых слов S будем называть множество всевозможных q-ичных слов длины N, у которых i-ый символ для любого i, $i \in [N]$, совпадает с i-ым символом какого-нибудь кодового слова $\boldsymbol{x} \in S$. Очевидно, что $S \subseteq \langle S \rangle$. Например, выпуклая оболочка двоичных слов $(0,0)$ и $(0,1)$ состоит из этих же самых двух слов, а выпуклая оболочка слов $(1,0)$ и $(0,1)$ состоит из слов $(1,0)$, $(0,1)$, $(0,0)$ и $(1,1)$.

Пусть $s \geqslant 1$ и $\ell \geqslant 1$ натуральные числа.

Определение 1.1.1. [36]. Код $X \subset \mathbf{q}^N$ называется *q-ичным разделяющим (s,ℓ)-кодом*, если для любых двух непересекающихся множеств кодовых слов $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, их выпуклые оболочки не пересекаются. Другими словами, существует такая координата $i \in [N]$, что координатные множества $\{\boldsymbol{x}_i, \boldsymbol{x} \in \mathcal{S}\} \subseteq \mathbf{q}$ и $\{\boldsymbol{x}_i, \boldsymbol{x} \in \mathcal{L}\} \subseteq \mathbf{q}$ не пересекаются. Также будем говорить, что такая координата i *разделяет* множества слов $\mathcal{S}$ и $\mathcal{L}$.

Заметим, что определение симметрично относительно параметров s и ℓ,

поэтому в дальнейшем мы ограничимся рассмотрением случая $s \geqslant \ell$. Обозначим за $t_s^{(q)}(N, s, \ell)$ максимальную возможную мощность q-ичного разделяющего (s, ℓ)-кода длины N. Мы хотели бы определить максимальную скорость q-ичного разделяющего (s, ℓ)-кода как

$$R_s(s, \ell) = \lim_{N \to \infty} \frac{\log_q t_s^{(q)}(N, s, \ell)}{N},$$

однако не знаем, существует ли соответствующий предел. Поэтому мы будем рассматривать две величины:

$$\overline{R}_s^{(q)}(s, \ell) = \overline{R}_s^{(q)}(\ell, s) \triangleq \overline{\lim_{N \to \infty}} \frac{\log_q t_s^{(q)}(N, s, \ell)}{N}, \tag{1.1.1}$$

$$\underline{R}_s^{(q)}(s, \ell) = \underline{R}_s^{(q)}(\ell, s) \triangleq \underline{\lim_{N \to \infty}} \frac{\log_q t_s^{(q)}(N, s, \ell)}{N}. \tag{1.1.2}$$

Ниже мы будем опускать индекс q, если речь идет о двоичных кодах.

1.2 Применение разделяющих кодов

Разделяющие коды возникли в теории автоматов [11, 12]. Сейчас же они применяются при конструкции хэш-функций [48], а также для защиты авторских прав [15–17, 47]. В англоязычной литературе задача защиты авторских прав называется *digital fingerprinting*.

Опишем подробнее, каким образом при защите авторских прав применяются разделяющие коды. Предположим, что продается некий цифровой продукт. Если недобросовестный покупатель (пират) выложит свою копию в свободный доступ, то все смогут получить его бесплатно, а автор не получит денег. Поэтому в каждую копию добавляется уникальная последовательность символов (ключ), по которой можно вычислить ее обладателя.

Рассмотрим случай, когда действует коалиция пиратов. Они могут сравнить свои файлы и найти позиции, в которых эти файлы отличаются. Все эти позиции должны быть частью ключа. Существуют две модели, описывающие, каким образом пираты могут менять свои файлы. В первой модели они могут ставить в найденных отличающихся позициях произвольные символы алфавита, во второй — на позиции можно использовать только символы, которые встречались в одном из файлов на этой позиции. В случае двоичного алфавита обе модели совпадают. Нетрудно заметить, что во второй модели множество ключей, которые могут получить пираты, совпадает с выпуклой оболочкой множества их ключей. Дальше мы рассматриваем только вторую модель.

Разделяющие $(s,1)$-коды защищают от "наивного" способа распространения. Наивным называется способ, при котором копия выкладывается в общий доступ без изменений. Если мы находим пиратскую копию с ключом пользователя, то мы считаем его виновным. Поэтому нам нужно быть уверенными, что никакая коалиция пиратов не могла получить этот ключ. Использование в качестве ключей слов разделяющего $(s,1)$-кода гарантирует нам выполнение этого свойства в предположении, что размер коалиции пиратов не превосходит s.

Если же в качестве ключей используются слова разделяющего (s,s)-кода, то любые две непересекающиеся коалиции размера не более s не могут получить один и тот же ключ. Таким образом, если мы найдем коалицию, которая могла получить ключ из пиратской копии, то мы знаем наверняка, что хотя бы один из ее членов действительно виновен.

1.3 Двоичные разделяющие коды

Остановимся подробнее на двоичных разделяющих кодах.

Определение 1.3.1. [36]. Код X называется *двоичным разделяющим* (s,ℓ)-*кодом*, если для любых двух непересекающихся множеств $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует такая координата i, для которой выполнено одно из следующих условий

$$x_i = 0 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 1 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}$$

или

$$x_i = 1 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 0 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}.$$

Это определение эквивалентно данному ранее определению q-ичных кодов при $q = 2$. Новые границы для скорости разделяющих кодов будут установлены с помощью известных границ для полностью разделяющих и свободных от перекрытий кодов. Дадим соответствующие определения.

Определение 1.3.2. [41]. Код X называется *полностью разделяющим* (s,ℓ)-*кодом*, если для любых двух непересекающихся множеств $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует две координаты i и j, для которых выполнены следующие условия

$$x_i = 0 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 1 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}$$

и

$$x_j = 1 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_j = 0 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}.$$

Определение 1.3.3. [43]. Двоичный код X называется *свободным от перекрытий* (s,ℓ)*-кодом* (кратко, *СП* (s,ℓ)*-кодом*), если для любых двух непересекающихся множеств $\mathcal{S}$ и $\mathcal{L}$, $|\mathcal{S}| \leqslant s$, $|\mathcal{L}| \leqslant \ell$, существует координата i, для которой

$$x_i = 0 \quad \text{для любого} \quad \boldsymbol{x} \in \mathcal{S} \quad \text{и} \quad y_i = 1 \quad \text{для любого} \quad \boldsymbol{y} \in \mathcal{L}.$$

В англоязычной литературе эти коды называются *cover-free codes*.

В силу симметрии всех трех определений относительно параметров s и ℓ будем в дальнейшем считать, что $s \geqslant \ell$. Обозначим через $t_{cs}(N,s,\ell)$ и $t_{cf}(N,s,\ell)$ максимальную мощность соответственно полностью разделяющих и свободных от перекрытий (s,ℓ)-кодов длины N, а через $N_{cs}(t,s,\ell)$ и $N_{cf}(t,s,\ell)$ обозначим минимальное число строк соответствующего кода мощности t. Как и ранее, в качестве скорости мы вынуждены рассматривать две величины:

$$\overline{R}_{cs}(s,\ell) \triangleq \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N_{cs}(t,s,\ell)}, \qquad \underline{R}_{cs}(s,\ell) \triangleq \varliminf_{t\to\infty} \frac{\log_2 t}{N_{cs}(t,s,\ell)}, \tag{1.3.1}$$

$$\overline{R}_{cf}(s,\ell) \triangleq \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N_{cf}(t,s,\ell)}, \qquad \underline{R}_{cf}(s,\ell) \triangleq \varliminf_{t\to\infty} \frac{\log_2 t}{N_{cf}(t,s,\ell)}. \tag{1.3.2}$$

Границы скоростей и конструкции разделяющих и полностью разделяющих кодов активно исследовались во многих работах, обзор результатов можно найти в статьях [12,19]. Зафиксируем здесь некоторые известные свойства.

Предложение 1.3.1. [12, 19].

1. *Для любых s и ℓ*

$$\begin{aligned} \overline{R}_{s}(s,\ell)/2 \leqslant \overline{R}_{cs}(s,\ell) \leqslant \overline{R}_{cf}(s,\ell) \leqslant \overline{R}_{s}(s,\ell), \\ \underline{R}_{s}(s,\ell)/2 \leqslant \underline{R}_{cs}(s,\ell) \leqslant \underline{R}_{cf}(s,\ell) \leqslant \underline{R}_{s}(s,\ell). \end{aligned} \tag{1.3.3}$$

2. *Для любого s*

$$\overline{R}_{cf}(s,s) = \overline{R}_{cs}(s,s), \qquad \underline{R}_{cf}(s,s) = \underline{R}_{cs}(s,s). \tag{1.3.4}$$

Предложение 1.3.2. *1. Если укоротить СП (s,ℓ)-код, удалив из него одно слово, а также все координаты, в которых у этого слова стоят единицы, то полученный код будет СП $(s-1,\ell)$-кодом.*

2. Если укоротить СП (s,ℓ)-код, удалив из него одно слово, а также все координаты, в которых у этого слова стоят нули, то полученный код будет СП $(s,\ell-1)$-кодом.

Предложение 1.3.3. *Если в каскадном коде X внешний код является разделяющим (s,ℓ)-кодом, а внутренний – свободным от перекрытий (s,ℓ)-кодом, то и код X является свободным от перекрытий (s,ℓ)-кодом.*

Предложение 1.3.4. *Если в каскадном коде X внутренний и внешний коды являются разделяющими (s,ℓ)-кодами, то и код X является разделяющим (s,ℓ)-кодом.*

Предложения 1.3.2 и 1.3.3 достаточно очевидны (см., например, [32]). Последнее свойство впервые было доказано в работе [10] для случая разделяющих $(2,1)$-кодов. Мы приводим это утверждение без доказательства.

Теорема 1.3.1 дает неравенство, связывающее скорости разделяющих и свободных от перекрытий кодов, которое в большинстве случаев оказывается сильнее неравенств (1).

Теорема 1.3.1. *Для скоростей двоичных разделяющих кодов и свободных от перекрытий кодов справедливы следующие неравенства*

$$\underline{R}_{cf}(s,\ell) \leqslant \underline{R}_{s}(s,\ell) \leqslant \overline{R}_{s}(s,\ell) \leqslant \overline{R}_{cf}(s-1,\ell). \tag{1.3.5}$$

Неравенство из теоремы 1.3.1 позволяют улучшить верхние границы для многих значений параметров s и ℓ (см. таблицу 1.2). При фиксированном ℓ и $s \to \infty$ наилучшие верхние границы скоростей свободных от перекрытий кодов были доказаны в работе [52] и выглядят следующим образом

$$\overline{R}_{cf}(s,\ell) \leqslant \frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}} \frac{\log_2 s}{s^{\ell+1}} (1+o(1)). \tag{1.3.6}$$

1.4 q-ичные разделяющие коды

Теорема 1.4.1 связывает скорости q-ичных разделяющих кодов со скоростями двоичных разделяющих и свободных от перекрытий кодов.

Теорема 1.4.1. *Введем обозначение $m = \min\{\max\{q-s,1\},\ell\}$.Для любого $q \geqslant 2$ скорости q-ичных разделяющих кодов $\overline{R}_{s}^{(q)}(s,\ell)$ ограничены следующим образом*

$$\overline{R}_{s}^{(q)}(s,\ell) \leqslant \frac{(2^{q-1}-1)\cdot \overline{R}_{s}(s,\ell)}{\log_2 q}, \tag{1.4.1}$$

$$\overline{R}_{s}^{(q)}(s,\ell) \leqslant \frac{\sum\limits_{k=m}^{\ell} \binom{q-1}{k} \cdot \overline{R}_{cf}(s-1,\ell)}{\log_2 q} \quad \text{для } s \geqslant 2, \tag{1.4.2}$$

$$\overline{R}_{s}^{(q)}(s,\ell) \leqslant \frac{\sum\limits_{k=m}^{\ell} \binom{q-1}{k-1} \cdot \overline{R}_{cf}(s,\ell-1)}{\log_2 q} \quad \text{для } \ell \geqslant 2. \tag{1.4.3}$$

Также отметим, что в работе [48] была указана оценка

$$\underline{R}_s^{(q)}(s,\ell) \geqslant \frac{\lfloor \log_2 q \rfloor \, \underline{R}_s(s,\ell)}{\log_2 q}. \tag{1.4.4}$$

Численные значения верхних границ скоростей троичных разделяющих кодов, полученные с помощью теоремы 1.4.1, приведены в таблице 1.3.

С помощью случайного кодирования получена новая нижняя оценка скорости $\underline{R}^{(q)}(s,\ell)$ и найдена ее асимптотика при фиксированных значениях ℓ и q и $s \to \infty$. Ансамбль был оптимизирован именно для этого случая, поэтому для конкретных маленьких значений s, ℓ и q результаты могут быть существенно улучшены. Для частного случая разделяющих $(s,1)$-кодов такая же оценка была доказана в работе [46].

Теорема 1.4.2. (Граница случайного кодирования)
При фиксированных $q \geqslant 2$, $\ell \geqslant 1$ и $s \to \infty$ для скоростей $\underline{R}^{(q)}(s,\ell)$ q-ичных разделяющих кодов справедливо следующее неравенство

$$\underline{R}_s^{(q)}(s,\ell) \geqslant \frac{(q-1)^\ell}{e^\ell \ln q} \frac{1}{s^{\ell+1}} (1+o(1)). \tag{1.4.5}$$

Объединив неравенства (1.3.6) и (1.4.2), мы получим верхнюю границу для скорости $\overline{R}_s^{(q)}(s,\ell)$ для фиксированных $q \geqslant 2$, $\ell \geqslant 1$ и $s \to \infty$

$$\overline{R}_s^{(q)}(s,\ell) \leqslant \frac{\sum\limits_{k=1}^{\ell} \binom{q-1}{k} (\ell+1)^{\ell+1}}{2e^{\ell-1} \log_2 q} \cdot \frac{\log_2 s}{s^{\ell+1}} \, (1+o(1)). \tag{1.4.6}$$

Отметим, что для достаточно больших q ($q > 2\ell$) отношение верхней границы (1.4.6) к нижней (1.4.5) ограничено сверху не зависящим от q выражением

$$\frac{\sum\limits_{k=1}^{\ell} \binom{q-1}{k} (\ell+1)^{\ell+1}}{2e^{-1}(q-1)^\ell} \ln s(1+o(1)) \leqslant \frac{e(\ell+1)^{\ell+1}}{2(\ell-1)!} \ln s(1+o(1)).$$

В частном случае q-ичных разделяющих $(s,1)$-кодов это отношение равно $2e \ln s(1+o(1))$.

1.5 Рекуррентные неравенства

Наилучшие верхние границы [31, 32] для скорости $\overline{R}_{cf}(s,\ell)$ СП (s,ℓ)-кодов получены с помощью рекуррентных неравенств [35]

$$\overline{R}_{cf}(s,\ell) \leqslant \overline{R}_{cf}(s-u,\ell-v) \cdot \frac{u^u v^v}{(u+v)^{u+v}},$$

$$1 \leqslant u \leqslant s-1, \quad 1 \leqslant v \leqslant \ell - 1. \tag{1.5.1}$$

и их модификации [4]

$$\overline{R}_{cf}(s,\ell) \leqslant \frac{\overline{R}_{cf}(s-u,\ell-v)}{\overline{R}_{cf}(s-u,\ell-v) + \frac{(u+v)^{u+v}}{u^u v^v}},$$

$$1 \leqslant u \leqslant s-1, \quad 1 \leqslant v \leqslant \ell - 1. \tag{1.5.2}$$

Аналогичные неравенства для скоростей $\overline{R}_s(s,\ell)$ и $\overline{R}_{cs}(s,\ell)$ сформулированы в виде теоремы 1.5.1.

Теорема 1.5.1. 1) *Для любых* $u \in [s-1]$, $v \in [\ell - 1]$

$$\overline{R}_s(s,\ell) \leqslant \overline{R}_s(s-u,\ell-v) \cdot \max_{0 \leqslant z \leqslant 1} \{z^u(1-z)^v + (1-z)^u z^v\}. \tag{1.5.3}$$

2) *Для любого* $v \in [\ell - 1]$ *и* $u = v + s - \ell$, $1 \leqslant u \leqslant s-1$,

$$\overline{R}_s(s,\ell) \leqslant \overline{R}_{cs}(s-u,\ell-v) \cdot \max_{0 \leqslant z \leqslant 1} \{z^u(1-z)^v + (1-z)^u z^v\}. \tag{1.5.4}$$

3) *Для любого* $v \in [\min(s,\ell) - 1]$,

$$\overline{R}_s(s,\ell)/2 \leqslant \overline{R}_{cs}(s,\ell) \leqslant \overline{R}_{cs}(s-v,\ell-v)\frac{1}{2^{2v}}. \tag{1.5.5}$$

Утверждения 1 и 2 теоремы позволили нам улучшить некоторые верхние границы скоростей $\overline{R}(s,\ell)$, что отражено в таблице 1.2. Применив утверждение 3 для $s = \ell$ и $u = v = s - 5$, получим следующую оценку для скорости разделяющих кодов

$$\overline{R}_s(s,s) \leqslant \frac{4.178}{2^{2s}}, \quad s \geqslant 5.$$

Нижняя граница

$$\underline{R}_s(s,s) \geqslant \frac{-\log_2(1-2^{-(2s-1)})}{2s-1} \sim \frac{\log_2 e}{s2^{2s}}, \quad s \to \infty,$$

которая доказывается с помощью стандартной техники случайного кодирования (см., например, [15]), отличается от полученной верхней не более чем в $2.9s$ раз.

В доказательстве теоремы 1.5.1 используются идеи теории кодирования. В частности, рассматривается "расстояние" между множествами кодовых слов $\mathcal{S}$ и $\mathcal{L}$ мощности s и ℓ, определяемое как количество разделяющих эти множества координат. При доказательстве теоремы мы используем аналог границы Плоткина (лемма 1.7.1) для этого "расстояния". Отметим, что подобные идеи использовались еще в [11, 12] для построения верхних границ разделяющих (2, 2)-кодов.

1.6 Таблицы верхних границ

В таблице 1.1 мы приводим наилучшие известные верхние границы [19] для скоростей полностью разделяющих (s, ℓ)-кодов. Эти значения используются для улучшения верхних границ скоростей разделяющих (s, ℓ)-кодов с помощью неравенств из теоремы 1.5.1.

Таблица 1.1: Верхние границы для полностью разделяющих (s, ℓ)-кодов

$s \mid \ell$	1	2	3	4	5
1	1	0.322	0.199	0.14	0.106
2	0.322	0.161	0.0662	0.0429	0.0286
3	0.199	0.0662	0.0353	0.0153	0.0101
4	0.14	0.0429	0.0153	0.00836	0.00370
5	0.106	0.0286	0.0101	0.00370	0.00204
6	0.083	0.0203	0.00669	0.00245	0.000911

В таблице 1.2 указаны верхние границы для скоростей разделяющих (s, ℓ)-кодов. Верхние индексы показывают, откуда следует граница.

Таблица 1.2: Верхние границы для разделяющих (s, ℓ)-кодов

$s \mid \ell$	1	2	3	4	5
1	1	0.5^{3}	0.322^{1}	0.199^{1}	0.14^{1}
2	0.5^{3}	0.283^{4}	0.120^{3}	0.0744^{1}	0.0455^{1}
3	0.322^{1}	0.120^{3}	0.0662^{3}	0.0295^{3}	0.0183^{1}
4	0.199^{1}	0.0744^{1}	0.0295^{3}	0.0163^{3}	0.00728^{3}
5	0.14^{1}	0.0455^{1}	0.0183^{1}	0.00728^{3}	0.00403^{3}
6	0.106^{1}	0.0286^{1}	0.0109^{1}	0.00441^{2}	0.00181^{3}

[1] Неравенство (1.3.5). [2] Утверждение 2 теоремы 1.5.1. [3] [19]. [4] [12].

Покажем на примере, как получаются эти значения. Рассмотрим верхнюю границу для скорости разделяющего $(4, 6)$-кода. Подставляя во второе неравенство из теоремы 1.5.1 значения параметров $v = 3$ и $u = 1$, получаем следующее неравенство

$$\overline{R}_s(4,6) \leqslant \overline{R}_{cs}(3,3) \max_{0 \leqslant z \leqslant 1} \{z(1-z)^3 + (1-z)z^3\}.$$

Выражение $z(1-z)^3 + (1-z)z^3$ принимает свое максимальное значение $\frac{1}{8}$ в

точке $z = \frac{1}{2}$. Следовательно, выполнено неравенство

$$\overline{R}_s(4,6) \leqslant \frac{\overline{R}_{cs}(3,3)}{8} \leqslant \frac{0.0353}{8} \approx 0.00441.$$

Полученная граница лучше ранее известной оценки 0.00485634, полученной в теореме 5 в работе [19].

В таблице 1.3 сравниваются старые значения верхних границ скорости троичных разделяющих (s,ℓ)-кодов с новыми, полученными с помощью теоремы 1.4.1. Наилучшие оценки выделены жирным шрифтом.

Таблица 1.3: Верхние границы для троичных разделяющих (s,ℓ)-кодов

(s,ℓ)	старые [19]	новые	(s,ℓ)	старые [19]	новые
(2, 2)	**0.3537**	0.5366	(4, 3)	0.07056	**0.05586**
(3, 3)	**0.1138**	0.1254	(5, 4)	0.02290	**0.01378**
(4, 4)	0.03675	**0.0308**	(4, 2)	0.1605	**0.1408**
(5, 5)	0.01202	**0.00764**	(5, 3)	0.05167	**0.03464**
(3, 2)	**0.2197**	0.2275	(5, 2)	0.1268	**0.08612**

1.7 Доказательства теорем

Доказательство теоремы 1.3.1. Левая часть неравенства (1.3.5) следует из (1). Докажем правую часть.

Рассмотрим произвольный разделяющий (s,ℓ)-код X мощности t и длины N. Построим новый код X' мощности t и длины $2N$, дописав к каждому кодовому слову из X его обращение, т. е. слово, где каждый символ заменен на противоположный. Код X' является СП (s,ℓ)-кодом, причем в каждом слове ровно N единиц. Теперь построим из кода X' код X'', удалив одно кодовое слово, а также все координаты, в которых у этого слова были единицы. Из предложения 1.3.2 следует, что полученный код X'' будет СП $(s-1,\ell)$-кодом мощности $t-1$ и длины N, следовательно выполнено неравенство (1.3.5).

Доказательство теоремы 1.4.1. Возьмем произвольный q-ичный разделяющий (s,ℓ)-код X мощности t и длины N. Используя этот код как внешний в каскадной конструкции, мы построим двоичный разделяющий (s,ℓ)-код. Рассмотрим два разных варианта внутреннего кода.

1. Построим таблицу размеров $(2^{q-1}-1)\times q$, где строками являются все ненулевые двоичные последовательности длины q, начинающиеся с нуля. Обозначим за D_1 код мощности q и длины $2^{q-1}-1$, чьими кодовыми

словами служат столбцы этой таблицы. Очевидно, что код D_1 является разделяющим (s,ℓ)-кодом для любых s и ℓ. Из предложения 1.3.4 следует, что каскадный код X' с внутренним кодом D_1 и внешним кодом X также будет разделяющим (s,ℓ)-кодом. Скорость получившегося кода X' равна

$$\frac{\log_q t}{N}\frac{\log_2 q}{2^{q-1}-1},$$

следовательно, выполняется неравенство (1.4.1).

2. Введем обозначение $C(q,\ell)=\sum\limits_{k=m}^{\ell}\binom{q}{k}$. Рассмотрим таблицу размеров $C(q,\ell)\times q$, где строками являются все ненулевые двоичные последовательности длины q, в которых от m до ℓ единиц. Обозначим за D_2 код мощности q и длины $C(q,\ell)$, чьими кодовыми словами служат столбцы этой таблицы. Покажем, что код D_2 является свободным от перекрытий (s,ℓ)-кодом. Действительно, рассмотрим два произвольных непересекающихся множества кодовых слов $\mathcal{S}$ и $\mathcal{L}$, $0<|\mathcal{S}|\leqslant s$, $0<|\mathcal{L}|\leqslant l$. Мы можем дополнить множество $\mathcal{L}$ до множества $\mathcal{L}'$ не лежащими в $\mathcal{S}$ кодовыми словами таким образом, что $|\mathcal{L}'|\geqslant m$. Тогда найдется такая координата, в которой все слова из $\mathcal{L}$ равны 0, а все остальные равны 1. Таким образом, код D_2 является свободным от перекрытий (s,ℓ)-кодом. Из предложения 1.3.3 следует, что каскадный код X' с внутренним кодом D_2 и внешним кодом X будет СП (s,ℓ)-кодом. Более того, в каждом слове кода X' будет ровно Q единиц, где

$$Q=\sum_{k=m}^{\ell}\binom{q}{k}\frac{k}{q}=\sum_{k=m}^{\ell}\binom{q-1}{k-1}.$$

Воспользовавшись предложением 1.3.2, получим требуемое. $\square$

Доказательство теоремы 1.4.2. В произвольном q-ичном коде X будем называть множество $\mathcal{U}$, состоящее из $s+\ell$ кодовых слов,(s,ℓ)-*плохим*, если существуют два таких подмножества $\mathcal{S}$, $|\mathcal{S}|=s$, и $\mathcal{L}$, $|\mathcal{L}|=\ell$, что нет такой координаты, в которой координатные множества $\{\boldsymbol{x}_i,\boldsymbol{x}\in\mathcal{S}\}\subseteq\mathbf{q}$ и $\{\boldsymbol{x}_i,\boldsymbol{x}\in\mathcal{L}\}\subseteq\mathbf{q}$ не пересекаются. Иными словами, множество кодовых слов называется (s,ℓ)-*плохим*, если его можно разбить на два подмножества, на которых нарушается свойство разделяющих (s,ℓ)-кодов.

Зафиксируем параметр p, $0<p<1/(q-1)$. Рассмотрим случайный ансамбль кодов длины N и мощности t, где каждый символ каждого слова выбирается независимо, причем для любого слова $(c_1,c_2,\ldots,c_N)$

$$\Pr\{c_i=k\}\triangleq p,\quad k=0,1,\ldots q-2,\qquad \Pr\{c_i=q-1\}\triangleq 1-p(q-1).\ (1.7.1)$$

Доказательство основано на следующем стандартном утверждении.

Предложение 1.7.1. *Если для некоторых параметров t и N математическое ожидание количества (s,ℓ)-плохих множеств будет меньше 1, то это означает, что существует q-ичный код мощности t и длины N без (s,ℓ)-плохих множеств, то есть, существует разделяющий (s,ℓ)-код мощности t и длины N.*

Обозначим за $P_0(s,\ell)$ вероятность того, что фиксированное множество $\mathcal{U}$ является (s,ℓ)-плохим, а за $P_1(s,\ell)$ вероятность того, что в фиксированной координате слова из множества $\mathcal{S}$ не пересекаются со словами из $\mathcal{L}$. Вероятность $P_0(s,\ell)$ можно оценить сверху следующим образом

$$P_0(s,\ell) \leqslant \binom{s+\ell}{s} \left(1 - P_1(s,\ell)\right)^N.$$

Если в какой-то координате в словах из $\mathcal{L}$ не встречается символ $q-1$, то условная вероятность того, что в этой координате слова из множества $\mathcal{S}$ не пересекаются со словами из $\mathcal{L}$, не меньше $(1-p\ell)^s$. Тогда

$$P_1(s,\ell) \geqslant (q-1)^\ell p^\ell (1-p\ell)^s$$

и

$$P_0(s,\ell) \leqslant \binom{s+\ell}{s} \left(1 - (q-1)^\ell p^\ell (1-p\ell)^s\right)^N. \tag{1.7.2}$$

Математическое ожидание количества (s,ℓ)-плохих множеств не превосходит $t^{s+\ell} P_0(s,\ell)$, поэтому неравенство

$$t^{s+\ell} \binom{s+\ell}{s} \left(1 - (q-1)^\ell p^\ell (1-p\ell)^s\right)^N \leqslant 1 \tag{1.7.3}$$

является достаточным условием существования q-ичного (s,ℓ) разделяющего кода мощности t и длины N. Отсюда следует нижняя граница для скорости

$$\underline{R}_s^{(q)}(s,\ell) \geqslant \frac{-\log_q \left(1 - (q-1)^\ell p^\ell (1-p\ell)^s\right)}{s+\ell}.$$

Максимальное значение выражения $p^\ell(1-p\ell)^s$ достигается в точке $p = \frac{1}{s+\ell}$, поэтому при $q \leqslant s+\ell+1$ верна оценка

$$\underline{R}_s^{(q)}(s,\ell) \geqslant \frac{-\log_q \left(1 - (q-1)^\ell \frac{s^s}{(s+l)^{s+l}}\right)}{s+\ell}.$$

Для фиксированных q, ℓ и $s \to \infty$

$$\frac{-\log_q \left(1 - (q-1)^\ell \frac{s^s}{(s+l)^{s+l}}\right)}{s+\ell} = \frac{(q-1)^\ell}{s^{\ell+1} \ln q} \frac{s^s}{(s+l)^s} (1+o(1)) = \frac{(q-1)^\ell}{e^\ell \ln q} \frac{1}{s^{\ell+1}} (1+o(1)).$$

Таким образом, неравенство (1.4.5) для скорости $\underline{R}_s^{(q)}(s,\ell)$ доказано. $\square$

Доказательство теоремы 1.5.1.

Обозначим за $\mathcal{P}_u(X)$ множество всех множеств кодовых слов кода X мощности u, т. е.

$$\mathcal{P}_u(t) \triangleq \{P \subset X : \quad |P| = u\}.$$

Без уменьшения общности будем считать, что $s \geqslant \ell$.

Доказательство утверждения 1. Обозначим за X произвольный двоичный код мощности t и длины N. Пусть $\mathcal{U}$ и $\mathcal{V}$ два непересекающихся множества кодовых слов кода X мощности u и v соответственно. Множество координат i кода X, разделяющих $\mathcal{U}$ и $\mathcal{V}$, обозначим за $D_{u,v}(\mathcal{U},\mathcal{V},X)$. Определим среднюю по всем возможным выборам упорядоченной пары множеств $\mathcal{U}$ и $\mathcal{V}$ мощность $D_{u,v}(\mathcal{U},\mathcal{V},X)$

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

и максимальную среднюю мощность

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

по всем кодам X фиксированной мощности t и длины N.

Лемма 1.7.1. *(Граница Плоткина). Выполнено следующее асимптотическое неравенство*

$$\overline{\lim_{t\to\infty}} \frac{\overline{D}_{u,v}(t,N(t))}{N(t)} \leqslant \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v + (1-z)^u z^v\}, \tag{1.7.4}$$

где $N(t)$ - произвольная функция.

Доказательство леммы 1.7.1. Пусть $\mathcal{K}$ множество кодовых слов кода X мощности $u+v$. Введем величину

$$I(X,\mathcal{K},i) \triangleq \begin{cases} 2, & \text{если } u=v \text{ и в } i\text{-ой координате в словах из } \mathcal{K} \\ & \text{ровно } u=v \text{ нулей} \\ 1, & \text{если } u\neq v \text{ и в } i\text{-ой координате в словах из } \mathcal{K} \\ & \text{ровно } u \text{ или ровно } v \text{ нулей} \\ 0, & \text{иначе.} \end{cases}$$

Обозначим за $M_{u,v}(X)$ сумму этих величин, т.е.

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

Величину $M_{u,v}(X)$ можно интерпретировать следующим образом. Запишем код в виде матрицы размера $N \times t$, где столбцами являются кодовые слова. Тогда число $M_{u,v}(X)$ равно сумме количества подматриц размера $1 \times (u+v)$, в которых ровно u нулей, и подматриц, в которых ровно v нулей. Вычислим $M_{u,v}(X)$ другим способом. Пусть количество нулей в i-ой строке кода X равно a_i, тогда

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

С другой стороны,

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

Используя два предыдущих равенства, получаем

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

$$\leqslant N \cdot \max_{a \in [t]} \left\{ \binom{a}{u} \cdot \binom{t-a}{v} + \binom{a}{v} \cdot \binom{t-a}{u} \right\}.$$

При $t \to \infty$ последнее неравенство превращается в (1.7.4). Лемма 1.7.1 доказана. $\square$

Для завершения доказательства первого утверждения теоремы нам понадобится

Лемма 1.7.2. *Для любых $u \in [s-1]$ и $v \in [\ell - 1]$ минимальная длина разделяющего $(s-u, \ell - v)$-кода мощности $t - (u+v)$ удовлетворяет неравенству*

$$N_s(t-(u+v), s-u, \ell - v) \leqslant \overline{D}_{u,v}(t, N_s(t,s,\ell)). \tag{1.7.5}$$

Доказательство леммы 1.7.2. Рассмотрим произвольный разделяющий (s,ℓ)-код X мощности t и длины $N = N_s(t,s,\ell)$. Выберем два таких непересекающихся множества кодовых слов $\mathcal{U}$ и $\mathcal{V}$ мощности u и v соответственно, что $|D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \leqslant \overline{D}_{u,v}(X)$. Очевидно, что такие множества найдутся, так как число $\overline{D}_{u,v}(X)$ равно среднему значению $|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|$ по всем выборам множеств $\mathcal{U}$ и $\mathcal{V}$. Определим код X' длины $|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|$ и мощности $t - (u+v)$,состоящий из всех кодовых слов кода X, кроме входящих в множества $\mathcal{U}$ и $\mathcal{V}$, ограниченных на координаты $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$. Покажем, что X' является разделяющим $(s-u, \ell - v)$-кодом. В самом деле, возьмем два произвольных непересекающихся множества кодовых слов $\mathcal{U}'$ и

$\mathcal{V}'$ кода X' мощности $s-u$ и $\ell-v$. К словам кода X, соответствующим словам кода X' из $\mathcal{U}'(\mathcal{V}')$, добавим слова из $\mathcal{U}(\mathcal{V})$. Обозначим эти новые множества кодовых слов за $\hat{\mathcal{U}}(\hat{\mathcal{V}})$. Так как код X является разделяющим (s,ℓ)-кодом, а множества $\hat{\mathcal{U}}$ и $\hat{\mathcal{V}}$ не пересекаются и имеют мощности s и ℓ соответственно, то должна существовать такая координата i, что выполняется одно из условий

$$x_i = 0 \text{ для } \forall\, x \in \hat{\mathcal{U}} \text{ и } x_i = 1 \text{ для } \forall\, x \in \hat{\mathcal{V}},$$

$$x_i = 1 \text{ для } \forall\, x \in \hat{\mathcal{U}} \text{ и } x_i = 0 \text{ для } \forall\, x \in \hat{\mathcal{V}}.$$

Заметим, что эта координата i принадлежит множеству $D_{u,v}(\mathcal{U},\mathcal{V},X)$, поэтому код X' мощности $t-u-v$ и длины $|D_{u,v}(\mathcal{U},\mathcal{V},X)| \leqslant \overline{D}_{u,v}(t,N(t,s,\ell))$ является разделяющим $(s-u,\ell-v)$-кодом. Лемма 1.7.2 доказана. $\square$

Перепишем неравенство (1.7.5) из леммы 1.7.2 в следующем виде:

$$\frac{N_s(t-(u+v),s-u,\ell-v)}{N_s(t,s,\ell)} \leqslant \frac{\overline{D}_{u,v}(t,N_s(t,s,\ell))}{N_s(t,s,\ell)}. \tag{1.7.6}$$

Устремляя t к бесконечности и применяя неравенство (1.7.4), получаем

$$\frac{\overline{R}_s(s,\ell)}{\overline{R}_s(s-u,\ell-v)} = \varlimsup_{t\to\infty} \frac{N_s(t-(u+v),s-u,\ell-v)}{N_s(t,s,\ell)} \leqslant$$

$$\leqslant \varlimsup_{t\to\infty} \frac{\overline{D}_{u,v}(t,N_s(t,s,\ell))}{N(t,s,\ell)} \leqslant \max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v + (1-z)^u z^v\}.$$

Утверждение 1 теоремы 1.5.1 доказано. $\square$

Доказательство утверждения 2. Доказательство второго утверждения теоремы во многом повторяет доказательство первого, но вместо леммы 1.7.2 нам понадобится

Лемма 1.7.3. *Для любого $v \in [\ell-1]$ и $u = v+s-\ell$, $s-(\ell-1) \leqslant u \leqslant s-1$ минимальная длина полностью разделяющего $(s-u,\ell-v)$-кода мощности $t-(u+v)$ удовлетворяет неравенству*

$$N_{cs}(t-(u+v),s-u,\ell-v) \leqslant \overline{D}_{u,v}(t,N_s(t,s,\ell)).$$

Доказательство леммы 1.7.3. Снова рассмотрим разделяющий (s,ℓ)-код X и два таких непересекающихся множества кодовых слов $\mathcal{U}$ и $\mathcal{V}$ мощности u и v соответственно, что выполнено неравенство

$$|D_{u,v}(\mathcal{U},\mathcal{V},X)| \leqslant \overline{D}_{u,v}(X).$$

В тех координатах из $D_{u,v}(\mathcal{U},\mathcal{V},X)$, в которых у всех слов из $\mathcal{U}$ стоят единицы, заменим символы всех кодовых слов на противоположные, т. е. все нули заменим единицами, а единицы – нулями.

Рассмотрим код X' длины $|D_{u,v}(\mathcal{U},\mathcal{V},X)|$ и мощности $t-(u+v)$, состоящий из всех слов кода X, за исключением слов из $\mathcal{U}$ и $\mathcal{V}$, ограниченных на координаты $D_{u,v}(\mathcal{U},\mathcal{V},X)$. Покажем, что он является полностью разделяющим $(s-u,\ell-v)$-кодом. Возьмем два произвольных непересекающихся множества кодовых слов $\mathcal{U}'$ и $\mathcal{V}'$ кода X' мощности $s-u$ и $\ell-v$. Обозначим за $\hat{\mathcal{U}}(\hat{\mathcal{V}})$ множество слов кода X, соответствующих множеству слов $\mathcal{U}'(\mathcal{V}')$ кода X'. Так как код X является разделяющим (s,ℓ)-кодом, а множества слов $\hat{\mathcal{U}}\cup\mathcal{U}$ и $\hat{\mathcal{V}}\cup\mathcal{V}$ не пересекаются и имеют мощности s и ℓ соответственно, то должна существовать такая координата i, что выполняется одно из условий

$$x_i=0 \text{ для } \forall\, x\in\hat{\mathcal{U}}\cup\mathcal{U} \text{ и } x_i=1 \text{ для } \forall\, x\in\hat{\mathcal{V}}\cup\mathcal{V},$$

$$x_i=1 \text{ для } \forall\, x\in\hat{\mathcal{U}}\cup\mathcal{U} \text{ и } x_i=0 \text{ для } \forall\, x\in\hat{\mathcal{V}}\cup\mathcal{V}.$$

Заметим, что эта координата принадлежит множеству $D_{u,v}(\mathcal{U},\mathcal{V},X)$, а так как у слов из множества $\mathcal{U}$ в этой координате стоят нули, то выполняется именно первое из двух условий. Рассматривая множества $\hat{\mathcal{U}}\cup\mathcal{V}$ и $\hat{\mathcal{V}}\cup\mathcal{U}$, имеющие мощности ℓ и s соответственно, мы получаем существование такой координаты j из $D_{u,v}(\mathcal{U},\mathcal{V},X)$, что

$$x_j=1 \text{ для } \forall\, x\in\hat{\mathcal{U}}\cup\mathcal{V} \text{ и } x_j=0 \text{ для } \forall\, x\in\hat{\mathcal{V}}\cup\mathcal{U}.$$

Так как координаты i и j лежат в множестве $D_{u,v}(\mathcal{U},\mathcal{V},X)$, то код X' является полностью разделяющим $(s-u,\ell-v)$-кодом.

Лемма 1.7.3 и утверждение 2 доказаны. $\square$

Доказательство утверждения 3. Доказательства утверждения 3 следует из леммы 1.7.4.

Лемма 1.7.4. *Для любого $v\in[\ell-1]$ минимальная длина полностью разделяющего $(s-v,\ell-v)$-кода мощности $t-2v$ удовлетворяет неравенству*

$$2N_{cs}(t-2v,s-v,\ell-v)\leqslant\overline{D}_{v,v}(t,N_{cs}(t,s,\ell)).$$

Доказательство леммы 1.7.4. Рассмотрим полностью разделяющий (s,ℓ)-код X и два таких непересекающихся множества кодовых слов $\mathcal{U}$ и $\mathcal{V}$ мощности v, что выполнено неравенство

$$|D_{v,v}(\mathcal{U},\mathcal{V},X)|\leqslant\overline{D}_{v,v}(X).$$

Заметим, что множество $D_{v,v}(\mathcal{U},\mathcal{V},X)$ можно представить в виде объединения таких множеств D_1 и D_0, что у всех слов из $\mathcal{U}$ в разделяющих координатах из D_1 стоят единицы, а в координатах из D_0 стоят нули. Без ограничения общности будем считать, что $|D_1|\leqslant|D_{v,v}(\mathcal{U},\mathcal{V},X)|/2\leqslant|D_0|$.

Рассмотрим код X' длины $|D_1|$ и мощности $t-2v$, состоящий из всех слов кода X, за исключением слов из $\mathcal{U}$ и $\mathcal{V}$, ограниченных на координаты

D_1. Покажем, что он является полностью разделяющим $(s-v, \ell-v)$-кодом. Возьмем два произвольных непересекающихся множества кодовых слов $\mathcal{U}'$ и $\mathcal{V}'$ кода X' мощности $s-v$ и $\ell-v$. Обозначим за $\hat{\mathcal{U}}(\hat{\mathcal{V}})$ множество слов кода X, соответствующих множеству слов $\mathcal{U}'(\mathcal{V}')$ кода X'. Рассматривая пары множеств $\hat{\mathcal{U}} \cup \mathcal{U}$, $\hat{\mathcal{V}} \cup \mathcal{V}$ и $\hat{\mathcal{U}} \cup \mathcal{V}$, $\hat{\mathcal{V}} \cup \mathcal{U}$, получаем существование таких координат i и j из D_1, что

$$x_i = 1 \text{ для } \forall\, x \in \hat{\mathcal{U}} \cup \mathcal{U} \text{ и } x_i = 0 \text{ для } \forall\, x \in \hat{\mathcal{V}} \cup \mathcal{V}$$

и

$$x_j = 0 \text{ для } \forall\, x \in \hat{\mathcal{U}} \cup \mathcal{V} \text{ и } x_j = 1 \text{ для } \forall\, x \in \hat{\mathcal{V}} \cup \mathcal{U}.$$

Таким образом, код X' является полностью разделяющим $(s-u, \ell-v)$-кодом мощности $t-2v$ и длины $|D_1| \leqslant \overline{D}_{v,v}(X)/2$.

Лемма 1.7.4 и утверждение 3 доказаны. $\square$

Теорема 1.5.1 доказана. $\square$

Глава 2

Верхние границы для дизъюнктивных кодов

В этой главе рассмотрены дизъюнктивные коды и обобщающие их дизъюнктивные коды со списочным декодированием; доказаны новые верхние границы скоростей дизъюнктивных кодов со списочным декодированием, зависящие от длины списка L и силы кода s; приведены в таблицах численные значения полученных границ, а также исследованы асимптотики этих границ при стремящейся к бесконечности длине списка и при при стремящейся к бесконечности силе кода.

2.1 Основные определения

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

Стандартный символ $\bigvee$ обозначает операцию дизъюнктивной (булевой) суммы двух двоичных чисел

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

а также покомпонентную дизъюнктивную сумму двух двоичных столбцов. Будем говорить, что двоичный столбец $\mathbf{u} \in \{0,1\}^N$ *покрывает* двоичный столбец $\mathbf{v}$ ($\mathbf{u} \succeq \mathbf{v}$), если $\mathbf{u} \bigvee \mathbf{v} = \mathbf{u}$.

Определение 2.1.1. [2], [29] Код X называется *дизъюнктивным кодом со списочным декодированием силы s с объемом списка L* (кратко, *СД s_L-кодом*), если дизъюнктивная сумма любых s столбцов кода X покрывает не более $L-1$ других столбцов кода X, не входящих в эту сумму. Обозначим через $t_{ld}(N, s, L)$ – максимальный объем СД s_L-кодов длины N, а через $N_{ld}(t,s,L)$ – минимальное число строк СД s_L-кодов объема t и определим

скорости СД s_L-кодов:

$$\overline{R}_L(s) \triangleq \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N_{ld}(t,s,L)}, \qquad \underline{R}_L(s) \triangleq \underline{\lim_{t\to\infty}} \frac{\log_2 t}{N_{ld}(t,s,L)}. \tag{2.1.1}$$

При $L = 1$ определение 2.1.1 совпадает с определением свободных от перекрытий кодов 1.3.3 при $\ell = 1$. Соответствующий код называется *дизъюнктивным s-кодом*. Скорости этих кодов будем обозначать $\overline{R}_{cf}(s) \triangleq \overline{R}_{cf}(s,1)$ и $\underline{R}_{cf}(s) \triangleq \underline{R}_{cf}(s,1)$. Дизъюнктивные s-коды были введены в 1964 году в статье Каутса и Синглтона [38], где были также установлены первые нетривиальные свойства дизъюнктивных s-кодов, разработаны их важные приложения и конструкции, которые в дальнейшем существенно развивались в [26, 27], а также была поставлена задача получения границ скоростей $\overline{R}_{cf}(s)$ и $\underline{R}_{cf}(s)$.

2.2 Нижняя и верхняя границы скорости дизъюнктивных кодов

Наилучшая к настоящему времени нижняя граница скорости $\underline{R}_{cf}(s)$ была получена в 1989 году в работе [30], в которой с помощью метода случайного кодирования на ансамбле двоичных равновесных кодов показано, что

$$\underline{R}_{cf}(s) \geqslant s^{-1} \cdot \max_{0<Q<1} A(s,Q), \qquad s = 1,2,\ldots, \tag{2.2.1}$$

$$A(s,Q) \triangleq \log_2 \frac{Q}{1-y} - sK(Q,1-y) - K\left(Q, \frac{1-y}{1-y^s}\right), \tag{2.2.2}$$

где используется стандартное обозначение расстояния Кульбака

$$K(a,b) \triangleq a \cdot \log_2 \frac{a}{b} + (1-a) \cdot \log_2 \frac{1-a}{1-b}, \quad 0 < a, b < 1, \tag{2.2.3}$$

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

$$y = 1 - Q + Q\, y^s \cdot \frac{1-y}{1-y^s}, \qquad 1 - Q \leqslant y < 1. \tag{2.2.4}$$

Если $s \to \infty$, то асимптотика границы (2.2.1)-(2.2.4) имеет вид

$$\frac{1}{s^2 \log_2 e}(1 + o(1)) = \frac{0.693}{s^2}(1 + o(1)). \tag{2.2.5}$$

Несложно показать (см. [38]), что $\overline{R}_{cf}(s) \leqslant 1/s$, $s = 1,2,\ldots$. Впервые нетривиальная верхняя граница скорости $\overline{R}_{cf}(s)$, которая до настоящего времени является наилучшей, была построена в 1982 году в работе [3]. Для

описания этой границы, обозначаемой в данной работе символом $\overline{R}_{DR}(s)$, $s = 1{,}2, \ldots$, и называемой *рекуррентной границей*, введем стандартное обозначение двоичной энтропии

$$h(v) \triangleq -v \log_2 v - (1-v)\log_2(1-v), \qquad 0 < v < 1, \tag{2.2.6}$$

и функцию

$$f_s(v) \triangleq h(v/s) - v\, h(1/s), \quad 0 < v < 1, \quad s = 1, 2, \ldots, \tag{2.2.7}$$

аргумента v, $0 < v < 1$. В [3] показано (см. также [32]), что функция $f_s(v) > 0$, выпукла вверх и принимает максимальное значение:

$$\max_{0<v<1} f_s(v) = f_s(v_s) \quad \text{при} \quad v_s \triangleq \frac{s}{1 + 2^{s \cdot h\left(\frac{1}{s}\right)}}, \quad s = 1, 2, \ldots. \tag{2.2.8}$$

Положим

$$\overline{R}_{DR}(1) \triangleq 1, \quad \overline{R}_{DR}(2) \triangleq \max_{0<v<1} f_2(v) = f_2(v_2) = 0.322, \tag{2.2.9}$$

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

$$\overline{R}_{DR}(s) = f_s\left(1 - \frac{\overline{R}_{DR}(s)}{\overline{R}_{DR}(s-1)}\right), \quad s = 3, 4, \ldots. \tag{2.2.10}$$

Для скорости дизъюнктивных s-кодов $\overline{R}_{cf}(s)$ и рекуррентной последовательности $\overline{R}_{DR}(s)$, $s = 1, 2, \ldots$, описываемой (2.2.9)-(2.2.10), в [3] были доказаны неравенства

$$\overline{R}_{cf}(s) \leqslant \overline{R}_{DR}(s) \leqslant \frac{2\log_2[e(s+1)/2]}{s^2}, \qquad s = 2, 3, \ldots, \tag{2.2.11}$$

которые давали асимптотическую верхнюю границу для скорости $\overline{R}_{cf}(s)$:

$$\overline{R}_{cf}(s) \leqslant \frac{2\log_2 s}{s^2}\,(1 + o(1)), \quad s \to \infty. \tag{2.2.12}$$

В разделе 2.5 будет доказана

Теорема 2.2.1. *Если $s \geqslant 8$, то рекуррентная последовательности $\overline{R}_{DR}(s)$, определяемая* (2.2.9) – (2.2.10)*, удовлетворяет неравенству*

$$\overline{R}_{DR}(s) \geqslant \frac{2\log_2[(s+1)/8]}{(s+1)^2}, \qquad s \geqslant 8. \tag{2.2.13}$$

Из (2.2.11) и (2.2.13) вытекает асимптотическое равенство

$$\overline{R}_{DR}(s) = \frac{2\log_2 s}{s^2}\,(1 + o(1)), \quad s \to \infty. \tag{2.2.14}$$

2.3 Границы скоростей списочных дизъюнктивных кодов

Дизъюнктивные коды со списочным декодированием (СД s_L-коды) были введены в 1981 году в докладе [2] при разработке системы связи АЛОХА с центральной станцией, когда для различения сигналов на выходе канала со случайным синхронным множественным доступом используется кодирование. Затем некоторые конструкции данных кодов рассматривались в работе [51] (см. также [26] и [33]) в связи с возникающей в молекулярной биологии задачей построения *двухступенчатых процедур групповых проверок* для анализа библиотеки ДНК-клонов. На первой ступени выделяется множество из не более $s + L - 1$ элементов, которые далее на второй ступени проверяются поодиночке. Отметим, что при фиксированном $s \geqslant 2$ скорости двухступенчатых процедур $\overline{R}_L(s)$ и $\underline{R}_L(s)$ являются монотонно неубывающими функциями параметра $L \geqslant 1$ и их пределы

$$\overline{R}_\infty(s) \triangleq \lim_{L\to\infty} \overline{R}_L(s), \qquad \underline{R}_\infty(s) \triangleq \lim_{L\to\infty} \underline{R}_L(s) \tag{2.3.1}$$

можно интерпретировать как *максимальные скорости* двухступенчатых процедур групповых проверок, основанных на списочных кодах.

Пусть X – произвольный СД s_L-код длины N и объема t. Символом $M_s(\boldsymbol{y}, X)$, $\boldsymbol{y} \in \{0,1\}^N$, обозначим множество всех s-наборов столбцов кода X, такое, что для каждого s-набора из $M_s(\boldsymbol{y}, X)$ дизъюнктивная сумма составляющих его s столбцов равна $\boldsymbol{y}$.

Предложение 2.3.1. *[29]. Для любого $\boldsymbol{y} \in \{0,1\}^N$ выполняется неравенство*

$$|M_s(\boldsymbol{y}, X)| \leqslant \binom{s+L-1}{s}.$$

Поскольку число всех s-наборов столбцов кода X равно $\binom{t}{s}$, то

$$\binom{t}{s} = \sum_{\boldsymbol{y}} |M_s(\boldsymbol{y}, X)| \leqslant \binom{s+L-1}{s} 2^N.$$

Согласно определению (2.1.1), для минимального числа строк $N_{ld}(t, s, L)$ (скорости $\overline{R}_L(s)$) эти неравенства приводят к нижней (верхней) границе:

$$N_{ld}(t, s, L) \geqslant \log_2 \frac{\binom{t}{s}}{\binom{s+L-1}{s}} \quad \Longrightarrow \quad \left(\overline{R}_L(s) \leqslant \frac{1}{s}\right), \quad s \geqslant 1, \quad L \geqslant 1. \tag{2.3.2}$$

Столбец (кодовое слово) произвольного СД s_L-кода X назовем *плохим* для кода X, если в X существуют $\lfloor s/L \rfloor$ других столбцов, дизъюнктивная

сумма которых его покрывает. В противном случае столбец назовем *хорошим* и отметим, что множество хороших столбцов кода X является дизъюнктивным $\lfloor s/L \rfloor$-кодом.

Предложение 2.3.2. *СД s_L-код X может содержать не более $L-1$ плохих столбцов.*

Доказательство предложения (2.3.2). Если существует набор плохих столбцов мощности L, то он покрывается дизъюнктивной суммой не более $L \cdot \lfloor s/L \rfloor \leqslant s$ столбцов кода, что противоречит определению СД s_L-кода. $\square$

Другими словами, любой СД s_L-код объема t длины N содержит не менее $t-(L-1)$ кодовых слов, образующих дизъюнктивный $\lfloor s/L \rfloor$-код длины N. Поэтому для максимальной мощности $t_{ld}(N,s,L)$ и скорости $R_L(s)$ справедливы верхние границы

$$t_{ld}(N,s,L) \leqslant t_{ld}\left(N, \lfloor s/L \rfloor, 1\right) + L - 1 \quad \Longrightarrow \quad \overline{R}_L(s) \leqslant \overline{R}_{cf}\left(\lfloor s/L \rfloor\right), \quad L \leqslant s. \tag{2.3.3}$$

Свойства (2.3.2)-(2.3.3) будут использоваться в доказательстве верхней границы теоремы (2.3.1) для скорости $\overline{R}_L(s)$. Эта граница будет построена как обобщение рекуррентной верхней границы (2.2.9)-(2.2.10) для скорости дизъюнктивных s-кодов.

В следующей теореме получена наилучшая к настоящему времени верхняя граница скорости дизъюнктивных списочных кодов.

Теорема 2.3.1. *(Верхняя рекуррентная граница $r_L(s)$). Имеют место следующие три утверждения.*

1. Для любого фиксированного $L \geqslant 1$ скорость СД s_L-кодов удовлетворяет неравенству

$$\overline{R}_L(s) \leqslant \min\left\{\frac{1}{s}, r_L(s)\right\}, \qquad s = 1, 2, \ldots,$$

в правой части которого последовательность $r_L(s)$, $s = 1, 2, \ldots$, определяется рекуррентно:

- *если $1 \leqslant s \leqslant L$, то*

$$r_L(s) \triangleq 1/s, \qquad s = 1, 2, \ldots, L\,; \tag{2.3.4}$$

- *если $s \geqslant L+1$, то $r_L(s)$ является единственным решением уравнения*

$$r_L(s) \triangleq \max_{(2.3.6)} f_{\lfloor s/L \rfloor}(v), \qquad s = L+1, L+2, \ldots, \tag{2.3.5}$$

в котором при $n = 1, 2, \ldots$ *функция* $f_n(v)$ *параметра* v, $0 < v < 1$, *определена равенством (2.2.7), а максимум берется по всем* v, *удовлетворяющим условию*

$$0 < v < 1 - \frac{r_L(s)}{\min\left\{\frac{1}{s-1}, r_L(s-1)\right\}}; \tag{2.3.6}$$

- *если* $s > 2L$ *то уравнение* (23) *можно записать в виде равенства*

$$r_L(s) = f_{\lfloor s/L \rfloor}\left(1 - \frac{r_L(s)}{\min\left\{\frac{1}{s-1}, r_L(s-1)\right\}}\right), \quad L \geqslant 1, \quad s > 2L. \tag{2.3.7}$$

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

$$r_L(s) = \begin{cases} \geqslant 1/s, & \text{если} \quad s = s(L) - 1, \\ < 1/s, & \text{если} \quad s \geqslant s(L), \end{cases}$$

и $s(L) = L \log_2 L(1 + o(1))$ *при* $L \to \infty$.

3. Если $L \geqslant 1$ *фиксировано и* $s \to \infty$, *то*

$$r_L(s) = \frac{2L \log_2 s}{s^2}(1 + o(1)). \tag{2.3.8}$$

Определение рекуррентной границы (2.3.4)-(2.3.7) и асимптотика (2.3.8) представляют собой обобщения рекуррентной границы (2.2.9)-(2.2.10) и асимптотики (2.2.14).

2.4 Дизъюнктивные планы поиска

Определение 2.4.1. [38]. Код X называется *дизъюнктивным* s*-планом* ($(\leqslant s)$*-планом*), если дизъюнктивная (булева) сумма любого набора, содержащего ровно s ($\leqslant s$) столбцов кода X, отлична от дизъюнктивной суммы любого другого набора, содержащего ровно s ($\leqslant s$) столбцов кода X.

Обозначим через $N(t, = s)$ ($N(t, \leqslant s)$) минимальное число строк дизъюнктивного s-плана ($(\leqslant s)$-плана) объема t и определим *скорость* дизъюнктивных s-планов ($(\leqslant s)$-планов)

$$R(= s) \triangleq \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N(t, = s)}, \qquad R(\leqslant s) \triangleq \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N(t, \leqslant s)}. \tag{2.4.1}$$

Легко показать(см. [38]), что скорость

$$R(\leqslant s) \leqslant R(= s) \leqslant 1/s, \qquad s = 1, 2, \ldots, \tag{2.4.2}$$

s	7	8	9	10	11	12	13	14
$1/s$	0.143	0.125	0.111	0.100	0.091	0.083	0.077	0.071
$\overline{R}_2(s-1)$	0.163	0.141	0.117	0.102	0.086	0.076	0.066	0.059

а определение (2.4.1) дает необходимое и достаточное условие однозначного восстановления при планировании N неадаптивных групповых проверок, описываемых строками кода X, для дизъюнктивной модели поиска s $(\leqslant s)$ дефектных элементов во множестве из t элементов. Скорости дизъюнктивных планов и дизъюнктивных кодов связаны неравенством

$$\overline{R}_{cf}(s) \leqslant R(\leqslant s) \leqslant \overline{R}_{cf}(s-1), \tag{2.4.3}$$

которое было отмечено в [38]. Связь дизъюнктивных планов с СД-кодами дает неравенство

$$R(=s) \leqslant \overline{R}_2(s-1), \qquad s \geqslant 2,$$

которое является следствием следующего предложения.

Предложение 2.4.1. *[29]. Если дизъюнктивные суммы всех s-наборов столбцов кода X отличны друг от друга, то код X является СД $(s-1)_2$-кодом.*

Численные значения верхней границы $\overline{R}_2(s-1)$ при $L=2$ и $s=7,8\ldots,14$ приведены в таблице 2.4: Видно, что при $s=$ 11-14 верхняя граница $\overline{R}_2(s-1) < 1/s$. Можно проверить с помощью индукции, что это неравенство будет выполняться и при $s > 14$. Поэтому мы можем сделать вывод, что скорость дизъюнктивных s-планов $R(=s) < 1/s$ при $s \geqslant 11$. Для $s=2$ нетривиальное неравенство $R(=2) \leqslant 0.4998 < 1/2$ было доказано в работе [20]. При $3 \leqslant s \leqslant 10$ неравенство $R(=s) < 1/s$ можно рассматривать как гипотезу.

2.5 Доказательства теорем

Доказательство теоремы 2.2.1. Пусть при фиксированном $s = 2,3,\ldots$ функция $f_s(x)$ параметра x, $0 < x < 1$, определена (2.2.6)-(2.2.7), а

$$K_s \triangleq \left[\max_{0\leqslant x\leqslant \frac{K_s-K_{s-1}}{K_s}} f_s(x)\right]^{-1}, \quad s=2,3,\ldots, \quad K_1 \triangleq 1,$$

обозначает рекуррентную последовательность, введенную в [3]. Тогда утверждение теоремы 2.2.1, т.е. неравенство (2.2.13), равносильно неравенству

$$K_s \leqslant \frac{(s+1)^2}{2\log_2[(s+1)/8]}, \qquad s \geqslant 8. \tag{2.5.1}$$

При $9 \leqslant s \leqslant 236$ справедливость (2.5.1) проверяется с помощью вычислений на компьютере. При $s \geqslant 237$ доказательство (2.5.1) опирается на следующие свойства последовательности K_s:

$$K_s = \left[f_s \left(1 - \frac{K_{s-1}}{K_s} \right) \right]^{-1}, \quad 1 - \frac{K_{s-1}}{K_s} < v_s, \quad s \geqslant 3; \tag{2.5.2}$$

$$v_s > \frac{s}{1+se} > \frac{2}{s}, \qquad s \geqslant 8, \tag{2.5.3}$$

в формулировках которых использованы (2.2.6)-(2.2.9). Для фиксированного $s \geqslant 3$ соотношения (2.5.2) и первое неравенство в (2.5.3) были установлены в [3], [32]. Для $s \geqslant 8$ второе неравенство в (2.5.3) очевидно. Кроме того, при $0 < x < 1$ и $s \geqslant 2$ имеют место оценки

$$\begin{aligned} f_s(x) \triangleq & -\frac{x}{s}\left(\log_2 x - \log_2 s\right) - \left(1 - \frac{x}{s}\right)\log_2\left[1 - \frac{x}{s}\right] - \\ & \frac{x}{s}\log_2 s + x\left(1 - \frac{1}{s}\right)\log_2\left[1 - \frac{1}{s}\right] = \\ = & -\frac{x}{s}\log_2 x + x\left(1 - \frac{1}{s}\right)\log_2\left[1 - \frac{1}{s}\right] - \left(1 - \frac{x}{s}\right)\log_2\left[1 - \frac{x}{s}\right] \geqslant \\ & \geqslant -\frac{x}{s}\log_2 x + x\left(1 - \frac{1}{s}\right)\log_2\left[1 - \frac{1}{s}\right] + \left(1 - \frac{x}{s}\right)\frac{x}{s}\log_2 e. \end{aligned} \tag{2.5.4}$$

и

$$(s-1)\log_2\left[1 - \frac{1}{s}\right] > -\log_2 e, \quad s \geqslant 2, \tag{2.5.5}$$

которые вытекают из определений (2.2.6)-(2.2.7) функции $f_s(x)$ и стандартного логарифмического неравенства

$$\ln u \leqslant u - 1, \qquad u > 0. \tag{2.5.6}$$

Далее при выводе (2.5.1) для $s \geqslant 237$ анализируются отдельно два случая. В первом случае рассматриваются значения $s \geqslant 237$, когда $1 - \frac{K_{s-1}}{K_s} > \frac{2}{s}$, а во втором случае – значения $s \geqslant 237$, когда $1 - \frac{K_{s-1}}{K_s} \leqslant \frac{2}{s}$.

1. Пусть $s \geqslant 237$ и $1 - \frac{K_{s-1}}{K_s} > \frac{2}{s}$. Тогда, применяя свойство монотонного возрастания функции $f_s(x)$, $0 < x \leqslant v_s$, и (2.5.2)-(2.5.5), несложно проверить

цепочку утверждений:

$$K_s = \frac{1}{f_s\left(1-\frac{K_{s-1}}{K_s}\right)} < \frac{1}{f_s\left(\frac{2}{s}\right)} \leqslant$$

$$\leqslant \frac{1}{\frac{2}{s^2}\log_2\left[\frac{s}{2}\right] + \frac{2\log_2 e}{s^2}\left(1-\frac{2}{s^2}\right) + \frac{2(s-1)}{s^2}\log_2\left[1-\frac{1}{s}\right]} =$$

$$= \frac{s^2}{2\log_2\left[\frac{s}{2}\right] + 2\log_2 e - \frac{4\log_2 e}{s^2} + 2(s-1)\log_2\left[1-\frac{1}{s}\right]} < \frac{s^2}{2\log_2\left[\frac{s}{4}\right]}.$$

Таким образом, справедливость (2.5.1) для данного случая доказана.

2. Пусть $s \geqslant 237$ и $1 - \frac{K_{s-1}}{K_s} \leqslant \frac{2}{s}$. Определим величину $t_s \triangleq 1 - \frac{K_{s-1}}{K_s} \leqslant \frac{2}{s}$. Поскольку справедливы оценки (2.5.4), (2.5.5), имеем

$$f_s(x) \geqslant \frac{x}{s}\left(-\log_2 x + \log_2 e - \frac{x\log_2 e}{s} + (s-1)\log_2\left[1-\frac{1}{s}\right]\right) \geqslant$$

$$\geqslant \frac{x}{s}\left(-\frac{x\log_2 e}{s} - \log_2 x\right), \quad 0 < x < 1,\ s \geqslant 2. \quad (2.5.7)$$

Заметим, что функция $q_s(x) \triangleq \left(-\frac{x\log_2 e}{s} - \log_2 x\right)$ монотонно убывает при $x > 0$. Следовательно, $q_s(t_s) \geqslant q_s\left(\frac{2}{s}\right)$, потому что $t_s \leqslant \frac{2}{s}$. В силу неравенства (2.5.7) это означает

$$f_s(t_s) \geqslant \frac{t_s}{s} q_s(t_s) \geqslant \frac{t_s}{s} q_s\left(\frac{2}{s}\right) = \frac{t_s}{s}\left(-\frac{2\log_2 e}{s^2} + \log_2\left[\frac{s}{2}\right]\right) > 0. \quad (2.5.8)$$

Можем написать

$$K_s - K_{s-1} = K_s t_s = \frac{t_s}{f_s(t_s)} \leqslant \frac{s}{\log_2\left[\frac{s}{2}\right] - \frac{2\log_2 e}{s^2}} \leqslant \frac{s}{\log_2\left[\frac{s}{4}\right]}, \quad s \geqslant 8, \quad (2.5.9)$$

где в первых двух равенствах воспользовались видом t_s и соотношением (2.5.2), затем применили (2.5.8) и, наконец, учли, что $s \geqslant 8$. Другими словами, мы установили рекуррентное неравенство

$$K_s \leqslant K_{s-1} + \frac{s}{\log_2\left[\frac{s}{4}\right]}, \quad s \geqslant 8,$$

которое для рассматриваемого случая дает (2.5.1) при $s \geqslant 237$, если показать, что

$$\frac{s^2}{2\log_2\left[\frac{s}{8}\right]} + \frac{s}{\log_2\left[\frac{s}{4}\right]} < \frac{(s+1)^2}{2\log_2\left[\frac{s+1}{8}\right]}, \quad s \geqslant 237. \quad (2.5.10)$$

В силу логарифмического свойства (2.5.6), неравенство (2.5.10) вытекает из

$$\frac{s^2}{2\log_2\left[\frac{s}{8}\right]}+\frac{s}{\log_2\left[\frac{s}{4}\right]}<\frac{(s+1)^2}{2\left(\log_2 s+\frac{\log_2 e}{s}-3\right)},\quad s\geqslant 237. \tag{2.5.11}$$

Элементарными преобразованиями проверяем, что (2.5.11) эквивалентно неравенству

$$s\left((2-\log_2 e)\log_2 s+2\log_2 e-6\right)+\log_2^2 s-(5+2\log_2 e)\log_2 s+6+6\log_2 e>0,$$

справедливость которого при $s\geqslant 237$ подтверждается очевидным образом.

Теорема 2.2.1 доказана. □

Доказательство теоремы 2.3.1.

Доказательство утверждения 1. Граница (2.3.2) означает, что при $s\leqslant L$ утверждение теоремы 2.3.1, т.е. неравенство $\overline{R}_L(s)\leqslant 1/s$, верно. Пусть теперь $s>L\geqslant 1$ и X – произвольный СД s_L-код мощности t и длины N, который содержит хотя бы один столбец (кодовое слово) произвольного фиксированного веса w, $1\leqslant w\leqslant N$. По аналогии с рассуждениями в [3, 32] для случая $L=1$, можем написать, что данный вес

$$w\leqslant N-N_{ld}(t-1,s-1,L), \tag{2.5.12}$$

где $N_{ld}(t,s,L)$ обозначает минимальную длину СД s_L-кода объема t из определения 2.1.1.

Из (2.5.12), первого неравенства в (2.3.3), а также верхних оценок [3,32] на количество слов фиксированного веса в дизъюнктивном $\lfloor s/L\rfloor$-коде вытекает, что для мощности t любого СД s_L-кода справедлива верхняя граница:

$$t\leqslant N_{ld}(t,s,L)+\sum_{w=\lfloor s/L\rfloor+1}^{N_{ld}(t,s,L)-N_{ld}(t-1,s-1,L)}\frac{s^2}{L^2}\frac{\binom{N_{ld}(t,s,L)}{\lceil q\rceil}}{\binom{\lfloor q\rfloor\lfloor s/L\rfloor}{\lfloor q\rfloor}}+L-1,\quad q=\frac{w}{\lfloor s/L\rfloor}. \tag{2.5.13}$$

Будем здесь и далее использовать обозначения (2.3.4)-(2.3.6) из формулировки теоремы 2.3.1 для описания рекуррентной верхней границы $r_L(s)$. Если $t\to\infty$, то с помощью (2.5.13) и аналитических рассуждения, аналогичных [3] и [32], получаем

$$\frac{\log_2 t}{N_{ld}(t,s,L)}\leqslant\max_{0\leqslant v\leqslant 1-\frac{N_{ld}(t-1,s-1,L)}{N_{ld}(t,s,L)}}f_{\lfloor s/L\rfloor}(v)(1+o(1)),\quad s>L,\quad t\to\infty. \tag{2.5.14}$$

Теперь покажем, что скорость СД s_L-кодов $\overline{R}_L(s) \leqslant r_L(s)$ при $s > L$. Доказывать будем от противного по индукции. Базой такой индукции будет неравенство

$$\overline{R}_L(L+1) \leqslant r_L(L+1). \tag{2.5.15}$$

Для доказательства (2.5.15) достаточно показать, что при $s = L+1$ тривиальная граница будет лучше рекуррентной, то есть, что

$$\frac{1}{L+1} \leqslant r_L(L+1). \tag{2.5.16}$$

Для каждого значения параметра $s = 2, 3, \ldots$ введем вспомогательную функцию аргумента x, $0 < x < 1$:

$$G_s(x) \triangleq x - \max_{0 \leqslant v \leqslant 1 - \frac{x}{\min\left\{\frac{1}{s-1}, r_L(s-1)\right\}}} f_{\lfloor s/L \rfloor}(v), \quad 0 < x < 1. \tag{2.5.17}$$

Непосредственно из определения (2.5.17) следует, что при $0 < x < 1$ функция $G_s(x)$ монотонно возрастает и ее единственным нулем на этом интервале является $r_L(s)$. Следовательно, для доказательства (2.5.16) достаточно показать, что $G_{L+1}\left(\frac{1}{L+1}\right) \leqslant 0$. Используя поочередно неравенства (2.5.4)-(2.5.5), отмеченные при выводе теоремы 2.2.1, получаем следующую оценку

$$\begin{aligned} G_{L+1}\left(\frac{1}{L+1}\right) &= \frac{1}{L+1} - \max_{0 \leqslant v \leqslant 1 - \frac{L}{L+1}} f_1(v) \leqslant \\ &\leqslant \frac{1}{L+1} - f_1\left(\frac{1}{L+1}\right) \leqslant \frac{1}{L+1} - \frac{1}{L+1} T_1\left(\frac{1}{L+1}\right) \leqslant \\ &\leqslant \frac{1}{L+1}\left(1 - \log_2(L+1) + \frac{\log_2 e}{L+1}\right) < 0. \end{aligned} \tag{2.5.18}$$

Справедливость последнего неравенства при $L = 2$ проверяется непосредственно подстановкой, а при больших L оно верно из соображений монотонности. Таким образом, доказано неравенство (2.5.16), а следовательно, и база индукции (2.5.15).

От противного проверим, что выполняется шаг индукции. Учитывая определение (2.1.1) скорости СД s_L-кодов $\overline{R}_L(s)$, напишем предположения индукции и противного, т.е.

$$\overline{R}_L(s-1) \triangleq \overline{\lim_{t \to \infty}} \frac{\log_2 t}{N_{ld}(t, s-1, L)} \leqslant r_L(s-1),$$

$$\overline{R}_L(s) \triangleq \overline{\lim_{t \to \infty}} \frac{\log_2 t}{N_{ld}(t, s, L)} > r_L(s). \tag{2.5.19}$$

Тогда верна цепочка неравенств

$$\overline{\lim_{t\to\infty}}\left(1-\frac{N_{ld}(t-1,s-1,L)}{N_{ld}(t,s,L)}\right)<$$
$$<\overline{\lim_{t\to\infty}}\left(1-\frac{N_{ld}(t-1,s-1,L)\cdot r_L(s)}{\log_2 t}\right)\leqslant 1-\frac{r_L(s)}{\underline{R}_L(s-1)}.$$

Из (2.5.14) и полученного неравенства следует, что скорость СД s_L-кодов

$$\overline{R}_L(s)=\overline{\lim_{t\to\infty}}\frac{\log_2 t}{N_{ld}(t,s,L)}\leqslant\overline{\lim_{t\to\infty}}\max_{0\leqslant v\leqslant 1-\frac{N_{ld}(t-1,s-1,L)}{N_{ld}(t,s,L)}} f_{\lfloor s/L\rfloor}(v)\leqslant$$
$$\leqslant\max_{0\leqslant v\leqslant 1-\frac{r_L(s)}{\underline{R}_L(s-1)}} f_{\lfloor s/L\rfloor}(v)\leqslant\max_{0\leqslant v\leqslant 1-\frac{r_L(s)}{\min\left\{\frac{1}{s-1},r_L(s-1)\right\}}} f_{\lfloor s/L\rfloor}(v)=r_L(s),$$

где в последнем равенстве применили определение (2.3.5)-(2.3.6) величины $r_L(s)$. Полученное противоречие доказывает индукционный переход.

Теперь для завершения вывода утверждения 1 установим равенство (2.3.7). Будем рассуждать от противного. Так как определяемая (2.2.6)-(2.2.8) функция $f_{\lfloor s/L\rfloor}(v)$, параметра v, $0<v<1$, выпукла вверх и достигает своего максимума при $v=v_{\lfloor s/L\rfloor}$, то предположение противного можно записать в виде:

$$r_L(s)=f_{\lfloor s/L\rfloor}\left(v_{\lfloor s/L\rfloor}\right),\quad v_{\lfloor s/L\rfloor}<1-\frac{r_L(s)}{\min\left\{\frac{1}{s-1},r_L(s-1)\right\}},\quad L\geqslant 1,\quad s>2L. \tag{2.5.20}$$

Отсюда следует

$$v_{\lfloor s/L\rfloor}<1-\frac{f_{\lfloor s/L\rfloor}\left(v_{\lfloor s/L\rfloor}\right)}{\min\left\{\frac{1}{s-1},r_L(s-1)\right\}}\quad\Longleftrightarrow\quad\min\left\{\frac{1}{s-1},r_L(s-1)\right\}>\frac{f_{\lfloor s/L\rfloor}\left(v_{\lfloor s/L\rfloor}\right)}{1-v_{\lfloor s/L\rfloor}}. \tag{2.5.21}$$

Покажем, что (2.5.21) неверно, т.е. выполняется неравенство

$$\min\left\{\frac{1}{s-1},r_L(s-1)\right\}\leqslant\frac{f_{\lfloor s/L\rfloor}\left(v_{\lfloor s/L\rfloor}\right)}{1-v_{\lfloor s/L\rfloor}},\quad L\geqslant 1,\quad s>2L. \tag{2.5.22}$$

Так как $v_{\left\lfloor\frac{s-1}{L}\right\rfloor}$ является точкой, где функция $f_{\left\lfloor\frac{s-1}{L}\right\rfloor}$ достигает своего глобального максимума, то верно следующее

$$\overline{R}_L(s-1)\leqslant r_L(s-1)\leqslant f_{\left\lfloor\frac{s-1}{L}\right\rfloor}\left(v_{\left\lfloor\frac{s-1}{L}\right\rfloor}\right),\quad L\geqslant 1,\quad s>2L.$$

Поэтому для вывода (2.5.22) достаточно проверить, что

$$f_{\left\lfloor\frac{s-1}{L}\right\rfloor}\left(v_{\left\lfloor\frac{s-1}{L}\right\rfloor}\right)\leqslant\frac{f_{\lfloor s/L\rfloor}\left(v_{\lfloor s/L\rfloor}\right)}{1-v_{\lfloor s/L\rfloor}},\quad L\geqslant 1,\quad s>2L. \tag{2.5.23}$$

Если $s \neq kL$, то $\left\lfloor \frac{s-1}{L} \right\rfloor = \lfloor s/L \rfloor$, а потому справедливость (2.5.23) очевидна. Если $s = kL$, то $\left\lfloor \frac{s-1}{L} \right\rfloor = k-1$, а $\lfloor s/L \rfloor = k$. Тогда (2.5.23) вытекает из неравенства $f_{k-1}(v_{k-1}) \leqslant \frac{f_k(v_k)}{1-v_k}$, $k > 2$, полученного в [3].

Утверждение 1 доказано полностью. □

Доказательство утверждения 2. Будем использовать функцию $G_s(x)$, определенную формулой (2.5.17). С учетом свойства монотонного возрастания функции $f_{\lfloor s/L \rfloor}(v)$, $0 \leqslant v \leqslant 1/s$, вытекающего из оценки (2.5.3), и определений (2.2.6)-(2.2.7), получаем цепочку неравенств

$$G_s\left(\frac{1}{s}\right) \geqslant \frac{1}{s} - \max_{0 \leqslant v \leqslant 1-\frac{s-1}{s}} f_{\lfloor s/L \rfloor}(v) = \frac{1}{s} - \max_{0 \leqslant v \leqslant \frac{1}{s}} f_{\lfloor s/L \rfloor}(v) = \frac{1}{s} - f_{\lfloor s/L \rfloor}\left(\frac{1}{s}\right) >$$
$$> \frac{1}{s} - h\left(\frac{1}{s\,\lfloor s/L \rfloor}\right) > \frac{1}{s} - \frac{1}{s\,\lfloor s/L \rfloor}\log_2\left[s\,\lfloor s/L \rfloor\right] - \frac{2\log_2 e}{s\,\lfloor s/L \rfloor}, \quad s > 3.$$

Отсюда следует, что при фиксированном L, $L \geqslant 1$, существует целое число $s(L) \geqslant 3$, такое, что последовательность $G_s\left(\frac{1}{s}\right) > 0$ при $s > s(L)$. Вместе со свойством, отмеченным после (2.5.17), это означает, что $r_L(s) < \frac{1}{s}$ при $s > s(L)$. В частности, при достаточно больших L и при $s > L\left(\log_2 L + 3\log_2\left[\log_2 L\right]\right)$ будет выполнено неравенство

$$\frac{1}{s} - \frac{1}{s\,\lfloor s/L \rfloor}\log_2\left(e^2 s\,\lfloor s/L \rfloor\right) = \frac{1}{s}\left(1 - \frac{\log_2\lfloor s/L \rfloor + \log_2\left[e^2 s\right]}{\lfloor s/L \rfloor}\right) > 0.$$

Таким образом, имеем $s(L) \leqslant L\log_2 L(1+o(1))$.

Для доказательства неравенства $s(L) \geqslant L\log_2 L(1+o(1))$ проверим по индукции, что $G_s(1/s) < 0$ при $L < s < L\log_2 L - L$. База индукции для $s = L+1$, т.е. неравенство (2.5.18), была доказана при выводе утверждения 1. Из предположения индукции, т.е. неравенства $G_{s-1}(1/(s-1)) < 0$, вытекает, что $1/(s-1) < r_L(s-1)$ и, следовательно, верхняя граница для скорости $\overline{R}_L(s-1)$ совпадает с тривиальной. Поэтому проверкой индукционного перехода служит цепочка соотношений:

$$G_s\left(\frac{1}{s}\right) = \frac{1}{s} - \max_{0 \leqslant v \leqslant 1-\frac{s-1}{s}} f_{\lfloor s/L \rfloor}(v) = \frac{1}{s} - f_{\lfloor s/L \rfloor}\left(\frac{1}{s}\right) \leqslant$$
$$\leqslant \frac{1}{s}\left(1 - \frac{\log_2 s - \frac{\log_2 e}{s\lfloor s/L \rfloor}}{\lfloor s/L \rfloor}\right) < 0,$$

где в первом неравенстве для оценки последовательности $f_{\lfloor s/L \rfloor}(1/s)$ воспользовались (2.5.7), а во втором учли, что $L < s < L\log_2 L - L$.

Таким образом, получили $s(L) = L\log_2 L(1+o(1))$.

Утверждение 2 доказано. □

Доказательство утверждения 3. Для фиксированного $L \geqslant 1$ введем последовательность $K_L(s)$, $s \geqslant L+1$, задаваемую рекуррентно:

$$K_L(L) \triangleq 1, \quad K_L(s) \triangleq \left[f_{\lfloor s/L \rfloor} \left(1 - \frac{K_L(s-1)}{K_L(s)} \right) \right]^{-1}, \quad s = L+1, L+2, \ldots. \tag{2.5.24}$$

Из определений (2.3.4)-(2.3.7) нетрудно увидеть, что при любом фиксированном $L \geqslant 1$ справедливы соотношения

$$r_L(s) \leqslant \frac{1}{K_L(s)}, \quad s \geqslant 1, \quad \text{и} \quad r_L(s) = \frac{1}{K_L(s)}(1+o(1)) \quad \text{при} \quad s \to \infty.$$

С помощью рассуждений , аналогичных выводу теоремы 2.2.1, можно установить неасимптотическую верхнюю границу

$$K_L(s) \leqslant \frac{(s+1)^2}{2L \log_2 \left[\frac{s+1}{8} \right]}, \quad L \geqslant 1, \quad s \geqslant 8. \tag{2.5.25}$$

Следовательно, для доказательства асимптотического равенства (2.3.8) достаточно показать, что имеет место асимптотическое неравенство

$$K_L(s) \geqslant \frac{s^2}{2L \log_2 s}(1+o(1)), \quad s \to \infty. \tag{2.5.26}$$

При любом $s > L$ функция $f_{\lfloor s/L \rfloor}(v)$ аргумента v, $0 \leqslant v \leqslant 1$, выпукла вверх. Поэтому для любого a, $0 < a < 1$, выполнено неравенство

$$f_{\lfloor s/L \rfloor}(v) \leqslant f_{\lfloor s/L \rfloor}(a) + (v-a) f'_{\lfloor s/L \rfloor}(a), \quad 0 \leqslant v \leqslant 1, \quad 0 < a < 1. \tag{2.5.27}$$

Положим в (2.5.27) число $v \triangleq 1 - \frac{K_L(s-1)}{K_L(s)}$. Затем, подставив правую часть (2.5.27) в определение (2.5.24), после элементарных преобразований приходим к неравенству

$$K_L(s) \geqslant K_L(s-1) + \frac{1 - g_{\lfloor s/L \rfloor}(a) K_L(s-1)}{f'_{\lfloor s/L \rfloor}(a) + g_{\lfloor s/L \rfloor}(a)}, \quad s > L, \quad 0 < a < 1. \tag{2.5.28}$$

где

$$g_{\lfloor s/L \rfloor}(a) \triangleq f_{\lfloor s/L \rfloor}(a) - a f'_{\lfloor s/L \rfloor}(a), \quad s > L, \quad 0 < a < 1. \tag{2.5.29}$$

Для функций (2.2.7) и (2.5.29) в [3, 32] были доказаны свойства:

$$g_{\lfloor s/L \rfloor}\left(\frac{2}{\lfloor s/L \rfloor} \right) \leqslant \frac{2 \log_2 e}{\lfloor s/L \rfloor^2 - 2}, \quad s > L, \tag{2.5.30}$$

$$f'_{\lfloor s/L \rfloor}\left(\frac{2}{\lfloor s/L \rfloor} \right) + g_{\lfloor s/L \rfloor}\left(\frac{2}{\lfloor s/L \rfloor} \right) \leqslant \frac{\log_2 \left[\frac{\lfloor s/L \rfloor}{2} \right]}{\lfloor s/L \rfloor}, \quad s > L. \tag{2.5.31}$$

Также заметим, что для достаточно больших $s > s_0$ из (2.5.25) и (2.5.30) следует неравенство

$$1 - g_{\lfloor s/L \rfloor}\left(\frac{2}{\lfloor s/L \rfloor}\right) K_L(s-1) > 0. \tag{2.5.32}$$

Если $s > s_0$, то полагая в (2.5.28) число $a \triangleq \frac{2}{\lfloor s/L \rfloor}$ и принимая во внимание (2.5.30)-(2.5.32), получаем

$$K_L(s) \geqslant K_L(s-1) + \frac{\lfloor s/L \rfloor}{\log_2\left[\frac{\lfloor s/L \rfloor}{2}\right]} - K_L(s-1)\frac{2\lfloor s/L \rfloor \log_2 e}{\left(\lfloor s/L \rfloor^2 - 2\right)\log_2\left[\frac{\lfloor s/L \rfloor}{2}\right]}. \tag{2.5.33}$$

Если $s \to \infty$, то в силу (2.5.25), для последнего слагаемого в правой части (2.5.33) имеет место асимптотическая оценка:

$$K_L(s-1)\frac{2\lfloor s/L \rfloor \log_2 e}{\left(\lfloor s/L \rfloor^2 - 2\right)\log_2\left[\frac{\lfloor s/L \rfloor}{2}\right]} = o\left(\frac{s}{\log_2 s}\right).$$

Поэтому, при $s \to \infty$ рекуррентное неравенство (2.5.33) позволяет написать асимптотическую нижнюю границу:

$$K_L(s) \geqslant \sum_{k=2L}^{s} \frac{\lfloor k/L \rfloor}{\log_2\left[\frac{\lfloor k/L \rfloor}{2}\right]}(1 + o(1)) \geqslant$$

$$\geqslant \sum_{k=2L}^{s} \frac{k}{L \log_2 s}(1 + o(1)) = \frac{s^2}{2L \log_2 s}(1 + o(1)). \tag{2.5.34}$$

Асимптотическое неравенство (2.5.26) является следствием (2.5.34). Утверждение 3 доказано. □

Теорема 2.3.1 доказана. □

Глава 3

Пропускная способность почти дизъюнктивных кодов

В этой главе рассмотрено понятие почти дизъюнктивных кодов. Методом случайного кодирования на ансамбле двоичных равновесных кодов доказана оценка пропускной способности почти дизъюнктивных кодов. Полученные границы для малых значений параметра s приведены в таблице, а также проведено сравнение пропускной способности почти дизъюнктивных кодов и асимптотической скорости дизъюнктивных кодов.

3.1 Основные определения

Будем пользоваться терминологией и обозначениями, введенными в предыдущих главах настоящей диссертации.

Определение 3.1.1. Множество $\mathcal{S}$, $\mathcal{S} \subset [t]$, мощности s назовем *плохим* для кода X, если дизъюнктивная сумма кодовых слов с номерами из $\mathcal{S}$ покрывает какое-то другое кодовое слово из X, т.е.

$$\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) \succeq \boldsymbol{x}(j), \quad j \subset [t] \setminus \mathcal{S}. \tag{3.1.1}$$

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

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

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

Определение 3.1.2. Зафиксируем параметр ε, $0 \leqslant \varepsilon < 1$. Код X длины N и мощности t назовем почти дизъюнктивным кодом силы s с вероятностью ошибки ε (почти дизъюнктивным (s, ε)-кодом), если

$$\frac{|\mathbf{B}(s, X)|}{\binom{t}{s}} \leqslant \varepsilon \quad \Longleftrightarrow \quad |\mathbf{G}(s, X)| \geqslant (1 - \varepsilon)\binom{t}{s}. \tag{3.1.2}$$

Пример 3.1.1. Пусть код X длины $N = 7$ и мощности $t = 5$ задается следующей матрицей:

$$X = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{vmatrix} \tag{3.1.3}$$

Тогда число 2-подмножеств равно $\binom{5}{2} = 10$, а множество $\mathbf{B}(2, X)$, состоящее из плохих множеств мощности 2 для кода X, имеет вид

$$\mathbf{B}(2, X) = \{(1; 3), (1; 5), (3; 5)\}.$$

Таким образом, заключаем, что X является $(2, 0.3)$-кодом.

Отметим, что выполняется следующее естественное свойство:

Предложение 3.1.1. *Пусть X является произвольным почти дизъюнктивным (s, ε)-кодом X, $s \geqslant 2$. Тогда код X является и почти дизъюнктивным $(s - 1, \varepsilon)$-кодом.*

Доказательство. Очевидно, что если множество A является плохим, то и содержащее его множество B будет плохим. Тогда число интересующих нас пар будет равно $(t-s+1)\mathbf{B}(s-1, X)$. В то же время к каждому плохому множеству B мощности s можно поставить в пару не более s плохих подмножеств A мощности $s - 1$. Таким образом, выполняется неравенство

$$(t - s + 1)\mathbf{B}(s - 1, X) \leqslant s\mathbf{B}(s, X).$$

Поделив обе части на $s\binom{t}{s-1}$, получим

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

Таким образом, доля плохих множеств мощности $s - 1$ в коде X не превосходит ε, а это означает, что код X является почти дизъюнктивным $(s-1, \varepsilon)$-кодом. □

Концепция почти дизъюнктивных (s,ε)-кодов является естественным обобщением классического дизъюнктивного s-кода, который был введен в 1964 году в статье Каутса и Синглтона [38]. В частности, дизъюнктивный s-код является почти дизъюнктивным $(s,0)$-кодом.

Используя традиционную теоретико-информационную терминологию, принятую в вероятностной теории кодирования [14, 37], введем

Определение 3.1.3. Зафиксируем параметр R, $R > 0$. Ввиду неравенства (3.1.2) определим *ошибку* для почти дизъюнктивных (s,ε)-кодов:

$$\varepsilon(s,R,N) \triangleq \min_{X\,:\,t=\lceil 2^{RN}\rceil} \left\{ \frac{|\mathbf{B}(s,X)|}{\binom{t}{s}} \right\}, \quad R>0, \tag{3.1.4}$$

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

$$\mathbf{E}(s,R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \varepsilon(s,R,N)}{N}, \quad R>0, \tag{3.1.5}$$

назовем *экспонентой ошибки* для почти дизъюнктивных s-кодов, а число

$$C(s) \triangleq \sup\{R:\ \mathbf{E}(s,R)>0\} \tag{3.1.6}$$

будем называть *пропускной способностью* почти дизъюнктивных s-кодов.

Непосредственно из определений (3.1.4)-(3.1.6) и предложения 3.1.1 вытекает

Предложение 3.1.2. *Для $s \geqslant 2$ имеет место неравенство*

$$C(s-1) \geqslant C(s).$$

В работе [38] было доказано, что при любых значениях параметра s пропускная способность с нулевой ошибкой $R_{cf}(s,1) \leqslant 1/s$. Эти же рассуждения переносятся на случай пропускной способности $C(s)$.

Предложение 3.1.3. *Имеет место неравенство*

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

Доказательство. Зафиксируем параметры R, $R>0$, и ε, $0 \leqslant \epsilon < 1$. Пусть X – произвольный почти дизъюнктивный (s,ε)-код длины N и мощности $t = \lfloor 2^{RN} \rfloor$. Каждому хорошему множеству кодовых слов мощности s сопоставим его дизъюнктивную сумму. Заметим, что разным хорошим множествам соответствуют разные дизъюнктивные суммы. Действительно, предположим, что дизъюнктивные суммы хороших s-множеств S_1 и S_2 совпадают.

Тогда множество S_1 покрывает каждое слово из S_2, а так как множество S_1 является хорошим, то это означает, что $S_2 \subset S_1$, чего не может быть.

Таким образом, число хороших множеств мощности s не превосходит числа различных двоичных строк длины N. В то же время, мы знаем, что число хороших множеств не меньше $(1-\varepsilon)\binom{t}{s}$. Следовательно,

$$(1-\varepsilon)\binom{t}{s} \leqslant \mathbf{G}(s, X) \leqslant 2^N,$$

что эквивалентно неравенству

$$\varepsilon \geqslant 1 - 2^N / \binom{t}{s} = 1 - 2^{-N(sR-1)+o(1)}.$$

Из этого неравенства и определения (3.1.5) следует, что условие $R < 1/s$ является необходимым для положительности экспоненты ошибки $\mathbf{E}(s, R)$ как функции параметра R. Поэтому из определения (3.1.3) вытекает, что пропускная способность $C(s) \leqslant 1/s$. □

3.2 Нижняя граница пропускной способности

Напомним, что наилучшие границы для дизъюнктивных кодов выглядят следующим образом [3, 28]

$$\frac{\ln 2}{s^2}(1+o(1)) \leqslant \underline{R}_{cf}(s) \leqslant \overline{R}_{cf}(s) \leqslant \frac{2\log_2 s}{s^2}(1+o(1)), \quad s \to \infty. \tag{3.2.1}$$

Теорема 3.2.1. *Справедливы следующие два утверждения.*

1. *Величины $C(s)$ удовлетворяет неравенствам:*

$$C(s) \geqslant \underline{C}(s) \triangleq \max_{0<Q<1} C(s, Q) = C(s, Q(s)), \qquad s \geqslant 1, \tag{3.2.2}$$

$$C(s, Q) \triangleq h(Q) - [1-(1-Q)^s]\, h\left(\frac{Q}{1-(1-Q)^s}\right), \quad s \geqslant 1, \quad 0 < Q < 1, \tag{3.2.3}$$

2. *При $s \to \infty$ асимптотика границы случайного кодирования $\underline{C}(s)$, задаваемой (3.2.2) – (3.2.3) и асимптотика оптимального значения $Q(s)$ в (3.2.2) имеют вид:*

$$\underline{C}(s) = \frac{\ln 2}{s}(1+o(1)), \quad Q(s) = \frac{\ln 2}{s}(1+o(1)). \tag{3.2.4}$$

Замечание 3.2.1. При выводе теоремы 3.2.1 будет показано, что нижняя граница пропускной способности, описываемая соотношениями (3.2.2)-(3.2.4) и полученная с помощью метода случайного кодирования на ансамбле равновесных двоичных кодов, для данного ансамбля является точной, т.е. задает логарифмическую асимптотику средней по ансамблю вероятности ошибки почти дизъюнктивных s-кодов.

В таблице 3.1 представлены некоторые численные значения пропускной способности $C(s)$, оптимальные значения параметра веса кода $Q(s)$, на которых она достигается, а также значения нижних и верхних границ скорости дизъюнктивных кодов из [52].

Таблица 3.1: Сравнение пропускной способности и скорости

s	$\underline{C}(s)$	$Q(s)$	$\overline{R}_{cf}^{(ub)}(s)$	$\underline{R}_{cf}^{(lb)}(s)$
2	0.3832	0.2864	0.3220	0.1825
3	0.2455	0.2028	0.1993	0.0787
4	0.1810	0.1569	0.1405	0.0438
5	0.1434	0.1280	0.1057	0.0279
6	0.1188	0.1080	0.0830	0.0193
7	0.1014	0.0935	0.0674	0.0142
8	0.0884	0.0824	0.0560	0.0108
9	0.0784	0.0736	0.0474	0.0085
10	0.0704	0.0666	0.0407	0.0069

Мы видим, что верхняя граница скорости $\overline{R}_{cf}^{(ub)}(s)$ меньше нижней границы пропускной способности $\underline{C}(s)$ для $2 \leqslant s \leqslant 10$, верхней границы пропускной способности с нулевой ошибкой $\overline{R}_{cf}^{(ub)}(s) < \underline{C}(s)$, то есть, скорость строго меньше пропускной способности.К тому же, из асимптотических формул (3.2.1) и (3.2.4) вытекает строгое неравенство $\overline{R}_{cf}(s) < C(s)$ для больших значений параметра s.

В недавней статье [1] для указанных величин (t, N, s, ε) были установлены параметрические соотношения связи:

$$t = q^{\left\lfloor \frac{q}{\log_2 q} \right\rfloor},\ N = q(q+1),\ \varepsilon = \varepsilon(q) \to 0 \text{ при } s = q \cdot \sigma,\ \sigma < \ln 2, \qquad (3.2.5)$$

где параметр q – степень простого числа, и $q \to \infty$. Формулы (3.2.5) означают, что при $s \to \infty$ и $q \to \infty$ асимптотика скорости соответствующих почти дизъюнктивных (s, ε)-кодов имеет вид:

$$\frac{\log_2 t}{N} = \frac{1}{q}(1 + o(1)) = \frac{\ln 2}{s}(1 + o(1)).$$

Отметим, что хотя формула и похожа на полученную в теореме 3.2.1, однако в этой конструкции параметр s жестко связан с длиной кода N, и поэтому при фиксированном s пропускная способность в смысле нашего определения равна нулю.

3.3 Доказательства теоремы и лемм

Доказательство теоремы 3.2.1

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

$$|\mathbf{B}(s, X)| \triangleq \sum_{\mathcal{S}\in[t],|\mathcal{S}|=s} \psi(X, \mathcal{S}), \tag{3.3.1}$$

где

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

Зафиксируем параметры Q, $0 < Q < 1$, и $R > 0$. Определим ансамбль $\{N, t, Q\}$ 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 (3.3.1) следует, что для ансамбля $\{N, t, Q\}$ математическое ожидание $\overline{|\mathbf{B}(s, X)|}$ числа $|\mathbf{B}(s, X)|$ равно

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

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

$$\mathcal{E}^{(N)}(s, R, Q) \triangleq \binom{t}{s}^{-1} \overline{|\mathbf{B}(s, X)|} = \Pr\{\mathcal{S} \in \mathbf{B}(s, X)\}. \tag{3.3.2}$$

Поэтому очевидную верхнюю *границу случайного кодирования* для ошибки (3.1.4) почти дизъюнктивных s-кодов можно представить следующим образом:

$$\varepsilon(s, R, N) \triangleq \min_{X\,:\,t=\lfloor 2^{RN} \rfloor} \left\{ \frac{|\mathbf{B}(s, X)|}{\binom{t}{s}} \right\} \leqslant \mathcal{E}^{(N)}(s, R, Q), \quad 0 < Q < 1. \tag{3.3.3}$$

Перепишем функцию $\mathcal{E}^{(N)}(s,R,Q)$, определенную (3.3.2), в виде:

$$\mathcal{E}^{(N)}(s,R,Q) \;=\; \sum_{k=\lfloor QN\rfloor}^{\min\{N,s\lfloor QN\rfloor\}} \Pr\left\{\mathcal{S}\in\mathbf{B}(s,X)\;\middle|\;\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}\mathcal{P}^{(N)}(s,Q,k). \tag{3.3.4}$$

Здесь мы применили формулу полной вероятности и воспользовались обозначением:

$$\mathcal{P}^{(N)}(s,Q,k) \;\triangleq\; \Pr\left\{\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\},\quad \lfloor QN\rfloor\leqslant k\leqslant\min\{N,s\lfloor QN\rfloor\}. \tag{3.3.5}$$

Для ансамбля $\{N,t,Q\}$ и произвольного k, $\lfloor QN\rfloor\leqslant k\leqslant\min\{N,s\lfloor QN\rfloor\}$, условная вероятность события (3.1.1) равна

$$\Pr\left\{\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\succeq\boldsymbol{x}(j)\;\middle|\;\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}=\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}. \tag{3.3.6}$$

Далее, воспользовавшись представлением (3.3.4), условной вероятностью (3.3.6) и стандартной оценкой

$$\Pr\left\{\bigcup_i C_i\,\middle|\,C\right\}\;\leqslant\;\min\left\{1\,;\,\sum_i\Pr\{C_i|C\}\right\},$$

получим верхнюю границу

$$\mathcal{E}^{(N)}(s,R,Q)\;\leqslant\;\sum_{k=\lfloor QN\rfloor}^{\min\{N,\,s\lfloor QN\rfloor\}}\mathcal{P}^{(N)}(s,Q,k)\;\cdot\;\min\left\{1\,;\,(t-s)\,\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}\right\}, \tag{3.3.7}$$

где мощность кода t равна $\lfloor 2^{RN}\rfloor$.

Далее будет доказана

Лемма 3.3.1. *Пусть $\lfloor QN\rfloor\leqslant k\leqslant\min\{N,s\lfloor QN\rfloor\}$. Для условной вероятности в правой части* (3.3.4) *выполнена следующая оценка*

$$\Pr\left\{\mathcal{S}\in\mathbf{B}(s,X)\;\middle|\;\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}\geqslant\min\left\{1/4;\;\frac{t-s}{2}\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}\right\}, \tag{3.3.8}$$

где величина $D(s)$ не зависит от длины N и мощности t кода X.

Легко понять, что лемма (3.3.1) устанавливает асимптотическую точность оценки логарифмической асимптотики $\mathcal{E}^{(N)}(s,R,Q)$, которая следует

из (3.3.7). Также отметим, что в статье [53] доказан и более сильный результат, а именно то, что на рассматриваемом ансамбле нельзя улучшить нижнюю оценку пропускной способности из теоремы 3.2.1 и для более общего случая почти дизъюнктивных кодов со списочным декодированием, т.е. пропускная способность на ансамбле не зависит от длины списка.

Следующая лемма, которая тоже будет доказана в разделе 3.3, позволяет сделать выводы об аналитических свойствах функции $\mathcal{P}^{(N)}(s, Q, k)$.

Лемма 3.3.2. *Пусть X_n и Y_n — две последовательности случайных величин, i-ая случайная величина принимает целые значения из отрезка $[0, i]$, причем для любого $\varepsilon > 0$ существуют $\delta_1(\varepsilon) > 0$ и $\delta_2(\varepsilon) > 0$ такие, что*

$$\Pr\left(\left|\frac{X_n}{n} - q_1\right| > \varepsilon\right) < 2^{-\delta_1(\varepsilon)n}(1 + o(1)), \qquad n \to \infty,$$

$$\Pr\left(\left|\frac{Y_n}{n} - q_2\right| > \varepsilon\right) < 2^{-\delta_2(\varepsilon)n}(1 + o(1)), \qquad n \to \infty.$$

Пусть случайная величина Z_n равна весу объединения двух случайных столбцов веса X_n и Y_n соответственно. Тогда для любого $\varepsilon > 0$ существует $\delta(\varepsilon) > 0$ такое, что

$$\Pr\left(\left|\frac{Z_n}{n} - (q_1 + q_2 - q_1 q_2)\right| > \varepsilon\right) < 2^{-\delta(\varepsilon)n}(1 + o(1)), \qquad n \to \infty. \quad (3.3.9)$$

Применив $s-1$ раз лемму 3.3.2 к столбцам с относительным весом Q, мы получим, что относительный вес объединения s столбцов сконцентрирован около величины $q = 1 - (1 - Q)^s$. Иными словами, верно равенство

$$\mathcal{P}^{(N)}(s, Q, k) = 2^{-Nf(s,Q,q)(1+o(1))}, \quad q = k/N, \quad (3.3.10)$$

причем функция $f(s, Q, q)$ неотрицательна при всех допустимых значениях параметров и равна нулю только при $q = 1 - (1 - Q)^s$.

Оценим экспоненту ошибки.

$$\frac{-\log_2 \mathcal{E}^{(N)}(s, R, Q)}{N} \sim \frac{-\log_2 \left(\sum\limits_{k=\lfloor QN \rfloor}^{\min(N, s\lfloor QN \rfloor)} \mathcal{P}^{(N)}(s, Q, k) \min\left\{1; t\frac{\binom{k}{\lfloor QN \rfloor}}{\binom{N}{\lfloor QN \rfloor}}\right\} \right)}{N} \sim$$

$$\frac{-\log_2 \left(N \max\limits_{\lfloor QN \rfloor \leqslant k \leqslant \min(N, s\lfloor QN \rfloor)} \mathcal{P}^{(N)}(s, Q, k) \min\left\{1; t\frac{\binom{k}{\lfloor QN \rfloor}}{\binom{N}{\lfloor QN \rfloor}}\right\} \right)}{N} \sim$$

$$\min_{Q \leqslant q \leqslant \min(1, sQ)} [f(s, Q, q) + (h(Q) - qh(Q/q) - R)^+]. \quad (3.3.11)$$

Нас интересует точная верхняя грань по всем R, при которых эта величина положительна. Из леммы 3.3.2 следует, что при $q \neq 1-(1-Q)^s$ выражение $f(s,Q,q)+(h(Q)-qh(Q/q)-R)^+$ положительно, следовательно, нам нужно рассмотреть только случай $q=1-(1-Q)^s$. При таком q выражение $f(s,Q,q)+(h(Q)-qh(Q/q)-R)^+$ положительно только при $R<h(Q)-qh(Q/q)$. Таким образом, верна оценка 3.2.2.

Утверждение 1 доказано. □

Доказательство утверждения 2. Перепишем выражение (3.2.3) в более удобной форме:

$$C(s,Q)=(1-Q-(1-Q)^s)\log_2\left[1-\frac{Q(1-Q)^{s-1}}{1-(1-Q)^s}\right]-$$

$$-Q\log_2\left[1-(1-Q)^s\right]-(1-Q)^s\log_2\left[1-Q\right]. \qquad (3.3.12)$$

Зафиксируем параметр $a>0$. Тогда при подстановке $Q=\frac{a}{s}$ в (3.3) асимптотика $C(s,Q)$ принимает следующий вид:

$$C\left(s,\frac{a}{s}\right)=\frac{-a\log_2\left[1-e^{-a}\right]}{s}(1+o(1)),\quad s\to\infty. \qquad (3.3.13)$$

С помощью производных легко проверить, что максимум

$$\max_{a>0}\left\{-a\log_2\left[1-e^{-a}\right]\right\}=\ln 2$$

достигается при $a=\ln 2$. Следовательно,

$$\underline{C}(s)=\max_{0<Q<1}C(s,Q)\geqslant\frac{\ln 2}{s}(1+o(1)),\quad s\to\infty. \qquad (3.3.14)$$

Чтобы закончить доказательство утверждения 2, покажем, что имеет место и противоположное асимптотическое неравенство.

Пусть $0<Q(s)<1$, $s=2,3,...,$ – некоторая последовательность, для которой выполнено

$$\max_{0<Q<1}C(s,Q)\triangleq C(s,Q(s))=\underline{C}(s).$$

Предположим, что $Q(s)>b$ для некоторого $b>0$. Тогда из (3.3) можно получить неравенство

$$C(s,Q(s))\leqslant(1-b)^sO(1),\quad s\to\infty,$$

которое противоречит (3.3.14). Таким образом, без ограничения общности можно считать, что $Q(s)\to 0$ при $s\to\infty$.

Аналогично предположим, что

$$0 < Q(s) = f(s)/s < 1, \quad \lim_{s\to\infty} f(s) = \infty, \quad f(s) = o(s).$$

Тогда имеем

$$\lim_{s\to\infty}(1 - Q(s))^s \leqslant \lim_{s\to\infty} e^{-f(s)} = 0.$$

Воспользуемся этим свойством и разложением логарифма в нуле

$$\log_2(1 + x) = \log_2 e \cdot x(1 + o(1))$$

и преобразуем (3.3) к виду

$$C(s, Q(s)) = Q(s)[1 - Q(s)]^s O(1), \quad s \to \infty.$$

Тогда приходим к равенству

$$\lim_{s\to\infty} sC(s, Q(s)) = \lim_{s\to\infty} sQ(s)(1 - Q(s))^s O(1) = 0,$$

которое противоречит (3.3.14). Значит, без ограничения общности можем считать, что $sQ(s) \to a$ при $s \to \infty$, причем $0 \leqslant a < \infty$.

Аналогичным образом можно показать, что если $a = 0$, то приходим к асимптотическому неравенству $C(s, Q(s)) = -Q\ln(sQ) \cdot O(1)$, которое противоречит (3.3.14). Таким образом, имеет место асимптотика (3.2.4).

Утверждение 2 доказано. □

Доказательства лемм

Доказательство леммы 3.3.1. Для фиксированного множества $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, и числа $j \in [t] \setminus \mathcal{S}$ введем событие

$$A(j) = A_{\mathcal{S}}(j) \triangleq \left\{ X \,:\, \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succeq \boldsymbol{x}(j) \right\}. \tag{3.3.15}$$

Тогда для любого $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$ условная вероятность в левой части доказываемого неравенства (3.3.8) имеет вид

$$\Pr\left\{ \mathcal{S} \in \mathbf{B}(s,X) \,\middle|\, \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\} = \Pr\left\{ \bigcup_{j\in[t]\setminus\mathcal{S}} A(j) \,\middle|\, \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\}. \tag{3.3.16}$$

Известно, что в ансамбле $\{N, t, Q\}$ для любого $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$ и любого $j \in [t] \setminus \mathcal{S}$, условная вероятность

$$\Pr\left\{ A(j) \,\middle|\, \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\} = p, \qquad p \triangleq \frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}. \tag{3.3.17}$$

Применяя для условной вероятности объединения (3.3.16) стандартную нижнюю границу

$$\Pr\left\{\bigcup_i C_i \,\middle|\, C\right\} \geqslant \sum_i \Pr\{C_i|C\} - \sum_{i<j} \Pr\left\{C_i\, C_j|C\right\}$$

и учитывая (3.3.17), получаем

$$\Pr\left\{\mathcal{S}\in\mathbf{B}(s,X)\,\middle|\,\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\} = \Pr\left\{\bigcup_{j\in[t]\setminus\mathcal{S}} A(j)\,\middle|\,\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}\geqslant$$

$$\geqslant (t-s)p - \sum_{j,j'\in[t]\setminus\mathcal{S},j<j'}\Pr\left\{A(j)\cap A(j')\,\middle|\,\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\} =$$

$$(t-s)p-\binom{t-s}{2}p^2 \geqslant (t-s)p-(t-s)^2p^2. \qquad (3.3.18)$$

Обозначим за t_0 минимальное t, при котором выполняется неравенство $p(t_0-s)\geqslant 0.5$. Если $t<t_0$, то $p(t-s)<0.5$. и

$$\Pr\left\{\mathcal{S}\in\mathbf{B}(s,X)\,\middle|\,\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}\geqslant (t-s)p/2. \qquad (3.3.19)$$

Теперь рассмотрим случай $t\geqslant t_0$. Так как интересующая нас условная вероятность монотонно возрастает при росте t, то

$$\Pr\left\{\mathcal{S}\in\mathbf{B}(s,X)\,\middle|\,\left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right|=k\right\}\geqslant (t_0-s)p/2\geqslant 1/4.$$

Лемма 3.3.1 доказана. □

Доказательство леммы 3.3.2. Для начала вычислим следующую вероятность $\Pr(Z_n=k|x_n=k_1,Y_n=k_2)$, $\max(k_1,k_2)\leqslant k\leqslant\min(k_1+k_2,n)$. Легко видеть, что

$$\Pr(Z_n=k|x_n=k_1,Y_n=k_2)=\frac{\binom{n-k_1}{k-k_1}\binom{k_1}{k_1+k_2-k}}{\binom{n}{k_2}}=$$

$$=2^{-n\left(h\left(\frac{k_2}{n}\right)-\left(1-\frac{k_1}{n}\right)h\left(\frac{k-k_1}{n-k_1}\right)-\frac{k_1}{n}h\left(\frac{k_1+k_2-k}{k_1}\right)\right)(1+o(1))}=2^{-nf(w_1,w_2,w)(1+o(1))},$$

где $f(w_1, w_2, w) = h(w_2) - (1 - w_1)h\left(\frac{w-w_1}{1-w_1}\right) - w_1 h\left(\frac{w_1+w_2-w}{w_1}\right)$, $w_1 = k_1/n$, $w_2 = k_2/n$, $w = k/n$. Заметим, что функция $f(w_1, w_2, w)$ обращается в ноль при $w = w_1 + w_2 - w_1 w_2$. Производная функции по переменной w

$$(f(w_1, w_2, w))'_w = \log_2 \left(\frac{(w - w_1)(w - w_2)}{(1 - w)(w_1 + w_2 - w)} \right)$$

обращается в ноль в этой же точке $w = w_1 + w_2 - w_1 w_2$, которая является точкой минимума. Таким образом, функция $f(w_1, w_2, w)$ положительна везде, кроме $w = w_1 + w_2 - w_1 w_2$, где она обращается в ноль. Иными словами, для любого $\varepsilon > 0$ найдется $\delta_3(\varepsilon) > 0$ такое, что

$$\Pr\left(\left| \frac{Z_n}{n} - (w_1 + w_2 - w_1 w_2) \right| > \varepsilon \right) < 2^{-n\delta_3(\varepsilon)(1+o(1))}. \tag{3.3.20}$$

Зафиксируем произвольное $\varepsilon > 0$ и возьмем $\varepsilon' > 0$ такое, что $(3 + \varepsilon' + q_1 + q_2 +)\varepsilon' < \varepsilon$. Тогда

$$\Pr\left(\left| \frac{Z_n}{n} - (q_1 + q_2 - q_1 q_2) \right| > \varepsilon \right) =$$

$$\sum_{k_1,k_2=0}^{n} \Pr\left(\left| \frac{Z_n}{n} - (q_1 + q_2 - q_1 q_2) \right| > \varepsilon \middle| X_n = k_1, Y_n = k_2 \right) \Pr(X_n = k_1, Y_n = k_2) \leqslant$$

$$\leqslant \Pr\left(\left| \frac{Z_n}{n} - (q_1 + q_2 - q_1 q_2) \right| > \varepsilon \middle| q_1 - \varepsilon' < \frac{X_n}{n} < q_1 + \varepsilon', q_2 - \varepsilon' < \frac{Y_n}{n} < q_2 + \varepsilon' \right) +$$

$$+ 2^{-n\delta_1(\varepsilon')(1+o(1))} + 2^{-n\delta_2(\varepsilon')(1+o(1))} \leqslant 2^{-n\delta_3(\varepsilon')} + 2^{-n\delta_1(\varepsilon')(1+o(1))} + 2^{-n\delta_2(\varepsilon')(1+o(1))} \leqslant$$

$$\leqslant 2^{-n\min(\delta_1(\varepsilon'),\delta_2(\varepsilon'),\delta_3(\varepsilon'))(1+o(1))}. \tag{3.3.21}$$

Лемма 3.3.2 доказана. □

Глава 4

Многоступенчатый поиск дефектов

В этой главе рассмотрена задача многоступенчатого поиска дефектов; представлена явная конструкция четырехступенчатой процедуры для поиска двух дефектов, использующей $2\log_2 t(1+o(1))$ тестов; для общего случая произвольного числа дефектов получена процедура поиска, состоящая из $2s-1$ ступени и использующая $(2s-1)\log_2 t(1+o(1))$ тестов в худшем случае.

4.1 Основные определения и обозначения

Пусть имеется множество объектов T мощности t, среди которых есть не более чем s дефектных элементов, которые мы будем обозначать как S_{un}. Наша цель – найти это множество дефектов, используя минимальное количество тестов $Q(S)$, где S – это некоторое подмножество T, а результат теста равен 1, если $S \cap S_{un} \neq \varnothing$, и равен 0, если $S \cap S_{un} = \varnothing$.

Выделяют два принципиально различных типа алгоритмов. В адаптивных алгоритмах мы планируем эксперименты, опираясь на результаты предыдущих. В неадаптивных алгоритмах все эксперименты заданы изначально и поэтому могут проводиться параллельно. Промежуточным вариантом между этими двумя типами являются многоступенчатые алгоритмы поиска. В многоступенчатом алгоритме все проводимые эксперименты делятся на p групп. Тесты из одной группы могут проводиться одновременно, но тесты из последующих групп могут зависеть от результатов предыдущих. В этой терминологии неадаптивный алгоритм можно называть одноступенчатым алгоритмом. Тесты неадаптивного алгоритма можно записать в виде матрицы $N \times t$. Столбец $\boldsymbol{x}(j)$ поставим в соответствие j-му элементу множества T; строчке $\boldsymbol{x}_i$ поставим в соответствие i-й тест. На пересечении i-ой строки и j-ого столбца стоит единица в том и только в том случае, если j-ый объект включается в i-ый тест. Для произвольного множества дефектов S_{un} определим *вектор ответов*:

$$\mathbf{r}(X, S_{un}) = \bigvee_{j \in S_{un}} \boldsymbol{x}(j).$$

Дадим формальное определение p-ступенчатого алгоритма поиска.

Определение 4.1.1. Пусть есть множество объектов T, $|T| = t$, и множество дефектных объектов $S_{un} \in T$, $|S_{un}| \leqslant s$. Будем говорить, что $\mathcal{A}$ является *p-ступенчатым алгоритмом* поиска s дефектов среди t объектов, если выполнено следующее:

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

2. код X_i, соответствующий i-ой ступени поиска, определяется как

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

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

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

Будем обозначать через $N^{(p)}(t, s)$ минимальное количество тестов, необходимое для нахождения s дефектов среди t объектов с помощью p-ступенчатого алгоритма. В случае адаптивного алгоритма, когда число ступеней неограниченно, будем писать $N^{(\infty)}(t, s)$. Нас будут интересовать величины

$$\underline{R}^{(p)}(s) = \varliminf_{t\to\infty} \frac{\log_2 t}{N^{(p)}(t, s)}, \qquad \overline{R}^{(p)}(s) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N^{(p)}(t, s)}, \tag{4.1.1}$$

которые мы будем называть *асимптотической нижней и верхней скоростью* p-ступенчатого алгоритма поиска.

Теоретико-информационная граница дает верхнюю оценку скорости

$$\overline{R}^{(p)}(s) \leqslant \frac{1}{s}, \qquad s \to \infty. \tag{4.1.2}$$

Известно, что асимптотическая скорость неадаптивных алгоритмов удовлетворяет неравенству

$$\frac{\ln 2}{s^2}(1 + o(1)) \leqslant \underline{R}^{(1)}(s) \leqslant \overline{R}^{(1)}(s) \leqslant \frac{2\log_2(e(s+1)/2)}{s^2}, \qquad s \to \infty \tag{4.1.3}$$

Верхняя оценка была доказана Дьячковым и Рыковым в [3], а нижняя – Дьячковым и Рашадом в [28] с помощью случайного кодирования на равновесном ансамбле.

Для двуступенчатых алгоритмов было показано, что $\underline{R}^{(2)}(s) \geqslant c/s$, где c – некоторая константа. Эта оценка была получена независимо с помощью вероятностного метода для построения дизъюнктивных кодов со списочным

декодированием [25, 45] и для построения селекторов [23]. В недавней работе [52] Щукиным В.Ю. была значительно улучшена константа перед главным членом асимптотики количества тестов. А именно, было доказано, что

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

Таким образом, для двуступенчатых алгоритмов верхняя и нижняя оценки скорости поиска отличаются в константу раз.

Среди адаптивных алгоритмов существуют такие, которые достигают теоретико-информационной верхней границы скорости, то есть

$$\underline{R}^{(\infty)}(s) = \overline{R}^{(\infty)}(s) = \frac{1}{s}.$$

Однако для $s > 1$ количество ступеней в известных оптимальных стратегиях является стремящейся к бесконечности функцией от количества объектов t.

4.2 Многоступенчатый поиск дефектов на языке гиперграфов

Предположим, что в многоступенчатой процедуре поиска уже проведено какое-то количество тестов, матрицу которых мы обозначим за X. Мы будем использовать гиперграф для компактного и наглядного представления полученной в результате этих тестов информации. Такой подход был впервые предложен в статье [22]. Множество вершин V гиперграфа $H = (V, E)$ будет совпадать с множеством объектов T, а множество гиперребер будет состоять из всех таких подмножеств множества объектов, которые могут являться множеством дефектов S_{un}. Иными словами, множество $S \subset T$ будет гиперребром нашего гиперграфа, если $|S| \leqslant s$ и $\mathbf{r}(X, S_{un}) = \mathbf{r}(X, S)$.

Посмотрим на то, какие получаются гипеграфы в известных алгоритмах поиска дефектов.

При неадаптивном поиске после проведения тестов гиперграф состоит из единственного гиперребра, которое совпадает с множеством дефектов. При двуступенчатом поиске, основанном на списочных дизъюнктивных кодах, после первой ступени получается гиперграф, гиперребра которого включают в себя только конечное число вершин. В двуступенчатой процедуре поиска двух дефектов, предложенной в статье [22], после первой ступени получается граф, состоящий из нескольких копий полного двудольного графа. Использование особенностей полученного графа позволяет найти дефекты за не более чем $2.44 \log_2 t(1+o(1))$ тестов, что значительно лучше оценки $3.11 \log_2 t(1+o(1))$, получаемой с помощью списочных кодов.

Опишем многоступенчатый алгоритм, который можно использовать для поиска $\leqslant s$ дефектов.

Первая ступень: Обозначим за X_1 код, соответствующий первой ступени группового тестирования. За $E(r,s)$ обозначим ребра полученного гиперграфа $H=(T,E)$, то есть множество подмножеств $\mathcal{S}\subset T$ размера не более s, для которых выполняется равенство $r(X,\mathcal{S})=r(X,\mathcal{S}_{un})$. Будем называть две вершины *соседними*, если они принадлежат какому-то одному гиперребру из H. Обозначим за V множество вершин гиперграфа, входящих хотя бы в одно гиперребро. Предположим, что существует такое разбиение вершин на k непересекающихся множеств $V=V_1\sqcup V_2\sqcup\ldots\sqcup V_k$, что все соседние вершины принадлежат разным множествам. Тогда в каждом из этих множеств находится не более одного дефектного элемента.

Вторая ступень:

Проверим, какие из множеств V_i содержат дефектные элемента. Для этого проведем k тестов, включая в i-ый тест все элементы множества v_i. После этой ступени мы узнаем количество дефектов $|S_{un}|$, а также получим $|S_{un}|$ множеств $\{V_{i_1},\ldots,V_{i_{|\mathcal{S}un|}}\}$, каждое из которых содержит ровно один дефект.

Отметим, что с помощью $\sum\limits_{j=1}^{\mathcal{S}_{un}}\left\lceil\log_2|V_{i_j}|\right\rceil$ тестов мы можем найти все дефектные элементы на третьей ступени. Но если мы хотим получить максимальную скорость поиска при конечном числе ступеней, то нужно действовать иначе.

Последующие $|S_{un}|$ ступеней:

Далее мы будем последовательно находить по одному дефекту за одну ступень. На третьей ступени мы найдем первый дефект, соответствующий вершине v_1 из множества V_{i_1}, потратив на это $\left\lceil\log_2|V_{i_j}|\right\rceil$ тестов. Исключив из множеств $V_{i_2},\ldots,V_{i_k}$ все вершины, не входящие в какое-то гиперребро вместе с вершиной v_1, мы получим множества $V_{i_2,2},\ldots,V_{i_k,2}$. На следующей ступени мы найдем дефект из множества $V_{i_2,2}$ за $\lceil\log_2|V_{i_2,2}|\rceil$, и так далее. Общее количество ступеней всей описанной процедуры будет равно $S_{un}+2$. Общее количество тестов, как и вся дальнейшая процедура поиска, определяется кодом X_1, применяемым на первой ступени.

4.3 Оптимальный поиск двух дефектов

В этом разделе мы рассмотрим процедуру поиска двух дефектов, для которой нам удалось построить удачный код X_1 для первой ступени.

Первая ступень:

Пусть $C=\{0,1,\ldots q-1\}^{\hat{N}}$ – это q-ичный код мощности $t=q^{\hat{N}}$, состоящий из всех q-ичных слов длины $\hat{N}$. Пусть D – это множество всех двоичных слов длины N' с фиксированным числом единиц wN', $0<w<1$, имеющее

мощность не менее q, то есть, $q \leqslant \binom{N'}{wN'}$. В качестве кода X_1 для первой ступени мы используем каскадный код длины $N_1 = \hat{N} \cdot N'$ и мощности $t = q^{\hat{N}}$ с внутренним кодом D и внешним кодом C. Мы будем говорить, что код X_1 состоит из $\hat{N}$ слоев или уровней. Обозначим за $r_j(X_1, \mathcal{S}_{un})$ часть вектора $r(X_1, \mathcal{S}_{un})$, ограниченную на j-ый слой. Длина каждого вектора $r_j(X_1, \mathcal{S}_{un})$, $1 \leqslant j \leqslant \hat{N}$ равна N'. Относительный вес вектора $r_j(X_1, \mathcal{S}_{un})$ обозначим за w_j, то есть вес вектора $r_j(X_1, \mathcal{S}_{un})$ равен $w_j N'$.

Если веса векторов ответов на всех уровнях равны и равны весу слов кода D, то есть $w_j = w$ для всех $j \in [\hat{N}]$, то это значит, что есть только один дефектный элемент, который легко находится.

Если же дефектных элементов 2, то будем для простоты считать, что $\mathcal{S}_{un} = \{1, 2\}$. Соответствующие этим элементам два слова кода C обозначим за c_1 и c_2. Мы знаем, что существует координата $i, 1 \leqslant i \leqslant \hat{N}$, в которой эти слова отличаются, то есть, $c_1(i) \neq c_2(i)$. Отметим, что для таких координат i относительный вес w_i больше w, а для остальных координат соответствующий относительный вес совпадает с w.

Нам нужно найти разбиение множества всех элементов на непересекающиеся подмножества, чтобы никакие две вершины, образующие ребро, не лежали в одном подмножестве. То есть для случая $s = 2$ эта задача совпадает с поиском правильной раскраски графа. Возьмем произвольную координату $i \in [\hat{N}]$, для которой $w_i > w$, и покрасим вершины множества V в q цветов. Цвет вершины j определяется q-ичным символом из i-ой координаты слова $c(j)$ кода C. Легко проверить, что эта раскраска действительно является правильной.

Вторая ступень:

На втором ступени мы просто проводим q тестов, для того чтобы выяснить, какие два из q множеств разбиения содержат дефектные элементы.

Третья ступень:

Обозначим количество неизолированных вершин графа за $\hat{t}$. На третьей ступени мы с помощью двоичного поиска найдем дефектный элемент в одном из двух оставшихся множеств разбиения. Для этого нам понадобится не более $\lceil \log_2 \hat{t} \rceil$ тестов. Оценим величину $\hat{t}$ сверху. В двоичном векторе, соответствующем вершине, которая еще может быть дефектной, единицы могут стоять там, где стоят единицы у вектора ответов, следовательно,

$$\hat{t} \leqslant \binom{w_1 N'}{wN'} \cdot \ldots \cdot \binom{w_{\hat{N}} N'}{wN'}.$$

Четвертая ступень:

Пусть v – это вершина графа, соответствующая найденному на предыдущей ступени алгоритма дефектному элементу. Второй дефект соответствует какой-то смежной с v вершине. Для его поиска необходимо провести

$\lceil \log_2 \deg(v) \rceil$ тестов. Оценим сверху степень вершины v, рассмотрев отдельно каждый уровень:

$$\deg(v) \leqslant \binom{wN'}{(2w - w_1)N'} \cdot \ldots \cdot \binom{wN'}{(2w - w_{\hat{N}})N'}.$$

Общее число тестов N_T, необходимое для поиска 2 дефектов среди $t \leqslant \binom{N'}{wN'}^{\hat{N}}$ объектов, равно $\hat{N} \cdot N' + q + \max\limits_{w_i} \left(\lceil \log_2 \hat{t} \rceil + \lceil \log_2 \deg(v) \rceil \right)$. Нас интересует верхняя оценка величины $\frac{N_T}{\log_2 t}$.

Устремляя число слоев $\hat{N}$ к бесконечности, мы получаем оценку:

$$\frac{N_T}{\log_2 t} \leqslant \frac{\hat{N} \cdot N' + \max\limits_{w_i} \left(\log_2 \hat{t} + \log_2 \deg(v) \right)}{(1 + o(1))\hat{N} \log_2 \binom{N'}{wN'}}.$$

Довольно очевидно, что в худшем случае все значения w_i равны между собой, поэтому

$$\frac{N_T}{\log_2 t} \leqslant \frac{\hat{N} \cdot N' + \max\limits_{w'} \log_2 \left(\binom{w'N'}{wN'} \binom{wN'}{(2w - w')N'} \right)}{(1 + o(1))\hat{N} \log_2 \binom{N'}{wN'}}. \tag{4.3.1}$$

Выбирая оптимальное значение параметра w, $wN' \in \mathbb{Z}$, мы можем минимизировать необходимое число тестов при фиксированном значении q.

Устремив q к бесконечности, мы можем переписать (4.3.1) как

$$\frac{N_T}{\log_2 t} \leqslant \sup_{w \leqslant w' \leqslant \min(1, 2w)} f(w, w')(1 + o(1)),$$

где

$$f(w, w') = \frac{1 + w' \cdot h\left(\frac{w}{w'}\right) + w \cdot h\left(\frac{2w - w'}{w}\right)}{h(w)}.$$

В итоге мы получаем

$$\frac{N_T}{\log_2 t} \leqslant \inf_{0 < w < 1} \sup_{w \leqslant w' \leqslant \min(1, 2w)} f(w, w'). \tag{4.3.2}$$

Найдем y, максимизирующее значение функции

$$g(x,y) = y \cdot h(x/y) + x \cdot h((2x - y)/x).$$

$$\begin{aligned} \frac{dg(x,y)}{dy} &= h(x/y) - \frac{x}{y} h'(x/y) - h'((2x - y)/x) = \\ &= \log_2 y - 2 \log_2 (y - x) + \log_2 (2x - y). \end{aligned}$$

Это эквивалентно равенству

$$(y-x)^2 - 2xy + y^2 = 0.$$

Значит, если мы возьмем $w = 1/(2+\sqrt{2})$, то максимум из (4.3.2) достигается при $w' = 1/2$, и равен 2. Таким образом, количество тестов описанной четырехступенчатой процедуры стремится к $2\log_2 t(1+o(1))$, что совпадает с теоретико-информационной границей. Получаем следующую теорему:

Теорема 4.3.1. *Асимптотическая скорость поиска двух дефектов четырехступенчатым алгоритмом равна 1/2,*

$$\overline{R}^{(4)}(2) = \underline{R}^{(4)}(2) = \frac{1}{2}.$$

4.4 Поиск произвольного количества дефектных элементов

Напомним, что раскраска вершин гиперграфа называется правильной, если нет одноцветных гиперребер. Отметим, что раскраска, которую мы использовали в предыдущем разделе, является правильной раскраской гиперграфа, порожденного кодом X_1, для любого s. Это свойство позволяет нам разбить множество объектов на несколько (не меньше двух) групп, в каждой из которых будут дефекты. Для двух дефектов мы получали два множества, содержащих ровно по одному дефекту. В общем случае возможны разные варианты, худший из которых – это разделение на 2 множества, содержащие 1 и $s-1$ дефектов соответственно, причем нам не известно, какой именно вариант реализовался. Поэтому мы будем использовать код X_1 максимальной скорости.

Опишем алгоритм более формально. Пусть $C = \{0,1,\dots q-1\}^{\hat{N}}$, $|C| = q^{\hat{N}}$, — это множество всех q-ичных слов длины $\hat{N}$. Пусть D — это множество всех двоичных слов длины N' фиксированного веса $N'/2$, причем мощность множества D не меньше q. На первой ступени будем использовать каскадный двоичный код X длины $\hat{N}\cdot N'$ и мощности $q^{\hat{N}}$ с внутренним кодом D и внешним кодом C. Заметим, что если дефект только один, то мы сразу же это поймем по весу вектора ответов $r_1(X,\mathcal{S}_{un})$ и легко сможем его найти. Если дефектов два или больше, то найдется координата i, в которой не все слова кода C, соответствующие дефектам, совпадают. Это означает, что вес вектора ответов, ограниченного на слой i, больше исходного веса w. Разобьем неизолированные вершины V на q групп согласно q-ичному символу в i-ой координате.

На следующей ступени мы проводим q тестов и находим, какие группы содержат хотя бы один дефект. В дальнейшем мы работаем с каждой группой отдельно, применяя к ним только что описанную схему. В худшем случае (если все время будет отделяться один дефект) нам понадобится $2s-1$ ступень, а общее количество тестов N_T оценивается сверху суммой количества тестов, необходимого для того, чтобы раскидать дефекты по непересекающимся группам, и количества тестов, которое нам придется потратить на поиск единственного дефектного элемента в некой группе. Таким образом, получается оценка

$$N_T \leqslant (s-1)\hat{N}\cdot N' + s\hat{N}\cdot N' + q(s-1),$$

которая при $t \to \infty$ выглядит так

$$N_T \leqslant (2s-1)\log_2 t(1+o(1)).$$

В итоге доказана следующая теорема:

Теорема 4.4.1. *Скорость поиска s дефектов $2s-1$-ступенчатым алгоритмом удовлетворяет неравенству*

$$\frac{1}{2s-1} \leqslant \underline{R}^{(2s-1)}(s) \leqslant \overline{R}^{(2s-1)}(s) \leqslant \frac{1}{s}.$$

Скорость поиска дефектов этим алгоритмом ниже скорости поиска с помощью списочных дизъюнктивных кодов, однако он является конструктивным, в то время как для списочных кодов нет конструкций с ненулевой асимптотической скоростью, а есть только теоремы о существовании таких кодов.

4.5 Таблицы для конечного числа объектов

В этом разделе мы применяем наш четырехступенчатый алгоритм из раздела 4.3 для конкретных значений параметра t. Оценим необходимое число тестов более аккуратно. На первой ступени мы используем $N_1 = \hat{N}\cdot N'$ тестов. В случае, если у нас только один дефект, мы можем его найти на основе результатов тестов первой ступени. Поэтому в дальнейшем будем считать, что у нас ровно два дефекта.

Пусть $W = wN'$ и $W_i = w_i N'$. Если наша раскраска определяется символами из i-го уровня кода X_1, то число подозрительных множеств разбиения равно $\binom{W_i}{W}$, а не q. На следующем этапе нам нужно найти те множества разбиения, которые содержат дефект. Получается, что нам надо решить задачу группового тестирования для двух дефектов, причем объектами являются подозрительные множества разбиения. К тому же нам достаточно найти только

один дефект. Здесь мы используем тривиальную оценку на количество тестов $N_2 \leqslant \binom{W_i}{W} - 2$, которая является точной только для малого числа объектов.

Общее число вершин во всем подозрительных множествах равно

$$\binom{W_1}{W} \cdot \ldots \cdot \binom{W_{\hat{N}}}{W}.$$

Достаточно очевидно, что мощности всех множеств разбиения равны. Поэтому мощность $\hat{t}$ одного подозрительного множества равна

$$\hat{t} = \binom{W_1}{W} \cdot \ldots \cdot \binom{W_{\hat{N}}}{W} / \binom{W_i}{W}$$

Таким образом, на третьей стадии алгоритма нам потребуется $\left\lceil \log_2 \hat{t} \right\rceil$ тестов.

Перед последней стадией алгоритма поиска нам уже известен один из дефектов. На каждом уровне $j \neq i$ у нас есть $\binom{W}{2W-W_j}$ способов выбрать q-ичную координату второго дефекта, но на уровне i осталось не более двух подозрительных координат. Поэтому необходимое число тестов на четвертой стадии не превосходит

$$\left\lceil \log_2 \left(2 \frac{\binom{W}{2W-W_1} \cdot \ldots \cdot \binom{W}{2W-W_{\hat{N}}}}{\binom{W}{2W-W_i}} \right) \right\rceil.$$

Дальше приводятся три таблицы с оптимальными значениями количества тестов для небольших значений $t \leqslant 1000$, для $t = 10^k$, $3 \leqslant k \leqslant 18$, а также для тех значений t, при которых отношение количества тестов к $\log_2 t$ мало.

Таблица 4.1: Количество тестов для $t \leqslant 1000$

t	тесты	t	тесты	t	тесты
8-9	8	29-36	14	126-256	20
10-16	10	37-64	15	257-441	22
17-27	12	65-81	16	442-784	24
28	13	82-125	18	785-1000	25

В таблицах 4.2 и 4.3 также приводится теоретико-информационная нижняя оценка количества тестов $\underline{N}$, которая равна минимальному целому числу, удовлетворяющему неравенству

$$2^{\underline{N}} \geqslant 1 + \binom{t}{1} + \binom{t}{2}.$$

По результатам из таблиц 4.2 и 4.3 видно, что отношение числа тестов к $\log_2 t$ постепенно убывает и стремится к 2.

Таблица 4.2: Количество тестов для $t = 10^k$

$t = q^{N_1}$	тесты	$\underline{\mathrm{N}}$	тесты $/ \log_2 t$
10^3	26	19	2.609
10^4	33	26	2.483
10^5	41	33	2.468
10^6	48	39	2.408
10^7	56	46	2.408
10^8	64	53	2.408
10^9	71	59	2.375
10^{10}	79	66	2.378
10^{11}	86	73	2.354
10^{12}	94	79	2.358
10^{13}	102	86	2.362
10^{14}	109	93	2.344
10^{15}	117	99	2.348
10^{16}	124	106	2.333
10^{17}	132	112	2.337
10^{18}	139	119	2.325

Таблица 4.3: Количество тестов для t с маленьким отношением числа тестов к $\log_2 t$

$q^{N_1} = t$	тесты	$\underline{\mathrm{N}}$	тесты $/ \log_2 t$
$28^2 = 784$	24	19	2.496
$15^3 = 3375$	29	23	2.474
$21^3 = 9261$	32	26	2.428
$28^3 = 21952$	35	28	2.427
$15^4 = 50625$	37	31	2.368
$21^4 = 194481$	41	35	2.334
$21^5 = 4084101$	51	43	2.322
$15^6 = 11390625$	54	46	2.304
$21^6 = 85766121$	60	52	2.277
$21^9 = 794280046581$	89	79	2.251
$21^{11} \approx 3.5 \cdot 10^{14}$	108	96	2.235

Заключение

В настоящей диссертационной работе были получены новые нижние и верхние границы для асимптотических скоростей $\overline{R}_s^{(q)}(s,\ell)$ и $\underline{R}_s^{(q)}(s,\ell)$ разделяющих кодов. Тем не менее, как в случае фиксированного ℓ и $s \to \infty$, так и в случае $s = \ell$, $s \to \infty$, между верхними и нижними границами остается зазор, по порядку равный логарифму от самих оценок.

Также в диссертации были установлены верхние оценки асимптотической скорости дизъюнктивных кодов со списочным декодированием, обобщающие ранее доказанные границы для классических дизъюнктивных кодов. Представляет интерес порядок главного члена асимптотики скорости списочных дизъюнктивных кодов $R_L(s)$ при $s \to \infty$. На текущий момент существуют две гипотезы, которые следуют из доказанных верхней и нижней границ: L/s^2 и $L \ln s/s^2$.

Кроме того, в диссертации доказаны новые оценки для пропускной способности $C(s)$ почти дизъюнктивных кодов. В дальнейшем интересно было бы найти константу в асимптотике пропускной способности почти дизъюнктивных кодов $C(s)$. Сейчас известно только, что $(1 + o(1)) \ln 2/s \leqslant C(s) \leqslant 1/s$.

Наконец, были рассмотрены многоступенчатые алгоритмы поиска дефектов в задаче группового тестирования. В частности, был предложен четырехступенчатый алгоритм поиска двух дефектов, достигающий теоретико-информационной границы сложности. Дальнейшее исследование темы может быть связано с поиском достигающих теоретико-информационной границы алгоритмов с ограниченным числом ступеней для произвольного числа дефектов.

Литература

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

[2] Дьячков А.Г., Рыков В.В. Применение кодов для канала с множественным доступом в системе связи АЛОХА // *Тр. VI Всесоюзн. школы-семинара по вычислительным сетям*, Москва - Винница, **4** (1981), 18–24.

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

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

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

[6] Пинскер М.С., Сагалович Ю.Л. Нижняя граница мощности кода состояний автомата // *Пробл. передачи информ.*, **8**:3 (1972), 59–66.

[7] Сагалович Ю.Л. Метод повышения надежности конечного автомата // *Пробл. передачи информ.*, **1**:2 (1965), 27–35.

[8] Сагалович Ю.Л. Верхняя граница мощности кода состояний автомата // *Пробл. передачи информ.*, **9**:1 (1973), 73–83.

[9] Сагалович Ю.Л. Кодирование состояний и надежность автоматов // *М.: Связь*, 1975.

[10] Сагалович Ю.Л. Каскадные коды состоянии автомата // *Пробл. передачи информ.*, **14**:2 (1978), 132–138.

[11] Сагалович Ю.Л. Полностью разделяющие системы // *Пробл. передачи информ.*, **18**:2 (1982), 74–82.

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

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

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

[15] Barg A., Blakley G.R., Kabatiansky G.A. Digital fingerprinting codes: Problem statements, constructions, identification of traitors // *IEEE Trans. Inf. Theory*, **49**:4 (2003), 852–865.

[16] Barg A., Kabatiansky G.A. Robust parent-identifying codes and combinatorial arrays // *IEEE Trans. Inf. Theory*, **59**:2 (2013), 994–1003.

[17] Boneh D., Shaw J. Collusion-secure fingerprinting for digital data // *IEEE Trans. Inform. Theory*, **44**:5 (1998), 1897–1905.

[18] Cicalese F. Fault-Tolerant Search Algorithms // *Monographs in Theoretical Computer Science–An EATCS Series*, Springer-Verlag, **15**, 2013.

[19] Cohen G.D., Schaathun H.G. Asymptotic overview on separating codes // *Tech. Report 248*, Department of Informatics, University of Bergen, Bergen, Norway, 2003.

[20] Coppersmith D., Shearer J. New Bounds for Union-free Families of Sets // *Journal of Combinatorics*, **5** (1998), 581–596.

[21] Damaschke P., Sheikh Muhammad A. A toolbox for provably optimal multistage strict group testing strategies // *International Computing and Combinatorics Conference*, Springer Berlin Heidelberg, (2013), 446–457.

[22] Damaschke P., Sheikh Muhammad A., Wiener G. Strict group testing and the set basis problem // *Journal of Combinatorial Theory, Series A*, **126** (2014), 70–91.

[23] De Bonis A., Gasieniec L., Vaccaro U. Optimal two-stage algorithms for group testing problems // *SIAM J. Comp.*, **34**:5 (2005), 1253–1270.

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

[25] D'yachkov A.G. Lectures on Designing Screening Experiments // *Com2MaC Lect, Note Ser.*, **10** 2003.

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

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

[28] D'yachkov A.G., Rashad A.M. Universal Decoding for Random Design of Screening Experiments // *Microelectronics and Reliability*, **29**:6 (1989), 965–971.

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

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

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

[32] D'yachkov A.G., Vilenkin P.A., Macula A.J., Torney D.C., Families of Finite Sets in Which No Intersection of ℓ Sets Is Covered by the Union of s Others // *Journal of Combinatorial Theory, Series A*, **99**:2 (2002), 195–218.

[33] D'yachkov A.G., Vilenkin P.A., Macula A.J., Torney D.C., Yekhanin S.M. New Results in the Theory of Superimposed Codes // *Proc. of ACCT-7*, Bansko, (2000), 126–136.

[34] D'yachkov A.G., Vilenkin P.A., Yekhanin S.M. Upper Bounds on the Rate of Superimposed (s, ℓ)-Codes Based on Engel's Inequality // *Proc. of ACCT-8*, Tsarskoe Selo, (2002), 95–99.

[35] Engel, K. Interval Packing and Covering in the Boolean Lattice // *Combinatorics, Probability and Computing*, **5**:4 (1996), 373–384.

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

[37] Gallager R.G. Information Theory and Reliable Communication // *New York, Wiley*, **2**, 1968.

[38] Kautz W.H., Singleton R.C. Nonrandom Binary Superimposed Codes // *IEEE Trans. Inform. Theory.*, **10**:4 (1964), 363–377.

[39] Korner J., Simonyi G. Separating Partition Systems and Locally Different Sequences // *SIAM J. Discrete Math.*, **1**:3 (1988), 355–359.

[40] Macula A.J., Rykov V.V., Yekhanin S., Trivial two-stage group testing for complexes using almost disjunct matrices // *Discrete Applied Mathematics*, **137**:1 (2004), 97–107.

[41] Mago G. Monotone Functions in Sequential Circuits // *IEEE Trans. Comput.*, **22**:10 (1973), 928–933.

[42] McEliece R.J., Rodemich E.R., Rumsey H.C., Welch L.R. New Upper Bounds on the Rate Of Code Via Delsarte-MacWilliams Inequalities // *IEEE Trans. Inform. Theory*, **23**:2 (1977), 157–166.

[43] Mitchell C.J., Piper F.C. Key Storage in Secure Networks // *Discrete Appl. Math.*, **21**:3 (1988), 215–228.

[44] Nguyen Quang A., Zeisel T. Bounds on Constant Weight Binary Superimposed Codes // *Problems of Control and Inform. Theory.*, **17**:4 (1988), 223–230.

[45] Rashad A.M. Random Coding Bounds on the Rate for List-Decoding Superimposed Codes // *Problems of Control and Informatio Theory*, **19**:2 (1990), 141–149.

[46] Shangguan C., Wang X., Ge G., Miao Y. New Bounds For Frameproof Codes // *arXiv preprint arXiv:1411.5782*, 2014.

[47] Staddon J.N., Stinson D.R., Wei R. Combinatorial properties of frameproof and traceability codes // *IEEE Trans. Inform. Theory*, **47**:3 (2001), 1042–1049.

[48] Stinson D. R., Wei R., Chen K. On generalized separating hash families // *Journal of Combinatorial Theory, Series A*, **115**:1 (2008), 105–120.

[49] Stinson D.R., Zaverucha G.M. New bounds for generalized separating hash families // *Technical Report 2007-21, Center for Applied Cryptographic Research*, University of Waterloo, 2007.

[50] Stinson D.R., Zaverucha G.M. Some improved bounds for secure frameproof codes and related separating hash families // *IEEE Transactions on Information Theory*, **54**:6 (2008), 2508–2514.

[51] Vilenkin P.A. On Constructions of List-Decoding Superimposed Codes // *Proc. of ACCT-6*, Pskov, (1998), 228–231.

Публикации автора

[52] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю. Границы скорости дизъюнктивных кодов // *Пробл. передачи информ.*, **50**:1 (2014), 31–63.

[53] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю. Почти дизъюнктивные коды со списочным декодированием // *Пробл. передачи информ.*, **51**:2 (2015), 27–49.

[54] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Cover-free codes and separating system codes // *Designs, Codes and Cryptography*, (2016), doi:10.1007/s10623-016-0265-9.

[55] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Almost cover-free codes and designs // *Designs, Codes and Cryptography*, (2016), doi:10.1007/s10623-016-0279-3.

[56] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Symmetric disjunctive list-decoding codes // *Designs, Codes and Cryptography*, (2016), doi:10.1007/s10623-016-0278-4.

[57] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Almost Disjunctive List-Decoding Codes // *Proc. of ACCT-14*, Svetlogorsk, (2014), 115–126.

[58] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Bounds on the Rate of Superimposed Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Honolulu, (2014), 2341–2345.

[59] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Almost Cover-Free Codes and Designs // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2899–2903.

[60] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Cover-Free Codes and Separating System Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2894–2898.

[61] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Symmetric Disjunctive List-Decoding Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2236–2240.

[62] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. Threshold Decoding for Disjunctive Group Testing // *Proc. of ACCT-15*, Albena, 2016.

[63] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. On Multistage Learning a Hidden Hypergraph // *Proc. IEEE Int'l Symp. Inf. Theory*, Barcelona, 2016.

[64] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu. On a Hypergraph Approach to Multistage Group Testing Problems // *Proc. IEEE Int'l Symp. Inf. Theory*, Barcelona, 2016.