Федеральное государственное бюджетное учреждение науки
Институт проблем передачи информации им. А.А. Харкевича
Российской академии наук (ИППИ РАН)

На правах рукописи

Лебедев Владимир Сергеевич

Коды для каналов множественного доступа и задачи комбинаторного поиска

Специальность 05.13.17 — Теоретические основы информатики

ДИССЕРТАЦИЯ
на соискание ученой степени
доктора физико–математических наук

Москва — 2021

Содержание

Введение

Актуальность темы

Разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации часто приводит к математическим моделям обработки информации, которые описываются каналом множественного доступа (КМД).

Рассмотрим несколько задач, которые имеют различные приложения.

Первая задача может быть сформулирована следующим образом. Сколько надо задать вопросов с ответами да–нет, чтобы найти некоторое загаданное число от 1 до M, если среди ответов может быть не более t неправильных?

Если все вопросы задаются одновременно, а потом мы получаем одновременно все ответы, то подобный поиск называется неадаптивным. Если при выборе следующего вопроса мы можем использовать результаты предыдущих, то поиск называется адаптивным. Мы будем интересоваться только адаптивным поиском для данной задачи. Отметим, что сформулированная задача с неадаптивным поиском эквивалентна классической задаче теории кодирования.

Вторая задача может быть сформулирована следующим образом. Рассмотрим множество, состоящее из M элементов и содержащее не более, чем d дефектных элементов. Требуется выявить все дефектные элементы на основании наименьшего числа групповых тестов. Каждый тест соответствует выбору тестируемой группы элементов, и в дизъюнктивной модели результат теста положителен, если хоть

один дефектный элемент попал в тестируемую группу. Также важна задача, когда результат теста показывает сколько дефектных элементов попало в тестируемую группу.

Третья задача имеет важные приложения для криптографии. Пусть имеется T пользователей и N секретных ключей. Каждый пользователь имеет свой набор ключей, и группа пользователей может вести обмен информацией, если найдется общий для всей группы секретный ключ. Мы хотим, чтобы для любой группы из w пользователей и группы из r других пользователей нашелся такой ключ, что все пользователи первой группы имеют этот ключ и, тем самым, могут вести обмен информацией, тогда как ни у одного из r пользователей второй группы этого ключа нет. Тем самым, пользователи первой группы могут обмениваться информацией секретно от пользователей второй группы.

Естественно, что нам хотелось бы минимизировать число секретных ключей при фиксированном числе пользователей или, что тоже самое, максимизировать число пользователей при фиксированном числе ключей.

Рассмотрим эти задачи с точки зрения канала множественного доступа.

Математическая модель канала множественного доступа (КМД) представляет из себя дискретный канал, имеющих d входов и один выход. Через КМД посимвольно передаются последовательности q-ичных символов из алфавита $0, 1, \ldots, q-1$ длины n, представляющие из себя закодированные сообщения. Набор из M таких сообщений мы будем называть кодом, если для любого набора из d сообщений, которые поступают на вход канала, можно их восстановить

по последовательности длины n на выходе. Задача для КМД состоит в том, чтобы для фиксированного количества сообщений минимизировать длину n, или (что эквивалентно) при фиксированном n максимизировать число сообщений M.

Можно рассмотреть немного другую постановку задачи для КМД. Разобьем M последовательностей длины n на d групп и скажем, что имеется d пользователей, у каждого из которых свой код для передачи информации. Эти пользователи ведут передачу одновременно через канал множественного доступа. Тогда условие, что для любого набора из d сообщений, которые поступают на вход канала, можно их восстановить по последовательности длины n на выходе вытекает, что такая передача возможна.

Свойства КМД активно изучаются на протяжении многих десятилетий. Отметим иследования Алсведе Р. [91], [90], Бассалыго Л.А. [3], [4], Бурнашева М.В. [14], [15], Дьячкова [32], [29], [30], Зиновьева В.А. [42], [50], [54], [55], [56], [57], Зяблова В.В. [61], [62], [63], [64], Кабатянского Г.А. [21], Леонтьева В.К. [74], [75], Пинскера М.С [5], [6], Прелова В.В. [7], Райгородского А.М. [164], [83], Сагаловича Ю.Л. [87], Цитовича И.И. [88], Цыбакова Б.С. [79], Шеннона [166], которые наиболее близки к тематике рассматриваемых в диссертации проблем. Вместе с тем, имеется и много нерешенных задач, актуальных для теории информации, которые описываются в терминах КМД и являются предметом рассмотрения настоящей диссертации.

Если мы рассмотрим канал, в котором возможны ошибки, но $d = 1$, то получим одну из задач обеспечения помехоустойчивости информационных коммуникаций для целей передачи информации.

Задачу с адаптивным тестированием (первая задача, сформули-

рованная выше) называют задачей Улама, или задачей Реньи-Улама и она имеет много важных приложений (см. [1]). Впервые задачу угадывания с возможностью ложных ответов сформулировал венгерский математик Альфред Реньи (см. [165]). Большую роль в исследовании этой задачи сыграли результаты, полученные Берлекампом (см. [103]). Эта задача приобрела популярность после того, как в своей автобиографии "Приключения математика" (см. [174]) американский математик Станислав Улам задал подобный вопрос для $M = 10^6$. Для данного значения M, точнее для $M = 2^{20}$, эта задача решена. Минимальное число вопросов $N(2^{20}, t)$ в задаче с адаптивным тестированием задается таблицей

t	0	1	2	3	4	5	6	7	8	9
$N(2^{20}, t)$	20	25	29	33	37	40	43	46	50	53

и при $t \geq 8$ имеем $N(2^{20}, t) = 3t + 26$.

Для произвольного значения M точный ответ известен только для небольших значений t (см. [162], [116]). Асимптотически точный ответ для двоичного случая был получен в работе [41] .

Нас будет интересовать обобщение данной задачи на q-ичный случай (см. [98]). Рассмотрим множество, состоящее из M элементов. Мы разбиваем множество $[M]$ на q подмножеств S_0, S_1 $\ldots S_{q-1}$. Ответ показывает в какой группе находится загаданное число. Сколько надо задать таких вопросов, чтобы найти некоторое загаданное число от 1 до M, если среди ответов может быть не более t неправильных?

С точки зрения канала множественного доступа, получаем задачу передачи информации по q-ичному каналу, при наличии без-

ошибочной обратной связи. Эта задача для фиксированного числа ошибок изучалась в работах [113], [114], [91]. Для случая одиночной ошибки точный ответ был получен Аигнером [99] и Малиновским [160] независимо. Случай двух и трех ошибок был решен Деппе [116]. Отметим обзор Хила о поиске с лжецами [143], написанный в 1995 году. В этом обзоре он хорошо осветил результаты для фиксированного числа объектов, среди которых ведется поиск. В 2002 году Пелс написал научно-популярный обзор "Поисковые игры с ошибками – пятьдесят лет борьбы с лжецами" ([163]).

Интересно, что в случае фиксированного числа ошибок для получения асимптотически точного ответа достаточно одноразовой обратной связи (см. [3]).

Ссылки на другие интересные результаты можно найти в книгах [131], [132], [112]. Таким образом, обобщения двоичного случая на случай $q > 2$ в основном получены для фиксированного числа ошибок.

Возникает вопрос, можно ли обобщить известные результаты на случай $q > 2$, когда доля ошибок линейна по сравнению с кодовой длиной.

Перейдем к рассмотрению следующей, не менее популярной задачи. Рассмотрим множество, состоящее из M элементов и содержащее не более, чем d дефектных элементов. Если рассмотреть все такие множества и заменить недефектные элементы на 0, а дефектные на 1, то получим множество X двоичных векторов длины M и веса не более, чем d. Наша задача – выявить все дефектные элементы на основании наименьшего числа вопросов (групповых тестов). Дефектные элементы выглядят в точности так же, как правильные,

поэтому единственно возможный путь в нахождении дефектных элементов - это групповое тестирование. Иначе говоря, нам надо определить неизвестный вектор $x \subset X$, обходясь минимальным числом вопросов.

Определим, что каждый вопрос соответствует выбору тестируемой группы $S \subseteq [M]$ (через $[M]$, как обычно, обозначено множество целых чисел от 1 до M). Фактически, мы разбиваем множество $[M]$ на два подмножества $S_1 = S$ и $S_0 = M \setminus S$. Ответы зависят только от числа дефектных элементов, попавших в тестируемую группу. По сути, правила, по которым даются ответы на вопросы, и описывают модель тестирования.

Пусть $N_n(d)$ максимальное число элементов, среди которых можно найти d дефектных элементов за n тестов. Для адаптивного алгоритма $a = a(N, d, n)$ обозначим через $a_n(d)$ максимальное число элементов, для которых доказано, что данная проблема решается за n тестов, то есть алгоритм a является успешным. Таким образом, $a_n(d)$ является нижней границей для $N_n(d)$.

Для случая одной фальшивой монеты решения подобных задач давно известны. Удивительно, но уже для случая двух фальшивых монет, точный ответ на большинство подобных задач до сих пор неизвестен.

Таким образом, для задачи нахождения значения $N_n(2)$ точный ответ не получен и это является трудной комбинаторной проблемой.

В работе [109] авторы получили верхнюю границу
$N_n(2) \leq \lfloor 2^{(n+1)/2} - 1/2 \rfloor$ и для предложенного ими алгоритма поиска l доказали, что $\frac{l_n(2)}{N_n(2)} > 0.95$.

Этот результат был улучшен в [110], где предложенный алгоритм

поиска u давал оценку $\frac{u_n(2)}{N_n(2)} > 0.983$. Более того, в [110] также было показано, что для алгоритма поиска v существует такое n_0, что $\frac{v_n(2)}{N_n(2)} > 0.995$ для $n \geq n_0$.

Отметим еще несколько работ по данной тематике.

В работе [173] предложен алгоритм поиска для числа элементов, которые представляются некоторыми суммами чисел Фибоначчи. Данный результат уступает приведенным выше оценкам при большом числе элементов.

В [175] предложен алгоритм поиска p и показано, что $\frac{p_n(2)}{N_n(2)} > 0.991$ если $n \geq 22$.

Возникает вопрос о построении алгоритма, который бы дал константу, равную единице.

Также задача нахождения дефектных элементов в дизъюнктивной модели тесно связана с дизъюнктивными кодами. Дизъюнктивные s-коды и s-планы были введены У. Каутцом и Р. Синглтоном в 1964 году в основополагающей статье [149], где также получены первые нетривиальные свойства и описан ряд прикладных задач.

Двоичная матрица $C = \|c_{ij}\|$ размера $n \times M$ называется дизъюнктивным s-кодом, если для любого столбца с номером k и любого подмножества $J \subset [M]$, не содержащего в себе k, мощности $|J| = s$, существует координата $i \in [N]$ такая, что $c_{ij} = 1$ для $j = k$ и $c_{ij} = 0$ для всех $j \in J$.

Асимптотической скоростью дизъюнктивных s-кодов будем называть величину

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

где $t(s, N)$ означает максимальный объем дизъюнктивных s-кодов длины N.

В частности, в работе [149] показано

$$R(s) \le R(\le s) \le R(s-1).$$

В случае $s = 2$ в 1982 году П. Эрдеш и др. [135] доказали оценки, из которых следуют неравенства

$$0.182 \le R(2) \le 0.322.$$

Эти неравенства представляют из себя наилучшие известные нижнюю и верхнюю границы для $R(2)$ и в настоящее время. В том же 1982 году А.Г. Дьячков и В.В. Рыков [30] иным методом вывели верхнюю границу, которая в случае $s = 2$ совпадает с правой частью приведенного выше неравенства а при $s \to \infty$ асимптотически эквивалентна неравенству

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

Нижняя граница скорости $R(s)$ была получена в 1983 году А.Г. Дьячковым и В.В. Рыковым в работе [31], из которой следует асимптотическое неравенство

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

Определенный интерес представляет собой работы, написанные независимо П. Эрдешом и др. в 1985 году [136] а также Ф. Хвангом В. и Сосом в 1987 году [144], которые, в частности, содержат следующую оценку

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

А.Г. Дьячков и др. [126] впоследствие улучшили результат 1983 года и в 1989 году новым методом доказали нижнюю границу для скорости $R(s)$, из которой при $s \to \infty$ получается асимптотическое неравенство:

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

Естественное обобщение дизъюнктивных s-кодов на случай (w, r) кодов появилось в [161], в которой подобные коды рассматривались в связи с проблемами криптографии (третья задача, описанная выше).

Кодом, свободным от (w, r) перекрытий, называется семейство подмножеств $\mathcal{A} = \{A_1, \ldots, A_T\}$ множества $[N] = \{1, 2, \ldots, N\}$, если для любых I, J подмножеств $[T] = \{1, 2, \ldots, T\}$, таких что $|I| = w$, $|J| = r$ и $I \cap J = \mathcal{O}$, выполняется условие

$$\bigcap_{i \in I} A_i \nsubseteq \bigcup_{j \in J} A_j.$$

Это определение эквивалентно следующему определению кодов:

Двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется кодом, свободным от (w, r) перекрытий, если для любой пары непересекающихся подмножеств $J_1, J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует координата $i \in [N]$ такая, что $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$.

Имеется тесная связь указанных кодов с разделяющими системами (подробное описание результатов по $(1, 2)$ и $(2, 2)$ разделяющим системам можно найти в [86], [87]).

Основной задачей для кодов, свободных от (w, r) перекрытий, является нахождение максимального числа столбцов $T(N, w, r)$ для данного числа строк N, или минимального числа строк $N(T, w, r)$

для заданного числа столбцов T. Для случая $w = r = 1$ задача нахождения точного значения величины $T(N, w, r)$ полностью решена: $T(N, 1, 1) = \binom{N}{\lfloor N/2 \rfloor}$ (теорема Шпернера).

В общем случае известны лишь несколько примеров оптимальных кодов, свободных от (w, r) перекрытий, и различные оценки величины $N(T, w, r)$ для больших T (см. [128], [133], [170]).

Верхняя граница для скорости $(2, 2)$ кодов была получена Сагаловичем в [87], который использовал идею рассмотрения кода, длина которого является кодовым расстоянием другого кода.

Возникает вопрос обобщения этой идеи на случай произвольных (w, r).

В статье Эрдеша и Реньи [134] рассматривалась следующая задача поиска фальшивых монет на точных весах. Предположим, что настоящая монета весит 10 гр., а фальшивая – 9 гр. Если на весы положили L монет и их (суммарный) вес равен W, то среди взвешенных монет ровно $s = 10L - W$ фальшивых. На языке теории группового тестирования (или планирования эксперимента) это означает, что результатом теста является число дефектных элементов (т.е. фальшивых монет) среди тестированных.

Пусть имеется n монет, занумерованных множеством $\{1, \ldots, n\}$, и пусть $X \subset \{1, \ldots, n\}$ – это множество фальшивых монет и нет ограничения на число фальшивых монет. Будем рассматривать неадаптивный поиск (или поиск без обучения), когда все тесты-взвешивания заранее запланированы. Можно представлять это как то, что все взвешивания осуществляются одновременно на нескольких весах, т.е. это *параллельный* поиск в отличие от последовательного, т.е. адаптивного, поиска.

Далее, пусть имеется m весов-взвешиваний. Обозначим через $H_i \subset \{1, \ldots, n\}$ множество монет, которые взвешиваются на i-ых весах, и через $s_i = |X \cap H_i|$ результат взвешивания. Введем двоичный вектор "состояния" $x = (x(1), \ldots, x(n))$, как характеристический вектор множества X, т.е. $x(i) = 0$, если i-ая монета настоящая, и $x(i) = 1$, если i-ая монета фальшивая. Сопоставим набору (плану) взвешиваний двоичную $m \times n$ матрицу H, строками h_i которой являются характеристические векторы множеств H_i. Тогда для вектора результатов взвешиваний $s = (s_1, \ldots, s_m)$ справедливо соотношение $s_i = (x, h_i)$ или, что равносильно,

$$Hx^T = s,$$

где умножение матрицы на вектор понимается как умножение над полем рациональных чисел $\mathbb{Q}$, а не в конечном поле. Отметим, что за этим исключением, данное уравнение выглядит так же, как синдромное уравнение в теории кодирования. Очевидно, что план взвешиваний позволяет найти фальшивые монеты тогда и только тогда, когда данное уравнение относительно x имеет единственное двоичное решение. Будем называть такую матрицу H *разрешающей матрицей.*

Линдстрем [158] построил разрешающие $m \times n$ матрицы, где $n = n(m)$ равно суммарному количеству единиц в двоичных представлениях всех натуральных чисел, не превосходящих m. Т.е.

$$n(m) = \sum_{i=1}^{m} wt(\mathbf{i}),$$

где $wt(\mathbf{i})$ – это вес Хэмминга вектора $\mathbf{i}$, равного двоичному представлению числа i. В частности, для $n = k2^{k-1}$ разрешающая матрица из

[158] имеет $2^k - 1$ строк и в [106] независимо была предложена рекуррентная конструкция таких множеств. Отметим, что рекуррентная конструкция [106] была обобщена в [82] для произвольной размерности n.

Возникает вопрос изучения кодов, связанных с суммирующим каналом для случая $q > 2$.

Описание других интересных моделей комбинаторного поиска и группового тестирования можно найти в [131] и [132]. На русском языке основные проблемы теории поиска, наряду с проблемами сортировки и идентификации, хорошо изложены в [89].

Следовательно, актуальной является задача разработки новых методов и алгоритмов кодирования информации в канале множественного доступа, позволяющих на основании комбинаторного подхода получать более точные оценки характеристик некоторых кодов, используемых для передачи и защиты информации.

Цель работы

Целью диссертационной работы является разработка методов получения более точных оценок характеристик некоторых кодов, используемых для передачи и защиты информации, в том числе обслуживающих некоторые каналы множественного доступа. Для этого необходимо:

-для задачи Улама получить новый подход с точки зрения КМД, позволяющий обобщить результаты Берлекампа на q-ичный случай $(q > 2)$;

-для дизъюнктивной модели ввести композиционное расстояние, чтобы применить подход из теории кодирования и КМД для получе-

ния более точных верхних границ для скорости кодов, свободных от (w, r) перекрытий;
-для случая двух пользователей в дизъюнктивной модели построить алгоритм кодирования, дающий оптимальную константу при главном члене асимптотического разложения;
-для суммирующего канала целью было дальнейшее исследование задач, обобщающих двоичный суммирующий канал на q-ичный случай.

Научная новизна

работы состоит в том, что в ней впервые предложен комбинаторный подход рассмотрения задач поиска с точки зрения методов теории кодирования, позволяющий получить следующие научные результаты:

1. Предложен новый метод исправления ошибок для q-ичного канала с безошибочной обратной связью.

2. Впервые введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием.

3. Предложен новый алгоритм поиска двух дефектных элементов, позволяющий получить оптимальную константу при главном члене для общего числа элементов.

4. Для суммирующего канала обобщен результат Линдстрема на случай $q = 3$ и $q = 4$.

Все результаты, представленные в диссертации, являются новыми.

Основные положения, выносимые на защиту:

1. Для передачи информации по q-ичному каналу с безошибочной обратной связью предложен новый подход к исправлению ошибок, позволяющий обобщить результаты Берлекампа, полученные для двоичного канала.

2. Полученные автором границы для композиционного расстояния позволяют для дизъюнктивной модели доказать оптимальность некоторых кодов, свободных от (w, r) перекрытий, и улучшить верхнюю границу на скорость таких кодов.

3. Получен алгоритм поиска двух дефектных элементов, позволяющий получить оптимальную константу при главном члене для общего числа элементов.

4. Для суммирующего канала обобщен результат Линдстрема на случай $q = 3$ и $q = 4$.

Основные методы исследования

В работе используются методы комбинаторной теории кодирования.

Теоретическая и практическая ценность работы

Работа носит теоретический характер. Результаты работы могут применяться в дальнейших исследованиях в области теории кодиро-

вания, криптографии и комбинаторного поиска. Также результаты работы могут быть использованы в разных практических областях – в практической криптографии, медицине, биологии и др.

Апробация диссертации

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

1. Семинар по теории кодирования под рук. Л.А. Бассалыго в 2002–2019 гг., ИППИ РАН.

2. Семинар по дискретной математике под рук. С.П. Тарасова в 2010 г., МИАН.

3. Семинар по дискретной математике под рук. Ш.Кима в 2000-2003 г., Пхоханский университет науки и технологии.

4. Семинар по дискретной математике под рук. Р. Алсведе в 2001–2010 г., Университет Билефельда.

5. Семинар по дискретной математике под рук. Крамера в 2017-2018 г., Мюнхенский технический университет.

Результаты диссертации докладывались автором на следующих конференциях.

1. Eighth International Workshop on Algebraic and Combinatorial Coding Theory, September 8-14. 2002, Tsarskoe Selo (Russia).

2. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory. Kranevo, Bulgaria. June 19-25, 2004.

3. Tenth International Workshop on Algebraic and Combinatorial Coding Theory, September 3-9. 2006, Zvenigorod (Russia).

4. Eleventh Int. Workshop on Algebraic and Combinatorial Coding Theory. Pamporovo, Bulgaria. June 16-22, 2008.

5. Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, September 5-11. 2010, Novosibirsk (Russia).

6. Thirteenth Int. Workshop on Algebraic and Combinatorial Coding Theory. Pomorie, Bulgaria. June 15-21, 2012.

7. Seventh International Workshop on Optimal Codes and Related Topics, September 6-12. 2013, Albena (Bulgaria).

8. Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, September 7-13. 2014, Svetlogorsk (Russia).

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

10. 15th International Workshop on Algebraic and Combinatorial Coding Theory, Albena, Bulgaria, 2016.

11. Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2018, Sep 2018, Svetlogorsk (Russia).

12. IEEE International Symposium on Information Theory (ISIT), July 7-12, Paris, 2019.

13. Algebraic and Combinatorial Coding Theory (ACCT), IEEE, Bulgaria, 2020

14. IEEE International Symposium on Information Theory (ISIT), June 21-26, Los-Angeles, 2020.

Личный вклад автора

Основные результаты диссертации получены автором лично или при непосредственном его участии.

Благодарности

Автор выражает глубокую благодарность Л.А. Бассалыго за полезные обсуждения и ценные замечания, а также слушателям семинара по теории кодирования в ИППИ РАН за полезные замечания и проявленную заинтересованность в результатах работы.

1 Кодирование при наличии бесшумной обратной связи

1.1 Основные определения

Основной проблемой в теории кодирования является задача нахождения верхних и нижних границ на максимальный размер $M(n,t,q)$ кода, исправляющего t ошибок на длине n над алфавитом $\mathcal{Q} = \{0,1,\ldots,q-1\}$. Предположим, что мы имеем безошибочную обратную связь, что соответствует адаптивному поиску при наличии не более t неверных ответов.

Рассмотрим канал с одним отправителем (кодером) и одним принимающим (декодером). На входе и выходе канала используется один и тот же q-ичный алфавит $Q = \{0,1,\ldots,q-1\}$. Будем предполагать, что имеется безошибочная обратная связь. Это означает, что после того, как кодер посылает элемент x_i в канал, он знает какой элемент y_i был принят на выходе канала и может использовать эту информацию при дальнейшей передаче. Пусть имеется конечное множество сообщений $[M] = \{1,\ldots,M\}$ и один из его элементов предоставляется кодеру для передачи по каналу. Данное сообщение $m \in [M]$ кодируется функцией $\phi^m = (\phi_1^m, \phi_2^m, \ldots, \phi_n^m)$ так, что

$$x_i = \phi_i^m(y_1,\ldots,y_{i-1}).$$

Мы предполагаем, что число неправильно переданных символов на длине n не превосходит t и декодер имеет систему множеств $\{D_m : m \in [M] \quad D_m \subset Q^n\}$ так, что $D_i \cap D_j = \emptyset$ для $i \neq j$ с помощью которой по полученной последовательности он может восстановить

какое сообщение передавалось по каналу.

Определение 1. *Кодом, исправляющим t ошибок в канале с безошибочной обратной связью называется система пар $\{(\phi^m, D_m) : m \in [M]\}$ со свойствами, описанными выше.*

Обозначим через $\tau = t/n$ долю ошибок в канале и через $R = \log_q M/n$ скорость кода, передающего M сообщений. Как обычно, основной задачей является определение пропускной способности канала $C_q(\tau)$, которая определяется как супремум скорости кодов при больших значениях n. Хорошо известно, что асимптотически $C_q(\tau) \leq H_q(\tau)$, где

$$H_q(\tau) = \begin{cases} 1 - h_q(\tau) - \tau \log_q(q-1) & \text{если } 0 \leq \tau \leq \frac{q-1}{q} \\ 0 & \text{если } \frac{q-1}{q} \leq \tau \leq 1, \end{cases} \tag{1}$$

где $h_q(\tau) = -\tau \log_q \tau - (1-\tau)\log_q(1-\tau)$.

Двоичная энтропия равна $h(\tau) = -\tau \log \tau - (1-\tau)\log(1-\tau)$, и на протяжении всей статьи под $\log \tau$ мы будем понимать логарифм по основанию 2.

Предлагается новый метод решения данной задачи, отличный от методов, используемых Берлекампом. Основная идея состоит в том, что кодер при возникновении ошибок прекращает передачу информационных символов и занимается исправлением этих ошибок. После того, как появившиеся ошибки исправлены, передача информации возобновляется.

Для исправления ошибок используется нулевой символ, который стирает символ, идущий перед ним. Такой алгоритм называется алгоритмом 1-удаления, и он показывает, что для $\frac{1}{q} \leq \tau \leq \frac{1}{2}$ справедливо равенство $C_q(\tau) = (1-2\tau)\log_q(q-1)$.

Асимптотически точный ответ для произвольного значения t получить не удалось.

Заметим, что в недавней работе [118] был получен асимптотически точный ответ для произвольного значения t, если рассматривать канал передачи, в котором ошибка меняет передаваемый символ не произвольным образом, а, к примеру, увеличивает значение не более, чем на x (по модулю q). Было доказано, что для $1 \leq x \leq q/2 - 1$ справедливо равенство

$$C_q^x(\tau) = 1 - h(\tau)\log_q 2 - \tau \log_q x$$

для $\tau \leq x/(x+1)$ и

$$C_q^x(\tau) = 1 - \log_q(x+1)$$

для $\tau > x/(x+1)$

Вернемся к классическому случаю передачи по q-ичному каналу. Имеется последовательность значений t для которых алгоритм близкий к алгоритму 1-удаления дает асимптотически точный ответ.

Вместо одного нуля можно использовать r нулей идущих подряд для удаления. Это асимптотически дает прямые, выходящие из точек $(1/(r+1), 0)$ и являющимися касательными к асимптотической границе Хэмминга, если по оси абсцисс откладывать долю ошибок, а по оси ординат асимптотическую скорость кода.

Дадим более формальное описание данного алгоритма.

1.2 Описание алгоритма r-удаления

Поставим каждому передаваемому сообщению $m \in [M]$ в соответствие информационную последовательность

$m = (m_1, m_2, \ldots, m_{n-(r+1)t})$ не содержащую блока из r нулей идущих подряд.

Алгоритм построения кодовой последовательности $x_1, x_2, \ldots, x_i$ состоит в том, что кодер посылает в канал либо элемент $x_i = m_{p(i)}$ из последовательности m, либо нулевой элемент, если он находится в состоянии исправления ошибок. После того как будет передана последовательность $m = (m_1, m_2, \ldots, m_{n-(r+1)t})$ (если произошло меньшее, чем t число ошибок) кодер может передавать любой ненулевой элемент, например 1, для определенности. Фактически это означает, что

$$m = (m_1, m_2, \ldots, m_{n-(r+1)t}, 1, 1, \ldots).$$

Далее, когда мы говорим, что кодер что-то передает мы будем иметь ввиду, что это элементы информационной последовательности m. При этом кодовый элемент x_i, который посылается в канал, определяется согласно алгоритму передачи и зависит от того, произошли ли ошибки в канале, и какие именно ошибки произошли.

Таким образом, чтобы полностью описать действие алгоритма в момент времени i, необходимо определить состояние кодера (находится ли он в состоянии исправления ошибок, или нет) и для случая, когда кодер не находится в состоянии исправления ошибок описать, как изменяется значение $p(i)$.

Для определения состояния кодера, когда он исправляет ошибки, важнейшую роль играет процесс **r-удаления**. Для последовательности $b_1, b_2, \ldots, b_k$ определим процесс **r-удаления** следующим образом: ищется подпоследовательность $b_i, b_{i+1}, \ldots, b_{i+r-1}$ с минималь-

ным возможным i, так, что

$$b_i = b_{i+1} = \ldots = b_{i+r-1} = 0.$$

После этого из последовательности $b_1, b_2, \ldots, b_k$ получаем последовательность $b_1, b_2, \ldots, b_{i-2}, b_{i+r}, \ldots, b_k$, если $i > 2$ и последовательность $b_{i+r}, \ldots, b_k$, если $i = 1$ или $i = 2$. Далее продолжаем процесс **r-удаления** для новой полученной последовательности. Таким образом, процесс **r-удаления** состоит из итераций удалений, описанных выше.

Обозначим через $S(b_1, b_2, \ldots, b_k)$ число итераций, то есть максимальное возможное число таких удалений.

Например, если к последовательности $0, 5, 0, 0, 0, 3, 8, 0, 0, 7$ применить процесс **2-удаления**, то получим $3, 7$ и

$S(0, 5, 0, 0, 0, 3, 8, 0, 0, 7) = 3$.

Кроме того, обозначим через $T(i)$ число ошибок, которые произошли при передаче последовательности $x_1, x_2, \ldots, x_i$.

В самом начале $p(1) = 1$ и кодер ведет передачу по следующим правилам.

Если $T(i-1) = S(y_1, y_2, \ldots, y_{i-1})$, то $x_i = m_{p(i)}$.

Если $T(i-1) > S(y_1, y_2, \ldots, y_{i-1})$, то $x_i = 0$.

В случае безошибочной передачи ($y_i = x_i$) значение p увеличивается на 1, т.е. $p(i+1) = p(i)+1$. Для того, чтобы определить действия кодера при возникновении ошибки, рассмотрим два случая. Основная идея состоит в том, что кодер передает 0 до тех пор, пока в процессе **r-удаления** не будут удалятся все ошибочные символы.

Пусть при передаче информационного символа $x_i = m_{p(i)}$ произошла ошибка, и передался ненулевой символ $y_i \neq 0$. Тогда ко-

дер посылает в канал ноль до тех пор, пока не найдется минимальное $j > i$ такое, что $T(j) = S(y_1, y_2, \ldots, y_j)$. Каждая новая ошибка будет соответствовать приему ненулевого символа. Условие $T(j) = S(y_1, y_2, \ldots, y_j)$ означает, что все символы $y_i, y_{i+1}, \ldots, y_j$ будут стерты после применения процесса **r-удаления**. Значит в этом случае значение p не меняется ($p(j+1) = p(i)$) и кодер передает $x_{j+1} = x_i = m_{p(i)}$.

Пусть теперь при передаче x_i произошла ошибка и передался нулевой символ $y_i = 0$. Кодер в этом случае проверяет условие $T(j) = S(y_1, y_2, \ldots, y_j)$ для $j \geq i$ и посылает в канал ноль до тех пор, пока не найдется минимальное $j \geq i$ такое, что это условие будет выполнено. И опять каждая новая ошибка будет соответствовать приему ненулевого символа, и каждый ненулевой символ удаляется вместе с r нулями. Условие $T(j) = S(y_1, y_2, \ldots, y_j)$, как и в предыдущем случае, гарантирует, что после применения к последовательности $y_1, y_2, \ldots, y_j$ процесса **r-удаления** все ошибочные символы вместе со стирающими нулевыми символами будут стерты, поэтому получится последовательность $m_1, m_2, \ldots, m_{p'}$. В этом случае вместе с ошибочными символами стираются и нулевые информационные символы, которые находились непосредственно перед $m_{p(i)}$. Можно заметить, что $m_{p'}$ это ненулевой символ с максимально возможным индексом, таким, что этот индекс меньше $p(i)$, то есть $m_{p'} \neq 0$ и $p' < p(i)$. Значит в этом случае $p(j+1) = p'$ (если все символы сотрутся, то число $p(j+1)$ становится равным 1 и кодер фактически начинает передачу сначала).

Например, пусть $r = 1$, $t = 2$ и кодер передает 123. Пусть оказалось, что вместо 3 передался 0. $T(3) = S(1, 2, 0) = 1$ и после примене-

ния процесса **1-удаления** получаем 1. Значит $x_4 = 2$. Пусть опять произошла ошибка, и опять передался 0. $T(4) = S(1,2,0,0) = 2$, и после применения процесса **1-удаления** получаем пустую последовательность. Значит $x_5 = 1$ и по описанному алгоритму $x = (1,2,3,2,1,2,3)$, $y = (1,2,0,0,1,2,3)$.

Рассмотрим еще один пример. Кодер передает 3102, а $r = 2$ и $t = 1$. Пусть оказалось, что вместо 2 передался 0. Тогда, после применения процесса **2-удаления**, получаем 3. Значит $p' = 1$, $p(5) = 2$ и кодер вновь передает 1. То есть в этом случае $x = 3102102$, $y = 3100102$.

Возможно алгоритм передачи проще понять, если описать, как будет действовать декодер. Декодер применяет к полученной последовательности процесс **r-удаления** и берет первые $n-(r+1)t$ символов полученной последовательности. Фактически правила передачи для кодера и определялись из этого простого декодирования: кодер может каждый раз применять процесс **r-удаления** и определять какой символ он должен послать в канал, чтобы передача велась корректно.

Обозначим через $g_r(\tau) = \lim_{n\to\infty} \log_q M/n$ функцию, соответствующую асимптотической скорости передачи описанным выше методом, где M число передаваемых сообщений, равное числу последовательностей $(m_1, m_2, \ldots, m_{n-(r+1)t})$ не содержащую блока из r нулей идущих подряд.

Таким образом, доказана следующая теорема

Теорема 1. *Для* $\frac{1}{q} \le \tau \le \frac{1}{2}$ *справедливо равенство*

$$C_q(\tau) = (1 - 2\tau)\log_q(q-1).$$

Кроме этого, докажем, что функция $g_r(\tau)$ является касательной к $H_q(\tau)$, выходящей из точки $(1/(r+1), 0)$.

Касательная к границе Хэмминга имеет вид

$$T_r(\tau) = \log_q \frac{\tau_r}{(1-\tau_r)(q-1)} \cdot \tau + b,$$

где τ_r абсцисса точки касания.

$H_q(\tau_r)$ можно записать в виде

$$H_q(\tau_r) = \log_q \frac{q\tau_r^{\tau_r}(1-\tau_r)^{(1-\tau_r)}}{(q-1)^{\tau_r}}.$$

Следовательно, касательная к границе Хэмминга с абсциссой точки касания τ_r задается уравнением

$$T_r(\tau) = \log_q \frac{\tau_r}{(1-\tau_r)(q-1)} \cdot \tau + \log_q q(1-\tau_r).$$

Если эта касательная проходит через точку $(1/(r+1), 0)$, то

$$\log_q \frac{\tau_r}{(1-\tau_r)(q-1)} \cdot \frac{1}{r+1} = -\log_q q(1-\tau_r).$$

Значит,

$$\frac{(1-\tau_r)(q-1)}{\tau_r} = (q(1-\tau_r))^{r+1}.$$

Если $z_r = q(1-\tau_r)$, то тогда

$$\tau_r z_r^{r+1} = q(1-\tau_r) - (1-\tau_r).$$

$$(1 - z_r/q) z_r^{r+1} = z_r - z_r/q.$$

$$q z_r^{r+1} - z_r^{r+2} = q z_r - z_r.$$

Следовательно, z_r удовлетворяет соотношению

$$z_r^{r+1} = q z_r^r - (q-1).$$

Асимптотически при $n \to \infty$ число последовательностей не содержащих блока из r нулей идущих подряд на длине $n-(r+1)t$ как раз равно $z_r^{n-(r+1)t}$, что хорошо известно (см., например, [12]). Действительно, если обозначить через $F(n)$ число последовательностей не содержащих блока из r нулей идущих подряд на длине n, то $F(n) = qF(n-1) - (q-1)F(n-r-1)$, откуда можно получить требуемый результат.

Следствие 1. *Касательные к $H_q(\tau)$, выходящие из точек $(1/2, 0)$ и $(1/3, 0)$ пересекаются при*

$$\tau^* = \frac{\log_q \lambda - \log_q(q-1)}{3\log_q \lambda - 2\log_q(q-1)},$$

где $\lambda = \frac{(q-1)+\sqrt{(q-1)(q+3)}}{2}$.

Доказательство. Касательная к $H_q(\tau)$, выходящая из точки $(1/2, 0)$ задается уравнением

$$g_1(\tau) = -2\log_q(q-1) \cdot \tau + \log_q(q-1).$$

Касательная к $H_q(\tau)$, выходящая из точки $(1/3, 0)$ задается уравнением

$$g_2(\tau) = -3\log_q \lambda \cdot \tau + \log_q \lambda,$$

где $\lambda = \frac{(q-1)+\sqrt{(q-1)(q+3)}}{2}$.

Следовательно,

$$\tau^* = \frac{\log_q \lambda - \log_q(q-1)}{3\log_q \lambda - 2\log_q(q-1)}$$

является абсциссой точки пересечения этих касательных.

Утверждение 1. *Точка пересечения $\tau^* = \frac{\log_q \lambda - \log_q(q-1)}{3\log_q \lambda - 2\log_q(q-1)}$ находится левее точки $1/(q+1)$ по оси абсцисс.*

Доказательство. Нам нужно показать, что $(q+1)\log_q \frac{\lambda}{(q-1)} < \log_q \frac{\lambda^3}{(q-1)^2}$. Это эквивалентно тому, что $\lambda^{q-2} < (q-1)^{q-1}$. Подставляя выражение для λ получаем

$$((1+\sqrt{\frac{q+3}{q-1}})/2)^{q-2} < q-1. \tag{2}$$

Учитывая то, что $\sqrt{\frac{q+3}{q-1}} < 1 + \frac{5}{q-2}$ получаем, что неравенство (2) верно для всех $q \geq 3$.

1.3 О перечислении q-ичных последовательностей, содержащих подблок 00 фиксированное число раз.

Задача подсчета числа последовательностей длинны n, состоящих из символов $\{0, 1, \ldots, q-1\}$, в которых никакие два нуля не идут подряд давно известна. Для двоичного случая число таких последовательностей совпадает с числами Фибоначчи ($F(n+1) = F(n) + F(n-1)$). Данная связь описана в многих книгах по комбинаторике, в том числе и в популярных (см., например, [19]). Наиболее общие результаты для похожих задач можно найти в [138], [139], [104]. В частности, одним из следствий данных результатов является то, что интересующие нас число q-ичных последовательностей удовлетворяет рекуррентному соотношению

$$F_q(n+1) = (q-1)F_q(n) + (q-1)F_q(n-1) \tag{3}$$

с начальными условиями $F_q(1) = q,\ F_q(2) = q^2 - 1$. Методы решения рекуррентных соотношений с постоянными коэффициентами хорошо

известны [19], [139], [104]. В данном случае все сводится к решению квадратного уравнения $x^2-(q-1)x-(q-1)=0$. Получаем, что

$$F_q(n)=A((q-1)/2+\sqrt{(q-1)(q+3)}/2)^n+$$

$$+B((q-1)/2-\sqrt{(q-1)(q+3)}/2)^n,$$

где константы A и B определяются из начальных условий и равны соответственно

$$A=\frac{\lambda_1^2}{(q-1)(\lambda_1-\lambda_2)} \tag{4}$$

$$B=\frac{-\lambda_2^2}{(q-1)(\lambda_1-\lambda_2)}$$

Нам бы хотелось получить подобную формулу для числа последовательностей, состоящих из символов $\{0,1,\ldots,q-1\}$, в которых два нуля, идущие подряд, встречаются фиксированное число раз. В дальнейшем, на протяжении всей статьи, мы будем придерживаться обозначений $\lambda_1=(q-1)/2+\sqrt{(q-1)(q+3)}/2$ и $\lambda_2=(q-1)/2-\sqrt{(q-1)(q+3)}/2$ и без пояснений использовать то, что $\lambda_1\lambda_2=-(q-1)$ и $\lambda_1+\lambda_2=(q-1)$.

Рассмотрим теперь задачу, которая изучалась в работе [20]. Для двух произвольных q-ичных последовательностей $x=(x_1,x_2,\ldots,x_n)$ и $y=(y_1,y_2,\ldots,y_n)$, где $x_i,y_i\in\{0,1,\ldots,q-1\}$ число

$$H_{st}(x,y)=\sum_{i=1}^{n-1}h_i(x,y),$$

где

$$h_i(x,y=\begin{cases}1 & \text{если } \ x_i=y_i,x_{i+1}=y_{i+1}\\ 0 & \text{в остальных случаях}\end{cases} \tag{5}$$

называется стебельным сходством между x и y.

Число

$$D_{st}(x, y) = (n - 1) - H_{st}(x, y)$$

называется стебельным расстоянием между x и y.

Решалась задача нахождения объема сфер для стебельного расстояния. В работе [20] доказано, что стебельное расстояние является метрикой и объем сферы радиуса r не зависит от центра сферы. Если в качестве центра сферы взять нулевую последовательность, то стебельное сходство с последовательностью x совпадет с количеством подблоков вида 00 в последовательности x. Таким образом, задачи, описанные выше, эквивалентны.

Интерес к задачам, связанных со стебельным сходством и расстоянием, обуславливается связью с задачами молекулярной биологии. Подробнее про рассматриваемые в этой области задачи и о связях таких задач с термодинамическим расстоянием между ДНК-цепочками можно прочитать в [33], [34].

Мы вернемся к результатам, полученным в работе [20] чуть позже, а пока попробуем подсчитать число q-ичных последовательностей, содержащих подблок 00 ровно r раз, рекуррентным методом.

Пусть $f(n, r)$ - число q-ичных последовательностей длины n, содержащих подблок 00 ровно r раз.

Обозначим через $f_a(n, r)$ - число последовательностей с описанным выше свойством, для которых дополнительно известно, что последний n-ый элемент у них равен a, $a \in \{0, 1, \ldots, q - 1\}$. Другими словами, $f_a(n, r)$ - число последовательностей длины n, содержащих подблок 00 ровно r раз и оканчивающихся на символ a.

В дальнейшем мы часто будем обозначать через b какой-то (фик-

сированный) ненулевой элемент. Для $r \geq 1$ справедливы соотношения:

$$f_0(n,r) = f_0(n-1,r-1) + (q-1)f_b(n-1,r).$$

$$f_b(n,r) = f(n-1,r).$$

Таким образом, получаем

$$f(n,r) = (q-1)f(n-1,r) + (q-1)f(n-2,r) + f_0(n-1,r-1). \quad (6)$$

Кроме того, мы будем использовать то, что

$$f_0(n,r) = f_0(n-1,r-1) + (q-1)f(n-2,r). \quad (7)$$

Будем искать решение (6) в виде

$$f(n,r) = (A_r n^r + \ldots + A_1 n + A_0)\lambda_1^n + (A'_r n^r + \ldots + A'_1 n + A'_0)\lambda_2^n \quad (8)$$

Подставим (8) в (6) и приравняем соответствующие коэффициенты, причем для простоты записи будем писать λ без нижнего индекса и использовать то, что $\lambda^2 - (q-1)\lambda - (q-1) = 0$.

Равенство коэффициентов при $n^r\lambda^{n-2}$ приводит к тождеству

$$A_r\lambda^2 = (q-1)A_r\lambda + A_r.$$

Используя аналогичное свойство, получим, что для коэффициентов при $n^{r-1}\lambda^{n-2}$ справедливо соотношение

$$0 = (q-1)(-r\lambda - 2r)A_r + C_{r-1}\lambda,$$

где коэффициент C_{r-1} , был определен на предыдущем шаге, когда мы находили $f_0(n,r-1) = (C_{r-1}n^{r-1} + \ldots + C_1 n + C_0)\lambda^n$. (Отметим,

что $f_0(n,0) = (q-1)f(n-2,0)$, а в дальнейшем, после того, как мы найдем $f(n,s)$, можно вычислить $f_0(n,s)$, используя (7)).

Следовательно, первое уравнение позволяет определить коэффициент A_r.

$$A_r = \frac{\lambda C_{r-1}}{r(q-1)(\lambda+2)} \tag{9}$$

Соотношение коэффициентов при $n^{r-2}\lambda^{n-2}$ дадут уравнение, содержащее только A_r и A_{r-1}, из которого определяем A_{r-1}. И так далее. Будем называть полученную систему уравнений – система уравнений $SUR(r)$.

Другими словами, матрица системы уравнений для A_i будет иметь треугольный вид и ее решение не представляет проблем. Константы A_0 и A'_0 находятся, используя начальные условия для $f(n,r)$.

Таким образом, доказано следующее:

Утверждение 2. *Число q-ичных последовательностей, содержащих подблок* 00 *ровно r раз равно*

$$(A_r n^r + \ldots + A_1 n + A_0)\lambda_1^n + (A'_r n^r + \ldots + A'_1 n + A'_0)\lambda_2^n,$$

где константы A_i и A'_i определяются из системы уравнений $SUR(r)$.

Как уже отмечалось, в работе [20] был предложен метод подсчета $f(n,r)$, который мы будем называть методом стебельного расстояния. Было введено множество

$T(r,k) =$

$\{t^{(k+1)} : t_1 \geq 0, t_{k+1} \geq 0, t_i \geq 1, i = 1,2,\ldots,k, \sum_{i=1}^{k} t_i = n - (r + k)\}$

и доказано следующее утверждение.

Утверждение 3. [20] *Число q-ичных последовательностей, содержащих подблок* 00 *ровно r раз равно*

$$f(n,r) = \sum_{k=1}^{\min\{r,\lceil n-r/2\rceil\}} \binom{r-1}{k-1} \sum_{T(r,k)} \{F^3(t_1) \prod_{i=2}^{k} F^2(t_i) F^3(t_{k+1})\}, \quad (10)$$

где $F^3(n) = (q-1)F_q(n-1)$, *причем* $F^3(1) = (q-1)$, $F^3(0) = 1$; $F^2(n) = (q-1)^2 F_q(n-2)$, *причем* $F^2(2) = (q-1)^2$, $F^2(1) = q-1$.

Напомним, что $F_q(n) = f(n,0)$.

Сравним результаты данных методов, в случае, когда множество $T(r,k)$ легко получить и (10) сводится к обычному суммированию. Рассмотрим случай $r = 1$.

Метод стебельного расстояния в этом случае дает нам

$$f(n,1) = 2(L_1\lambda_1^{n-2} + L_2\lambda_2^{n-2}) + \sum_{i=1}^{n-3} (L_1\lambda_1^i + L_2\lambda_2^i)(L_1\lambda_1^{n-i-2} + L_2\lambda_2^{n-i-2}), \quad (11)$$

где

$$L_1 = \frac{\lambda_1}{\lambda_1 - \lambda_2}, \quad L_2 = \frac{-\lambda_2}{\lambda_1 - \lambda_2}.$$

Коэффициент при $n\lambda_1^n$ будет равен L_1^2/λ_1^2.

Из рекуррентного метода вытекает, что $f(n,1) = (A_1 n + A_0)\lambda_1^n + (A_1' n + A_0')\lambda_2^n$. Мы знаем, что

$$A_r = \frac{A}{r!(\lambda_1 + 2)^r \lambda_1^{r-1}},$$

где A определено в (4), следовательно

$$A_1 = \frac{\lambda_1}{(q-1)(\lambda_1 - \lambda_2)(\lambda_1 + 2)}.$$

Константы при $n\lambda_1^n$, полученные этими методами совпадают, так как

$$\lambda_1(\lambda_1 - \lambda_2) = (q-1)(\lambda_1 + 2).$$

Аналогичным образом можно проверить совпадение коэффициентов при $n\lambda_2^n$.

Таким образом, оставшаяся сумма из (11) может быть преобразована к виду $A_0\lambda_1^n + A_0'\lambda_2^n$.

Таким образом, рекуррентный метод позволяет определить $f(n,r)$ при условии, что мы уже подсчитали $f(n,r-1)$ и $f_0(n,r-1)$. При этом из (7) сразу следует, что для старшего коэффициента

$$C_{r-1} = \frac{(q-1)A_{r-1}}{\lambda^2}. \tag{12}$$

Из соотношений (4), (9) и (12) вытекает, что

$$A_r = \frac{1}{r!(\lambda_1+2)^r\lambda_1^{r-2}(q-1)(\lambda_1-\lambda_2)}.$$

Можно переписать полученное соотношение в виде

$$A_r = \frac{1}{r!(\lambda_1+2)^{r-1}\lambda_1^{r-1}(\lambda_1-\lambda_2)^2}.$$

Таким образом, получаем следующее утверждение.

Утверждение 4. *Число q-ичных последовательностей, содержащих подблок* 00 *ровно r раз асимптотически равно*

$$\frac{1}{r!(\lambda_1+2)^{r-1}\lambda_1^{r-1}(\lambda_1-\lambda_2)^2}n^r\lambda_1^n$$

при n, стремящемся к бесконечности.

Еще раз отметим, что предложенный рекуррентный метод позволяет достаточно просто вычислять $f(n,r)$ только для фиксированного значения r. В остальных случаях (например, когда r растет

как φn при n, стремящемся к бесконечности) можно воспользоваться методом стебельного расстояния из [20].

Замечание 1. Если по каким-то причинам нас интересует значение

$$f(n,r) = (A_r n^r + \ldots + A_1 n + A_0)\lambda_1^n + (A'_r n^r + \ldots + A'_1 n + A'_0)\lambda_2^n$$

для какого-то определенного r, и мы не хотим просчитывать предыдущие значения $f(n,s)$ для $s < r$, то можно константы $A_1, A_2, \ldots, A_r$ и $A'_1, A'_2, \ldots, A'_r$ определять, вычислив $f(n,r)$ для конкретных начальных значений n.

1.4 Обобщение алгоритма 1-удаления

Рассмотрим описанный выше алгоритм при $r = 1$. Раньше информационная последовательность $(m_1, m_2, \ldots, m_{n-2t})$ не содержала нулей, а $2t$ позиций использовались для исправления ошибок.

Теперь мы рассмотрим информационную последовательность $m = (m_1, m_2, \ldots, m_{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil})$, содержащую ровно z нулей. Кроме того, рассмотрим проверочную последовательность, которая состоит только из ненулевых элементов. Занумеруем $\binom{z+t}{z}$ вариантов расположения z информационных нулей среди не более, чем $z+t$ нулей последовательностями, не содержащими нулей, то есть последовательностями, составленными из элементов $Q\backslash\{0\}$. Для этого потребуется $\lceil \log_{q-1} \binom{z+t}{z} \rceil$ позиций. Это и определяет проверочную последовательность $h = (h_1, h_2, \ldots, h_{\lceil \log_{q-1} \binom{z+t}{z} \rceil})$. Таким образом, информационная последовательность будет состоять из $n - 2t - \lceil \log_{q-1} \binom{z+t}{z} \rceil$ символов, а проверочная из $\lceil \log_{q-1} \binom{z+t}{z} \rceil$ символов.

Кодер будет вести передачу информационной последовательности описанным выше алгоритмом 1-удаления, за исключением того, что кодер будет сравнивать число ошибок с числом неинформационных нулей в последовательности y (кодер знает эту информацию) и, безошибочно переданные информационные нули, вместе с удаленными ими ненулевыми информационными символами, в дальнейшем никогда не передаются (формальные определения даются ниже).

Замечание 2. Если применить к информационной последовательности процесс 1-удаления, то можно определить для каждого информационного нуля какой ненулевой информационный символ он стирает, а какой ноль ничего не стирает.

После безошибочной передачи последнего информационного нуля в последовательности m, расположение z информационных нулей среди $z+t$ возможных нулей становится известно(не все нули могут еще появиться к этому моменту, но информационные появились все, следовательно, это расположение однозначно определяется). Следовательно, кодер в этот момент может определить проверочную последовательность h.

В каждый момент времени i кодер, после того, как послал в канал x_i и увидел, какой символ y_i был принят на выходе канала, подсчитывает число $V(i)$ неинформационных нулевых символов, которые возникли в результате ошибки и которые в процессе 1-удаления в последовательности y не стирают никакой ненулевой символ. Прежде чем передавать первый элемент h_1 проверочной последовательности, кодер передает $V(i)$ единиц (естественно, если будут возникать ошибки, то кодер их исправляет, используя алгоритм 1-удаления) и только после этого, кодер начинает передавать проверочную после-

довательность.

Замечание 3. Заметим, что $V(i) \leq V(i+1)$ и $V(i)$ может принимать различные значения в различные моменты времени i. Возможны такие конфигурации ошибок, при которых уже переданные элементы стираются в процессе 1-удаления и требуют повторной передачи. Каждый раз, прежде чем (в момент времени i) передавать первый элемент h_1 проверочной последовательности кодер передает $V(i)$ единиц после информационной и перед проверочной последовательностью.

После того как будет передана проверочная последовательность кодер вновь передает единицы. Число таких единиц зависит от того, сколько ошибок произошло в канале (если произойдет не t ошибок, а $t-L$,то кодер будет передавать $2L$ дополнительных единиц в конце процесса передачи).

Еще раз отметим, что кодер ведет передачу, используя алгоритм **1-удаления**. Это означает, что при возникновении ошибок, кодер их сразу же исправляет (т.е. посылает в канал нули, которые стирают ошибочные символы) и только после этого продолжает передачу элементов последовательности

$$a^* = (m_1, m_2, \ldots, m_{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil}, 1, \ldots, 1,$$
$$h_1, h_2, \ldots, h_{\lceil \log_{q-1} \binom{z+t}{z} \rceil}, 1, 1, \ldots).$$

Формальное описание нового алгоритма дано в следующей теореме.

Теорема 2. *Обобщенный алгоритм 1-удаления передает*

$$\binom{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil}{z} \cdot (q-1)^{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil - z}$$

сообщений.

Доказательство. Поставим каждому передаваемому сообщению

$m \in [M]$ в соответствие последовательность

$m = (m_1, m_2, \ldots, m_{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil})$, имеющую ровно z нулей.

В каждый момент времени i кодер посылает в канал q-ичный символ x_i, смотрит какой символ y_i принят на выходе канала, формирует три последовательности $a(i)$, $b(i)$, $c(i)$ и подсчитывает величины $T(i)$, $S(i)$ и $V(i)$.

Через $T(i)$ обозначено число ошибок в канале в момент времени i, а через $S(i)$ обозначено число неинформационных нулей в последовательности $y_1, y_2, \ldots, y_i$.

Последовательность $c(i)$ состоит из информационных нулей и стираемых ими ненулевых информационных символов в последовательности $y(i) = (y_1, y_2, \ldots, y_i)$.

Последовательности $b(i)$ это та последовательность ненулевых символов, которые остаются после применения процесса 1-удаления к последовательности $y(i) = (y_1, y_2, \ldots, y_i)$.

Последовательность $a(i)$ состоит из символов, которые кодер собирается передавать.

Все три последовательности $a(i)$, $b(i)$, $c(i)$ определяются индуктивно.

В начальный момент времени

$$a(0) = (m_1, m_2, \ldots, m_{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil}),$$

$$b(0) = \varnothing,\ c(0) = \varnothing,\ V(0) = 0,\ S(0) = 0,\ T(0) = 0.$$

Пусть в момент времени $i-1$

$$a(i-1) = (a_1(i-1), a_2(i-1), \ldots, a_k(i-1)),$$

$$b(i-1) = (b_1(i-1), \ldots, b_s(i-1)),$$

$$c(i-1) = (c_1(i-1), \ldots, c_r(i-1)),$$

$$V(i-1) = v_{i-1}.$$

1. Если $T(i-1) > S(i-1)$, то кодер посылает в канал $x_i = 0$ и последовательности a, c не меняются. Значение V тоже не меняется, т.е. $V(i) = V(i-1)$.

Если $y_i = x_i = 0$, то $T(i) = T(i-1)$, $S(i) = S(i-1) + 1$,

$$b(i) = (b_1(i-1), \ldots, b_{s-1}(i-1))$$

(полагаем $b_{-1}(i-1) = b_0(i-1) = \varnothing$).

Если $y_i \neq 0$, то $T(i) = T(i-1) + 1$, $S(i) = S(i-1)$,

$$b(i) = (b_1(i-1), \ldots, b_s(i-1), y_i).$$

Пусть теперь $T(i-1) = S(i-1)$. Кодер посылает в канал $x_i = a_1(i-1)$.

2. Если $y_i = x_i$ (т.е. $T(i) = T(i-1)$, $S(i) = S(i-1)$), то

$$a(i) = (a_2(i-1), \ldots, a_k(i-1)),$$

$$V(i) = V(i-1).$$

При этом

$$b(i) = (b_1(i-1), \ldots, b_s(i-1), a_1(i-1)),$$

$$c(i) = c(i-1),$$

если $a_1(i-1) \neq 0$ и

$$b(i) = (b_1(i-1), \ldots, b_{s-1}(i-1)),$$

$$c(i) = (c_1(i-1), \ldots, c_r(i-1), b_s(i-1), a_1(i-1)),$$

если $a_1(i-1) = 0$.

(полагаем $b_{-1}(i-1) = b_0(i-1) = \varnothing$)

3. Если $x_i \neq y_i$ и $y_i \neq 0$, то последовательности $a,\ c$ не меняются. Значение V тоже не меняется, т.е. $V(i) = V(i-1)$.

$$b(i) = (b_1(i-1), \ldots, b_s(i-1), y_i).$$

Отметим, что в этом случае $T(i) = T(i-1) + 1$, $S(i) = S(i-1)$ и кодер попадает в состояние исправления ошибок.

4. Если $x_i \neq y_i$ и $y_i = 0$, то последовательность c не меняется, и при $s \geq 1$

$$a(i) = (b_s(i-1), a_1(i-1), \ldots, a_k(i-1)),$$

$$b(i) = (b_1(i-1), \ldots, b_{s-1}(i-1)),$$

а при $s = 0$ (т.е., когда $b(i-1) = \varnothing$), последовательность a не меняется,

$$b(i) = \varnothing,$$

$$V(i) = V(i-1) + 1.$$

Отметим, что в этом случае $T(i) = T(i-1) + 1$, $S(i) = S(i-1) + 1$.

Пусть в момент времени l последовательность $a(l) = \varnothing$. В этот момент времени расположение z информационных нулей среди $z+t$ возможных нулей в последовательности y становится известно(не все нули могут еще появиться в последовательности y к этому моменту, но информационные появились все, следовательно это расположение однозначно определяется). Следовательно, кодер в этот момент опре-

деляет проверочную последовательность и заново определяет последовательность $a(l)$ (вместо пустой):

$$a(l) = (1, 1, \ldots, 1, h_1, h_2, \ldots, h_{\lceil \log_{q-1} \binom{z+t}{z} \rceil}, 1, 1, \ldots),$$

где число единиц перед символом h_1 равно $V(l)$.

Обозначим через $m^* = b(l)$.

Замечание 4. Можно заметить, что последовательность m^* получится, если применить к информационной последовательности m процесс 1-удаления.

Также заметим, что начиная с момента времени l верно следующее: если в момент времени j значение $V(j)$ меняется, то в этот момент последовательность $a(j)$ имеет вид

$$a(j) = (m^*, 1, 1, \ldots, 1, h_1, h_2, \ldots, h_{\lceil \log_{q-1} \binom{z+t}{z} \rceil}, 1, 1, \ldots).$$

Кодер в этот момент времени j (когда значение $V(j)$ меняется) переопределяет $a(j)$ так, чтобы число единиц между m^* и символом h_1 стало равно $V(j)$ (добавляет одну единицу). В остальном правила из пунктов 1-4 остаются прежними. Таким образом, процесс передачи полностью описан.

Кодер заканчивает передачу после того, как кодовая последовательность x и, соответственно, последовательность y будут иметь длину n.

Каждой произошедшей ошибке соответствует ровно один символ, который она стирает (либо дополнительная единица), поэтому $n - 2t - \lceil \log_{q-1} \binom{z+t}{z} \rceil$ информационных элементов и $\lceil \log_{q-1} \binom{z+t}{z} \rceil$ проверочных элементов кодер сможет передать на длине n.

Алгоритм декодирования состоит в следующем: Подсчитаем разницу между значением $z + t$ и числом нулей в последовательности

$y_1, y_2, \ldots, y_n$. Пусть она равна L. Применим процесс **1-удаления** к последовательности $y_1, y_2, \ldots, y_n$ и после этого дополнительно удалим $2L$ последних символов. Мы получим последовательность

$$(m^*, 1, 1, \ldots, 1, h_1, h_2, \ldots, h_{\lceil \log_{q-1} \binom{z+t}{z} \rceil}).$$

По последним $\lceil \log_{q-1} \binom{z+t}{z} \rceil$ элементам последовательности, полученной в результате этих действий, определим места z информационных нулей среди $z+t$ возможных нулей и определим информационные нули.

После этого декодер может не только определить информационную последовательность m, но и восстановить полностью весь процесс передачи сообщения (однозначно восстановить $x_1, x_2, \ldots, x_n$). Двигаясь от первой к последней координате полученной последовательности $y_1, y_2, \ldots, y_n$, он определяет какие ненулевые символы передались правильно (т.е. которые не будут стерты в процессе 1-удаления неинформационными нулями) и, следовательно, являются информационными (а нулевые информационные он уже знает), в каких позициях произошли ошибки, и как эти ошибки были стерты в процессе 1-удаления неинформационными нулями. Таким образом, декодер определяет в какой очередности передавались информационные символы и, следовательно, однозначно восстанавливает последовательность m.

Проиллюстрируем процесс декодирования на следующем примере.

Пусть, например, первая часть информационной последовательности состоит из четырех элементов m_1, m_2, m_3, m_4, содержащих ровно один ноль, вторая часть состоит из одного элемента m_5, и в канале

происходит не более одной ошибки. Пусть на выходе канала декодер получил вектор y, в котором

$$y_1 = 1, y_2 = 2, y_3 = 0, y_4 = 0, y_5 = 1, y_6 = 3,$$

а то, что $y_7 = m_5 = 1$ означает, что информационным является нулевой элемент y_3, а $y_7 = m_5 = 2$ означает, что информационным является нулевой элемент y_4.

Тогда в случае $y_7 = 1$ имеем:

$y_1 = 1$. Пока ничего сказать не можем.

$y_2 = 2$. Следовательно, первый символ передался без ошибки (иначе кодер передавал бы $x_2 = 0$). Значит $m_1 = 1$.

$y_3 = 0$. Мы знаем, что это информационный ноль. Значит $m_2 = 2$ и $m_3 = 0$.

$y_4 = 0$. Мы сразу можем определить, что произошла ошибка и вместо элемента $x_4 = m_4$ передался ноль.

$y_5 = 1$. Кодер действует по описанному алгоритму и повторно передает стертый информационный элемент $m_1 = 1$. (В данном примере в этом не было необходимости, но, если бы ошибка произошла бы не сразу после передачи информационного нуля, то возникла бы следующая ситуация: $y_i = 0$, $y_{i-1} \neq 0$. Тогда, если $y_{i+1} = y_{i-1}$, то ошибка произошла в позиции i, а если $y_{i+1} \neq y_{i-1}$ то в позиции $i-1$.)

$y_6 = 3$. Согласно алгоритму, информационные элементы $m_2 = 2$ и $m_3 = 0$ повторно не передаются. Следовательно $m_4 = 3$.

В этом случае передавалось сообщение 1203.

Теперь рассмотрим случай $y_7 = 2$:

$y_1 = 1$. Пока ничего сказать не можем.

$y_2 = 2$. Первый символ передался без ошибки. Значит $m_1 = 1$.

$y_3 = 0$. Произошла ошибка либо во второй, либо в третьей позиции.

$y_4 = 0$. Это информационный ноль. Значит ошибка была во второй позиции и кодер ее стер, передавая $x_3 = 0$. Таким образом, $m_2 = 0$.

$y_5 = 1$. Значит $m_3 = 1$.

$y_6 = 3$. Следовательно, $m_4 = 3$ и в этом случае передавалось сообщение 1013.

Утверждение 5. *Обобщенный алгоритм 1-удаления асимптотически улучшает предыдущий алгоритм на интервале* $(\tau^*, 1/(q+1))$.

Доказательство. 1-стирающий алгоритм позволяет передать $M_1 = (q-1)^{n-2t}$ сообщений. Обобщенный стирающий алгоритм передает $M_2 = \binom{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil}{z} \cdot (q-1)^{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil - z}$ сообщений.

$$\frac{M_2}{M_1} = \frac{\binom{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil}{z}}{\binom{z+t}{z}(q-1)^z}$$

Введем обозначения $\zeta = z/n$ и, напомним, что $\tau = t/n$.

Асимптотически $\frac{\log_2 \frac{M_2}{M_1}}{n}$ при $n \to \infty$ и фиксированных τ и ζ ведет себя, как

$$(1 - 2\tau - \frac{(\zeta+\tau)h(\zeta/(\zeta+\tau))}{\log(q-1)})h(\frac{\zeta}{1-2\tau-\frac{(\zeta+\tau)h(\zeta/(\zeta+\tau))}{\log(q-1)}}) -$$

$$-(\zeta+\tau)h(\zeta/(\zeta+\tau)) - \zeta\log(q-1)$$

Обозначим полученную функцию при фиксированном параметре τ через $\varphi(\zeta)$. Обобщенный алгоритм 1-удаления асимптотически улучшает предыдущий алгоритм для какого-то фиксированного значения

τ, если для этого τ функция $\varphi(\zeta)$ строго больше нуля. В нуле данная функция равна нулю, поэтому достаточно показать, что при этом τ производная в нуле положительна и, следовательно, функция $\varphi(\zeta)$ возрастает.

Утверждение 6. *Для произвольной всюду дифференцируемой функции $f(x)$ справедливо равенство*

$$[f(x)h(\frac{x}{f(x)})]' = -\log\frac{x}{f(x)} + (1-f'(x))\log(1-\frac{x}{f(x)}).$$

Доказательство. Производная равна

$$\begin{aligned} f'(x)\cdot[-\frac{x}{f(x)}\log\frac{x}{f(x)} - (1-\frac{x}{f(x)})\log(1-\frac{x}{f(x)})] + \\ f(x)\cdot[\log(1-\frac{x}{f(x)}) - \log\frac{x}{f(x)}]\cdot\frac{f(x)-xf'(x)}{f^2(x)} = \\ \log\frac{x}{f(x)}\cdot[-\frac{xf'(x)}{f(x)} - \frac{f(x)-xf'(x)}{f(x)}] + \\ \log(1-\frac{x}{f(x)})\cdot[-f'(x)(1-\frac{x}{f(x)}) + (1-\frac{xf'(x)}{f(x)})] = \\ -\log(x/f(x)) + \log(1-x/f(x))\cdot(1-f'(x)). \end{aligned}$$

Утверждение доказано.

При $x\to 0$ слагаемое $\log(1-\frac{x}{f(x)})(1-f'(x))$, где функция $f(x)$ равна $(1-2\tau-\frac{(x+\tau)h(x/(x+\tau))}{\log(q-1)})$ стремится к нулю.

Следовательно, вычисление производной в нуле для $\varphi(\zeta)$ приводит к равенству

$$\begin{aligned} \varphi^{'}(0) = -\log\frac{\zeta}{1-2\tau} + \log\frac{\zeta}{\tau} - \log(q-1) = \\ = \log(1-2\tau) - \log\tau - \log(q-1) \end{aligned}$$

Таким образом, при $\tau < \frac{1}{q+1}$ производная положительна и утверждение доказано.

Конечно представляет интерес вопрос, насколько новый алгоритм улучшает предыдущий. Подобная задача представляется не очень простой и требует дальнейших исследований. Введем обозначение $R_{new}(\tau) = \lim_{n\to\infty} \log_q M_2/n$ и сравним значения $R_{new}(\tau)$ с касательными $g_1(\tau)$ и $g_2(\tau)$. Величина $R_{new}(\tau)$ считалась для нескольких значений параметра ζ, и через ζ_{max} обозначено значение, дающее большее значение для $R_{new}(\tau)$.

Приведем некоторые численные значения для $q = 5$.

τ	0.16	0.15	0.14	0.13	0.12	0.11	0.1	0.09	0.08
ζ_{max}	0.04	0.01	0.018	0.027	0.036	0.047	0.057	0.069	0.081
$g_1(\tau)$	0.58	0.61	0.621	0.637	0.654	0.672	0.689	0.706	-
$R_{new}(\tau)$	0.58	0.61	0.621	0.641	0.659	0.679	0.701	0.722	0.744
$H_q(\tau)$	0.59	0.61	0.627	0.648	0.669	0.689	0.712	0.734	0.757
$g_2(\tau)$	-	-	-	-	-	-	-	0.714	0.743

Данная таблица показывает, что для $q = 5$ новый алгоритм достаточно далек от асимптотической границы Хэмминга.

Ситуация существенно лучше для большего значения q. Возьмем $q = 37$. Таблица для значений τ правее точки касания прямой g_2 дает следующее.

τ	0.0008	0.0009	0.001	0.0011	0.0012	0.0013
ζ_{max}	0.026	0.026	0.026	0.026	0.026	0.026
$g_2(\tau)$	0.9974	0.9971	0.9968	0.9965	0.9962	0.9959
$R_{new}(\tau)$	0.9973	0.9971	0.9968	0.9965	0.99622	0.99593
$H_q(\tau)$	0.9974	0.9971	0.9968	0.9965	0.9962	0.9959

Таблица для значений τ левее точки касания прямой g_2 дает такую картину.

τ	0.0007	0.0006	0.0005	0.0004	0.0003	0.0002
ζ_{max}	0.026	0.026	0.026	0.027	0.027	0.027
$g_2(\tau)$	0.99773	0.9980	0.9983	0.9986	0.9989	0.9992
$R_{new}(\tau)$	0.9977	0.9979	0.9983	0.9986	0.9989	0.9993
$H_q(\tau)$	0.9977	0.9980	0.9983	0.9986	0.9989	0.9992

Если взять $\tau = 0.00001$, то $H_q(\tau) = 0.99995$, а $R_{new}(\tau) = 0.999955$.

Приведем еще одну таблицу. В ней для различных значений q вычисляются точка пересечения прямых g_1 и g_2 (Left) и величина $1/(q+1)$ (Right). В настоящей работе доказано, что новый алгоритм дает улучшение для этих промежутков значений τ.

q	3	4	5	6	7	8	9	10	11
$Left$	0.191	0.129	0.096	0.075	0.061	0.051	0.044	0.038	0.034
$Right$	0.25	0.2	0.166	0.142	0.125	0.111	0.1	0.09	0.083

1.5 Тени, задаваемые отношением слово-подслово

Рассмотрим множество $\mathcal{X}^k$ слов $x^k = x_1x_2\cdots x_k$ длины k над алфавитом $\mathcal{X} = \{0, 1, \ldots, q-1\}$.

Для слова $a^k = a_1a_2\cdots a_k \in \mathcal{X}^k$ определим левую тень

$$shad^L(a^k) = a_2\cdots a_k, \tag{13}$$

которая состоит из подслова, получающегося в результате удаления первого символа a_1 из a^k, и определим правую тень

$$shad^R(a^k) = a_1 \cdots a_{k-1}, \tag{14}$$

которая состоит из подслова, получающегося в результате удаления последнего символа a_k из a^k. Заметим, что $shad^L(a^k) = shad^R(a^k)$ тогда и только тогда, когда $a^k = aa \cdots a$, $a \in \mathcal{X}$, так как из того, что $a_2 a_3 \cdots a_k = a_1 a_2 \cdots a_{k-1}$ вытекает $a_1 = a_2 = a_3 = \cdots = a_k$.

Определим тень слова a^k:

$$shad(a^k) = shad^L(a^k) \cup shad^R(a^k). \tag{15}$$

Заметим, что для слов a^k, не образованных одним элементом, тень $shad(a^k)$ состоит из двух подслов.

Далее, для любого подмножества $A \subset \mathcal{X}^k$ определим левую тень

$$shad^L(A) = \bigcup_{a^k \in A} shad^L(a^k), \tag{16}$$

правую тень

$$shad^R(A) = \bigcup_{a^k \in A} shad^R(a^k), \tag{17}$$

и тень

$$shad(A) = shad^L(A) \cup shad^R(A). \tag{18}$$

Мы хотим найти минимальную тень N-множества $A \subset \mathcal{X}^k$, или значение

$$\nabla_k(q, N) = \min\{|shad(A)| : A \subset \mathcal{X}^k, |A| = N\}. \tag{19}$$

Будем, для краткости, писать $\nabla_k(N)$, если q фиксировано и $\nabla(N)$, если k также фиксировано. Мы также будем использовать обозначения $\nabla_k^L(N)$ и $\nabla_k^R(N)$, соответственно $\nabla^L(N)$ и $\nabla^R(N)$, для левых и правых теней.

Рассмотрим следующие конфигурации:

(i) Слова $xxx\ldots x$, $x \in \mathcal{X}$, (число таких слов $q = |\mathcal{X}|$). Тень таких слов имеет мощность 1.

(ii) Слова

$$a^k = cdcd\ldots cd$$

$$b^k = dcdc\ldots dc \quad , \qquad \text{если } k \text{ четно}$$

и, аналогично,

$$a^k = cd\ldots c$$

$$b^k = dc\ldots d \quad , \qquad \text{если } k \text{ нечетно.}$$

Тень таких слов имеет мощность 2.

(iii) Для множества $\mathcal{X}B\mathcal{X}$ q слов by, $y \in \mathcal{X}$ имеют одинаковые правые тени. Для левых теней аналогичное замечание также справедливо.

Заметим, что для всех этих конфигураций $\nabla(N) \leq N$ и докажем это в общем случае.

Рассмотрим двоичный случай.

Лемма 1 *Для $q = 2$, $k \geq 3$ справедливо*

$$\nabla(N) \leq N \qquad \textit{для всех } N \leq 2^k.$$

Доказательство. Запишем N в виде $N = 4M + p$, где $0 \leq p < 4$.

Случай $p = 0$:

Выберем произвольное $B \subset \mathcal{X}^{k-2}$ мощности $|B| = M$, тогда $A = \mathcal{X}B\mathcal{X}$, имеет мощность N. Легко видеть, что

$$|shad(A)| = |\mathcal{X}B \cup B\mathcal{X}| \leq |B\mathcal{X}| + |\mathcal{X}B| = 4M = N.$$

Случай $3 \geq p \geq 1$*:*

Выберем $\mathcal{B} \subset \mathcal{X}^{k-2} - \{0^{k-2}\}$ мощности $|\mathcal{B}| = M$ и $A_p = \mathcal{X}\mathcal{B}\mathcal{X} \cup C_p$, где $C_1 = \{00^{k-2}0\}$, $C_2 = \{00^{k-2}0, 00^{k-2}1\}$ и $C_3 = \{00^{k-2}0, 00^{k-2}1, 10^{k-2}0\}$. Ясно, что $|shad(A_p)| \leq 4M + p$.

□

Для q-ичного случая справедлива

Лемма 2. *Рассмотрим* $\mathcal{X} = \{0, 1, \ldots, q-1\}$, $k \geq 3$, *и* $N \leq q^k$. *Запишем* $N = q^2M + p$, $0 \leq p < q^2$, *тогда*

$$\nabla(N) \leq 2qM + \begin{cases} 0 & \text{если } p = 0 \\ \lceil\sqrt{p}\rceil + \lfloor\sqrt{p}\rfloor - 1 & \text{если } \lceil\sqrt{p}\rceil\lfloor\sqrt{p}\rfloor \geq p > 0 \\ 2\lceil\sqrt{p}\rceil - 1 & \text{в остальных случаях} \end{cases} \quad (20)$$

и

$$\nabla(N) \leq \frac{2}{q}N - \frac{2}{q}p + \begin{cases} 0 & \text{если } p = 0 \\ \lceil\sqrt{p}\rceil + \lfloor\sqrt{p}\rfloor - 1 & \text{если } \lceil\sqrt{p}\rceil\lfloor\sqrt{p}\rfloor \geq p > 0 \\ 2\lceil\sqrt{p}\rceil - 1 & \text{в остальных случаях .} \end{cases} \quad (21)$$

Доказательство.

Случай $p = 0$:

Выберем произвольное $\mathcal{B} \subset \mathcal{X}^{k-2}$ мощности $|\mathcal{B}| = M$ и $A = \mathcal{X}\mathcal{B}\mathcal{X}$. Тогда $|shad(A)| \leq 2qM$.

Случай $q^2 - 1 \geq p \geq 1$:

Выберем $\mathcal{B} \subset \mathcal{X}^{k-2} - \{0^{k-2}\}$ мощности $|\mathcal{B}| = M$ и $A_p = \mathcal{X}\mathcal{B}\mathcal{X} \cup D_p$, где D_p это сбалансированное подмножество $\mathcal{X}0^{k-2}\mathcal{X}$ из p элементов. Это означает, что мы берем $D_p = \mathcal{Y}0^{k-2}\mathcal{Y}'$, где разница $|\{\mathcal{Y}\setminus\mathcal{Y}'\}\cup\{\mathcal{Y}'\setminus\mathcal{Y}\}|$ между множествами $|\mathcal{Y}|$ и $|\mathcal{Y}'|$ будет минимально возможной.

Тогда

$$|shad(A_p)| \leq 2qM + 2\lceil\sqrt{p}\rceil - 1$$

и (20) доказано. Отсюда, с помощью небольших преобразований, получаем (21).

Выше мы получили нашу первую верхнюю границу на размер минимальной тени, используя множества, имеющие структуру $A = \mathcal{X}B\mathcal{X}$. Мы обобщим эту конструкцию и будем брать объединение подобных множеств. Рассмотрим множества

$$\mathcal{X}^l 0^m \mathcal{X}^r. \tag{22}$$

Определим теперь нашу основную концепцию.

Определение 2 *Для неотрицательных целых l (left), m (middle) и r (right), удовлетворяющих условиям*

$$l \geq r \tag{23}$$

и

$$k = l + m + r, \tag{24}$$

определим базисное множество $\mathcal{B}(k,l,r)$ из $\mathcal{X}^k$ как следующее объединение:

$$\mathcal{B}(k,l,r) = \bigcup_{s=0}^{l-r} \mathcal{X}^{l-s} 0^m \mathcal{X}^{r+s}. \tag{25}$$

Например, $\mathcal{B}(7,3,1)$ это объединение строк матрицы

$$\begin{array}{ccccccc} \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} & \mathcal{X} \end{array}$$

а $\mathcal{B}(8,3,2)$ это объединение строк матрицы

$$\begin{array}{cccccccc} \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} & \mathcal{X}. \end{array}$$

Обозначим эти матрицы через $[\mathcal{B}(7,3,1)]$, $[\mathcal{B}(8,3,2)]$ и в общем случае через $[\mathcal{B}(k,l,r)]$.

Выделим основные свойства подобных множеств.

Лемма 3. Для каждого $l \geq r \geq 1$, $m + r > l$ (то есть, $k = l + m + r > 2l$) и $q = 2$ имеем

(i) $|\mathcal{B}(k,l,r)| = 2^{l+r} + 2^{l+r-1}(l-r) = 2^{l+r-1}(l-r+2)$

(ii) $shad\,\mathcal{B}(k,l,r) = \mathcal{B}(k-1,l,r-1)$

(iii) $\mathcal{B}(k,l,r) \subset \mathcal{B}(k,l+1,r-1)$

(iv) $|shad\,\mathcal{B}(k,l,r)| = |\mathcal{B}(k-1,k,r-1)| = \dfrac{|\mathcal{B}(k,l,r)|}{2} + 2^{l+r-2}$

(v) $|shad\,\mathcal{B}(k,l,r)| = 2^{l+r-2}(l-r+3)$

Пример 1. $k = 9$, $l = 4$, $r = 1$

$$\begin{aligned} |\mathcal{B}(9,4,1)| &= 2^5 + 2^4 3 = 32 + 48 = 80 \\ \nabla_9(80) &\leq 2^{4+1-2}(4-1+3) = 48 \end{aligned}$$

В дальнейшем, важную роль будет играть следующий результат.

Следствие 2. Для $N = 2^{l+r-1}(l-r+2)$ и $k = l+m+r > 2l \geq 2r \geq 2$ справедливо

$$\nabla_k(N) \leq \frac{1}{2}\frac{l-r+3}{l-r+2}N. \tag{26}$$

Доказательство.

(i).

Для начала, в качестве примера базисного множества $\mathcal{B}(k,l,r)$ рассмотрим $(k,l,r) = (9,4,2)$:

$$\begin{array}{ccccccccc} \mathcal{X} & \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X}\mathcal{X} & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X}\mathcal{X} & \mathcal{X} & \mathcal{X} & \mathcal{X}. \end{array}$$

Определим $\mathcal{X}\mathcal{X} = 1$ и заметим, что $\mathcal{B}(9,4,2)$ состоит из объединения следующих множеств

$$\begin{array}{ccccccccc} \mathcal{X} & \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X}\mathcal{X} & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X}\mathcal{X} & \mathcal{X} & \mathcal{X} & \mathcal{X}. \end{array}$$

Эти множества имеют мощность $2^6 + 2^5 + 2^5$.

Для общего случая $l \leq m + r$ получим, что

$$|\mathcal{B}(k,l,r)| = 2^{l+r} + 2^{l+r-1}(l-r).$$

(ii).

Проиллюстрируем данное утверждение на нашем примере

$$\begin{array}{lcl} shad^L\mathcal{B}(9,4,2) & & shad^R\mathcal{B}(9,4,2) \\ & & \mathcal{X}\,\mathcal{X}\,\mathcal{X}\,\mathcal{X}\,0\,0\,0\,\mathcal{X} \\ \mathcal{X}\,\mathcal{X}\,\mathcal{X}\,0\,0\,0\,\mathcal{X}\,\mathcal{X} & = & \mathcal{X}\,\mathcal{X}\,\mathcal{X}\,0\,0\,0\,\mathcal{X}\,\mathcal{X} \\ \mathcal{X}\,\mathcal{X}\,0\,0\,0\,\mathcal{X}\,\mathcal{X}\,\mathcal{X} & = & \mathcal{X}\,\mathcal{X}\,0\,0\,0\,\mathcal{X}\,\mathcal{X}\,\mathcal{X} \\ \mathcal{X}\,0\,0\,0\,\mathcal{X}\,\mathcal{X}\,\mathcal{X}\,\mathcal{X} & & . \end{array} \qquad (27)$$

Заметим, что если мы добавим первую строку второй матрицы в первую матрицу (соответственно последнюю строку первой матрицы во вторую матрицу), то $shad\mathcal{B}(9,4,2) = \mathcal{B}(8,4,1)$, следовательно k и r увеличиваются на 1.

(iii).

Заметим только, что $\mathcal{B}(8,3,2)$ образуется двумя первыми строками первой матрицы.

В общем случае для $l > r$ имеем

$$\mathcal{B}(k-1,l-1,r) \subset shad^L\mathcal{B}(k,l,r) \subset shad\mathcal{B}(k,l,r) = \mathcal{B}(k-1,l,r-1)$$

(iv).

Заметим только, что в $shad^L\mathcal{B}(k,l,r)$ на одно $\mathcal{X}$ меньше в каждой строке, чем в $\mathcal{B}(k,l,r)$ и на одну дополнительную строку больше. Эта строка $\mathcal{X}^l 0^m \mathcal{X}^{r-1}$ из $shad^R\mathcal{B}(k,l,r)$ соответствует $\mathcal{X}^{l-1}\mathcal{X}\mathcal{X}\,0^m\mathcal{X}^{r-1}$ мощности 2^{l+r-2}.

(v).

Следует из (i) и (ii). □

Легко видеть, что утверждения (i), (iv) из леммы 3 обобщаются на (i′), (iv′).

Лемма 4. Для всех $l \geq r \geq 1$, $m+r > l$, (то есть $k = l+m+r > 2l$) и $q \geq 2$ справедливо

$$(i') \qquad |\mathcal{B}(k,l,r)| = q^{l+r} + q^{l+r-1}(l-r)(q-1)$$

$$\begin{aligned}(iv') \quad |shad\mathcal{B}(k,l,r)| &= |\mathcal{B}(k-1,l,r-1)| \\ &= \frac{|\mathcal{B}(k,l,r)|}{q} + q^{l+r-2}(q-1) \\ &= q^{l+r-2}((l-r+2)(q-1)+1). \end{aligned} \tag{28}$$

Опять важное для дальнейшего следствие.

Для $N = |\mathcal{B}(k,l,r)| = q^{l+r} + q^{l+r-1}(l-r)(q-1)$ и из того, что $|shad\mathcal{B}(k,l,r)| = \frac{N}{q} + q^{l+r-2}(q-1)$ получаем

$$\begin{aligned}\frac{\nabla_k(q,N)}{N} &\leq \frac{1}{q} + \frac{1}{q}\frac{(q-1)}{q+(l-r)(q-1)} \\ &= \frac{1}{q}\left(1 + \frac{q-1}{(l-r+1)(q-1)+1}\right) \\ &\leq \frac{1}{q}\left(1 + \frac{1}{l-r+1}\right). \end{aligned} \tag{29}$$

Следовательно, справедливо

Следствие 3. Для $N = q^{l+r}+q^{l+r-1}(l-r)(q-1)$ и $k = l+m+r > 2l \geq 2r \geq 2$

$$\nabla_k(q,N) \leq \frac{1}{q}\left(1 + \frac{1}{l-r+1}\right)N. \tag{30}$$

Рассмотрим нижнюю границу.

Для любого $A \subset \mathcal{X}^k$ определим для любого $\mathcal{Y} \subset \mathcal{X}$

$$A^1_{\mathcal{Y}} = \{x_2 \dots x_k \in \mathcal{X}^{k-1} : \mathcal{Y}x_2 \dots x_k \subset A \text{ and } xx_2 \dots x_k \notin A\}. \tag{31}$$

для любых $x \in \mathcal{X} \setminus \mathcal{Y}$.

Ясно, что эти множества содержатся в $\mathcal{X}^{k-1}$ и различны. Более того,

$$shad(A) \supset shad^L(A) = \bigcup_{\mathcal{Y} \subset \mathcal{X}} A^1_{\mathcal{Y}}, \tag{32}$$

$$A = \bigcup_{\mathcal{Y} \subset \mathcal{X}} \mathcal{Y} A^1_{\mathcal{Y}}, \tag{33}$$

и, поскольку $|\mathcal{Y}| \leq q$, получаем

$$|shad(A)| \geq \frac{1}{q}|A|. \tag{34}$$

Отсюда, используя следствие 3, вытекает

Утверждение 7. Для $N = q^{l+r} + q^{l+r-1}(l-r)(q-1)$ и $k = l+m+r > 2l \geq 2r \geq 2$

$$\frac{1}{q}N \leq \nabla_k(q,N) \leq \frac{1}{q}\left(1 + \frac{1}{l-r+1}\right)N, \tag{35}$$

причем нижняя граница справедлива для всех N.

Заметим, что $|\mathcal{B}(k,l,r)| = |\mathcal{B}(k-2r, l-r, 0)|q^{2r}$. Следовательно, нас интересует мощность множества $\mathcal{B}(k,l,0)$ для произвольных l и $m = k-l-r$, $l > m$ (случай $l \leq m$ был рассмотрен ранее).

Утверждение 8. Для любых l и m таких, что $l > m$ имеем

$$|\mathcal{B}(k,l,0)| = q^{l-1}(l(q-1)+q) - (q-1)\sum_{i=1}^{l-m} q^{l-m-i}|\mathcal{B}(m+i-1, i-1, 0)|$$

и для $N = |\mathcal{B}(k,l,1)| = q^2|\mathcal{B}(k-2, l-1, 0)|$ справедливо

$$\frac{\nabla(N)}{N} \leq \frac{1}{q}(1 + \frac{1}{l}).$$

Доказательство. Обозначим через $H(l,m,a)$ число последовательностей из $\mathcal{X}^{l+m}$, не покрывающихся первыми a строками матрицы $[\mathcal{B}(k,l,0)]$. Рассмотрим j-ую строку $\mathcal{X}^{l-j+1}0^m\mathcal{X}^{j-1}$ в матрице $[\mathcal{B}(k,l,0)]$. Сколько новых последовательностей она добавит? Используя наше обозначение, получаем

$$q^{l-j+1}(q-1)H(l,m,j-m-1)$$

таких последовательностей.

Справедливо соотношение

$$H(l,m,a) = q^{m+a-1} - |\mathcal{B}(m+a-1,a-1,0)|. \tag{36}$$

Пусть $i = j-m-1$, тогда для $i = 1,2,\dots l-m$ мы добавляем

$$q^{l-i-m}(q-1)(q^{m+i-1} - |\mathcal{B}(m+i-1,i-1,0)|)$$

последовательностей и, это доказывает, что $|\mathcal{B}(k,l,0)|$ равно

$$q^l + q^{l-1}m(q-1) + \sum_{i=1}^{l-m} q^{l-m-i}(q-1)(q^{m+i-1} - |\mathcal{B}(m+i-1,i-1,0)|).$$

Значит, оно равно

$$q^l + q^{l-1}m(q-1) + q^{l-1}(l-m)(q-1) \\ - \sum_{i=1}^{l-m} q^{l-m-i}(q-1)|\mathcal{B}(m+i-1,i-1,0)|.$$

Получаем

$$\nabla(N) \le \frac{1}{q}\frac{|\mathcal{B}(k,l,0)|}{q|\mathcal{B}(m+l-1,l-1,0)|}N.$$

Таким образом,

$$\frac{\nabla(N)}{N} \leq \frac{1}{q} + \frac{(q-1)q^l - (q-1)|\mathcal{B}(l-1,l-m-1,0)|}{q^{l-1}(q+(l-1)(q-1)) - (q-1)\sum\limits_{i=1}^{l-m-1} q^{l-m-i}|\mathcal{B}^*},$$

где $\mathcal{B}^* = \mathcal{B}(m+i-1, i-1, 0)$.

Мы получили эту формулу, используя то, что

$$shad(\mathcal{B}(m+l+1,l,1)) = \mathcal{B}(m+l,l,0).$$

Можно доказать, что для такого N

$$\frac{(q-1)(q^{l-1} - |\mathcal{B}(l-1,l-m-1,0)|)}{q^{l-1}((l-1)(q-1)+q) - (q-1)\sum_{i=1}^{l-m-1} q^{l-m-i}\mathcal{B}^*} \leq \frac{1}{l}.$$

Действительно,

$$(q^{l-1} - |\mathcal{B}(l-1,l-m-1,0)|)(q-1)l \leq$$

$$q^{l-1}((l-1)(q-1)+q) - (q-1)\sum_{i=1}^{l-m-1} q^{l-m-i}|\mathcal{B}(m+i-1,i-1,0)|,$$

если

$$\sum_{i=1}^{l-m-1} q^{l-m-i}|\mathcal{B}(m+i-1,i-1,0)| \leq |\mathcal{B}(l-1,l-m-1,0)|)l.$$

Ясно, что для любого натурального u

$$q|\mathcal{B}(m+u-1,u-1,0)| < |\mathcal{B}(m+u,u,0)|.$$

Поэтому

$$\sum_{i=1}^{l-m-1} q^{l-m-i}|\mathcal{B}(m+i-1,i-1,0)| \leq |\mathcal{B}(l-1,l-m-1,0)|(l-m-1),$$

и утверждение доказано.

Рассмотрим также расширенные базисные множества

Для базисного множества $\mathcal{B}(k,l,r)$ мы использовали компоновочные множества

$$\mathcal{X}^l 0^m \mathcal{X}^r \tag{37}$$

и брали объединения таких множеств. Определим теперь дуальные компоновочные множества как

$$0^m \mathcal{X}^{k-2m} 0^m.$$

Добавим эти дуальные компоновочные множества в базисное множество и определим расширенное базисное множество $\widetilde{\mathcal{B}}(k,l,1)$ как

$$\widetilde{\mathcal{B}}(k,l,1) = \bigcup_{s=0}^{l-1} \mathcal{X}^{l-s} 0^m \mathcal{X}^{1+s} \bigcup 0^m \mathcal{X}^{k-2m} 0^m = \mathcal{B}(k,l,r) \bigcup 0^m \mathcal{X}^{k-2m} 0^m. \tag{38}$$

Множество $\widetilde{\mathcal{B}}(k,l,1)$ имеет большую мощность, чем $|\mathcal{B}(k,l,1)|$ но их тени совпадают!

Утверждение 9. Для $l \geq m$ имеем

(i) $\widetilde{\mathcal{B}}(k,l,1) = |\mathcal{B}(k,l,1)| + 1$ for $l = m$

(ii) $\widetilde{\mathcal{B}}(k,l,1) = |\mathcal{B}(k,l,1)| + 2^{l-m-1}$ for $m < l \leq 2m$

(iii) $\widetilde{\mathcal{B}}(k,l,1) = |\mathcal{B}(k,l,1)| + 2^{l-m-1} - |\mathcal{B}(l-m-1, l-2m-1, 0)|$ for $l > 2m$

(iv) $shad(\widetilde{\mathcal{B}}(k,l,1)) = |\mathcal{B}(k-1,l,0)|$

Доказательство. Для $l = m$ мы добавляем новое слово $0^m 10^m$. В случае (ii) новым блоком является $0^m 1\mathcal{X}^{l-m-1}10^m$. Из-за того, что он имеет 1 в $m+1$-ой координате, он не покрывается последними m строками базисной матрицы $[\mathcal{B}(k,l,1)]$. Из-за того, что он имеет 1 в $l+1$-ой координате, он не покрывается первыми m строками базисной матрицы $[\mathcal{B}(k,l,1)]$. Всего мы имеем l строк в $[\mathcal{B}(k,l,1)]$, следовательно это доказывает случай (ii). Для случая $l > 2m$ мы также имеем 1 в $m+1$-ой и $l+1$-ой координатах, но в этом случае получаем $H(l-2m-1, m, l-2m)$ новых последовательностей. Используя (24), это доказывает случай (iii).

Рассмотрим слово $b^{k-1} \in \mathcal{X}^{k-1}$. Тогда

$$up - shad(b^{k-1}) = \{a^k : \ a^k \in \mathcal{X}^k, \ b^{k-1} \in shad(a^k)\}.$$

Теперь, для любого подмножества $B \subset \mathcal{X}^{k-1}$, мы определим верхнюю тень:

$$up - shad(B) = \bigcup_{b^{k-1} \in B} up - shad(b^{k-1}).$$

Для фиксированного k нас интересует функция

$$\triangle(M) = \min\{|up - shad(B)| : B \subset \mathcal{X}^{k-1}, |B| = M\}.$$

Следующая функция важна для нас для нахождения связи между введенными тенями.

Определение 3. *Рассмотрим множество C последовательностей длинны n и мощности M. Тогда $s_n(C,M)$ это число пар (z, x^n), $z \in \mathcal{X}$, $x^n = (x_1, x_2, \ldots, x_n) \in C$ таких, что выполнено*

$(z, x_1, x_2, \ldots, x_{n-1}) \in C$.

Обозначим через

$$s_n(M) = max_C s_n(C,M). \tag{39}$$

Лемма 5. Следующие условия эквивалентны для $C \subseteq \mathcal{X}^n$

(i) $|C| \neq q^n$

(ii) $\exists z \in \mathcal{X}$ такое, что $c^n = (c_1, c_2, \ldots, c_n) \in C$, $(z, c_1, c_2, \ldots, c_{n-1}) \notin C$

(iii) $\nabla(\triangle(C)) \neq C$

(iv) $\triangle(\nabla(C)) \neq C$

Доказательство.

$(ii) \Rightarrow (iii)$ Рассмотрим $c \in C$, удовлетворяющее (i).

Тогда $(z, c_1, c_2, \ldots, c_n) \in \triangle(C)$ и справедливо

$y^n = (z, c_1, c_2, \ldots, c_{n-1}) \in \nabla(\triangle(C))$.

Но из (ii) вытекает $y^n \notin C$. Следовательно $\nabla(\triangle(C)) \neq C$.

$(iii) \Rightarrow (i)$ Множество $\triangle(c^n)$ состоит из $\mathcal{X}c_1, c_2, \ldots, c_n \cup c_1, c_2, \ldots, c_n\mathcal{X}$. Таким образом,

$$\nabla(\triangle(c^n)) = c_1, c_2, \ldots, c_n \cup \mathcal{X}c_1, c_2, \ldots, c_{n-1} \cup c_2, \ldots, c_n\mathcal{X}$$

Поэтому $C \subseteq \nabla(\triangle(C))$. Следовательно, (i) доказано.

$(ii) \Rightarrow (iv)$ Рассмотрим $c^n \in C$, удовлетворяющее свойству (ii). Тогда $(c_1, c_2, \ldots, c_{n-1}) \in \nabla(C)$ и получаем $y^n = (z, c_1, c_2, \ldots, c_{n-1}) \in \triangle(\nabla(C))$. Но из (ii) мы имеем $y^n \notin C$.

$(iv) \Rightarrow (i)$ Для любого $c^n \in C$ имеем

$$\nabla(c^n) = c_2, \ldots, c_n \cup c_1, c_2, \ldots, c_{n-1}$$

и

$$\triangle(\nabla(c^n)) = \mathcal{X}c_2, \ldots, c_n \cup c_2, \ldots, c_n\mathcal{X} \cup \mathcal{X}c_1, c_2, \ldots, c_{n-1} \cup c_1, c_2, \ldots, c_{n-1}\mathcal{X}.$$

Таким образом,

$$C \subseteq \nabla(\triangle(C)) \subseteq \triangle(\nabla(C)).$$

Следовательно получаем (i).

$(i) \Rightarrow (ii)$ Предположим, что мы имеем для всех $z \in \mathcal{X}$ и для всех $c^n \in C$ свойство (ii). Тогда $\mathcal{X}c_1, c_2, \ldots, c_{n-1} \in C$.

Значит $\mathcal{X}\mathcal{X}c_1, c_2, \ldots, c_{n-2} \in C$, $\mathcal{X}\mathcal{X}\mathcal{X}c_1, c_2, \ldots, c_{n-3} \in C$ и так далее. Следовательно, $\mathcal{X}\mathcal{X}\mathcal{X}\ldots\mathcal{X}\mathcal{X} \in C$ и получается противоречие с (i).

Из (ii) и определения 3 сразу следует

Следствие 4. Если $M' < M$, то из этого следует, что

$$s(M') < s(M).$$

Таким образом, функция $s(M)$ является монотонно возрастающей.

Утверждение 10. Для любых q, k, and $M \leq q^{k-1}$ справедливо

$$\nabla_k(s_{k-1}(M)) = M.$$

Доказательство. Пусть C ($|C| = M$) является множеством, на котором достигается максимум в (39). Мы будем добавлять последовательность $(z, x_1, x_2, \ldots, x_n)$ в множество D,если для этого z и $(x_1, x_2, \ldots, x_n) \in C$ выполняется условие из определения. Тогда $|D| = s_n(M)$ и $shad(D) = C$. Значит

$$\nabla_k(s_{k-1}(M)) \leq M.$$

Если бы было множество C' меньшей мощности M', $M' < M$ и такое, что $s(M') = s(M)$, то это бы противоречило следствию 4. Следовательно, $\nabla_k(s_{k-1}(M)) = M$.

Из доказанного вытекает

Следствие 5. Если $N < q^k$, то

$$\frac{1}{q}N < \nabla_k(q, N). \tag{40}$$

Задачи нахождения изопериметрических чисел на графах давно изучаются.

Рассмотрим граф $G(V, E)$, где V это множество вершин, а E это множество ребер графа. Пусть $X \subseteq V$ является некоторым множеством вершин. Тогда через ∂X обозначим множество ребер, имеющих один конец в X, а другой конец в $V \backslash X$. Таким образом,

$$\partial X = \{(x, y) \in E; x \in X, y \in V \backslash X\}.$$

Реберно-изопериметрическое число этого графа определяется как

$$i(G) = min \frac{|\partial X|}{|X|},$$

где минимум берется по всем непустым подмножествам $X \subset V$, удовлетворяющим условию $|X| \leq |V|/2$.

Обозначим через $N(X)$ множество вершин из $V \backslash X$, соединенных ребром с какой-то вершиной из X.

Таким образом,

$$N(X) = \{y \in V \backslash X; x \in X, (x, y) \in E\}.$$

Вершинно-изопериметрическое число этого графа определяется как

$$i_v(G) = min \frac{|N(X)|}{|X|},$$

где минимум берется по всем непустым подмножествам $X \subset V$, удовлетворяющим условию $|X| \leq |V|/2$.

Мы хотим рассмотреть графы, связанные с отношением слово-подблок: U-D граф и D-U граф.

Вершинами для этих графов являются все последовательности из $\mathcal{X}^n$.

Для U-D графа вершины $a^n = a_1a_2\cdots a_n$ и $b^n = b_1b_2\cdots b_n$ соединены ребром ($a^n \neq b^n$) тогда и только тогда, когда существует c^{n+1} такое, что

$$c^{n+1} \in up - shad(a^n); \quad b^n \in shad(c^{n+1}).$$

Мы хотели бы иметь биекцию между ребрами U-D графа и словами из $\mathcal{X}^{n+1}$.

Таким образом, для $a^n = b^n$ в графе проведем ребро (петлю) тогда и только тогда, когда $a_1 = a_2 = a_3 = \cdots = a_n$.

Заметим, что степень вершины равна $2q-1$ для a^n с $a_1 = a_2 = a_3 = \cdots = a_n$ и $2q$ для остальных вершин.

Для D-U графа ребро соединяет вершины $a^n = a_1a_2\cdots a_n$ и $b^n = b_1b_2\cdots b_n$, где $a^n \neq b^n$, тогда и только тогда, когда существует слово d^{n-1} такое, что

$$d^{n-1} \in shad(a^n); \quad b^n \in up - shad(d^{n-1}).$$

Общее число ребер в D-U графе равно $q^{n-1}q(q-1)+q^{n+1} = q^n(2q-1)$.

Имеется тесная связь с графом де Брейна.

Напомним, что для фиксированных n и $k = n+1$ мы интересуемся величиной

$$\nabla(N) = \min\{|shad(A)| : A \subset \mathcal{X}^k, |A| = N\}.$$

в теории графов n-размерный граф де Брейна на q символах это ориентированный граф. Граф имеет q^n вершин, являющихся всевоз-

можными n-последовательностями из данных q символов. Если одна из вершин может быть получена из другой сдвигом влево на одну позицию и добавлением нового символа в конец, то граф имеет ориентированное ребро, соединяющее данные вершины. Следовательно множество (ориентированных) ребер это

$$E = \{((v_1, v_2 \cdots, v_n), (w_1, w_2 \cdots, w_n)) : \\ v_2 = w_1, v_3 = w_2, \cdots v_n = w_{n-1}\}$$

Каждая вершина имеет ровно q входящих и q выходящих ребер. Рассмотрим неориентированный (k-1)-размерный граф де Брейна. Он очень близок к U-D графу. (Последовательности a^k из $\mathcal{X}^k$ являются ребрами в этом графе. Левая тень $shad^L(a^k)$ и правая тень $shad^R(a^k)$ будут вершинами, инцидентными данному ребру). Для a^n с $a_1 = a_2 = a_3 = \cdots = a_n$ имеется петля в U-D графе и две петли в графе де Брейна.

Проблема минимальной тени эквивалентна проблеме нахождения N ребер, инцидентных минимально возможному числу вершин. Теорема показывает, что проблема нахождения M вершин в U-D графе, которые дают максимально возможное число ребер между ними является обратной проблемой. Таким образом, функция $s_{k-1}(M)$ очень важна для нас. Она также связана с проблемой нахождения верхней тени.

Утверждение 11. Для любых q, k и $M \leq q^{k-1}$ справедливо соотношение

$$\triangle(M) = 2qM - s_{k-1}(M).$$

Доказательство.

Граф де Брейна является регулярным. Степень вершины равна $2q$. Значит мы имеем $2qM$ ребра, которые инцидентны с M вершинами из множества C, но некоторые ребра мы посчитали дважды. Число ребер, посчитанных дважды равно $s_{k-1}(M)$ и, значит, число ребер инцидентных множеству C равно $2qM - s_{k-1}(M)$, что доказывает теорему.

Утверждение 12. Для любого $M \leq q^{k-1}$ справедливо соотношение

$$s_{k-1}(q^{k-1} - M) = q^k - 2qM + s_{k-1}(M).$$

Доказательство.

Пусть C ($|C| = M$) является множеством вершин на котором достигается максимум в (39). Пусть множество B мощности $|B| = \triangle_{k-1}(M)$ состоит из ребер инцидентных M вершинам из множества C. Тогда любое ребро не из B дает тень не из C. Следовательно,

$$\nabla_k(q^k - \triangle(M)) \leq q^{k-1} - M$$

Получаем, что

$$\triangle(M) = 2qM - s_{k-1}(M).$$

Из этого и следствия 5 получаем

$$s_{k-1}(q^{k-1} - M) \geq q^k - 2qM + s_{k-1}(M).$$

Мы можем проделать тоже самое с множеством $\mathcal{X}^{k-1} \backslash C$ и тогда получим

$$\nabla_k(q^k - \triangle_{k-1}(q^{k-1} - M)) \leq M.$$

Значит

$$s_{k-1}(M) \geq q^k - 2q(q^{k-1} - M) + s_{k-1}(q^{k-1} - M).$$

Тогда

$$s_{k-1}(q^{k-1} - M) \leq q^k - 2qM + s_{k-1}(M)$$

и это доказывает утверждение.

Используя это утверждение, мы можем посчитать скорость R для больших значений N.

Утверждение 13. Для $N = 2^k - 2^l(l+3)$ и $l < k/2$ в двоичном случае справедливо

$$R \leq 1/2(1 + \frac{1}{2^{k-l} - l - 3}).$$

Доказательство. Для $l < k/2$ и $M = 2^{l-1}(l+2)$ получаем $s(M) = 2^l(l+1)$. Из теоремы 8 вытекает, что

$$s_{k-1}(2^{k-1} - 2^{l-1}(l+2)) = 2^k - 2^{l-1}4(l+2) + 2^l(l+1) = 2^k - 2^l(l+3).$$

Следовательно,

$$R \leq \frac{2^{k-1} - 2^{l-1}(l+2)}{2^l(2^{k-l} - l - 3)} = 1/2(1 + \frac{1}{2^{k-l} - l - 3}).$$

Утверждение 14. Для $N = q^k - q^l(q + (q-1)(l+1))$ и $l < k/2$ в q-ичном случае справедливо

$$R \leq \frac{1}{q}(1 + \frac{q-1}{q^{k-l} - (q + (q-1)(l+1))}).$$

Доказательство. Для $l < k/2$ и $M = q^{l-1}(q + l(q-1))$ получаем $s(M) = q^l(q + (q-1)(l-1))$. Из предыдущего вытекает, что

$$s_{k-1}(q^{k-1} - q^{l-1}(q + l(q-1))) \\ = q^k - 2qq^{l-1}(q + l(q-1)) + q^l(q + (q-1)(l-1)).$$

$$s_{k-1}(q^{k-1} - q^{l-1}(q + l(q-1))) = q^k - q^l(q + (q-1)(l+1)).$$

Следовательно,

$$R \leq \frac{q^{k-1} - q^{l-1}(q + l(q-1))}{q^k - q^l(q + (q-1)(l+1))} = \frac{1}{q}(1 + \frac{q-1}{q^{k-l} - (q + (q-1)(l+1))}).$$

Обозначим через $i(Up - Down)$ реберно-изопериметрическое число графа U-D. Для любых q, k и $M \leq q^{k-1}$ справедлива

Утверждение 15. Для $|N| \leq q^k/2 - i(B(k-1,q)q^{k-1}/4$ имеем

$$\frac{\nabla_k(N)}{N} \geq \frac{1}{q}(1 + \frac{i(Up - Down)}{2q - i(Up - Down)}). \tag{41}$$

Доказательство. Для $M \leq q^{k-1}/2$ вытекает, что

$$2q - \frac{2s(M)}{M} \geq i(Up - Down)$$

поскольку

$$min\{|\partial X|; |X| = M\} = \triangle(M) - s(M) = 2qM - 2s(M). \tag{42}$$

Следовательно,

$$s(M) \leq qM - i(Up - Down)M/2.$$

Таким образом,

$$\frac{\nabla_k(qM - i(Up - Down)M/2)}{qM - i(Up - Down)M/2} \geq \frac{M}{qM - i(Up - Down)M/2}.$$

Получаем

$$\frac{M}{qM - i(Up - Down)M/2} = \frac{1}{q}(1 + \frac{i(Up - Down)}{2q - i(Up - Down)}),$$

что доказывает утверждение.

В ([130]) доказано, что

$$i(U - D) \geq \frac{q}{2(n-1)}.$$

Следовательно, получаем

Следствие 6. Для $|N| \leq q^k/2 - \frac{q^k}{8(k-2)}$ справедливо

$$\frac{\nabla_k(N)}{N} \geq \frac{1}{q}(1 + \frac{1}{4k-9}). \tag{43}$$

Посмотрим на реберно-изопериметрическое число для графа де-Брейна.

В ([130]) Delorme и Tillich получили верхнюю границу для реберно-изопериметрического числа графа де-Брейна:

$$i(B(n,q)) \leq \frac{2q\pi}{n+1}.$$

Мы улучшим эту границу.

Утверждение 16. *Реберно-изопериметрическое число графа де-Брейна удовлетворяет следующему неравенству*

$$i(B(n,q)) \leq \frac{2q}{n - 2\log_q n + 1},$$

а для двоичного случая

$$i(B(n,q)) \leq \frac{4}{n - \log n + 2}.$$

Доказательство.

Из (42) следует, что используя $M = |\mathcal{B}(n,l,0)|$ получаем

$$i(B(n,q)) \leq 2q - \frac{2s(M)}{M}.$$

Имеем

$$\frac{M}{s(M)} \leq \frac{|\mathcal{B}(n,l,0)|}{|\mathcal{B}(k,l,1)|} \leq \frac{1}{q}(1+\frac{1}{l}),$$

а для двоичного случая

$$\frac{M}{s(M)} \leq \frac{|\mathcal{B}(n,l,0)|}{|\mathcal{B}(k,l,1)|} \leq \frac{1}{2}(1+\frac{1}{l+1}).$$

Значит

$$i(B(n,q)) \leq 2q - \frac{2ql}{l+1} = \frac{2q}{l+1},$$

а для двоичного случая

$$i(B(n,2)) \leq 4 - \frac{4(l+1)}{l+2} = \frac{4}{l+2}.$$

Из леммы 5 получаем, что

$$|\mathcal{B}(n,l,0)| \leq 2^{l-1}(l+2).$$

Следовательно, для $m \geq \log n$ имеем $l \leq n - \log n$ и для $n \geq 4$

$$|\mathcal{B}(n,l,0)| \leq \frac{2^n(n-\log n+4)}{2n} \leq \frac{2^n}{2}.$$

Значит, для двоичного случая получаем

$$i(B(n,2)) \leq \frac{4}{n-\log n+2}.$$

Из леммы 5 вытекает, что

$$|\mathcal{B}(n,l,0)| \leq q^{l-1}(l(q-1)+q).$$

Следовательно, для $m \geq 2\log n$ имеем $l \leq n - 2\log n$ и для $n \geq q$

$$|\mathcal{B}(n,l,0)| \leq \frac{q^n((n-2\log n+1)q)}{n^2 q} \leq \frac{q^n}{2}.$$

Значит

$$i(B(n,q)) \leq \frac{2q}{n - 2\log_q n + 1}.$$

Также интересно посмотреть на вершинно-изопериметрическое число.

В ([130]) Delorme и Tillich получили верхнюю границу для вершинно-изопериметрического числа:

$$i_v(B(n,q)) \leq \frac{2\sqrt{q}\pi}{(n+1)\sqrt{1 - ((2q\pi)/(n+1))^2}}.$$

В ([105]) Bultermann улучшил эту границу:

$$i_v(B(n,q)) \leq \frac{4}{n-2}$$

для $n \geq 9$.

Рассмотрим базисное множество $\mathcal{B}(n,l,1)$, где $l + m + 1 = n$.

$$N(\mathcal{B}(n,l,1)) = \mathcal{X}^l 10^m \cup 0^m 1 \mathcal{X}^l.$$

Значит

$$|N(\mathcal{B}(n,l,1))| = 2^l + |0^m 1 \mathcal{X}^{l-m-1} 0 \mathcal{X}^m| + |0^m 1 \mathcal{X}^{l-m-1} 1 \mathcal{X}^m|.$$

Таким образом, имеем

$$|N(\mathcal{B}(n,l,1))| = 2^l + 2^{l-1} + 2^{l-m-1}(2^m - 1) = 2^{l+1} - 2^{l-m-1}.$$

Из оценок на мощность базисных множеств вытекает, что

$$|\mathcal{B}(n,l,1)| \geq 2^l(l+1) - 2^{l-m-1}(l-m+1)(l-m-1).$$

Следовательно,

$$\frac{|N(\mathcal{B}(n,l,1))|}{|\mathcal{B}(n,l,1)|} \leq \frac{2^{l+1} - 2^{l-m-1}}{2^l(l+1) - 2^{l-m-1}(l-m+1)(l-m-1)}.$$

Положим $m = 2\log n$, тогда $l = n - 2\log n - 1$ и для $n \to \infty$ получаем

$$\frac{|N(\mathcal{B}(n,l,1))|}{|\mathcal{B}(n,l,1)|} \leq \frac{2}{n}(1 + o(1)).$$

Очевидно, что

$$|\mathcal{B}(n,l,1)| \leq 2^l(l+1).$$

Следовательно, для $m \geq \log n$ получаем $l \leq n - \log n - 1$ и

$$|\mathcal{B}(n,l,1)| \leq \frac{2^n(n - \log n)}{2n} \leq \frac{2^n}{2}.$$

Значит, для $n \to \infty$ получаем

$$i_v(B(n,2)) \leq \frac{2}{n}(1 + o(1)).$$

Утверждение 17. Вершинно-изопериметрическое число графа де-Брейна $B(n,q)$ удовлетворяет следующему неравенству для $n \to \infty$

$$i_v(B(n,q)) \leq \frac{q+2}{qn}(1 + o(1)).$$

Доказательство. Для двоичного случая мы уже доказали это выше. Для q-ичного случая вновь рассмотрим базисное множество $\mathcal{B}(n,l,1)$, где $l + m + 1 = n$.

$$N(\mathcal{B}(n,l,1)) = \mathcal{X}^l\overline{\mathcal{X}}0^m \cup 0^m\overline{\mathcal{X}}\mathcal{X}^l,$$

где через $\overline{\mathcal{X}}$ обозначен любой ненулевой элемент.

Тогда

$$|N(\mathcal{B}(n,l,1))| = q^l(q-1) + |0^m\overline{\mathcal{X}}\mathcal{X}^{l-m-1}0\mathcal{X}^m| + |0^m\overline{\mathcal{X}}\mathcal{X}^{l-m-1}\overline{\mathcal{X}}(\mathcal{X}^m \backslash 0^m)|.$$

Следовательно, получаем

$$|N(\mathcal{B}(n,l,1))| = q^l(q-1) + 2q^{l-1}(q-1) - q^{l-m-1}(q-1).$$

Положим $m = 2\log n$. Тогда возможно проверить, как в двоичном случае, что для больших n имеем $|\mathcal{B}(n,l,1)| \leq \frac{q^n}{2}$ и

$$i_v(B(n,q)) \leq \frac{q+2}{qn}(1+o(1)).$$

1.6 Выводы

В данной главе рассматривается задача передачи информации по q-ичному каналу с безошибочной обратной связью.

Во втором параграфе главы описан алгоритм r удаления. Основным результатом второго параграфа является Теорема 1. Она показывает, что алгоритм 1 удаления является оптимальным для доли ошибок в канале, большей $1/q$.

В третьем параграфе оценивается число q-ичных последовательностей, содержащих подблок 00 ровно r раз. Основным результатом третьего параграфа является Утверждение 4.

В четвертом параграфе главы описан обобщенный алгоритм 1 удаления. Основными результатами четвертого параграфа являются Теорема 2 и Утверждение 5. Они показывают, что обобщенный алгоритм 1 удаления позволяет передавать больше сообщений на интервале, приведенном в Утверждении 5.

Основные результаты главы опубликованы в работах [2], [70], [72], [93].

2 Дизъюнктивный канал множественного доступа

Предположим, что имеется N пользователей и каждый пользователь передает свое сообщение в виде двоичной последовательности длины t. При передаче сообщений в канал могут быть активны (передавать свои последовательности согласно разработанной заранее стратегии передачи) ровно два пользователя. В каждый момент передачи (от 1 до t) на выходе канала приходит ноль, если оба пользователя передавали в этот момент ноль, и приходит единица в остальных случаях. Стратегия передачи должна быть устроена так, чтобы по выходу канала можно было бы определить, какие именно пользователи передавали свои сообщения. И опять, если стратегия передачи может меняться в зависимости от выхода канала в каждый момент передачи, то такая стратегия называется адаптивной. Мы будем рассматривать только адаптивные стратегии.

В классической модели группового тестирования мы имеем множество $[N] := \{1, \ldots, N\}$ элементов, содержащих некоторое подмножество $D \subset [N]$ дефектных элементов. Основная задача группового тестирования заключается в нахождении множества D за минимальное число тестов. Каждый тест является некоторым подмножеством множества $[N]$. При этом подразумевается, что имеется некая тестовая функция, которая для каждого подмножества $S \subset [N]$ позволяет выяснить наличие дефектных элементов в этом подмножестве (дает ответ на тест). Формально тестовая функция $f_S : 2^{[N]} \to \{0, 1\}$

может быть определена следующим образом:

$$f_S(\mathcal{D}) = \begin{cases} 0 & \text{если} \quad |\mathcal{S} \cap \mathcal{D}| = 0 \\ 1 & \text{если} \quad |\mathcal{S} \cap \mathcal{D}| > 0. \end{cases} \tag{44}$$

Набор тестов образует алгоритм поиска. Назовем алгоритм поиска успешным, если, после его применения, мы однозначно определяем $\mathcal{D}$ по ответам $f_{\mathcal{S}_1}, \ldots, f_{\mathcal{S}_t}$. Алгоритмы бывают адаптивными и неадаптивными. В адаптивном алгоритме при выборе очередного теста могут быть использованы результаты предыдущих тестов. В неадаптивном алгоритме все тесты независимы. В данной работе мы будем рассматривать только адаптивные алгоритмы поиска.

В дальнейшем нам понадобятся следующие обозначения. Пусть $|\mathcal{D}| = D$ число дефектных элементов, а $N_t(D)$ максимальное число элементов среди которых можно найти D дефектных элементов за t тестов. Для адаптивного алгоритма $a = a(N, D, t)$ обозначим через $a_t(D)$ максимальное число элементов, для которых доказано, что $D, a_t(D)$ проблема решается за t тестов, то есть алгоритм a является успешным. Таким образом, $a_t(D)$ является нижней границей для $N_t(D)$.

2.1 Дизъюнктивный канал множественного доступа с двумя активными пользователями

В этом разделе мы рассматриваем классическую $(2, N)$ проблему группового тестирования нахождения двух дефектных элементов среди N элементов. Мы предлагаем новый адаптивный алгоритм такой, что $(2, \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor)$ проблема может быть решена за t тестов. Подчеркнем еще раз, что в данном параграфе изучаются толь-

ко адаптивные алгоритмы для случая $D = 2$. На протяжении этого параграфа мы анализируем наихудший случай и хотим предъявить алгоритм, который оптимален почти для всех значений N. Более точно, мы опишем алгоритм w такой, что $\frac{w_t(2)}{N_t(2)} \to 1$, если $t \to \infty$. Далее, мы докажем, что $w_t(2) \geq \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor$ для достаточно больших значений t ($t \geq 44$). То, что это неравенство справедливо и для $t \leq 44$, будет показано в конце параграфа.

Рассмотрим $w_t = \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor$ элементов и пусть $[N] = \mathcal{Z} \cup \mathcal{X} \cup \mathcal{Y}$ разбиение, позволяющее утверждать, что $f_{\mathcal{Z}}(\mathcal{D}) = 0$, $f_{\mathcal{X}}(\mathcal{D}) = 1$, а в множестве $\mathcal{Y}$ нет элементов, которые можно было бы добавить в $\mathcal{X}$ или $\mathcal{Z}$, сохраняя справедливость этих условий. Перед первым тестом $\mathcal{X} = [N]$, $\mathcal{Z} = \emptyset$, $\mathcal{Y} = \emptyset$. Мы будем следить за изменениями в этом разбиении после каждого теста.

- **1-й тест:** Возьмем в качестве первого теста $\mathcal{S}_1 = [1, x_1]$, где $x_1 = \lfloor (\sqrt{2} - 1)2^{\frac{t}{2}} \rfloor$.

  Если $f_{\mathcal{S}_1} = 0$, то получаем, что

  $$\mathcal{Z} = [1, x_1],\ \mathcal{X} = [x_1 + 1, w_t],\ \mathcal{Y} = \emptyset,$$

  и мы сводим задачу к тому же алгоритму, но для меньшего числа элементов.

  Если $f_{\mathcal{S}_1} = 1$, то получаем, что $\mathcal{X} = [1, x_1]$, $\mathcal{Y} = [x_1 + 1, w_t]$, $\mathcal{Z} = \emptyset$. Оценим число возможных вариантов A_1 расположения двух дефектных элементов после такого ответа на первый тест,

которое равно:

$$\begin{aligned} A_1 &= \binom{x_1}{2} + x_1 \cdot (w_t - x_1) \\ &\leq \frac{\left((\sqrt{2}-1)2^{\frac{t}{2}}\right)^2}{2} \\ &\quad +(\sqrt{2}-1)2^{\frac{t}{2}}\left(2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} - (\sqrt{2}-1)2^{\frac{t}{2}}\right) = \\ &= \frac{(2-2\sqrt{2}+1)2^t}{2} + (\sqrt{2}-1)2^t - t(\sqrt{2}-1)2^{\frac{3t}{4}} \\ &= 2^{t-1} - t(\sqrt{2}-1)2^{\frac{3t}{4}} \end{aligned}$$

- **2-й тест (после ответа $f_{\mathcal{S}_1} = 1$):** Возьмем в качестве второго теста $\mathcal{S}_2 = [1, x_2]$, где x_2 такое целое число, что величина

$$A_2 := \binom{x_2}{2} + x_2 \cdot (w_t - x_2)$$

будет наиболее близка к $A_1/2$.

Заметим, что $A_1/2$ не обязательно является целым числом. Мы будем брать ближайшее целое к $A_1/2$. Чтобы оценить A_2 вычислим разность между числом возможных вариантов расположения двух дефектных элементов после тестов мощности $i+1$ и i:

$$\frac{(i+1)i}{2} + (i+1)(w_t - i - 1) - \frac{i(i-1)}{2} - i(w_t - i) = w_t - i - 1 \leq w_t.$$

Следовательно,

$$A_2 \leq 2^{t-2} - t(\sqrt{2}-1)2^{\frac{3t}{4}-1} + w_t.$$

Заметим, что эта оценка на число возможных вариантов расположения двух дефектных элементов не зависит от того, каким

был ответ на второй тест. В случае $f_{\mathcal{S}_2} = 0$ получается разбиение

$$\mathcal{Z} = [1, x_2],\ \mathcal{X} = [x_2 + 1, x_1],\ \mathcal{Y} = [x_1 + 1, w_t],$$

а в случае $f_{\mathcal{S}_2} = 1$ получается разбиение

$$\mathcal{Z} = \emptyset,\ \mathcal{X} = [1, x_2],\ \mathcal{Y} = [x_2 + 1, w_t].$$

Но, и в том, и в другом случае, оценка для величины A_2 справедлива, так как мы разбиваем все варианты расположения двух дефектных элементов пополам (с учетом целочисленности).

Далее будем действовать аналогичным образом. Пусть после k тестов у нас получилось разбиение $\mathcal{Z} = [1, z_k]$, $\mathcal{X} = [z_k + 1, z_k + x_k]$, $\mathcal{Y} = [z_k + x_k + 1, w_t]$ (мощность множества $\mathcal{Y}$ в дальнейшем будем обозначать через y_k).

- $(k+1)$**-й тест:** Возьмем в качестве $(k+1)$-ого теста интервал $[z_k + 1, z_k + x_{k+1}]$ длины x_{k+1}, где x_{k+1} такое целое, что

$$A_{k+1} = \binom{x_{k+1}}{2} + x_{k+1} \cdot y_{k+1} \tag{45}$$

наиболее близко к $A_k/2$.

Напомним, что $w_t = \lfloor 2^{(t+1)/2} - t2^{\frac{t}{4}} \rfloor$, следовательно,

$$A_{k+1} \leq 2^{t-k-1} - t(\sqrt{2} - 1)2^{\frac{3t}{4}-k} + kw_t \tag{46}$$

Заметим, что из этого сразу вытекает

$$x_{k+1} \leq \frac{A_{k+1}}{y_{k+1}}. \tag{47}$$

Таким образом, после $k+1$ теста у нас получилось разбиение

$\mathcal{Z} = [1, z_{k+1}]$, $\mathcal{X} = [z_{k+1}+1, z_{k+1}+x_{k+1}]$, $\mathcal{Y} = [z_{k+1}+x_{k+1}+1, w_t]$.

Замечание 5. Отметим, что тесты с второго по $k+1$-й направлены на уменьшение множества $\mathcal{X}$. Причем каждый раз мы включаем в тест не половину элементов множества $\mathcal{X}$, а чуть меньше. Это интуитивно понятно, поскольку нулевой ответ лучше, так как позволяет сократить число элементов, среди которых мы ищем дефектные (элементы из множества $\mathcal{X}$ переходят в множество $\mathcal{Z}$, а не в $\mathcal{Y}$).

Тесты с $(k+2)$-го по $(2k+1)$-й направлены на уменьшение множества $\mathcal{Y}$. Нулевой ответ переводит элементы из множества $\mathcal{Y}$ в множество $\mathcal{Z}$, а единичный определяет два множества, в каждом из которых находится ровно по одному дефектному элементу.

- $(k+2)$**-й тест:** Возьмем в качестве $(k+2)$-ого теста первые $\lfloor \frac{2^{t-k-2}}{x_{k+1}} \rfloor$ элементов множества $\mathcal{Y}$ (если в $\mathcal{Y}$ оказалось меньше элементов, то возьмем все).

  Если ответ на данный тест 1, то, согласно следующему результату, мы можем найти два дефектных элемента за $2^{\frac{t+1}{2}}$ тестов.

  Этот результат получен в [108] для специального случая, когда два дефектных элемента располагаются в двух непересекающихся подмножествах множества $[N]$ по одному в каждом подмножестве.

  Утверждение 18. *Пусть известно, что множество* $A \subset [N]$ *содержит ровно один дефектный элемент и множество*

$B \subset [N]$ также содержит ровно один дефектный элемент и эти множества не пересекаются. Тогда минимальное число тестов, необходимых для нахождения дефекта из множества A, $|A| = m$ и дефекта из множества B, $|B| = n$ равно $\lceil \log mn \rceil$.

Если ответ на данный тест 0, то мы включим в следующий тест $\lfloor \frac{2^{t-k-3}}{x_{k+1}} \rfloor$ элементов из множества $\mathcal{Y}$ и так далее.

Если, в какой то момент ответ на тест даст 1, то в дальнейшем применяем алгоритм из леммы 1. Если же все ответы 0, то тестируемые элементы перемещаются из множества $\mathcal{Y}$ в множество $\mathcal{Z}$, и мы продолжаем процедуру до тех пор, пока в множестве $\mathcal{Y}$ остаются элементы.

- $(2k+1)$**-й тест:** Возьмем $\lfloor \frac{2^{t-2k-1}}{x_{k+1}} \rfloor$ элементов из множества $\mathcal{Y}$ (если в $\mathcal{Y}$ осталось меньше элементов, то возьмем все оставшиеся).

Далее будет доказано, что если выбрать $k = \lfloor \frac{t}{4} \rfloor$, то после $(2k+1)$-ого теста (или раньше) в множестве $\mathcal{Y}$ не останется элементов. Таким образом, мы опять сведем задачу к тому же алгоритму, но для меньшего числа элементов (их останется x_{k+1}).

Теперь мы докажем, что адаптивный алгоритм, предложенный выше позволяет решить $(2, \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor)$ проблему за t тестов.

Теорема 3. *Для адаптивного алгоритма $w = w(N, D, t)$ справедливо*

$$w_t(2) = \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor.$$

Доказательство: Доказательство будем вести индукцией по числу тестов. Справедливость данного утверждения для начальных значений будет показана позже. Мы предположим, что утверждение верно для числа тестов, меньших t и докажем данное предположение для числа тестов равных t.

Если после первого теста $f_{\mathcal{S}_1} = 0$, то мы знаем, что множество $\mathcal{Z} = \mathcal{S}_1$ не содержит дефектных элементов и

$$\lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor - \lfloor (\sqrt{2}-1)2^{\frac{t}{2}} \rfloor \leq 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} - 2^{\frac{t+1}{2}} + 2^{\frac{t}{2}} + 1 = 2^{\frac{t}{2}} - t2^{\frac{t}{4}} + 1.$$

Справедлива оценка

$$2^{\frac{t}{2}} - t2^{\frac{t}{4}} + 1 \leq \lfloor 2^{\frac{t}{2}} - (t-1)2^{\frac{t-1}{4}} \rfloor = w_{t-1},$$

если $t \geq 3$. Следовательно, для этого случая утверждение доказано.

Если после первого теста $f_{\mathcal{S}_1} = 1$, то число элементов y_1 не меньше, чем

$$\lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor - \lfloor (\sqrt{2}-1)2^{\frac{t}{2}} \rfloor \geq 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} - 1 - 2^{\frac{t+1}{2}} + 2^{\frac{t}{2}} \geq 2^{\frac{t}{2}} - t2^{\frac{t}{4}} - 1.$$

После $(k+1)$ теста мы имеем

$$\mathcal{Z} = [1, z_{k+1}],\ \mathcal{X} = [z_{k+1}+1, z_{k+1}+x_{k+1}],$$

$$\mathcal{Y} = [z_{k+1}+x_{k+1}+1, z_{k+1}+x_{k+1}+y_{k+1}].$$

Рассмотрим тесты с $k+2$ по $2k+1$.

Если результаты всех таких тестов дают 0 , то получаем

$$R = \lfloor \frac{2^{t-k-2}}{x_{k+1}} \rfloor + \lfloor \frac{2^{t-k-3}}{x_{k+1}} \rfloor + \ldots + \lfloor \frac{2^{t-2k-1}}{x_{k+1}} \rfloor \geq \frac{y_{k+1}(2^{t-k-1} - 2^{t-2k-1})}{A_{k+1}} - k.$$

Мы хотим, чтобы в множестве $\mathcal{Y}$ не осталось элементов, значит нужно показать, что $R \geq y_{k+1}$.

Для этого нужно, чтобы

$$y_{k+1}(2^{t-k-1} - 2^{t-2k-1} - A_{k+1}) \geq kA_{k+1}.$$

Число элементов множества $\mathcal{Y}$ после тестов со второго по $k+1$-ый может только увеличиваться, поэтому по формуле выше

$y_{k+1} \geq y_1 \geq 2^{\frac{t}{2}} - t2^{\frac{t}{4}} - 1.$

Из формулы, приведенной выше, имеем

$$2^{t-k-1} - 2^{t-2k-1} - A_{k+1} \geq t(\sqrt{2}-1)2^{\frac{3t}{4}-k} - 2^{t-2k-1} - k2^{\frac{t+1}{2}}.$$

Для выбора $k = \lfloor \frac{t}{4} \rfloor$ будем проверять условие

$(2^{\frac{t}{2}} - t2^{\frac{t}{4}} - 1)(t(\sqrt{2}-1)2^{\frac{3t}{4}-k} - 2^{t-2k-1} - k2^{\frac{t+1}{2}})$
$\geq k(2^{t-k-1} - t(\sqrt{2}-1)2^{\frac{3t}{4}-k} + k2^{\frac{t+1}{2}}).$

Это условие выполняется при $t \geq 20$ и значит для таких значений t получаем $R \geq y_{k+1}$.

Замечание 6. Естественно встает вопрос об оптимальности выбора параметра $k = \lfloor \frac{t}{4} \rfloor$. Может быть алгоритм w позволяет утверждать, что $w_t(2) = \lfloor 2^{\frac{t+1}{2}} - 2^{\gamma} \rfloor$, где $\gamma < t/4$? При таком выборе общего числа элементов получаем

$$A_{k+1} \leq 2^{t-k-1} - (\sqrt{2}-1)2^{\frac{t}{2}+\gamma-k} + kw_t. \tag{48}$$

Получается, что величина

$$(\sqrt{2}-1)2^{\frac{t}{2}+\gamma-k} - 2^{t-2k-1} - k2^{\frac{t+1}{2}}$$

должна быть достаточно большой, откуда следует, что

$$\begin{cases} t/2 + \gamma - k & \geq & t - 2k \\ t/2 + \gamma - k & \geq & t/2. \end{cases} \tag{49}$$

Отсюда вытекает, что $\gamma \geq t/4$.

За $2k+1$ тестов мы свели задачу к такой же задаче, но для x_{k+1} элемента. Справедливы следующие соотношения

$$x_{k+1} \leq \frac{A_{k+1}}{y_{k+1}} \leq \frac{2^{t-k-1} - t(\sqrt{2}-1)2^{\frac{3t}{4}-k} + k2^{\frac{t+1}{2}}}{y_{k+1}}$$

$$y_{k+1} \geq 2^{\frac{t}{2}} - t2^{\frac{t}{4}} - 1$$

$$w_{t-(2k+1)} = \lfloor 2^{\frac{t}{2}-k} - (t-2k-1)2^{\frac{t-2k-1}{4}} \rfloor$$

Мы хотим показать, что $x_{k+1} \leq w_{t-(2k+1)}$ для $k = \lfloor \frac{t}{4} \rfloor$, значит нужно, чтобы выполнялось соотношение

$$2^{t-k-1} - t(\sqrt{2}-1)2^{\frac{3t}{4}-k} + k2^{\frac{t+1}{2}} \leq (2^{\frac{t}{2}-k} - (t-2k-1)2^{\frac{t-2k-1}{4}} - 1)(2^{\frac{t}{2}} - t2^{\frac{t}{4}} - 1). \quad (50)$$

Можно проверить, что эта оценка (неравенство) заведомо справедливо при $t \geq 44$.

Ниже будет показано, что при $t \leq 44$ мы можем решить $(2, \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor)$ проблему. Таким образом, теорема доказана.

Посмотрим теперь, чему равно число тестов при небольшом количестве элементов.

Как уже отмечалось, в [110] был построен алгоритм, решающий $(2, c_t)$ проблему за t тестов, где

$$c_t = \begin{cases} 89 \cdot 2^{k-6} & \text{для } t = 2k \geq 12, \\ 63 \cdot 2^{k-5} & \text{для } t = 2k+1 \geq 13. \end{cases}$$

Алгоритм, предложенный нами является обобщением данного алгоритма. Алгоритм из [110] состоит в том, что первый тест выделяет $x_1^t = c_t - c_{t-1}$ элементов в множество $\mathcal{X}$, а второй и третий тесты

уменьшают множество $\mathcal{Y}$ на y_1^t и y_2^t, где $x_1^t y_1^t \leq 2^{t-2}$ и $x_1^t y_2^t \leq 2^{t-3}$. Фактически, в [110] было показано, что для $t = 12$ и $t = 13$ выполнено соотношение

$$c_t - y_1^t - y_2^t = c_{t-3} \tag{51}$$

и, если в дальнейшем увеличивать размер тестов вдвое ($x_1^{t+2} = 2x_1^t$, $y_1^{t+2} = 2y_1^t$, $y_2^{t+2} = 2y_2^t$), то соотношение (51) будет выполняться для всех t. К сожалению $c_{44} = 5832704$, что меньше, чем $w_{44} = \lfloor 2^{\frac{44+1}{2}} - 44 \cdot 2^{11} \rfloor) = 5841529$.

Рассмотрим алгоритм c^1, который определим следующим образом. Для алгоритма c^1 возьмем значения x_1^t, y_1^t и y_2^t при $14 \leq t \leq 20$, которые приведены в следующей таблице:

t	$c_t^1(2)$	x_1^t	y_1^t	y_2^t	$c_t^1 - y_1^t - y_2^t$
12	89	26	39	19	31
13	126	37	55	27	44
14	178	52	78	39	61
15	252	74	110	55	87
16	357	105	156	78	123
17	506	149	219	109	178
18	717	211	310	155	252
19	1015	298	439	219	357
20	1437	422	621	310	506

Условия $x_1^t y_1^t \leq 2^{t-2}$ и $x_1^t y_2^t \leq 2^{t-3}$ для приведенных численных значений легко проверяются для каждого случая.

В дальнейшем будем увеличивать размер тестов вдвое ($x_1^{t+2} = 2x_1^t$, $y_1^{t+2} = 2y_1^t$, $y_2^{t+2} = 2y_2^t$). Можно увидеть, что соотношение (51) будет выполняться для всех $t \geq 20$. Таким образом, получим $c_{44}^1 =$

5898237, что больше, чем 5841529. Для алгоритма c^1 при $t \leq 44$ значения c_t^1 также больше, чем $w_t = \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor$. Значит $w_t(2) \geq \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor$ и для $t \leq 44$.

Следствие 7. *Для $t \to \infty$ справедливо*

$$\frac{w_t}{N_t(2)} \to 1.$$

Доказательство. Мы имеем

$$\frac{w_t}{N_t(2)} \geq \frac{w_t}{\lfloor 2^{\frac{t+1}{2}} - \frac{1}{2} \rfloor},$$

где $w_t = \lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor$.

Легко видеть, что

$$\frac{\lfloor 2^{\frac{t+1}{2}} - t2^{\frac{t}{4}} \rfloor}{\lfloor 2^{\frac{t+1}{2}} - \frac{1}{2} \rfloor} \to 1,$$

при $t \to \infty$.

2.2 Поиск одного из нескольких дефектов

В [137] рассматривалась задача обнаружения одного дефектного элемента в конечном множестве, где элемент i является дефектным с вероятностью p_i. Случай, когда все вероятности одинаковы, возникал уже в [155].

В [101] изучалась задача обнаружения по крайней мере k недефектных элементов. Это исследование было мотивировано практической задачей для фирмы по производству электроники. Производственному отделу фирмы для нужд производственного процесса

требуется 10^6 недефектных микросхем. Имеется метод тестирования группы микросхем. При этом закупаются микросхемы с качеством 99% (т.е. микросхема дефектна с вероятностью 0,01), и требуется отыскать много недефектных элементов за небольшое число групповых тестов.

Мы будем рассматривать комбинаторный вариант этой задачи. Итак, требуется обнаружить m из D дефектных элементов. Мотивация такой задачи приведена в [140]. Через $[N] := \{1, 2, \ldots, N\}$ обозначим множество элементов, через $\mathcal{D} \subset [N]$ – множество дефектных элементов, через $D = |\mathcal{D}|$ – его мощность, а через $[i, j]$ – множество целых чисел $\{x \in \mathbb{N} : \ i \leq x \leq j\}$. Всюду далее проводится анализ для наихудшего случая.

Классическая задача группового тестирования состоит в обнаружении неизвестного множества $\mathcal{D}$ всех дефектных элементов в $[N]$.

Для подмножества $\mathcal{S} \subset [N]$ тестом $t_{\mathcal{S}}$ называется функция $t_{\mathcal{S}} \colon 2^{[N]} \to \{0, 1\}$ вида

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| = 0, \\ 1 & \text{в противном случае.} \end{cases} \tag{52}$$

Следуя [89], определим стратегии поиска. В классическом групповом тестировании стратегия называется успешной, если она позволяет *однозначно определить* $\mathcal{D}$. В нашем случае стратегия успешна, если она позволяет определить m элементов множества $\mathcal{D}$. Напомним понятия адаптивной и неадаптивной стратегии.

Стратегия называется адаптивной, если k-й тест определяется на основании результатов первых $k-1$ тестов. Стратегии, где все тесты выбираются независимо, называются неадаптивными.

Пусть f – некоторая функция $f\colon [0,N] \to \mathbb{R}^+$. Определим *общие групповые тесты с плотностью* как функции $t_{\mathcal{S}}\colon 2^{[N]} \to \{0,1\}$ вида

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| < f(|\mathcal{S}|), \\ 1, & \text{если } |\mathcal{S} \cap \mathcal{D}| \geq f(|\mathcal{S}|). \end{cases} \tag{53}$$

В [140] рассматривается случай $f(|\mathcal{S}|) = \alpha|\mathcal{S}|$. При этом предполагается, что известна нижняя оценка на мощность множества $\mathcal{D}$. Цель состоит в обнаружении $m \leq D$ дефектных элементов.

В мажоритарном групповом тестировании (введенном в [70]) имеются две функции

$$f_1, f_2\colon \{0,1,\ldots,N\} \to \mathbb{R}^+,$$

задающие веса на числе D дефектных элементов, где

$$f_1(D) \leq f_2(D) \quad \text{для всех} \quad D \in [0,1,\ldots,N].$$

Зададим структуру тестов $t_{\mathcal{S}}\colon 2^{[N]} \to \{0,1,\{0,1\}\}$ следующим образом:

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| < f_1(D), \\ 1, & \text{если } |\mathcal{S} \cap \mathcal{D}| \geq f_2(D), \\ \{0,1\} & \text{в противном случае (т.е. результат 0 или 1} \\ & \text{выбирается произвольно).} \end{cases} \tag{54}$$

Если предполагается, что мощность множества $\mathcal{D}$ неизвестна, но имеется некоторая ее верхняя оценка. При мажоритарном групповом тестировании не всегда возможно определить множество $\mathcal{D}$ всех дефектных элементов. В общем случае возможно найти семейство $\mathbb{F}$

множеств, содержащее $\mathcal{D}$. Это семейство зависит от функций f_1 и f_2, множества $\mathcal{D}$ и используемой стратегии. В этом случае стратегия называется успешной, если она позволяет найти семейство $\mathbb{F}$ наименьшего возможного размера.

Обобщая идеи обеих моделей, дадим единое описание: пусть заданы две функции

$$f_1, f_2 \colon [0, N] \times [0, N] \to \mathbb{R}^+,$$

такие, что $f_1(D, S) \leq f_2(D, S)$ для любых значений D и S.

Определим тест $t_{\mathcal{S}} \colon 2^{[N]} \to \{0, 1, \{0, 1\}\}$ следующим образом:

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| < f_1(D, |\mathcal{S}|), \\ 1, & \text{если } |\mathcal{S} \cap \mathcal{D}| \geq f_2(D, |\mathcal{S}|), \\ \{0, 1\} & \text{в противном случае (т.е. результат 0 или 1} \\ & \text{выбирается произвольно).} \end{cases} \tag{55}$$

Для такой тестовой функции обозначим через $n(N, D, m)$ минимальное число тестов, требуемой для определения m дефектных элементов.

Следующая нижняя граница на минимальное число тестов является обобщением теоремы из [140], где нижняя граница дана для случая

$$f_1(D, |\mathcal{S}|) = f_2(D, |\mathcal{S}|) = \alpha|\mathcal{S}|.$$

Данная оценка справедлива для произвольной двоичной тестовой функции (т.е. такой, которая принимает значения 0 или 1).

Теорема 4. Справедлива оценка

$$n(N, D, 1) \geq \lceil \log(N - D + 1) \rceil.$$

Доказательство. Пусть имеется успешная стратегия s, позволяющая обнаружить дефектный элемент за $n = n(N, D, 1)$ тестов, и $n < \lceil \log(N - D + 1) \rceil$.

В зависимости от результатов n тестов, имеется не более 2^n различных возможностей для дефектного элемента. Обозначим их через $\mathcal{E}$. Согласно предположению имеем

$$|\mathcal{E}| \leq 2^n < N - D + 1.$$

Значит, $|[N] \setminus \mathcal{E}| > D - 1$, и существует множество $\mathcal{F} \subset [N] \setminus \mathcal{E}$, такое что $|\mathcal{F}| = D$. Теперь рассмотрим случай $\mathcal{D} = \mathcal{F}$. Тогда очевидно, что с помощью стратегии s найти дефектный элемент за n тестов невозможно. Теорема доказана.

Рассмотрим следующий специальный случай модели тестирования:

Пороговое групповое тестирование без зазора: $f(D, |\mathcal{S}|) = u$, т.е.

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| < u, \\ 1, & \text{если } |\mathcal{S} \cap \mathcal{D}| \geq u. \end{cases} \tag{56}$$

Групповое тестирование с плотностью: $f(D, |\mathcal{S}|) = \alpha|\mathcal{S}|$ для всех значений, т.е.

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| < \alpha|\mathcal{S}|, \\ 1, & \text{если } |\mathcal{S} \cap \mathcal{D}| \geq \alpha|\mathcal{S}|. \end{cases} \tag{57}$$

Для всех этих тестовых функций будем рассматривать адаптивную модель поиска одного дефектного элемента.

Сначала мы рассмотрим тестовую функцию для классического случая и приведем оптимальную стратегию поиска одного из D де-

фектных элементов, состоящая из $\lceil \log(N - D + 1) \rceil$ тестов. Далее даны стратегии для тестовой функции в пороговом случае и показано, что в случае $m = 1$ стратегия оптимальна. Кроме того, показано, как эту стратегию можно применять в комбинации со стратегией поиска m элементов. Затем приведена стратегия для тестовой функции и сделано несколько замечаний о неадаптивном групповом тестировании.

2.3 Классическая тестовая функция

В этом разделе рассматривается классическая тестовая функция. Предполагается, что значение D $(0 < D < N)$ известно. Целью является определение m дефектных элементов.

Через $n_{(\mathrm{Cla})}(N, D, m)$ обозначим минимальное число тестов, необходимых для определения m дефектных элементов.

Утверждение 19. Справедлива оценка

$$n_{(\mathrm{Cla})}(N, D, 1) \leq \lceil \log(N - D + 1) \rceil.$$

Опишем стратегию, состоящую из $\lceil \log(N-D+1) \rceil$ тестов. Известно, что в множестве $\mathcal{S}_0 = \{D, D + 1, \ldots, N\}$ имеется по крайней мере один дефектный элемент. Начнем с тестового множества $\mathcal{S}_1 \subset \mathcal{S}_0$ мощности $\left\lfloor \frac{N-D+1}{2} \right\rfloor$. Если результат теста положительный, то по крайней мере один дефектный элемент содержится в $\mathcal{S}_1$, в противном случае по крайней мере один дефектный элемент содержится в $\mathcal{S}_0 \setminus \mathcal{S}_1$. Таким образом, в зависимости от результата теста заменяем $\mathcal{S}_0$ либо на $\mathcal{S}_1$, либо на $\mathcal{S}_0 \setminus \mathcal{S}_1$ и повторяем процедуру. Этим методом один дефектный элемент находится за $\lceil \log(N - D + 1) \rceil$ тестов.

Следствие 8. Справедливы соотношения

$$n_{(\mathrm{Cla})}(N, D, 1) = \lceil \log(N - D + 1) \rceil,$$

$$n_{(\mathrm{Cla})}(N, D, m) \leq m \lceil \log(N - D + 1) \rceil.$$

Замечание 7. Если значение D неизвестно, но известно, что $D' \leq D \leq D''$, где $1 \leq D' < D'' < N$, то для нахождения одного дефектного элемента требуется $\lceil \log(N - D' + 1) \rceil$ тестов.

2.4 Пороговая тестовая функция без зазора

Пороговое тестирование

$$t_S(\mathcal{D}) = \begin{cases} 0, & \text{если } |\mathcal{S} \cap \mathcal{D}| \leq l, \\ 1, & \text{если } |\mathcal{S} \cap \mathcal{D}| \geq u, \end{cases} \tag{58}$$

было введено в [115]. Зазор между верхним и нижним порогом определяется как $g = u - l - 1$. Мы будем рассматривать тестовую функцию, которая соответствует случаю без зазора ($g = 0$). Легко видеть, что в этом случае $u = l - 1$. Вначале предположим, что D известно.

Обозначим через $n_{(\mathrm{Thr})}(N, D, u, m)$ минимальное число тестов, за которое можно определить m дефектных элементов, если имеется N элементов, D из них дефектны и $f(D, |\mathcal{S}|) = u$.

Сперва рассмотрим задачу определения одного дефектного элемента.

Утверждение 20. Если $D \geq u$, то

$$n_{(\mathrm{Thr})}(N, D, u, 1) \leq \lceil \log(N - D + 1) \rceil.$$

В противном случае ни один дефектный элемент определить невозможно.

Доказательство. Опишем стратегию, требующую $\lceil \log(N-D+1) \rceil$ тестов. Идея доказательства состоит в разбиении множества из N элементов на подмножества

$$\mathcal{I}_1 = [1, u-1], \quad \mathcal{I}_2 = [u, N-D+u], \quad \mathcal{I}_3 = [N-D+u+1, N].$$

При этом, в $\mathcal{I}_2$ заведомо имеется хотя бы один дефектный элемент, поскольку объединение двух других подмножеств имеет мощность $D-1$. Найти дефектный элемент в $\mathcal{I}_2$ позволяет следующая стратегия из $\lceil \log(N-D+1) \rceil$ тестов.

Начнем с тестового множества

$$\mathcal{S}_1 = \left\{ 1, \ldots, u-1, u, \ldots, (u-1) + \left\lceil \frac{m(1)}{2}(N-D+1) \right\rceil \right\},$$

где $m(1) = 1$.

По индукции положим

$$m(j) = \begin{cases} 2m(j-1) - 1, & \text{если } t_{S_{j-1}}(\mathcal{D}) = 1, \\ 2m(j-1) + 1, & \text{если } t_{S_{j-1}}(\mathcal{D}) = 0, \end{cases}$$

и

$$\mathcal{S}_j = \left\{ 1, \ldots, u-1, u, u+1, \ldots, (u-1) + \left\lceil \frac{m(j)}{2^j}(N-D+1) \right\rceil \right\}.$$

За $\lceil \log(N-D+1) \rceil$ тестов находим такое i, что $t_{[1,i]} = 1$, $t_{[1,i-1]} = 0$, поскольку, очевидно, $t_{[1,u-1]} = 0$ и $t_{[1,N-D+u]} = 1$. Таким образом, используя эту стратегию, находим дефектный элемент на позиции i.

Следствие 9. Если $D \geq u$, то

$$n_{(\mathrm{Thr})}(N, D, u, 1) = \lceil \log(N-D+1) \rceil.$$

Эту стратегию можно обобщить на случай поиска m дефектных элементов.

Утверждение 21. Пусть $D \geq m$. Тогда

$$n_{(\mathrm{Thr})}(N, D, u, m) \leq m\lceil \log(N - D + 1)\rceil.$$

Доказательство.

Применим стратегию для нахождения одного дефектного элемента, описанную выше. Будем использовать упорядоченное множество $[N]$, и через $\pi_j(i)$ обозначим j-ю позицию перед i-м раундом тестирования. Положим $\pi_j(1) = j$. В первом раунде применим описанную стратегию и найдем дефектный элемент d_1. Затем положим

$$\pi_j(2) = \begin{cases} d_1, & \text{если } j = 1, \\ 1, & \text{если } j = d_1, \\ j, & \text{если } j \notin \{1, d_1\} \end{cases}$$

(т.е. поменяем местами элементы на позициях d_1 и 1), и применим ту же стратегию из $\lceil \log(N - D + 1)\rceil$ тестов для определения дефектного элемента d_2 в новом множестве $\{\pi_1(2), \pi_2(2), \ldots, \pi_N(2)\}$. Теперь поменяем местами элементы на позициях d_2 и 2, и будем повторять процедуру, в конце каждого раунда меняя местами элементы на позициях d_j и j, пока не найдем дефектный элемент d_u. После этого дефектный элемент на позиции d_j будем менять местами с элементом на позиции $N - D + 1 + j$. Итого за m итераций определим m дефектных элементов.

Замечание 8. Если $u - 1$ дефектных элементов уже найдено, можно применить любую стратегию классического группового тестирования для поиска оставшихся $D - u + 1$ дефектных элементов

в множестве из $N-u+1$ неизвестных элементов, добавляя найденные $u-1$ элементов к каждому тесту.

Применим эту идею для поиска всех дефектных элементов, используя следующий хорошо известный результат:

$$n_{(\mathrm{Cla})}(N, D, D) \leq \left\lceil \log \binom{N}{D} \right\rceil + D - 1.$$

Действуем следующим образом. После $u-1$ раундов тестирования применяем этот результат для обнаружения среди оставшихся $N-u+1$ элементов $D-u+1$ дефектных, получая таким образом всего

$$T(u) = (u-1)\lceil \log(N-D+1) \rceil + \left\lceil \log \binom{N-u+1}{D-u+1} \right\rceil + D - u + 1$$

тестов. Получаем следующую оценку сверху.

Справедливо неравенство

$$n_{(\mathrm{Thr})}(N, D, u) \leq T(u).$$

Если D неизвестно, можно провести один тест на всех элементах. Если ответ будет отрицательным, никакой дефектный элемент найти невозможно. Если ответ будет положительным, то мы знаем, что $D \geq u$.

Тем самым, нас интересует случай, когда D неизвестно, но $u \leq D \leq N$.

Для неизвестного D обозначим через $n_{(\mathrm{Thr})}(N, u, m)$ минимальное число тестов, необходимых для определения m дефектных объектов в наихудшем случае, если имеется N элементов и $f(|\mathcal{D}|, |\mathcal{S}|) = u$ для всех значений. Тогда имеет место следующая оценка.

Справедливо неравенство

$$n_{(\mathrm{Thr})}(N, u, m) \leq m\lceil \log(N-u+1) \rceil.$$

Опишем стратегию, состоящую из $m\lceil\log(N-u+1)\rceil$ тестов. Используем m адаптивных раундов, начиная с тестового множества

$$\mathcal{S}_1 = \left\{1, \ldots, u-1, u, \ldots, (u-1) + \left\lceil \frac{m(1)}{2}(N-u+1) \right\rceil \right\},$$

где $m(1) = 1$.

Для $j \leq \lceil\log(N-u+1)\rceil$ полагаем

$$m(j) = \begin{cases} 2m(j-1) - 1, & \text{если } t_{S_{j-1}}(\mathcal{D}) = 1, \\ 2m(j-1) + 1, & \text{если } t_{S_{j-1}}(\mathcal{D}) = 0, \end{cases}$$

и

$$\mathcal{S}_j = \left\{1, \ldots, u-1, u, \ldots, (u-1) + \left\lceil \frac{m(j)}{2^j}(N-u+1) \right\rceil \right\}.$$

Вначале, за $\lceil\log(N-u+1)\rceil$ тестов определяем один дефектный элемент d_1. Затем вместо множества $\{1, 2, \ldots, N\}$ используем множество $\{\pi_1, \pi_2, \ldots, \pi_N\}$, где

$$\pi_j = \begin{cases} d_1, & \text{если } j = 1, \\ 1, & \text{если } j = d_1, \\ j, & \text{если } j \notin \{1, d_1\}, \end{cases}$$

и, действуя аналогично, за $\lceil\log(N-u+1)\rceil$ тестов определяем дефектный элемент d_2 в новом множестве $\{\pi_1, \pi_2, \ldots, \pi_N\}$. Повторяем эту процедуру, пока не найдем $u-1$ дефектных элементов. Тогда мы знаем, что в множестве $[u, N]$ содержатся оставшиеся $D-u+1$ дефектных элементов. Их можно найти за $m-u+1$ раундов, используя $\lceil\log(N-u+1)\rceil$ тестов.

2.5 Тестирование с плотностью

Пусть $n_{(\mathrm{Den})}(N, D, m, \alpha)$ – минимальное число тестов density, требуемое для определения m дефектных элементов, если имеется N элементов, D из которых дефектны. В [140] получены следующие оценки на $n_{(\mathrm{Den})}(N, D, m, \alpha)$ в предположении, что $D \geq \alpha N$:

$$\lceil \log N \rceil + \max_{N' \leq 2m/\alpha} n_{(\mathrm{Den})}(N', m, m, \alpha) \geq n_{(\mathrm{Den})}(N, D, m, \alpha), \tag{59}$$

$$\lceil \log N \rceil \geq n_{(\mathrm{Den})}(N, D, 1, \alpha). \tag{60}$$

Там же показано, что в общем случае

$$\log(N - D + 1) \leq n_{(\mathrm{Den})}(N, D, 1, \alpha). \tag{61}$$

Модель тестирования (57) дает те же результаты, что и модель (52), если размер тестового множества меньше, чем $1/\alpha$. В стратегии, приведенной в доказательстве предложения 1, наибольшее тестовое множество $\mathcal{S}_0$ имеет мощность $\left\lfloor \frac{N-D+1}{2} \right\rfloor$. Если в модели density мощность $|S_0|$ меньше, чем $1/\alpha$, то применяя эту стратегию, получаем

$$n_{(\mathrm{Den})}(N, D, 1, \alpha) \leq \lfloor \log(N - D + 1) \rfloor.$$

Эта ситуация имеет место, когда $D \geq N + 1 - \frac{2}{\alpha}$. Таким образом, получаем

Утверждение 22. Пусть $D \geq N + 1 - \frac{2}{\alpha}$. Тогда справедливо равенство

$$n_{(\mathrm{Den})}(N, D, 1, \alpha) = \lceil \log(N - D + 1) \rceil.$$

Покажем, как можно улучшить этот результат. Опишем стратегию, оптимальную при $D \geq \alpha N$ (она требует $\lceil \log(N - D + 1) \rceil$ тестов).

Положим

$$s_i = \left\lceil \frac{2^{n-i} - 1}{1 - \alpha} \right\rceil,$$

где $i = 1, 2, \ldots, n-1$ и $s_n = 1$. Для заданного D выберем наибольшее n, при котором

$$D > \sum_{i=1}^{n} s_i - 2^n + 1. \tag{62}$$

Рассмотрим тестовые множества

$$\mathcal{S}_i = \{a_i + 1, a_i + 2, \ldots, a_i + s_i\}$$

для $i = 1, \ldots, n$, где $a_1 = 0$ и

$$a_i = \begin{cases} a_{i-1} + s_{i-1}, & \text{если } t_{S_{i-1}}(\mathcal{D}) = 0, \\ a_{i-1}, & \text{если } t_{S_{i-1}}(\mathcal{D}) = 1. \end{cases} \tag{63}$$

Заметим, что $|S_i| = s_i$.

Утверждение 23. Если $t_{S_{n-j}}(\mathcal{D}) = 1$, то один дефектный элемент можно найти за n тестов.

Доказательство.

Используем индукцию по j. Случай $j = 0$ очевиден. Рассмотрим также случай $j = 1$ (для пояснения идеи стратегии). Имеем $s_{n-1} = \left\lceil \frac{1}{1-\alpha} \right\rceil$ и $t_{S_{n-1}}(\mathcal{D}) = 1$. Тогда

$$s_{n-1} - 2 < \alpha s_{n-1} \leq s_{n-1} - 1.$$

Таким образом, в множестве S_{n-1} содержится не более одного недефектного элемента. Если $t_{S_n}(\mathcal{D}) = 1$, то найден дефектный элемент; в противном случае (т.е. если $t_{S_n}(\mathcal{D}) = 0$) можно взять любой элемент из $S_n \setminus S_{n-1}$.

Итак, предположим, что для $j-1$ утверждение доказано. Положим $t_{S_{n-j}}(\mathcal{D}) = 1$, тогда по предположению индукции можно считать, что $t_{S_{n-i}}(\mathcal{D}) = 0$ для всех i, $0 \le i < j$.

Таким образом, число недефектных элементов в S_{n-j} не больше $2^j - 1$, поскольку $t_{S_{n-i}}(\mathcal{D}) = 1$ и

$$s_{n-j} - 2^j < \alpha s_{n-j} \le s_{n-j} - 2^j + 1.$$

С другой стороны, число недефектных элементов в S_{n-i} при всех $0 \le i < j$ больше или равно 2^i, поскольку $t_{S_{n-i}}(\mathcal{D}) = 0$. Таким образом, все элементы в $S_{n-j} \setminus \bigcup\limits_{i<j} S_{n-i}$ дефектные.

Множество $S_{n-j} \setminus \bigcup\limits_{i<j} S_{n-i}$ непусто, поскольку для любых k и α, $0 < \alpha < 1$, справедливо

$$1+\sum_{i=1}^{k} \left\lceil \frac{2^i - 1}{1-\alpha} \right\rceil < 1+k+\sum_{i=1}^{k} \frac{2^i - 1}{1-\alpha} = 1+k+\frac{2^{k+1} - k - 2}{1-\alpha} < \frac{2^{k+1} - 1}{1-\alpha}.$$

Утверждение 24. Пусть выполнено условие , и пусть $N \le 2^n + D - 1$. Тогда за n тестов описанной стратегии один дефектный элемент будет найден.

Доказательство. Рассмотрим тестовые множества, заданные в (63). Если для некоторого i выполняется $t_{S_i}(\mathcal{D}) = 1$, то утверждение теоремы следует из леммы. Если $t_{S_i}(\mathcal{D}) = 0$ для всех $i = 1, 2, \ldots, n$, обозначим через c_i число недефектных элементов в S_i. Число дефектных элементов в S_i равно $s_i - c_i$. Тогда получаем $s_i - c_i < \alpha s_i$, и значит, $c_i \ge 2^i$.

Общее число недефектных элементов не менее $2^n - 1$, и, поскольку

$$N - D = 2^n - 1,$$

то можно взять любой элемент множества $[N] \setminus \bigcup_{t=1}^{n} S_t$. Заметим, что если

$$N < 2^n + D - 1,$$

то найдется i, такое что $t_{S_i}(\mathcal{D}) = 1$.

Следствие 10. Если $D \geq \alpha N$, то

$$n_{(\mathrm{Den})}(N, D, 1) = \lceil \log(N - D + 1) \rceil.$$

Доказательство. Имеем

$$D > \sum_{k=0}^{n-1} \left(\left\lceil \frac{2^k - 1}{1 - \alpha} \right\rceil - 2^k \right).$$

Заметим, что

$$n - 1 + \sum_{k=1}^{n-1} \left(\frac{2^k - 1}{1 - \alpha} - 2^k \right) = \frac{\alpha}{1 - \alpha}(2^n - n - 1).$$

Если взять

$$D > \frac{\alpha}{1 - \alpha}(2^n - n - 1)$$

и

$$N < 2^n + \frac{\alpha}{1 - \alpha}(2^n - n - 1) - 1,$$

то

$$\frac{N}{D} < \frac{1 - \alpha}{\alpha} + 1 + \frac{(1 - \alpha)n}{\alpha(2^n - n - 1)}.$$

Таким образом, если $D \geq \alpha N$, то можно применить результаты, полученные выше.

2.6 Выводы

Основным результатом данной главы является Теорема 3. Она показывает, что предложенный алгоритм поиска двух дефектных элементов позволяет получить формулу для общего числа элементов, среди которых можно найти два дефектных. Из данной формулы вытекает, что константа при главном члене асимптотики для общего числа элементов является оптимальной.

Также решается задача поиска одного из нескольких дефектов для разных случаев модели тестирования.

Основные результаты главы опубликованы в работах [1], [2].

3 Коды, свободные от (w, r) перекрытий.

3.1 Основные определения и обозначения

Начнем эту главу с определения кодов, свободных от (w, r) перекрытий, которые в англоязычной литературе известны как superimposed codes или cover-free families, а в русскоязычной литературе также встречаются как (w, r) дизъюнктивные коды.

Определение 4. *Двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется кодом, свободным от (w, r) перекрытий, если для любой пары непересекающихся подмножеств $J_1, J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует координата $i \in [N]$ такая, что $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$.*

Данное определение эквивалентно определению, использующее матрицы инциндентности семейства множеств. Предположим, что имеются N элементов. Любому подмножеству этих элементов поставим в соответствие двоичный вектор c длинны N естественным образом: если i-ый элемент принадлежит данному подмножеству, то $c_i = 1$.

Тогда кодом, свободным от (w, r) перекрытий, называется семейство подмножеств $\mathcal{A} = \{A_1, \ldots, A_T\}$ множества $[N] = \{1, 2, \ldots, N\}$, если для любых I, J подмножеств $[T] = \{1, 2, \ldots, T\}$, таких что $|I| = w,\ |J| = r$ и $I \cap J = \mathcal{O}$, выполняется условие

$$\bigcap_{i \in I} A_i \nsubseteq \bigcup_{j \in J} A_j.$$

Приведем пример кода, свободного от $(2, 2)$ перекрытий.

Предположим, что мы хотим найти минимальное множество дво-

ичных строк длины 8, обладающих тем свойством, что проекция набора таких строк на любые четыре координаты i_1, i_2, i_3, i_4 обязательно содержит подвектор длинны 4 с 1 в координатах i_1, i_2 и 0 в координатах i_3, i_4. Как много строк нам придется взять? Ответ: 14 строк. В качестве примера такого множества векторов можно взять слова веса 4 из расширенного кода Хэмминга:

1 1 0 1 0 0 0 1
0 1 1 0 1 0 0 1
0 0 1 1 0 1 0 1
0 0 0 1 1 0 1 1
1 0 0 0 1 1 0 1
0 1 0 0 0 1 1 1
1 0 1 0 0 0 1 1
1 1 1 0 0 1 0 0
0 1 1 1 0 0 1 0
1 0 1 1 1 0 0 0
0 1 0 1 1 1 0 0
0 0 1 0 1 1 1 0
1 0 0 1 0 1 1 0
1 1 0 0 1 0 1 0

Ниже мы докажем, что никакое множество из 13 векторов длины 8 указанным свойством обладать не может. Таким образом, приведенная двоичная матрица является решением поставленной задачи. Более того, чуть позже будет приведено доказательство того, что это решение единственное с точностью до перестановки строк и столбцов матрицы.

Мы часто будем называть столбцы матрицы C кодовыми словами

и будем использовать словосочетание код размера $N \times T$, вместо более распространенного в теории кодирования – код длины N и мощности T. Отметим, что коды, свободные от (w, r) перекрытий, существуют только при выполнении условия $T \geq w + r$.

Еще раз отметим, что основной задачей для кодов, свободных от (w, r) перекрытий, является нахождение максимального числа столбцов $T(N, w, r)$ для данного числа строк N, или минимального числа строк $N(T, w, r)$ для заданного числа столбцов T. Для случая $w = r = 1$ задача нахождения точного значения величины $T(N, w, r)$ полностью решена: $T(N, 1, 1) = \binom{N}{\lfloor N/2 \rfloor}$ (теорема Шпернера). В общем случае известны лишь несколько примеров оптимальных кодов, свободных от (w, r) перекрытий, (см. [151]) и различные оценки величины $N(T, w, r)$ для больших T (см. [128], [133], [170]). В частности, $N(8, 2, 2) = 14$, что иллюстрирует приведенный выше пример. В следующем параграфе мы будем изучать поведение величины $N(T, w, r)$ при $r \geq w \geq 2$ и при малых значениях T.

3.2 Конструкции кодов, свободных от (w, r) перекрытий

Понятие супер-простой блок схемы было впервые введено в работе [42]

Приведем два определения из этой работы:

Тактическую конфигурацию $T(n, w, l, \alpha)$ определим как матрицу из элементов 0 и 1, строки которой имеют длину n, каждая строка содержит точно w единиц и любой возможный на длине l набор единиц встречается точно в α строках.

Назовем кодом $A(n, w, \lambda, l, \alpha)$ такую $T(n, w, l, \alpha)$, в которой любой возможный на длине n набор $\lambda + 1 \geq l$ единиц встречается не более чем в одной строке. В таком коде максимальная корреляция любой пары строк (максимальная величина их скалярного произведения) равна λ, а минимальное расстояние Хэмминга $d = 2(w - \lambda)$.

К сожалению, данные обозначения не прижились и, поэтому переформулируем приведенное выше определение t-(v, k, λ) супер-простой блок схемы, как блок схемы, у которой пересечение любых двух ее блоков содержит не более t элементов.

В работе [42] было доказано, что кодовые слова веса 6 кода Препараты на длине $n = 4^m$,$m = 2, 3, \cdots$, с минимальным кодовым расстоянием d=6 образуют $3 - (4^m, 6, (4^m - 4)/3)$ супер-простую блок схему.

Мы рассматриваем супер-простые блок схемы, поскольку из них получаются нужные нам коды. Справедлива следующая теорема.

Теорема 5. *Супер-простая* t-(v, k, λ) *блок схема является кодом, свободным от* $(t, \lambda - 1)$ *перекрытий, размера* $N \times v$, *где* $N = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}$

Рассмотрим любые t -точки $p_1, p_2, \ldots, p_t$. Имеется точно λ блоков, которые содержат эти точки, т.е. $|S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t}| = \lambda$. Рассмотрим любые другие r точки $h_1, h_2, \ldots, h_r$, $r = \lambda - 1$. Поскольку для двух (или более) блоков супер-простой t блок схемы они не могут иметь более t общих точек, для любого l с $1 \leqslant l \leqslant r$, имеем

$$|S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t} \bigcap S_{h_l}| \leq 1.$$

Таким образом,

$$|S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t} \bigcap \{ \bigcup_{l=1,\ldots,r} S_{h_l} \}| \leq r < \lambda.$$

$$S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t} \subseteq \bigcup_{l=1,\ldots,r} S_{h_l},$$

$$|S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t} \bigcap \{ \bigcup_{l=1,\ldots,r} S_{h_l} \}| = |S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t}| = \lambda.$$

Следовательно, имеем

$$S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_t} \nsubseteq \bigcup_{l=1,\ldots,r} S_{h_l}.$$

Это и доказывает теорему.

Отметим, что в статьях [161], [170] был доказан следующий результат:

Утверждение 25. $(t+1)-(v,k,1)$ *блок схема является кодом, свободным от* (w,r) *перекрытий размера* $N \times v$, *где*

$$w = t, N = \frac{\binom{v}{t+1}}{\binom{k}{t+1}} = \frac{(v-t)\binom{v}{t}}{(k-t)\binom{k}{t}} \ u \ r < \frac{v-t}{k-t}.$$

Известно, что $3-(Q^2+1, Q+1, 1)$ блок схемы существуют, когда Q является степенью простого. Следовательно для таких Q существуют $(2,Q)$ коды размера $Q(Q^2+1) \times (Q^2+1)$, в частности, существует $(2,3)$ код размера 30×10. Чуть позже мы докажем оптимальность этого кода, т.е. то, что $N(10,2,3) = 30$.

Хорошо известно, что кодовые слова веса 4 расширенного кода Хэмминга $[8,4,4]$ образуют $3-(8,4,1)$ блок схему. Таким образом, другим способом доказано существование кода, свободного от $(2,2)$

перекрытий, размера 14×8, который ранее строился довольно хитрым способом. Чуть позже мы также докажем оптимальность этого кода, и более того, докажем его единственность с точностью до перестановок строк и столбцов матрицы.

Легко видеть, что всякая (t+1)-$(v, k, 1)$ блок схема (такую блок схему еще называют системой Штейнера) является супер-простой t-$(v, k, (v-t)/(k-t))$ блок схемой и, следовательно, в этом случае теорема 5 эквивалентна утверждению, приведенному выше.

Таким образом, для получения новых результатов мы будем интересоваться супер-простыми блок схемами, которые не получаются из систем Штейнера. Известно, что существуют 2-$(v, 4, 3)$ супер-простые блок схемы тогда и только тогда, когда $v \equiv 0$ или $1 \pmod 4$ при $v \geq 8$ и существуют 2-$(v, 4, 4)$ супер-простые блок схемы тогда и только тогда, когда $v \equiv 1 \pmod 3$ при $v \geq 10$. Следовательно, получаем

Следствие 11. *Существует код, свободный от* $(2, 2)$ *перекрытий, размера* 18×9.

Позже мы докажем, что данный код будет оптимальным, то есть $N(9, 2, 2) = 18$.

Утверждение 26. *Пусть* C *является* (n, M, d) *кодом. Предположим, что кодовые слова веса* w *в коде* C *образуют* $t - (n, w, \lambda)$ *блок схему с* $\lambda > 1$. *Если*

$$w = t + \lceil d/2 \rceil,$$

то тогда данная блок схема является супер-простой блок схемой.

Доказательство. Для двоичного вектора c длинны n, мы отождествим вектор c с его носителем и рассмотрим c как подмножество

множества $[n]$. Пусть c_1 и c_2 являются двумя различными словами кода C вес которых равен w и пусть x это число элементов в $c_1 \cap c_2$. Тогда справедливо равенство

$$d(c_1, c_2) = 2w - 2x = 2t + 2\lceil d/2 \rceil - 2x.$$

Если $x \geq t + 1$, тогда из этого сразу же следует, что $d(c_1, c_2) < d$- противоречие.

Следствие 12. *Кодовые слова веса* 6 *расширенного кода БЧХ для* $n = 2^{2s+1}$, $s = 2, 3, \cdots$ *и* $d = 6$ *образуют* $3 - (2^{2s+1}, 6, (4^s - 4)/3)$ *супер простую блок схему.*

Размеры кодов, свободных от $(2, 2)$ перекрытий, с $v \geq 12$, получающихся из 2-$(v, 4, 3)$ супер-простой блок схемы могут быть улучшены с помощью следующей конструкции.

Нам понадобятся 3-покрывающие матрицы.

Определение 5. *t-покрывающая матрица над алфавитом q, длинны n размера k состоит из k q-ичных векторов длинны n, обладающих свойством, что проекция на любые t координат содержит все q^t возможных подвекторов.*

Обозначим через $g_3(n)$ минимальный размер двоичной 3-покрывающей матрицы длинны n. Таблицы известных значений $g_3(n)$ можно найти в статьях

Утверждение 27. *Для кодов, свободных от* $(2, 2)$ *перекрытий, имеем*

$$N(2T, 2, 2) \leq N(T, 2, 2) + g_3(T).$$

Доказательство. Пусть матрица A является матрицей кода, свободного от $(2, 2)$- перекрытий, размера $N \times T$ и B является мат-

рицей двоичной 3-покрывающей матрицей длины T. Тогда, легко проверить, что матрица

$$\begin{array}{|cc|}\hline A & A \\ B & \bar{B} \\ \hline\end{array}$$

является матрицей кода, свободного от $(2,2)$ перекрытий, (верхнее подчеркивание означает, что это матрица в которой нули заменяются на единицы, и наоборот, единицы меняются на нули).

Замечание 9. Конструкции, использующие похожие идеи, рассматривались в для построения 3-покрывающих матриц и в для построения кодов, свободных от $(2,2)$ перекрытий. Однако конструкции из более ранних статей дают худший результат по сравнению с теоремой 2. Более того, в статье G. Mago, "Monotone Function in Sequential Circuits" 1973 года допущена ошибка в первом шаге конструкции: не существует полностью разделяющего $(1,2)$ кода размера 4×4 и, следовательно, приведенные в этой статье таблицы содержат ошибки (в частности не существует кода, свободного от $(2,2)$ перекрытий, размера 12×8)!

Приведем таблицы для размеров некоторых кодов, свободных от $(2,2)$ перекрытий.

$T =$	4	5	6	7	8	9
$N(T,2,2) =$	6	10	14	14	14	18

$T =$	10	12	16	18	20	22	24	28	32	36	40	44	48
$N(T,2,2) \leq$	20	22	26	30	32	34	37	42	43	48	50	53	59

$T =$	72	80	88	112	128	144	512
$N(T,2,2) \leq$	74	76	80	96	100	109	126

Рассмотрим теперь коды, свободные от $(2,3)$ перекрытий.

Утверждение 27. *Существуют коды, свободные от* $(2,3)$ *перекрытий, размера* 48×16*,* 45×12*,* 56×21*, and* 76×24*.*

Данное утверждение следует из существования $3-(17,5,1)$, $3-(14,4,1)$, $3-(22,6,1)$, $3-(26,6,1)$ дизайнов и простых соображений, позволяющих из кодов, свободных от (w,r) перекрытий, строить подкоды, свободные от $(w-1,r)$ перекрытий, от $(w,r-1)$ перекрытий и от $(w-1,r-1)$ перекрытий. Для этого ищется столбец с минимальным числом нулей (минимальным числом единиц), либо два столбца, дающих минимальное расстояние в коде и рассматривается соответственное этим позициям множество строк.

Пример 2. Кодовые слова веса 6 в коде Нордстрема-Робинсона образуют код, свободный от а (3,3) перекрытий, размера 112×16.

Из этого кода можно получить $(2,3)$ код размера 42×15. Таким образом $N(15,2,3) \leq 42$.

Пример 3. Кодовые слова веса 6 кода препарата длинны $n = 64$ с минимальным расстоянием d=6 образуют $(3,19)$ код размера $\binom{64}{3} \times 64$.

Пример 4. Кодовые слова веса 6 расширенного кода БЧХ длинны $n = 128$ с $d = 6$ образуют $(3,19)$ код размера $\binom{128}{3} \times 128$.

Занесем результаты о размерах кодов, свободных от $(3,6)$ перекрытий, в следующую таблицу.

Таблица. Существование некоторых $(3,6)$ кодов.

T	17	20	26	32	51	361
$N(T,3,6) \leq$	680	816	910	4683	10008	15504
Comments	trivial	S(4,5,23)	S(4,6,27)	S(4,5,47)	Table 1	con.cst.

В следующих таблицах мы приводим размеры некоторых кодов, свободных от $(3, r)$ перекрытий,

Таблица. Существование некоторых $(3, r)$ кодов.

(w,r)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)	(3,10)	(3,11)
T	50	51	52	53	54	55	56
$N(T, 3, r) \leq$	8830	10008	11313	12757	14352	16109	18043

(w,r)	(3,12)	(3,13)	(3,14)	(3,15)	(3,16)	(3,17)	(3,18)
T	57	58	59	60	61	62	63
$N(T, 3, r) \leq$	20165	22492	25038	27821	30856	34162	37758

Таблица. Некоторые $(3, r)$ коды.

(w,r)	(3,11)	(3,12)	(3,13)	(3,14)	(3,15)	(3,16)
T	120	121	122	123	124	125
$N(T, 3, r) \leq$	229913	241909	254421	267468	281068	295240

Докажем теперь оптимальность некоторых из построенных кодов.

3.3 Оптимальность некоторых кодов, свободных от перекрытий

Теорема 6. *Для кодов, свободных от* (w, r) *перекрытий, имеем*

$$N(8, 2, 2) = 14.$$

$$N(9, 2, 2) = 18.$$

$$N(10, 2, 3) = 30.$$

$$N(11,3,3) = 66.$$

Доказательство основано на применении следующей Леммы, являющейся естественным обобщением идеи, используемой в [87].

Лемма 6. *Пусть имеется код C, свободный от (w,r) перекрытий, размера $N \times T$. Тогда существует $(w-1, r-1)$ код размера $[d/2] \times (T-2)$, где d это минимальное расстояние кода C.*

Доказательство. Рассмотрим код C. Без ограничение общности предположим, что первые два столбца c^1, c^2 образуют пару кодовых слов, расстояние между которыми равно $d(c^1, c^2) = d$. Предположим, что

$$|\{i : c_i^1 = 1; c_i^2 = 0\}| \leq |\{i : c_i^1 = 0; c_i^2 = 1\}|.$$

Пусть

$$U_C = \{i : c_i^1 = 1; c_i^2 = 0\}.$$

Таким образом, $|U_C| \leq d/2$ (иначе можно просто перенумеровать первые два столбца).

Рассмотрим подматрицу C_1 из C, состоящие из i-ых строк C, где i берется из множества индексов U_C. Мы утверждаем, что $C_1 \setminus \{c^1; c^2\}$, полученные из подкода C_1 путем удаления первых двух столбцов, образует код, свободный от $(w-1, r-1)$ перекрытий, размера $|U_C| \times (T-2)$. Рассмотрим произвольные подмножества X, Y из $\{3, 4, \ldots, T\}$, такие что $|X| = w-1$, $|Y| = r-1$, и $X \cap Y = \mathcal{O}$. Положим $\tilde{X} = X \cup \{1\}$ и $\tilde{Y} = Y \cup \{2\}$. Из того, что код C япляется свободным от перекрытий, мы можем найти координату i, такую что $c_{ij} = 1$ для $j \in \tilde{X}$ и $c_{ij} = 0$ для $j \in \tilde{Y}$. Поскольку $c_{i1} = 1$ и $c_{i2} = 0$, мы имеем $i \in U_C$. Заметим, что для этого i, выполняется $c_{ij} = 1$ для

$j \in X$ и $c_{ij} = 0$ для $j \in Y$. Это и доказывает лемму.

Также полезно следующее утверждение, когда известно, что вес кодовых строк одинаков.

Утверждение 28. *Предположим, что имеется код, свободный от (w,r) перекрытий, размера $N \times T$ в котором все строки имеют вес k. Тогда для любых целых положительных x, y таких, что $1 \leq x < w, 1 \leq y < r$, имеем*

$$N(T-x-y, w-x, r-y) \leq N \frac{\binom{k}{x}\binom{T-k}{y}}{\binom{T}{x}\binom{T-x}{y}}.$$

Доказательство. Пусть C код, свободный от (w,r) перекрытий, размера $N \times T$. Рассмотрим множество Ω троек (I, J, α), где $I (resp.\ J)$ подмножество $[T]$, такое, что $|I| = x$ $(resp.\ |J| = y)$, и α является элементом $[N]$ так, что $c_{\alpha i} = 1$ для $i \in I$ и $c_{\alpha j} = 0$ для $j \in J$. Подсчитаем число элементов из Ω двумя способами.

Для каждой фиксированной пары (I, J), из определения $N(T, w, r)$ следует то, что существует как минимум $N(T-x-y, w-x, r-y)$ значений $\alpha' s$ таких, что $(I, J, \alpha) \in \Omega$. Поскольку число пар (I, J) равно $\binom{T}{x}\binom{T-x}{y}$, получаем, что число таких троек

$$N(T-x-y, w-x, r-y)\binom{T}{x}\binom{T-x}{y} \leq |\Omega|.$$

С другой стороны, для любой строки в кодовой матрице C, существует $\binom{k}{x}\binom{T-k}{y}$ возможностей для (I, J). Поскольку код имеет N строк, получаем, что число троек равно

$$|\Omega| = N\binom{k}{x}\binom{T-k}{y}.$$

Это доказывает утверждение.

Доказательство теоремы. Докажем сначала, что $N(9,2,3) \geq 26$. Обозначим через

$$d(N,T) = \max_{|C|=T} d(C)$$

максимальное возможное кодовое расстояние кода размера N на T. Граница Плоткина, хорошо известная в теории кодирования, утверждает, что

$$N \geq \begin{cases} 2d(T-1)/T & \text{T=2z} \\ 2dT/(T+1) & \text{T=2z+1.} \end{cases}$$

Из Леммы 6 вытекает, что $[d/2]$ не меньше, чем $N(T-2, w-1, r-1)$. Хорошо известно, что $N(7,1,2) = 7$. Следовательно $d \geq 14$, и, поэтому, $N \geq 26$.

Аналогичным образом доказываются остальные утверждения теоремы.

3.4 Единственность некоторых кодов, свободных от перекрытий.

Мы докажем, что некоторые оптимальные коды, рассмотренные выше, являются единственными с точностью до перестановки строк и столбцов.

Будем говорить, что два кода C и C' эквивалентны друг другу, если один может быть получен из другого с помощью серии перестановок строк и столбцов.

Теорема 7. *Код, свободный от* $(1,2)$ *перекрытий, размера* 9×12, *код свободный от* $(2,2)$ *перекрытий, размера* 14×8, *свободный от*

$(2,3)$ *перекрытий, размера* 30×10 *являются единственными.*

Докажем, что двоичная матрица C является кодом, свободным от $(1,2)$ перекрытий, размера 9×12 тогда и только тогда, когда она эквивалентна матрице инциндентности $2-(9,3,1)$ блок схемы.

Предположим, что двоичная матрица C эквивалентна матрице инциндентности $2-(9,3,1)$ блок схемы. Тогда хорошо известно ([128], [136]), что C является кодом, свободным от $(1,2)$ перекрытий. Действительно, поскольку столбцы веса три пересекаются не более, чем по одной единице, то два столбца никак не могут покрыть третий.

Значит, надо доказать обратное утверждение. Поскольку $N(11;1,1) = 6$ и $N(9;1,2) = 9$, мы имеем, что $|S_p| \leqq 3$ для всех $p \in \{1,2,\cdots,12\}$ и $|L_x| \geqq 4$ для всех $x \in \{1,2,\cdots,9\}$, соответственно, где S_p это столбец, а L_x это строка кодовой матрицы. Подсчитывая число 1 в C по строкам и столбцам, получаем, что $|S_p| = 3$ для всех $p \in \{1,2,\cdots,12\}$ и $|L_x| = 4$ для всех $x \in \{1,2,\cdots,9\}$. Предположим, что $|S_{p_1} \cap S_{p_2}| \geqq 2$ для некоторых p_1, p_2. Поскольку C является (1,2) кодом, и $|S_{p_i}| = 3$, должна быть строка x такая, что $L_x = \{p\}$, что приводит к противоречию. Следовательно, $|S_{p_1} \cap S_{p_2}| \leqq 1$ для любых p_1, p_2 in $\{1,2,\cdots,12\}$. Это доказывает, что C является матрицей инциндентности $1-(12,4,3)$ блок схемы.

Для доказательства того, что C является матрицей инциндентности $2-(9,3,1)$ блок схемы достаточно показать, что $|L_x \cap L_y| = 1$ для любых x, y из $\{1,2,\cdots,9\}$. Поскольку $|S_p| = 3$ для любого $p \in \{1,2,\cdots,12\}$ число единиц в C равно 72. С другой стороны, поскольку $|S_{p_1} \cap S_{p_2}| \leq 1$ для всех $p_1 \neq p_2$, существует не более одного p так, что $c_{xp} = c_{yp} = 1$ для каждой пары (x,y) из $\{1,2,\cdots,9\}$. Следовательно, число $\binom{1}{1}$ в C не более, чем 72, причем равенство воз-

можно только когда $|L_x \cap L_y| = 1$ для всех $x \neq y$. Это доказывает, что C является матрицей инцидентности $2-(9,3,1)$ блок схемы.

Из определения кода, свободного от (w,r) перекрытий, сразу вытекает, что для w точек $p_1, p_2, \ldots, p_w$ таких, что $|L_x| > w$ для $x \in S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_w}$ справедливо

$$|S_{p_1} \bigcap S_{p_2} \bigcap \cdots \bigcap S_{p_w}| \geq r+1.$$

Теперь докажем, что двоичная матрица C является $(2,2)$ кодом размера 14×8 тогда и только тогда, когда эта матрица является матрицей инцидентности $3-(8,4,1)$ блок схемы.

Уже было отмечено ранее, что $3-(8,4,1)$ блок схема является $2-(8,4,3)$ супер простым дизайном. Пусть C является матрицей $3-(8,4,1)$ блок схемы. Ранее было показано, что она является $(2,2)$ кодом размера 14×8.

Теперь, пусть C является $(2,2)$ кодом размера 14×8. Если $|L_x|=$ 2 или 3 для какого то $x \in \{1,2,\cdots 14\}$ тогда существует $(2,2)$ код размера 14×6 с $|L_x|$=0 или 1. Но тогда существует $(2,2)$ код размера 13×6, чего не может быть. Аналогично мы можем доказать, что нет такого $x \in \{1,2,\cdots,14\}$ так, что $|L_x|$=5 или 6. Значит $L_x = 4$ для всех $x \in \{1,2,\ldots 14\}$. Значит $|S_{p_1} \bigcap S_{p_2}| \geq 3$ для любых p_1, p_2 из $\{1,2,\cdots,8\}$. Подсчитаем число подматриц $(1,1)'s$ в C и получим $|S_{p_1} \bigcap S_{p_2}| = 3$ для любых p_1, p_2. Это доказывает, что C является $2-(8,4,3)$ блок схемой. Теперь предположим, что существуют три точки p_1, p_2 и p_3 так, что $|S_{p_1} \bigcap S_{p_2} \bigcap S_{p_3}| \geq 2$. Тогда существует не более одной строки x которая содержит p_1, p_2 и не содержит p_3. Пусть p_4 какая то другая точка, отличная от p_1, p_2, p_3, которая содержится в x. Не найдется строки y такой, что $c_{yp_1} = c_{yp_2} = 1$ и $c_{yp_3} = c_{yp_4} =$

0, что приводит к противоречию. Это доказывает, что C является $2-(8,4,3)$ супер простым дизайном, следовательно, $3-(8,4,1)$ блок схемой.

И, наконец, докажем, что двоичная матрица C является $(2,3)$ кодом размера 30×10 тогда и только тогда, когда она инцидентна матрице $3-(10,4,1)$ блок схемы.

Ранее мы отмечали, что матрица $3-(10,4,1)$ образует $(2,3)$ код размера 30×10 и было доказано, что этот код оптимален.

Пусть теперь C является $(2,3)$ кодом размера 30×10. Поскольку $N(9;2,2) = 18$ и $N(9;1,3) = 9$, получаем $9 \leq |S_p| \leq 12$ для всех $p \in \{1,2,\cdots,10\}$. Из граничы Плоткина и того, что $N(8;1,2) = 8$ следует $d(C) = 16$. Значит $|S_{p_1} \cap S_{p_2}| \leq 4$ для любых двух точек p_1 и p_2.

Пусть A_i это число строк матрицы C веса i, т.е. $A_i = |\{x \mid |L_x| = i\}|$. Подсчитав число подматриц $(1,1)$ и $(1,0)$ в матрице C, получим следующие соотношения

$$A_2 + A_3 + \cdots + A_7 = 30 \tag{64}$$

$$\sum_{i=2}^{7} A_i \cdot \binom{i}{2} \leq 180. \tag{65}$$

$$\sum_{i=2}^{7} A_i \cdot i(10-i) \geq 720. \tag{66}$$

Получаем, что

$$A_5 \geq 8A_2 + 3A_3 + 3A_7 \tag{67}$$

и

$$4A_5 + 9A_6 + 15A_7 \leq 5A_2 + 3A_3 \tag{68}$$

Значит

$$27A_2 + 9A_3 + 9A_6 + 27A_7 \leq 0 \tag{69}$$

Значит $A_3 = A_2 = A_6 = A_7 = 0$. Следовательно, $A_5 = 0$ и $A_4 = 30$. Это доказывает то, что $|L_x| = 4$ для всех $x \in \{1, 2, \cdots, 30\}$. Подсчитав число 1 в матрице C мы получаем, что $|S_p| = 12$ для всех p. Следовательно, $|S_{p_1} \cap S_{p_2}| = 4$ для любых двух p_1 и p_2. Это доказывает, что C является $2 - (10, 4, 4)$ блок схемой. С помощью аналогичных аргументов приведенным ранее доказывается, что C будет $2 - (10, 4, 4)$ супер простой блок схемой, и, следовательно, $3 - (10, 4, 1)$ блок схемой.

Хорошо известно, что 2-(9,3,1), 3-(8,4,1) и 3-(10,4,1) блок схемы единственны. Следовательно, теорема 7 доказана.

3.5 Асимптотические границы для скорости кодов

Напомним, что для кода C размера $N \times T$, его скорость $R(C)$ определяется как $\frac{\log_2 T}{N}$.

Определение 6. Для целых положительных w и r, величина

$$R(w, r) = \lim_{T \to \infty} \frac{\log_2 T}{N(T; w, r)}$$

называется *асимптотической скоростью* (w, r) кода.

Опишем сначала каскадную конструкцию, которая использовалась для конструкции кодов, свободных от перекрытий. Данная конструкция хорошо известна (см. [127], [171]). (отметим, что в теории кодирования идея каскадной конструкции часто применяется см., например, [49], [51], [54], [55], [57].)

Напомним, что код C над алфавитом $[q]$ называется *q-ичным (w, r) разделяющим кодом*, если для любой пары множеств $I,\ J \subset [T]$ таких, что $|I| = w$, $|J| = r$ и $I \cap J = \emptyset$, существует целое an $x \in [N]$ такое, что $\{c_{xi},\ i \in I\}$ и $\{c_{xj},\ j \in J\}$ не пересекаются.

Пусть B является (внешним) q-ым кодом размера $N_q \times T_q$ и пусть C является (внутренним) кодом размера $N_1 \times T_1$ с $T_1 = q$. Тогда можно построить каскадный код $B \diamond C$ размера $N \times T$, где $N = N_q N_1$ и $T = T_q$, т.е. каждый q-ичный элемент $\theta \in [q]$ в кодовой матрице внешнего кода B заменяется на θ-ое кодовое слово внутреннего кода C.

Дьячков и пр. получили следующий результат.

Утверждение 29. (каскадная конструкция) [127] *Пусть B является q-ичным (w, r) разделяющим кодом размера $N_q \times T_q$ и C является (w, r) кодом размера $N_1 \times T_1$ с $T_1 = q$. Тогда каскадный код $B \diamond C$ будет (w, r) кодом размера $N \times T$, где $N = N_q N_1$ и $T = T_q$.*

Утверждение 30. [127] *Пусть $w, r \geq 1$ и $\lambda \geq 1$ целые числа и $q \geq wr\lambda$ является степенью простого. Тогда*

$$N(q^{\lambda+1}; w, r) \leq N(q; w, r) wr\lambda + 1.$$

С помощью каскадной конструкции можно строить коды.

Для того, чтобы получить верхние границы, обобщим лемму, доказанную выше. Для этого нам понадобится ввести понятие обобщенного расстояния.

Следующая важная для нас величина будет определена для произвольного двоичного кода C размера $N \times T$. Эта величина характеризует свойства произвольного набора кодовых слов, и мы будем называть ее композиционным расстоянием для этого набора, исхо-

дя из того, что для набора из двух слов эта величина совпадает с расстоянием Хэмминга для этих кодовых слов.

Рассмотрим целые положительные x и y. Зафиксируем набор I, состоящий из $x+y$ кодовых слов, и обозначим подматрицу матрицы C, образованную этими кодовыми словами, через $C_{x,y}(I)$.

Таким образом, матрица $C_{x,y}(I)$ имеет размер $N \times (x+y)$. Назовем композиционным расстоянием для набора I число строк матрицы $C_{x,y}(I)$ веса x и обозначим это число через $d(C_{x,y}(I))$.

Другими словами, $d(C_{x,y}(I))$ равно числу строк i подматрицы $C_{x,y}(I)$ таких, что

$$\sum_{j=1}^{x+y} c_{ij} = x$$

Определение 7. *Минимальным композиционным расстоянием для двоичного кода C назовем величину $d_{x,y} = \min_{I=x+y} d(C_{x,y}(I))$.*

Обозначим через R_d скорость двоичного кода длины N с минимальным композиционным расстоянием $d_{x,y}$. Далее мы докажем верхние границы для скорости кода с минимальным композиционным расстоянием $d_{x,y}$, а затем покажем, как можно использовать эти границы для получения асимптотических верхних границ для скорости кодов, свободных от (w,r) перекрытий.

Рассмотрим двоичный код C размера $N \times T$. Зафиксируем целые положительные x, y.

Утверждение 31. *Для двоичного кода C длины N с минимальным композиционным расстоянием $d_{x,y}$ справедливо неравенство*

$$R(d_{x,y}) \leq 1 - \frac{(x+y)^{x+y} d_{x,y}}{x^x y^y \binom{x+y}{x} N}.$$

Лемма 7. *Если существует код C, свободный от (w, r) перекрытий, размера $N \times T$, то существует код, свободный от $(w-x, r-y)$ перекрытий, размера*

$$\frac{d_{x,y}}{\binom{x+y}{x}} \times (T - x - y).$$

Доказательство . Рассмотрим код C. Пусть $I(|I| = x + y)$ - набор номеров кодовых слов, на котором достигается минимальное композиционное расстояние $d_{x,y}$. Разобьем множество I на два подмножества I_1 и I_2 мощности x и y так, чтобы число позиций, в которых слова из первого подмножества принимают значение 1, а из второго 0, было минимальным. Обозначим множество таких позиций через I_3. Очевидно, что $I_3 \leq \frac{d_{x,y}}{\binom{x+y}{x}}$. Рассмотрим теперь подматрицу кода C, образованную строками из I_3 и столбцами из $[T] - \{I_1 \cup I_2\}$. Из определения кода следует, что эта подматрица является кодом, свободным от $(w - x, r - y)$ перекрытий, что и доказывает лемму.

Следствие 13. *Если существует код C, свободный от (w, r) перекрытий, с объемом T и минимальным композиционным расстоянием $d_{x,y}$, то для целых положительных x, y таких, что $x < w, y < r$ справедливо неравенство*

$$N(T - x - y, w - x, r - y) \leq \frac{d_{x,y}}{\binom{x+y}{x}}$$

Теорема 8. *Для скорости кодов, свободных от (w, r) перекрытий, справедлива асимптотическая границ*

$$R(w, r) \leq \min_{0<x<w} \min_{0<y<r} \frac{R(w - x, r - y)}{R(w - x, r - y) + (x + y)^{x+y}/(x^x y^y)}.$$

Доказательство. Рассмотрим оптимальный код, свободный от (w, r) перекрытий, с объемом T, длиной $N(T, w, r)$ и скоростью R. Используя следствие 4, получим

$$R \leq 1 - \frac{(x+y)^{x+y} N(T-x-y, w-x, r-y)}{x^x y^y N(T, w, r)}.$$

Применим определение для величины $R(w-x, r-y)$ и перейдем к пределу в правой и левой частях доказанного выше неравенства. В результате получим рекуррентное неравенство для скорости $R(w, r)$, которое можно записать в виде

$$R(w, r)(1 + \frac{(x+y)^{x+y}}{x^x y^y R(w-x, r-y)}) \leq 1.$$

Из полученного неравенства следует утверждение теоремы.

Теорема 8 дает наилучшие на данное время асимптотические верхние границы для скорости кодов, свободных от (w, r) перекрытий, для $r > w > 2$.

Для построения следующих таблиц будем использовать верхние границы $R(1, 2) \leq 0.321928$, $R(1, 3) \leq 0.199282$, и $R(1, 4) \leq 0.140457$, которые получены в работе [30].

Таблица. Численные значения для верхней границы скорости кода $R(w, r)$

(w, r)	(2,3)	(2,4)	(2,5)	(2,6)	(3,4)	(3,5)
$R(w, r) \leq$	0.07448	0.04552	0.02867	0.02038	0.01828	0.01091

(w, r)	(4,4)	(4,5)	(4,6)	(5,5)	(5,6)
$R(w, r) \leq$	0.009578	0.004549	0.002567	0.002388	0.001136

3.6 Тривиальные коды, свободные от (w, r) перекрытий

Наиболее простые примеры кодов, свободных от (w, r) перекрытий, дает следующая конструкция. Рассмотрим матрицу, строками которой являются все различные вектора веса w. Тогда эта матрица задает код, свободный от (w, r) перекрытий, для любого $r \leq T - w$. Мы будем называть такую матрицу тривиальным кодом, свободным от (w, r) перекрытий. Таким образом, тривиальный код имеет размер $N \times T$, где $N = \binom{T}{w}$. Следовательно, для любого T, такого что $T \geq w + r$ справедливо неравенство

$$N(T, w, r) \leq \binom{T}{w}.$$

В данном параграфе мы будем искать условия, при выполнении которых тривиальные коды являются оптимальными, то есть

$$N(T, w, r) = \binom{T}{w}.$$

Подобная задача не является новой, поэтому приведем результаты, полученные ранее. В [128] отмечено, что $N(T, w, r) = \binom{T}{w}$, если $T = w + r$. Более сильное условие доказано в [133]:

Утверждение 32. *Если* $T \leq w + r + r/w$, *то* $N(T, w, r) = \binom{T}{w}$.

Напомним, что мы рассматриваем только случай $r \geq w \geq 2$. Для классического случая с $w = 1$ еще в 1975 году Л.А.Бассалыго отметил, что при $N \leq \binom{r+2}{2}$ нетривиальных кодов, свободных от $(1, r)$ перекрытий, не существует. Этот факт следует из рекурентного соотношения

$$N(T, 1, r) \geq N(T - 1, 1, r - 1) + (r + 1),$$

справедливого для нетривиальных $(1, r)$ кодов. Отметим, что в этом случае $(w = 1)$ тривиальные коды представляют собой единичные матрицы (с точностью до перестановки строк). Таким образом,

$$N(T, 1, r) = T, \quad \text{если} \quad T \leq \binom{r+2}{2}$$

В работе [136] через $n(r)$ была обозначена минимальная длина кода, свободного от $(1, r)$ перекрытий, отличного от тривиального. Авторы [136] высказали предположение, что $\lim n(r)/r^2 = 1$, отметив, что они могут доказать равенство $n(r) = (r+1)^2$ лишь для $r \leq 3$. Для произвольного r в [136] доказано, что

$$5/6r^2(1 + o(1)) \leq n(r) < r^2(1 + o(1)) \quad r \to \infty$$

Для рассматриваемого нами случая $r \geq w \geq 2$ мы введем следующее обозначение:

Определение 8. *Обозначим через $TR(w, r)$ такое максимальное T, при котором $N(T, w, r) = \binom{T}{w}$.*

Таким образом, утверждение 1 доказывает справедливость неравенства

$$TR(w, r) \geq w + r + r/w$$

при $r \geq w \geq 2$.

Рассмотрим ситуацию, когда w фиксировано, а r велико. Из (3) вытекает, что $TR(w, r) \geq \frac{w+1}{w} r + w$. Мы докажем границу, которая при фиксированном w и больших r слегка улучшает константу при r. Для доказательства этой границы нам понадобится рекурентное неравенство, которое мы сформулируем в виде Леммы. Для удобства записи введем обозначение $F(T, x, y) = \lfloor \frac{x(T+1)}{x+y} \rfloor$

Лемма 8. *Для целых положительных x, y ($x < w$, $y < r$) справедливо неравенство*

$$N(T, w, r) \geq N(T - x - y, w - x, r - y) \cdot \frac{\binom{T}{x+y}\binom{x+y}{x}}{\binom{F(T,x,y)}{x}\binom{T-F(T,x,y)}{y}}.$$

Теорема 9. *Для любых $w \geq 2$ и $r \geq \frac{(w-1)(w+\sqrt{18w+81}+9)}{2}$ справедливо неравенство*

$$TR(w, r) \geq \frac{w+1}{w-1}r - \sqrt{\frac{36r}{w-1}}$$

Доказательство. Для заданных w и r, удовлетворяющих условию теоремы, положим $x = w - 1$, $y = \lfloor \frac{x(T+1)}{x+2} \rfloor - x + 1$.

В этом случае $F(T, x, y) = x+1$. Действительно, с одной стороны, неравенство $\frac{x(T+1)}{x+y} < x + 2$ сразу же следует из определения y.

$x(T + 1) < (x + 2)(x + \lfloor \frac{x(T+1)}{x+2} \rfloor - x + 1)$

$$x(T + 1) < (x + 2)(\lfloor \frac{x(T + 1)}{x + 2} \rfloor + 1)$$

Осталось воспользоваться тем, что

$$\frac{x(T + 1)}{x + 2} < \lfloor \frac{x(T + 1)}{x + 2} \rfloor + 1$$

С другой стороны, нужно показать, что неравенство $\frac{x(T+1)}{x+y} \geq x + 1$ будет выполнено при нашем выборе

$$T = \frac{w+1}{w-1}r - \sqrt{\frac{36r}{w-1}}$$

Подставим это T в неравенство

$$T + 1 \geq \frac{(x + 1)(x + y)}{x}$$

Таким образом, надо показать, что

$$r + \frac{2}{w-1}r - \sqrt{\frac{36r}{w-1}} + 1 \geq y + y/(w-1) + w$$

При $w > 2$

$$r - y \geq \frac{w-1}{w+1}\sqrt{\frac{36r}{w-1}}$$

Поскольку мы рассматриваем только $T \geq w + r$, требуемое неравенство заведомо будет выполняться для w и r, удовлетворяющих условию теоремы.

Для $w = 2$ выполнение того, что $F(T, x, y) = x + 1$ можно проверить непосредственно.

Воспользуемся результатом леммы при нашем выборе x и y.

$$N(T, w, r) \geq N(T - x - y, w - x, r - y)\frac{\binom{T}{x+y}\binom{x+y}{x}}{(x+1)\binom{T-x-1}{y}}.$$

Из этого неравенства вытекает, что

$$N(T, w, r) \geq \frac{N(T - x - y, 1, r - y)\binom{T}{w}}{T - x - y}$$

Положим $T = \frac{w+1}{w-1}r - \sqrt{\frac{36r}{w-1}}$. Условие $r \geq \frac{(w-1)(w+\sqrt{18w+81}+9)}{2}$ обеспечивает то, что при таком выборе $T \geq w + r$. Кроме того,

$$r - y \geq \frac{x}{x+2}\sqrt{\frac{36r}{x}}, \qquad T - x - y < \frac{2}{x}r$$

Из этих двух неравенств следует, что

$$T - x - y \leq (r - y)^2/2,$$

и, значит, вытекает, что

$$N(T - x - y, 1, r - y) = T - x - y.$$

Получаем, что при $T = \frac{x+2}{x}r - \sqrt{\frac{36r}{x}}$

$$N(T, w, r) \geq \binom{T}{w}.$$

Теорема доказана.

Каскадная конструкция кодов, свободных от (w, r) перекрытий, хорошо известна [128] [87] [171] и была кратко описана в предыдущем параграфе. В качестве одного из следствий этой конструкции приведем следующий результат.

Утверждение 33 [128]. *Пусть q является степенью простого числа и $q \geq wr$. Тогда*

$$N(q^2, w, r) \leq N(q, w, r)(wr + 1).$$

Таким образом, если взять простое q так, что $wr \leq q \leq 2wr$, то для $T = q^2$ получим $N \leq \binom{q}{w}(wr+1)$. Вычеркнем $q^2 - C(w)r^{(w+1)/w}$ столбцов из полученной матрицы. Получится код, свободный от (w, r) перекрытий, размера $N \times C(w)r^{(w+1)/w}$. При больших r, выбирая $C(w)$ таким образом, чтобы число строк в построеном коде было меньше, чем $\binom{C(w)r^{(w+1)/w}}{w}$, мы получим пример нетривиального кода. Таким образом, мы доказали следующее утверждение.

Утверждение 34. *Для фиксированного $w \geq 2$ при больших r существует константа $C(w)$ такая, что*

$$TR(w, r) \leq C(w)r^{(w+1)/w}.$$

Другие известные конструкции кодов, свободных от (w, r) перекрытий, (см., например, [151]) для некоторых случаев улучшают константу $C(w)$, но порядок степени при r остается тем же. Поэтому,

очень интересными представляются любые примеры семейств нетривиальных кодов, свободных от (w, r) перекрытий, которые позволили бы улучшить порядок степени при r в верхней оценке для $TR(w, r)$.

Напомним, что нижняя граница для $TR(w, r)$ при $w = r$ утверждает, что $TR(w, r) \geq w + r + 1$. Хорошо известно, что $TR(2, 2) = 5$, и в качестве примера нетривиального $(2, 2)$ кода с $T = 6$ можно взять любые 6 столбцов матрицы. Мы приведем еще два примера нетривиальных кодов, показывающих, что эта граница достигается для $(3, 3)$ и $(5, 5)$ кодов.

Утверждение 35. *Справедливо неравенство* $N(8, 3, 3) \leq 52$.

Доказательство. Обозначим через $A(i)$ матрицу размера $4 \times \binom{4}{i}$, содержащую в качестве столбцов все слова веса i длины 4. Через 0 и 1 обозначим вектор-столбец длины 4, состоящий из 0 и 1 соответственно. Рассмотрим следующую матрицу размера 8×52:

A(3)	0	A(1)	1	A(2)
0	A(3)	1	A(1)	A(2)

Расположение матрицы A над матрицей B означает, что мы берем в качестве столбцов все различные вектора вида (a, b), где a столбец из A, а b столбец из B. Нетрудно проверить, что матрица, транспонированная к приведенной, задает код, свободный от $(3, 3)$ перекрытий. Таким образом, $TR(3, 3) = 7$.

Утверждение 36. *Для кодов, свободных от* $(5, 5)$ *перекрытий, имеем* $TR(5, 5) = 11$.

Доказательство. Используя обозначения из утверждения 4, но с длиной 6, рассмотрим следующую матрицу размера 12×784:

A(5)	0	A(1)	1	A(2)	A(5)	A(4)	A(1)	A(3)
0	A(5)	1	A(1)	A(5)	A(2)	A(1)	A(4)	A(3)

Можно проверить, что матрица, транспонированная к приведенной, задает код, свободный от $(5,5)$ перекрытий.

Замечание 9. При доказательстве утверждения 5 мы привели пример кода, свободного от $(5,5)$ перекрытий, размера 784×12. Однако можно доказать, что $N(12,5,5) \leq 774$.

Передем теперь к изучению оптимальности и единственности тривиальных кодов, свободных от (w,r) перекрытий.

Начнем с того, что оценку на размер кода можно уточнить в случае, когда $F(T,x,y) \leq w$, где $F(T,x,y) = \lfloor \frac{x(T+1)}{x+y} \rfloor$.

Утверждение 37. *Если $F(T,x,y) \leq w$, то для целых положительных x, y ($x < w$, $y < r$) справедливо неравенство*

$$N(T,w,r) \geq N(T-x-y, w-x, r-y) \cdot \frac{\binom{T}{x+y}\binom{x+y}{x}}{\binom{w}{x}\binom{T-w}{y}}.$$

Более того, эта оценка достигается только в том случае, когда вес любой строки для матрицы кода, свободного от перекрытий равен w.

Доказательство. Рассмотрим матрицу C, являющейся матрицей оптимального кода, свободного от (w,r) перекрытий. Подсчитаем число подматриц матрицы C, таких что их размер равен 1 на $(x+y)$, а число единиц равно x. Если вести подсчет по столбцам, то число таких подматриц будет не меньше, чем

$$N(T-x-y, w-x, r-y) \cdot \binom{T}{x+y} \cdot \binom{x+y}{x}.$$

Действительно, когда мы фиксируем выбор $(x+y)$ столбцов и в них выбор x столбцов, в которых стоят единицы, то числи строк, в которых именно такое расположение нулей и единиц, не может быть меньше, чем $N(T-x-y, w-x, r-y)$, поскольку только в таких строках данное расположение единиц и нулей и подматрица, соответствующая таким строкам и столбцам, не входящим в выбранные, образует код, свободный от $(w-x, r-y)$ перекрытий.

Если вести подсчет по строкам, то число таких подматриц равно

$$\sum_{i=1}^{n} \binom{a_i}{x} \binom{T-a_i}{y},$$

где через a_i обозначено число единиц в i-ой строке матрицы C.

Следовательно,

$$N(T-x-y, w-x, r-y) \cdot \binom{T}{x+y} \binom{x+y}{x} \leq N \max_a \binom{a}{x} \binom{T-a}{y}.$$

Максимум функции $f(a) = \binom{a}{x}\binom{T-a}{y}$ ищется по целым значениям a, поэтому точка максимума принадлежит интервалу $(x-1, T-y+1)$, на котором функция $f(a)$ положительна и выпукла вверх. На этом интервале $f(a) \geq f(a-1)$ тогда и только тогда, когда $a \leq F(T,x,y)$. Действительно, разделим $f(a)$ на $f(a-1)$ и распишем биномиальные коэффициенты через факториалы. После сокращения получим

$$\frac{a(T-a+1-y)}{(a-x)(T-a+1)} \geq 1,$$

что эквивалентно тому, что $a(x+y) \leq x(T+1)$.

Поэтому

$$\max_a \binom{a}{x} \binom{T-a}{y} = \binom{F(T,x,y)}{x} \binom{T-F(T,x,y)}{y},$$

откуда и вытекает справедливость утверждения.

При этом, если $F(T, x, y) \leq w$, то максимум достигается в точке $a = w$, так как вес любой строки матрицы, которая задает оптимальный код, свободный от (w, r) перекрытий, не меньше чем w. Действительно, любую строчку с меньшим весом можно удалить и код останется кодом, свободным от (w, r) перекрытий - это сразу вытекает из определения такого кода. Из доказательства утверждения сразу видно, что равенство в формулировке утверждения возможно только в том случае, когда вес любой строки равен w.

3.7 Коды, свободные от (w, r) перекрытий, с ограничениями на возможные коалиции

Одним из наиболее важных приложений кодов, свободных от (w, r)- перекрытий, является следующая криптографическая проблема (см., например, [161]). Имеется T пользователей и N секретных ключей. Каждый пользователь имеет свой набор ключей, и группа пользователей может вести обмен информацией, если найдется общий для всей группы секретный ключ. Двоичный код в данной задаче используется как матрица инцидентности, задающая распределение ключей между пользователями. Код, свободный от (w, r) перекрытий, гарантирует, что для любой группы из w пользователей и группы из r других пользователей найдется такой ключ, что все пользователи первой группы имеют этот ключ (и, поэтому, могут вести обмен информацией), тогда как ни у одного из r пользователей второй группы этого ключа нет. Тем самым, пользователи первой группы могут обмениваться информацией секретно от пользователей

второй группы. Однако, нетрудно представить себе ситуацию, когда некоторые пользователи никогда одновременно не войдут в первую группу по тем или иным причинам. Предположим, что нам задано множество S, состоящее из w-элементных подмножеств $[T]$, показывающих, какие наборы пользователей могут войти в первую группу. В этой ситуации естественным представляется следующее определение.

Определение 9. *Двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется кодом, свободным от (w, r) перекрытий, с ограничениями S ($S \subset 2^T$) на возможные коалиции, если для любой пары непересекающихся подмножеств $J_1 \in S$, $J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует $i \in [N]$ такое, что $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$.*

Еще раз отметим, что мы рассматриваем только $T \geq w + r$ и $w \leq r$. Обозначим через $N_S(T, w, r)$ минимальное число строк для кода, свободного от (w, r) перекрытий, с ограничениями S на возможные коалиции с заданным числом столбцов T. Будем называть код тривиальным, если $N_S(T, w, r) = |S|$.

Утверждение 38. *a) Для любого S*

$$N(T, w, r) \leq N_S(T, w, r) + \binom{T}{w} - |S|.$$

b) Для любого значения T, $w + r \leq T \leq TR(w, r)$ имеет место равенство

$$N(T, w, r) = \binom{T}{w}.$$

c) Если $TR(w, r) \geq T$, то для любого S

$$N_S(T, w, r) = |S|.$$

Доказательство. Легко видеть, что к матрице кода, свободного от (w, r) перекрытий, с ограничениями S на возможные коалиции можно добавить $\binom{T}{w} - |S|$ строк веса w так, что получится код, свободный от (w, r) перекрытий. Таким образом, справедливость п. a) доказана. Теперь, если $N(T, w, r) = \binom{T}{w}$ для некоторого T, то для $T-1$ утверждение п. b) тоже верно. Действительно, определим систему S, которая включает в себя все w-подмножества множества $[T]$, не содержащие некоторого фиксированного элемента (т.е. на самом деле подмножества множества $[T-1]$). Подставляя в п. a) указанное соотношение, получаем:

$$N(T-1, w, r) \geq N(T, w, r) - \binom{T}{w} + |S|.$$

Требуемое соотношение $N(T-1, w, r) = \binom{T-1}{w}$ вытекает из того, что $N(T, w, r) = \binom{T}{w}$ и $|S| = \binom{T-1}{w}$. Утверждение п. c) также является прямым следствием утверждения из п. a) и определения тривиального кода.

Пример 5. Пусть $S_1 = \{\binom{T}{2} \backslash \{1,3\} \backslash \{4,5\} \backslash \{2,6\}\}$. Рассмотрим следующий код, свободный от $(2, 2)$ перекрытий, с ограничениями S_1 на возможные коалиции:

$$
\begin{array}{cccccc}
1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0
\end{array}
$$

Из утверждения 6 и того, что $N(8, 2, 2) = 14$ вытекает, что код, свободный от $(2, 2)$ перекрытий, с ограничениями S_1 на возможные коалиции, приведенный в примере, является оптимальным и нетривиальным.

3.8 Коды, свободные от перекрытий, и разделяющие коды

Коды, свободные от (w, r) перекрытий, тесно связаны с разделяющими (w, r) кодами.

Определение 10. *Двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется разделяющим (w, r) кодом, если для любой пары непересекающихся подмножеств $J_1, J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует координата $i \in [N]$ такая, что множества c_{ij}, где $j \in J_1$ и c_{ij}, где $j \in J_2$ не пересекаются.*

Таким образом, для двоичных разделяющих кодов либо $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$, либо наоборот $c_{ij} = 0$ для всех $j \in J_1$ и $c_{ij} = 1$ для всех $j \in J_2$.

Достаточно подробную библиографию по разделяющим кодам можно найти в работах [87] и [151].

Коды определяются как матрицы, в которой каждый столбец является кодовым словом. Как обычно, задача состоит в нахождении наибольшего количества кодовых слов при фиксированной длине кода. Матрица кода напрямую связаны с групповым тестированием, при этом кодовая задача согласуется с задачей поиска (нахождение минимального числа вопросов при фиксированном количестве элементов в рассматриваемом множестве). Каждую строку матрицы можно рассматривать как вопрос. Элемент $j, 1 \leq j \leq T$ входит в подмножество $S_i, 1 \leq i \leq N$ тогда и только тогда, когда $c_{ij} = 1$.

В основополагающей работе [149] показано, что $(1, d)$ коды, свободные от перекрытий, размера $N \times T$ позволяют за N вопросов определить не более, чем d дефектов в множестве объема T в неадаптивной классической модели поиска.

Мы построим новую модель группового тестирования, связанную с разделяющими кодами и кодами, свободными от перекрытий.

Рассмотрим следующую модель группового тестирования.

Напомним, что $S_1 = S$ и $S_0 = T \setminus S$, а вопросом является произвольное подмножество S множества $[T]$. Однако ответы мы теперь будем рассматривать такие:

$$V(S) = \begin{cases} 1 & \text{если } |S_1 \cap D| > |S_0 \cap D| \\ 0 & \text{если } |S_1 \cap D| < |S_0 \cap D| \end{cases} \tag{70}$$

Для оставшегося случая, когда $\mid S_1 \cap D \mid = \mid S_0 \cap D \mid$, можно рассмотреть несколько вариантов ответов:

I1. ответ может быть произвольным.

I2. ответ 1, если $|S_1| \geq |S_0|$ и ответ 0, если $|S_1| < |S_0|$

I3. ответ 1 всегда, когда $\mid S_1 \cap D \mid = \mid S_0 \cap D \mid$.

I4. ответ $*$ всегда, когда $\mid S_1 \cap D \mid = \mid S_0 \cap D \mid$. (тогда ответы на вопросы образуют множество $0, 1, *$ и такая модель напоминает отыскание фальшивых монет с помощью взвешиваний на чашечных весах).

Мы разберем только случай I3. Но сначала рассмотрим наиболее простой вариант, когда дополнительно известно, что число дефектных элементов нечетно. Следующая теорема относятся именно к такому случаю, и в ней изучается неадаптивное тестирование.

Еще раз напомним, что d' это число дефектных элементов ($d' \leq d$).

Теорема 10. *Пусть имеется (w, w) разделяющий код размера $N \times T$. Тогда за N вопросов можно найти все дефектные элементы, если $d = 2w - 1$, а ответы на вопросы даются согласно I3.*

Доказательство. Каждую строку матрицы можно рассматривать как вопрос. Элемент $j, 1 \leq j \leq T$ входит в подмножество $S_i, 1 \leq i \leq N$ тогда и только тогда, когда $c_{ij} = 1$.

Рассмотрим наборы, состоящие из r столбцов матрицы разделяющего кода, где $r = 1, 2 \ldots, w$. Для каждого такого набора A будем проверять следующее условие. Пусть набор A состоит из столбцов $j_1, j_2, \ldots, j_r$. Обозначим через $L_0(A)$ и $L_1(A)$ множество строк, для которых $c_{ij_1} = c_{ij_2} = \ldots = c_{ij_r} = 0$ и $c_{ij_1} = c_{ij_2} = \ldots = c_{ij_r} = 1$ соответственно.

Скажем, что на наборе A выполняется условие $G1(r)$, если набор A таков, что на любой вопрос из $L_0(A)$ дается ответ 0, а на вопрос из $L_1(A)$ всегда дается ответ 1.

Если $d' = 2r - 1$, то найдется ровно $\binom{d'}{(d'+1)/2}$ наборов из r столбцов, на которых выполняется условие $G1(r)$.

Действительно, если набор A, $|A| = r$ целиком состоит из дефектных элементов, то на наборе A выполняется условие $G1(r)$. Если в наборе A есть хоть один не дефектный столбец, то вне этого набора будет не менее, чем r дефектов. Пусть множество столбцов B содержит r дефектных столбцов, не входящих в A. Тогда из определения разделяющего кода с $J_1 = A$ и $J_2 = B$ вытекает, что для такого набора A условие $G1(r)$ не будет выполнено.

Если $d' \geq 2r + 1$, то не найдется ни одного набора, на котором выполняется условие $G1(r)$.

Действительно, это следует из определения разделяющего кода и того, что любой набор A, $|A| = r$ может быть дополнен до множества из w столбцов так, что в этом множестве число дефектов меньше, чем в неком другом наборе из w столбцов (наличие в матрице хоть одного не дефектного столбца вытекает из того, что $T \geq 2w$).

Таким образом, мы в какой-то момент найдем наименьшее r для которого найдется некоторое количество (ровно $\binom{d'}{(d'+1)/2}$) наборов из r столбцов на которых выполняется условие $G1(r)$ и следовательно мы восстановим все дефектные элементы.

Рассмотрим теперь модель, когда ответы на вопросы даются со-

гласно I3.

$$V(S) = \begin{cases} 1 & \text{если } |S_1 \cap D| \geq |S_0 \cap D| \\ 0 & \text{если } |S_1 \cap D| < |S_0 \cap D| \end{cases} \tag{71}$$

Теорема 11. *Пусть $T > 2w$ и матрица вопросов обладает свойством (w, w) кода, свободного от перекрытий размера $N \times T$ для $d = 2w - 1$ или свойством $(w, w + 1)$ кода, свободного от перекрытий размера $N \times T$ для $d = 2w$. Тогда за N вопросов можно найти все дефектные элементы, если ответы даются согласно I4.*

Доказательство. Для множеств из r столбцов обозначим через $L_1(A)$ множество строк, для которых $c_{ij_1} = c_{ij_2} = \ldots = c_{ij_r} = 1$, где $r = 1, 2 \ldots, w$.

На наборе A выполняется условие $G2(r)$, если набор A таков, что на любой вопрос из $L_1(A)$ всегда дается ответ 1.

Если $d' = 2r - 1$, то найдется ровно $\binom{d'}{(d'+1)/2}$ наборов A, $|A| = r$ на которых выполняется условие $G2(r)$.

Если $d' = 2r$, то найдется ровно $\binom{d'}{d'/2}$ наборов A, $|A| = r$ на которых выполняется условие $G2(r)$.

Действительно, если набор A, $|A| = r$ целиком состоит из дефектных элементов, то на таком наборе выполняется условие $G2(r)$. Для того, чтобы на множестве из r столбцов, содержащем хоть один не дефектный столбец условие $G2(r)$ не выполнялось надо, чтобы матрица вопросов обладала свойством (r, w) кода, свободного от перекрытий, для $d = 2w - 1$ и свойством $(r, w + 1)$ кода, свободного от перекрытий для случая $d = 2w$. Поскольку r пробегает значения от 1 до w, то получим условия, сформулированные в теореме. Более того, видно, что в случае $d = 2w - 1$ от матрицы вопросов достаточ-

но свойства $(w-1, w)$ кода, свободного от перекрытий, и свойством (w, w) разделяющего кода, но при этом надо проверять не только условие $G2(r)$, но и условие $G1(r)$ из теоремы 1.

Если $d' \geq 2r+1$, то не найдется ни одного набора, на котором выполняется условие $G2(r)$.

Действительно, рассмотрим множество B из w столбцов так, что в это множество входит дефектных столбцов не меньше, чем

$\min\{w, \lfloor (d'+1)/2 \rfloor\}$. Тогда из определения кода, свободного от перекрытий, следует, что на любом наборе из r столбцов при $r \leq (d'-1)/2$ условие $G2(r)$ не будет выполняться.

Случай $d' = 2r-1$ мы можем отличить от случая $d' = 2r$ по числу наборов A, $|A| = r$ на которых выполняется условие $G2(r)$.

Замечание 10. Как видно из доказательства теоремы, в случае $d = 2w-1$ для матрицы вопросов достаточно свойства $(w-1, w)$ кода, свободного от перекрытий, и свойства (w, w) разделяющего кода. Если матрица обладает свойством (w, w) кода, свободного от перекрытий, то, эти свойства, очевидно, будут выполняться. Еще раз отметим, что только свойства (w, w) разделяющего кода здесь будет недостаточно. Здесь существенно используется различие между кодами, свободными от перекрытий, и разделяющими кодами.

3.9 Окрашенные коды, свободные от перекрытий

Одно из наиболее важных приложений кодов, свободных от (w, г) перекрытий, описывается следующей криптографической проблемой.

Имеется T пользователей и N секретных ключей. Каждый поль-

зователь имеет свой набор ключей, и группа пользователей может вести обмен информацией, если найдется общий для всей группы секретный ключ. Требуется, чтобы для любой группы из w пользователей и группы из r других пользователей нашелся такой ключ, что все пользователи первой группы имеют этот ключ, и тем самым, могут вести обмен информацией, тогда как ни у одного из r пользователей второй группы этого ключа нет.

Тем самым, пользователи первой группы могут обмениваться информацией секретно от пользователей второй группы.

Предположим теперь, что у всех пользователей имеется одинаковый набор ключей, но каждый ключ имеет несколько состояний, в которых он может находиться.

Причем, пусть для простоты все ключи имеют одно и то же число таких состояний.

Пользователь не может поменять состояние ключа и может обмениваться информацией с пользователями, идентичный ключ которых находится в том же состоянии.

Пусть теперь имеется несколько групп пользователей (число таких групп не больше числа состояний ключа).

Мы хотим, чтобы нашелся ключ такой, что для любой группы пользователей он имеет одинаковое состояние (а для разных групп - разные состояния), и тем самым, пользователи внутри каждой группы могли бы вести обмен информацией секретно от других групп.

Естественно представлять себе эту ситуацию в виде q-ичной матрицы $C = c_(ij)$ размера $N \times T$, в которой $c_{ij} = k$, если у j-то пользователя i-й секретный ключ находится в состоянии k. Тогда описанное выше свойство означает, что для любых групп $R_0, R_1 \dots R_{q-1} \subset [T]$

размера $|R_s| = r_s$ существует координата $i \in [N]$ такая, что $c_{ij} = s$ для всех $j \in R_s$, где $s = 0, 1, \ldots, q-1$.

Мы будем в дальнейшем называть такую матрицу кодом, свободным от $(r_0, r_1, \ldots, r_{q-1})$ перекрытий, или окрашенным кодом, свободным от перекрытий.

Нам бы хотелось минимизировать число секретных ключей при фиксированном числе пользователей, или, что то же самое, максимизировать число пользователей при фиксированном числе ключей.

Таким образом, проблема состоит в нахождении такой матрицы C, что указанное свойство выполняется, а число столбцов матрицы по возможности максимально. Часто мы будем называть столбцы матрицы C кодовыми словами, а саму матрицу q-ичным кодом.

Обозначим через $N(T, r_0, r_1, \ldots, r_{q-1})$ минимально возможную длину для кодов, свободных от $(r_0, r_1, \ldots, r_{q-1})$ перекрытий, данной мощности T.

Окрашенный код будет называться оптимальным, если

$N = N(T, r_0, r_1, \ldots, r_{q-1})$. Скоростью q-ичного кода длины N и мощности T называется, как обычно, величина $R = \log_q T/N$. В данной статье нас будет интересовать асимптотическое поведение скорости таких (оптимальных) кодов.

Определение 11. *q-ичная матрица $C = \|c_{ij}\|$ размера $N \times T$ является $(r_0, r_1, \ldots, r_{q-1})$ кодом, свободным от перекрытий, если для любых подмножеств $R_0, R_1 \ldots R_{q-1} \subset [T]$ размера $|R_s| = r_s$ существует координата $i \in [N]$ такая, что $c_{ij} = s$ для всех $j \in R_s$, где $s = 0, 1, \ldots, q-1$.*

Если для любых подмножеств $R_0, R_1 \ldots R_{q-1} \subset [T]$, у которых $|R_s| = r_s$ существует ровно одна такая координата, то мы скажем,

что такой код является совершенным окрашенным кодом, свободным от перекрытий.

Рассмотрим случай $r_0 = r_1 = \ldots = r_{q-1} = 1$.

Пусть $T = q + x$ и $x \leq q$. Граница Плоткина утверждает, что

$$N = \frac{(q+x)!}{2^x x!}.$$

Рассмотрим случай $x = q$, который выглядит наиболее интересным. Для этого случая имеем

$$N_i = \frac{(q+x-1)!}{2^{(x-1)} x!} = N/q,$$

где N_i это число элементов i в первом столбце.

Значит, если $q = 2s$, то $N = (2q-1)!!$ не делится на q и, следовательно, не существует совершенных кодов для этого случая.

Обозначим через $N_{m_1,m_2,\ldots,m_k}$ число строк, которые содержат элемент m_j в j-м столбце.

$$N_{m_1,m_2,\ldots,m_k} = \frac{(2q-s)!}{2^{(q-k)} q!}$$

Если $q \neq 2^s - 1$, то не существует совершенных кодов для этого случая с $T = 2q$.

Утверждение 39. *Пусть C является совершенным $(r_0, r_1, \ldots, r_{q-1})$ окрашенным кодом, свободным от перекрытий размера T. Тогда существует совершенный $(1, r_0, r_1, \ldots, r_{q-1})$ окрашенный код, свободный от перекрытий размера $T' = T + 1$.*

$N(6, 1, 1, 1) = 15$

$$
\begin{array}{cccccc}
0 & 0 & 1 & 2 & 2 & 1 \\
0 & 1 & 0 & 1 & 2 & 2 \\
0 & 2 & 1 & 0 & 1 & 2 \\
0 & 2 & 2 & 1 & 0 & 1 \\
0 & 1 & 2 & 2 & 1 & 0 \\
1 & 1 & 2 & 0 & 0 & 2 \\
1 & 2 & 1 & 2 & 0 & 0 \\
1 & 0 & 2 & 1 & 2 & 0 \\
1 & 0 & 0 & 2 & 1 & 2 \\
1 & 2 & 0 & 0 & 2 & 1 \\
2 & 2 & 0 & 1 & 1 & 0 \\
2 & 0 & 2 & 0 & 1 & 1 \\
2 & 1 & 0 & 2 & 0 & 1 \\
2 & 1 & 1 & 0 & 2 & 0 \\
2 & 0 & 1 & 1 & 0 & 2
\end{array}
$$

$$N(5, 1, 1, 1) = 15$$

Мы можем удалить столбец из примера и получим опять совершенный код.

$$N(4, 1, 1, 1) = 12$$

Если мы удалим два столбца из примера, то у нас возникнет три строки, содержащие только по два элемента. Удаляя эти строки, опять получим совершенный код.

Заметим, что существует тривиальный совершенный код с $T = q + 1$, значит для $T = 4$ существует как минимум два неэквивалентных кода.

Из Утверждения следует, что существуют коды с $T = q + 2$ и $T = q + 3$ для всех q. Следовательно первый случай, для которого неизвестно существование совершенного кода, это случай $q = 5$ и $T = 9$.

Было бы интересно найти (1,1,1,1,1) совершенный код с $T = 9$, или доказать его несуществование.

Аналогично, бы интересно найти (1,1,1,1,1,1,1) совершенный код с $T = 14$, или доказать его несуществование.

Наиболее простые примеры окрашенных кодов, свободных от перекрытий, дает следующая конструкция.

Будем считать, что $r_0 \leq r_1 \leq \ldots \leq r_{q-1}$. Рассмотрим матрицу, строками которой являются все различные наборы, содержащие элемент r_s ровно s раз, где $s = 0, 1, \ldots, q-2$, а элемент $q-1$ занимает все оставшиеся позиции в строке. Мы будем называть такую матрицу тривиальным окрашенным кодом, свободным от перекрытий.

Более точно: выберем позиции, которые будет занимать элемент ноль. Число вариантов такого выбора равно $\binom{T}{r_0}$. Для каждого варианта расположения нуля рассмотрим все варианты расположения r_1 единиц. Это будут разные позиции, но их число всегда будет равно $\binom{T-r_0}{r_1}$. Продолжая этот процесс получим матрицу размера $N \times T$, где

$$N = \binom{T}{r_0}\binom{T-r_0}{r_1}\ldots\binom{T-r_0-r_1-\ldots-r_{q-3}}{r_{q-2}}$$

Утверждение 40. *Пусть $r_0 \leq r_1 \leq \ldots \leq r_{q-1}$, причем $r_i \geq lr_{i-1}$. Тогда, если $T \leq r_0 + r_1 + \ldots + r_{q-1} + l$, то тривиальный окрашенный код, свободный от перекрытий, оптимален.*

Доказательство. Рассмотрим матрицу C произвольного окрашенного кода, свободного от перекрытий. Удалим все строки, в ко-

торых найдется элемент s, встречающийся реже чем r_s раз. Полученный код, очевидно, тоже будет окрашенным кодом, свободным от перекрытий. Предположим, что в строке элемент s встречается T_s раз. Тогда эта строка образует

$$F = \binom{T_0}{r_0}\binom{T_1}{r_1}\dots\binom{T_{q-1}}{r_{q-1}}$$

различных подматриц размера $1 \times (r_0 + r_1 + \ldots + r_{q-1})$, которые содержат r_s элементов, имеющих значение s для всех $s = 0, 1, \ldots, q-1$.

Нужно доказать, что максимум F достигается, когда $T_s = r_s$ для $s = 0, 1, \ldots, q-2$ и $T_{q-1} = r_{q-1} + l$. Тогда, учитывая, сколько всего имеется таких подматриц во всей матрице C, получим

$$N \geq \binom{T}{r_0}\binom{T-r_0}{r_1}\dots\binom{T-r_0-r_1-\ldots-r_{q-3}}{r_{q-2}}\binom{r_{q-1}+l}{r_{q-1}}/F,$$

что и доказывает утверждение. Таким образом, достаточно показать, что если какое-то $T_i \geq r_i$ для $i \in 0, 1, \ldots, q-2$, то уменьшая это T_i на единицу и, соответственно, увеличивая T_i на единицу, мы не уменьшим величину F. А это вытекает из того, что

$$\binom{r_{q-1}+b+1}{r_{q-1}}\binom{r_i+a-1}{r_i} \geq \binom{r_{q-1}+b}{r_{q-1}}\binom{r_i+a}{r_i}$$

эквивалентно неравенству

$$ar_{q-1} \geq (b+1)r_i,$$

которое справедливо, поскольку

$a \geq 1$ и $b \leq l-1$.

Следующая важная для нас величина будет определена для произвольного q-ичного кода C размера $N \times T$.

Рассмотрим целые положительные $(x_0, x_1, \ldots, x_{q-1})$ Зафиксируем набор I, состоящий из $T = x_0 + x_1 + \ldots + x_{q-1}$ кодовых слов, и обозначим подматрицу матрицы C, образованную этими кодовыми словами, через $C_X(I)$.

Таким образом, матрица $C_X(I)$ имеет размер $N \times X$. Назовем X-расстоянием для набора I число строк матрицы $C_X(I)$, таких что каждая строка содержит x_s элементов, имеющих значение s для всех s от 0 до $q-1$. Обозначим это число через $d(C_X(I))$.

Определение 12. Минимальным X-расстоянием для q-ичного кода C назовем величину $d_X = \min_{|I|=X} d(C_X(I))$.

Обозначим через $R^N(d_X)$ скорость q-ичного кода длины N с минимальным X-расстоянием d_X. Далее мы докажем верхние границы для скорости кода с минимальным X-расстоянием d_X, а затем покажем, как можно использовать эти границы для получения асимптотических верхних границ для скорости окрашенных кодов, свободных от перекрытий.

Теорема 12. *Для q-ичного кода C длины N с минимальным X-расстоянием d_X справедлива следующая асимпттотическая граница:*

$$R^N(d_X) \leq \left(1 - \frac{X^X x_0! x_1! \ldots x_{q-1}! d_X}{x_0^{x_0} x_1^{x_1} \ldots x_{q-1}^{x_{q-1}} X! N}\right)(1 - \log_q(q-1))$$

Доказательство. Подсчитаем число подматриц матрицы C, таких что их размер равен $1 \times X$, а число элементов s равно x_s, где $s + 0, 1, \ldots, q-1$. Если вести подсчет по столбцам, то число таких подматриц не меньше чем $\binom{T}{X} d_X$.

Теперь будем вести подсчет по строкам. Если в строке элемент s встречается T_s раз, то асимптотически число таких подматриц для

каждой строки равно

$$\binom{T_0}{x_0}\binom{T_1}{x_1}\dots\binom{T_{q-1}}{x_{q-1}}$$

Асимптотически величина $\binom{T_i}{x_i}$ эквивалентна $\frac{T_i^{x_i}}{x_i!}$, поскольку все x_i-е являются константами.

Максимум функции

$$x_0 \ln T_0 + x_1 \ln T_1 + \ldots + x_{q-1} \ln T_{q-1}$$

при ограничении $x_0 + x_1 + \ldots + x_{q-1} = T$ достигается при $T_i = \frac{x_i T}{X}$, поэтому асимптотически число подматриц матрицы C меньше чем

$$\frac{x_0^{x_0} x_1^{x_1} \dots x_{q-1}^{x_{q-1}} T^X}{X}$$

Отсюда вытекает, что

$$\frac{(T-X+1)^X d_X}{X!} \le \frac{x_0^{x_0} x_1^{x_1} \dots x_{q-1}^{x_{q-1}} N T^X}{X^X x_0! x_1! \dots x_{q-1}!}(1+o(1)).$$

Для максимального числа слов кода с минимальным X-расстоянием d_X справедливо соотношение

$$T(N, d_X) \le \frac{qT(N-1, d_X)}{q-1}$$

Действительно, пусть C - матрица размера $N \times T$, составленная из кодовых слов с минимальным X-расстоянием d_X. Рассмотрим произвольную строку в этой матрице и найдем элемент b, который встречается реже других в этой строке. Пусть J - множество столбцов, которые в выбранной строке имеют элемент b. Удаляя данную строку и столбцы множества J, получим код C_1 размера $N_1 \times T_1$, у которого

$T_1 \geq T(q-1)/q$, а X-расстоянием d_X не меньше, чем в исходном коде C.

Применим это соотношение i раз и выберем наименьшее целое i, такое что

$$N - i \leq \frac{X^X d_X x_0! x_1! \dots x_{q-1}!}{x_0^{x_0} x_1^{x_1} \dots x_{q-1}^{x_{q-1}} X!}.$$

После логарифмирования по основанию q имеем

$$\log_q T(N, d_X) \leq i - i \log_q (q-1) + \log_q T(N-i, d_X)$$

Переходя к пределу при стремящемся к бесконечности получаем требуемое неравенство. Теорема доказана.

Теперь докажем лемму, которая показывает, как связана величина d_X с кодами, свободными от $(r_0, r_1, \dots, r_{q-1})$ перекрытий.

Лемма 8. *Если существует окрашенный код C, свободный от $(r_0, r_1, \dots, r_{q-1})$ перекрытий, размера $N \times T$, то существует окрашенный код, свободный от $(r_0 - x_0, r_1 - x_1, \dots, r_{q-1} - x_{q-1})$ перекрытий, размера*

$$(d_X x_0! x_1! \dots x_{q-1}!/X!) \times (T - X).$$

Доказательство. Рассмотрим код C. Пусть I набор номеров мощности $|I| = X$ тех кодовых слов, на котором достигается минимальное X-расстояние d_X. Разобьем множество I на q подмножеств $I_0, I_1, \dots, I_{q-1})$ мощности $I_s = x_s$, так чтобы число позиций, в которых слова из s-го подмножества принимают значение s было минимальным. Обозначим множество таких позиций через $I(q)$. Очевидно, что

Рассмотрим теперь подматрицу кода C, образованную строками из $I(q)$ и столбцами из $[T]$ I_0 $I_1, \ldots$ I_{q-1}. Из определения кода следует, что эта подматрица является кодом, свободным от $(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})$ перекрытий, что и доказывает лемму 3.

Следовательно, если существует $(r_0, r_1, \ldots, r_{q-1})$ окрашенный код C мощности T с минимальным X-расстоянием d_X, то, для натуральных x_s $(x_s < r_s)$, имеем

$$N(T - X, r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1}) \leq \frac{d_X x_0! x_1! \ldots x_{q-1}!}{X!}.$$

Теорема 13. *Для скорости кодов, свободных от* $(r_0, r_1, \ldots, r_{q-1})$ *перекрытий, справедлива асимптотическая граница:*

$$R \leq \frac{R(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})}{R(r_0 - x_0, \ldots, r_{q-1} - x_{q-1})/(1 - \log_q(q-1)) + X^X/(x_0^{x_0} \ldots x_{q-1}^{x_{q-1}})}.$$

Доказательство. Рассмотрим оптимальный $(r_0, r_1, \ldots, r_{q-1})$ код мощности T, длины $N(T, r_0, r_1, \ldots, r_{q-1})$ со скоростью $R_T(r_0, r_1, \ldots, r_{q-1})$. Из теоремы 12 вытекает, что при $T \to \infty$

$$R_T \leq (1 - \frac{X^X d_X x_0! x_1! \ldots x_{q-1}!}{x_0^{x_0} x_1^{x_1} \ldots x_{q-1}^{x_{q-1}} X! N(T, r_0, r_1, \ldots, r_{q-1})})(1 - \log_q(q-1)) + o(1)$$

Значит имеем

$$R_T \leq (1 - \frac{X^X N(T - X, r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})}{x_0^{x_0} x_1^{x_1} \ldots x_{q-1}^{x_{q-1}} N(T, r_0, r_1, \ldots, r_{q-1})})(1 - \log_q(q-1)).$$

Воспользуемся определением $R_{T-X}(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})$ и передем к пределу при $T \to \infty$. В результате получим рекуррентное неравенство

$$R(1 + \frac{X^X(1 - \log_q(q-1))}{x_0^{x_0} x_1^{x_1} \ldots x_{q-1}^{x_{q-1}} R(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})}) \leq 1 - \log_q(q-1).$$

Из полученного неравенства следует утверждение теоремы.

3.10 Выводы

В данной главе изучаются коды, свободные от (w, r) перекрытий.

Основным результатом третьего параграфа данной главы является Теорема 6. Она позволяет утверждать, что некоторые коды являются оптимальными.

В четвертом параграфе доказывается единственность некоторых из этих кодов. Основные результаты дает Теорема 7.

Основными результатами пятого параграфа являются Теорема 8 и Утверждение 31. Они показывают, как можно получать верхние границы на скорость кодов, свободных от (w, r) перекрытий. Для этого в пятом параграфе вводится композиционное расстояние, позволяющее применить подход получения верхних границ на мощность кода из теории кодирования.

В шестом параграфе доказываются результаты для тривиальных кодов, свободных от перекрытий. Основным результатом шестого параграфа является Утверждение 32.

Кроме того, в данной главе изучаются коды с ограничениями на возможные коалиции и окрашенные коды, свободные от перекрытий. Для них основные результаты получены в Теореме 12 и 13.

Результаты этой главы опубликованы в работах [66], [67], [68], [69], [151], [152].

4 Суммирующий канал множественного доступа

Множество $B = \{b_1, \ldots, b_m\}$ метрического пространства $\mathcal{B}$ называется разрешающим множеством (resolving set [142]), если любая точка x пространства определяется однозначно расстояниями $\rho_1 = d(x, b_1), \ldots, \rho_m = d(x, b_m)$ до точек B. Иначе говоря, из того что $d(x, b_i) = d(y, b_i)$ для всех $i = 1, \ldots, m$ следует $x = y$. Минимальная мощность разрешающего множества называется *метрической размерностью* пространства $\mathcal{B}$. Формально это определение впервые появилось в статьях [142],[169] как метрическая размерность графов, когда сам граф (неориентированный) превращается в метрическое пространство стандартным способом - расстояние между двумя вершинами графа равно минимальной длине пути между этими вершинами, измеряемой числом ребер. Но само это понятие встречается в неявном виде еще в статье Эрдеша и Реньи [134] и, более того, в контексте рассматриваемого нами пространства Хэмминга (двоичного).

Заметим, что метрическая размерность n-мерного евклидова пространства равна $n + 1$. Обозначим через

$$H_q^n = \{x = (x(1), \ldots, x(n)) : x(i) \in \{0, 1, \ldots, q-1\}\}$$

n-мерное q-ичное пространство Хэмминга, состоящее из q^n слов длины n над алфавитом $\{0, 1, \ldots, q-1\}$ и снабженное метрикой Хэмминга $d(x, y) = |\{i : x(i) \neq y(i)\|$. Метрическую размерность пространства H_q^n будем обозначать через $m_{n,q}$.

Легко проверить, что шар радиуса 1 с центром в точке $\mathbf{0}$ является

разрешающим множеством для пространства H_q^n и, следовательно,

$$m_{n,q} \leq 1 + (q-1)n \tag{72}$$

Эрдеш и Реньи доказали, что

$$2\frac{n}{\log_2 n}(1+o(1)) \leq m_{n,2} \leq 3\frac{n}{\log_2 n}(1+o(1)), \tag{73}$$

где верхняя граница была получена так называемым вероятностным методом или методом случайного кодирования. Явные конструкции разрешающих множеств для двоичных пространств Хэмминга, предложенные в [158] и [106], позволили доказать, что

$$m_{n,2} = 2\frac{n}{\log_2 n}(1+o(1)) \tag{74}$$

В недвоичном случае нижняя граница метрической размерности пространств Хэмминга имеет тот же вид (с заменой основания логарифма с 2 на q), а именно,

$$m_{n,q} \geq 2\frac{n}{\log_q n}(1+o(1)), \tag{75}$$

а вероятностный метод дает следующую верхнюю границу [147]

$$m_{n,q} \leq 2(2+\log_q 2)\frac{n}{\log_q n}(1+o(1)) \tag{76}$$

Мы предполагаем, что

$$m_{n,q} = 2\frac{n}{\log_q n}(1+o(1)), \tag{77}$$

для всех q, и докажем справедливость (77) для $q = 3$ и $q = 4$ (этот результат был анонсирован авторами в [148]).

Существует несколько обобщений этих задач на недвоичный случай.

Нам понадобится следующее обобщение, предложенное и исследованное Линдстремом [159]. Множество q-ичных векторов $\{h_1, \ldots, h_r\}$ в n-мерном евклидовом пространстве называется обнаруживающим множеством (detecting set, [159]), если любой q-ичный вектор $x = (x(1), \ldots, x(n)) : x(i) \in \{0, 1, \ldots, q-1\}$ пространства однозначно определяется своими скалярными произведениями с векторами $\{h_1, \ldots, h_r\}$. Иными словами, для $r \times n$-матрицы H, строками которой являются векторы h_i, в синдромном соотношении все q^n синдромов s различны. Линдстрем [159]) нашел асимптотически точный (при $n \to \infty$) ответ для задачи восстановления q-ичного вектора x по скалярным произведениям (x, h_i), при этом построенные векторы h_i являются двоичными векторами, не ухудшая асимптотический ответ, а именно, минимальное $r = \frac{2n}{\log_q n}(1 + o(1))$. Ниже мы воспользуемся этим результатом для вычисления асимптотики $r_{n,3}$.

Отметим, что в двоичном случае имеется простая связь между скалярным произведением и расстоянием Хэмминга

$$d(x, h) = wt(x) + wt(h) - 2(x, h),$$

где $wt(a)$–это число ненулевых координат вектора a (вес Хэмминга). Поэтому, строки разрешающей $m \times n$ матрицы вместе с добавленным вектором $\mathbf{1}$ являются разрешающим множеством в пространстве H_2^n. К сожалению, подобного соотношения нет в случае $q > 2$.

4.1 Метрическая размерность пространств Хэмминга

Пусть $B = \{b_1, \ldots, b_m\}$ - это разрешающее множество пространства H_q^n, и $d(x, B) = (d(x, b_1), \ldots, d(x, b_m))$ - это вектор расстояний от точки x до точек B. Разным точкам пространства, а их q^n, соответствуют разные векторы расстояний, которых, в свою очередь, не более чем $(n+1)^m$. Следовательно, $q^n \leq (n+1)^m$ или

$$m \geq \frac{n}{\log_q(n+1)} \tag{78}$$

Отметим, что если бы мы могли выбирать точки множества $B = \{b_1, \ldots, b_m\}$ шаг за шагом, т.е., узнав $d(x, b_1), \ldots, d(x, b_i)$, мы выбирали бы точку x_{i+1} (адаптивный поиск, при котором множество B зависит от точки x), то неизвестна нижняя граница, более сильная чем (78).

Для мощности разрешающих множеств справедлива в два раза более сильная асимптотическая граница (75). Известны два ее доказательства - энтропийное и методом Мозера. Ниже мы дадим простое доказательство этой границы, которое аналогично данному выше для границы (78).

Утверждение 41. *Если B разрешающее множество пространства H_q^n, то $|B| \geq 2\frac{n}{\log_q n}(1 + o(1))$.*

Доказательство. Для произвольной точки $b \in H_q^n$ рассмотрим множество точек

$$S_b = \{x \in H_q^n : |d(b, x) - \frac{q-1}{q}n| < \sqrt{n \ln n}\}$$

Его мощность равна

$$\sum_{i=L-l}^{L+l} C_n^i (q-1)^i = q^n \sum_{i=L-l}^{L+l} C_n^i (\frac{q-1}{q})^i (\frac{1}{q})^{n-i},$$

где $L = (q-1)nq^{-1}$ и $l = \sqrt{n \ln n}$. Из неравенства Хёффдинга [146] для бернулиевских случайных величин следует, что $|S_b| \geq (1 - 2n^{-2})q^n$. Так как $m = |B| \leq n$ для минимального разрешающего множества B, то множество $S(B) = \bigcap_{b \in B} S_b$ имеет мощность не меньше чем $(1-2n^{-1})q^n$. Разным точкам $S(B)$ соответствуют разные векторы расстояний, которых не более чем $(2\sqrt{n \ln n})^m$. Тем самым, $(1 - 2n^{-1})q^n \leq (2\sqrt{n \ln n})^m$ и, следовательно,

$$m \geq 2\frac{n}{\log_q n}(1 + o(1)) \tag{79}$$

Введем ряд обозначений, которые нам понадобятся в дальнейшем. Для произвольных векторов $x, a \in H_q^n$, $x = (x(1), \ldots, x(n))$, $a = (a(1), \ldots, a(n))$ определим их сходство

$$s(x, a) = |\{i : x(i) = a(i)\}| = n - d(x, a) \tag{80}$$

Для произвольного вектора $a \in H_q^n$ определим множество

$$A^\alpha = \{i \in [n] : a(i) = \alpha\}, \tag{81}$$

а для произвольных векторов $x, a \in H_q^N$ определим величину

$$w_{uv}(x, a) = |\{j \in [n] : x(j) = u, a(j) = v\}| = |X^u \bigcap A^v| \tag{82}$$

Нетрудно заметить, что

$$s(x, a) = \sum_{i=0}^{q-1} w_{ii}(x, a) \tag{83}$$

Утверждение 42. *Для метрической размерности $r_{n,3}$ троичного пространства Хэмминга справедливо асимптотическое равенство*

$$m_{n,3} = \frac{2n}{\log_3 n}(1 + o(1))$$

Доказательство. Как уже было отмечено, в [159] были построены множества из $r = \frac{2n}{\log_q n}(1 + o(1))$ двоичных векторов $\{h_i\}$, $i = 1, \ldots, r$ таких, что любой q-ичный вектор x n-мерного евклидова пространства однозначно задается его r скалярными произведениями (x, h_i). Возьмем соответствующее множество $\{h_i : i = 1, \ldots, r\}$ для $q = 3$ и определим вектор b_i как вектор, полученный из вектора h_i заменой всех единиц на двойки. Тогда для любого вектора $b \in B = \{b_1, \ldots, b_r\}$ справедливо

$$s(x, b) = w_{00}(x, b) + w_{22}(x, b)$$

Мы хотим найти величину скалярного произведения (x, h), $h \in \{h_1, \ldots, h_r\}$ через $s(x, b)$ и затем применить результат Линдстрема [159]. Величина (x, h) равна

$$(x, h) = w_{11}(x, h) + 2w_{21}(x, h) = w_{12}(x, b) + 2w_{22}(x, b) \qquad (84)$$

Преобразуя правую часть (84), получаем

$$(x, h) = |B^2| + s(x, b) - |X^0|.$$

Величина $|B^2| = w_{02}(x, b) + w_{12}(x, b) + w_{22}(x, b)$, равная числу единиц в соответствующем векторе h, нам известна. Величина $|X^0| = w_{00}(x, b) + w_{02}(x, b)$ равна числу нулей в векторе x и она узнается за один дополнительный вопрос (чему равно $s(x, 0)$). Таким образом, теорема доказана. □

Пусть $A = \{a_1, \ldots, a_m\}$ и $B = \{b_1, \ldots, b_m\}$ это разрешающие множества мощности m (где без ограничения общности m четно) пространств $H_4^{k_1}$ и $H_2^{2k_2}$ соответственно. С помощью этих множеств мы построим в теореме 2 разрешающее множество мощности $2m+8$ пространства $H_4^{k_1+k_2+\frac{m}{2}}$.

Теорема 14. *Для метрической размерности четверичного пространства Хэмминга справедливо асимптотическое равенство*

$$m_{n,4} = \frac{2n}{\log_4 n}(1 + o(1). \tag{85}$$

Доказательство. Определим следующую операцию Φ: двоичному вектору $\tau = (\tau(1), \ldots, \tau(2k))$ длины $2k$ ставится в соответствие четверичный вектор $\Phi(\tau)$ длины k, так, что

$$\Phi(\tau) = (\varphi(\tau(1), \tau(2)), \varphi(\tau(3), \tau(4)), \ldots, \varphi(\tau(2k-1), \tau(2k))),$$

где

$$\varphi(0,0) = 0, \quad \varphi(0,1) = 1, \quad \varphi(1,0) = 2, \quad \varphi(1,1) = 3.$$

Из двоичного разрешающего множества $B \subset H_2^{2k_2}$ мощности m с помощью операции Φ мы получим множество $C = \{c_1, c_2, \ldots, c_m\}$ той же мощности в пространстве $H_4^{k_2}$.

Определим множество векторов $G = \{g_1, g_2, \ldots, g_{2m+8}\}$ мощности $2m+8$ в пространстве $H_4^{k_1+k_2+\frac{m}{2}}$ следующим образом

В случае $1 \le i \le m/2$

$$g_i(j) = \begin{cases} a_i(j), & \text{если} \quad 1 \le j \le k_1, \\ c_i(j-k_1), & \text{если} \quad k_1+1 \le j \le k_1+k_2, \\ 0, & \text{если} \quad k_1+k_2+1 \le j \le k_1+k_2+m/2. \end{cases} \tag{86}$$

В случае $m/2+1 \le i \le m$

$$g_i(j) = \begin{cases} a_i(j), & \text{если } \ 1 \le j \le k_1, \\ c_i(j-k_1), & \text{если } \ k_1+1 \le j \le k_1+k_2, \\ 1, & \text{если } \ j = k_1+k_2+i-m/2, \\ 0, & \text{для остальных j } \ . \end{cases} \tag{87}$$

В случае $m+1 \le i \le 3m/2$

$$g_i(j) = \begin{cases} a_i(j), & \text{если } \ 1 \le j \le k_1, \\ 3-c_i(j-k_1), & \text{если } \ k_1+1 \le j \le k_1+k_2, \\ 1, & \text{если } \ j = k_1+k_2+i-m, \\ 0, & \text{для остальных j } \ . \end{cases} \tag{88}$$

В случае $3m/2+1 \le i \le 2m$

$$g_i(j) = \begin{cases} a_i(j), & \text{если } \ 1 \le j \le k_1, \\ 3-c_i(j-k_1), & \text{если } \ k_1+1 \le j \le k_1+k_2, \\ 2, & \text{если } \ j = k_1+k_2+i-3m/2, \\ 0, & \text{для остальных j } \ . \end{cases} \tag{89}$$

В случае $2m+1 \le i \le 2m+4$

$$g_i(j) = \begin{cases} i-2m-1, & \text{если } \ 1 \le j \le k_1, \\ 1, & \text{если } \ k_1+1 \le j \le k_1+k_2, \\ i-2m-1, & \text{если } \ k_1+k_2+1 \le j \le k_1+k_2+m/2. \end{cases} \tag{90}$$

В случае $2m+5 \le i \le 2m+8$

$$g_i(j) = \begin{cases} i-2m-5, & \text{если } 1 \le j \le k_1, \\ 2, & \text{если } k_1+1 \le j \le k_1+k_2, \\ i-2m-5, & \text{если } k_1+k_2+1 \le j \le k_1+k_2+m/2. \end{cases} \quad (91)$$

Определим операцию сопряжения в алфавите $\{0,1,2,3\}$ как $\widehat{q} = 3-q$, и соответственно в пространстве H_4^n как $\widehat{a} = (\widehat{a(1)}, \ldots, \widehat{a(n)})$.

Легко видеть, что матрица, составленная из первых $2m$ векторов множества $G = \{g_1, g_2, \ldots, g_{2m+8}\}$, имеет следующую структуру:

$$\begin{pmatrix} A_1 \; C_1 \; 0 \\ A_2 \; C_2 \; E \\ A_1 \; \widehat{C_1} \; E \\ A_2 \; \widehat{C_2} \; 2E \end{pmatrix}$$

где матрицы A_1, C_1 составлены из векторов a_i и c_i для $1 \le i \le m/2$, матрицы A_2, C_2 составлены из векторов a_i и c_i для $\frac{m}{2}+1 \le i \le m$, а E - это единичная матрица размера $m/2 \times m/2$.

Покажем, что любой вектор x из пространства $H_4^{k_1+k_2+\frac{m}{2}}$ определяется однозначно по расстояниям (или сходствам) до векторов множества $G = \{g_1, g_2, \ldots, g_{2m+8}\}$. Разобьем восстанавливаемый вектор x на три части y_1, y_2, z, где компоненты y_i имеют длины k_i, а z имеет длину $m/2$.

Справедливо следующее

Утверждение 43. Для произвольных векторов a и x из пространства H_4^n выполняется равенство

$$s(x,a) + s(x,\widehat{a}) \equiv |X^1| + |X^2| + |A^0| + |A^3| \mod 2.$$

Доказательство. Используя введенные обозначения, имеем

$$s(x,\widehat{a}) = w_{03}(x,a) + w_{12}(x,a) + w_{21}(x,a) + w_{30}(x,a). \qquad (92)$$

Следовательно,

$$\begin{aligned}
&s(x,a) + s(x,\widehat{a}) = \\
&(w_{00}(x,a) + w_{10}(x,a) + w_{20}(x,a) + w_{30}(x,a))+ \\
&(w_{03}(x,a) + w_{13}(x,a) + w_{23}(x,a) + w_{33}(x,a))+ \\
&(w_{10}(x,a) + w_{11}(x,a) + w_{12}(x,a) + w_{13}(x,a))+ \\
&(w_{20}(x,a) + w_{21}(x,a) + w_{22}(x,a) + w_{23}(x,a))- \\
&2(w_{10}(x,a) + w_{20}(x,a) + w_{13}(x,a) + w_{23}(x,a)) = \\
&|X^1| + |X^2| + |A^0| + |A^3|- \\
&2(w_{10}(x,a) + w_{20}(x,a) + w_{13}(x,a) + w_{23}(x,a)).
\end{aligned}$$

Утверждение доказано.

Расстояния от x до последних восьми векторов множества G позволяют определить количество единиц и двоек в y_2. Тогда из Леммы 1 вытекает, что с помощью суммы расстояний от вектора x до i-го и $(i+m)$-го векторов при $i \in [1, m/2]$ можно определить четность суммы $s(z(i),0) + s(z(i),1)$, а с помощью суммы расстояний от вектора x до j-го и $(j+m)$-го векторов при $j \in [m/2+1, m]$ можно определить четность суммы $s(z(i),1) + s(z(i),2)$, где $i = j - m/2$.

Следовательно, мы можем определить *все значения* $z(i)$. Действительно, из того, что $s(z(i),0) + s(z(i),1)$ четно, следует, что $z(i) \in \{2,3\}$, а из того, что $s(z(i),0) + s(z(i),1)$ нечетно, следует, что $z(i) \in \{0,1\}$. Аналогично, из того, что $s(z(i),1) + s(z(i),2)$ четно, следует, что $z(i) \in \{0,3\}$, а из того, что $s(z(i),1) + s(z(i),2)$ нечетно, следует, что $z(i) \in \{1,2\}$.

Утверждение 44. Для произвольных векторов a и x из пространства H_4^N справедливо равенство

$$s(x,a) - s(x,\widehat{a}) + N = s(\Phi^{-1}(x), \Phi^{-1}(a))$$

Доказательство. В силу того, что

$$N = \sum_{i,j} w_{ij}(x,a)$$

получаем

$$\begin{aligned} s(x,a) - s(x,\widehat{a}) + N = \\ (2w_{00}(x,a) + w_{01}(x,a) + w_{02}(x,a) + 0) + \\ (w_{10}(x,a) + 2w_{11}(x,a) + 0 + w_{13}(x,a)) + \\ (w_{20}(x,a) + 0 + 2w_{22}(x,a) + w_{23}(x,a)) + \\ (0 + w_{31}(x,a) + w_{32}(x,a) + 2w_{33}(x,a)) = \\ s(\Phi^{-1}(x), \Phi^{-1}(a)), \end{aligned}$$

что и завершает доказательство.

Теперь рассмотрим разность расстояний от вектора x до i-го и $(i+m)$-го векторов множества G при $i \in [1,m]$. Для неизвестного вектора $x = (y_1, y_2, z)$ мы уже нашли его компоненту z, а так как первые компоненты i-го и $i+m$-го векторов множества G совпадают, то из рассматриваемой разности мы находим разницу расстояний между второй компонентой x до соответствующих частей i-го и $(i+m)$-го векторов множества G. Теперь из утверждения 27 и того, что B это разрешающее множество пространства $H_2^{2k_2}$, находим вектор y_2. Осталось только по значениям $s(x,a)$ восстановить вектор-компоненту y_1, что можно сделать, так как множество A является разрешающим множеством пространства $H_4^{k_1}$.

Теперь из простых рекуррентных соотношений вытекает равенство (85).

Действительно, пусть последовательность разрешающих множеств мощности m_{i+1} пространства $H_4^{k_{1,i+1}}$ строится описанным выше путем, используя двоичные разрешающие множества мощности m_i пространства $H_2^{2k_{2,i}}$. Тогда

$$m_{i+1} = 2m_i + 8,$$

$$k_{1,i+1} = k_{1,i} + k_{2,i} + m_i/2.$$

Если взять

$$m_i = c_1 2^i - 8,$$

$$k_{1,i} = c_1(i - c_2)2^{i-2} + 8,$$

$$k_{2,i} = c_1(i - c_2)2^{i-2} + 4,$$

где $i \geq c_2$, то рекуррентные соотношения будут выполняться. Константы c_1 и c_2 можно взять, к примеру, равными 6 и 3 соответственно, тогда существование двоичных разрешающих множеств нужной мощности следует из (74), а существование разрешающего множества мощности 40 пространства H_4^8 (для начального шага конструкции $i = 3$) следует из (72).

Теорема доказана.

4.2 Адаптивный поиск одного дефектного элемента для аддитивной модели группового тестирования.

В комбинаторном групповом тестировании классической является задача нахождения d дефектных элементов в множестве из N элементов. Результаты теории группового тестирования имеют многочисленные приложения в различных областях, в частности в молекулярной биологии, медицине, теории планирования эксперимента и других. Описание основных результатов и приложений теории группового тестирования можно найти в [89], [131] и [132].

Пусть $[N] := \{1, 2, \ldots, N\}$ множество целых чисел от 1 до N.

Пусть имеется $D \subset [N]$ подмножество, которое мы будем называть множеством дефектных элементов. Обозначим через $d = |D|$ мощность множества D и будем считать, что значение d известно на протяжении всей статьи.

Также обозначим через $[i, j]$ множество целых чисел $\{x \in N : i \leq x \leq j\}$ и через $2^{[N]}$ множество всех подмножеств множества $[N]$.

Обобщая идею из главы два, сформулируем задачу нахождения множества $G \subset [N]$, состоящего из части дефектных элементов и принадлежащему некоторому семейству подмножеств $\Psi = \{G_1, G_2, \ldots G_l\}$. То, каким образом мы будем задавать семейство подмножеств Ψ будет определять новую комбинаторную проблему поиска. В данной работе мы найдем оптимальный ответ для случая $|G_i| = 1$ в аддитивной модели поиска, то есть тогда, когда семейство Ψ состоит из одноэлементных подмножеств.

Для нахождения G, мы можем выбирать в качестве вопросов под-

множества $S_i \subset [N]$ для $1 \leq i \leq n$ и в качестве ответов получать значения $t(S_i)$ некоторой тестовой функции $t : 2^{[N]} \to R$. Отметим, что функция $t(S) = t_D(S)$ зависит от множества дефектов D, но мы для краткости будем в дальнейшем опускать индекс D. По вопросам теста и ответам на них получаем результат теста - множество G.

Определение 12. *Пусть имеются семейство* $\Psi = \{G_1, G_2, \dots G_l\}$ *подмножеств множества* D*, тестовая функция* t*, последовательность* $s = (S_1, S_2, \dots, S_n)$ *подмножеств (вопросов)* $S_i \subset [N]$ *и ответы* $t(s) := (t(S_1), \dots, t(S_n))$.
Назовем $(s, t(s), \Phi(s, t(s)), n)$ *тестом длины* n*, где* Φ *- это некоторое отображение из* $(2^{[N]} \times R)^n$ *в* $2^{[N]}$.
Назовем тест $(s, t(s), \Phi(s, t(s)), n)$ *успешным, если для любого множества дефектов* D *справедливо* $\Phi(s, t(s)) \in \Psi$.

Для классической модели группового тестирования тестовая функция $t : 2^{[N]} \to \{0, 1\}$ определяется следующим образом.

$$t^{(Cla)}(S) = \begin{cases} 0, & \text{если } |S \cap D| = 0, \\ 1, & \text{если } |S \cap D| > 0. \end{cases} \tag{93}$$

Рассмотрим также тестовую функцию

$$t^{(Thr)}(S) = \begin{cases} 0, & \text{если } |S \cap D| < u, \\ 1, & \text{если } |S \cap D| \geq u. \end{cases} \tag{94}$$

Данная модель была впервые рассмотрена в [115] и называется пороговой моделью без зазора.

Для аддитивной модели тестовая функция имеет вид

$$t^{(Add)}(S) = |S \cap D| \tag{95}$$

Классическая проблема группового тестирования состоит в том, чтобы найти неизвестное подмножество D дефектных элементов. Таким образом, в этом случае $\Psi = \{D\}$.

Мы рассмотрим следующие случаи. Каждый случай порождает новую проблему в теории комбинаторного поиска. Пусть $D = \{i_1, \ldots, i_d\}$, где $i_1 < i_2 < \ldots < i_d$.

Случай 1. $\Psi = \{i_1, \ldots, i_d\}$.

Случай 2. $\Psi = \{i_j\}$ для некоторого фиксированного j.

Проблема состоит в построении успешного теста с минимально возможным числом вопросов для всевозможных вариантов ответов (т.е. рассматривается наихудший случай).

Также интересен

Случай 3. $\Psi = \{G_i\}$, $G_i \subset D$, $|G(i)| = m$, $i = 1, 2, \ldots, \binom{d}{m}$,

но мы в этой статье его изучать не будем.

Тест может быть адаптивным и неадаптивным. В неадаптивном тесте все вопросы задаются одновременно. В адаптивном тесте вопрос S_i зависит от результатов $(t(S_1), \ldots, t(S_{i-1}))$. Мы будем рассматривать только адаптивные тесты.

Проблема нахождения минимального числа вопросов в успешном тесте эквивалентна проблеме нахождения максимального числа элементов для которых существует успешный тест длинны n.

Обозначим через $N_{(Cla)}(n, d)$ ($N_{(Thr)}(n, d, u)$) максимальное число элементов, среди которых мы можем найти один дефектный за n вопросов в классической (пороговой) модели.

Как уже отмечалось выше, справедлив следующий результат.

Имеем $N_{(Cla)}(n, d) = 2^n + d - 1$.

Пусть $d \geq u$, тогда $N_{(Thr)}(n, d, u) = 2^n + d - 1$.

Мы рассмотрим модель с аддитивной тестовой функцией. Будет показано, что число элементов среди которых мы можем найти один дефектный элемент за n вопросов совпадает с числом элементов из приведенного результата. Это несколько неожиданно. На первый взгляд кажется, что поскольку количество получаемой информации после ответов на вопросы в аддитивной модели существенно больше, чем для классической модели, то можно воспользоваться этой информацией и увеличить число элементов среди которых мы можем найти один дефектный элемент за n вопросов.

4.3 Поиск произвольного дефектного элемента

В этом параграфе мы рассмотрим аддитивное тестирование. Напомним, что $t^{(Add)}(S) = |S \cap D|$.

Обозначим через $N_{(Add)}(n, d)$ максимальное число элементов среди которых мы можем найти один дефектный элемент за n вопросов (построить успешный тест длины n для случая 1).

Теорема 15. Имеем

$$N_{(Add)}(n, d) = 2^n + d - 1.$$

Доказательство теоремы дадим чуть позже. Поскольку для аддитивной модели после каждого вопроса мы получаем больше информации, чем в классической модели достаточно доказать, что число элементов не может быть больше указанного в теореме. Основную идею этого доказательства проще понять в случае, когда имеется два дефектных элемента (результаты для поиска двух дефектных элементов в классической модели можно найти в работе [23]). Сфор-

мулируем утверждение для случая двух дефектных элементов, расположенных специальным образом, в качестве Леммы.

Лемма 8. Предположим, что один дефектный элемент находится среди первых $2^{r-1}+1$ элементов, а второй дефектный среди последующих $2^{r-1}+1$ элементов для некоторого натурального r. Тогда потребуется как минимум r вопросов для нахождения одного дефектного элемента.

Доказательство Леммы 8.

Рассмотрим множества $T_0 = [1, 2^{r-1}+1]$ и $T_1 = [2^{r-1}+2, 2^r+2]$. В каждом из них содержится по одному дефектному элементу.

Для $r = 1$ утверждение леммы справедливо. Действительно, для множеств $[1, 2]$ и $[3, 4]$ мы не знаем 1-ый, 2-ой, 3-ий или 4-ый элемент дефектный. Потребуется как минимум один вопрос.

Для произвольного натурального r рассмотрим вопрос S, $S \subseteq [1, 2^r+2]$ и обозначим

$T_{01} = S \bigcap T_0$, $T_{00} = T_0 \backslash T_{01}$, $T_{11} = S \bigcap T_1$, $T_{10} = T_1 \backslash T_{11}$.

Предположим, что после ответа на вопрос S нам неким образом будет доступна дополнительная информация: сколько в точности дефектных элементов содержится в множествах T_{01}, T_{00}, T_{11}, T_{10}. Тогда обозначим

$$A = \begin{cases} T_{00}, & \text{если } |T_{01}| \leq |T_{00}| \\ T_{01}, & \text{если } |T_{00}| < |T_{01}|. \end{cases} \tag{96}$$

и

$$B = \begin{cases} T_{10} & \text{если } |T_{11}| \leq |T_{10}| \\ T_{11} & \text{если } |T_{10}| < |T_{11}|. \end{cases} \tag{97}$$

Для произвольного вопроса S возможен такой ответ, что один дефектный элемент находится в множестве A, а второй дефектный элемент находится в множестве B.

Поскольку $|A| \geq 2^{r-2}+1$ и $|B| \geq 2^{r-2}+1$, в наихудшем случае потребуется как минимум r вопросов для нахождения одного дефектного элемента, и утверждение леммы доказано.

Значит, если у нас имеется 2^n+2 элемент, то после вопроса, делящего элементы пополам (что, конечно же необязательно), возможен ответ 1, что приводит нас к ситуации из Леммы 1 с $r = n$ и, следовательно, потребуются еще дополнительно n вопросов. Это показывает, что Лемма 1 является очень частным случаем теоремы, для доказательства которой нам понадобятся следующие обозначения.

Каждое подмножество $S_i \subset N$ взаимно однозначно соответствует последовательности

$$a_i = (a_i(1), a_i(2), \ldots, a_i(N)) \in \{0,1\}^N,$$

где $a_i(j) = 1$, если $j \in S_i$ и $a_i(j) = 0$ в противном случае. Таким образом, мы можем записать последовательность вопросов как матрицу $(a_i(j))_{i=1,\ldots,n;\ j=1,\ldots,N}$ с n строками и N столбцами. Напомним, что в адаптивном тестировании iтая строка определяется по $i-1$ предыдущим строкам и полученным ответам на предыдущие $i-1$ вопросы. Пусть $h_1, h_2, \ldots h_s \in \{0,1\}$. Положим

$$T_{h_1 h_2 \ldots h_s} := \{1 \leq j \leq N : \forall i \in [1,s]\ a_i(j) = h_i\} \qquad (98)$$

Легко видеть, что $N_{(Add)}(n,d) \geq N_{(Thr)}(n,d,1) = 2^n + d - 1$.

Предположим, что $N = 2^n + d$. Покажем, что в наихудшем случае невозможно найти один дефектный элемент за n вопросов.

После r вопросов мы получаем разбиение N элементов по 2^r множествам

$$T_{h_1 h_2 \ldots h_r},\ h_i \in \{0,1\},$$

которые определены выше.

Предположим, что нам стала доступна дополнительная информация - сколько дефектных элементов содержится в каждом множестве $T_{h_1h_2\ldots h_r}$ и обозначим это количество через $D_{h_1h_2\ldots h_r}$.

Если мы докажем, что даже используя дополнительную информацию мы не сможем построить успешный тест длины n, то это будет означать, что и без этой информации невозможно найти один дефектный элемент за n вопросов.

Докажем следующее утверждение, из которого сразу будет следовать теорема.

Для произвольного множества $T_{h_1h_2\ldots h_s}$, содержащего как минимум один дефективный элемент и имеющего мощность

$$|T_{h_1h_2\ldots h_s}| = 2^{n-s} + D_{h_1h_2\ldots h_s}$$

потребуется больше, чем $n - s$ вопросов для нахождения одного дефектного элемента.

Докажем это индукцией по $n - s$.

$n - s = 0$: Легко видеть, что для этого случая $|T_{h_1h_2\ldots h_s}| = 1 + D_{h_1h_2\ldots h_s}$. Значит в множестве $T_{h_1h_2\ldots h_s}$ имеется один не дефектный элемент и невозможно указать дефектный элемент не задавая вопросов.

$n - s = 1$: Легко видеть, что для этого случая $|T_{h_1h_2\ldots h_s}| = 2 + D_{h_1h_2\ldots h_s}$ и в наихудшем случае невозможно определить один дефектный элемент за один вопрос.

Докажем индукционный переход от $n - s$ к $n - s + 1$. Вопрос S_s разбивает каждое множество $T_{h_1h_2\ldots h_{s-1}}$, содержащее дефектные элементы на множества $T_{h_1h_2\ldots h_{s-1}0}$ и $T_{h_1h_2\ldots h_{s-1}1}$.

Возможен такой ответ, что

$$t_{(Add)} = \begin{cases} 0, & \text{если } |T_{h_1h_2\ldots h_s}| \le 2^{n-s} \\ D_{h_1h_2\ldots h_{s-1}}, & \text{если } |T_{h_1h_2\ldots h_s}| \ge 2^{n-s} + D_{h_1h_2\ldots h_{s-1}} \\ |T_{h_1h_2\ldots h_s}| - 2^{n-s}, & \text{в остальных случаях } . \end{cases} \quad (99)$$

(Мы используем то, что $D_{h_1h_2\ldots h_{s-1}1} + D_{h_1h_2\ldots h_{s-1}0} = D_{h_1h_2\ldots h_s}$).

Для третьего случая справедливо $|T_{h_1h_2\ldots h_s}| = 2^{n-s} + D_{h_1h_2\ldots h_s}$ и оба множества $T_{h_1h_2\ldots h_{s-1}1}$ и $T_{h_1h_2\ldots h_{s-1}0}$ содержат дефектные элементы.

Рассмотрим первый или второй случаи.

И вновь предположим, что нам стала доступна дополнительная информация о том, какие элементы не являются дефектными так, что суммарное число этих элементов равно 2^{n-s}. Мы можем больше не рассматривать эти элементы. В оставшемся множестве находятся

$D_{h_1h_2\ldots h_s}$ дефектных элементов и его мощность равна ($h_s = 0$ или $h_s = 1$) величине

$|T_{h_1h_2\ldots h_s}| = 2^{n-s} + D_{h_1h_2\ldots h_s}$.

Следовательно, согласно индукционному предположению, нам понадобится больше, чем $n - s + 1$ вопрос, утверждение доказано.

Мы рассматриваем постановку задачи, в которой изначально известно, что общее число дефектов равно d. Значит тест успешен только когда $N \le 2^n + d - 1$.

А мы перейдем к случаю, когда дефектные элементы упорядочены и мы хотим найти не произвольный дефектный элемент, а какой-то определенный.

4.4 Нахождение j-ого дефектного элемента

Обозначим через $N_{(Add)}(n,d,j)$ максимальное число элементов, среди которых мы можем найти j-ый дефектный элемент за n вопросов (построить успешный тест для проблемы два с тестовой длиной n).

Теорема 16. Имеем для $1 \le j \le d$

$$N_{(Add)}(n,d,j) = 2^n + d - 1.$$

Доказательство

Нахождение jого дефектного элемента d_j не может быть проще нахождения произвольного дефектного элемента.

$$N_{(Add)}(n,d,j) \le N_{(Add)}(n,d) = 2^n + d - 1.$$

Следовательно, нам достаточно построить успешный тест длины $N = 2^n + d - 1$, а то, что нельзя сделать лучше вытекает из теоремы 2.

Докажем по индукции по n, что для произвольного множества T мощности $|T| \le 2^n + x - 1$, содержащего x дефектных элементов мы можем найти d_z за n вопросов для $1 \le z \le x$.

Для $n = 1$ в качестве первого вопроса рассмотрим $S_1 = [1, z]$. Поскольку имеется x дефектных и только один недефектный элемент, то по ответу определяем d_z

$$t^{(Add)}(S_1) = \begin{cases} z-1 & \text{тогда } \ d_z = z+1, \\ z & \text{тогда } \ d_z = z. \end{cases} \qquad (100)$$

Следовательно, индукционная гипотеза справедлива для $n = 1$.

Допустим, что для $n-1$ индукционная гипотеза справедлива и рассмотрим $[N] = [1, 2^n + x - 1]$ элементов среди которых x дефектных, а мы хотим найти d_z для произвольного $1 \leq z \leq x$. Рассмотрим первый вопрос $S_1 = [1, 2^{n-1} + z - 1]$.

Пусть $t^{(Add)}(S_1) = k$. Возможны следующие варианты.

k≥z В этом случае $T' = S_1$, $x' = k$ и $z' = z$.

Следовательно, $|T'| = 2^{n-1} + z - 1 \leq 2^{n-1} + k - 1$. Задача свелась к исходной с параметрами T', x', z' и можно применить предположение индукции.

k<z В этом случае $T' = [N] \backslash S_1$, $x' = x - k$, $z' = z - k$.

Поскольку $T' = [2^{n-1} + z, 2^n + x - 1]$ мы имеем

$|T'| = 2^{n-1} + x - z \leq 2^{n-1} + x - k - 1$. Задача свелась к исходной с параметрами T', x', z' и можно применить предположение индукции для $n-1$ вопроса.

Теорема доказана.

Известно, что для тестов в случае неизвестного D необходимо N тестов для определения одного дефектного элемента или установления их отсутствия. Если D известно, то можно тестировать $N - D$ элементов для нахождения одного дефектного, или же использовать код, свободный от $(D, 1)$ перекрытий, для нахождения всех дефектных элементов и тем самым одного.

Неадаптивная модель для мажоритарного группового тестирования рассматривалась в [70]. В этой работе целью было определение всех дефектных элементов.

Результаты работы [30] для кодов со взвешенными строками могут быть использованы для получения стратегий для тестов, если число дефектных элементов известно.

4.5 Выводы

В данной главе решалась задача определения метрической размерности недвоичного пространства Хэмминга. Основным результатом главы является Теорема 14. В ней доказывается асимптотическое равенство для метрической размерности четверичного пространства Хэмминга.

Кроме того, в третем параграфе данной главы доказывается Теорема 15. Она показывает, что для задачи поиска только одного из d дефектного элемента суммирующая модель не дает преимущества по сравнению с классической моделью.

Результаты данной главы опубликованы в работах [65], [73].

Заключение

В диссертации предложен новый подход к некоторым задачам комбинаторной теории поиска. Эти задачи рассматриваются с точки зрения канала множественного доступа. Благодаря этому подходу удалось перенести некоторые результаты для двоичного канала с обратной связью на q-ичный случай и для дизъюнктивной модели получить более точные верхние границы для скорости кодов, свободных от (w, r) перекрытий. Основные результаты, полученные в диссертации, перечислены ниже.

1. Предложен алгоритм передачи информации по q-ичному каналу с безошибочной обратной связью, который является оптимальным для большой доли ошибок в канале.

2. Предложен алгоритм поиска двух дефектных элементов, улучшающий ранее известные алгоритмы.

3. Построены коды, свободные от (w, r) перекрытий, и доказана оптимальность и единственность некоторых из них.

4. Введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием.

5. Получена верхняя граница на скорость кодов, свободных от (w, r) перекрытий.

6. Для суммирующего канала обобщен результат Линдстрема на случай $q = 3$ и $q = 4$.

7. Получен оптимальный ответ для задачи поиска только одного дефектного элемента для классической и суммирующей модели поиска, когда известно, что дефектных элементов ровно d.

Этот подход может быть применен для дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска. Также результаты работы могут быть использованы в разных практических областях – в практической криптографии, медицине, биологии и др.

Список литературы

[1] Алсведе, Р. Обнаружение одного из D дефектных элементов в некоторых моделях группового тестирования / Р. Алсведе, К. Деппе, В. С. Лебедев // Пробл. передачи информ. – 2012. – Т.48, N 2. – С. 100-109.

[2] Алсведе, Р. Тени, задаваемые отношением слово-подслово / Р. Алсведе, В. С. Лебедев // Пробл. передачи информ. – 2012. – Т.48, N 1. – С. 37-53.

[3] Бассалыго, Л. А. Недвоичные коды, исправляющие ошибки при наличии одноразовой безошибочной обратной связи / Л. А. Бассалыго // Пробл. передачи информ. – 2005. – Т. 41, N 2. – С. 63–67.

[4] Бассалыго, Л. А. Модель ограниченного асинхронного множественного доступа при наличии ошибок / Л. А. Бассалыго // Пробл. передачи информ. – 2009. – Т. 45, N 1. – С. 41–50.

[5] Бассалыго, Л. А. Вычисление асимптотики суммарной пропускной способности M-частотного бесшумного канала с множественным доступом для T пользователей / Л. А. Бассалыго, М. С. Пинскер // Пробл. передачи информ. – 2000. – Т. 36, N 2. – С. 3–9.

[6] Бассалыго, Л. А. Ограниченный асинхронный множественный доступ / Л. А. Бассалыго, М. С. Пинскер // Пробл. передачи информ. – 1983. – Т. 19, N 4. – С. 92–96.

[7] Бассалыго, Л. А. Пропускная способность при нулевой ошибке и наличии общей информации для детерминированных каналов с множественным доступом / Л. А. Бассалыго, М. С. Пинскер, В. В. Прелов // Пробл. передачи информ. – 1982. – Т. 18, N 1. – С. 3–11.

[8] Бассалыго, Л. А. Гиперканал множественного доступа / Л. А. Бассалыго, В. В. Рыков // Пробл. передачи информ. – 2013. – Т. 49, N 4. – С. 3–12.

[9] Балакирский, В. Б. Алгоритм последовательного декодирования в канале множественного доступа / В. Б. Балакирский // Пробл. передачи информ. – 1985. – Т. 21, N 3. – С. 3–13.

[10] Белокопытов, А. Я. Параметризация пропускной способности двоичного суммирующего канала множественного доступа при наличии общей информации / А. Я. Белокопытов // Пробл. передачи информ. – 1988. – Т. 24, N 2. – С. 100–104.

[11] Белокопытов, А. Я. Блоковая передача информации по суммирующему каналу множественного доступа с обратной связью / А. Я. Белокопытов, В. Н. Лузгин // Пробл. передачи информ. – 1987. – Т. 23, N 4. – С. 114–118.

[12] Бобу, А. В. О числе ребер однородного гиперграфа с диапазоном разрешенных пересечений / А. В. Бобу, А. Э. Куприянов, А. М. Райгородский // Пробл. передачи информ. – 2017. – Т. 53, N 4. – С. 16–42.

[13] Бобу, А. В. Асимптотическое исследование задачи о макси-

мальном числе ребер однородного гиперграфа с одним запрещенным пересечением / А. В. Бобу, А. Э. Куприянов, А. М. Райгородский // Матем. сб. – 2016. – Т. 207, N 5. – С. 17–42.

[14] Бурнашев, М. В. Об оптимальных детекторах в задачах обнаружения с многими пользователями / М. В. Бурнашев // Пробл. передачи информ. – 2004. – Т. 40, N 1. – С. 48–57.

[15] Бурнашев, М. В. О функции надежности двоичного симметричного канала с обратной связью / М. В. Бурнашев // Пробл. передачи информ. – 1988. – Т. 24, N 1. – С. 3–10.

[16] Бурнашев, М. В. Передача информации по дискретному каналу с обратной связью. Случайное время передачи / М. В. Бурнашев // Пробл. передачи информ. – 1976. – Т. 12, N 4. – С. 10–30.

[17] Васильева, А. Ю. О совершенных кодах, не включающих кодов Препараты / Д. С. Кротов, А. Ю. Васильева // Пробл. передачи информ. – 2016. – Т. 52, N 3. – С. 92–96.

[18] Введенская, Н. Д. Оценка пропускной способности алгоритмов множественного доступа класса FCFS / Н. Д. Введенская , М. С. Пинскер // Пробл. передачи информ. – 1990. – Т. 26, N 1. – С. 58–67.

[19] Виленкин, Н. Я. Комбинаторика / Н. Я. Виленкин - М, издательство "Наука". – 1969.

[20] Воронина, А. Н. Об объемах сфер для стебельного расстояния

/ А. Н. Воронина // Пробл. передачи информ. – 2010. – Т. 46, N 1. – С. 9-19.

[21] Влэдуц, С.Г. Об исправлении ошибок при искажениях в канале и синдроме / Влэдуц С.Г., Кабатянский Г.А., Ломаков В.В // Пробл. передачи информ. – 2015 – Т. 51, N 2. – С. 50–56.

[22] Голубев, Г. К. О последовательном планировании эксперимента при непараметрическом оценивании гладких функций регрессии / Г. К. Голубев // Пробл. передачи информ. – 1992. – Т. 28, N 3. – С. 76–79.

[23] Деппе, К. Задача группового тестирования с двумя дефектами / К. Деппе, В. С. Лебедев // Пробл. передачи информ. – 2013. – Т. 49, N 4. – С. 87–94.

[24] Дьячков, А.Г. Асимптотика вероятности ошибки при передаче по каналу с белым гауссовским шумом и бесшумной мгновенной обратной связью / А. Г. Дьячков // Пробл. передачи информ. – 1970. – Т. 6, N 1. – С. 33–44.

[25] Дьячков, А.Г. Об оптимальном линейном методе передачи по гауссовскому стационарному каналу без памяти с полной обратной связью / А. Г. Дьячков, М. С. Пинскер // Пробл. передачи информ. – 1971. – Т. 7, N 2. – С. 38–46.

[26] Дьячков, А.Г. Верхние границы вероятности ошибки при передаче с обратной связью для дискретных каналов без памяти / А. Г. Дьячков // Пробл. передачи информ. – 1975. – Т. 11, N 4. – С. 13–28.

[27] Дьячков, А.Г. Границы средней вероятности ошибки для ансамбля кодов с фиксированной композицией / А. Г. Дьячков // Пробл. передачи информ. – 1980. – Т. 16, N 4. – С. 3–8.

[28] Дьячков, А.Г. Границы вероятности ошибки для симметричной модели планирования отсеивающих экспериментов / А. Г. Дьячков // Пробл. передачи информ. – 1981. – Т. 17, N 4. – С. 41–52.

[29] Дьячков, А.Г. Об одной модели кодирования для суммирующего канала с множественным доступом / А. Г. Дьячков, В. В. Рыков // Пробл. передачи информ. – 1981. – Т. 17, N 2. – С. 26–38.

[30] Дьячков, А.Г. Границы длины дизъюктивных кодов / А. Г. Дьячков, В. В. Рыков // Пробл. передачи информ. – 1982. – Т. 18, N 3. – С. 7-13.

[31] Дьячков, А.Г. Улучшение нижней границы длины кодов для суммирующего канала с множественным доступом / А. Г. Дьячков, В. В. Рыков // Пробл. передачи информ. – 1983. – Т. 19, N 4. – С. 103–105.

[32] Дьячков, А.Г. Нижняя граница средней по ансамблю вероятности ошибки для канала множественного доступа / А. Г. Дьячков // Пробл. передачи информ. – 1986. – Т. 22, N 1. – С. 98–103.

[33] Дьячков, А.Г. О ДНК кодах / Дьячков А.Г., Виленкин П.А., Исмагилов И.К., Сарбаев Р.С., Макула А., Торни Д., Уайт С. // Пробл. передачи информ. – 2005. – Т. 41. – N. 4. – С. 57-77.

[34] Дьячков, А.Г. ДНК коды для аддитивного стебельного сходства / Дьячков А.Г., Воронина А. // Пробл. передачи информ. – 2009. – Т. 45. N. 2. – С. 56-77.

[35] Дьячков, А.Г. Границы скорости дизъюнктивных кодов / Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В.Ю. // Пробл. передачи информ. –2014. – Т. 50, N 1. – С. 31–63.

[36] Дьячков, А.Г. Почти дизъюнктивные коды со списочным декодированием / Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В.Ю. // Пробл. передачи информ. – 2015. – Т. 51, N 2. –С. 27–49.

[37] Дьячков, А.Г. Об одной комбинаторной задаче в теории дизъюнктивных кодов / А. Г. Дьячков, Насер Аль Насер // Вестн. Моск. ун-та. Сер. 1. Матем., мех. – 1993. – 4. –С. 30–34.

[38] Дьячков, А.Г. О Bs-последовательностях / А. Г. Дьячков, В. В. Рыков // Матем. заметки. – 1984. – Т. 36, N 4. – С. 593–601.

[39] Егорова, Е. Е. Композиционный канал ограниченного множественного доступа / Е. Е. Егорова, В. С. Потапова // Пробл. передачи информ. – 2018. – Т. 54, N 2. – С. 20–28.

[40] Жигулин, Л. Ф. Экспонента вероятности ошибки в системе с обратной связью при использовании каскадного кода / Л. Ф. Жигулин, В. В. Зяблов // Пробл. передачи информ. – 1973 – Т. 9, N 1. – С. 3–10.

[41] Зигангиров, К. Ш. О числе исправляемых ошибок при переда-

че по ДСК с обратной связью / К. Ш. Зигангиров // Пробл. передачи информ. – 1976. – Т.12, N 2. – С. 3–19.

[42] Зиновьев, В. А. Равновесные коды и тактические конфигурации / Зиновьев В.А, Семаков Н.В. // Пробл. передачи информ. – 1969. – Т. 5, N 3, – С. 28–36.

[43] Зиновьев, В. А. Обобщенные коды Препараты и 2-разрешимые системы четверок Штейнера / В. А. Зиновьев, Д. В. Зиновьев // Пробл. передачи информ. – 2016. – Т. 52, N 2. – С. 15–36.

[44] Зиновьев, В. А. Системы четверок Штейнера S(v,4,3) неполного ранга / В. А. Зиновьев, Д. В. Зиновьев // Пробл. передачи информ. – 2014. – Т. 50, N 3. – С. 76–86.

[45] Зиновьев, В. А. Двоичные совершенные и расширенные совершенные коды длины 15 и 16 с рангами 13 и 14 / В. А. Зиновьев, Д. В. Зиновьев // Пробл. передачи информ. – 2010. – Т. 46, N 1. – С. 20–24.

[46] Зиновьев, В. А. О новых полностью регулярных q-ичных кодах / В. А. Зиновьев, Д. Рифа // Пробл. передачи информ. – 2007. – Т. 43, N 2. – С. 34–51.

[47] Зиновьев, В. А. Двоичные совершенные коды длины 15, построенные обобщенной каскадной конструкцией / В. А. Зиновьев, Д. В. Зиновьев // Пробл. передачи информ. – 2004. – Т. 40, N 1. – С. 27–39.

[48] Зиновьев, В. А. Двоичные расширенные совершенные коды длины 16, построенные обобщенной каскадной конструкцией

/ В. А. Зиновьев, Д. В. Зиновьев // Пробл. передачи информ. – 2002. – Т. 38, N 4. – С. 56–84.

[49] Зиновьев, В. А. Об обобщенных каскадных конструкциях совершенных двоичных нелинейных кодов / В. А. Зиновьев, А. С. Лобстейн // Пробл. передачи информ. – 2000. – Т. 36, N 4. – С. 59–73.

[50] Зиновьев, В. А. Универсальные семейства кодов / В. А. Зиновьев, Г. Л. Кацман // Пробл. передачи информ. – 1993. – Т. 29, N 2. – С. 3–8.

[51] Зиновьев, В. А. О каскадных равновесных кодах, превышающих границу Варшамова-Гилберта / В. А. Зиновьев, Т. Эриксон // Пробл. передачи информ. – 1987. – Т. 23, N 1. – С. 110–111.

[52] Зиновьев, В. А. Об общей конструкции укорочения кодов / В. А. Зиновьев, С. Н. Лицын // Пробл. передачи информ. – 1987. – Т. 23, N 2. – С. 28–34.

[53] Зиновьев, В. А. Об обобщении оценки Джонсона для равновесных кодов / В. А. Зиновьев // Пробл. передачи информ. – 1984. – Т. 20, N 3. – С. 105–108.

[54] Зиновьев, В. А. Обобщенные каскадные коды для каналов с пакетами ошибок и независимыми ошибками / В. А. Зиновьев // Пробл. передачи информ. – 1981. – Т. 17, N 4. – С. 53–62.

[55] Зиновьев, В. А. Исправление пакетов ошибок и независимых ошибок обобщенными каскадными кодами / В. А. Зиновьев, В.

В. Зяблов // Пробл. передачи информ. – 1979. – Т. 15, N 2. – С. 58–70.

[56] Зиновьев, В. А. Коды с неравной защитой информационных символов / В. А. Зиновьев, В. В. Зяблов // Пробл. передачи информ. – 1979. – Т. 15, N 3. – С. 50–60.

[57] Зиновьев, В. А. Обобщенные каскадные коды / В. А. Зиновьев // Пробл. передачи информ. – 1976. – Т. 12, N 1. – С. 5–15.

[58] Зиновьев, В. А. О совершенных кодах / В. А. Зиновьев, В. К. Леонтьев // Пробл. передачи информ. – 1972. – Т. 8, N 1. – С. 26–35.

[59] Зиновьев, В. А. Совершенные и квазисовершенные равновесные коды / Н. В. Семаков, В. А. Зиновьев // Пробл. передачи информ. – 1969. – Т. 5, N 2. – С. 14–18.

[60] Зиновьев, В. А. Эквидистантные q-ичные коды с максимальным расстоянием и разрешимые уравновешенные неполные блок-схемы / Н. В. Семаков, В. А. Зиновьев // Пробл. передачи информ. – 1968. – Т. 4, N 2. – С. 3–10.

[61] Зяблов, В. В. О пропускной способности многопользовательского векторного суммирующего канала / А. А. Фролов, В. В. Зяблов // Пробл. передачи информ. – 2014. – Т. 50, N 2. – С. 20–30.

[62] Зяблов, В. В. О пропускной способности для пользователя системы множественного доступа в векторном дизъюнктивном

канале при наличии ошибок / Д. С. Осипов, А. А. Фролов, В. В. Зяблов // Пробл. передачи информ. – 2013. – Т. 49, N 4. – С. 13–27.

[63] Зяблов, В. В. Система множественного доступа для векторного дизъюнктивного канала / Д. С. Осипов, А. А. Фролов, В. В. Зяблов // Пробл. передачи информ. – 2012. – Т. 48, N 3. – С. 52–59.

[64] Зяблов, В. В. Об оптимальном выборе порога в системе множественного доступа, основанной на перестроении ортогональных частот / В. В. Зяблов, Д. С. Осипов // Пробл. передачи информ. – 2008. – Т. 44, N 2. – С. 23–31.

[65] Кабатянский, Г. А. О метрической размерности недвоичных пространств Хэмминга / Г. А. Кабатянский, В. С. Лебедев // Пробл. передачи информ. – 2018. – Т.54, N 1. – С. 54-62.

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

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

[68] Лебедев, В.С. Замечание о единственности кодов, свободных от (w,r) перекрытий / В. С. Лебедев // Пробл. передачи информ. – 2005. – Т.41, N 3. – С. 17-22.

[69] Лебедев, В.С. Асимптотические границы для скорости окрашенных кодов, свободных от перекрытий / В. С. Лебедев // Пробл. передачи информ. – 2008. – Т.44, N 2. – С. 46-53.

[70] Лебедев, В.С. О перечислении q-ичных последовательностей, содержащих подблок 00 фиксированное число раз / В. С. Лебедев // Пробл. передачи информ. – 2010. – Т.46, N 4. – С. 116-121.

[71] Лебедев, В.С. Разделяющие коды и новая модель комбинаторного поиска / В. С. Лебедев // Пробл. передачи информ. – 2010. – Т.46, N 1. – С. 3-8.

[72] Лебедев, В.С. Кодирование при наличии бесшумной обратной связи / В. С. Лебедев // Пробл. передачи информ. – 2016. – Т.52, N 2. – С. 3-14.

[73] Лебедев, В.С. Адаптивный поиск одного дефектного элемента для аддитивной модели группового тестирования / В. С. Лебедев // Пробл. передачи информ. – 2017. – Т.53, N 3. – С. 78-83.

[74] Леонтьев, В. К. О совершенных кодах в аддитивном канале / В. К. Леонтьев, Г. Л. Мовсисян, Ж. Г. Маргарян // Пробл. передачи информ. – 2008. – Т. 44, N 4. – С. 12–19.

[75] Леонтьев, В. К. О фрагментах слов над q-ичным алфавитом / В. К. Леонтьев, С. А. Мухина // Пробл. передачи информ. – 2008. – Т. 44, N 3. – С. 63–69.

[76] Леонтьев, В. К. О фрагментах слов / В. К. Леонтьев, С. А. Мухина // Пробл. передачи информ. – 2006. – Т. 42, N 3. – С. 73–77.

[77] Леонтьев, В. К. О некоторых метрических задачах в n-мерном кубе / В. К. Леонтьев // Ж. вычисл. матем. и матем. физ. – 2002. – Т. 42, N 2. – С. 249–255.

[78] Лиханов, Н. Б. Алгоритмы случайного множественного доступа в канал, разрешающий одновременную успешную передачу n-1 пакетов и имеющий n-арную обратную связь / Н. Б. Лиханов, И. Плотник, Е. Шавитт, М. Сиди, Б. С. Цыбаков // Пробл. передачи информ. – 1993. – Т. 29, N 1. – С. 82–91.

[79] Лиханов, Н. Б. Верхняя граница для пропускной способности системы случайного множественного доступа пакетов в канал с ошибками / Б. С. Цыбаков, Н. Б. Лиханов // Пробл. передачи информ. – 1989. – Т. 25, N 4. – С. 50–62.

[80] Мак-Вильяме, Теория кодов, исправляющих ошибки. / Мак-Вильяме Ф.Дж.7 Слоэн Н.Дж.А. – М.: Связь, – 1979.

[81] Малютов, М. Б. Последовательный поиск существенных переменных неизвестной функции / М. Б. Малютов, И. И. Цитович // Пробл. передачи информ. – 1997. – Т.33, N 4. – С. 88–107.

[82] Мартиросян, С. С. К построению сигнатурных кодов и задача о взвешивании монет / С. С. Мартиросян, Г. Г. Хачатрян // Пробл. передачи информ. – 1989 – Т. 25, N 4. – С. 96-97.

[83] Пономаренко, Е. И. Новые оценки в задаче о числе ребер гиперграфа с запретами на пересечения / Е. И. Пономаренко, А. М. Райгородский // Пробл. передачи информ. – 2013. – Т. 49, N 4. – С. 98–104.

[84] Прелов, В. В. Передача информации по каналу с множественным доступом при специальной иерархии источников / В. В. Прелов // Пробл. передачи информ. – 1984. – Т. 20, N 4. – С. 3–10.

[85] Прелов, В. В. Об асимптотике пропускной способности некоторых каналов связи / В. В. Прелов // Пробл. передачи информ. – 1966. – Т. 2, N 1. – С. 14–27.

[86] Сагалович, Ю. Л. Полные разделяющие системы / Ю. Л. Сагалович // Пробл. передачи информ. – 1982. – Т. 18, N 2. – С. 74–82.

[87] Сагалович, Ю. Л. Разделяющие системы / Ю. Л. Сагалович // Пробл. передачи информ. – 1994. – Т. 30, N 2. – С. 14–35.

[88] Цитович, И. И. О последовательном планировании экспериментов для различения гипотез / И. И. Цитович // Теория вероятн. и ее примен. – 1984. – Т. 29, N 4. – С. 778–781.

[89] Ahlswede, R. Задачи поиска / Ahlswede R. and Wegener I. – Мир. – 1982.

[90] Ahlswede, R. Channels with arbitrarily varying channel probability functions in the presence of noiseless feedback / Ahlswede R. // Z. Wahrsch. th. u. verw. Geb. – 1973 – 25. – P. 239–252.

[91] Ahlswede, R. Searching with lies under error cost constraints / R. Ahlswede, F. Cicalese, and C. Deppe // General Theory of Information Transfer and Combinatorics, a Special issue of Discrete Applied Mathematics/ – 2008. – 156:9. – P. 1444–1460.

[92] Ahlswede, R. Shadows and isoperimetry under the sequence-subsequence relation / Ahlswede R. and Cai N. // Combinatorica – 1997 – 17 (1). – P. 11–29.

[93] Ahlswede, R. Non-binary error correcting codes with noiseless feedback, localized errors, or both / R. Ahlswede, C. Deppe, V. Lebedev // Annals of the European Academy of Sciences. – 2005. – No. 1. – P. 285-309.

[94] Ahlswede, R. Non-binary error correcting codes with noiseless feedback / R. Ahlswede, C. Deppe, V. Lebedev // Proc. Tenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod (Russia), September 3-9. – 2006. – P. 7-10.

[95] Ahlswede, R. Shadows under the word-subword relation / R. Ahlswede, V. Lebedev // Proc. Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, Novosibirsk (Russia), September 5-11. – 2010. – P. 16-19.

[96] Ahlswede, R. Bounds for threshold and majority group testing / R. Ahlswede, C. Deppe, V. Lebedev // 2011 IEEE International Symposium on Information Theory, Sankt-Peterburg, Russia, Aug. 1-5. – 2011. – P. 69-73.

[97] Ahlswede, R. Finding one of D defective elements in some group

testing models / R. Ahlswede, C. Deppe, V. Lebedev // Proc. Thirteenth Int. Workshop on Algebraic and Combinatorial Coding Theory. Pomorie, Bulgaria. June 15-21. – 2012. – P. 15-20.

[98] Aigner, M. Searching with lies / M. Aigner // J. Comb.Theory, Ser.A. – 1996. – 74 – P. 43–56.

[99] Aigner, M. Ulams Millionenspiel / M. Aigner // Math. Semesterber. – 1995. – 42 – P. 71–80.

[100] Aydinian H., Cicalese F., Deppe C., Lebedev V., A Combinatorial Model of Two-Sided Search / Aydinian H., Cicalese F., Deppe C., Lebedev V. // International Journal of Foundations of Computer Science. – 2018. – V. 29, N. 4. – P. 481-504.

[101] Bar-Lev, S.K. Incomplete Identification Models for Group-Testable Items / Bar-Lev S.K., Boneh A., Perry D. // Naval Res. Logistics. – 1990. – V. 37, N. 5 – P. 647–659.

[102] Beluhov, N. Search for a moving target in a graph / Beluhov N. Kolev E. // Electronic Notes in Discrete Mathematics – 2017. – V. 57, P. 39–46.

[103] Berlekamp, C. R. Block coding with noiseless feedback / C. R. Berlekamp // Doctoral dissertation, MIT. – 1964.

[104] Brualdi R. A. Introductory combinatorics / R. A. Brualdi // Elsever North-Holland/ – 1977.

[105] Bultermann, J. A new upper bound for the isoperimetric numbers

of de-Bruijn networks / J. Bultermann // Appl. Math. Lett. – 1997 – V. 10, N. 6. – P. 97–100.

[106] Cantor, D. Determining a subset from a certain combinatorial properties / Cantor D., Mills W. // Canadian J. Math. – 1966 – V.18. – P. 42–48.

[107] Chang, S.C. Coding for T-user multiple access channels / Chang S.C. and Weldon E.J. // IEEE Trans. Inform. Theory. –1979 – V. 25 (6). – P. 684-691.

[108] Chang, G.J. A group testing problem on two disjoint sets / Chang G.J. and Hwang F.K. // SIAM J. Algebraic Discr. Methods. – 1981. – V.2. P. 35-38.

[109] Chang, G.J. Group testing with two defectives / Chang G.J., Hwang F.K., and Lin S. // Discrete Applied Math. – 1982. – V. 4, N. 2. – P. 97-102.

[110] Chang G.J. Group testing with two and three defectives / Chang G.J., Hwang F.K., and Weng J.F. // Graph Theory and Its Applications: East and West, ed.Capobianco. The New York Academy of Sciences, New York. – 1989. – P. 86-96.

[111] Colborn, C. J. CRC Handbook of Combinatorial Designs / C. J. Colbourn, and J. H. Dinitz // CRC Press, Inc., – 1996.

[112] Cicalese, F. Fault-tolerant search algorithms / F. Cicalese // Springer-Verlag Berlin Heidelberg. – 2013.

[113] Cicalese, F. Perfect two-fault tolerant search with minimum adaptiveness / F. Cicalese, D. Mundici // Adv. Appl. Math. –2000. – V. 25, N.1. – P. 65-101.

[114] Cicalese, F. Quasi-Perfect minimally adaptive q-ary search with unreliable tests / F. Cicalese and C. Deppe // Algorithms and Computation, Lecture Notes in Computer Science, Springer Verlag. – 2003. – P. 527-536.

[115] Damaschke, P. Threshold group testing, General Theory of Information Transfer and Combinatorics / P. Damaschke // Lecture Notes in Computer Science, Springer Verlag. – 2006. – V. 4123. – P. 707-718.

[116] Deppe, C. Solution of Ulam's searching game with three lies or an optimal adaptive strategy for binary three-error-correcting-codes / C. Deppe // Discrete Math. – 2000. – V. 224, 3. – P. 79-98.

[117] Deppe, C. Bounds for the capacity error function for unidirectional channels with noiseless feedback / C. Deppe, V. Lebedev, G. Maringer // Theoretical Computer Science. –2021. – 856. – P. 1-13.

[118] Deppe, C. Algorithms for q-ary error-correcting codes with limited magnitude and feedback / C. Deppe, V. Lebedev // Discrete Mathematics. –2021. – 344 (2). – P. 112199.

[119] Deppe, C. Multiaccess problem with two active users / C. Deppe, V. Lebedev // Proc. Fourteenth International Workshop on Al-

gebraic and Combinatorial Coding Theory, Svetlogorsk (Russia), September 7-13. – 2014. – P. 133-138.

[120] Deppe, C. Optimal Algorithms for Q-ary Error-Correcting Feedback Codes with Limited Magnitude / C. Deppe, V. Lebedev // Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT. – 2018. –P. 64-67.

[121] Deppe, C. Q-ary Error-Correcting Codes with Feedback / C. Deppe, V. Lebedev // Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT. – 2018. – P. 68-71.

[122] Deppe, C. Algorithms for Q-ary Error-Correcting Codes with Partial Feedback and Limited Magnitude / C. Deppe, V. Lebedev // International Symposium on Information Theory (ISIT), IEEE, Jul. – 2019. – P. 2244-2248.

[123] Deppe, C. How to apply the rubber method for channels with feedback / C. Deppe, V. Lebedev, G. Maringer // Proc. Algebraic and Combinatorial Coding Theory (ACCT), IEEE. – 2020. – P. 73-76.

[124] Deppe, C. Bounds for the capacity error function for unidirectional channels with noiseless feedback / C. Deppe, V. Lebedev, G. Maringer // IEEE International Symposium on Information Theory (ISIT), IEEE, Jun – 2020. – P.2061-2066.

[125] D'yachkov, A. G. A Survey of Superimposed Code Theory / D'yachkov A. G., Rykov V. V. // Prob. of Control and Inform. Theory. – 1983. – V.12, N4. – P. 229-242.

[126] D'yachkov, A. G. Superimposed Distance Codes / D'yachkov A. G., Rykov V. V., Rashad A. M. // Problems of Control and Inform. Theory. – 1989 – V.18,N4. – P. 237-250.

[127] D'yachkov, A. G. New results in the theory of superimposed codes / A. D'yachkov, A. Macula, D. Torney, P. Vilenkin, S. Yekhanin // Seventh International Workshop on Algebraic and Combinatorial Coding Theory, June 18-24., Bansko (Bulgaria) – 2000 – P. 126-136.

[128] D'yachkov, A. G. Families of Finite Sets in which No Intersection of l Sets is Covered by the Union of s Others / A. D'yachkov, A. Macula, D. Torney, P. Vilenkin // J. Combin. Theory Ser. A. – 2002 – V. 99. – P. 195-218.

[129] D'yachkov, A. G. Upper Bounds on the Rate of Superimposed (s,l)-Codes Based on Engel's Inequality / D'yachkov A., Vilenkin P., Yekhanin S. // Eighth International Workshop on Algebraic and Combinatorial Coding Theory, September 8-14., Tsarskoe Selo (Russia). – 2002 – P. 95-99.

[130] Delorme, C. The spectrum of de Bruijn and Kautz / Delorme C., Tillich J-P. // Graphs, Europ. J.Combinatorics. – 1998. – 19. – P. 307-319.

[131] Du, D.Z. Combinatorial Group Testing and its Applications, 2nd edition / Du D.Z. and Hwang F.K. // World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, Series on Applied Mathematics. – 2000. – 12.

[132] Du, D.Z. Pooling Designs and Nonadaptive Group Testing. Important Tools for DNA Sequencing. / Du D.Z. and Hwang F.K. // World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, Series on Applied Mathematics. – 2006.– 18.

[133] Engel, K. Interval Packing and Covering in the Boolean Lattice. / Engel K. // Combinatorics Prob. and Computing. – 1996. – V. 5 – P. 373-384.

[134] Erdos, P. On two problems of information theory / Erdos P. and Renyi A. // Publ.Math. Inst. Hung. Acad.Sci. – 1963. – V.8. – P. 241-254.

[135] Erdos, P. Families of Finite Sets in Which No Set Is Covered by the Union of two Others / P. Erdos, F. Frankl, F. Furedi // J. Combin. Theory, Ser. A, – 1982. – V. 33 – P. 158-166.

[136] Erdos, P. Families of Finite Sets in which No Set Is Covered by the Union of r Others / P. Erdos, F. Frankl, F. Furedi // Israel Journal of Math. – 1985. – V. 51, N. 1-2. – P. 75-89.

[137] Garey, M.R. Isolating a single defective using group testing / Garey M.R. and Hwang F.K. // J. Amer. Statist. Assoc. – 1974. – V.69. – P. 151-153.

[138] Guibas, L.J. String overlaps, pattern matching and nontransitive games / Guibas L.J., Odlyzko A.M. // J. Combin. Theory Ser. A. – 1981. – V. 30, N. 2. – P. 183-208.

[139] Graham Handbook of combinatorics / Graham, Grotschel and Lovasz // MIT Press. – 1995. – V. 2.

[140] Gerbner, D. Search with Density Tests / Gerbner D., Keszegh B., Palvolgyi D. // Search Methodologies II (ZiF Workshop. Bielefeld, Germany. October 25-29. – 2010. – P. 33.

[141] Gronau, H.-D.O.F On super-simple $2-(v, 4, \lambda)$ designs / H.-D.O.F Gronau, R.S.Mullin // J.Combin. Math. Combin. Comput. – 1992. – V. 11. – P. 113-121.

[142] Harary, F. On the metric dimension of a graph / Harary F. and Meter R. // Ars Combinatorica. – 1976. – V.2. – P. 191-195.

[143] Hill, R. Searching with lies / R. Hill // Surveys in Combinatorics, Lecture Note Series. 1995. – V. 218. – P. 41-70.

[144] Hwang, F. K. Non adaptive hypergeometric group testing / Hwang F. K., Sos V. Z. // Studia Sci. Math. Hungarica, – 1987. – V. 22. – P. 257-263.

[145] Heubach, S. Combinatorics of compositions and words / Heubach S., Mansour T. // CRC Pres – 2009.

[146] Hoeffding, W. Probability inequalities for sums of bounded random variables / W. Hoeffding // Journal of the American Statistical Association. – 1963. – 58 (301). – P. 13-30.

[147] Chvatal, V. Mastermind / Chvatal V. // Combinatorica. – 1983. – V.3. – P. 325-329.

[148] Kabatianski, G. The Mastermind game and the rigidity of the Hamming space / G. Kabatianski, V. Lebedev, J. Thorpe // Proc. IEEE Int. Symp. Inform. Theory. – 2000. – P. 375.

[149] Kautz, W. H. Nonrandom Binary Superimposed Codes / W. H. Kautz, R. C. Singleton // IEEE Trans. Inform. Theory – 1964. – V. IT-10, N 3. – P. 363-377.

[150] Kapralov, S. On the (2,2) Superimposed Codes of Length 18 / S. Kapralov // Proc. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory. Kranevo, Bulgaria. June 19-25. – 2004. – P. 236-240.

[151] Kim, H.K. On Optimal Superimposed Codes / H.K. Kim , V. S. Lebedev // J. Combin. Des. – 2004. – V. 12, N 2. – P. 79-91.

[152] Kim, H.K. Some New Results on Superimposed Codes / H.K. Kim , V. S. Lebedev, D.Y. Oh // J. Combin. Des. – 2005. – V. 13. – P. 276-285.

[153] Kim, H.K. Uniqueness of Some Optimal Superimposed Codes / H.K. Kim , V. S. Lebedev // Proc. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory. Kranevo, Bulgaria. June 19-25. – 2004. – P. 241-246.

[154] Koopman, B. Search and screening / B. Koopman // Persimmon Press, New York – 1946.

[155] Kumar, S. Finding a Single Defe tive in Binomial Group-Testing / Kumar S., Sobel M. // J. Amer. Statist. Asso. – 1971. – V. 66, N. 336. – P. 824-828.

[156] Lebedev, V. S. Some tables for (w,r) superimposed codes / V. S. Lebedev // Proc. Eighth International Workshop on Algebraic and

Combinatorial Coding Theory, Tsarskoe Selo (Russia), September 8-14. – 2002. – P. 185-189.

[157] Lebedev, V. S. Colored Superimposed Codes / V. S. Lebedev // Proc. Eleventh Int. Workshop on Algebraic and Combinatorial Coding Theory. Pamporovo, Bulgaria. June 16-22. – 2008. – P. 177-180.

[158] Lindstrom, B. On a combinatorial detection problem,I / B. Lindstrom // Publ.Math. Inst. Hung. Acad.Sci. – 1964. – V.9. – P. 195-207.

[159] Lindstrom, B. On a combinatorial problem in number theory / B. Lindstrom // Canad. Math. Bull. – 1965. – V. 8, N. 4. – P. 477-490.

[160] Malinowski, A. K-ary searching with a lie / A. Malinowski // ARS Combin. –1994. – V. 37. – P. 301-308.

[161] Mitchell, C. J. Key storage in secure networks / C. J. Mitchell and F. C. Piper // Discrete Applied Mathematics – 1988. – V. 21. P. 215-228.

[162] Pelc, A. Solution of Ulam's problem on searching with a lie / A. Pelc // J. Combin.Theory, Ser.A. – 1987. – 44. P. 129-140.

[163] Pelc, A. Searching games with errors – fifty years of coping with liars / A. Pelc // Theoret. Comput. Sci. – 2002. – V. 270. – P. 71–109.

[164] Raigorodskii, A.M. Combinatorial geometry and coding theory /

A.M. Raigorodskii // Fundamenta Informatia. – 2016. – V. 145. – P. 359-369.

[165] Renyi, A. On a problem of information theory / A. Renyi // MTA Mat. Kut. Int. Kozl. – 1961. – 6B. – P. 505-516.

[166] Shannon, C. E. The zero-error capacity of a noisy channel / C. E. Shannon // IRE Trans. Inform. Th. – 1956. – 3. – P. 3-15.

[167] Shannon, C. E. Two-way communication channels / C. E. Shannon // Proc. 4th Berkeley Sympos. Math. Statist. and Prob., – 1961. – V. I. – P. 611–644.

[168] Sobel, M. Binomial and hypergeometric group testing / M. Sobel // Studia Sci. Math. Hungar. – 1968. – V.3. – P. 19-42.

[169] Slatter, P. Leaves on trees / P. Slatter // Cong. Numer. – 1975. – V.14. – P. 549-599.

[170] Stinson, D. R. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption / D. R. Stinson // Designs, Codes and Cryptography. – 1997. – V. 12, N. 3. – P. 215-243.

[171] Stinson, D. R. New Constructions for Perfect Hash Families and Related Structures using Combinatorial Designs and Codes / D.R. Stinson, R.Wei, L. Zhu // J. Combinatorial Designs. – 2000. – V. 8. – P. 189-200.

[172] Stinson, D. R. Some new bounds for cover-free families / D.R. Stinson, R.Wei, L. Zhu // J. Combin. Theory Ser. A. – 2000. – V. 90. – P. 224-234.

[173] Tosic, R. An optimal search procedure / R. Tosic // Journal of Statistical Planning and Inference. – 1980. – V. 4. N. 2. – P. 169-171.

[174] Ulam, S.M. Adventures of a mathematician / S. M. Ulam // Charles Scribner's Sons, New York. – 1976.

[175] Weng, S.Y. The Research of Group Testing Questions in (2,n) / S.Y. Weng // master-thesis, National Central University, Taiwan. – 1999.