РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Журнал основан в январе 1965 г. **ISSN: 0555-2923** **Выходит 4 раза в год**

Том 57, 2021 **Вып. 1**

Январь–Февраль–Март

М о с к в а

С О Д Е Р Ж А Н И Е

Теория информации

Шеной К.Г., Шарма В. Анализ каналов со сбором энергии при конечной длине блока . . 3

Бенерджи К.Г., Гупта М.К. Компромиссное соотношение между стоимостью хранения и восстановления для неоднородных распределенных систем хранения данных 40

Прелов В.В. f-дивергенция и склеивание вероятностных распределений 64

Теория кодирования

Зиновьев В.А., Зиновьев Д.В. Об обобщенной каскадной конструкции кодов в модульной метрике и метрике Ли 81

Патанкер Н., Сингх С.К. Аффинные эвалюационные коды по гиперэллиптической кривой 96

CONTENTS

Information Theory

Shenoy, K.G. and Sharma, V., Finite Blocklength Analysis of Energy Harvesting Channels . . 3
Benerjee, K.G. and Gupta, M.K., Trade-off for Heterogeneous Distributed Storage Systems between Storage and Repair Cost 40
Prelov, V.V., The f-Divergence and Coupling of Probability Distributions 64

Coding Theory

Zinoviev, V.A. and Zinoviev, D.V., On the Generalized Concatenated Construction for Codes in L_1 and Lee Metrics 81
Patanker, N. and Singh, S.K., Affine Variety Codes over a Hyperelliptic Curve 96

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 1**

УДК 621.391 : 519.724

© 2021 г. **К.Г. Шеной, В. Шарма**

АНАЛИЗ КАНАЛОВ СО СБОРОМ ЭНЕРГИИ ПРИ КОНЕЧНОЙ ДЛИНЕ БЛОКА[1]

Рассматриваются каналы с аддитивным белым гауссовским шумом и дискретные каналы без памяти, в которых на передающем конце применяется сбор энергии из окружающей среды. Такими каналами можно моделировать беспроводные сенсорные сети, а также так называемый "интернет вещей". С помощью предлагаемого единого подхода, справедливого для любого канала со сбором энергии, такие каналы исследуются при условии бесконечного накопителя энергии, а также приводятся соответствующие границы достижимости и верхние границы на пропускную способность канала в режиме конечной длины блока. Кроме того, приводятся также асимптотические границы умеренных уклонений.

Ключевые слова: достижимые скорости, обратная теорема кодирования, пропускная способность канала, конечная длина блока, СЭ-АБГШ-каналы, СЭ-ДКБП, умеренные уклонения.

DOI: 10.31857/S0555292321010010

§ 1. Введение

В теоретико-информационном анализе каналов пропускной способностью канала называется наибольшая скорость, с которой источник может передавать сообщения приемнику при условии сколь угодно малой вероятности ошибки. Однако подойти сколь угодно близко к пропускной способности канала можно лишь при использовании кодов с очень большой длиной блока. На практике же длина блока ограничена, и поэтому желательно изучить величину отклонения от пропускной способности, а также изменение максимального объема кода, как функцию от длины блока. Для фиксированной вероятности ошибки изучение достижимых скоростей при конечной длине блока с особым вниманием к коэффициентам второго порядка известно в литературе как анализ вторых приближений.

Как и для обычной пропускной способности, характеризация пропускной способности канала при конечной длине блока состоит из двух вопросов, а именно: граница достижимости для максимального объема кода (числа сообщений) M и обратная теорема кодирования. При заданной вероятности ошибки в вопросе о достижимости обычно исследуется существование кода с помощью рассуждений, основанных, например, на случайном кодировании или оперировании общими границами достижимости, показывающими, что та или иная граница достигается. С другой стороны, обратная теорема кодирования – это верхняя граница на максимальный объем кода, которая должна выполняться для любого возможного кода. В настоящей статье рассматриваются оба вопроса для каналов со сбором энергии.

[1] Часть результатов настоящей статьи была представлена в [1].

Каналы и сети со сбором энергии (СЭ-каналы и СЭ-сети) привлекают в последнее время значительное внимание благодаря прогрессу в области беспроводных сенсорных сетей и средств связи, основанных на альтернативной энергии (см. [2–4]). Передача символов требует затрат энергии на приемном конце. Поэтому исследование канала производится в тандеме с системой сбора энергии. Система сбора энергии моделируется как буферная или перезаряжаемая батарея, в которой накапливается энергия, поступающая из некоторого внешнего источника (например, солнечная энергия). Такой накопитель энергии может иметь как конечную, так и бесконечную емкость, а процесс поступления энергии может быть как дискретным, так и непрерывным. Задача, представляющая интерес, заключается в сравнении производительности каналов с системой сбора энергии и без таковой (например, можно ли количественно оценить влияние на пропускную способность канала, пропускную способность при конечной длине блока и т.д.).

Анализ для дискретных каналов без памяти (ДКБП) при конечной длине блока впервые был выполнен в [5]. Неасимптотические результаты о вторых приближениях для каналов с аддитивным белым гауссовским шумом (АБГШ-каналов), а также для некоторых других типов каналов, был представлен в [6, 7]. Затем в [7, 8] изучались приближения третьего порядка и было выведено метаобращение теоремы кодирования – результат, включающий в себя и улучшающий известные обратные теоремы кодирования. Более точные результаты для различных ДКБП были получены в [9]. Неасимптотический анализ для каналов с состояниями был выполнен в [10]. В постановке задачи со сбором энергии в предположении бесконечной емкости накопителя пропускная способность для СЭ-АБГШ-каналов была получена в [11, 12]. Границы достижимости при конечной длине блока для двоичных каналов без шума со сбором энергии были получены в [13]. Результат о достижимости для СЭ-АБГШ-каналов с членом второго порядка $O(\sqrt{n})$ представлен в [1]. Как границы достижимости, так и обратные результаты для СЭ-АБГШ-каналов были недавно улучшены в работе [14], где рассматривался процесс поступления энергии с н.о.р. блоками.

Помимо анализа при конечной длине блока мы также приводим границы на коэффициент умеренных уклонений для СЭ-АБГШ-каналов и СЭ-ДКБП. В этой постановке рассматривается передача со скоростями, меньшими пропускной способности, где отклонение от пропускной способности стремится к нулю при некоторой скорости, называемой режимом умеренного уклонения. В этом режиме вероятность ошибки будет стремиться к нулю с ростом длины блока n. Целью является характеризация экспоненты вероятности ошибки для умеренных уклонений. Анализ умеренных уклонений для каналов без памяти был выполнен в [15, 16]. В [16] коэффициент умеренных уклонений был охарактеризован через дисперсию канала. Для ДКБП с обратной связью переменной длины анализ умеренных уклонений был проведен в [17].

Основные результаты. В статье предложена схема, позволяющая непосредственно вычислить достижимые скорости для широкого класса каналов со сбором энергии. Мы сосредоточимся на анализе СЭ-АБГШ-каналов и СЭ-ДКБП с бесконечным буфером. В частности,

1. Получены достижимые скорости при конечной длине блока для СЭ-АБГШ-каналов и СЭ-ДКБ в предположении фиксированной максимальной вероятности ошибки. Показано, что схема накопления и передачи (save and transmit), где фаза накопления имеет длину $O(\sqrt{n})$, достаточна для обеспечения надежной связи в постановке со сбором энергии. При сравнении со случаем без сбора энергии (но с эквивалентным ограничением по средней мощности) видно, что член второго порядка по-прежнему равен $\Theta(\sqrt{n})$. Отметим, что коэффициенты при членах второго порядка не обязательно будут одинаковыми.

2. Далее, приведена обратная теорема кодирования при конечной длине блока, т.е. верхняя граница на достижимые скорости для СЭ-АБГШ-каналов. Она выводится модификацией метаобращения теоремы кодирования из [7] для конкретного случая СЭ-АБГШ-каналов. Для случая квазистатических каналов с замиранием в [18] желаемые границы также были получены с помощью модификации этого метаобращения. Более того, мы даем альтернативное, более короткое доказательство верхней границы для СЭ-АБГШ-каналов, впервые полученной в [14]. Кроме того, проведен анализ ДКБП со сбором энергии и для них получены верхние границы при конечной длине блока. Анализ как границы достижимости, так и обратной теоремы кодирования в этом контексте для СЭ-ДКБП является новым. Мы можем показать, что и в границе достижимости, и в нижней границе член второго порядка для СЭ-АБГШ-каналов и СЭ-ДКБП равен $O(\sqrt{n})$. Как следствие, это также дает сильную обратную теорему кодирования для таких каналов, поскольку вероятность ошибки не влияет на член первого порядка. Кроме того, наши результаты распространены на случай, когда последовательность сообщений посылается в системе, где можно использовать остаточную энергию от предыдущей передачи.
3. Далее, приведены нижние и верхние границы умеренных уклонений для обоих типов каналов. Для этого показывается, что границы на дисперсии канала, полученные при доказательстве границ для конечной длины блока, также являются границами на коэффициент умеренных отклонений. Эти границы для каналов со сбором энергии являются новыми, т.е. не представлены в других источниках. Наконец, построены графики наших нижних и верхних границ скорости для некоторых значений параметров и сделаны соответствующие выводы.
4. И наконец, построены графики наших границ при конечной длине блока для СЭ-АБГШ-каналов в режимах малого, среднего и большого отношения сигнал/шум и проведено их сравнение с эквивалентным АБГШ-каналом без сбора энергии. Для СЭ-ДКБП в качестве примера взяты двоичный симметричный канал со сбором энергии (СЭ-ДСК) и двоичный канал со стиранием (ДКС) со сбором энергии, и результаты для них приведены в виде соответствующих графиков. Кроме того, обсуждаются случаи, когда на графиках выявляются нетривиальные факты о скоростях в канале.

После этого, в § 10, наши результаты и методы подробно сравниваются с результатами и методами из [14, 18].

§ 2. Предварительные сведения

2.1. Основные обозначения. Полужирными символами (например, $\boldsymbol{x}$) обозначаются векторы (пространства $\mathbb{R}^n$ с заданным $n \in \mathbb{N}$). Когда требуется явно указать длину вектора, будем указывать это в виде $\boldsymbol{x}^k = (x_1, x_2, \ldots, x_k)$. Аналогично, $\boldsymbol{x}_i^j = (x_i, x_{i+1}, \ldots, x_j)$. Строчными буквами обозначаются детерминированные скалярные или векторные величины, а прописными – случайные величины или случайные векторы соответственно. Через $[M]$ будем обозначать множество $\{1, 2, \ldots, M\}$. Через $\mathcal{P}(\mathcal{X})$ будем обозначать множество распределений вероятностей на $\mathcal{X}$ (в случаях, когда алфавит очевиден, будем писать просто $\mathcal{P}$). Оператор математического ожидания обозначается через $\mathbf{E}$, а если необходимо указать распределение (скажем, P), то через $\mathbf{E}_P$. Время от времени для указания порядков величин будем использовать символику Бахмана – Ландау $O(\cdot)$, $\Theta(\cdot)$ и т.д. Все логарифмы по умолчанию по основанию 2, но иногда при необходимости явно указывается основание.

2.2. Каналы, вероятность ошибки и пропускная способность. Для заданных алфавита на входе $\mathcal{X}$ и алфавита на выходе $\mathcal{Y}$ *каналом*, обозначаемым через $W(y\,|\,x)$ или, эквивалентным образом, через $P_{Y\,|\,X}$, называется условная вероятностная мера

на $\mathcal{Y}$ при условии $x \in \mathcal{X}$. Если для канала существует плотность распределения, она обозначается через $f_{Y|X}$.

Для заданного распределения вероятностей P на $\mathcal{X}$ и канала W определим выходную меру PW как

$$PW(y) = \sum_{x \in \mathcal{X}} P(x)W(y\,|\,x).$$

Есть два понятия вероятности ошибки, которые мы будем использовать. Пусть задан код $\mathcal{C}$ с M сообщениями, и пусть $U \in [M]$ – случайная величина, равномерно распределенная на $[M]$, обозначающая передаваемое сообщение, а $\widehat{U} \in [M]$ – сообщение, декодированное на приемном конце. *Максимальной вероятностью ошибки* для кода $\mathcal{C}$ называется величина

$$P_{e,\max}(\mathcal{C}) := \max_{1 \leqslant m \leqslant M} \Pr\bigl[\widehat{U} \neq m\,|\,U = m\bigr]. \tag{1}$$

Аналогично, *средняя вероятность ошибки* определяется как

$$P_{e,\mathrm{avg}}(\mathcal{C}) := \frac{1}{M} \sum_{m=1}^{M} \Pr\bigl[\widehat{U} \neq m\,|\,U = m\bigr]. \tag{2}$$

Пропускная способность канала одинакова в обоих случаях. Однако в режиме с конечной длиной блока имеются отличия в членах высших порядков, что приводит к разнице в $O(\log n)$ (см. [7]). В настоящей статье мы будем придерживаться критерия максимальной вероятности ошибки, поскольку он более удобен при анализе ДКБП со сбором энергии. По техническим соображениям границы, использующие максимальную вероятность ошибки, обычно требуют работы с последовательностями, в отличие от средней вероятности ошибки, где нужно работать с распределениями.

Будем называть (n, M, ε)-кодом код с M кодовыми словами длины n и вероятностью ошибки не выше ε. Положим

$$M^*(n, \varepsilon) := \max\{M : \text{существует } (n, M, \varepsilon)\text{-код}\}.$$

Для заданного (n, M, ε)-кода величина $\dfrac{\log M}{n}$ называется его *скоростью*. Для $0 < \varepsilon < 1$ определим *ε-пропускную способность* C_ε как

$$C_\varepsilon = \lim_{n \to \infty} \frac{\log M^*(n, \varepsilon)}{n}$$

и назовем *пропускной способностью* канала величину

$$C = \lim_{\varepsilon \to 0} C_\varepsilon.$$

Заметим, что оба предела существуют. Ясно, что $C_\varepsilon \geqslant C$. Однако для некоторых классов каналов, таких как ДКБП и обычные АБГШ-каналы с ограничением по средней мощности, имеет место равенство $C_\varepsilon = C$ для любых $0 < \varepsilon < 1$. Тогда будем говорить, что канал удовлетворяет *сильному обращению теоремы кодирования*, что означает, что если вести передачу со скоростями выше пропускной способности, то вероятность ошибки для кода будет стремиться к 1 при длине блока n, стремящейся к бесконечности.

Для заданного $0 < \varepsilon < 1$ и любого канала пусть $M_m(\varepsilon)$ – максимальное число кодовых слов в коде с критерием максимальной вероятности ошибки, а $M_a(\varepsilon)$ – то же самое для средней вероятности ошибки. Очевидно, $M_m(\varepsilon) \leqslant M_a(\varepsilon)$. Используя

кодирование с выбрасыванием (см., например, [19]), также получаем

$$M_m(\varepsilon') \geqslant \frac{\varepsilon' - \varepsilon}{\varepsilon'} M_a(\varepsilon) \tag{3}$$

при $\varepsilon' > \varepsilon$. Это означает, что любая верхняя граница для скоростей при критерии средней вероятности ошибки является также и верхней границей в случае максимальной вероятности ошибки. Однако нижние границы для достижимых скоростей при критерии средней вероятности ошибки при переходе к максимальной вероятности ошибки несколько ухудшаются.

2.3. АБГШ-канал. Для вектора $\boldsymbol{a} \in \mathbb{R}^n$ и невырожденной матрицы $\boldsymbol{K} \in \mathbb{R}^{n\times n}$ пусть

$$\mathcal{N}(\boldsymbol{a}; \boldsymbol{K}) := \frac{\exp\{-(\boldsymbol{x} - \boldsymbol{a})^T \boldsymbol{K}^{-1}(\boldsymbol{x} - \boldsymbol{a})\}}{(2\pi)^{n/2}(\det(\boldsymbol{K}))^{1/2}}$$

– многомерное нормальное распределение со средним $\boldsymbol{a}$ и матрицей ковариации $\boldsymbol{K}$. Канал с аддитивным белым гауссовским шумом (АБГШ-канал) с дисперсией шума σ^2 задается условием

$$Y = x + Z,$$

где $x \in \mathbb{R}$ – вход канала, а $Z \sim \mathcal{N}(0; \sigma^2)$. Его n-мерная версия получается независимым применением одномерного ($n = 1$) случая к каждой из входных переменных x_i, $1 \leqslant i \leqslant n$. АБГШ-канал с ограничением на среднюю мощность S – это АБГШ-канал, вход которого $\boldsymbol{x}$ удовлетворяет условию

$$\|\boldsymbol{x}\|_2^2 := \sum_{i=1}^{n} x_i^2 \leqslant nS. \tag{4}$$

Пропускная способность АБГШ-канала с ограничением на среднюю мощность P (обозначаемая через C_G) дается выражением

$$C_G := \frac{1}{2}\log_2\Big(1 + \frac{P}{\sigma^2}\Big) \text{ бит на обращение к каналу.}$$

В [5, 6] было показано, что для АБГШ-канала с ограничением на среднюю мощность P максимальный объем кода $M^*(n, \varepsilon, P)$ для достаточно больших n удовлетворяет соотношению

$$\log M^*(n, \varepsilon, P) = nC_G + \sqrt{nV_G}\Phi^{-1}(\varepsilon) + O(\log(n)),$$

где вероятность ошибки не выше ε,

$$V_G = \frac{P(P+2)}{2(P+1)^2}\log_2^2(e), \quad \Phi(x) = \int\limits_{-\infty}^{x} \frac{e^{-u^2/2}}{\sqrt{2\pi}}\, du.$$

2.4. Дискретные каналы без памяти (ДКБП). ДКБП описывается конечным алфавитом $\mathcal{X}$ на входе, конечным алфавитом $\mathcal{Y}$ на выходе и вероятностями перехода вида $W = P_{Y|X}$, где для любого $n \geqslant 1$

$$P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}\,|\,\boldsymbol{x}) = \prod_{i=1}^{n} P_{Y|X}(y_i\,|\,x_i).$$

Хотя в принципе выход может зависеть от предыдущих входов (так называемый ДКБП с обратной связью), мы будем рассматривать только ДКБП без обратной связи. Пропускная способность C_D неэкзотического[2] ДКБП W (см. [7, Приложение Н], а также [9]) дается формулой Шеннона:

$$C_D = \sup_{P\in\mathcal{P}(\mathcal{X})} I(P;W) \triangleq \sup_{P\in\mathcal{P}(\mathcal{X})} \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P(x)W(y\,|\,x)\log\left(\frac{W(y\,|\,x)}{PW(y)}\right),$$

где $I(P;W)$ – взаимная информация (см. [19]) между входом и выходом канала.

Теперь определим некоторые понятия, которые понадобятся нам в дальнейшем.

О п р е д е л е н и е 1. Для заданных канала W и распределения на выходе Q информационной плотностью [20] канала называется величина

$$i(x,y;Q) = \log\left(\frac{W(y\,|\,x)}{Q(y)}\right). \tag{5}$$

Зачастую $Q = PW$ для некоторого $P \in \mathcal{P}(\mathcal{X})$, и в этом случае будем обозначать информационную плотность через $i_P(x,y)$.

Заметим, что

$$I(P;W) = \sum_{x,y} P(x)W(y\,|\,x)i_P(x,y).$$

Аналогично, дисперсия информационной плотности имеет вид

$$V(P;W) := \left[\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P(x)W(y\,|\,x)(i_P(x,y))^2\right] - (I(P;W))^2.$$

Результат при конечной длине блока для неэкзотических ДКБП W с вероятностью ошибки $0<\varepsilon<1$ и $V(P;W)>0$ для распределения P, на котором достигается пропускная способность, дается выражением (см. [5–9])

$$\log M^*(n,\varepsilon) = nC_D + \sqrt{nV_D}\Phi^{-1}(\varepsilon) + O(\log(n)),$$

где

$$V_D = \begin{cases} V_{\min} := \min\limits_{P\in\Pi} V(P;W), & \varepsilon \leqslant 1/2,\\ V_{\max} := \max\limits_{P\in\Pi} V(P;W), & \varepsilon > 1/2, \end{cases}$$

а $\Pi = \{P\in\mathcal{P}(\mathcal{X}):\ I(P;W) = C_D\}$ – множество распределений, на которых достигается пропускная способность.

2.5. ДКБП с ограничениями по стоимости. Пусть $\Lambda\colon \mathcal{X}\to\mathbb{R}$ – неотрицательная функция, которую будем называть функцией энергии. Ее значением является просто энергия символа x, что обобщает стандартную функцию энергии $\Lambda(x) = x^2$ для АБГШ-канала. В дальнейшем будем предполагать, что функция энергии разделима,

[2] ДКБП называется экзотическим, если максимальная дисперсия его информационной плотности, т.е. $V_{\max}$, равна 0, и для некоторого входного символа x_0 равенство $P(x_0) = 0$ выполнено для любого распределения P, на котором достигается пропускная способность, но при этом $D(W(\cdot\,|\,x_0)\,\|\,Q_Y^*) = C$ и $V(W(\cdot\,|\,x_0)\,\|\,Q_Y^*) > 0$. Здесь $D(P_1\,\|\,P_2)$ – КЛ-дивергенция между P_1 и P_2, а $V(P_1\,\|\,P_2) = \sum\limits_x P_1(x)\log^2\left(\dfrac{P_1(x)}{P_2(x)}\right) - D^2(P_1\,\|\,P_2)$.

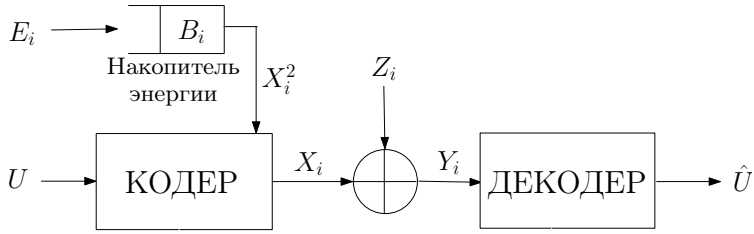

Рис. 1. Блок-схема АБГШ с системой сбора энергии

т.е. для вектора $\boldsymbol{x} \in \mathcal{X}^n$

$$\Lambda(\boldsymbol{x}) := \sum_{i=1}^{n} \Lambda(x_i). \tag{6}$$

Зададим множества ограничений $\mathbb{F}_a$ и $\mathcal{F}_a$ для $a \geqslant 0$ следующим образом:

$$\mathbb{F}_a = \{\boldsymbol{x} \in \mathcal{X}^n : \Lambda(\boldsymbol{x}) \leqslant na\}, \tag{7}$$

$$\mathcal{F}_a = \{P \in \mathcal{P} : \mathbf{E}_P[\Lambda(X)] \leqslant na\}. \tag{8}$$

В ДКБП с ограничениями по стоимости (см. [21,22]), где кодовые слова выбираются из множества $\mathbb{F}_a$, пропускная способность приобретает вид

$$C_D(a) = \sup_{P \in \mathcal{F}_a} I(P;W). \tag{9}$$

Более того, для любого $a > 0$ максимальный достижимый объем кода, обозначаемый через $M^*(n,\varepsilon,a)$, при определенных условиях регулярности (см. результат в [7] и некоторые улучшения в [22]) имеет вид

$$\log M^*(n,\varepsilon,a) = nC_D(a) + \sqrt{nV_D(a)}\Phi^{-1}(\varepsilon) + O(\log n),$$

где $V_D(a)$ – дисперсия канала (см. [6]).

ДКБП со сбором энергии (СЭ-ДКБП) можно рассматривать как обобщение ДКБП с ограничениями по стоимости, и его анализ при конечной длине блока вынесен в § 4.

2.6. АБГШ-канал со сбором энергии. Система сбора энергии состоит из накопителя энергии (буфера), где в течение некоторого периода времени собирается энергия из различных источников. Обычно энергия собирается из внешних источников, таких как, например, солнечная энергия. СЭ-АБГШ-канал состоит из системы сбора энергии на передающем конце и последующего АБГШ-канала, как показано на рис. 1. Предполагается, что для передачи символа x по каналу требуется x^2 единиц энергии из буфера, и если необходимая энергия имеется в наличии, происходит успешная передача, а в противном случае возникает сбой. Случай сбоя можно рассматривать как ошибку или же передавать в этом случае усеченный подходящим образом символ. В настоящей статье в вопросах достижимости мы будем рассматривать сбой как ошибку передачи. Будем предполагать, что накопитель энергии имеет бесконечную пропускную способность и что утечек энергии не происходит. При этом процесс поступления энергии $\{E_i\}$ предполагается н.о.р., неотрицательным, с конечным средним $\mathbf{E}[E_1]$ и конечной дисперсией σ_E^2.

Система работает следующим образом. Вначале в интервале времени i собирается энергия E_i, она используется для передачи символа вместе с некоторой энергией

из буфера, если необходимо, и затем оставшаяся энергия сохраняется. Пусть B_i – энергия в буфере в i-м интервале передачи. Предполагается, что $B_0 = 0$. Тогда энергия в буфере при $1 \leqslant i \leqslant n$ изменяется согласно следующему закону:

$$B_i = (B_{i-1} + E_i - X_i^2)^+,$$

где $(x)^+ = \max\{x, 0\}$. В нашем случае $\boldsymbol{X}$ планируется таким образом, чтобы величина внутри $(\cdot)^+$ была неотрицательной.

Для обычного АБГШ-канала с ограничением по мощности S входные последовательности должны удовлетворять условию (4). Ограничение для АБГШ-канала со сбором энергии с входом $\boldsymbol{x}$ и вектором энергии $\boldsymbol{e}$ имеет вид

$$\left\|\boldsymbol{x}^k\right\|_2^2 \leqslant \left\|\boldsymbol{e}^k\right\|_1, \quad 1 \leqslant k \leqslant n;$$

иными словами, требуется, чтобы в любой момент времени было достаточно энергии для передачи желаемого символа. Для достижения этой цели разрешается, чтобы вектор $\boldsymbol{x}$ зависел от $\boldsymbol{e}$.

Пропускная способность СЭ-АБГШ-канала (см. [11, 12]) дается выражением

$$C_{EG} = \frac{1}{2}\log\left(1 + \frac{\mathbf{E}[E_1]}{\sigma^2}\right). \tag{10}$$

Кроме того, для этого канала также была показана справедливость сильной обратной теоремы кодирования (см. [11]). Из этого логически вытекала бы обратная теорема кодирования вида $\log M \leqslant nC_{EG} + o(n)$. Но поскольку нас интересует улучшение этого выражения, нам необходимы более тонкие инструменты для вывода обратной теоремы кодирования при конечной длине блока. Поэтому нам потребуются для этого некоторые результаты из [7]. Для ясности изложения будем использовать обозначения из [7].

Сформулируем следующие границы на пропускную способность СЭ-АБГШ-каналов при конечной длине блока.

Теорема 1. *Рассмотрим СЭ-АБГШ-канал с дисперсией шума σ^2, в котором процесс сбора энергии $\{E_i\}$ н.о.р. на передающем конце, имеет среднее $\mathbf{E}[E_1]$ и дисперсию $\sigma_E^2 < \infty$. Для заданной максимальной вероятности ошибки $\varepsilon > 0$ справедливо следующее*:

1 (граница достижимости). *При достаточно большой длине блока n максимальный объем кода $M^*(n, \varepsilon)$ удовлетворяет неравенству*

$$\log M^*(n, \varepsilon) \geqslant nC_{EG} + \sqrt{n}\left[\sqrt{V_{EG}}\Phi^{-1}(\lambda\varepsilon) - K_{\varepsilon,\lambda}C_{EG}\right] - \log n + O(1), \tag{11}$$

где C_{EG} определено в (10),

$$V_{EG} = \frac{\mathbf{E}[E_1]}{\mathbf{E}[E_1] + \sigma^2}\log_2^2(e), \quad K_{\varepsilon,\lambda} = \sqrt{\frac{4(2\,\mathbf{E}[E_1]^2 + \sigma_E^2)}{(1-\lambda)\varepsilon\,\mathbf{E}[E_1]^2}},$$

причем это выполнено для любого $0 < \lambda < 1$;

2 (верхняя граница). *Кроме того,*

$$\log M^*(n, \varepsilon) \leqslant nC_{EG} + \sqrt{nV_{EG2}}\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n + O(1), \tag{12}$$

где

$$V_{EG2} = \frac{\mathbf{E}[E_1]^2 + \mathbf{E}[E_1^2] + 4\sigma^2\,\mathbf{E}[E_1]}{4(\mathbf{E}[E_1] + \sigma^2)^2}\log_2^2(e).$$

Доказательство границы достижимости вынесено в § 3, а верхней границы – в § 6. Поскольку члены второго порядка (коэффициенты при $\sqrt{n}$) не совпадают, заключаем, что

$$\log M^*(n,\varepsilon) = nC_{EG} + \Theta(\sqrt{n}).$$

2.7. ДКБП со сбором энергии. ДКБП со сбором энергии – это ДКБП, в котором происходит сбор энергии при кодировании (на передающем конце). Пусть $\Lambda(\cdot)$ – функция энергии (см. (6)), связанная с этим ДКБП. Модель та же, что и для СЭ-АБГШ-канала, за исключением следующих различий и предположений:

1. АБГШ-канал заменяется на ДКБП;
2. Энергия, потребляемая для символа x_i, равна $\Lambda(x_i)$. Кроме того, имеется символ x_0, такой что $\Lambda(x_0) = 0$;
3. Дополнительно предполагается, что ДКБП не являются экзотическими.

Анализ ДКБП со сбором энергии в общем и целом аналогичен анализу СЭ-АБГШ-каналов. Однако, используя метод типов (подробнее о типах см. в [19, 21]), можно улучшить верхнюю границу, приведя ее к виду, похожему на границу для обычного ДКБП без сбора энергии.

Пропускная способность СЭ-ДКБП, процесс сбора энергии которого имеет среднее $\mathbf{E}[E_1]$, дается выражением

$$C_{ED} := \sup_{P \in \mathcal{F}_{\mathbf{E}[E_1]}} I(P;W), \tag{13}$$

где $\mathcal{F}_a$ определено в (8).

В настоящей статье доказываются следующие границы на скорость для СЭ-ДКБП при конечной длине блока.

Теорема 2. *Для заданного $0 < \varepsilon < 1$ при критерии максимальной вероятности ошибки рассмотрим СЭ-ДКБП с архитектурой сбора, использования и накопления энергии, в котором процесс сбора энергии $\{E_i\}$ н.о.р. с $\mathbf{E}[E_1^2] < \infty$.*

1 (граница достижимости). *Для заданного распределения на входе $P_X \in \mathcal{F}_{\mathbf{E}[E_1]}$ максимальный объем кода $M^*(n,\varepsilon)$ при достаточно большой длине блока n удовлетворяет неравенству*

$$\begin{aligned}&\log M^*(n,\varepsilon) \geqslant \\ &\geqslant nI(P_X;W) - \sqrt{n}K_{\varepsilon,\lambda}I(P_X;W) + \sqrt{nV(P_X;W)}\Phi^{-1}(\lambda\varepsilon) - \log n + O(1)\end{aligned} \tag{14}$$

для любого $0 < \lambda < 1$. Здесь

$$K_{\varepsilon,\lambda} = \frac{2\sqrt{\mathrm{Var}(\Delta_1)}}{\mathbf{E}[E_1]\sqrt{(1-\lambda)\varepsilon}}, \quad \Delta_1 = E_1 - \Lambda(X_1);$$

2 (верхняя граница). *Для заданнного $\eta > 0$ максимальный объем кода $M^*(n,\varepsilon)$ удовлетворяет неравенству*

$$\begin{aligned}&\log M^*(n,\varepsilon) \leqslant \\ &\leqslant nC_{ED} + \sqrt{n}C'(\mathbf{E}[E_1])D_\varepsilon + \sqrt{nV_\varepsilon^*(\eta)}\left(\Phi^{-1}(\varepsilon) + \frac{K_\varepsilon\varepsilon}{4}\right) + O(\log n),\end{aligned} \tag{15}$$

где $C'(\cdot)$ – производная функции пропускной способности с ограничением по стоимости (9), а D_ε, K_ε и $V_\varepsilon^*(\eta)$ – функции от ε, не зависящие от n.

2.8. Кодер и декодер для каналов со сбором энергии. Для традиционных каналов (АБГШ, ДКБП и т.д.) кодер и декодер имеют доступ к кодовой книге (случайным или еще каким-нибудь образом) для целей кодирования и декодирования

соответственно. В постановке задачи со сбором энергии кодеру доступны значения поступающей энергии. Поэтому любое кодовое слово $c \in \mathcal{C}$, где $\mathcal{C}$ – кодовая книга, является вектором вида $c(m, \boldsymbol{e}^n)$ длины n, где n – длина блока, для сообщения m и вектора энергии $\boldsymbol{e}^n$. Из соображений причинности i-й символ кодового слова может зависеть только от $\boldsymbol{e}^i$. Декодеру же эти значения энергии недоступны, поэтому ему неизвестна и зависящая от этих значений кодовая книга. С другой стороны, ему доступна первичная кодовая книга, не зависящая от значений энергии. Поэтому в контексте каналов со сбором энергии кодовое слово, соответствующее сообщению m, должно иметь смысл отображения $m \to c(m, \cdot)$. Заметим, что определения объема кода M, вероятности ошибки и т.д., данные в п. 2.2, при этом не изменяются. Это аналогично тому, что происходит при анализе каналов с информацией о состоянии, известной только на передающем конце.

В доказательстве достижимых границ мы увидим, что создается кодовая книга, не зависящая от значений энергии и доступная также на приемном конце. После этого кодер, используя значения энергии, модифицирует кодовые слова так, чтобы они удовлетворяли необходимым ограничениям. Таким способом организуется пара кодер-декодер. Аналогичный метод применяется в каналах с переменными состояниями, где информация о состоянии доступна кодеру, но не известна декодеру [23].

§ 3. Граница достижимости для СЭ-АБГШ-каналов при конечной длине блока

В этом параграфе доказывается часть 1 теоремы 1. Пусть задано $0 < \varepsilon < 1$. Вначале построим код со средней вероятностью ошибки $\varepsilon_n = \varepsilon - 1/\sqrt{n}$, где $n > \varepsilon^{-2}$. Применяя кодирование с выбрасыванием, получаем следующую границу:

$$\log M_m(n, \varepsilon) \geqslant \log M_a(n, \varepsilon_n) - \frac{1}{2}\log n - \log \varepsilon, \tag{16}$$

где M_m – объем кодовой книги для критерия максимальной вероятности ошибки, полученный с помощью выбрасывания, а M_a соответствует средней вероятности ошибки. Будем предполагать, что в начале передачи буфер пуст. Это соответствует наихудшему возможному сценарию, поскольку если бы в начале буфер был непустым, это могло бы лишь способствовать передаче, и поэтому наша граница достижимости по-прежнему бы выполнялась. Предлагаемая схема кодирования состоит из двух фаз: фаза накопления и фаза собственно передачи. В литературе это известно (см. [12]) как *схема накопления и передачи* (save and transmit scheme).

3.1. Фаза накопления. В этой фазе передается символ 0, требующий нулевой энергии, в течение заданного количества интервалов передачи. Во время этого периода в буфере накапливается энергия. Приемнику известно об этих интервалах, и во время них выход канала им игнорируется, так как он не несет никакой информации. При этом, конечно, с точки зрения передачи информации эти интервалы тратятся впустую. Для того чтобы эта схема не влияла на коэффициент первого порядка, необходимо, чтобы число таких интервалов, отведенных для сбора энергии, составляло не более чем $o(n)$.

Зафиксируем $0 < \lambda < 1$ и положим

$$K_{\varepsilon,\lambda} = \sqrt{\frac{4(2\,\mathbf{E}[E_1]^2 + \sigma_E^2)}{(1-\lambda)\varepsilon\,\mathbf{E}[E_1]^2}}.$$

Через N_n обозначим число интервалов, отведенных на фазу накопления. Во время этой фазы буфер наполняется энергией, а после N_n интервалов времени ожидается, что накопленная энергия превысит некоторое пороговое значение, которое мы обозначим через E_{0n}. Пусть $N_n = K_{\varepsilon_n,\lambda}\sqrt{n}$ (всюду, где потребуется, берем округление

до целого сверху, если это N_n не целое) и $E_{0n} = N_n\,\mathbf{E}[E_1]/2$. Через $\mathcal{E}_0$ обозначим событие, состоящее в том, что в системе не удалось накопить энергию E_{0n}. Имеем

$$\Pr(\mathcal{E}_0) = \Pr\left[\sum_{i=1}^{N_n} E_i \leqslant E_{0n}\right] = \Pr\left[\sum_{i=1}^{N_n}(E_i - \mathbf{E}[E_1]) \leqslant -E_{0n}\right] \leqslant$$
$$\leqslant \Pr\left[\left|\sum_{i=1}^{N_n}(E_i - \mathbf{E}[E_1])\right| \geqslant E_{0n}\right] \leqslant \frac{4\sigma_E^2}{K_{\varepsilon_n,\lambda}\,\mathbf{E}[E_1]^2\sqrt{n}} \leqslant \frac{4\sigma_E^2}{K_{\varepsilon,\lambda}\,\mathbf{E}[E_1]^2\sqrt{n}}, \tag{17}$$

где на последнем шаге использовалось неравенство Чебышева и тот факт, что $K_{\varepsilon,\lambda}$ монотонно убывает по ε. Эта граница гарантирует, что вероятность ошибки убывает хотя бы как $O(n^{-1/2})$ и поэтому может быть сделана сколь угодно малой при достаточно большом n.

3.2. Схема кодирования и декодирования. Используя случайное кодирование, порождаем кодовую книгу, содержащую M_a кодовых слов длины n, с н.о.р. гауссовскими элементами с нулевым средним и дисперсией $\mathbf{E}[E_1]$. Эта кодовая книга доступна также и декодеру. Через $V_i(m)$ обозначим i-й символ m-го кодового слова.

На приемном конце используется некоторый вариант порогового декодирования. Напомним определение величины $i_P(x,y)$, где W – рассматриваемый гауссовский канал, а PW – распределение на выходе (гауссовское со средним 0 и дисперсией $\mathbf{E}[E_1] + \sigma^2$) для соответствующего гауссовского входа. Правило декодирования состоит в том, чтобы выбрать единственное сообщение $\widehat{m}$, такое что

$$i_P\big(\boldsymbol{V}^n(\widehat{m}), \boldsymbol{Y}\big) \geqslant \log\gamma_n, \tag{18}$$

где γ_n – неотрицательное число, которое будет выбрано позже. Это тот же детектор, который используется в обычных АБГШ-каналах.

Заметим, что в том, что касается передатчика, эта кодовая книга не является *зависящей от энергии* кодовой книгой, которая обсуждалась в п. 2.8. Это вполне соответствует тому, что декодеру не доступен процесс поступления энергии. Однако в следующем пункте мы построим реальный передаваемый символ $\boldsymbol{X}^n$, который будет функцией от поступающей энергии. Поэтому эту кодовую книгу мы будем называть *первичной*.

3.3. Фаза передачи. Пусть n – число интервалов времени, в которых передаются символы по АБГШ-каналу. Подсчитаем число обращений к каналу начиная с момента N_n+1. После того как мы накопим энергию по крайней мере E_{0n}, мы должны обеспечить, что с высокой вероятностью при дальнейшей передаче не возникнет сбоя. Пусть $\boldsymbol{v}^n$ – вход до проверки накопителя энергии. В момент i, $1 \leqslant i \leqslant n$, есть два случая:

1. Накопилось достаточно энергии, и тогда на вход канала подается $x_i = v_i$;
2. Энергии недостаточно, и тогда передается $x_i = 0$.

Если требуется передать сообщение m, то при заданном $\boldsymbol{V}^n(m)$, определенном в п. 3.2, соответствующий символ $\boldsymbol{X}^n(m)$ получается применением следующих правил.

Обозначим множество последовательностей $(\boldsymbol{v}^n, \boldsymbol{e}^n)$, удовлетворяющих вышеуказанным ограничениям, через $\mathcal{A}_n$, где

$$\mathcal{A}_n = \bigcap_{\ell=1}^{n} \{(\boldsymbol{v}^n, \boldsymbol{e}^n) :\ s_\ell \geqslant -E_{0n}\}, \tag{19}$$

и пусть $s_\ell = \sum\limits_{k=1}^{\ell} e_k - v_k^2$. Заметим, что передаваемое кодовое слово удовлетворяет условиям передачи со сбором энергии, поскольку энергия E_{0n} уже собрана к началу передачи. Через $\mathcal{E}_1$ обозначим то событие, что условия на энергию не выполнены. Пусть $\{V_i\}$, $1 \leqslant i \leqslant n$, – н.о.р. случайные величины (не обязательно гауссовские) с нулевым средним, дисперсией $\mathbf{E}[E_1]$ и $\mathbf{E}[V_1^4] < \infty$. Формально имеем

$$\Pr(\mathcal{E}_1) = \Pr(\mathcal{A}_n^c) = \Pr\left[\bigcup_{\ell=1}^{n}\{S_\ell \leqslant -E_{0n}\}\right] \leqslant \Pr\left[\bigcup_{\ell=1}^{n}\{|S_\ell| \geqslant E_{0n}\}\right] =$$
$$= \Pr\Big[\max_{1\leqslant\ell\leqslant n} |S_\ell| \geqslant E_{0n}\Big] \tag{20}$$

и $S_\ell = \sum\limits_{k=1}^{\ell} E_k - V_k^2$. Теперь S_ℓ – сумма н.о.р. случайных величин с нулевым средним и конечной дисперсией. Применим неравенство Колмогорова [24, гл. 3], утверждающее следующее.

Л е м м а 1 (неравенство Колмогорова). *Пусть Z_i – независимые случайные величины с нулевым средним, и пусть $S_n = \sum\limits_{i=1}^{n} Z_i$. Если $\mathbf{E}[Z_i] = 0$ и $\mathbf{E}[Z_i^2] < \infty$, то для любого $0 < a < \infty$*

$$\Pr\Big(\max_{1\leqslant i\leqslant n} |S_i| \geqslant a\Big) \leqslant \frac{\mathbf{E}[S_n^2]}{a^2}.$$

Отсюда

$$\Pr(\mathcal{E}_1) \leqslant \frac{\mathbf{E}[S_n^2]}{E_{0n}^2} = \frac{4(2\,\mathbf{E}[E_1]^2 + \sigma_E^2)}{K_{\varepsilon_n,\lambda}^2\,\mathbf{E}[E_1]^2} \leqslant \frac{4(2\,\mathbf{E}[E_1]^2 + \sigma_E^2)}{K_{\varepsilon,\lambda}^2\,\mathbf{E}[E_1]^2}. \tag{21}$$

В отличие от (17), правая часть этого неравенства не зависит от n. Однако подходящим образом выбирая $K_{\varepsilon,\lambda}$, можно сделать ее сколь угодно малой. Наш выбор $K_{\varepsilon,\lambda}$ будет гарантировать, что $\Pr(\mathcal{E}_1) \leqslant (1-\lambda)\varepsilon$. Таким образом, общее число интервалов времени, отведенных под накопление и передачу в этой схеме, составляет $N_n + n$.

Хотелось бы отметить, что во всех этих результатах величины V_i не предполагаются гауссовскими и что канал не играет никакой роли за исключением ограничений на вход. Это означает, что полученная граница справедлива и для негауссовских каналов со сбором энергии с независимыми входами, удовлетворяющими вышеуказанным ограничениям на моменты.

3.4. Вывод нижней границы. Пусть $\mathcal{E}_H = \mathcal{E}_0 \cup \mathcal{E}_1$. При критерии средней вероятности ошибки (см. (2)) мы видим, что

$$P_{e,\mathrm{avg}} = \frac{1}{M_a}\sum_{i=1}^{M_a} \Pr\big[\widehat{U} \neq i \,|\, U = i\big] =$$
$$= \frac{1}{M_a}\sum_{i=1}^{M_a} \Pr\big[\widehat{U} \neq i,\, \mathcal{E}_H^c \,|\, U = i\big] + \Pr\big[\widehat{U} \neq i,\, \mathcal{E}_H \,|\, U = i\big] \leqslant$$
$$\leqslant \frac{1}{M_a}\sum_{i=1}^{M_a} \Pr\big[\widehat{U} \neq i,\, \mathcal{E}_H^c \,|\, U = i\big] + \Pr[\mathcal{E}_H]. \tag{22}$$

Отметим, что все эти вероятности имеют собственное математическое ожидание относительно всех кодовых книг. Теперь сделаем важное наблюдение. И первичная кодовая книга, и гауссовский канал, и декодер функционируют независимо от системы сбора энергии. Единственный способ, каким переменные, отвечающие за сбор энергии, влияют на общую картину, – это через $\boldsymbol{Y}^n$, поскольку $Y_i = X_i + Z_i$. Значит, при событии $\mathcal{E}_H^c$ отсюда следует, что $\boldsymbol{X}^n = \boldsymbol{V}^n$. Но это то же самое, что сказать, что когда ограничение по собранной энергии выполнено, символы из первичной кодовой книги остаются неизменными, подвергаясь лишь воздействию шума.

Рассмотрим $\Pr\bigl[\widehat{U} \neq i,\, \mathcal{E}_H^c \,|\, U = i\bigr]$. Как отмечено выше, при событии $\mathcal{E}_H^c$ канал ведет себя как стандартный АБГШ-канал, и поэтому возникающие ошибки – это только ошибки в таком канале. Следовательно, используя неравенство для вероятности объединения событий, получаем

$$\begin{aligned}
&\Pr\bigl[\widehat{U} \neq i,\, \mathcal{E}_H^c \,|\, U = i\bigr] \leqslant \Pr\bigl[\{i_P(\boldsymbol{V}^n(i); \boldsymbol{Y}^n) \leqslant \log\gamma_n\},\, \mathcal{E}_H^c \,|\, U = i\bigr] + \\
&+ \sum_{\substack{1 \leqslant j \leqslant M_a \\ j \neq i}} \Pr\bigl[\{i_P(\boldsymbol{V}^n(j); \boldsymbol{Y}^n) \geqslant \log\gamma_n\},\, \mathcal{E}_H^c \,|\, U = i\bigr] \leqslant \\
&\leqslant \Pr\bigl[i_P(\boldsymbol{V}^n(i); \boldsymbol{V}^n(i) + \boldsymbol{Z}^n) \leqslant \log\gamma_n \,|\, U = i\bigr] + \\
&+ \sum_{\substack{1 \leqslant j \leqslant M_a \\ j \neq i}} \Pr\bigl[i_P(\boldsymbol{V}^n(j); \boldsymbol{V}^n(i) + \boldsymbol{Z}^n) \geqslant \log\gamma_n \,|\, U = i\bigr]. \qquad (23)
\end{aligned}$$

Дальнейшее доказательство вполне аналогично выводу границ для АБГШ-канала (см. [7]), и поэтому в итоге получаем следующую границу для любого $\gamma_n > 0$:

$$\Pr\bigl[\widehat{U} \neq i,\, \mathcal{E}_H^c \,|\, U = i\bigr] \leqslant \Pr\left[\log\left(\frac{W^n(\boldsymbol{V}^n + \boldsymbol{Z}^n \,|\, \boldsymbol{V}^n)}{P_{\boldsymbol{Y}^n}(\boldsymbol{V}^n + \boldsymbol{Z}^n)}\right) \leqslant \log\gamma_n\right] + \frac{M_a}{\gamma_n}. \qquad (24)$$

Таким образом, первый член в правой части неравенства (22) ограничен сверху величиной (24). Верхняя граница на $\Pr(\mathcal{E}_H)$ уже получена – она вытекает из (17), (21) и неравенства для вероятности объединения событий.

Имеем

$$\Pr\left[\log\left(\frac{W^n(\boldsymbol{V}^n + \boldsymbol{Z}^n \,|\, \boldsymbol{V}^n)}{P_{\boldsymbol{Y}^n}(\boldsymbol{V}^n + \boldsymbol{Z}^n)}\right) \leqslant \log\gamma_n\right] = \Pr\left\{\sum_{i=1}^n G_i \leqslant \log\gamma_n\right\}, \qquad (25)$$

где $G_i = \log\Bigl(\dfrac{\boldsymbol{W}(V_i + Z_i \,|\, V_i)}{\boldsymbol{P}_Y(V_i + Z_i)}\Bigr)$. Отметим, что G_i – н.о.р. величины в силу сделанных ранее замечаний. Более того,

$$C_{EG} := \mathbf{E}[G_i] = \frac{1}{2}\log\left(1 + \frac{\mathbf{E}[E_1]}{\sigma^2}\right), \qquad (26)$$

$$V_{EG} := \mathrm{Var}(G_i) = \frac{\mathbf{E}[E_1]}{\mathbf{E}[E_1] + \sigma^2}\log_2^2(e). \qquad (27)$$

Третий момент $\mathbf{E}[|G_i|^3]$ также конечен. Для дальнейшего сформулирует теорему Берри–Эссеена (см. [24, теорема 6.4.1]).

Лемма 2 (теорема Берри–Эссеена). *Пусть X_i, $1 \leqslant i \leqslant n$, – последовательность н.о.р. случайных величин со средним μ, дисперсией $\sigma^2 < \infty$ и $\mathbf{E}[|X_1|^3] < \infty$.*

Положим $S_n = \sum\limits_{i=1}^{n} X_i$. *Тогда для любого* $x \in \mathbb{R}$

$$\left| \Pr\left(\frac{S_n - n\mu}{\sigma\sqrt{n}} \leqslant x \right) - \Phi(x) \right| \leqslant C \frac{E|X_1 - \mu|^3}{\sigma^3\sqrt{n}},$$

где $C < 1/2$ (*см.* [25]). *Отметим, что эта граница равномерна по* x.

Положим

$$K = \frac{\mathbf{E}[|G_i - \mathbf{E}[G_i]|^3]}{2V_{EG}^{3/2}}.$$

Применяя теорему Берри–Эссеена, для любого $u \in \mathbb{R}$ имеем

$$\left| \Pr\left\{ \frac{\left(\sum\limits_{i=1}^{n} G_i\right) - nC_{EG}}{\sqrt{nV_{EG}}} \leqslant u \right\} - \Phi(u) \right| \leqslant \frac{K}{\sqrt{n}}.$$

Подставляя

$$u = \frac{\log\gamma_n - nC_{EG}}{\sqrt{nV_{EG}}},$$

получаем

$$\Pr\left\{ \sum_{i=1}^{n} G_i \leqslant \log\gamma_n \right\} \leqslant \Phi\left(\frac{\log\gamma_n - nC_{EG}}{\sqrt{nV_{EG}}} \right) + \frac{K}{\sqrt{n}}. \tag{28}$$

Пусть

$$\alpha_n = \lambda\varepsilon_n - \frac{4\sigma_E^2}{K_{\varepsilon_n,\lambda}\,\mathbf{E}[E_1]^2\sqrt{n}} - \frac{2K}{\sqrt{n}}.$$

В терминах ε имеем

$$\alpha_n \geqslant \lambda\varepsilon - \frac{4\sigma_E^2}{K_{\varepsilon,\lambda}\,\mathbf{E}[E_1]^2\sqrt{n}} - \frac{2K+\lambda}{\sqrt{n}} := \alpha_n'. \tag{29}$$

Положим

$$\log\gamma_n = nC_{EG} + \sqrt{nV_{EG}}\Phi^{-1}(\alpha_n).$$

Выберем n достаточно большим, так чтобы $\alpha_n > 0$. Из (22), (24), (25) и (28) имеем

$$\log M_a(n,\varepsilon_n) \geqslant \log\gamma_n - \frac{1}{2}\log n + O(1) \geqslant$$
$$\geqslant nC_{EG} + \sqrt{nV_{EG}}\Phi^{-1}(\alpha_n) - \frac{1}{2}\log n + O(1). \tag{30}$$

Используя (16) и (29), получаем

$$\log M_m(n,\varepsilon) \geqslant nC_{EG} + \sqrt{nV_{EG}}\Phi^{-1}(\alpha_n') - \log n + O(1), \tag{31}$$

замечая, что Φ^{-1} – монотонно возрастающая функция.

Упростим $\Phi^{-1}(\alpha'_n)$, используя формулу Тейлора. Существует $u \in (\alpha'_n, \lambda\varepsilon)$, такое что

$$f(\alpha'_n) = f(\lambda\varepsilon) + (\alpha'_n - \lambda\varepsilon)f'(u),$$

где $f(x) = \Phi^{-1}(x)$. Заметим, что $f(x)$ имеет производную, которая положительна, строго убывает до $x = 1/2$, а затем возрастает. Таким образом, на интервале $(\alpha'_n, \lambda\varepsilon)$ выполнено

$$f'(u) \leqslant \widehat{f} = \max\{f'(\alpha'_{n_0}), f'(\lambda\varepsilon)\},$$

где n_0 – наименьшее n, для которого $\alpha'_n > 0$. Отсюда при нашем выборе α'_n получаем, что

$$\log M^*(n,\varepsilon) \geqslant \log M_m(n,\varepsilon') \geqslant nC_{EG} + \sqrt{nV_{EG}}\Phi^{-1}(\lambda\varepsilon) - \log(n) + O(1). \tag{32}$$

Пусть $\widehat{n} = n + N_n$. Мы уже использовали $\widehat{n}$ интервалов времени, в n из которых велась передача. Результат будем выражать как функцию от $\widehat{n}$ – общего числа использованных интервалов времени. Имеем

$$\begin{aligned}\log M^*(\widehat{n},\varepsilon) &\geqslant (\widehat{n} - N_n)C_{EG} + \sqrt{nV_{EG}}\Phi^{-1}(\lambda\varepsilon) - \log(\widehat{n} - N_n) + O(1), \geqslant \\ &\geqslant \widehat{n}C_{EG} - K_{\varepsilon,\lambda}\sqrt{\widehat{n}}C_{EG} + \sqrt{nV_{EG}}\Phi^{-1}(\lambda\varepsilon) - \log\widehat{n} + O(1).\end{aligned} \tag{33}$$

Отметим, что

$$\sqrt{n} \leqslant \sqrt{\widehat{n}} \quad \text{и} \quad \sqrt{n} \geqslant \sqrt{\widehat{n}} - \frac{K_{\varepsilon,\lambda}}{2},$$

где второе неравенство вытекает из цепочки

$$\sqrt{\widehat{n}} = \sqrt{n + K_{\varepsilon,\lambda}\sqrt{n}} = \sqrt{n}\sqrt{1 + \frac{K_{\varepsilon,\lambda}}{\sqrt{n}}} \leqslant \sqrt{n}\left(1 + \frac{K_{\varepsilon,\lambda}}{2\sqrt{n}}\right) = \sqrt{n} + \frac{K_{\varepsilon,\lambda}}{2}, \tag{34}$$

в которой использовался тот факт, что $(1+x)^{1/2} \leqslant 1 + \frac{x}{2}$ для $x > 0$. Из (33) и (34) видно, что независимо от знака $\Phi^{-1}(\lambda\varepsilon)$ получаемые нижние границы отличаются на константу, не зависящую от n. Сводя все вместе, для достаточно больших $\widehat{n}$ получаем

$$\log M^*(\widehat{n},\varepsilon) \geqslant \widehat{n}C_{EG} + \sqrt{\widehat{n}}\left[\sqrt{V_{EG}}\Phi^{-1}(\lambda\varepsilon) - K_{\varepsilon,\lambda}C_{EG}\right] - \log\widehat{n} + O(1).$$

Для полноты изложения приведем точное выражение:

$$\begin{aligned}&\log M^*(\widehat{n},\varepsilon) \geqslant \widehat{n}C_{EG} + \sqrt{\widehat{n}}\left[\sqrt{V_{EG}}\Phi^{-1}(\lambda\varepsilon) - K_{\varepsilon,\lambda}C_{EG}\right] - \log\widehat{n} - \log\varepsilon K - \\ &- \frac{K_{\varepsilon,\lambda}}{2} - \sqrt{V_{EG}}\Phi^{-1}(\lambda\varepsilon)\widehat{f}\left[\frac{4\sigma_E^2}{K_{\varepsilon,\lambda}\,\mathbf{E}[E_1]^2} + 2K + \lambda\right].\end{aligned} \tag{35}$$

На этом завершается доказательство границы достижимости из теоремы 1.

§ 4. Граница достижимости для СЭ-ДКБП при конечной длине блока

Используем ту же стратегию случайного кодирования, что и в случае СЭ-АБГШ-канала. Выберем любое распределение на входе $P_X \in \mathcal{F}_{\mathbf{E}[E_1]}$. Построим матрицу размера $M \times n$, все элементы которой н.о.р. в соответствии с распределением P_X. Далее доказательство проводится в точности так же, как и для границы достижимости в случае СЭ-АБГШ-канала, заменяя член X_i^2 на $\Lambda(X_i)$ всюду, где он встречается.

В частности, для получения наилучшей границы можно взять $P_X^* \in \Gamma$ (где Γ – множество распределений на входе, на которых достигается пропускная способность, содержащихся в $\mathcal{F}_{\mathbf{E}[E_1]}$). Если таких распределений, на которых достигается пропускная способность, много, то можно изменять $V(P_X^*; W)$, выбирая распределение P_X^*. Поэтому рассмотрим

$$V_{ED} = \begin{cases} V_{\min} := \min\limits_{P\in\Gamma} V(P;W), & \text{если } \varepsilon \leqslant \dfrac{1}{2\lambda}, \\ V_{\max} := \max\limits_{P\in\Gamma} V(P;W), & \text{если } \varepsilon > \dfrac{1}{2\lambda}. \end{cases}$$

Сводя все вместе, получаем следующую границу достижимости:

$$\log M^*(\widehat{n},\varepsilon) \geqslant \widehat{n}C_{ED} - \sqrt{\widehat{n}}K_{\varepsilon,\lambda}C_{ED} + \sqrt{\widehat{n}V_{ED}}\Phi^{-1}(\lambda\varepsilon) - \log\widehat{n} + O(1) \tag{36}$$

для всех достаточно больших $\widehat{n}$. Точный вид этой границы такой:

$$\log M^*(\widehat{n},\varepsilon) \geqslant \widehat{n}C_{ED} - \sqrt{\widehat{n}}K_{\varepsilon,\lambda}C_{ED} + \sqrt{\widehat{n}V_{ED}}\Phi^{-1}(\lambda\varepsilon) - \log\widehat{n} - \log\varepsilon K - \\ - \frac{K_{\varepsilon,\lambda}}{2} - \sqrt{V_{ED}}\Phi^{-1}(\lambda\varepsilon)\widehat{f}\left[\frac{4\sigma_E^2}{K_{\varepsilon,\lambda}\,\mathbf{E}[E_1]^2} + 2K + \lambda\right]. \tag{37}$$

§ 5. Обратные теоремы кодирования

В этом параграфе мы приведем общую верхнюю границу на скорости при конечной длине блока для каналов со сбором энергии. Для вывода этих новых границ мы используем методы из [7]. Затем мы применим эти границы к СЭ-АБГШ-каналам и СЭ-ДКБП.

Напомним следующие функции вероятности ошибки $\beta_\alpha(P,Q)$ (см. [7]).

Определение 2. Для заданных распределений P и Q на $\mathcal{X}$ для $\alpha \in [0,1]$ положим

$$\beta_\alpha(P,Q) := \min Q[T=1] := \min \int\limits_{\mathcal{X}} P_{T|X}(1\,|\,x)\,dQ(x), \tag{38}$$

где минимум берется по всем распределениям $(P_{T|X})$ тестовых функций $T\colon \mathcal{X} \to \to \{0,1\}$, таким что $P[T=1] \geqslant \alpha$.

По существу это функции вероятности ошибки 2-го рода (принятия гипотезы P, когда верна Q), когда вероятность ошибки 1-го рода меньше $1-\alpha$.

Метаобращение теоремы кодирования, доказанное в [7], является одной из наилучших известных общих верхних границ для любого канала. Этот результат имеет два варианта: один для средней вероятности ошибки, а второй – для максимальной. Отметим, что это границы для одного символа, которые естественно обобщаются для длины блока n.

Лемма 3 (метаобращение теоремы кодирования (для средней вероятности ошибки)). *Для любого (M,ε)-кода со средней вероятностью ошибки ε справедливо неравенство*

$$M \leqslant \sup_{P_X} \frac{1}{\beta_{1-\varepsilon}(P_{XY}, P_X Q_Y)}$$

для любого распределения на выходе Q_Y.

Лемма 4 (метаобращение теоремы кодирования (для максимальной вероятности ошибки)). *Для любого (M,ε)-кода с максимальной вероятностью ошибки ε*

справедливо неравенство

$$M \leqslant \frac{1}{\beta_{1-\varepsilon}(P_{Y\,|\,X=c(\overline{m})}, Q_Y)} \leqslant \sup_{x\in\mathbb{F}} \frac{1}{\beta_{1-\varepsilon}(P_{Y\,|\,X=x}, Q_Y)}$$

для любого распределения на выходе Q_Y и кодовых слов из множества $\mathbb{F} \subset \mathcal{X}$, где $\mathcal{X}$ – алфавит на входе, а $c(\overline{m})$ – кодовое слово для сообщения $\overline{m}$, удовлетворяющего условию

$$\overline{m} = \arg\min_{m\in[M]} \Pr\bigl[\widehat{U} = m \,|\, U = m\bigr] \tag{39}$$

в канале Q_Y.

Однако не сразу понятно, с помощью какой техники можно включить эффект сбора энергии в приведенное выше выражение. Это связано с тем, что указанное множество $\mathbb{F}$ (множество ограничений) меняется с изменением энергии. Кроме того, в отличие от традиционных каналов, кодовая книга также будет меняться в зависимости от доступной энергии. Следовательно, любое кодовое слово имеет вид $c(m, \boldsymbol{e})$ для сообщения m и вектора энергии $\boldsymbol{e}$.

Обратная теорема кодирования (общий вид) для каналов со сбором энергии. В описанной выше постановке задачи со сбором энергии получаем следующие верхние границы.

Теорема 3. *Для заданных канала со сбором энергии W и процесса сбора энергии $E \sim P_E$ с н.о.р. поступлениями любой (M, ε)-код (со средней вероятностью ошибки) удовлетворяет неравенству*

$$M \leqslant \sup_{P_{X^n\,|\,E^n}} \frac{1}{\beta_{1-\varepsilon}(P_{E^nX^nY^n}, P_{E^nX^n}Q_{Y^n})}, \tag{40}$$

где

$$P_{E^nX^nY^n}(e^n, x^n, y^n) = P_{E^n}(e^n)P_{X^n\,|\,E^n}(x^n\,|\,e^n)W(y^n\,|\,x^n),$$

для любого распределения на выходе Q_{Y^n}. Здесь супремум берется по всем распределениям, удовлетворяющим ограничениям на сбор энергии. В случае максимальной вероятности ошибки имеем

$$M \leqslant \frac{1}{\beta_{1-\varepsilon}\left(W(\,\cdot\,|\,c(\overline{m}, *))P_{E^n}(*), Q_{Y^n}P_{E^n}\right)} \tag{41}$$

для любого распределения на выходе Q_{Y^n} и кодового слова $c(\overline{m}, *)$, для которого сообщение $\overline{m}$ удовлетворяет условию (39). *Здесь $\cdot$ означает алфавит на выходе, а $*$ – алфавит энергии.*

Доказательство. Неравенство (40) доказано в [14]. Доказательство неравенства (41) см. в Приложении А. ▲

Граница (40) использовалась для вывода обратной теоремы кодирования при конечной длине блока для СЭ-АБГШ-каналов, обобщенной на режим поступления энергии н.о.р. блоками [14]. Мы выведем этот же результат для СЭ-АБГШ-каналов при критерии максимальной вероятности ошибки, но с помощью границы (41).

Имеется следующая более слабая, но аналитически более удобная верхняя граница при критерии максимальной вероятности ошибки.

Теорема 4. *Рассмотрим канал со сбором энергии W, процесс сбора энергии $E \sim P_E$ с н.о.р. поступлениями и функцию стоимости Λ, определенную в п.* 2.7.

При условии, что каждое кодовое слово $\boldsymbol{x}(m, \boldsymbol{e}^n)$ *удовлетворяет ограничению по сбору энергии*

$$\sum_{i=1}^{n} \Lambda(x_i(m, \boldsymbol{e}^n)) \leqslant \sum_{i=1}^{n} e_i \tag{42}$$

для вектора энергии $\boldsymbol{e}^n$ *и максимальной вероятности ошибки* ε, *справедливо неравенство*

$$M \leqslant \sup_{\boldsymbol{x}^n \in \mathbb{F}_{\overline{E}_n}} \frac{1}{\beta_{1-\varepsilon-\tau_n}\left(W(\,\cdot\,|\,\boldsymbol{x}^n), Q_{Y^n}\right)}, \tag{43}$$

где $\tau_n = \Pr\Big(\sum\limits_{i=1}^{n} E_i \geqslant n\overline{E}_n\Big)$,

$$\mathbb{F}_{\overline{E}_n} = \left\{\boldsymbol{x}^n : \sum_{i=1}^{n} \Lambda(x_i) \leqslant n\overline{E}_n\right\}, \tag{44}$$

а $\overline{E}_n$ – *неотрицательная последовательность, выбранная так, что* $\tau_n < 1 - \varepsilon$.

Доказательство см. в Приложении В. ▲

Для СЭ-АБГШ-каналов имеется хорошая структура, позволяющая получать более точные границы при использовании неравенств (40) или (41). Эти подробности уточняются в доказательстве верхней границы для СЭ-АБГШ-канала. Однако при работе с СЭ-ДКБП такая структура отсутствует. Теорема 4 будет использована для получения полезной верхней границы в этом случае.

§ 6. Верхняя граница для СЭ-АБГШ-каналов при конечной длине блока

Мы утверждаем, что достаточно рассматривать кодовые слова $\boldsymbol{x}^n$, удовлетворяющие условию

$$\sum_{k=1}^{n} x_k^2 = \sum_{k=1}^{n} e_k, \tag{45}$$

где $\boldsymbol{e}^n$ – вектор энергии. Короче говоря, мы собираемся игнорировать сбои, которые могут произойти при $1 \leqslant k < n$, и будем расходовать всю энергию при передаче в момент времени n. Возможность первого из этих предположений подтверждается тем, что при этом ограничения только ослабляются, что может лишь увеличить пропускную способность. Таким образом, любая верхняя граница для ослабленной версии будет являться и верхней границей для исходной. Что касается второго предположения, то это хорошо известный трюк с отображением Яглома, когда имея наилучший код длины n, но удовлетворяющий условию (45) со строгим неравенством ($<$), можно построить новый код с той же вероятностью ошибки, но с длиной кодовых слов $n+1$. Дополнительный символ выбирается таким образом, чтобы исчерпать всю оставшуюся энергию. Этот новый код, очевидно, удовлетворяет условию (45), является верхней границей для исходного кода длины n и, в свою очередь, ограничивается сверху наибольшим кодом длины $n+1$, удовлетворяющим (45).

Пусть $0 < \varepsilon < 1$ – фиксированная максимальная вероятность ошибки. Выберем в качестве W гауссовский канал с дисперсией σ^2 и $Q_{Y^n} = \prod\limits_{i=1}^{n} Q_Y$, где Q_Y – гауссовское распределение со средним 0 и дисперсией $\mathbf{E}[E_1] + \sigma^2$. Далее, для распределений P_1

и P_2 и любого $\gamma > 0$ величина $\beta_\alpha(P_1, P_2)$ ограничена снизу (см. [7, формула (106)]) как

$$\beta_\alpha(P_1, P_2) \geqslant \frac{1}{\gamma}\left(\alpha - P_1\left[\frac{dP_1}{dP_2} \geqslant \gamma\right]\right). \tag{46}$$

Из (41) и (46) для любого $\gamma_n > 0$ имеем

$$M \leqslant \frac{\gamma_n}{1 - \varepsilon - \Pr\left[\log \dfrac{W(\boldsymbol{Y}^n \mid \boldsymbol{x}^n(\overline{m}, \boldsymbol{E}))}{Q_{Y^n}} \geqslant \log \gamma_n\right]}, \tag{47}$$

где вероятность берется относительно распределения $W(\,\cdot \mid \boldsymbol{x}(\overline{m}, *))P_{E^n}(*)$. Так как здесь W – гауссовский канал, то можно заменить Y_i на $x_i(\overline{m}, \boldsymbol{e}) + Z_i$, где Z_i – н.о.р. $\mathcal{N}(0, \sigma^2)$-величины. Тогда вероятность в знаменателе можно преобразовать следующим образом:

$$\begin{aligned}
&\Pr\left[\log \frac{W(\boldsymbol{Y}^n \mid \boldsymbol{x}^n(\overline{m}, \boldsymbol{E}))}{Q_{Y^n}} \geqslant \log \gamma_n\right] = \\
&= \Pr\left[\sum_{i=1}^n \frac{(x_i(\overline{m}, \boldsymbol{E}) + Z_i)^2}{2(\mathbf{E}[E_1] + \sigma^2)} \log_2(e) - \sum_{i=1}^n \frac{Z_i^2}{2\sigma^2} \log_2(e) \geqslant \log(\gamma_n) - nC_{EG}\right] = \\
&= \Pr\left[\sum_{i=1}^n \left(\frac{Z_i}{\sigma} - \frac{x_i(\overline{m}, \boldsymbol{E})\sigma}{\mathbf{E}[E_1]}\right)^2 \leqslant \frac{2(\mathbf{E}[E_1] + \sigma^2)}{\mathbf{E}[E_1]}(nC_{EG} - \log \gamma_n)\ln 2 + \right. \\
&\left. + \sum_{i=1}^n x_i^2(\overline{m}, \boldsymbol{E})\left(\frac{\sigma^2}{\mathbf{E}[E_1]^2} + \frac{1}{\mathbf{E}[E_1]}\right)\right] = \\
&= \Pr\left[\sum_{i=1}^n \left(\frac{Z_i}{\sigma} - \frac{x_i(\overline{m}, \boldsymbol{E})\sigma}{\mathbf{E}[E_1]}\right)^2 \leqslant \frac{2(\mathbf{E}[E_1] + \sigma^2)}{\mathbf{E}[E_1]}(nC_{EG} - \log \gamma_n)\ln 2 + \right. \\
&\left. + \sum_{i=1}^n E_i\left(\frac{\sigma^2}{\mathbf{E}[E_1]^2} + \frac{1}{\mathbf{E}[E_1]}\right)\right],
\end{aligned} \tag{48}$$

где (48) вытекает из (45). Далее, рассмотрим эту вероятность при условии $\boldsymbol{E} = \boldsymbol{e}$, замечая, что $\boldsymbol{E}$ не зависит от $\boldsymbol{Z}$. Тогда получим, что эта вероятность является интегральной функцией распределения (ИФР) для нецентрального χ^2-распределения с n степенями свободы и параметром нецентральности

$$B = \sum_{i=1}^n \frac{x_i^2(\overline{m}, \boldsymbol{e})\sigma^2}{\mathbf{E}[E_1]^2} = \sum_{i=1}^n \frac{e_i\sigma^2}{\mathbf{E}[E_1]^2}. \tag{49}$$

ИФР нецентральной случайной χ^2-величины $\widehat{Z}$ равна

$$\Pr(\widehat{Z} \leqslant u) = 1 - Q_{n/2}^M(\sqrt{B}, \sqrt{u}), \tag{50}$$

где $Q_d^M(a, b)$ – Q-функция Маркума порядка d (см. [26]). Теперь заметим, что эта ИФР не зависит от индивидуальных значений x_i или e_i, а зависит только от суммы всех e_i. Замена $x_i(\overline{m}, \boldsymbol{E})$ на $\sqrt{E_i}$ в (48) не изменит эту ИФР. Поэтому из (49) и (50)

получаем, что (48) равно

$$\Pr\left[\sum_{i=1}^{n}\left(\frac{Z_i}{\sigma}-\frac{\sqrt{E_i}\sigma}{\mathbf{E}[E_1]}\right)^2 \leqslant \frac{2(\mathbf{E}[E_1]+\sigma^2)}{\mathbf{E}[E_1]}(nC_{EG}-\log\gamma_n)\ln 2 + \right.$$
$$\left. + \sum_{i=1}^{n} E_i\left(\frac{\sigma^2}{\mathbf{E}[E_1]^2}+\frac{1}{\mathbf{E}[E_1]}\right)\right]. \tag{51}$$

Это в точности та упоминавшаяся ранее структура, которая позволяет работать с упрощенным выражением. В результате все слагаемые в сумме являются н.о.р. (а не просто независимыми). Переставляя члены подходящим образом, получаем, что (51) равно

$$\Pr\left[\frac{\sum\limits_{i=1}^{n}\eta_i}{\sqrt{nV_{EG2}}} \leqslant \frac{nC_{EG}-\log\gamma_n}{\sqrt{nV_{EG2}}}\right], \tag{52}$$

где η_i – независимые одинаково распределенные величины с нулевым средним и дисперсией

$$V_{EG2} = \frac{\mathbf{E}[E_1]^2+\mathbf{E}[E_1^2]+4\sigma^2\,\mathbf{E}[E_1]}{4(\mathbf{E}[E_1]+\sigma^2)^2}\log_2^2(e).$$

При этом третий момент для η_i конечен. Применяя теорему Берри – Эссеена (лемма 2) и выбирая

$$\log\gamma_n = nC_{EG}-\sqrt{nV_{EG2}}\Phi^{-1}(\alpha_n),$$

где α_n выбрана так, что $0<\alpha_n<1-\varepsilon$, получаем

$$\Pr\left[\frac{\sum\limits_{i=1}^{n}\eta_i}{\sqrt{nV_{EG2}}} \leqslant \frac{nC_{EG}-\log\gamma_n}{\sqrt{nV_{EG2}}}\right] \leqslant \alpha_n+\frac{\varkappa}{\sqrt{n}}, \tag{53}$$

где $\varkappa = \mathbf{E}[|\eta_i|^3]/V_{EG2}^{3/2}$.

Возьмем $\alpha_n = 1-\varepsilon-\dfrac{2\varkappa}{\sqrt{n}}$. Для достаточно больших n имеем $0<\alpha_n<1-\varepsilon$. Из (47), (51) и (53) получаем

$$\log M \leqslant nC_{EG}-\sqrt{nV_{EG2}}\Phi^{-1}(\alpha_n)-\log(\varkappa/\sqrt{n}).$$

Раскладывая Φ^{-1} в ряд Тейлора и оценивая шаги, как в доказательстве границы достижимости из теоремы 1, получаем

$$\log M \leqslant nC_{EG}+\sqrt{nV_{EG2}}\Phi^{-1}(\varepsilon)+\frac{1}{2}\log n+O(1),$$

что и дает требуемую верхнюю границу.

Для полноты изложения приведем точный вид границы:

$$\log M \leqslant nC_{EG}+\sqrt{nV_{EG2}}\Phi^{-1}(\varepsilon)+\frac{1}{2}\log n-\log\varkappa+2\varkappa\sqrt{V_{EG2}}\widehat{f}_2, \tag{54}$$

где

$$\widehat{f}_2 = \max\left\{f(\varepsilon), f\left(\varepsilon+\frac{2\varkappa}{\sqrt{n_0}}\right)\right\}, \quad f(x)=\frac{d}{dx}\Phi^{-1}(x),$$

а n_0 – наименьшее n, при котором $\varepsilon + \dfrac{2\varkappa}{\sqrt{n}} < 1$.

§ 7. Верхняя граница для СЭ-ДКБП при конечной длине блока

К сожалению, в этом случае нельзя просто воспроизвести доказательство обратной теоремы кодирования для СЭ-АБГШ-канала, данное в § 6, поскольку в нем эксплуатировалась структура АБГШ-канала, которая в данном случае отсутствует. Однако имеется другая структура, которую можно использовать здесь, а именно метод типов (см. [21]). Будем использовать схему теоремы 4. Пусть задано $0 < \varepsilon < 1$, и обозначим дискретный канал рассматриваемого СЭ-ДКБП через $W(y\,|\,x)$. Случайные величины E_i (поступающая энергия) предполагаются н.о.р., как и выше.

Напомним определения, данные в (7) и (8). Из (43) имеем

$$M \leqslant \sup_{\boldsymbol{x}^n \in \mathbb{F}_{\overline{E}_n}} \frac{1}{\beta_{1-\varepsilon-\tau_n}\left(W(\,\cdot\,|\,\boldsymbol{x}^n), Q_{Y^n}\right)}. \tag{55}$$

Возьмем $\overline{E}_n = \mathbf{E}[E_1] + \delta_n$, где $\delta_n > 0$. Тогда τ_n имеет вид

$$\tau_n = \Pr\left(\sum_{i=1}^{n} E_i \geqslant n(\mathbf{E}[E_1] + \delta_n)\right). \tag{56}$$

Мы хотим добиться, чтобы $\tau_n \leqslant \dfrac{\varepsilon}{4}$. Для этого выберем $\delta_n = \dfrac{D_\varepsilon}{\sqrt{n}}$, где $D_\varepsilon = \sqrt{\dfrac{4\sigma_E^2}{\varepsilon}}$, и применим неравенство Чебышева.

Можно представить (55) в виде

$$M \leqslant \sup_{P \in \mathcal{F}_{\overline{E}_n} \cap \mathcal{P}_n} \sup_{\boldsymbol{x}^n \in T_P} \frac{1}{\beta_{1-\varepsilon-\tau_n}\left(W(\,\cdot\,|\,\boldsymbol{x}^n), Q_{Y^n}\right)}, \tag{57}$$

где через T_P обозначен тип класса распределения P, а $\mathcal{P}_n$ – множество всех типов для последовательностей длины n. Рассмотрим внутренний супремум

$$\sup_{\boldsymbol{x}^n \in \mathcal{T}_P} \frac{1}{\beta_{1-\varepsilon-\tau_n}(W(\,\cdot\,|\,\boldsymbol{x}^n), Q_{Y^n})}.$$

Здесь значение β-функции вероятности ошибки не зависит от того, какая именно последовательность $\boldsymbol{x}$ выбирается, при условии, что последовательности имеют одинаковый тип [7] и $Q_{Y^n} = \prod\limits_{k=1}^{n} Q_Y$ для некоторого распределения Q_Y на $\mathcal{Y}$. Поэтому выбираем любую последовательность $\boldsymbol{x}$ из $\mathcal{T}_{P_0}$, где $P_0 \in \mathcal{F}_{\overline{E}_n} \cap \mathcal{P}_n$.

Пусть $Q_Y = P_0 W$. Напомним теорему 48 работы [7] для стандартных, неэкзотических ДКБП. Хотя в ней была дана граница для максимального подкода типа P_0 максимального кода, заметим, что на самом деле граница дается на значение β-функции вероятности ошибки, как указано далее.

Лемма 5. *Для $0 < \varepsilon < 1$, всех $P_0 \in \mathcal{P}_n$, $\boldsymbol{x} \in \mathcal{T}_{P_0}$ и достаточно больших n справедливо неравенство*

$$-\log \beta_{1-\varepsilon}(W^n(\,\cdot\,|\,\boldsymbol{x}), (P_0 W)^n) \leqslant nC_D + \sqrt{nV_D}\,\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n + O(1),$$

где

$$V_D = \begin{cases} V_{\min} = \min\limits_{P \in \Gamma} V(P; W), & 0 < \varepsilon \leqslant 1/2, \\ V_{\max} = \max\limits_{P \in \Gamma} V(P; W), & 1/2 < \varepsilon < 1, \end{cases}$$

а Γ – *множество распределений, на которых достигается пропускная способность.*

Заметим, что величина в правой части не зависит от распределения данного типа. Поэтому, если сделать следующие изменения:

1. Заменить Γ на

$$\Gamma_{\overline{E}_n} = \{P \in \mathcal{F}_{\overline{E}_n} : I(P;W) = C_{ED}\}. \tag{58}$$

   Это можно сделать, поскольку внешний супремум в (57) берется по $\mathcal{F}_{\overline{E}_n}$. Заметим, что в оригинальном доказательстве леммы 5 использовался тот факт, что множество Γ компактно и выпукло. Эти свойства выполнены и для $\Gamma_{\overline{E}_n}$, поэтому можно использовать это множество всюду, где использовалось Γ;
2. Последний супремум, дававший равномерную (по распределениям на входе) границу, брался по множеству $\mathcal{P}$. Здесь мы заменяем его на $\mathcal{F}_{\overline{E}_n}$;
3. Заменить ε на $\varepsilon + \tau_n$;

то получим

$$\log M^*(n,\varepsilon) \leqslant nC_D(\overline{E}_n) + \sqrt{n\widehat{V}(\overline{E}_n)}\Phi^{-1}(\varepsilon+\tau_n) + O(\log(n)), \tag{59}$$

где $C_D(\cdot)$ определено в (9) и

$$\widehat{V}(\overline{E}_n) = \begin{cases} V_{\min}^{(n)} = \min\limits_{P\in\Gamma_{\overline{E}_n}} V(P;W), & 0 < \varepsilon+\tau_n \leqslant 1/2, \\ V_{\max}^{(n)} = \max\limits_{P\in\Gamma_{\overline{E}_n}} V(P;W), & 1/2 < \varepsilon+\tau_n < 1. \end{cases} \tag{60}$$

Границу (59) можно упростить дальше, рассматривая разложения функций $C_D(\overline{E}_n)$, $\widehat{V}(\overline{E}_n)$ и $\Phi^{-1}(u)$.

Итак, $C_D(a)$ – неубывающая вогнутая функция (см. [21]). Поэтому для любых $a > 0$, $b > 0$ справедливо

$$C_D(a+b) \leqslant C_D(a) + bC_D'(a),$$

где $C_D'(\cdot)$ – производная функции $C_D(a)$. Положим $a = \mathbf{E}[E_1]$ и $b = \delta_n$. Заметим, что в этом случае $C_D'(a)$ – постоянная, поскольку $\mathbf{E}[E_1]$ – константа.

Используя разложение в ряд Тейлора, получаем, что для некоторой константы K_ε справедливо

$$\Phi^{-1}(\varepsilon+\tau_n) \leqslant \Phi^{-1}(\varepsilon) + \tau_n K_\varepsilon.$$

Пусть теперь ε_R – корень уравнения

$$\Phi^{-1}(\varepsilon) + \frac{K_\varepsilon \varepsilon}{4} = 0.$$

Возьмем любое $\eta > 0$. Заметим, что для достаточно больших n выполнено $\Gamma_{\overline{E}_n} \subset \subset \Gamma_{\mathbf{E}[E_1]+\eta}$. Поэтому можно заменить $\widehat{V}(\overline{E}_n)$ на

$$V_\varepsilon^*(\eta) = \begin{cases} \min\limits_{P\in\Gamma_{\mathbf{E}[E_1]+\eta}} V(P;W), & 0 < \varepsilon \leqslant \varepsilon_R, \\ \max\limits_{P\in\Gamma_{\mathbf{E}[E_1]+\eta}} V(P;W), & \varepsilon_R < \varepsilon < 1. \end{cases}$$

Заметим, что $C_D(\mathbf{E}[E_1]) \equiv C_{ED}$. Таким образом, для достаточно больших n имеем

$$\log M^*(n,\varepsilon) \leqslant nC_{ED} + \sqrt{n}C'(\mathbf{E}[E_1])D_\varepsilon + \sqrt{nV_\varepsilon^*(\eta)}\left(\Phi^{-1}(\varepsilon) + \frac{K_\varepsilon\varepsilon}{4}\right) + O(\log n).$$

В отличие от предыдущих случаев здесь мы не приводим никакой точной границы. Это происходит потому, что исходные границы для ДКБП в [7] были даны с неизвестными константами в члене $O(1)$.

§ 8. Начальная и остаточная энергия

В нашем анализе рассматривается передача одного сообщения, что является вполне обычным в теории информации [19], как и в теоретико-информационных рассмотрениях систем со сбором энергии [11, 12]. На практике передается много сообщений, и в начале передачи некоторых сообщений имеется некоторая случайная остаточная энергия. Если емкость буфера конечна, то с положительной вероятностью эта остаточная энергия будет нулевой. Таким образом, наши границы соответствуют наихудшему сценарию, когда в буфере нет начальной энергии. Во-вторых, если в накопителе энергии имеется некоторая остаточная энергия e_0, то в случае $e_0 > E_{0n}$ не требуется ждать, пока накопится энергия E_{0n}. Однако чтобы учесть общий случай передачи нескольких сообщений, мы при любой энергии e_0 будем оставлять блок из N_n промежутков времени до начала передачи (в противном случае из-за случайного характера величины e_0 придется изменять структуру этих промежутков и стратегии кодирования/декодирования для передачи каждого сообщения). При выводе нижних границ нужно иметь в виду следующие шаги.

1. Как и ранее, в фазе накопления энергия накапливается в течение N_n промежутков времени. Единственная разница состоит в том, что пороговое значение энергии увеличивается до $E_{0n} + e_0$. Однако формула (17) не изменяется, поскольку мы по-прежнему ставим цель накопить энергию E_{0n};
2. Величины V_i теперь выбираются гауссовскими с дисперсией $\mathbf{E}[E_1] + e_0/n$. В формуле (19) величина $\mathcal{A}_n$ заменяется на $\mathcal{A}'_n$, которая отличается от $\mathcal{A}_n$ только тем, что E_{0n} заменяется на $E_{0n} + e_0$. Положим

$$\mathcal{B}_n = \bigcap_{\ell=1}^{n} \{(\boldsymbol{v}^n, \boldsymbol{e}^n) : \; s'_\ell \geqslant -E_{0n}\}, \tag{61}$$

где $s'_\ell = \sum\limits_{k=1}^{\ell} (e_\ell - v_\ell^2 + e_0/n)$. Очевидно, все слагаемые в этой сумме н.о.р. с нулевым средним, как и требуется в неравенстве Колмогорова, и $\mathcal{B}_n \subset \mathcal{A}'_n$. В оценке для $\Pr(\mathcal{E}_1)$ никаких изменений не происходит.

С учетом этих изменений можно показать, что

$$\log M^*(n, \varepsilon) \geqslant nC_{EG}^{(n)} + \sqrt{n}\Big[\sqrt{V_{EG}^{(n)}}\Phi^{-1}(\lambda\varepsilon) - K_{\varepsilon,\lambda}C_{EG}^{(n)}\Big] - \log n + O(1), \tag{62}$$

где

$$C_{EG}^{(n)} = \frac{1}{2}\log\left(1 + \frac{\mathbf{E}[E_1] + e_0/n}{\sigma^2}\right), \quad V_{EG}^{(n)} = \frac{\mathbf{E}[E_1] + e_0/n}{\mathbf{E}[E_1] + \sigma^2 + e_0/n}\log_2^2(e).$$

Точная граница имеет вид

$$\log M^*(n, \varepsilon) \geqslant nC_{EG} + \sqrt{n}\left[\sqrt{V_{EG}}\Phi^{-1}(\lambda\varepsilon) - K_{\varepsilon,\lambda}C_{EG}\right] - \log n + \frac{e_0 K_{\varepsilon,\lambda}}{2\sigma^2\sqrt{n}} -$$
$$- \log \varepsilon K - \frac{K_{\varepsilon,\lambda}}{2} - \sqrt{V_{EG}}\Phi^{-1}(\lambda\varepsilon)\widehat{f}\left[\frac{4\sigma_E^2}{K_{\varepsilon,\lambda}\,\mathbf{E}[E_1]^2} + 2K + \lambda\right]. \tag{63}$$

Граница для СЭ-ДКБП аналогична границе (36), но с заменой $\mathbf{E}[E_1]$ на $\mathbf{E}[E_1] + e_0/n$. Заметим, что можно было бы и дальше упрощать выражение, выделяя члены с e_0/n из членов первого и второго порядка и собирая их в $O(1)$. Однако нам было важно

показать влияние начальной энергии, состоящее в том, что границы улучшаются, как и достижимая скорость.

При рассмотрении верхних границ будем предполагать, что перед началом передачи в накопителе энергии предварительно собрано некоторое детерминированное количество энергии, скажем, e_0. В качестве примера рассмотрим вывод обратной теоремы кодирования для СЭ-АБГШ-каналов. Заменим $\sum\limits_{k=1}^{n} e_k$ в (45) на $e_0 + \sum\limits_{k=1}^{n} e_k$. Положим $\overline{E}_n = \mathbf{E}[E_1] + e_0/n$. В качестве Q_Y возьмем $\mathcal{N}(0, \overline{E}_n)$. Дальше вплоть до (48) выполняются аналогичные шаги, но с указанными заменами. В (51) заменяем E_i на $E_i + e_0/n$, что не влияет на ИФР в данном случае. Отсюда получаем

$$\log M^*(n,\varepsilon) \leqslant nC_{EG}^{(n)} + \sqrt{nV_{EG2}^{(n)}}\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n - \log \varkappa + 2\varkappa\sqrt{V_{EG2}^{(n)}}\widehat{f}_2, \tag{64}$$

где

$$V_{EG2}^{(n)} = \frac{2\overline{E}_n^2 + \sigma_E^2 + 4\sigma^2\overline{E}_n}{4(\overline{E}_n + \sigma^2)^2}\log_2^2(e).$$

Далее, имеем

$$C_{EG}^{(n)} \leqslant C_{EG} + \frac{1}{2}\log\Bigl(1 + \frac{e_0}{n\sigma^2}\Bigr)$$

и

$$\bigl|V_{EG2}^{(n)} - V_{EG2}\bigr| \leqslant \frac{c_v e_0}{n}$$

для некоторой неотрицательной константы c_v. Таким образом, верхняя граница изменяется лишь в члене $O(1)$. Это не означает, что начальная энергия практически не оказывает никакого воздействия, а скорее значит, что с ростом n ее влияние значительно уменьшается; например, если $e_0 = O(n)$, то она будет влиять на член первого порядка. В обратной теореме кодирования для СЭ-ДКБП происходит то же самое, когда мы заменяем E_i на $E_i + e_0/n$. Член с e_0 поглощается в определении δ_n, данном в (56). Это снова приводит лишь к изменениям в $O(1)$, и наши границы остаются верными. Тем самым, мы заключаем, что начальная детерминированная энергия, накопленная в буфере, не влияет на члены первого и второго порядков в границах достижимости и верхних границах.

Остаточная энергия. В предыдущих рассуждениях количество начальной энергии предполагалось фиксированным. На практике, когда посылается несколько сообщений одно за другим, остаточное количество энергии после каждой успешной передачи изменяется случайным образом. Как и ранее, рассмотрим постановку задачи для СЭ-АБГШ-канала с n интервалами для передачи и фиксированной максимальной вероятностью ошибки ε. Для каждого сообщения, как и ранее, имеются фазы накопления и передачи. В дальнейшем будем предполагать, что если в течение передачи сообщения в некоторый момент энергии не хватило, то передача этого сообщения прекращается и оно возвращается передатчику. Однако энергия, накапливаемая в течение *оставшейся* части этого промежутка, сохраняется и будет использована при передаче следующего сообщения. В дальнейшем будем обозначать энергию, оставшуюся после передачи в ℓ-м промежутке, через R_ℓ. Выведем для нее оценки снизу r_ℓ.

Определим случайную последовательность r_ℓ следующим образом. Положим $r_0 = e_0$ для начальной энергии e_0 в начале промежутка $\ell = 1$. Тогда r_ℓ для $\ell \geqslant 1$ изменяется по закону

$$r_\ell = (r_{\ell-1} + \zeta_\ell)^+, \tag{65}$$

где

$$\zeta_\ell = \sum_{k=1}^{n+N_n} E_{(\ell-1)(n+N_n)+k} - \sum_{j=1}^{n} \Lambda(X_{(\ell-1)(n+N_n)+j}),$$

а $\Lambda(\cdot)$ – функция энергии, описанная ранее для СЭ-ДКБП и для СЭ-АБГШ-каналов, $\Lambda(x) = x^2$. Кроме того, $\mathbf{E}[\zeta_\ell] = (n+N_n)\,\mathbf{E}[E_1] - nP$ при $1 \leqslant \ell \leqslant L$, где предполагается, что входы канала X_i – н.о.р. случайные величины с конечным средним и $\mathbf{E}[\Lambda(X_i)] = P$, где P будет выбрано позже. Можно показать, что $r_\ell \leqslant R_\ell$ для $\ell \geqslant 1$. Соотношение (65) – это уравнение Линдли, хорошо известное при изучении систем массового обслуживания с очередями GI/GI/1 (см. [27]). Поэтому r_ℓ будет иметь стационарное распределение, если $\mathbf{E}[\zeta_1] < 0$. Однако для наших целей работа в таком режиме не дает ничего. Вместо этого мы будем выбирать $\mathbf{E}[\zeta_1] > 0$, но достаточно близкое к 0, благодаря чему

$$P \leqslant \left(1 + \frac{N_n}{n}\right) \mathbf{E}[E_1].$$

При таком выборе мы остаемся в описанных выше условиях и можем применять все приведенные выше результаты. Более того, остаточная энергия r_ℓ будет стремиться к ∞ с ростом ℓ. Из [28] получаем, что для r_ℓ справедливо

$$\frac{r_\ell}{\ell} \xrightarrow{p} \mathbf{E}[\zeta_1], \quad \frac{r_\ell - \ell\,\mathbf{E}[\zeta_1]}{\sqrt{\ell}\sigma_\zeta} \xrightarrow{d} \mathcal{N}(0,1) \tag{66}$$

при ℓ, стремящемся к бесконечности, где $\sigma_\zeta^2 = \mathrm{Var}(\zeta_1)$. Таким образом, при достаточно больших ℓ можно считать, что $e_0 = r_\ell \approx \ell\,\mathbf{E}[\zeta_1] - a\sqrt{\ell}\sigma_\zeta$, где a выбирается достаточно большим, чтобы событие $\dfrac{r_\ell - \ell\,\mathbf{E}[\zeta_1]}{\sqrt{\ell}\sigma_\zeta} \geqslant -a$ имело большую вероятность. Используя вышеупомянутые границы, зависящие от e_0, можно вывести нижнюю границу для остаточной энергии. У нас имеются дальнейшие улучшения этой аппроксимации, но для краткости изложения эти подробности мы опускаем.

§ 9. Асимптотика умеренных уклонений

В этом параграфе обсуждаются границы на асимптотическое поведение умеренных уклонений для СЭ-АБГШ-канала и СЭ-ДКБП. Здесь, в отличие от анализа вторых приближений в предыдущих параграфах, мы позволяем вероятности ошибки стремиться к нулю как функции от длины блока n. Однако так мы будем поступать в режиме умеренных уклонений, который формально определяется следующим образом (см. [16]).

Определение 3 (коэффициент умеренных уклонений). Для заданного канала W пусть ρ_n – последовательность неотрицательных вещественных чисел, такая что $\rho_n \to 0$ и $n\rho_n^2 \to \infty$. Тогда для кодов объема M_n, такого что $\log M_n = n(C - \rho_n)$, где C – пропускная способность канала, коэффициентом умеренных уклонений (КУУ) ξ называется предел (если он существует)

$$\xi = \lim_{n\to\infty} \frac{\log \varepsilon(n)}{n\rho_n^2},$$

где $\varepsilon(n)$ – вероятность ошибки как функция длины блока n.

Для каналов без памяти с дисперсией канала $V > 0$ в [16] было показано, что коэффициентом умеренных уклонений является $\xi = -\dfrac{1}{2V}$. В случае каналов со сбо-

ром энергии он устроен более сложно. Это происходит благодаря тому, что точное значение дисперсии не известно, а также в силу того, что каналы со сбором энергии на самом деле не являются каналами без памяти из-за наличия вектора энергии. Однако в их составе имеется подсистема без памяти, и именно этот факт мы все время использовали в нашем анализе.

9.1. КУУ для СЭ-АБГШ-каналов. Сформулируем теорему, дающую границу на КУУ для СЭ-АБГШ-каналов.

Теорема 5. *Для СЭ-АБГШ-канала, в котором процесс поступления энергии E_i – н.о.р. с дисперсией σ_E^2, КУУ удовлетворяет следующим неравенствам*:

$$\liminf_{n\to\infty} \frac{\log \varepsilon(n)}{n\rho_n^2} \geqslant -\frac{1}{2V_{EG2}}, \tag{67}$$

$$\limsup_{n\to\infty} \frac{\log \varepsilon(n)}{n\rho_n^2} \leqslant -\frac{1}{2V_{EG}}, \tag{68}$$

где V_{EG} определено в (11), *а V_{EG2} – в* (12).

Доказательство. Для доказательства (67) рассмотрим неравенство (47) с заменой ε на $\varepsilon(n)$, которое перепишем следующим образом:

$$\varepsilon(n) \geqslant \Pr\left[\log \frac{W(\boldsymbol{Y}^n \,|\, \boldsymbol{x}^n(\overline{m}, \boldsymbol{E}))}{Q_{Y^n}} \leqslant \log \gamma_n\right] - \frac{\gamma_n}{M}.$$

Кроме того, из (52) вытекает

$$\Pr\left[\log \frac{W(\boldsymbol{Y}^n \,|\, \boldsymbol{x}^n(\overline{m}, \boldsymbol{E}))}{Q_{Y^n}} \leqslant \log \gamma_n\right] = \Pr\left[\sum_{i=1}^n \eta_i \geqslant nC_{EG} - \log \gamma_n\right].$$

Теперь положим $\log M = n(C_{EG} - \rho_n)$ и $\log \gamma_n = n(C_{EG} - \alpha\rho_n)$ для любого $\alpha > 1$. Из [29, теорема 3.7.1] получаем

$$\liminf_{n\to\infty} \frac{\log \Pr\Big[\sum\limits_{i=1}^n \eta_i \geqslant nC_{EG} - \log \gamma_n\Big]}{n\rho_n^2} \geqslant -\inf_{x\geqslant\alpha} \frac{x^2}{2V_{EG2}} = -\frac{\alpha^2}{2V_{EG2}},$$

откуда, замечая, что V_{EG2} является дисперсией η_i, и устремляя $\alpha \to 1$, получаем (67).

Для доказательства границы (68) требуется модифицировать некоторые из наших аргументов, использовавшихся при обсуждении схемы накопления и передачи. Это связано с тем, что мы хотим показать существование кодов с $\log M = n(C_{EG} - \rho_n)$. До сих пор анализ проводился так, чтобы работать с оптимальным порядком $\sqrt{n}$, но теперь это не так, поскольку $\rho_n > 1/\sqrt{n}$.

Вспомним события $\mathcal{E}_0$ и $\mathcal{E}_1$, введенные, соответственно, в (17) и (20), и покажем, что при подходящем выборе N_n и E_{0n} можно добиться того, чтобы

$$\Pr(\mathcal{E}_0) + \Pr(\mathcal{E}_1) \leqslant \frac{\varepsilon(n)}{2}.$$

Для этого выбираем

$$N_n = \max\left\{\frac{16\sigma_E^2}{\varepsilon(n)\,\mathbf{E}[E_1]^2}, \frac{4\sqrt{n(2\,\mathbf{E}[E_1]^2 + \sigma_E^2)}}{\mathbf{E}[E_1]\sqrt{\varepsilon(n)}}\right\}.$$

Очевидно, $N_n \to \infty$ при $n \to \infty$, и при этом как $\Pr(\mathcal{E}_0)$, так и $\Pr(\mathcal{E}_1)$ ограничены сверху величиной $\varepsilon(n)/4$.

Следовательно, вероятность ошибки $\varepsilon(n)$ ограничена величиной

$$\varepsilon(n) \leqslant \frac{\varepsilon(n)}{2} + \Pr\left[\log\left(\frac{W^n(\boldsymbol{Y}^n \mid \boldsymbol{X}^n)}{P_{\boldsymbol{Y}^n}(\boldsymbol{Y}^n)}\right) \leqslant \log\gamma_n\right] + \frac{M}{\gamma_n},$$

$$\frac{\log(\varepsilon(n)/2)}{n\rho_n^2} \leqslant \frac{1}{n\rho_n^2}\log\left[\Pr\left\{\sum_{i=1}^n G_i \leqslant \log\gamma_n\right\} + 2^{-(1-\alpha)n\rho_n}\right].$$

Теперь положим $\log\gamma_n = n(C_{EG} - \alpha\rho_n)$, где $\alpha < 1$ и $\log M = n(C_{EG} - \rho_n)$. Коды такого объема существуют согласно лемме Файнштейна. Тогда из (25) и [29, теорема 3.7.1] получаем

$$\limsup_{n\to\infty} \frac{1}{n\rho_n^2}\log\Pr\left\{\sum_{i=1}^n G_i \leqslant \log\gamma_n\right\} \leqslant -\inf_{x\leqslant -\alpha}\frac{x^2}{2V_{EG}} = -\frac{\alpha^2}{2V_{EG}}. \tag{69}$$

Полагая $\alpha \to 1$, приходим к (68). ▲

9.2. КУУ для СЭ-ДКБП. Границы на КУУ для СЭ-ДКБП должны быть аналогичны границам для СЭ-АБГШ-канала. Однако поскольку V_{ED} изменяется при разном выборе λ, требуются некоторые уточнения.

Т е о р е м а 6. *Для СЭ-ДКБП справедливы следующие границы на КУУ*:

$$\liminf_{n\to\infty}\frac{\log\varepsilon(n)}{n\rho_n^2} \geqslant -\inf_{\eta>0}\frac{1}{2V_{\min,\eta}}, \tag{70}$$

$$\limsup_{n\to\infty}\frac{\log\varepsilon(n)}{n\rho_n^2} \leqslant -\frac{1}{2V_{\min}}, \tag{71}$$

где

$$V_{\min} = \min_{P\in\Gamma_{\mathbf{E}[E_1]}} V(P;W), \quad V_{\min,\eta} = \min_{P\in\Gamma_{\mathbf{E}[E_1]+\eta}} V(P;W),$$

а Γ – *множество распределений на входе, на которых достигается пропускная способность, принадлежащих множеству* $\mathcal{F}_{\mathbf{E}[E_1]}$.

Д о к а з а т е л ь с т в о. Граница (70) вытекает из [16, теорема 6] при следующих изменениях:

1. Распределения должны быть допустимыми, т.е. принадлежать $\mathcal{F}_{\overline{E}_n}$;
2. Следует заменить $\varepsilon(n)$ на $\varepsilon(n)+\tau_n$. Но в нашей конструкции $\tau_n < \varepsilon(n)/4$. Поэтому это то же самое, что и заменить $\varepsilon(n)$ на $\frac{5}{4}\varepsilon(n)$.

Для доказательства (71) заметим, что все шаги очень похожи на шаги в доказательстве (68). Для начала выбираем распределение P_X, на котором достигается пропускная способность, и выполняем точно такие же действия, как и раньше. Получаем

$$\limsup_{n\to\infty}\frac{\log\varepsilon(n)}{n\rho_n^2} \leqslant -\frac{1}{2V(P_X;W)}.$$

Поскольку это верно для любого $P_X \in \Gamma$, самая точная граница получается при замене $V(P_X;W)$ на $V_{\min}$. ▲

§ 10. Обсуждение и сравнение с предыдущими результатами

10.1. Сравнение с [14]. В работе [14] рассматривался вариант СЭ-АБГШ-канала, в котором энергия поступает блоками. В этой модели каждый блок имеет длину L, и процесс поступления н.о.р. поблочно. Внутри блока все поступления одинаковы. Изучалось влияние на скорости при конечной длине блока в случаях постоянного L, а также L, растущего сублинейно по n (т.е. $L = \omega(1)$). Для средней вероятности ошибки $0 \leqslant \varepsilon < 1/2$ было показано, что для такого СЭ-АБГШ-канала с блоковым поступлением энергии при постоянном L, достаточно больших n и единичной дисперсии шума справедливо

$$C_{EG} + V_\varepsilon^- \sqrt{\frac{L}{n}} - o\left(\sqrt{\frac{L}{n}}\right) \leqslant \frac{1}{n} M^*(n,\varepsilon) \leqslant C_{EG} + V_\varepsilon^+ \sqrt{\frac{L}{n}} + o\left(\sqrt{\frac{L}{n}}\right), \tag{72}$$

где

$$V_\varepsilon^- = \sup_{0<\lambda<1} -C_{EG} \sqrt{2\left(\frac{\mathbf{E}[E_1^2]}{\mathbf{E}[E_1]^2} + 1\right) \log \frac{1}{\lambda\varepsilon}} + \sqrt{\frac{\mathbf{E}[E_1](\log e)^2}{L(1+\mathbf{E}[E_1])} \Phi^{-1}((1-\lambda)\varepsilon)}, \tag{73}$$

$$V_\varepsilon^+ = \frac{\log e}{2(1+\mathbf{E}[E_1])} \sqrt{\sigma_E^2 + \frac{2\,\mathbf{E}[E_1](\mathbf{E}[E_1]+2)}{L}}\ \Phi^{-1}(\varepsilon). \tag{74}$$

Модель СЭ-АБГШ-канала, рассмотренная нами, по существу такая же, что и в [14], но у нас $L = 1$, и при этом в [14] рассматривался только критерий средней вероятности ошибки. При сравнении этого результата с (11) видно, что выражения совпадают за исключением первого члена, в котором содержится $\log \frac{1}{\lambda\varepsilon}$ вместо нашего $\frac{2}{\lambda\varepsilon}$. Таким образом, здесь коэффициенты вторых приближений несколько точнее наших. Что же касается выражения для V_ε^+, мы повторили его в точности, поскольку в этом случае использовалось альтернативное доказательство. В терминах техники доказательства в нашем случае мы разбили ограничения по сбору энергии на две части, а именно фазу сбора энергии и фазу передачи, и рассматривали их по отдельности (с помощью неравенства Колмогорова), в то время как в [14] они рассматривались вместе с помощью производящих функций моментов. Кроме того, в [14] использовалась гауссовость канала для упрощения выражений как в границе достижимости, так и в обратной теореме кодирования.

10.2. Альтернативная обратная теорема кодирования для СЭ-АБГШ-канала с использованием результатов работ [7, 18]. Метод модификации метаобращения теоремы кодирования из работы [7], который мы применили для канала со сбором энергии, применялся также в [18, Приложение III] для анализа квазистатических АБГШ-каналов с замиранием. Хотя мы и не смогли применить этот метод непосредственно из-за очень больших различий между рассматриваемыми моделями, наш подход в некотором смысле навеян им. Приведем также набросок альтернативного вывода верхней границы, предложенного рецензентом настоящей статьи.

В предположении средней вероятности ошибки ε пусть $\varepsilon(E^n)$ – средняя вероятность ошибки при заданной реализации энергии E^n. Заметим, что граница при средней вероятности ошибки будет ограничивать сверху границу при максимальной вероятности ошибки. Полагая $\overline{E}_n = \sum_{i=1}^n E_i/n$ и замечая, что условие на сбор энергии, при котором не происходит сбоя, равносильно $\sum_{i=1}^n X_i^2 \leqslant n\overline{E}_n$, при фиксированном большом n согласно [7] получаем

$$\varepsilon(E^n) \geqslant \Phi\left(\frac{\log M - nC(\overline{E}_n) - 1/2 \log n - K(\overline{E}_n)}{\sqrt{nV(\overline{E}_n)}}\right). \tag{75}$$

Вычисление математического ожидания относительно распределения E^n в соотношении (75) должно привести к желаемой обратной теореме кодирования. Получаем

$$\varepsilon \geqslant \mathbf{E}\,\Phi\left(\frac{\log M - nC(\overline{E}_n) - 1/2\log n - K(\overline{E}_n)}{\sqrt{nV(\overline{E}_n)}}\right). \tag{76}$$

Чтобы внести математическое ожидание под знак функции Φ, заметим, что для любой веществennозначной случайной величины U справедливо

$$\mathbf{E}\,\Phi\left(\frac{U+a}{b}\right) = \Pr(U \geqslant bZ - a) = \int\limits_{-\infty}^{\infty} f_Z(z)\Pr(U \geqslant bz - a)\,dz, \tag{77}$$

где $Z \sim N(0,1)$. Если U – независимая гауссовская величина с нулевым средним и дисперсией σ_U^2, то (77) равно $\Phi\Big(\frac{a}{\sqrt{b^2+\sigma_U^2}}\Big)$. С помощью разложения в ряд Тейлора по $V(\overline{E}_n)$, соотношения (77) и теоремы Берри – Эссеена неравенство (76) приводится к виду

$$\varepsilon \geqslant \mathbf{E}\,\Phi\left(\frac{\log M - nC(\overline{E}_n) - 1/2\log n - K(\overline{E}_n)}{\sqrt{nV_{EG2}}}\right) - \frac{c_1(\mathcal{E}[E_1])}{n^{1/3}} \tag{78}$$

для постоянной $c_1(\mathcal{E}[E_1])$, не зависящей от n. Применяя неравенство

$$C(\overline{E}_n) \leqslant C_{EG} + \frac{\overline{E}_n - \mathbf{E}[E_1]}{2(\mathbf{E}[E_1] + \sigma^2)}$$

и равномерную оценку для $K(\overline{E}_n)$, получаем верхнюю границу

$$\begin{aligned}\log M &\leqslant nC(P) + \sqrt{nV_{EG}}\Phi^{-1}\left(\varepsilon + \frac{c_1(\mathbf{E}[E_1])}{n^{1/3}} + \frac{c_2}{\sqrt{n}}\right) + 0{,}5\log n + O(1) \leqslant \\ &\leqslant nC(P) + \sqrt{nV_{EG}}\Phi^{-1}(\varepsilon) + n^{1/6}c_1(\mathbf{E}[E_1]) + 0{,}5\log n + O(1),\end{aligned} \tag{79}$$

что слабее, чем (12). Кроме того, в этом доказательстве неявно используются свойства структуры гауссовского канала, которые нельзя напрямую применить к СЭ-ДКБП. Однако это дает прямой способ получения верхних границ (не обязательно наилучших) на скорости для каналов специального вида (таких как каналы с замиранием) при наличии АБГШ; дальнейшие подробности см. в [18].

§ 11. Численные результаты

Здесь мы представляем в виде графиков результаты вычислений границ при конечной длине блока для скорости, а также для для числа интервалов времени, необходимых для фазы накопления в схеме накопления и передачи, в зависимости от длины блока. Для вычислений этих величин использовались выведенные выше формулы при конкретных наборах значений параметров. Для случая СЭ-ДКБП описаны двоичный симметричный канал (ДСК) и двоичный канал со стиранием (ДКС) со сбором энергии, и для них построены графики соответствующих границ. Отметим, что на всех графиках не учитывались постоянные члены в границах для скоростей, т.е. коэффициенты в $O(1/n)$. Кроме этого, наши результаты сравнивались с нижними границами при конечной длине блока для эквивалентного канала без сбора энергии. Например, в случае СЭ-АБГШ-канала рассматривался АБГШ-канал с ограничением на среднюю мощность $\mathbf{E}[E_1]$, а в случае СЭ-ДКБП – соответствующие ДКБП с ограничением по мощности $\mathbf{E}[E_1]$. В случаях, когда нижняя граница

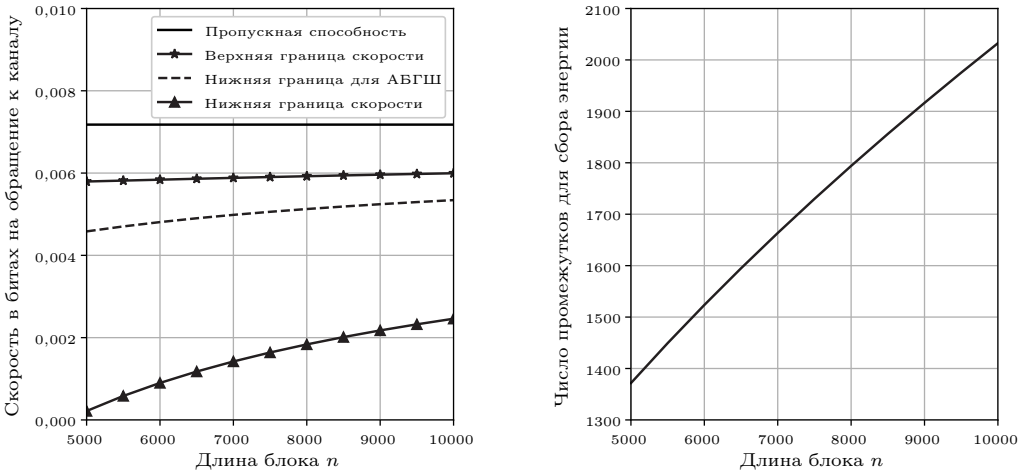

Рис. 2. Графики скоростей для СЭ-АБГШ-канала в зависимости от общей длины блока (сбор энергии плюс передача) в режиме низких ОСШ. На втором графике показано число промежутков времени, необходимых для сбора энергии

для эквивалентного канала оказывается выше верхней границы для канала со сбором энергии, это позволяет сделать выводы о влиянии сбора энергии на скорость. В дальнейшем под разрывом между скоростями мы подразумеваем эту разность между границами, деленную на верхнюю границу и выраженную в процентах.

11.1. Результаты для СЭ-АБГШ-канала. Выбираются максимальная вероятность ошибки $\varepsilon = 0{,}1$, $\mathbf{E}[E_1] = 1$ и $\sigma_E^2 = 5$. Длины блока n берутся в промежутке от 5000 до 10000. Рассматриваются три различных режима:

1. Низкие ОСШ (-20 дБ). В этом режиме (рис. 2) видно, что нижняя граница дает плохое приближение к скорости при конечной длине блока. Из-за большего количества ошибок в этом режиме требуется также большее количество промежутков времени для сбора энергии (примерно от 20,5% до 27,6%), чтобы снизить ошибки, вызываемые сбоями.
2. Умеренные ОСШ (0 дБ). По сравнению с низкими ОСШ этот режим (см. рис. 3) дает лучшее приближение к скорости при конечной длине блока. Разрыв между скоростями значительно снижается и составляет примерно от 19% до 27%. При этом число промежутков времени в фазе накопления также значительно снижается (от 16% до 22%).
3. Высокие ОСШ (20 дБ). В этом режиме (рис. 4) разрыв между скоростями составляет примерно от 18,2% до 24,2%, а число промежутков времени в фазе накопления находится между 15,8% и 21,6%. Это результат улучшения по сравнению с умеренными ОСШ, и он не столь значителен, как при переходе от низких ОСШ к умеренным.

Итак, границы при конечной длине блока достаточно хорошо аппроксимируют скорость при конечной длине блока в режимах умеренных и высоких значений ОСШ. Дальнейшие улучшения потребуют улучшения нижней границы, что в свою очередь может потребовать изменения схемы передачи. За исключением случая низких ОСШ, мы видим, что верхняя граница передачи со сбором энергии лежит ниже нижней границы для эквивалентного АБГШ-канала. Отсюда можно заключить, что скорости передачи со сбором энергии при конечной длине блока ниже, чем для случая передачи без сбора энергии, в режимах умеренных и высоких ОСШ.

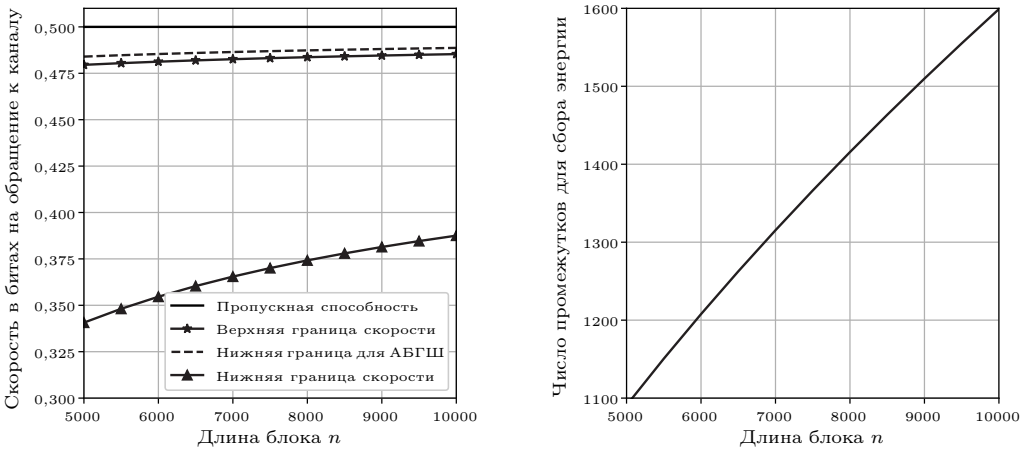

Рис. 3. Графики скоростей для СЭ-АБГШ-канала в зависимости от общей длины блока (сбор энергии плюс передача) в режиме умеренных ОСШ. На втором графике показано число промежутков времени, необходимых для сбора энергии

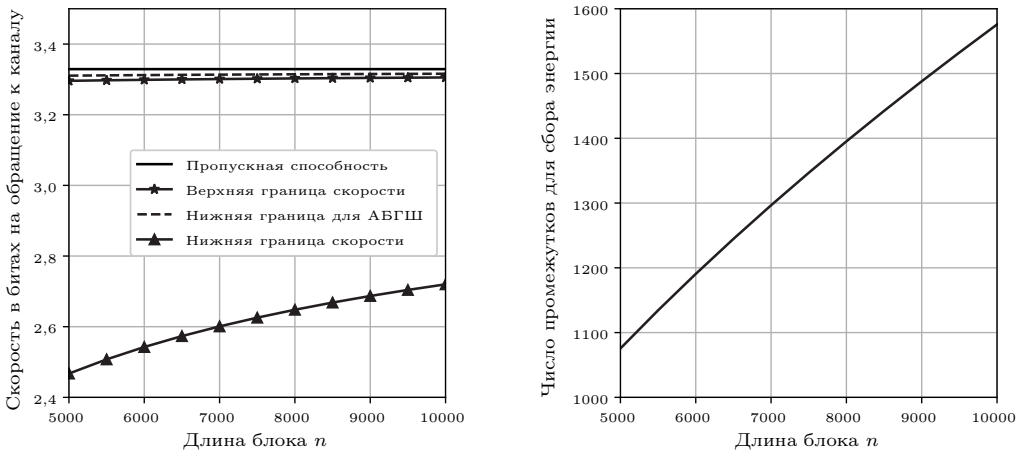

Рис. 4. Графики скоростей для СЭ-АБГШ-канала в зависимости от общей длины блока (сбор энергии плюс передача) в режиме высоких ОСШ. На втором графике показано число промежутков времени, необходимых для сбора энергии

11.2. СЭ-ДСК. Рассмотрим двоичный симметричный канал W с вероятностью перехода α, т.е. $\mathcal{X} = \mathcal{Y} = \{0,1\}$, $W(0\,|\,1) = W(1\,|\,0) = \alpha$. Положим $p_0 := \Pr(X = 0)$. Если распределение, на котором достигается пропускная способность, удовлетворяющее условиям по сбору энергии, единственно при указанном p_0, то

$$C_{ED} = C_{\text{ДСК}} = h(\alpha p_0 + \overline{\alpha}\,\overline{p}_0) - h(\alpha),$$

$$V(P;W) = V_{\text{ДСК}} = \sum_{x\in\{\alpha,\overline{\alpha}\}} \sum_{y\in\{p_0,\overline{p}_0\}} xy \left[\log\left(\frac{x}{xy + \overline{x}\,\overline{y}}\right)\right]^2 - C^2_{\text{ДСК}},$$

где $\overline{u} := 1-u$, а $h(x) = -x\log_2(x) - \overline{x}\log_2(\overline{x})$ – функция двоичной энтропии. Заметим, что такой выбор p_0 обусловлен ограничениями по сбору энергии. В этом примере выбраны $\alpha = 0{,}05$, функция энергии $\Lambda(x) = 3x$ и $\mathbf{E}[E_1] = 1$. Этим гарантирует-

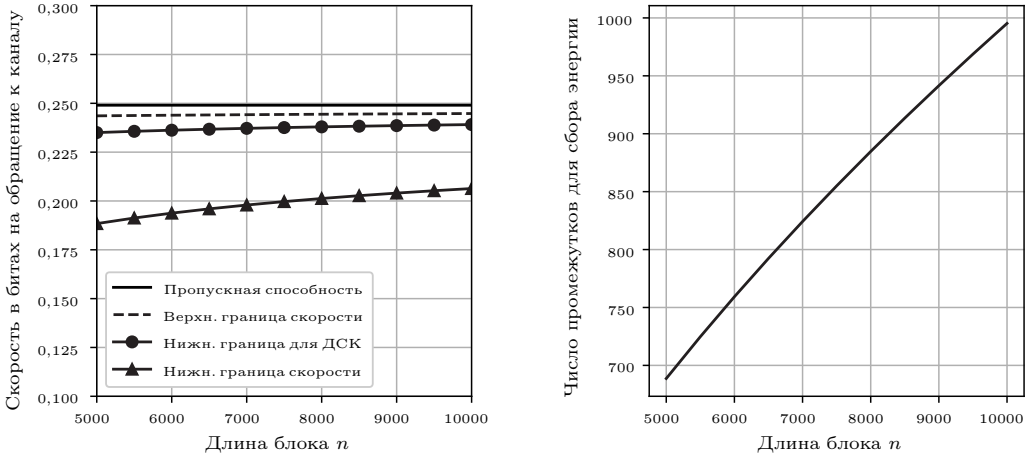

Рис. 5. Графики скоростей для СЭ-ДСК в зависимости от общей длины блока (сбор энергии плюс передача). На правом графике показано число промежутков времени, необходимых для сбора энергии

ся единственность распределения, на котором достигается пропускная способность, при $p_0 = 2/3$. Здесь мы берем $\varepsilon = 0{,}1$ и $\sigma_E^2 = 0{,}2$. На рис. 5 построены нижняя и верхняя границы для этого примера для значений n от 5000 до 10000.

Видно, что разница между верхней и нижней границами для этого примера составляет от 13,7% до 23%. Длина, необходимая для сбора энергии, варьируется при выбранных параметрах от 9,8% до 13,8%. В этом случае нижняя граница передачи без сбора энергии лежит ниже верхней границы передачи со сбором энергии. Следовательно, в этом случае нельзя сделать никакого вывода о скоростях в зависимости от σ_E^2.

11.3. СЭ-ДКС. Двоичный канал со стиранием W – это канал с двоичными входами $\mathcal{X} = \{0, 1\}$, троичными выходами $\mathcal{Y} = \{0, E_R, 1\}$, такой что $W(0\,|\,0) = W(1\,|\,1) = 1 - \alpha$ и $W(E_R\,|\,0) = W(E_R\,|\,1) = \alpha$, где α – вероятность стирания. Аналогично случаю ДСК, если имеется единственное распределение, на котором достигается пропускная способность, с $p_0 = \Pr(X = 0)$, то

$$C_{ED} = C_{\text{ДКС}} = (1 - \alpha)h(p_0),$$
$$V(P; W) = V_{\text{ДКС}} = (1 - \alpha)p_0(\log(p_0))^2 + (1 - \alpha)(1 - p_0)(\log(1 - p_0))^2 - C_{\text{ДКС}}^2.$$

При тех же значениях параметров, что и для случая ДСК, получаем графики границ, представленные на рис. 6.

Для выбранных значений параметров наблюдается разница между верхней и нижней границами от 8,6% до 12,2%, а число промежутков времени для сбора энергии составляет от 9,3% до 12,8%. Здесь наши границы дают лучшее приближение к скоростям, в отличие от случая ДСК. Кроме того, в этом случае нижняя граница передачи без сбора энергии лежит выше верхней границы, что означает, что в этом случае влияние сбора энергии ухудшает скорость.

11.4. Влияние дисперсии процесса сбора энергии $\boldsymbol{\sigma_E^2}$. Сравнивая границы (11) и (12), полученные для СЭ-АБГШ-канала, мы видим, что обе границы понижаются с ростом σ_E^2. Это показано на рис. 7. Интересно, что по сравнению с нижними границами для АБГШ-канала верхние границы для СЭ-АБГШ-канала отличаются лишь на $O(\log n/n)$ при $\sigma_E^2 = 0$. Однако нижние границы сильнее подвергаются влиянию дисперсии.

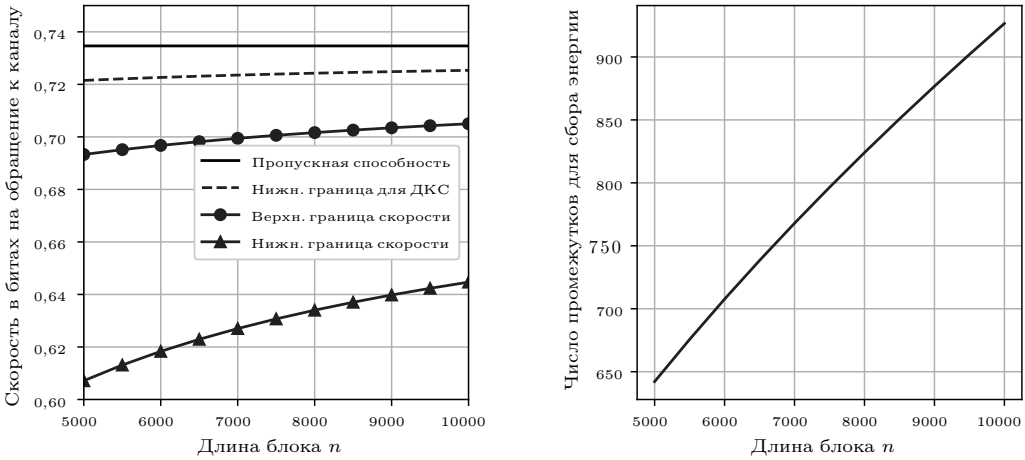

Рис. 6. Графики скоростей для СЭ-ДКС в зависимости от общей длины блока (сбор энергии плюс передача). На правом графике показано число промежутков времени, необходимых для сбора энергии

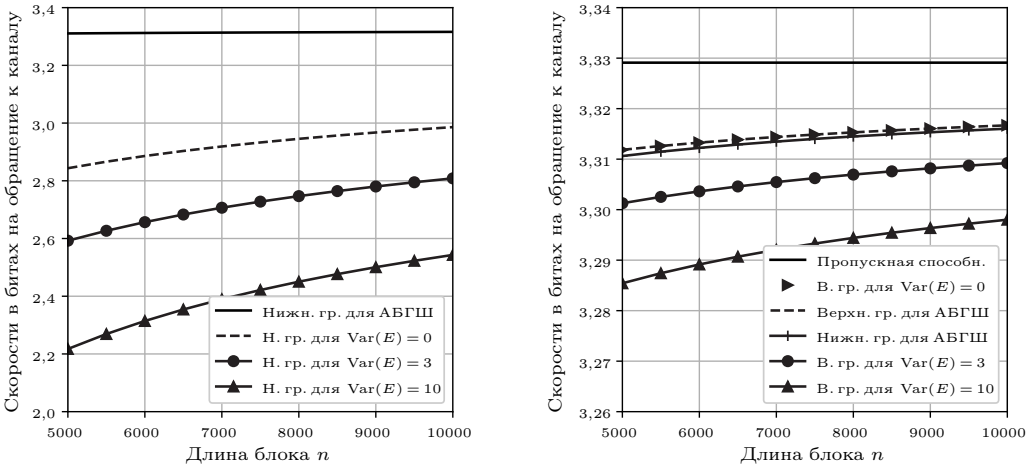

Рис. 7. Графики скоростей при конечной длине блока для СЭ-АБГШ-канала при различных значениях дисперсии процесса сбора энергии

§ 12. Обсуждение результатов и заключение

В статье показано, что как для СЭ-АБГШ-канала, так и для СЭ-ДКБП объем кода при конечной длине блока ведет себя как $nC - \Theta(\sqrt{n})$ при критерии максимальной вероятности ошибки. Это показано с помощью вывода нижних и верхних границ второго порядка по $\sqrt{n}$. Также получена оценка асимптотики умеренных уклонений для обоих типов каналов.

Кроме того, построены графики этих границ для нескольких примеров. В некоторых случаях, таких как АБГШ-канал со значениями ОСШ от умеренных до высоких, а также в случае ДКС наблюдалось, что скорости ухудшаются с ростом дисперсии процесса сбора энергии. Для дальнейшей проверки этой гипотезы было бы желательно уменьшить зазор между нижними и верхними границами. В дальнейших исследованиях было бы полезно получить согласующиеся границы при конечной длине блока и в режиме умеренных уклонений.

Авторы благодарны рецензентам за ценные замечания и предложения, позволившие прояснить некоторые понятия и исправить ошибку в рукописи статьи.

ПРИЛОЖЕНИЕ A: ДОКАЗАТЕЛЬСТВО ГРАНИЦЫ (41)

Пусть $U \in [M]$ – передаваемое сообщение и аналогично $\widehat{U}$ – декодированное сообщение. Для канала W при максимальной вероятности ошибки ε имеются следующие шаги:

$$1-\varepsilon \leqslant \Pr\bigl[\widehat{U}=m \,|\, U=m\bigr] =$$
$$= \int\limits_{\boldsymbol{y},\boldsymbol{e}} \Pr\bigl[\widehat{U}=m \,|\, \boldsymbol{Y}=\boldsymbol{y}\bigr] W(\boldsymbol{y} \,|\, c(m,\boldsymbol{e}))\, dP_{\boldsymbol{E}}(\boldsymbol{e}), \tag{80}$$

причем это справедливо для любого сообщения m.

Далее, $\Pr\bigl[\widehat{U}=m \,|\, \boldsymbol{Y}=\boldsymbol{y}\bigr]$ – тест на приемном конце, обеспечивающий условие на вероятность ошибки. Даже если он не зависит от $\boldsymbol{e}$, поскольку декодер не имеет доступа к отсчетам энергии, он все равно является достоверным тестом на $(\boldsymbol{y},\boldsymbol{e})$.

Теперь представим себе, что вместо канала W сообщение посылается по вспомогательному каналу Q_Y, игнорирующему вход, но имеющему тот же алфавит на выходе. При использовании указанного декодирования пусть $\overline{m}$ – сообщение, на котором достигается максимальная вероятность ошибки относительно распределения Q_Y. Тогда, очевидно, $P\bigl(\widehat{U}=\overline{m} \,|\, U=\overline{m}\bigr) \leqslant \dfrac{1}{M}$ относительно Q_Y. Но тогда из (80) и определения β-функции ошибки получаем

$$\beta_{1-\varepsilon}\left(W(\,\cdot \,|\, c(\overline{m},*))P_{\boldsymbol{E}}(*), Q_{\boldsymbol{Y}}P_{\boldsymbol{E}}\right) \leqslant \int\limits_{\boldsymbol{y}} P\bigl(\widehat{U}=\overline{m} \,|\, \boldsymbol{Y}=\boldsymbol{y}\bigr)\, dQ_{\boldsymbol{Y}}(\boldsymbol{y}) \leqslant \frac{1}{M}.$$

ПРИЛОЖЕНИЕ B: ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4

До определенного момента следуем тем же шагам, что и в доказательстве исходного метаобращения теоремы кодирования (см. [7]). Для заданного распределения $Q_{\boldsymbol{Y}}$, которое по существу является контрольным каналом, не зависящим от входа, пусть максимальная вероятность ошибки этого "канала" равна ε'. Пусть U – случайная величина, обозначающая посылаемое сообщение, а $\widehat{U}$ – декодированное сообщение.

Рассмотрим определение максимальной вероятности ошибки. Имеется сообщение (назовем его $\overline{m}$), такое что

$$1-\varepsilon' = \Pr\bigl[\widehat{U}=\overline{m} \,|\, U=\overline{m}\bigr] = \int\limits_{\boldsymbol{y}} P_{\widehat{U}\,|\,\boldsymbol{Y}}(\overline{m} \,|\, \boldsymbol{y})\, dQ_{\boldsymbol{Y}}(\boldsymbol{y}). \tag{81}$$

Но при этом

$$1-\varepsilon' = \min_m \Pr\bigl[\widehat{U}=m \,|\, U=m\bigr] \leqslant \frac{1}{M}\sum_{m=1}^{M} \Pr\bigl[\widehat{U}=m \,|\, U=m\bigr] =$$
$$= \frac{1}{M}\sum_{m=1}^{M} \int\limits_{\boldsymbol{y}} \Pr\bigl[\widehat{U}=m \,|\, \boldsymbol{Y}=\boldsymbol{y}\bigr]\, dQ_{\boldsymbol{Y}}(\boldsymbol{y}) =$$
$$= \frac{1}{M}\int\limits_{\boldsymbol{y}} \left(\sum_{m=1}^{M} \Pr\bigl[\widehat{U}=m \,|\, \boldsymbol{Y}=\boldsymbol{y}\bigr]\right) dQ_{\boldsymbol{Y}}(\boldsymbol{y}) = \frac{1}{M}. \tag{82}$$

Объединяя (81) и (82), получаем

$$M \leqslant \frac{1}{\int\limits_{\boldsymbol{y}} P_{\widehat{U}\,|\,\boldsymbol{Y}}(\overline{m}\,|\,\boldsymbol{y})\,dQ_{\boldsymbol{Y}}(\boldsymbol{y})}. \tag{83}$$

Далее, для любого $\mathcal{E}_1 \subset \mathbb{R}_+^n$ справедливо

$$1-\varepsilon \leqslant \int\limits_{\boldsymbol{e}}\int\limits_{\boldsymbol{y}} P_{\widehat{U}\,|\,\boldsymbol{Y}}(\overline{m}\,|\,\boldsymbol{y})\,dP_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\boldsymbol{y}\,|\,c(\overline{m},\boldsymbol{e}))\,dP_{\boldsymbol{E}}(\boldsymbol{e}) \leqslant$$

$$\leqslant \int\limits_{\boldsymbol{e}\in\mathcal{E}_1}\int\limits_{\boldsymbol{y}} P_{\widehat{U}\,|\,\boldsymbol{Y}^n}(\overline{m}\,|\,\boldsymbol{y})\,dP_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\boldsymbol{y}\,|\,c(\overline{m},\boldsymbol{e}))\,dP_{\boldsymbol{E}}(\boldsymbol{e}) + P_{\boldsymbol{E}}(\mathcal{E}_1^c).$$

Преобразуя это выражение, используя определения, данные в условии леммы, и полагая $\mathcal{E}_1 = \Big\{\boldsymbol{e}:\ \sum\limits_{i=1}^{n} e_i \leqslant n\overline{E}_n\Big\}$ и $\tau_n = P_E(\mathcal{E}_1^c)$, получаем

$$1-\varepsilon-\tau_n \leqslant \int\limits_{\boldsymbol{e}\in\mathcal{E}_1}\int\limits_{\boldsymbol{y}} P_{\widehat{U}\,|\,\boldsymbol{Y}}(\overline{m}\,|\,\boldsymbol{y})\,dP_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\boldsymbol{y}\,|\,c(\overline{m},\boldsymbol{e}))\,dP_{\boldsymbol{E}}(\boldsymbol{e}) \implies \tag{84}$$

$$\implies 1-\varepsilon-\tau_n \leqslant \frac{1-\varepsilon-\tau_n}{1-\tau_n} \leqslant$$

$$\leqslant \int\limits_{\boldsymbol{y}} P_{\widehat{U}\,|\,\boldsymbol{Y}}(\overline{m}\,|\,\boldsymbol{y})\left\{\int\limits_{\boldsymbol{e}\in\mathcal{E}_1} dP_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\boldsymbol{y}\,|\,c(\overline{m},\boldsymbol{e}))\frac{dP_{\boldsymbol{E}}(\boldsymbol{e})}{1-\tau_n}\right\}. \tag{85}$$

Заметим, что мы делим на $1-\tau_n$, чтобы обеспечить, что выражение в фигурных скобках является распределением вероятностей. Из (83), (85) и определения β-функции ошибки получаем

$$\frac{1}{M} \geqslant \beta_{1-\varepsilon-\tau_n}\left(\int\limits_{\boldsymbol{e}\in\mathcal{E}_1} dP_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\,\cdot\,|\,c(\overline{m},\boldsymbol{e}))\frac{dP_{\boldsymbol{E}}(\boldsymbol{e})}{1-\tau_n}, Q_{\boldsymbol{Y}}\right) \geqslant$$

$$\geqslant \inf_{\boldsymbol{x}\in\mathbb{F}_{\overline{E}_n}} \beta_{1-\varepsilon-\tau_n}\left(\int\limits_{\boldsymbol{e}\in\mathcal{E}_1} dP_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\,\cdot\,|\,\boldsymbol{x})\frac{dP_{\boldsymbol{E}}(\boldsymbol{e})}{1-\tau_n}, Q_{\boldsymbol{Y}}\right) =$$

$$= \inf_{\boldsymbol{x}\in\mathbb{F}_{\overline{E}_n}} \beta_{1-\varepsilon-\tau_n}\big(P_{\boldsymbol{Y}\,|\,\boldsymbol{X}}(\,\cdot\,|\,\boldsymbol{x}), Q_{\boldsymbol{Y}}\big).$$

Отметим, что здесь мы можем брать инфимум по неслучайному множеству $\mathbb{F}_{\overline{E}_n}$, поскольку из $e^n \in \mathcal{E}_1$ вытекает, что $c(\overline{m}, e^n) \in \mathbb{F}$. Следовательно, получаем (43).

СПИСОК ЛИТЕРАТУРЫ

1. *Shenoy K.G., Sharma V.* Finite Blocklength Achievable Rates for Energy Harvesting AWGN Channels with Infinite Buffer // Proc. 2016 IEEE Int. Symp. on Information Theory (ISIT'2016). Barcelona, Spain. July 10–15, 2016. P. 465–469. https://doi.org/10.1109/ISIT.2016.7541342
2. *Kamalinejad P., Mahapatra C., Sheng Z., Mirabbasi S., Leung V.C., Guan Y.L.* Wireless Energy Harvesting for the Internet of Things // IEEE Commun. Mag. 2015. V. 53. № 6. P. 102–108. https://doi.org/10.1109/MCOM.2015.7120024

3. *Ku M.-L., Li W., Chen Y., Liu K.R.* Advances in Energy Harvesting Communications: Past, Present, and Future Challenges // IEEE Commun. Surv. Tutor. 2016. V. 18. № 2. P. 1384–1412. https://doi.org/10.1109/COMST.2015.2497324
4. *Raza M., Aslam N., Le-Minh H., Hussain S., Cao Y., Khan N.M.* A Critical Analysis of Research Potential, Challenges, and Future Directives in Industrial Wireless Sensor Networks // IEEE Commun. Surv. Tutor. 2017. V. 20. № 1. P. 39–95. https://doi.org/10.1109/COMST.2017.2759725
5. *Strassen V.* Asymptotische Abschätzungen in Shannons Informationstheorie // Trans. 3rd Prague Conf. on Information Theory, Statistical Decision Functions, Random Processes held at Liblice near Prague. June 5–13, 1962. Prague: Czechoslovak Acad. Sci., 1964. P. 689–723.
6. *Hayashi M.* Information Spectrum Approach to Second-Order Coding Rate in Channel Coding // IEEE Trans. Inform. Theory. 2009. V. 55. № 11. P. 4947–4966. https://doi.org/10.1109/TIT.2009.2030478
7. *Polyanskiy Y., Poor H.V., Verdú S.* Channel Coding Rate in the Finite Blocklength Regime // IEEE Trans. Inform. Theory. 2010. V. 56. № 5. P. 2307–2359. https://doi.org/10.1109/TIT.2010.2043769
8. *Polyanskiy Y., Poor H.V., Verdú S.* New Channel Coding Achievability Bounds // Proc. 2008 IEEE Int. Symp. on Information Theory (ISIT'2008). Toronto, ON, Canada. July 6–11, 2008. P. 1763–1767. https://doi.org/10.1109/ISIT.2008.4595291
9. *Tomamichel M., Tan V.Y.F.* A Tight Upper Bound for the Third-Order Asymptotics for Most Discrete Memoryless Channels // IEEE Trans. Inform. Theory. 2013. V. 59. № 11. P. 7041–7051. https://doi.org/10.1109/TIT.2013.2276077
10. *Tomamichel M., Tan V.Y.F.* Second-Order Coding Rates for Channels with State // IEEE Trans. Inform. Theory. 2014. V. 60. № 8. P. 4427–4448. https://doi.org/10.1109/TIT.2014.2324555
11. *Rajesh R., Sharma V., Viswanath P.* Capacity of Gaussian Channels with Energy Harvesting and Processing Cost // IEEE Trans. Inform. Theory. 2014. V. 60. № 5. P. 2563–2575. https://doi.org/10.1109/TIT.2014.2311822
12. *Ozel O., Ulukus S.* Achieving AWGN Capacity under Stochastic Energy Harvesting // IEEE Trans. Inform. Theory. 2012. V. 58. № 10. P. 6471–6483. https://doi.org/10.1109/TIT.2012.2204389
13. *Yang J.* Achievable Rate for Energy Harvesting Channel with Finite Blocklength // Proc. 2014 IEEE Int. Symp. on Information Theory (ISIT'2014). Honolulu, HI, USA. June 29 – July 4, 2014. P. 811–815. https://doi.org/10.1109/ISIT.2014.6874945
14. *Fong S.L., Tan V.Y.F., Özgür A.* On Achievable Rates of AWGN Energy-Harvesting Channels with Block Energy Arrival and Non-vanishing Error Probabilities // IEEE Trans. Inform. Theory. 2018. V. 64. № 3. P. 2038–2064. https://doi.org/10.1109/TIT.2017.2765545
15. *Altuğ Y., Wagner A.B.* Moderate Deviations in Channel Coding // IEEE Trans. Inform. Theory. 2014. V. 60. № 8. P. 4417–4426. https://doi.org/10.1109/TIT.2014.2323418
16. *Polyanskiy Y., Verdú S.* Channel Dispersion and Moderate Deviations Limits for Memoryless Channels // Proc. 48th Annu. Allerton Conf. on Communication, Control, and Computation. Monticello, IL, USA. Sept. 29 – Oct. 1, 2010. P. 1334–1339. https://doi.org/10.1109/ALLERTON.2010.5707068
17. *Truong L.V., Tan V.Y.F.* Moderate Deviation Asymptotics for Variable-Length Codes with Feedback, https://arXiv.org/abs/1707.04850v2 [cs.IT], 2017.
18. *Yang W., Durisi G., Koch T., Polyanskiy Y.* Quasi-static Multiple-Antenna Fading Channels at Finite Blocklength // IEEE Trans. Inform. Theory. 2014. V. 60. № 7. P. 4232–4265. https://doi.org/10.1109/TIT.2014.2318726
19. *Cover T.M., Thomas J.A.* Elements of Information Theory. Hoboken, NJ, USA: Wiley, 2006.
20. *Han T.S.* Information-Spectrum Methods in Information Theory. Berlin: Springer, 2003.
21. *Csiszár I., Körner J.* Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge: Cambridge Univ. Press, 2011.

22. *Kostina V., Verdú S.* Channels with Cost Constraints: Strong Converse and Dispersion // IEEE Trans. Inform. Theory. 2015. V. 61. № 5. P. 2415–2429. https://doi.org/10.1109/TIT.2015.2409261
23. *El Gamal A., Kim Y.-H.* Network Information Theory. Cambridge: Cambridge Univ. Press, 2011.
24. *Athreya K.B., Lahiri S.N.* Probability Theory. New Delhi, India: Hindustan Book Agency, 2006.
25. *Тюрин И.С.* Уточнение верхних оценок констант в теореме Ляпунова // УМН. 2010. Т. 65. № 3 (393). С. 201–202. https://doi.org/10.4213/rm9337
26. *Sun Y., Baricz Á., Zhou S.* On the Monotonicity, log-Concavity, and Tight Bounds of the Generalized Marcum and Nuttall Q-Functions // IEEE Trans. Inform. Theory. 2010. V. 56. № 3. P. 1166–1186. https://doi.org/10.1109/TIT.2009.2039048
27. *Wolff R.W.* Stochastic Modeling and the Theory of Queues. Englewood Cliffs, NJ: Prentice Hall, 1989.
28. *Gut A.* Stopped Random Walks. New York: Springer, 2009.
29. *Dembo A., Zeitouni O.* Large Deviations Techniques and Applications. Berlin: Springer, 2009. Corrected printing of the 1998 ed.

Шеной Кончади Гаутам
Шарма Виной
Отделение техники электросвязи,
Индийский научный институт, Бангалор, Индия
konchady@iisc.ac.in
vinod@iisc.ac.in

Поступила в редакцию
22.02.2019
После доработки
08.10.2020
Принята к публикации
15.12.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 2021 Вып. 1

УДК 621.391 : 519.72 : 004.7

© 2021 г. К.Г. Бенерджи, М.К. Гупта

КОМПРОМИССНОЕ СООТНОШЕНИЕ МЕЖДУ СТОИМОСТЬЮ ХРАНЕНИЯ И ВОССТАНОВЛЕНИЯ ДЛЯ НЕОДНОРОДНЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ[1]

Рассматриваются неоднородные распределенные системы хранения данных (РСХД), имеющие переменную степень реконструкции, где каждый узел системы имеет свою собственную ширину восстановления и свой собственный объем памяти. В частности, устройство сбора данных может реконструировать файл с помощью некоторых k узлов системы, а в случае отказа узла систему можно восстановить по некоторому множеству активных узлов. С помощью границы минимального разреза исследуется фундаментальное компромиссное соотношение между стоимостью хранения и восстановления для нашей модели неоднородной РСХД. Кроме того, задача формулируется как оптимизационная задача двухкритериального линейного программирования для различных неоднородных РСХД. Для некоторых РСХД показано, что полученная граница минимального разреза точна.

Ключевые слова: облачное хранилище, коды для распределенного хранения данных, неоднородная распределенная система хранения данных, информационный поток, компромиссное соотношение между стоимостью хранения и восстановления.

DOI: 10.31857/S0555292321010022

§ 1. Введение

Облачное хранилище – это распределенная система хранения данных (РСХД), в которой информация хранится в избыточном виде в различных узлах в виде закодированных пакетов. Для получения файла необходимо установить соединение с определенными узлами системы. В случае отказа узла его можно восстановить с помощью других узлов системы. Для таких РСХД требуется оптимизировать различные параметры системы, такие как объем памяти, ширина восстановления, доступность, надежность, безопасность и масштабируемость. Подобные РСХД используются во многих коммерческих системах, таких как Facebook, Yahoo!, IBM, Amazon и Microsoft Windows Azure [1–4].

В однородных РСХД (где каждый узел имеет одинаковый объем памяти и одинаковую степень восстановления) [5] закодированные пакеты данных из файла объема B распределяются между n узлами (каждый узел имеет объем памяти α) таким образом, что установив соединение с любыми k ($< n$) узлами, можно получить весь файл. В случае отказа произвольного узла система восстанавливается путем загрузки β пакетов из любых d ($< n$) активных узлов, называемых вспомогательными [5]. В таких системах надежность можно обеспечить или простым дублированием, или

[1] Предварительная английская версия данной статьи доступна по адресу https://arXiv.org/abs/1503.02276.

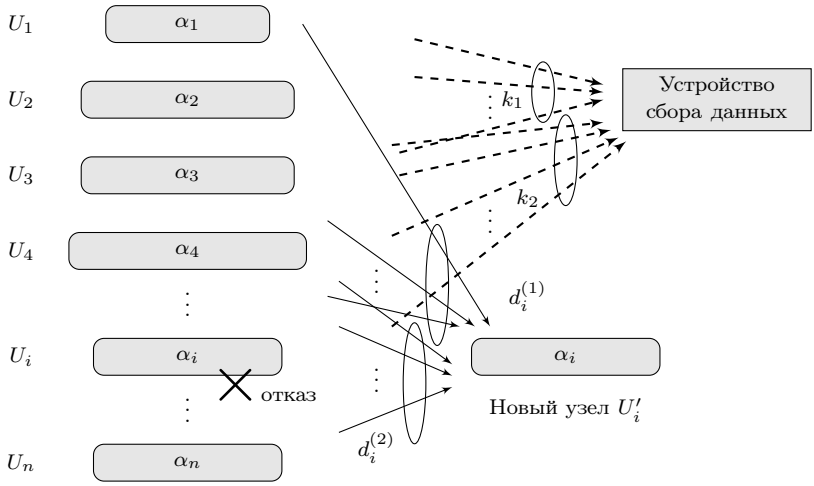

Рис. 1. Модель неоднородной РСХД. Здесь каждый узел имеет свои собственные объем памяти α_i, $i = 1, 2, \ldots, n$, и ширину восстановления. В этой системе переменная степень реконструкции для устройства сбора данных равна k_t, $t \in \{1, 2\}$. Степень восстановления при отказе произвольного узла U_i также неодинакова. Отказавший узел U_i восстанавливается с помощью некоторых $d_i^{(t)}$ узлов

кодированием пакетов сообщений. В случае простого дублирования неэффективно используется объем памяти. С другой стороны, кодирование пакетов данных с помощью МДР-кодов (кодов с максимальным достижимым расстоянием) со стиранием приводит к неэффективности минимизации ширины восстановления в процессе восстановления узлов. Для оптимизации этих конфликтующих параметров в основополагающей работе [5] были введены регенерирующие коды (regenerating codes). В [6,7] зависимость между объемом памяти узла α и шириной восстановления $d\beta$ изучалась с помощью построения кривых компромисса для регенерирующих кодов. Все точки на кривой компромисса можно получить с помощью линейных сетевых кодов над конечными полями [8, 9]. По кривым компромисса минимизацией обоих параметров в разном порядке получаются регенерирующие коды с минимальной шириной восстановления (minimum bandwidth regenerating codes) и регенерирующие коды с минимальным объемом памяти (minimum storage regenerating codes) [6]. Компромиссное соотношение между объемом памяти и шириной восстановления в задаче точного восстановления узлов изучалось в [10]. В [11] была вычислена нижняя граница пропускной способности разреза на ширину восстановления для конкретной постановки задачи с переменными параметрами в однородных РСХД. В [12] дан прекрасный обзор некоторых существующих результатов и моделей восстановления для РСХД. В недавней работе [13] изучено компромиссное соотношение между объемом памяти и шириной восстановления для линейных регенерирующих кодов с точным восстановлением узлов при $k = d = n - 1$.

Неоднородные РСХД более близки к реальным сценариям, где свойства узлов хранения данных не обязательно одинаковы в различных аспектах из-за различий в географической среде, стоимости запоминающих устройств и т.д. Многие такие неоднородные РСХД рассматривались в недавних работах [14–16]. В [17–19] изучалась задача распределения памяти с точки зрения максимизации вероятности успешного восстановления. Для неоднородных РСХД стоимость восстановления можно снижать, позволяя вспомогательным узлам кодировать слова, получаемые из других узлов [20]. В [21–25] исследовалось компромиссное соотношение между объемом памяти и шириной восстановления для обобщенных регенерирующих кодов

и было показано, что каждая точка на кривой компромисса достижима. В обобщенном регенерирующем коде множество узлов разбито на две части так, что все узлы в одной части имеют одинаковые параметры (α_i, d_i, β_i), $i = 1, 2$. В [26] была вычислена граница пропускной способности для неоднородных РСХД с переменной шириной восстановления и постоянной степенью восстановления. В [27] эта граница была вычислена для неоднородных РСХД с переменной шириной восстановления, где восстановление узлов производится с помощью некоторых конкретных вспомогательных узлов. В [28] исследовалось компромиссное соотношение между стоимостью хранения в системе и стоимостью восстановления системы для неоднородных РСХД с переменной стоимостью хранения и восстановления. В [29] были предложены селективные регенерирующие коды, и для них получено компромиссное соотношение между объемом памяти на узел и шириной восстановления, где селективные регенерирующие коды – это регенерирующие коды, в которых вспомогательные узлы для отказавшего узла выбираются разумным способом, уменьшающим ширину восстановления. В [30,31] анализировалось компромиссное соотношение между объемом памяти и шириной восстановления узла для задачи точного восстановления узлов. В [32] дана конструкция для внутренних точек нормированного компромиссного соотношения. В [33] улучшаются границы для регенерирующих кодов с точным восстановлением узлов. В [34] обсуждались улучшения для регенерирующих кодов с помощью разумного выбора вспомогательных узлов при отказе произвольного узла.

В настоящей статье рассматривается неоднородная РСХД, в которой файл размера B распределяется по n узлам, каждый из которых имеет различный объем памяти. Реконструкция файла ведется гибким образом, когда в любой момент времени устройство сбора данных может для реконструкции файла устанавливать соединение с k_t узлами для некоторого t. Следовательно, для заданного файла *степень реконструкции* k_t является переменной. С другой стороны, в случае отказа любого узла U_i, $i \in \{1, 2, \ldots, n\}$, его можно восстановить, загружая пакеты из некоторых $d_i^{(t)}$ узлов. Следовательно, *степень восстановления* $d_i^{(t)}$ также переменна относительно числа узлов. Восстановление отказавшего узла может выполняться двумя способами – точное восстановление и функциональное. Если пакеты, создаваемые в процессе восстановления являются точными копиями утерянных, это называется *точным восстановлением*. С другой стороны, если восстанавливаемые пакеты являются некоторыми функциями от утерянных, то восстановление называется *функциональным*. Модель такой неоднородной РСХД показана на рис. 1. Устройство сбора данных реконструирует распространяемый файл, устанавливая соединение с k_t узлами, $t \in \{1, 2\}$. При этом отказавший узел U_i восстанавливается с помощью некоторых $d_i^{(t)}$ узлов.

Пример такой неоднородной РСХД показан на рис. 2. В этой системе файл B разделен на четыре информационных пакета x_1, x_2, x_3 и x_4. Эти информационные пакеты закодированы одиннадцатью пакетами, являющимися их линейными комбинациями: $y_1 = x_1$, $y_2 = x_2$, $y_3 = x_3$, $y_4 = x_1 + x_2$, $y_5 = x_4$, $y_6 = x_1 + x_2$, $y_7 = x_1$, $y_8 = x_3$, $y_9 = x_2 + x_4$, $y_{10} = x_2$ и $y_{11} = x_1 + x_4$. Закодированные пакеты y_m, $m = 1, 2, \ldots, 11$, распределены по пяти узлам, так что пакеты y_1 и y_2 хранятся в узле U_1, пакеты y_3 и y_4 – в узле U_2, пакеты y_5 и y_6 – в узле U_3, пакеты y_7, y_8 и y_9 – в узле U_4 и оставшиеся два пакета – в узле U_5. Очевидно, узлы имеют объем памяти $\alpha_i = 2$ для $i = 1, 2, 3, 5$ и $\alpha_4 = 3$. В этом примере, если отказывает узел U_5, то его можно восстановить путем загрузки пакетов y_7 и y_9 из узла U_4. Поскольку восстановленные пакеты являются функциями от утерянных, то это – функциональное восстановление. С другой стороны, узел U_5 может быть восстановлен точно путем загрузки пакетов y_1, y_2 и y_5 из узлов U_1 и U_3 и решения $y_{10} = y_2$ и $y_{11} = y_1 + y_5$.

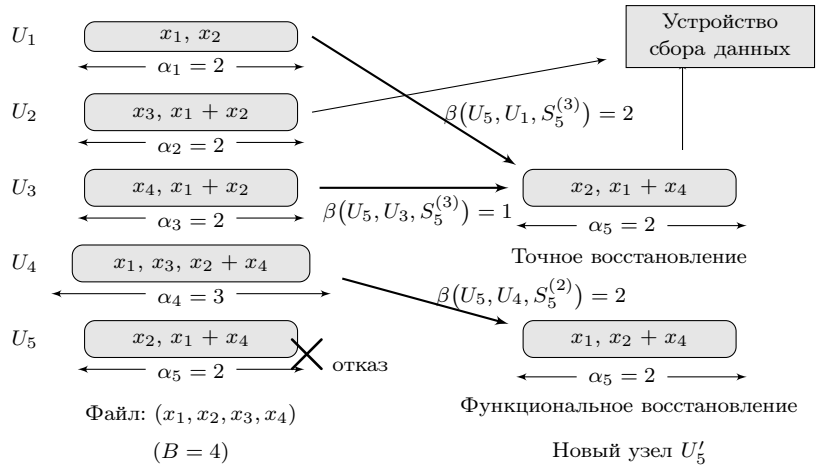

Рис. 2. Файл размером в 4 единицы данных ($= B$) разбит на 11 закодированных пакетов над полем $\mathbb{F}_q$. Эти пакеты разделены между 5 ($= n$) узлами таким образом, что любое устройство сбора данных может загрузить весь файл, установив соединение с не более чем 3 ($= k$) узлами. В этой неоднородной РСХД $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = (2, 2, 2, 3, 2)$. Отказавший узел может быть восстановлен с помощью не более чем 2 ($= d$) узлов. Функциональное и точное восстановление показаны для отказа узла U_5 с помощью множеств выживания $S_5^{(2)} = \{U_4\}$ и $S_5^{(3)} = \{U_1, U_3\}$, где множество выживания – это множество, состоящее из нескольких вспомогательных узлов. Множество выживания $S_5^{(3)}$ не представлено в табл. 1, поскольку $S_5^{(1)} \subsetneq S_5^{(3)}$

Под РСХД с параметрами (n, k, d) будем подразумевать систему хранения с n узлами, степенью реконструкции k и степенью восстановления d, такую что

– каждый узел содержит часть информации о файле данных,
– любое устройство сбора данных может реконструировать весь файл данных, загружая пакеты из k ($< n$) узлов, и
– отказавший узел восстанавливается с помощью некоторых d вспомогательных узлов.

Сводка результатов. В статье вычислена граница минимального разреза для рассматриваемых неоднородных РСХД. Для таких неоднородных РСХД сформулирована оптимизационная двухкритериальная задача линейного программирования с ограничениями, накладываемыми границей минимального разреза. Решения этой задачи представлены в виде кривой компромисса между стоимостью хранения в системе и стоимостью восстановления системы. В неоднородной РСХД стоимостью хранения в системе и стоимостью восстановления системы называются, соответственно, средняя стоимость хранения и средняя стоимость восстановления одной единицы данных в узле. Построены некоторые кривые компромисса и проведено их сравнение с компромиссным соотношением для неоднородных РСХД, рассмотренных в [28], и однородных РСХД, изучавшихся в [7]. Для поставленной задачи двухкритериальной оптимизации изучены некоторые специальные случаи. Вычислительная сложность нахождения параметров для кодов, достигающих фундаментальной границы, очень велика. Поэтому рассмотрен специальный случай с постоянными трафиком восстановления и степенью реконструкции. Кроме того, получено соотношение на параметры кодов, достигающих границы. Для некоторых конкретных значений параметров с помощью графов построены оптимальные коды (достигающие фундаментальной границы).

Структура статьи. Статья организована следующим образом. В § 2 приводятся необходимые предварительные сведения и описывается рассматриваемая модель. В § 3 изучается граница минимального разреза для этой модели. При ограничениях, накладываемых границей минимального разреза, формулируется задача двухкритериальной линейной оптимизации, с помощью которой строится кривая компромисса между стоимостью хранения и восстановления на узел. В § 4 исследуется фундаментальная граница для конкретной неоднородной РСХД. В заключительном § 5 даются общие замечания.

§ 2. Предварительные сведения

Основное внимание уделяется рассмотрению неоднородных РСХД с неодинаковыми параметрами узлов. Для произвольной неоднородной РСХД определим множество $\mathcal{A}_t = \{U_i : i \in I \subset \{1, 2, \ldots, n\}\}$, состоящее из узлов, в которых содержится достаточно пакетов для получения всего файла. Множество $\mathcal{A}_t$ назовем *реконструирующим множеством* и будем использовать обозначение $|I| = |\mathcal{A}_t| = k_t$. Для множества $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_t, \ldots\}$, состоящего из всех различных реконструирующих множеств для произвольной неоднородной РСХД, будем всегда предполагать, что это множество $\mathcal{A}$ конечно. Следовательно, $\exists\, \omega \in \mathbb{N}$, такое что $|\mathcal{A}| = \omega$. Далее, для неоднородной РСХД *степенью реконструкции* k_t называется мощность реконструирующего множества $\mathcal{A}_t$, т.е. $k_t = |\mathcal{A}_t|$ и $k = \max\{k_t : t \in \{1, 2, \ldots, \omega\}\}$. В примере, показанном на рис. 2, $\mathcal{A} = \{\mathcal{A}_i : i = 1, 2, \ldots, 7\}$, где $\mathcal{A}_1 = \{U_1, U_2, U_3\}$, $\mathcal{A}_2 = \{U_1, U_2, U_5\}$, $\mathcal{A}_3 = \{U_1, U_4\}$, $\mathcal{A}_4 = \{U_2, U_4\}$, $\mathcal{A}_5 = \{U_2, U_5\}$, $\mathcal{A}_6 = \{U_3, U_4\}$ и $\mathcal{A}_7 = \{U_4, U_5\}$. Таким образом, $(k_1, k_2, k_3, k_4, k_5, k_6, k_7) = (3, 3, 2, 2, 2, 2, 2)$, и поэтому $k = 3$.

Если в неоднородной РСХД отказывает узел U_i, $i \in \{1, 2, \ldots, n\}$, то из некоторых активных узлов, называемых вспомогательными, загружаются необходимые пакеты и образуется новый узел, скажем, U_i'. Этот новый узел U_i' занимает место отказавшего узла U_i, и таким образом система восстанавливается. В частности, множество таких вспомогательных узлов называется *множеством выживания* для отказавшего узла U_i. Заметим, что для всякого отказавшего узла может существовать более одного множества выживания. Для узла U_i обозначим число его различных множеств выживания через τ_i. Будем обозначать множество выживания с номером ℓ через $S_i^{(\ell)} = \{U_j : j \in J \subset \{1, 2, \ldots, n\} \setminus \{i\}\}$, где $\ell \in \{1, 2, \ldots, \tau_i\}$ [27]. Если отказавший узел U_i восстанавливается с помощью узлов из множества выживания $S_i^{(\ell)}$, то *степень восстановления* узла U_i равна $d_i^{(\ell)} = |J| = |S_i^{(\ell)}|$. Для неоднородной РСХД, представленной на рис. 2, множества выживания перечислены в табл. 1. В этом примере видно, что если отказывает узел U_5, то его можно восстановить, установив соединение либо с узлами U_1 и U_3, либо с U_1 и U_4. Следовательно, множества выживания для узла U_5 – это $S_5^{(1)} = \{U_1, U_3\}$ и $S_4^{(2)} = \{U_1, U_4\}$, как и указано в табл. 1. Заметим также, что в этой таблице перечислены только те множества выживания, которые не покрывают никакое другое множество выживания для того же самого отказавшего узла. Это условие, в частности, гарантирует активное участие каждого узла из любого множества выживания в процессе восстановления.

Для всякого отказавшего узла U_i, если система восстанавливается с помощью узлов из какого-либо конкретного множества выживания $S_i^{(\ell)}$, то число информационных пакетов, загружаемых из узла $U_j \in S_i^{(\ell)}$, обозначается через $\beta(U_i, U_j, S_i^{(\ell)}) > 0$. Отметим, что положительность значения $\beta(U_i, U_j, S_i^{(\ell)})$ соответствует активному участию каждого вспомогательного узла из множества выживания $S_i^{(\ell)}$. Например, на рис. 2 для восстановления отказавшего узла U_4 загружаются все пакеты из узлов $U_2 \in S_4^{(2)}$ и $U_5 \in S_4^{(2)}$, и недостающие пакеты y_7, y_8 и y_9 получаются из них как

Таблица 1

Множества выживания и ширина восстановления для неоднородной РСХД, представленной на рис. 2

Узлы U_i	Множества выживания $S_i^{(\ell)}$	Ширина восстановления $\gamma(U_i, S_i^{(\ell)})$	Число множеств выживания τ_i
U_1	$S_1^{(1)} = \{U_2, U_4\}$ $S_1^{(2)} = \{U_2, U_5\}$ $S_1^{(3)} = \{U_3, U_4\}$ $S_1^{(4)} = \{U_3, U_5\}$ $S_1^{(5)} = \{U_4, U_5\}$	$\gamma(U_1, S_1^{(1)}) = 2$ $\gamma(U_1, S_1^{(2)}) = 2$ $\gamma(U_1, S_1^{(3)}) = 2$ $\gamma(U_1, S_1^{(4)}) = 2$ $\gamma(U_1, S_1^{(5)}) = 2$	5
U_2	$S_2^{(1)} = \{U_1, U_4\}$ $S_2^{(2)} = \{U_3, U_4\}$ $S_2^{(3)} = \{U_4, U_5\}$	$\gamma(U_2, S_2^{(1)}) = 3$ $\gamma(U_2, S_2^{(2)}) = 2$ $\gamma(U_2, S_2^{(3)}) = 3$	3
U_3	$S_3^{(1)} = \{U_1, U_4\}$ $S_3^{(2)} = \{U_1, U_5\}$ $S_3^{(3)} = \{U_4, U_5\}$	$\gamma(U_3, S_3^{(1)}) = 3$ $\gamma(U_3, S_3^{(2)}) = 3$ $\gamma(U_3, S_3^{(3)}) = 3$	3
U_4	$S_4^{(1)} = \{U_1, U_2, U_3\}$ $S_4^{(2)} = \{U_2, U_5\}$	$\gamma(U_4, S_4^{(1)}) = 4$ $\gamma(U_4, S_4^{(2)}) = 4$	2
U_5	$S_5^{(1)} = \{U_1, U_3\}$ $S_5^{(2)} = \{U_1, U_4\}$	$\gamma(U_5, S_5^{(1)}) = 3$ $\gamma(U_5, S_5^{(2)}) = 3$	2

$y_7 = y_4 - y_{10}$, $y_8 = y_3$ и $y_9 = y_{11} + 2y_{10} - y_4$. Следовательно, $\beta(U_4, U_5, S_4^{(2)}) = 2$ и $\beta(U_4, U_2, S_4^{(2)}) = 2$.

Далее, дадим следующие формальные определения. Для отказавшего узла U_i и множества выживания $S_i^{(\ell)}$ введем вектор

$$\boldsymbol{\beta}_i^{(\ell)} = \big(\beta(U_i, U_{j_1}, S_i^{(\ell)}), \beta(U_i, U_{j_2}, S_i^{(\ell)}), \ldots, \beta(U_i, U_{j_m}, S_i^{(\ell)})\big)$$

числа пакетов, которые загружаются из вспомогательных узлов множества выживания $S_i^{(\ell)} = \{U_{j_1}, U_{j_2}, \ldots, U_{j_m}\}$ мощности m, т.е. $m = d_i^{(\ell)} = |S_i^{(\ell)}|$. Для отказавшего узла U_i введем вектор $\boldsymbol{\beta}_i = \big(\boldsymbol{\beta}_i^{(1)}, \boldsymbol{\beta}_i^{(2)}, \ldots, \boldsymbol{\beta}_i^{(\tau_i)}\big)$ из всех $\boldsymbol{\beta}_i^{(\ell)}$, т.е. $\boldsymbol{\beta} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_n)$.

Если отказавший узел U_i, $i \in \{1, 2, \ldots, n\}$, восстанавливается с помощью узлов из множества выживания $S_i^{(\ell)}$, то *шириной восстановления* для узла U_i (обозначаемой через $\gamma(U_i, S_i^{(\ell)})$) называется общее число пакетов, загружаемых всеми узлами из множества выживания $S_i^{(\ell)}$, т.е.

$$\gamma(U_i, S_i^{(\ell)}) = \sum_{j:\, U_j \in S_i^{(\ell)}} \beta(U_i, U_j, S_i^{(\ell)}).$$

Для примера из рис. 2, если узел U_4 отказывает и затем восстанавливается с помощью узлов из множества выживания $S_4^{(2)} = \{U_2, U_5\}$, то ширина восстановления для узла U_4 равна $\gamma(U_4, S_4^{(2)}) = \beta(U_4, U_2, S_4^{(2)}) + \beta(U_4, U_5, S_4^{(2)}) = 2 + 2 = 4$ единицы.

Замечание 1. Мы рассматриваем только отказы единичных узлов, поскольку случай одновременного отказа нескольких узлов можно рассматривать как последовательность единичных отказов.

Далее, неоднородную РСХД можно формально определить следующим образом.

Определение 1. Неоднородной РСХД с параметрами $(n, \boldsymbol{k}, \boldsymbol{d}, \boldsymbol{\alpha}, \boldsymbol{\beta}, B)$ называется система хранения с n узлами, такая что

– в каждом узле U_i $(i = 1, 2, \ldots, n)$ содержится часть информации о файле, закодированная в виде данных объема α_i,

– любое устройство сбора данных может полностью реконструировать файл путем загрузки пакетов из некоторых k_t узлов (k_t – мощность реконструирующего множества $\mathcal{A}_t$ с номером $t \in \{1, 2, \ldots, \omega\}$), и

– отказавший узел U_i восстанавливается с помощью загрузки $\sum\limits_{U_j \in S_i^{(\ell)}} \beta(U_i, U_j, S_i^{(\ell)})$ пакетов из вспомогательных узлов множества выживания $S_i^{(\ell)}$, $\ell \in \{1, 2, \ldots, \tau_i\}$,

где

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n),$$
$$\boldsymbol{d} = (\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_n), \quad \boldsymbol{d}_i = \big(|S_i^{(1)}|, |S_i^{(2)}|, \ldots, |S_i^{(\tau_i)}|\big),$$
$$\boldsymbol{\beta}_i^{(\ell)} = \big(\beta(U_i, U_{j_1}, S_i^{(\ell)}), \beta(U_i, U_{j_2}, S_i^{(\ell)}), \ldots, \beta(U_i, U_{j_m}, S_i^{(\ell)})\big), \quad m = |S_i^{(\ell)}|,$$
$$\boldsymbol{\beta}_i = \big(\boldsymbol{\beta}_i^{(1)}, \boldsymbol{\beta}_i^{(2)}, \ldots, \boldsymbol{\beta}_i^{(\tau_i)}\big), \quad \boldsymbol{\beta} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_n).$$

Чтобы построить кривую компромисса между объемом памяти и шириной восстановления для любой однородной РСХД, в [7] решалась задача оптимизации с ограничениями, накладываемыми границей минимального разреза между параметрами. Эта граница была вычислена путем анализа графа информационных потоков в данной однородной РСХД [7]. Аналогичным способом можно вывести границу минимального разреза и построить кривую компромисса для любой неоднородной РСХД. В настоящей статье граница минимального разреза выводится с помощью графа информационных потоков, как описано в [27, 28], где граф информационных потоков – это взвешенный ориентированный ациклический граф $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ с множеством вершин $\mathcal{V}$ и множеством ребер $\mathcal{E}$.

Для произвольной неоднородной РСХД с заданным реконструирующим множеством $\mathcal{A}_t = \{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{k_t}}\}$ ее граф информационных потоков $\mathcal{G}$ показан на рис. 3, где рассматриваются отказы всех узлов $U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{k_t}}$ одного за другим в указанном порядке и их восстановление с помощью множеств выживания $S_{\lambda_1}^{(\ell_{\lambda_1})}, S_{\lambda_2}^{(\ell_{\lambda_2})}, \ldots, S_{\lambda_{k_t}}^{(\ell_{\lambda_{k_t}})}$, где $\ell_{\lambda_i} \in \{1, 2, \ldots, \tau_{\lambda_i}\}$. Для любого реконструирующего множества $\mathcal{A}_t$ граф делится на $k_t + 3$ уровней, начиная с уровня -1 и заканчивая уровнем $k_t + 1$. На уровне -1 в графе содержится узел-источник "s", а на уровне $k_t + 1$ – узел (устройство) сбора данных "D". Типичный узел U_{λ_i} неоднородной РСХД, $i = 1, 2, \ldots, n$, представлен в графе в виде пары вершин "In_{λ_i}" и "Out_{λ_i}" из $\mathcal{V}$, соединенных ребром, т.е. $(\mathrm{In}_{\lambda_i}, \mathrm{Out}_{\lambda_i}) \in \mathcal{E}$, где λ_i – упорядоченные с помощью некоторой перестановки номера узлов. Объем памяти α_{λ_i} узла U_{λ_i} представлен в виде веса $w(\mathrm{In}_{\lambda_i}, \mathrm{Out}_{\lambda_i})$ ребра $(\mathrm{In}_{\lambda_i}, \mathrm{Out}_{\lambda_i}) \in \mathcal{E}$. В графе $\mathcal{G}$, представленном на рис. 3, на уровне 0 содержится $2n$ вершин, обозначенных In_{λ_i} и Out_{λ_i}, ассоциированных с узлами U_{λ_i}, $i \in \{1, 2, \ldots, n\}$.

В такой неоднородной РСХД отказавший узел U_{λ_i}, $i \in \{1, 2, \ldots, n\}$, восстанавливается путем образования нового узла U'_{λ_i}. В графе информационных потоков узел U'_{λ_i} представляется новой парой узлов In'_{λ_i} и $\mathrm{Out}'_{\lambda_i}$, $(\mathrm{In}'_{\lambda_i}, \mathrm{Out}'_{\lambda_i}) \in \mathcal{E}$, такой что $w(\mathrm{In}'_{\lambda_i}, \mathrm{Out}'_{\lambda_i}) = \alpha_{\lambda_i}$. На каждом уровне j, $j = 1, 2, \ldots, k_t$, в графе потоков содержится одна пара узлов In'_{λ_j} и $\mathrm{Out}'_{\lambda_j}$. Как показано на рис. 3, в неоднородной РСХД при отказе узла U_{λ_j} система восстанавливается с помощью загрузки данных объема $\beta\big(U_{\lambda_1}, U_{\mu_j}, S_{\lambda_1}^{(\ell_{\lambda_1})}\big)$ из узла $U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} = \big\{U_{\mu_j} : j = 1, 2, \ldots, d_{\lambda_i}^{(\ell_{\lambda_i})}\big\}$, где μ_j – некоторая перестановка номеров узлов. Для каждого отдельного восста-

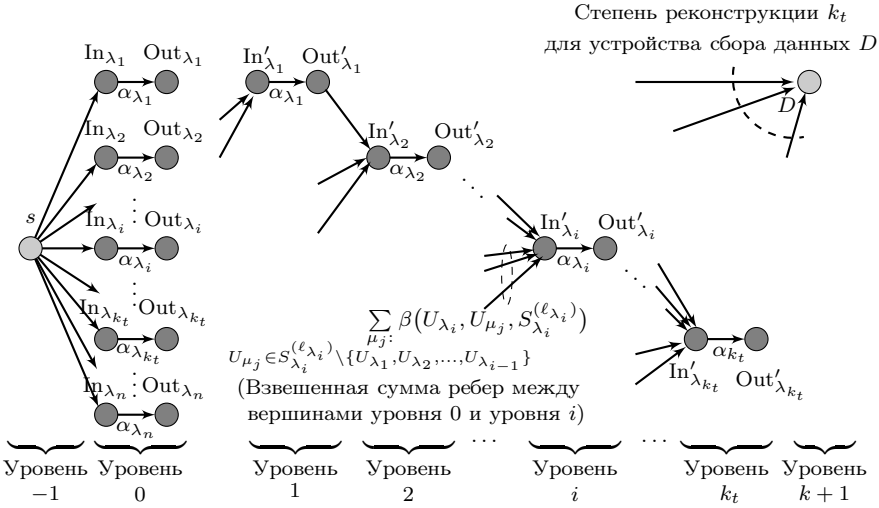

Рис. 3. Граф информационных потоков $\mathcal{G}=(\mathcal{V},\mathcal{E})$ для неоднородной РСХД с реконструирующим множеством $\mathcal{A}_t=\{U_{\lambda_1},U_{\lambda_2},\ldots,U_{\lambda_{k_t}}\}$. Граф разбит на k_t+3 уровней (k_t – переменная степень реконструкции, связанная с узлом сбора данных D). Каждый узел U_{λ_i}, $i=1,2,\ldots,n$, этой неоднородной РСХД представлен в виде пары узлов In_{λ_i} и Out_{λ_i}. Узел-источник s и узел (устройство) сбора данных D попадают на уровни -1 и k_t+1 соответственно. На уровне 0 в графе содержатся n пар узлов In_{λ_i} и Out_{λ_i}. На каждом уровне от 1 до k_t в графе содержится одна пара узлов In'_{λ_j} и $\mathrm{Out}'_{\lambda_j}$, $j=1,2,\ldots,k_t$, где каждая такая пара представляет узел из реконструирующего множества $\mathcal{A}_t$ этой неоднородной РСХД. Отметим, что вес каждого ребра, исходящего из s или входящего в D, равен ∞

новления системы процесс загрузки представляется отдельным ребром, соединяющим узел типа Out одного из предыдущих уровней с узлом In'_{λ_i}. Таким образом, если $\mu_j\in\{1,2,\ldots,\lambda_{i-1}\}$, то соответствующий вспомогательный узел уже был восстановлен ранее после отказа. Эти процессы загрузки представлены ребрами $(\mathrm{Out}'_{\mu_j},\mathrm{In}'_{\lambda_i})\in\mathcal{E}$, показанными в виде нисходящих стрелок в центральной части графа информационных потоков на рис. 3. Если же узел Out'_{μ_j} не встретился среди узлов $\mathrm{Out}'_{\lambda_1},\ldots,\mathrm{Out}'_{\lambda_{i-1}}$, то тогда узел Out_{μ_j} уровня 0 соединяется с узлом In'_{λ_j} (т.е. $(\mathrm{Out}_{\mu_j},\mathrm{In}'_{\lambda_j})\in\mathcal{E}$) ребром с весом $w(\mathrm{Out}_{\mu_j},\mathrm{In}'_{\lambda_i})=\beta\big(U_{\lambda_1},U_{\mu_j},S_{\lambda_1}^{(\ell_{\lambda_1})}\big)$. Эти случаи представлены восходящими стрелками в центральной части графа информационных потоков на рис. 3. В графе $\mathcal{G}$ на каждом уровне рассматривается отказ ровно одного узла.

Устройство сбора данных D устанавливает соединение со всеми k_t узлами множества $\mathcal{A}_t=\{U'_{\lambda_1},U'_{\lambda_2},\ldots,U'_{\lambda_{k_t}}\}=\{U_{\lambda_1},U_{\lambda_2},\ldots,U_{\lambda_{k_t}}\}$. В графе информационных потоков на рис. 3 устройство сбора данных D соединяется с узлами $\mathrm{Out}'_{\lambda_j}$ из уровней от 1 до k_t, $j=1,2,\ldots,k_t$, для загрузки определенных данных, поэтому $(\mathrm{Out}'_{\lambda_j},D)\in\mathcal{E}$, причем $w(\mathrm{Out}'_{\lambda_j},D)\to\infty$. Для неоднородной РСХД, представленной на рис. 2, пример графа информационных потоков показан на рис. 4. В частности, устройство сбора данных соединяется с узлами из множества $\mathcal{A}_1=\{U_1,U_2,U_3\}$. Если в графе информационных потоков отказы узлов происходят в порядке U_1, U_2 и U_3, то их можно восстанавливать с помощью узлов из множеств $S_1^{(1)}$, $S_2^{(1)}$ и $S_3^{(1)}$ соответственно. Заметим, что для восстановления отказавшего узла U_2 из узла U_1 загружается только один пакет y_1+y_2 (сумма пакетов, сохраненных в U_1), так что $\beta(U_2,U_1,S_2^{(1)})=1$.

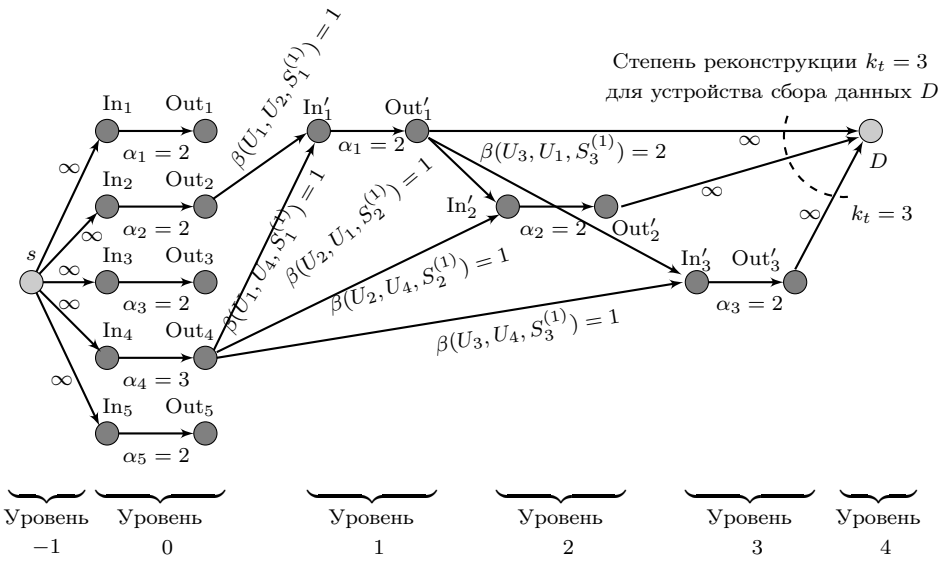

Рис. 4. Граф информационных потоков для неоднородной РСХД, представленной на рис. 2, для конкретного устройства сбора данных, устанавливающего соединение с узлами из реконструирующего множества $\mathcal{A}_1{=}\{U_1, U_2, U_3\}$. Этот конкретный граф информационных потоков построен для последовательности множеств выживания $\langle S_1^{(1)}, S_2^{(1)}, S_3^{(1)}\rangle$ (см. определение 4 для произвольной неоднородной РСХД)

В работах [7, 26–28] граница минимального разреза вычисляется с помощью анализа потоков, идущих по графу информационных потоков от узла-источника s до устройства сбора данных D, для любой РСХД. В настоящей статье выполняется аналогичный анализ информационных потоков для неоднородной РСХД. Поэтому определим поток на графе информационных потоков следующим образом.

О п р е д е л е н и е 2 (информационный поток). Функция $f\colon \mathcal{E} \to [0, \infty) \subset \mathbb{R}$ называется информационным потоком, или просто потоком, на графе информационных потоков $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, если выполнены следующие условия:

1. (ограничение по пропускной способности): для каждого ребра $(x, y) \in \mathcal{E}$ имеет место неравенство $f((x, y)) \leqslant c((x, y))$, где $c((x, y)) = w(x, y)$ и $c((x, y))$ – пропускная способность ребра (x, y), и
2. (ограничение по сохранению потока): для каждой вершины $y \in \mathcal{V} \setminus \{s, t\}$ справедливо равенство

$$\sum_{x\colon (x,y)\in\mathcal{E}} f((x, y)) = \sum_{z\colon (y,z)\in\mathcal{E}} f((y, z)).$$

Дальнейшие подробности и примеры таких функций можно найти в [35, 36].

Для заданного графа информационных потоков $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ значение потока, поступающего на устройство сбора данных D, определяется как общая сумма потоков, идущих по ребрам $(x, D) \in \mathcal{E}$ для всех возможных $x \in \mathcal{V}$. Для сетей максимальное возможное значение потока, приходящего в D, описывается теоремой о минимальном разрезе и максимальном потоке [35–37]. Согласно этой теореме максимальное возможное значение $\text{max-flow}(s, D)$ потока, идущего по сети от источника s до конкретного устройства сбора данных D, равно минимуму величины $\text{cut-capacity}(s, D)$,

где

$$\min \text{cut-capacity}(s, D) = \min_{\substack{\text{cut}(\mathcal{X},\overline{\mathcal{X}}) \\ s\in\mathcal{X},\, D\in\overline{\mathcal{X}} \\ \overline{\mathcal{X}}=\mathcal{V}\setminus\mathcal{X}}} \text{cut-capacity}(\mathcal{X}, \overline{\mathcal{X}}).$$

Заметим, что через $\text{cut}(\mathcal{X}, \overline{\mathcal{X}})$ обозначено множество всех ребер, имеющих один конец в множестве $\mathcal{X}$, а другой в множестве $\overline{\mathcal{X}}$, таких что при удалении всех этих ребер число компонент графа $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ увеличится. Здесь $\text{cut-capacity}(\mathcal{X}, \overline{\mathcal{X}})$ – сумма пропускных способностей всех ребер из множества $\text{cut}(\mathcal{X}, \overline{\mathcal{X}})$. Для конкретного устройства сбора данных D, соединяющегося с узлами U_{λ_i} из множества $\mathcal{A}_t \in \mathcal{A}$, имеется $|\mathcal{A}_t|! \prod_{i=1}^{|\mathcal{A}_t|} \tau_{\lambda_i}$ различных графов информационных потоков. Для каждого графа информационных потоков $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ узел D может получить весь файл B, поэтому

$$B \leqslant \min_{\mathcal{G}} \text{max-flow}(s, D).$$

По теореме о минимальном разрезе и максимальном потоке суммарный поток через разрез равен пропускной способности разреза. Таким образом,

$$B \leqslant \min_{\mathcal{G}} \min \text{cut-capacity}(s, D). \tag{1}$$

В [7] анализ потоков для графа информационных потоков был произведен с помощью выбора топологического порядка на отказывающих узлах, с которыми также соединяется устройство сбора данных для получения всего файла. В настоящей статье для анализа потоков мы определяем некоторые последовательности узлов и соответствующие множества выживания для нашей модели. Приведем эти определения.

Определение 3 (множество последовательностей узлов). Множество всевозможных последовательностей узлов из реконструирующего множества $\mathcal{A}_t \in \mathcal{A}$ называется множеством последовательностей узлов и обозначается через $\mathcal{A}(\mathcal{A}_t) = \{\langle U_{\lambda_i}\rangle_{i=1}^{|\mathcal{A}_t|} : U_{\lambda_i} \in \mathcal{A}_t\}$, где $\langle U_{\lambda_i}\rangle_{i=1}^{|\mathcal{A}_t|}$ – последовательность различных узлов множества $\mathcal{A}_t \in \mathcal{A}$. Очевидно, $|\mathcal{A}(\mathcal{A}_t)| = |\mathcal{A}_t|!$.

Например, на рис. 2 имеем $\mathcal{A}(\mathcal{A}_3) = \{\langle U_1, U_4\rangle, \langle U_4, U_1\rangle\}$, где $\mathcal{A}_3 = \{U_1, U_4\}$.

Определение 4 (последовательность выживания). Для любого реконструирующего множества $\mathcal{A}_t \in \mathcal{A}$ можно определить последовательность множеств выживания $S_{\lambda_i}^{(\ell)}$, $i = 1, 2, \ldots, |\mathcal{A}_t|$, $\ell = 1, 2, \ldots, \tau_{\lambda_i}$, такую что $U_{\lambda_i} \in \mathcal{A}_t$. Последовательность выживания, соответствующую последовательности узлов $\langle U_{\lambda_i}\rangle_{i=1}^{|\mathcal{A}_t|} \in \mathcal{A}(\mathcal{A}_t)$, можно обозначать через $\langle S_{\lambda_i}^{(\ell)}\rangle_{i=1}^{|\mathcal{A}_t|}$.

На рис. 2 последовательность $\langle S_1^{(3)}, S_4^{(2)}\rangle$ – одна из возможных последовательностей выживания среди десяти имеющихся для последовательности узлов $\langle U_1, U_4\rangle$.

Определение 5 (множество последовательностей выживания). Множество всех последовательностей выживания, соответствующих последовательности узлов $\langle U_{\lambda_i}\rangle_{i=1}^{|\mathcal{A}_t|}$, определяется следующим образом:

$$\mathcal{S}\big(\langle U_{\lambda_i}\rangle_{i=1}^{|\mathcal{A}_t|}\big) = \Big\{\langle S_{\lambda_i}^{(\ell)}\rangle_{i=1}^{|\mathcal{A}_t|} : \ell \in \{1, 2, \ldots, \tau_{\lambda_i}\}\Big\}.$$

Очевидно, $\big|\mathcal{S}\big(\langle U_{\lambda_i}\rangle_{i=1}^{|\mathcal{A}_t|}\big)\big| = \Big(\prod_{i=1}^{|\mathcal{A}_t|} \tau_{\lambda_i}\Big)!$.

Например, на рис. 2 имеем $\left\{\langle S_1^{(\ell_1)}, S_4^{(\ell_2)}\rangle : \ell_1 = 1,2,3,4,5 \text{ и } \ell_2 = 1,2\right\} = \mathcal{S}(\langle U_1, U_4\rangle)$ и т.д.

В [28] была получена кривая компромисса между стоимостью хранения в системе и стоимостью восстановления системы для произвольной неоднородной РСХД с одинаковыми степенями реконструкции. Аналогично можно получить кривую компромисса между стоимостью хранения в системе и стоимостью восстановления системы для модели неоднородной РСХД, рассматриваемой в настоящей статье. Определим для нашей модели понятия стоимости хранения в системе, стоимости восстановления узла и стоимости восстановления системы следующим образом.

Определение 6 (стоимость хранения в системе). Общая величина стоимости хранения единицы данных в неоднородной РСХД с параметрами $(n, \boldsymbol{k}, \boldsymbol{d}, \boldsymbol{\alpha}, \boldsymbol{\beta}, B)$ называется стоимостью хранения в системе $C_s(\boldsymbol{\alpha})$, где $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ – вектор объема памяти, $\boldsymbol{s} = (s_1, s_2, \ldots, s_n)$ – вектор стоимости хранения, α_i – объем памяти узла U_i, а s_i – стоимость хранения единицы данных в узле U_i, $i = 1, 2, \ldots, n$. Очевидно,

$$C_s(\boldsymbol{\alpha}) = \frac{1}{B}\sum_{j=1}^{n} s_j \alpha_j.$$

Определение 7 (стоимость восстановления узла). Средняя величина стоимости восстановления узла U_i, $i \in \{1, 2, \ldots, n\}$, в неоднородной РСХД с параметрами $(n, \boldsymbol{k}, \boldsymbol{d}, \boldsymbol{\alpha}, \boldsymbol{\beta}, B)$ называется стоимостью восстановления узла $r(\beta_i)$, соответствующей вектору стоимости восстановления $\boldsymbol{r} = (r_1, r_2, \ldots, r_n)$, т.е.

$$r(\beta_i) = \frac{1}{B\tau_i}\sum_{\ell=1}^{\tau_i}\sum_{j:\, U_j \in S_i^{(\ell)}} r_j \beta(U_i, U_j, S_i^{(\ell)}),$$

где r_j – стоимость загрузки единицы данных из узла U_j в процессе восстановления. Вектором восстановления узлов называется $r(\boldsymbol{\beta}) = (r(\beta_1), r(\beta_2), \ldots, r(\beta_n))$.

Определение 8 (стоимость восстановления системы). Стоимость восстановления системы $C_r(\boldsymbol{\beta})$ – это общая величина стоимости восстановления всех узлов в неоднородной РСХД с параметрами $(n, \boldsymbol{k}, \boldsymbol{d}, \boldsymbol{\alpha}, \boldsymbol{\beta}, B)$. На математическом языке

$$C_r(\boldsymbol{\beta}) = \sum_{j=1}^{n} r(\beta_j).$$

В следующем параграфе мы приводим некоторые результаты и анализ для границы минимального разреза для модели неоднородной РСХД, рассматриваемой в настоящей статье.

§ 3. Результаты

Мы показываем, что для нашей модели минимальным возможным значением переменной степени реконструкции является нижняя граница мощности любого множества разреза, разделяющего узел-источник и узел сбора данных. Для неоднородной РСХД граница минимального разреза вычислена в теореме 1. С использованием этой границы минимального разреза мы показываем, что для неоднородной РСХД размер файла должен быть меньше границы минимального разреза. Используя эту конкретную границу в качестве ограничения, мы формулируем оптимизационную задачу двухкритериального линейного программирования для минимизации стоимости хранения в системе и стоимости восстановления системы для рассматриваемой неоднородной модели. Для этой задачи мы вычисляем семейство решений,

подставляя некоторые числовые значения параметров системы. По числовому параметру строится кривая компромисса между стоимостью хранения в системе и стоимостью восстановления системы. Эта кривая сравнивается с кривой компромисса для однородной РСХД [7] и кривой компромисса для неоднородной РСХД из [28].

В неоднородной РСХД информация, доставляемая на устройство сбора данных D, зависит от минимума величины cut-capacity(s, D). В теореме 1 дается нижняя граница на $\min$ cut-capacity(s, D).

Теорема 1 (граница минимального разреза). *Для заданной неоднородной РСХД с устройством сбора данных D и переменной степенью реконструкции k_t справедливо неравенство* $\min$ cut-capacity$(s, D) \geqslant \mathfrak{Q}$, *где*

$$\mathfrak{Q} = \min_{\mathcal{A}_t \in \mathcal{A}} \min_{\langle U_{\lambda_i}\rangle_{i=1}^{k_t}} \sum_{\substack{i=1 \\ U_{\lambda_i} \in \mathcal{A}_t}}^{k_t} \min\left\{ \alpha_{\lambda_i}, \min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{k_t}} \sum_{\mu_j} \beta\Big(U_{\lambda_i}, U_{\mu_j}, S_{\lambda_i}^{(\ell_{\lambda_i})}\Big) \right\}, \tag{2}$$

причем $|\mathcal{A}_t| = k_t$, $\langle U_{\lambda_i}\rangle_{i=1}^{k_t} \in \mathcal{A}(\mathcal{A}_t)$, $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t} \in \mathcal{S}(\langle U_{\lambda_i}\rangle_{i=1}^{k_t})$, $\ell_i \in \{1, 2, \ldots, \tau_i\}$, *а индекс* μ_j *соответствует узлу* $U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \{U_{\lambda_1}, \ldots, U_{\lambda_{i-1}}\}$. *Остальные обозначения в этом выражении имеют обычный смысл, описанный ранее.*

Доказательство. Рассмотрим неоднородную РСХД с параметрами $(n, \boldsymbol{k}, \boldsymbol{d}, \boldsymbol{\alpha}, \boldsymbol{\beta}, B)$ и заданным реконструирующим множеством $\mathcal{A}_t = \{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{k_t}}\}$. Если все узлы $U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{k_t}}$ отказывают один за другим в порядке, заданном фиксированной последовательностью $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$, то для $\ell_i \in \{1, 2, \ldots, \tau_i\}$ эти узлы восстанавливаются с помощью множеств выживания $S_{\lambda_1}^{(\ell_{\lambda_1})}, S_{\lambda_2}^{(\ell_{\lambda_2})}, \ldots, S_{\lambda_{k_t}}^{(\lambda_{k_t})}$. Таким образом, процесс восстановления идет в том же порядке, т.е. в порядке множеств выживания, заданном последовательностью выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$. Для неоднородной РСХД рассмотрим граф информационных потоков $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. В любом графе информационных потоков $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ имеется узел-источник s, узел сбора данных D, причем устройство сбора данных D устанавливает соединение со всеми узлами из реконструирующего множества $\mathcal{A}_t$, и поэтому степень реконструкции равна k_t. В этой неоднородной РСХД отказавший узел U_i может быть восстановлен с узлов из некоторого множества выживания $S_i^{(\ell_i)}$, где $\ell_i \in \{1, 2, \ldots, \tau_i\}$.

Пусть $\mathcal{X} \subset \mathcal{V}$, $\overline{\mathcal{X}} = \mathcal{V} \setminus \mathcal{X}$, $s \in \mathcal{X}$ и $D \in \overline{\mathcal{X}}$, так что существует некоторое непустое подмножество $\mathrm{cut}(\mathcal{X}, \overline{\mathcal{X}}) \subset \mathcal{E}$. Далее, если $\mathcal{X} = \mathcal{V} \setminus \{D\}$, то cut-capacity$(\mathcal{X}, \overline{\mathcal{X}}) \to \infty$. Аналогично, если $\mathcal{X} = \{s\}$, то опять же cut-capacity$(\mathcal{X}, \overline{\mathcal{X}}) \to \infty$. Следовательно, $\min$ cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ будет получен при всех $\mathrm{Out}_j' \in \overline{\mathcal{X}}$ и $\mathrm{In}_i \in \mathcal{X}$, поскольку это даст конечное значение величины cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$, где $i \in \{1, 2, \ldots, n\}$ и $j \in \{1, 2, \ldots, k_t\}$.

Граф информационных потоков $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ является ориентированным ациклическим графом, поэтому его можно представить в топологическом порядке его вершин. Для этого топологического порядка последовательности отказов узла и соответствующие последовательности множеств выживания должны быть организованы согласно определениям, данным в предыдущих параграфах. С этой целью предположим, что устройство сбора данных D устанавливает соединение со всеми узлами множества $\mathcal{A}_t \in \mathcal{A}$ и реконструирует файл B. Множество $\mathcal{A}(\mathcal{A}_t)$ представляет собой набор всевозможных последовательностей узлов из $\mathcal{A}_t \in \mathcal{A}$. Последовательность $\langle U_{\lambda_i}\rangle_{i=1}^{k_t} \in \mathcal{A}(\mathcal{A}_t)$ описывает порядок отказа узлов конкретного множества $\mathcal{A}_t$. Напомним, что множество всевозможных последовательностей выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$, соответствующих последовательности узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$, обозначается через $\mathcal{S}\big(\langle U_{\lambda_i}\rangle_{i=1}^{k_t}\big)$.

Для заданной последовательности узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$ с заданной последовательностью выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$ проведем следующий анализ.

Для вершины $\mathrm{Out}'_{\lambda_1} \in \overline{\mathcal{X}}$, соответствующей первому узлу в последовательности узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$, возможны следующие два случая.

- Если $\mathrm{In}'_{\lambda_1} \in \mathcal{X}$, то ребро $(\mathrm{In}'_{\lambda_1}, \mathrm{Out}'_{\lambda_1}) \in \mathrm{cut}(\mathcal{X}, \overline{\mathcal{X}})$. Следовательно, вклад в величину cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ равен α_{λ_1}.
- Если $\mathrm{In}'_{\lambda_1} \in \overline{\mathcal{X}}$, то ребра $(\mathrm{Out}_{\mu_j}, \mathrm{In}'_{\lambda_1}) \in \mathrm{cut}(\mathcal{X}, \overline{\mathcal{X}})$, где $U_{\mu_j} \in S_{\lambda_1}^{(\ell_{\lambda_1})}$ и $S_{\lambda_1}^{(\ell_{\lambda_1})} \in \in \big\langle S_{\lambda_i}^{(\ell_{\lambda_1})}\big\rangle_{i=1}^{k_t}$ для любого $\ell_{\lambda_1} \in \{1, 2, \ldots, \tau_{\lambda_1}\}$. Следовательно, в этом случае вклад в величину cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ равен

$$\sum_{\mu_j\colon U_{\mu_j} \in S_{\lambda_1}^{(\ell_{\lambda_1})}} \beta\Big(U_{\lambda_1}, U_{\mu_j}, S_{\lambda_1}^{(\ell_{\lambda_1})}\Big).$$

Итак, вклад узла U_{λ_1} в $\min$ cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ равен

$$\min\left\{\alpha_{\lambda_1}, \sum_{\mu_j\colon U_{\mu_j} \in S_{\lambda_1}^{(\ell_{\lambda_1})}} \beta\Big(U_{\lambda_1}, U_{\mu_j}, S_{\lambda_1}^{(\ell_{\lambda_1})}\Big)\right\}.$$

Если узел U_p $(p = 1, 2, \ldots, n)$ отказывает в системе, то все узлы некоторого множества выживания $S_p^{(\ell_p)}$ породят новый узел U'_p с теми же характеристиками.

Далее в доказательстве будем использовать обозначение U_p, $p \in \{1, 2, \ldots, n\}$, вместо U'_p, поскольку характеристики обоих узлов U_p и U'_p одинаковы, и в каждый момент времени существует один из них.

Вычислим вклад узла $U_{\lambda_i} \in \langle U_{\lambda_i}\rangle_{i=1}^{k_t}$ в величину $\min$ cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ в общем случае. Предположим, что $\mathrm{Out}'_{\lambda_i} \in \overline{\mathcal{X}}$. Далее возможны следующие два случая.

- Если $\mathrm{In}'_{\lambda_i} \in \mathcal{X}$, то ребро $(\mathrm{In}'_{\lambda_i}, \mathrm{Out}'_{\lambda_i}) \in \mathrm{cut}(\mathcal{X}, \overline{\mathcal{X}})$. Следовательно, вклад в величину cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ равен α_{λ_i}.
- Если $\mathrm{In}'_{\lambda_i} \in \overline{\mathcal{X}}$, то все возможные ребра $(\mathrm{Out}_{\mu_j}, \mathrm{In}'_{\lambda_i})$, такие что $U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \setminus \{U_{\lambda_1}, U_{\lambda_2}, \ldots U_{\lambda_{i-1}}\}$ и $S_{\lambda_i}^{(\ell_{\lambda_i})} \in \big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$ для любого $\ell_{\lambda_i} \in \{1, 2, \ldots, \tau_{\lambda_i}\}$, входят в множество $\mathrm{cut}(\mathcal{X}, \overline{\mathcal{X}})$. Ребра $(\mathrm{Out}_{\lambda_j}, \mathrm{In}'_{\lambda_i})$, соответствующие узлам $U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \setminus \{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{i-1}}\}$, впервые входят с уровня 0 в $\mathrm{cut}(\mathcal{X}, \overline{\mathcal{X}})$. Ребра $(\mathrm{Out}'_{\lambda_m}, \mathrm{In}'_{\lambda_i})$ следует исключить, так как они рассматривались ранее на уровне m, где $m \in \in \{1, 2, \ldots, i-1\}$, таком что $U_{\lambda_m} \in S_{\lambda_i}^{(\ell_{\lambda_i})}$. Следовательно, в этом случае вклад в величину cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ равен

$$\sum_{\mu_j\colon U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{i-1}}\}} \beta\Big(U_{\lambda_i}, U_{\mu_j}, S_{\lambda_i}^{(\ell_{\lambda_i})}\Big).$$

Итак, вклад узла U_{λ_i} в величину $\min$ cut-capacity$(\mathcal{X}, \overline{\mathcal{X}})$ равен

$$\min\left\{\alpha_{\lambda_i}, \sum_{\mu_j\colon U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{i-1}}\}} \beta\Big(U_{\lambda_i}, U_{\mu_j}, S_{\lambda_i}^{(\ell_{\lambda_i})}\Big)\right\}.$$

Если устройство сбора данных D устанавливает соединение с каждым из узлов $U_{\lambda_i} \in \mathcal{A}_t$, $i \in \{1, 2, \ldots, k_t\}$, то для заданной последовательности узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$,

соответствующей заданной последовательности выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$, вклад в величину $\min\text{cut-capacity}(\mathcal{X},\overline{\mathcal{X}})$ равен

$$\sum_{i=1}^{k_t}\min\left\{\alpha_{\lambda_i},\sum_{\mu_j\colon U_{\mu_j}\in S_{\lambda_i}^{(\ell_{\lambda_i})}\setminus\{U_{\lambda_1},U_{\lambda_2},\ldots,U_{\lambda_{i-1}}\}}\beta\Big(U_{\lambda_i},U_{\mu_j},S_{\lambda_i}^{(\ell_{\lambda_i})}\Big)\right\}.$$

Далее, для заданного реконструирующего множества $\mathcal{A}_t$ можно найти значение $\min\text{cut-capacity}(s,D)$ для фиксированного D, вычисляя минимум по всевозможным значениям величины $\text{cut-capacity}(\mathcal{X},\overline{\mathcal{X}})$, вычисленным для всех возможных последовательностей узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$ во всех возможных соответствующих последовательностях выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$, т.е.

$$\min_{\langle U_{\lambda_i}\rangle_{i=1}^{k_t}}\min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{k_t}}\sum_{\substack{i=1\\U_{\lambda_i}\in\mathcal{A}_t}}^{k_t}\min\left\{\alpha_{\lambda_i},\sum_{\mu_j\colon U_{\mu_j}\in S_{\lambda_i}^{(\ell_{\lambda_i})}\setminus\{U_{\lambda_1},\ldots,U_{\lambda_{i-1}}\}}\beta\Big(U_{\lambda_i},U_{\mu_j},S_{\lambda_i}^{(\ell_{\lambda_i})}\Big)\right\}.\quad(3)$$

Однако индекс λ_i объема памяти узла определяется узлами в последовательности узлов. Поэтому величина, указанная в (3), равна

$$\min_{\langle U_{\lambda_i}\rangle_{i=1}^{k_t}}\sum_{\substack{i=1\\U_{\lambda_i}\in\mathcal{A}_t}}^{k_t}\min\left\{\alpha_{\lambda_i},\min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{k_t}}\sum_{\mu_j\colon U_{\mu_j}\in S_{\lambda_i}^{(\ell_{\lambda_i})}\setminus\{U_{\lambda_1},\ldots,U_{\lambda_{i-1}}\}}\beta\Big(U_{\lambda_i},U_{\mu_j},S_{\lambda_i}^{(\ell_{\lambda_i})}\Big)\right\}.$$

Следовательно, для данной неоднородной РСХД величина $\text{cut-capacity}(\mathcal{X},\overline{\mathcal{X}})$ равна

$$\min_{\mathcal{A}_t\in\mathcal{A}}\min_{\langle U_{\lambda_i}\rangle_{i=1}^{k_t}}\sum_{\substack{i=1\\U_{\lambda_i}\in\mathcal{A}_t}}^{k_t}\min\left\{\alpha_{\lambda_i},\min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{k_t}}\sum_{\mu_j\colon U_{\mu_j}\in S_{\lambda_i}^{(\ell_{\lambda_i})}\setminus\{U_{\lambda_1},\ldots,U_{\lambda_{i-1}}\}}\beta\Big(U_{\lambda_i},U_{\mu_j},S_{\lambda_i}^{(\ell_{\lambda_i})}\Big)\right\},$$

где $|\mathcal{A}_t|=k_t$, $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}\in\mathcal{A}(\mathcal{A}_t)$ и $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}\in\mathcal{S}\big(\langle U_{\lambda_i}\rangle_{i=1}^{k_t}\big)$.

Эта граница точна, поскольку граница минимального разреза вычисляется как минимум по всем возможным границам разреза. Иными словами, граница минимального разреза вычисляется для всех возможных реконструирующих множеств со всеми возможными последовательностями узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t}$, соответствующими всем возможным последовательностям выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$. Следовательно, существует хотя бы одна последовательность выживания, скажем, $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i}^*)}\big\rangle_{i=1}^{k_t}$, соответствующая последовательности узлов, скажем, $\langle U_{\lambda_i}^*\rangle_{i=1}^{k_t}$, для которой неравенство обращается в равенство, т.е. граница минимального разреза в теореме 1 является точной. ▲

Замечание 2. Для заданной неоднородной РСХД, если произвольное устройство сбора данных соединяется с каждым узлом U_{λ_j} из подмножества $\mathcal{A}_t\in\mathcal{A}$, то общее число возможных графов информационных потоков равно

$$\sum_{\mathcal{A}_t\in\mathcal{A}}\left(|\mathcal{A}_t|!\prod_{j=1}^{|\mathcal{A}_t|}\tau_{\lambda_j}\right).$$

В частности, для конкретного графа информационных потоков общее число вычислительных сравнений $|\mathcal{A}_t|$. Поэтому общее число вычислительных сравнений для

неоднородной РСХД равно

$$\sum_{\mathcal{A}_t \in \mathcal{A}} \left(|\mathcal{A}_t|(|\mathcal{A}_t|!) \prod_{j=1}^{|\mathcal{A}_t|} \tau_{\lambda_j} \right).$$

Следовательно, можно сказать, что временна́я сложность вычисления границы минимального разреза для неоднородной РСХД равна

$$O\left(|\mathcal{A}_t|! \prod_{j=1}^{|\mathcal{A}_t|} \tau_{\lambda_j} \right).$$

С помощью теоремы 1 можно вычислить минимальные объем памяти узла и ширину восстановления, необходимые для хранения файла размера B. Другими словами, верхнюю границу для хранения файла размера B дает следующая

Лемма 1. *Если файл размера B хранится в некоторой неоднородной РСХД с параметрами $(n, \boldsymbol{k}, \boldsymbol{d}, \boldsymbol{\alpha}, \boldsymbol{\beta}, B)$, то*

$$B \leqslant \mathcal{Q}, \tag{4}$$

где величина $\mathcal{Q}$ определена в (2)*, а остальные используемые обозначения имеют обычный смысл, описанный ранее.*

Доказательство. Любой узел сбора данных D должен быть способен реконструировать весь файл размера B. Следовательно, максимальное значение информационного потока, приходящего в любой узел сбора данных, должно быть не меньше B. Дальнейшее доказательство вытекает из теоремы о минимальном разрезе и максимальном потоке, теоремы 1 и неравенства (1). ▲

Величина $\min \text{cut-capacity}(s, D)$ для графа информационных потоков, приведенного на рис. 4, равна

$$\min\{\alpha_1, \beta(U_1, U_2, S_1^{(1)}) + \beta(U_1, U_4, S_1^{(1)})\} + \min\{\alpha_2, \beta(U_2, U_4, S_2^{(1)})\} +$$
$$+ \min\{\alpha_3, \beta(U_3, U_4, S_3^{(1)})\} = 2 + 1 + 1 = 4$$

единицы. Теперь можно составить задачу оптимизации для нахождения минимальных стоимости хранения в системе и стоимости восстановления системы при ограничении, что максимальная возможная информация, поступающая в узел сбора данных D, не меньше B.

Задача 1.

Минимизировать: $[C_s(\boldsymbol{\alpha}), C_r(\boldsymbol{\beta})]$

при условиях

Неравенство (4);

$\alpha_i \geqslant 0$;

$\beta\big(U_i, U_j, S_i^{(\ell)}\big) \geqslant 0$;

где $i = 1, 2, \ldots, n$, $\ell = 1, 2, \ldots, \tau_i$ и $U_j \in S_i^{(\ell)}$ для некоторого $j \in \{1, 2, \ldots, n\} \setminus \{i\}$.

Замечание 3. Можно вычислить кривую компромисса между стоимостью восстановления и стоимостью хранения с помощью оптимизационной задачи 1 как для точного, так и для функционального восстановления, используя множества выживания как наборы тех вспомогательных узлов, которые участвуют в точном или функциональном восстановлении отказавших узлов соответственно.

Построение оптимальных значений для обеих целевых функций двухкритериальной оптимизационной задачи 1 дает кривую компромисса между $C_s(\boldsymbol{\alpha})$ и $C_r(\boldsymbol{\beta})$. В настоящей статье оптимизационная задача 1 решается методом взвешенных сумм для некоторых численных примеров. Некоторые частные случаи оптимизационной задачи 1 рассматриваются в нижеследующих пунктах.

3.1. Некоторые частные случаи. Неоднородную РСХД, рассмотренную в этой статье, можно приводить к следующим случаям при некоторых соответствующих ограничениях.

1) (постоянная реконструкция): Если произвольное устройство сбора данных может получить файл, загружая данные из ровно k узлов для любой их комбинации из n узлов, то ограничительное неравенство (4) для оптимизационной задачи 1 имеет дополнительное свойство $k_t = k$ для $t = 1, 2, \ldots, \omega$.

Задача 2.

Минимизировать: $[C_s(\boldsymbol{\alpha}), C_r(\boldsymbol{\beta})]$

при условиях

$$B \leqslant \min_{\langle U_{\lambda_i}\rangle_{i=1}^{k}} \sum_{i=1}^{k} \min\left\{ \alpha_{\lambda_i}, \min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{k}} \sum_{\mu_j:\, U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \{U_{\lambda_1}, \ldots, U_{\lambda_{i-1}}\}} \beta\Big(U_{\lambda_i}, U_{\mu_j}, S_{\lambda_i}^{(\ell_{\lambda_i})}\Big) \right\};$$

$$0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_n;$$

где μ_j – номер узла $U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \{U_{\lambda_1}, \ldots, U_{\lambda_{i-1}}\}$ для $i = 1, 2, \ldots, k$.

2) (постоянная степень восстановления): Пусть для неоднородной РСХД отказавший узел можно восстановить с помощью *любых* d из оставшихся $n-1$ узлов. При таком предположении ограничительное неравенство (4) для оптимизационной задачи 1 сводится к следующему:

Задача 3.

Минимизировать: $[C_s(\boldsymbol{\alpha}), C_r(\boldsymbol{\beta})]$

при условиях

$$B \leqslant \min_{\mathcal{A}_t \in \mathcal{A}} \sum_{\substack{i=1 \\ U_{\lambda_i} \in \mathcal{A}_t}}^{k_t} \min\left\{ \alpha_{\lambda_i}, \sum_{\mu_j} \beta\Big(U_{\lambda_i}, U_{\mu_j}, S_{\lambda_i}^{(\ell_{\lambda_i})}\Big) \right\};$$

$$0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_n;$$
$$1 \leqslant \lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_{k_t} \leqslant n;$$

где μ_j – номер узла $U_{\mu_j} \in S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \{U_{\lambda_1}, \ldots, U_{\lambda_{i-1}}\}$, такого что $\{U_{\lambda_1}, \ldots, U_{\lambda_{i-1}}\} \subset \subset S_{\lambda_i}^{(\ell_{\lambda_i})}$, $i = 1, 2, \ldots, k_t$, и некоторого $j \in \{1, 2, \ldots, d\}$.

В этом случае $\big|S_m^{(\ell_m)}\big| = d$ и $\tau_m = \binom{n-1}{d}$ для $m = 1, 2, \ldots, n$. Здесь значение величины $\min \text{cut-capacity}(s, D)$ задается последовательностью узлов $\langle U_{\lambda_i}\rangle_{i=1}^{k_t} \in \mathcal{A}(\mathcal{A}_t)$, соответствующей последовательности выживания $\big\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\big\rangle_{i=1}^{k_t}$, такой что $\alpha_{\lambda_1} \leqslant \alpha_{\lambda_2} \leqslant \leqslant \ldots \leqslant \alpha_{\lambda_{k_t}}$ и $\{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_{i-1}}\} \subset S_{\lambda_i}^{(\ell_{\lambda_i})}$.

3) (постоянный объем загрузки для восстановления): В этом случае предполагается, что объем загрузки из любого вспомогательного узла для восстановления системы постоянен и равен, скажем, β. Тогда оптимизационная задача 1 при таком ограничении имеет дополнительные свойства $\beta\big(U_i, U_j, S_i^{(\ell_i)}\big) = \beta$, $\beta \geqslant 0$, $i = 1, 2, \ldots, n$, для всевозможных $j \in \{1, 2, \ldots, n\} \setminus \{i\}$ и $\ell_i = 1, 2, \ldots, \tau_i$.

Задача 4.

Минимизировать: $[C_s(\boldsymbol{\alpha}), C_r(\boldsymbol{\beta})]$

при условиях

$$B \leqslant \min_{\mathcal{A}_t \in \mathcal{A}} \min_{\langle U_{\lambda_i} \rangle_{i=1}^{k_t}} \sum_{\substack{i=1 \\ U_{\lambda_i} \in \mathcal{A}_t}}^{k_t} \min\left\{ \alpha_{\lambda_i}, \min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})} \rangle_{i=1}^{k_t}} \left| S_{\lambda_i}^{(\ell)} \setminus \{U_{\lambda_1}, \ldots, U_{\lambda_{i-1}}\} \right| \beta \right\};$$

$$0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_n; \ \beta \geqslant 0.$$

4) (однородная РСХД): Неоднородная РСХД сводится к однородной, если все параметры в ней постоянны. Таким образом, предположим, что эффективная степень реконструкции для любого устройства сбора данных равна k, а объем памяти каждого узла равен α. Кроме того, пусть отказавший узел может быть восстановлен с помощью *любых* d из оставшихся $n-1$ узлов путем загрузки β пакетов из каждого вспомогательного узла. При таких условиях ограничительное неравенство (4) для оптимизационной задачи 1 сводится к следующему:

Задача 5.

Минимизировать: $[C_s(\boldsymbol{\alpha}), C_r(\boldsymbol{\beta})]$

при условиях

$$B \leqslant \sum_{i=1}^{k} \min\{\alpha, (d-i-1)\beta\};$$

$$\alpha \geqslant 0;$$

$$\beta \geqslant 0.$$

5) (прочее): Рассмотренную в статье модель неоднородной РСХД можно сводить к еще более специальным РСХД при некоторых соответствующих условиях на ограничения. Например, неоднородные РСХД с постоянной реконструкцией и с постоянной степенью восстановления (случаи 1) и 2) соответственно) совместно приводят к случаю неоднородной РСХД, рассмотренной в [28].

Можно искать решения двухкритериальной оптимизационной задачи 1 для некоторых численных значений и по этим решениям строить кривую компромисса для нее. Можно сравнить полученную кривую компромисса с кривой компромисса для существующей неоднородной РСХД, исследованной в [28]. Итак, в следующем параграфе мы вычисляем некоторые оптимальные решения для численных значений параметров нашей модели и сравниваем ее с однородной моделью из [7] и неоднородной моделью из [28].

3.2. Численные результаты. Для оптимизационной задачи 1 мы решали задачи линейного программирования с одной целевой функцией. Эта целевая функция выбиралась как линейная комбинация двух целевых функций оптимизационной задачи 1. Затем эти задачи линейного программирования были решены с выбором различных отношений коэффициентов линейной комбинации в пределах от 10^{-3} до 10^3. Построение компромиссных соотношений и решения задач линейного программирования были выполнены с помощью программных средств MATLAB и `lp_solve` [38].

На рис. 5 построены четыре кривые компромисса между стоимостью восстановления системы C_r и стоимостью хранения в системе C_s для соответствующих РСХД. В частности, одна кривая на рис. 5 построена для однородной РСХД из [7], еще одна – для неоднородной РСХД из [28], а остальные две – для неоднородных РСХД, рассмотренных в настоящей статье. А именно, одна из двух последних кривых имеет минимальную эффективную степень реконструкции $k_{\min}$, равную 2,

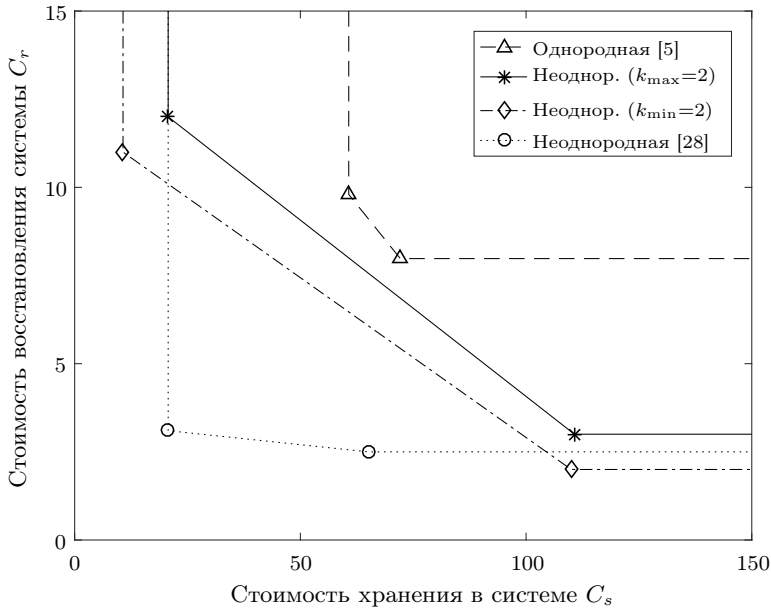

Рис. 5. Кривая оптимального компромисса между стоимостью восстановления системы C_r и стоимостью хранения в системе C_s для различных РСХД

а вторая – максимальную эффективную степень восстановления $k_{\max}$, равную 2. Общие для всех рассматриваемых РСХД параметры следующие: $n = 4$, $B = 1$ единица, $\boldsymbol{s} = (1\ 10\ 10\ 100)$ и $\boldsymbol{r} = (10\ 1\ 1\ 1)$. Однородная РСХД и неоднородная РСХД из [28] имеют степень реконструкции $k = 2$ и степень восстановления $d = 3$. Обе оставшиеся неоднородные РСХД имеют множества выживания $S_1^{(1)} = \{U_2, U_3, U_4\}$, $S_2^{(1)} = \{U_1, U_4\}$, $S_3^{(1)} = \{U_1, U_2\}$ и $S_4^{(1)} = \{U_2, U_3\}$.

Из рис. 5 видно, что наша модель неоднородной РСХД имеет более оптимальные стоимости хранения и восстановления, чем однородная РСХД, рассмотренная в [7]. Несмотря на то, что характеристики нашей неоднородной модели и неоднородной модели, исследованной в [28], различны, мы получили несколько более оптимальных точек для нашей модели, как показано на рис. 5. В п. 3.1 было показано, что неоднородную РСХД из [28] можно получить из нашей модели, накладывая в ней определенные условия.

Замечание 4. Заметим, что уменьшение размера произвольного файла B до 1 приводит к тому, что соответствующие целочисленные решения могут перестать быть целочисленными. Поэтому на конкретных кривых компромисса можно также рассматривать и нецелочисленные решения двухкритериальной оптимизационной задачи 1.

Теперь рассмотрим пример, приведенный на рис. 2. В этом примере средняя степень реконструкции равна 2,286 для данной неоднородной РСХД. Средние степени восстановления для узлов равны $(2, 2, 2, 2{,}5, 2)$, и среднее значение этих средних степеней восстановления равно 2,1. Для отказов узлов в РСХД, рассматриваемой в этом примере, значения ширины восстановления приведены в табл. 1. Таким образом, для вектора стоимости хранения $s = (1, 1, 1, 1, 1)$ и вектора стоимости восстановления $r = (1, 1, 1, 1, 1)$ стоимость хранения в системе и стоимость восстановления системы равны 2,750 и 3,667 единиц соответственно. Поэтому стоимость хранения на узел и стоимость восстановления на узел равны 0,550 и 0,733 единиц соответствен-

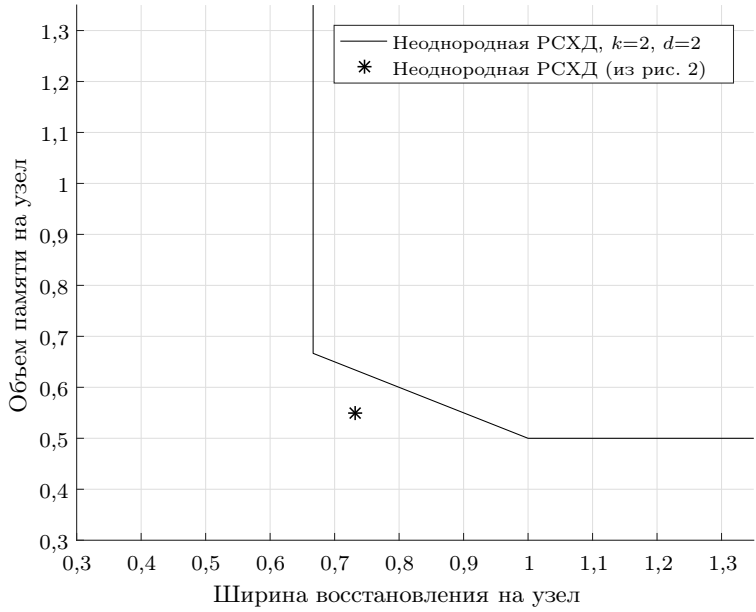

Рис. 6. Кривая компромисса между объемом памяти на узел и шириной восстановления на узел для однородной РСХД в сравнении со значениями этих параметров для примера неоднородной РСХД, приведенной на рис. 2

но. Далее, кривая компромиссного соотношения для однородной РСХД со степенью реконструкции 2 и степенью восстановления 2 построена на рис. 6. Этот рисунок приведен для сравнения примера (рис. 2) неоднородной РСХД с однородной РСХД, имеющей $k = 2$ и $d = 2$.

§ 4. Анализ границы

4.1. Модель. В неоднородной РСХД файл делится на пакеты , и эти закодированные пакеты распределяются по n различным узлам U_i, $i = 1, 2, \ldots, n$, где каждый узел имеет объем памяти α_i и степень восстановления d_i. Пользователь может реконструировать файл, загружая данные из любых k ($< n$) узлов. Если узел U_i откажет, то тогда устройство сбора данных загрузит β пакетов из некоторых d_i узлов, специально выбираемых из оставшихся $n - 1$ узлов. Эти d_i узлов называются вспомогательными узлами для отказавшего узла U_i. В таком случае ширина восстановления для узла U_i равна $\gamma_i = d_i\beta$. Заметим, что леммы 2 и 3 выведены для таких неоднородных РСХД.

Пример такой неоднородной РСХД показан на рис. 7. В этом примере файл размера 3 ($= B$) хранится в неоднородной РСХД с параметрами ($n = 6$, $k = 2$) и трафиком восстановления β, равным 1. В этой РСХД объем памяти узла α_i равен $2, 2, 2, 3, 2, 2$ для $i = 1, 2, 3, 4, 5, 6$ (см. рис. 7). Заметим, что $\alpha_i = \gamma_i = d_i$ для $i = 1, 2, 3, 4, 5, 6$. В [27] рассматривалось представление неоднородной РСХД в виде ациклического ориентированного графа, называемого графом информационных потоков. С помощью анализа минимального разреза в графе информационных потоков вычисляется фундаментальная граница на размер файла B для такой неоднородной РСХД. Эту границу (специальный случай леммы 1) описывает следующая

Лемма 2 (фундаментальная граница). *Для неоднородной РСХД с n узлами и степенью реконструкции k размер файла B должен удовлетворять следующему*

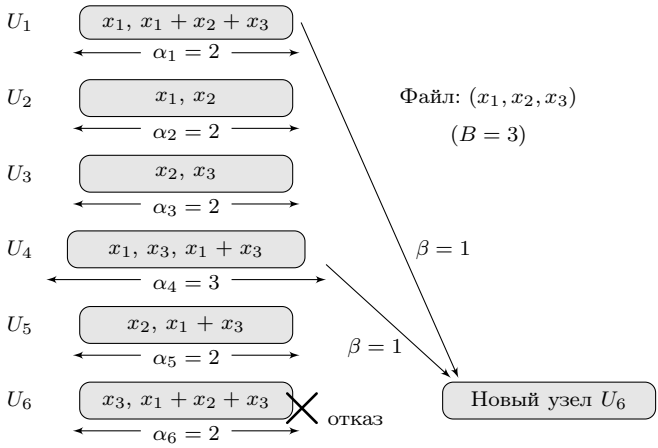

Рис. 7. Файл разделен на 3 $(= B)$ различных пакета x_1, x_2 и x_3 над полем $\mathbb{F}_q$. Эти три пакета закодированы в тринадцать различных пакетов и распределены по неоднородной РСХД с шестью узлами и степенью реконструкции 2

неравенству:

$$B \leqslant \min_{\langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{n}} \left\{ \sum_{i=1}^{k} \min\left\{ \alpha_{\lambda_i}, \left| S_{\lambda_i}^{(\ell_{\lambda_i})} \setminus \left(\bigcup_{j=0}^{i-1} \{U_{\lambda_j}\} \right) \right| \beta \right\} \right\},$$

где $\{U_{\lambda_0}\} = \varnothing$, $0 \leqslant j < i \leqslant k$, $S_{\lambda_i}^{(\ell_{\lambda_i})} \in \langle S_{\lambda_i}^{(\ell_{\lambda_i})}\rangle_{i=1}^{n}$ *и* $\ell_{\lambda_i} \in \{1, 2, \ldots, \tau_{\lambda_i}\}$.

Доказательство. Для рассматриваемой неоднородной РСХД любое множество $\mathcal{A} \subset \{U_1, U_2, \ldots, U_n\}$ мощности k является реконструирующим. Значит, любая последовательность узлов длины k будет последовательностью узлов для этой неоднородной РСХД. Тем самым, любая последовательность длины k, состоящая из множеств выживания, будет также последовательностью выживания для этой неоднородной РСХД. Поэтому доказательство следует из леммы 1. ▲

В [27] было показано существование кода, достигающего фундаментальной границы для таких неоднородных РСХД с параметрами (n, k). Следовательно, можно получать оптимальные коды, уменьшая параметры, лежащие на фундаментальной границе. В следующем пункте вычисляются параметры оптимальных кодов, получаемые минимизацией объема памяти узла и ширины восстановления.

4.2. Условия оптимальности. Рассмотрим неоднородную РСХД с параметрами (n, k) с τ_i множествами выживания $S_i^{(\ell_i)}$ и степенями восстановления $\left|S_i^{(\ell_i)}\right| = d_i$, $\ell_i = 1, 2, \ldots, \tau_i$, $i = 1, 2, \ldots, n$. Если $\alpha_i > \left|S_i^{(\ell_i)}\right|\beta$, то отказавший узел U_i восстановить нельзя, поэтому $\alpha_i \leqslant \left|S_i^{(\ell_i)}\right|\beta$ для всех i и ℓ_i. Для оптимальности должно выполняться равенство $\alpha_i = d_i\beta$. Следовательно, при постоянном трафике восстановления β объем памяти узла α_i и степень восстановления d_i должны быть пропорциональны друг другу. Рассмотрим $c_i \in (0, 1) \subset \mathbb{R}$, такие что $\sum\limits_{i=1}^{n} c_i = 1$ и $\dfrac{c_i}{\alpha_i} = \dfrac{c_j}{\alpha_j}$ при $1 \leqslant i < j \leqslant n$. Тогда $\alpha_i = c_i \sum\limits_{i=1}^{n} \alpha_i = c_i\alpha^*$, $i = 1, 2, \ldots, n$. Таким образом, параметры α_i и c_i пропорциональны друг другу. Снова, поскольку k – степень реконструкции, то $B \leqslant \sum\limits_{i\in\mathcal{K}} \alpha_i = \sum\limits_{i\in\mathcal{K}} c_i\alpha^*$ для произвольного множества $\mathcal{K} \subset \{1, 2, \ldots, n\}$, такого что

$|\mathcal{K}| = k$. Отсюда $B \leqslant \sum\limits_{i=1}^{k} c_i\alpha^*$ для $c_1 \leqslant c_2 \leqslant \ldots \leqslant c_n$. Для получения оптимального случая можно уменьшить α^* до $\alpha^*_{\min}$, такого что

$$B = \sum_{i=1}^{k} c_i\alpha^*_{\min} \implies \alpha^*_{\min} = B\left(\sum_{j=1}^{k} c_j\right)^{-1}. \tag{5}$$

Аналогично при фиксированном коэффициенте пропорциональности $\alpha^*_{\min}$ можно минимизировать трафик восстановления β таким образом, чтобы граница из теоремы 2 выполнялась с равенством. Для фиксированной последовательности выживания $\left\langle S^{(\ell_{\lambda_i})}_{\lambda_i}\right\rangle_{i=1}^{n}$ с достаточно большим трафиком восстановления β неравенство $\alpha_{\lambda_i} \leqslant \left|S^{(\ell_{\lambda_i})}_{\lambda_i} \setminus \left(\bigcup\limits_{j=0}^{i-1}\{U_{\lambda_j}\}\right)\right|\beta$ выполняется для любого $i = 1, 2, \ldots, k$. Если выбрать $\beta = \beta_{\min}$ так, чтобы

$$\beta_{\min} = \max_{\langle S^{(\ell_{\lambda_i})}_{\lambda_i}\rangle_{i=1}^{n}} \left\{\max_{1\leqslant i\leqslant k}\left\{\alpha_{\lambda_i}\left|S^{(\ell_{\lambda_i})}_{\lambda_i} \setminus \left(\bigcup_{j=0}^{i-1}\{U_{\lambda_j}\}\right)\right|^{-1}\right\}\right\}, \tag{6}$$

то $\beta_{\min}$ будет минимальным значениям трафика восстановления β, при котором

$$\left|S^{(\ell_{\lambda_i})}_{\lambda_i} \setminus \left(\bigcup_{j=0}^{i-1}\{U_{\lambda_j}\}\right)\right|\beta_{\min} \geqslant \alpha_{\lambda_i}$$

для любого λ_i из произвольной последовательности выживания. Формально результат можно сформулировать следующим образом.

Лемма 3. *Рассмотрим неоднородную РСХД, имеющую n узлов, степень реконструкции k и множества выживания $S^{(\ell_i)}_i$, $i = 1, 2, \ldots, n$, $\ell_i = 1, 2, \ldots, \tau_i$ для некоторого $\tau_i \in \mathbb{Z}$. Семейство кодов с $\alpha_i = c_i\alpha_{\min} = d_i\beta_{\min}$ и $\beta = \beta_{\min}$ достигает фундаментальной границы* (*теорема* 2), *где $\alpha_{\min}$ и $\beta_{\min}$ вычисляются по формулам* (5) *и* (6).

§ 5. Заключение

В статье предложена модель неоднородной РСХД с переменными степенью реконструкции, объемом памяти узла и шириной восстановления. В частности, файл может быть реконструирован с помощью определенного множества узлов, а система может быть восстановлена после отказа любого узла путем установления соединения с некоторым множеством вспомогательных узлов. Для такой неоднородной РСХД исследованы фундаментальные кривые компромисса между стоимостью восстановления системы и стоимостью хранения в системе. Для построения кривой компромисса сформулирована задача двухкритериальной оптимизации с ограничениями в виде границы минимального разреза и неотрицательности параметров этой неоднородной РСХД. Задача двухкритериальной оптимизации решена методом взвешенных сумм для некоторых численных значений параметров этой неоднородной модели. При анализе кривой компромисса наблюдается некоторые новые оптимальные точки по сравнению с существующей неоднородной моделью [28]. Рассмотренная модель близка к реальным сценариям. Наша неоднородная модель достаточно гибкая, что позволяет преобразовать ее в любую существующую неоднородную или однородную РСХД путем наложения соответствующих ограничений. Интересной задачей представлялось бы построение кодов, достигающих оптимальных точек на кривой компромисса.

Авторы благодарны рецензентам за внимательное прочтение рукописи, способствовавшее улучшению изложения.

СПИСОК ЛИТЕРАТУРЫ

1. Amazon Elastic Compute Cloud (Amazon EC2). Web Service. Jan. 2013. Available at http://aws.amazon.com/ec2/.
2. *Huang C., Simitci H., Xu Y., Ogus A., Calder B., Gopalan P., Li J., Yekhanin S.* Erasure Coding in Windows Azure Storage // Proc. 2012 USENIX Annu. Technical Conf. (USENIX ATC'12). Boston, MA. June 13–15, 2012. P. 15–26.
3. Microsoft SkyDrive Live. Online Storage Service. Jan. 2013. Available at https://skydrive.live.com/.
4. *Sathiamoorthy M., Asteris M., Papailiopoulos D., Dimakis A.G., Vadali R., Chen S., Borthakur D.* XORing Elephants: Novel Erasure Codes for Big Data // Proc. VLDB Endow. 2013. V. 6. № 5. P. 325–336. https://doi.org/10.14778/2535573.2488339
5. *Dimakis A.G., Godfrey P.B., Wu Y., Wainwright M.J., Ramchandran K.* Network Coding for Distributed Storage Systems // Proc. 26th IEEE Annu. Joint Conf. on Computer Communications (INFOCOM'2007). Anchorage, AK, USA. May 6–12, 2007. P. 2000–2008. https://doi.org/10.1109/INFCOM.2007.232
6. *Dimakis A.G., Godfrey P.B., Wu Y., Wainwright M.J., Ramchandran K.* Network Coding for Distributed Storage Systems // IEEE Trans. Inform. Theory. 2010. V. 56. № 9. P. 4539–4551. https://doi.org/10.1109/TIT.2010.2054295
7. *Wu Y., Dimakis A., Ramchandran K.* Deterministic Regenerating Codes for Distributed Storage // Proc. 45th Annu. Allerton Conf. on Communication, Control, and Computing. Monticello, IL, USA. Sept. 26–28, 2007. V. 1. P. 242–249.
8. *Wu Y.* Existence and Construction of Capacity-Achieving Network Codes for Distributed Storage // Proc. 2009 IEEE Int. Symp. on Information Theory (ISIT'2009). Seoul, Korea. June 28 – July 3, 2009. P. 1150–1154. https://doi.org/10.1109/ISIT.2009.5206008
9. *Wu Y.* Existence and Construction of Capacity-Achieving Network Codes for Distributed Storage // IEEE J. Sel. Areas Commun. 2010. V. 28. № 2. P. 277–288. https://doi.org/10.1109/JSAC.2010.100217
10. *Goparaju S., El Rouayheb S., Calderbank R.* New Codes and Inner Bounds for Exact Repair in Distributed Storage Systems // Proc. 2014 IEEE Int. Symp. on Information Theory (ISIT'2014). Honolulu, HI, USA. June 29 – July 4, 2014. P. 1036–1040. https://doi.org/10.1109/ISIT.2014.6874990
11. *Shah N.B., Rashmi K.V., Kumar P.V.* A Flexible Class of Regenerating Codes for Distributed Storage // Proc. 2010 IEEE Int. Symp. on Information Theory (ISIT'2010). Austin, TX, USA. June 13–18, 2010. P. 1943–1947. https://doi.org/10.1109/ISIT.2010.5513353
12. *Dimakis A.G., Ramchandran K., Wu Y., Suh C.* A Survey on Network Codes for Distributed Storage // Proc. IEEE. 2011. V. 99. № 3. P. 476–489. https://doi.org/10.1109/JPROC.2010.2096170
13. *Prakash N., Krishnan M.N.* The Storage-Repair-Bandwidth Trade-off of Exact Repair Linear Regenerating Codes for the Case $d = k = n-1$, https://arXiv.org/abs/1501.03983v2 [cs.IT], 2015.
14. *Kubiatowicz J., Bindel D., Chen Y., Czerwinski S., Eaton P., Geels D., Gummadi R., Rhea S., Weatherspoon H., Weimer W., Wells C., Zhao B.* OceanStore: An Architecture for Global-Scale Persistent Storage // ACM SIGPLAN Notices. 2000. V. 35. № 11. P. 190–201. https://doi.org/10.1145/356989.357007
15. *Bianchi G., Melen R.* Performance and Dimensioning of a Hierarchical Video Storage Network for Interactive Video Services // Eur. Trans. Telecommun. 1996. V. 7. № 4. P. 349–358. https://doi.org/10.1002/ett.4460070407
16. *Pawar S., El Rouayheb S., Zhang H., Lee K., Ramchandran K.* Codes for a Distributed Caching Based Video-on-Demand System // Conf. Rec. 46th Asilomar Conf. on Signals,

Systems and Computers (ASILOMAR'2011). Pacific Grove, CA, USA. Nov. 6–9, 2011. P. 1783–1787. https://doi.org/10.1109/ACSSC.2011.6190328

17. *Ntranos V., Caire G., Dimakis A.G.* Allocations for Heterogenous Distributed Storage, https://arXiv.org/abs/1202.1596 [cs.IT], 2012.
18. *Li Z., Ho T., Leong D., Yao H.* Distributed Storage Allocation for Heterogeneous Systems // Proc. 51st Annu. Allerton Conf. on Communication, Control, and Computing. Monticello, IL, USA. Oct. 2–4, 2013. P. 320–326. https://doi.org/10.1109/Allerton.2013.6736541
19. *Leong D., Dimakis A.G., Ho T.* Distributed Storage Allocations // IEEE Trans. Inform. Theory. 2012. V. 58. № 7. P. 4733–4752. https://doi.org/10.1109/TIT.2012.2191135
20. *Gerami M., Xiao M., Skoglund M.* Optimal-Cost Repair in Multi-hop Distributed Storage Systems // Proc. 2011 IEEE Int. Symp. on Information Theory (ISIT'2011). St. Petersburg, Russia. July 31 – Aug. 5, 2011. P. 1437–1441. https://doi.org/10.1109/ISIT.2011.6033777
21. *Akhlaghi S., Kiani A., Ghanavati M.R.* Cost-Bandwidth Tradeoff in Distributed Storage Systems // Comput. Commun. 2010. V. 33. № 17. P. 2105–2115. https://doi.org/10.1016/j.comcom.2010.07.022
22. *Akhlaghi S., Kiani A., Ghanavati M.R.* A Fundamental Trade-off between the Download Cost and Repair Bandwidth in Distributed Storage Systems // Proc. 2010 IEEE Int. Symp. on Network Coding (NetCod'2010). Toronto, ON, Canada. June 9–11, 2010. P. 97–102. https://doi.org/10.1109/NETCOD.2010.5487685
23. *Yu Q., Shum K.W., Sung C.W.* Minimization of Storage Cost in Distributed Storage Systems with Repair Consideration // Proc. 2011 IEEE Global Telecommunications Conf. (GLOBECOM'2011). Houston, TX, USA. Dec. 5–9, 2011. P. 2931–2935. https://doi.org/10.1109/GLOCOM.2011.6133729
24. *Pernas J., Yuen C., Gastón B., Pujol J.* Non-homogeneous Two-Rack Model for Distributed Storage Systems // Proc. 2013 IEEE Int. Symp. on Information Theory (ISIT'2013). Istanbul, Turkey. July 7–12, 2013. P. 1237–1241. https://doi.org/10.1109/ISIT.2013.6620424
25. *Gastón B., Pujol J., Villanueva M.* A Realistic Distributed Storage Systems That Minimizes Data Storage and Repair Bandwidth // Proc. 2006 Data Compression Conf. (DCC'2006). Snowbird, UT, USA. Mar. 20–22, 2013. P. 491. https://doi.org/10.1109/DCC.2013.72
26. *Ernvall T., El Rouayheb S., Hollanti C., Poor H.V.* Capacity and Security of Heterogeneous Distributed Storage Systems // Proc. 2013 IEEE Int. Symp. on Information Theory (ISIT'2013). Istanbul, Turkey. July 7–12, 2013. P. 1247–1251. https://doi.org/10.1109/ISIT.2013.6620426
27. *Benerjee K.G., Gupta M.K.* On Heterogeneous Regenerating Codes and Capacity of Distributed Storage Systems, https://arXiv.org/abs/1402.3801, [cs.IT], 2014.
28. *Yu Q., Shum K.W., Sung C.W.* Tradeoff between Storage Cost and Repair Cost in Heterogeneous Distributed Storage Systems // Trans. Emerg. Telecommun. Technol. 2015. V. 26. № 10. P. 1201–1211. https://doi.org/10.1002/ett.2887
29. *Kiani A., Akhlaghi S.* Selective Regenerating Codes // IEEE Commun. Lett. 2011. V. 15. № 8. P. 854–856. https://doi.org/10.1109/LCOMM.2011.061611.102271
30. *Senthoor K., Sasidharan B., Kumar P.V.* Improved Layered Regenerating Codes Characterizing the Exact-Repair Storage-Repair Bandwidth Tradeoff for Certain Parameter Sets // Proc. 2015 IEEE Information Theory Workshop (ITW'2015). Jerusalem, Israel. Apr. 26 – May 1, 2015. P. 224–228. https://doi.org/10.1109/ITW.2015.7133121
31. *Sasidharan B., Senthoor K., Kumar P.V.* An Improved Outer Bound on the Storage-Repair-Bandwidth Tradeoff of Exact-Repair Regenerating Codes // Proc. 2014 IEEE Int. Symp. on Information Theory (ISIT'2014). Honolulu, HI, USA. June 29 – July 4, 2014. P. 2430–2434. https://doi.org/10.1109/ISIT.2014.6875270
32. *Sasidaran B., Kumar P.V.* On the Interior Points of the Storage-Repair Bandwidth Tradeoff of Regenerating Codes // Proc. 51st Annu. Allerton Conf. on Communication, Control, and Computing. Monticello, IL, USA. Oct. 2–4, 2013. P. 788–795. https://doi.org/10.1109/Allerton.2013.6736605
33. *Duursma I.M.* Outer Bounds for Exact Repair Codes, https://arXiv.org/abs/1406.4852 [cs.IT], 2014.

34. *Ahmad I., Wang C.C.* When and by How Much Can Helper Node Selection Improve Regenerating Codes? // Proc. 52nd Annu. Allerton Conf. on Communication, Control, and Computing. Monticello, IL, USA. Sept. 30 – Oct. 3, 2014. P. 459–466. https://doi.org/10.1109/ALLERTON.2014.7028491

35. *Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W.* Network Information Flow // IEEE Trans. Inform. Theory. 2000. V. 46. № 4. P. 1204–1216. https://doi.org/10.1109/18.850663

36. *Elias P., Feinstein A., Shannon C.* A Note on the Maximum Flow Through a Network // IEEE Trans. Inform. Theory. 1956. V. 2. № 4. P. 117–119. https://doi.org/10.1109/TIT.1956.1056816

37. *Ford L.R., Jr., Fulkerson D.R.* Maximal Flow through a Network // Canad. J. Math. 1956. V. 8. P. 399–404. https://doi.org/10.4153/CJM-1956-045-5

38. lp_solve (mathematical optimization software). A Mixed Integer Linear Programming (MILP) Solver. Version 5.5.2.0, 2011. Available at http://lpsolve.sourceforge.net/5.5/.

Бенерджи Кришна Гопал
Гупта Маниш Кумар✉
Институт информационных технологий и техники связи им. Дхирубхая Амбани, Гандинагар, штат Гуджарат, Индия
✉mankg@computer.org

Поступила в редакцию
13.08.2019
После доработки
02.10.2020
Принята к публикации
30.12.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 2021 Вып. 1

УДК 621.391 : 519.72

© 2021 г. **В.В. Прелов**

f-ДИВЕРГЕНЦИЯ И СКЛЕИВАНИЕ ВЕРОЯТНОСТНЫХ РАСПРЕДЕЛЕНИЙ[1]

Рассматривается задача о нахождении минимальных и максимальных значений f-дивергенции дискретных распределений вероятностей P и Q при условии, что заданы одно из этих распределений и величина их склеивания. Для минимума f-дивергенции при указанных условиях получено явное выражение, а для ее максимума – точное выражение, которое в общем случае не является явным, но для многих частных случаев позволяет выписать как явные формулы, так и простые верхние границы, являющиеся в некоторых случаях оптимальными. Подобные явные формулы и верхние границы получены для дивергенции Кульбака – Лейблера и χ^2-дивергенции, являющихся важнейшими частными случаями f-дивергенции.

Ключевые слова: f-дивергенция, дивергенция Кульбака – Лейблера, χ^2-дивергенция, склеивание дискретных распределений вероятностей.

DOI: 10.31857/S0555292321010034

§ 1. Введение и формулировки основных результатов

Пусть $P = \{p_i,\ i \in \mathcal{N}\}$ и $Q = \{q_i,\ i \in \mathcal{N}\}$ – дискретные распределения вероятностей со значениями в конечном множестве $\mathcal{N} = \{1, 2, \dots, n\}$. Напомним, что f-дивергенция $D_f(P\,\|\,Q)$ распределения P относительно Q определяется равенством (см. [1, 2])

$$D_f(P\,\|\,Q) = \sum_{i\in\mathcal{N}} q_i f\left(\frac{p_i}{q_i}\right), \tag{1}$$

где $f\colon (0,\infty) \to \mathbb{R}$ – выпуклая функция, такая что $f(1) = 0$ (в дальнейшем будем всегда считать, что $f(\cdot)$ – дважды дифференцируемая функция, такая что $f''(x) > 0$, $x \neq 1$). При этом всегда по определению предполагается, что

$$0 \cdot f\left(\frac{0}{0}\right) = 0, \quad f(0) = \lim_{u\downarrow 0} f(u), \quad 0 \cdot f\left(\frac{a}{0}\right) = \lim_{\varepsilon\downarrow 0} \varepsilon f\left(\frac{a}{\varepsilon}\right) = a \lim_{t\to\infty} \frac{f(t)}{t},$$

где $a \neq 0$. Частными случаями f-дивергенции являются многие известные меры различия между распределениями вероятностей, используемые в теории информации, теории вероятностей и математической статистике. Наиболее важными примерами f-дивергенций являются дивергенция Кульбака – Лейблера (или просто дивергенция)

$$D(P\,\|\,Q) = \sum_{i\in\mathcal{N}} p_i \log \frac{p_i}{q_i} = D_f(P\,\|\,Q)$$

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364).

при $f(t) = t\log t$ и χ^2-дивергенция

$$\chi^2(P\,\|\,Q) = \sum_{i\in\mathcal{N}} \frac{(p_i - q_i)^2}{q_i} = D_f(P\,\|\,Q)$$

при $f(t) = (t-1)^2$, а также вариационное расстояние, дивергенция Хеллингера и др. (см., например, [3, 4]).

Напомним также, что α-склеиванием дискретных распределений вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$ и $Q = \{q_i,\ i \in \mathcal{N}\}$ называется совместное распределение P_{XY} случайных величин X и Y со значениями в множестве $\mathcal{N}$ и маргинальными распределениями $P_X = P$ и $P_Y = Q$, такое что $\Pr\{X = Y\} = \alpha$ (см. [5]). В дальнейшем величину склеивания распределений P и Q будем обозначать через $s(P, Q)$.

В работе [6] рассматривалась задача о нахождении минимальных и максимальных значений дивергенции Реньи $D_\lambda(P\,\|\,Q)$ при условии, что заданы одно из распределений P или Q и величина их склеивания $s(P, Q)$. В настоящей статье рассматривается аналогичная задача о нахождении минимальных и максимальных значений для произвольной f-дивергенции дискретных распределений вероятностей P и Q, а также ее важнейших частных случаев – дивергенции Кульбака – Лейблера и χ^2-дивергенции, которые, например, используются при получении границ для коэффициентов сжатия f-дивергенций [4]. Отметим, что задача о нахождении экстремальных значений f-дивергенции $D_f(P\,\|\,Q)$, когда вместо условия α-склеивания накладывалось условие на вариационное расстояние между P и Q, рассматривалась в [7–9].

Для формулировки полученных результатов введем необходимые определения и обозначения. Для заданных распределения вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$, действительного числа α, $0 \leqslant \alpha \leqslant 1$, и выпуклой функции $f(\cdot)$, задающей f-дивергенцию $D_f(P\,\|\,Q)$, определим величину $D_f^{\min}(P, \alpha)$ равенством

$$D_f^{\min}(P, \alpha) = \min_{Q:\, s(P,Q)=\alpha} D_f(P\,\|\,Q), \tag{2}$$

где минимум берется по всевозможным распределениям $Q = \{q_i,\ i \in \mathcal{N}\}$, для которых существует их α-склеивание с распределением P. Аналогично определяется и величина $D_f^{\min}(Q, \alpha)$, если задано распределение $Q = \{q_i,\ i \in \mathcal{N}\}$, т.е.

$$D_f^{\min}(Q, \alpha) = \min_{P:\, s(P,Q)=\alpha} D_f(P\,\|\,Q). \tag{3}$$

В случае, когда $P = \{p, 1-p\}$ и $Q = \{q, 1-q\}$, вместо $D_f(P\,\|\,Q)$ будем использовать обозначение $d_f(p\,\|\,q)$, т.е.

$$d_f(p\,\|\,q) = qf\Big(\frac{p}{q}\Big) + (1-q)f\Big(\frac{1-p}{1-q}\Big). \tag{4}$$

Заметим, что из свойств функции $f(\cdot)$ (выпуклости и равенства $f(1) = 0$) следует, что $d_f(p\,\|\,q)$ является выпуклой неотрицательной функцией как параметра p, так и параметра q, причем $d_f(p\,\|\,q) = 0$ при $p = q$.

Т е о р е м а 1. *Справедливы следующие равенства*:

$$D_f^{\min}(P, \alpha) = \begin{cases} 0, & \text{если } p_{\max} \leqslant \dfrac{1}{2} + \dfrac{\alpha}{2}, \\ d_f(p_{\max}\,\|\,1 - p_{\max} + \alpha), & \text{если } p_{\max} \geqslant \dfrac{1}{2} + \dfrac{\alpha}{2}, \end{cases} \tag{5}$$

$$D_f^{\min}(Q,\alpha)=\begin{cases}0, & \text{если } q_{\max}\leqslant\dfrac{1}{2}+\dfrac{\alpha}{2},\\ d_f(1-q_{\max}+\alpha\,\|\,q_{\max}), & \text{если } q_{\max}\geqslant\dfrac{1}{2}+\dfrac{\alpha}{2},\end{cases}\tag{6}$$

где $p_{\max}=\max\limits_{i\in\mathcal{N}}p_i$ *и* $q_{\max}=\max\limits_{i\in\mathcal{N}}q_i$.

Доказательства этой и нижеследующих теорем приведены в § 2. Отметим, что частный случай теоремы 1, когда $f(t)=t\log t$ или $f(t)=-\log t$, т.е. для дивергенции Кульбака – Лейблера, был доказан в [4].

Для формулировки следующей теоремы введем еще несколько определений. Для заданных распределения вероятностей $P=\{p_i,\ i\in\mathcal{N}\}$, действительного числа α, $0\leqslant\alpha\leqslant 1$, и выпуклой функции $f(\cdot)$, задающей f-дивергенцию $D_f(P\,\|\,Q)$, определим величину $D_f^{\max}(P,\alpha)$ равенством

$$D_f^{\max}(P,\alpha)=\max_{Q\colon s(P,Q)=\alpha}D_f(P\,\|\,Q),\tag{7}$$

где максимум берется по всевозможным распределениям $Q=\{q_i,\ i\in\mathcal{N}\}$, для которых существует их α-склеивание с распределением P. Аналогично определяется и величина $D_f^{\max}(Q,\alpha)$, если задано распределение $Q=\{q_i,\ i\in\mathcal{N}\}$, т.е.

$$D_f^{\max}(Q,\alpha)=\max_{P\colon s(P,Q)=\alpha}D_f(P\,\|\,Q).\tag{8}$$

Всякое равенство

$$\alpha=\sum_{i\in I}p_i+\beta,\quad\text{где } I\subseteq\mathcal{N},\tag{9}$$

назовем *допустимым* (P,I)*-представлением* α, если либо $\beta=0$, либо существует индекс $j\in\mathcal{N}\setminus I$, такой что $0<\beta<p_j$. Аналогично определяется *допустимое* (Q,I)*-представление* α, если задано распределение $Q=\{q_i,\ i\in\mathcal{N}\}$ и параметр α, $0\leqslant\alpha\leqslant 1$.

Всякое α-склеивание заданного распределения вероятностей $P=\{p_i,\ i\in\mathcal{N}\}$ с некоторым распределением $Q=\{q_i,\ i\in\mathcal{N}\}$ задается с помощью квадратной матрицы $M=\|p_{ij}\|_{i,j=1}^n$ с неотрицательными элементами p_{ij}, такой что $\sum\limits_{j=1}^n p_{ij}=p_i$ для всех $i\in\mathcal{N}$, $\sum\limits_{i=1}^n p_{ij}=q_j$ для всех $j\in\mathcal{N}$ и $\sum\limits_{i=1}^n p_{ii}=\alpha$. В этом случае положим $D_f(M)=D_f(P\,\|\,Q)$. Аналогично (с заменой в предыдущем определении распределения P на Q и наоборот) задается α-склеивание данного распределения вероятностей $Q=\{q_i,\ i\in\mathcal{N}\}$ с некоторым распределением $P=\{p_i,\ i\in\mathcal{N}\}$.

Каждому допустимому (P,I)-представлению α сопоставим множество $\mathcal{M}(P,I)$ матриц $M=\|p_{ij}\|_{i,j=1}^n$, осуществляющих α-склеивание заданного распределения вероятностей $P=\{p_i,\ i\in\mathcal{N}\}$ с некоторым распределением $Q=\{q_i,\ i\in\mathcal{N}\}$ и обладающих следующим свойством: на (главной) диагонали каждой такой матрицы стоят числа p_i и β, входящие в данное допустимое (P,I)-представление α, а все остальные ненулевые элементы матрицы находятся в некотором столбце (будем называть такой столбец *главным*) и, возможно, лишь один ненулевой элемент находится вне диагонали и этого главного столбца. Аналогично, каждому допустимому (Q,I)-представлению α сопоставляется множество $\mathcal{M}(Q,I)$ матриц $M=\|p_{ij}\|_{i,j=1}^n$, осуществляющих α-склеивание заданного распределения вероятностей $Q=\{q_i,\ i\in\mathcal{N}\}$ с некоторым распределением $P=\{p_i,\ i\in\mathcal{N}\}$.

Теорема 2. *Для любого распределения вероятностей*

$$P=\{p_i,\ i\in\mathcal{N}\},\quad p_1\geqslant p_2\geqslant\ldots\geqslant p_n>0,$$

и любого α, $0 \leqslant \alpha \leqslant 1$, *справедливо равенство*

$$D_f^{\max}(P,\alpha) = \max_{(P,I)} \max_{M \in \mathcal{M}(P,I)} D_f(M), \tag{10}$$

где первый максимум в правой части (10) *берется по всем допустимым* (P,I)*-представлениям* α*. В частности,*

$$D_f^{\max}(P,\alpha) = \begin{cases} \infty, & \text{если } \alpha \leqslant 1-p_n \text{ и } f^* = \infty, \\ K_P, & \text{если } \alpha > 1-p_n, \end{cases} \tag{11}$$

где $f^* = \lim\limits_{t\to\infty} \dfrac{f(t)}{t}$, *а*

$$K_P = \max\left\{ (\alpha - 1 + p_n) f\left(\frac{p_n}{\alpha - 1 + p_n}\right) + (1 - \alpha + p_{n-1}) f\left(\frac{p_{n-1}}{1 - \alpha + p_{n-1}}\right), \right.$$
$$\left. (\alpha - 1 + p_{n-1}) f\left(\frac{p_{n-1}}{\alpha - 1 + p_{n-1}}\right) + (1 - \alpha + p_n) f\left(\frac{p_n}{1 - \alpha + p_n}\right) \right\}. \tag{12}$$

Во многом аналогичная теорема справедлива и для величины $D_f^{\max}(Q,\alpha)$, определенной в (8).

Т е о р е м а 3. *Для любого распределения вероятностей*

$$Q = \{q_i,\ i \in \mathcal{N}\}, \quad q_1 \geqslant q_2 \geqslant \ldots \geqslant q_n > 0,$$

и любого α, $0 \leqslant \alpha \leqslant 1$, *справедливо равенство*

$$D_f^{\max}(Q,\alpha) = \max_{(Q,I)} \max_{M \in \mathcal{M}(Q,I)} D_f(M), \tag{13}$$

где первый максимум в правой части (13) *берется по всем допустимым* (Q,I)*-представлениям* α*. В частности,*

$$D_f^{\max}(Q,\alpha) = \begin{cases} \infty, & \text{если } \alpha \leqslant 1-q_n \text{ и } f(0) = \infty, \\ K_Q, & \text{если } \alpha > 1-q_n, \end{cases} \tag{14}$$

где

$$K_Q = \max\left\{ q_n f\left(\frac{\alpha - 1 + q_n}{q_n}\right) + q_{n-1} f\left(\frac{1 - \alpha + q_{n-1}}{q_{n-1}}\right), \right.$$
$$\left. q_{n-1} f\left(\frac{\alpha - 1 + q_{n-1}}{q_{n-1}}\right) + q_n f\left(\frac{1 - \alpha + q_n}{q_n}\right) \right\}. \tag{15}$$

Как видно из формулировок теорем 2 и 3, формулы (10) и (13) не позволяют для общего случая f-дивергенции выписывать явные выражения для $D_f^{\max}(P,\alpha)$ при $\alpha \leqslant 1-p_n$ и $f^* < \infty$ и для $D_f^{\max}(Q,\alpha)$ при $\alpha \leqslant 1-q_n$ и $f(0) < \infty$. Однако для многих конкретных f-дивергенций эти формулы позволяют получить как хорошие явные верхние границы для $D_f^{\max}(P,\alpha)$ и $D_f^{\max}(Q,\alpha)$ (которые в некоторых случаях являются оптимальными), так и явные выражения для них при малых значениях α. Ниже мы покажем это на примерах дивергенции Кульбака – Лейблера и χ^2-дивергенции.

Обозначим

$$D^{\max}(P,\alpha) = \max_{Q:\, s(P,Q)=\alpha} D(P\,\|\,Q) = D_f^{\max}(P,\alpha) \quad \text{при } f(t) = t\log t, \tag{16}$$

$$D^{\max}(Q,\alpha) = \max_{P:\, s(P,Q)=\alpha} D(P\,\|\,Q) = D_f^{\max}(Q,\alpha) \quad \text{при } f(t) = t\log t, \tag{17}$$

$$\chi^2_{\max}(P,\alpha) = \max_{Q:\, s(P,Q)=\alpha} \chi^2(P\,\|\,Q) = D_f^{\max}(P,\alpha) \quad \text{при } f(t) = (t-1)^2, \tag{18}$$

$$\chi^2_{\max}(Q,\alpha) = \max_{P:\, s(P,Q)=\alpha} \chi^2(P\,\|\,Q) = D_f^{\max}(Q,\alpha) \quad \text{при } f(t) = (t-1)^2, \tag{19}$$

где $D_f^{\max}(P,\alpha)$ и $D_f^{\max}(Q,\alpha)$ определены в (7) и (8) соответственно.

Теорема 4. *Для величин $D^{\max}(P,\alpha)$ и $D^{\max}(Q,\alpha)$, определенных в (16) и (17), справедливы следующие утверждения*:

- *Если заданы распределение вероятностей $P = \{p_i, i \in \mathcal{N}\}$, $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n > 0$, и число α, $0 \leqslant \alpha \leqslant 1$, то*

$$D^{\max}(P,\alpha) = \begin{cases} \infty, & \text{если } \alpha \leqslant 1 - p_n, \\ p_n \log \dfrac{p_n}{p_n - 1 + \alpha} + p_{n-1} \log \dfrac{p_{n-1}}{p_{n-1} + 1 - \alpha}, & \text{если } \alpha > 1 - p_n; \end{cases} \tag{20}$$

- *Если заданы распределение вероятностей $Q = \{q_i, i \in \mathcal{N}\}$, $q_1 \geqslant q_2 \geqslant \ldots \geqslant q_n > 0$, и число α, $0 \leqslant \alpha \leqslant 1$, то*

$$D^{\max}(Q,\alpha) = (1 + \alpha - q_n) \log \frac{1 + \alpha - q_n}{q_n} + (q_n - \alpha) \log \frac{q_n - \alpha}{q_{n-1}}, \tag{21}$$

если $\alpha \leqslant q_n$, и

$$D^{\max}(Q,\alpha) = (q_n - 1 + \alpha) \log \frac{q_n - 1 + \alpha}{q_n} + (1 - \alpha + q_{n-1}) \log \frac{1 - \alpha + q_{n-1}}{q_{n-1}}, \tag{22}$$

если $\alpha > 1 - q_n$;

- *Для всех α, $q_n \leqslant \alpha \leqslant 1 - q_n$, справедлива верхняя граница*

$$D^{\max}(Q,\alpha) \leqslant (1 - \alpha + q_n) \log \frac{1 - \alpha + q_n}{q_n}, \tag{23}$$

причем эта верхняя граница достигается, т.е. в (23) имеет место знак равенства, если $\alpha = \sum\limits_{i=1}^{n-1} a_i q_i + q_n$ при некоторых $a_i \in \{0,1\}$.

Из этой теоремы можно также вывести следствие для величин $D^{\max}(p_{\min},\alpha)$ и $D^{\max}(q_{\min},\alpha)$, определяемых равенствами

$$D^{\max}(p_{\min},\alpha) = \max_{(P,Q):\, s(P,Q)=\alpha,\, \min\limits_{i\in\mathcal{N}} p_i = p_{\min}} D(P\,\|\,Q), \tag{24}$$

$$D^{\max}(q_{\min},\alpha) = \max_{(P,Q):\, s(P,Q)=\alpha,\, \min\limits_{i\in\mathcal{N}} q_i = q_{\min}} D(P\,\|\,Q), \tag{25}$$

где максимумы в (24), (25) берутся по всевозможным распределениям $P = \{p_i, i \in \mathcal{N}\}$ и $Q = \{q_i,\ i \in \mathcal{N}\}$ с заданными параметрами $p_{\min} > 0$ в (24) и $q_{\min} > 0$ в (25), таким что $s(P,Q) = \alpha$.

Следствие 1. *Для величин $D^{\max}(p_{\min},\alpha)$ и $D^{\max}(q_{\min},\alpha)$, определенных в (24) и (25), в случае $|\mathcal{N}| = n \geqslant 3$ справедливы следующие утверждения*:

- *Для всех* $p_{\min} > 0$ *и* α, $0 \leqslant \alpha \leqslant 1$, *справедливо равенство*

$$D^{\max}(p_{\min}, \alpha) = \begin{cases} \infty, & \text{если } \alpha \leqslant 1 - p_{\min}, \\ p_{\min} \log \dfrac{p_{\min}^2}{p_{\min}^2 - (1-\alpha)^2}, & \text{если } \alpha > 1 - p_{\min}; \end{cases} \tag{26}$$

- *Для всех* $q_{\min} > 0$ *и* α, *таких что* $0 \leqslant \alpha \leqslant q_{\min}$ *или* $1 - q_{\min} \leqslant \alpha \leqslant 1$, *справедливы равенства*

$$D^{\max}(q_{\min}, \alpha) = \log \frac{1}{q_{\min}} - h(1 + \alpha - q_{\min}), \quad \text{если } \alpha \leqslant q_{\min}, \tag{27}$$

$$D^{\max}(q_{\min}, \alpha) = 2q_{\min} \left[\log 2 - h\left(\frac{1 - \alpha + q_{\min}}{2q_{\min}} \right) \right], \quad \text{если } \alpha \geqslant 1 - q_{\min}, \tag{28}$$

где $h(x) = -x \log x - (1-x) \log(1-x)$, $0 \leqslant x \leqslant 1$;

- *Для всех* $q_{\min} > 0$ *и* α, $q_{\min} < \alpha < 1 - q_{\min}$, *справедлива верхняя граница*

$$D^{\max}(q_{\min}, \alpha) \leqslant (1 - \alpha + q_{\min}) \log \frac{1 - \alpha + q_{\min}}{q_{\min}}, \tag{29}$$

причем эта верхняя граница достигается, т.е. в (29) *имеет место знак равенства, если* $2q_{\min} \leqslant \alpha < 1 - q_{\min}$ *и* $q_{\min} \leqslant \dfrac{1}{n+1}$, *а также если* $q_{\min} \leqslant \dfrac{1}{n}$ *и* $\alpha = kq_{\min}$, *где* k – *любое целое, такое что* $2 \leqslant k \leqslant n-1$.

Доказательство. Равенство (26) является прямым следствием формулы (20), так как, с одной стороны,

$$p_{n-1} \log \frac{p_{n-1}}{p_{n-1} + 1 - \alpha} \leqslant p_n \log \frac{p_n}{p_n + 1 - \alpha},$$

а с другой стороны, если $|\mathcal{N}| \geqslant 3$, то всегда существует распределение вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$, такое что $p_{n-1} = p_n = p_{\min}$. Аналогично доказывается, что и равенства (27), (28) являются прямыми следствиями соответствующих равенств (21), (22).

Наконец, достижение равенства в верхней границе (29) при сформулированных там условиях также следует из утверждения теоремы 4 о достижении верхней границы (23). Действительно, нетрудно предъявить соответствующее распределение вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$, зависящее от значения параметра α, для которого имеет место равенство $\alpha = \sum\limits_{i=1}^{n-1} a_i q_i + q_n$ при некоторых $a_i \in \{0, 1\}$. А именно, если $kq_{\min} < \alpha < (k+1)q_{\min}$, где $k = 2, 3, \ldots, n-2$, или $(n-1)q_{\min} < \alpha < 1 - q_{\min}$, то очевидно, что $\alpha = \sum\limits_{i=1}^{k-1} q_i + q_n$ для распределения $Q = \{q_i,\ i \in \mathcal{N}\}$, компоненты q_i которого задаются равенствами

$$q_i = \begin{cases} q_{\min} & \text{при} \quad i = 1, 2, \ldots, k-2, \\ \alpha - (k-1)q_{\min} & \text{при } i = k-1, \\ \dfrac{1-\alpha}{n-k} & \text{при } i = k, k+1, \ldots, n-1, \\ q_{\min} & \text{при } i = n, \end{cases}$$

и обладают тем свойством, что все $q_i \leqslant q_{\min}$, если $q_{\min} \leqslant \dfrac{1}{n+1}$.

Если же $\alpha = kq_{\min}$, где $k = 2, 3, \ldots, n-1$, то снова очевидно, что $\alpha = \sum\limits_{i=1}^{k-1} q_i + q_n$ для распределения $Q = \{q_i,\, i \in \mathcal{N}\}$, компоненты q_i которого задаются равенствами

$$q_i = \begin{cases} q_{\min} & \text{при } i = 1, 2, \ldots, n-1, \\ 1 - (n-1)q_{\min} & \text{при } i = n, \end{cases}$$

и при этом все эти $q_i \leqslant q_{\min}$, если $q_{\min} \leqslant \dfrac{1}{n}$. ▲

Теорема 5. *Для величин $\chi^2_{\max}(P, \alpha)$ и $\chi^2_{\max}(Q, \alpha)$, определенных в (18) и (19), справедливы следующие утверждения*:

- *Если заданы распределение вероятностей $P = \{p_i, i \in \mathcal{N}\}$, $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n > 0$, и число α, $0 \leqslant \alpha \leqslant 1$, то*

$$\chi^2_{\max}(P, \alpha) = \begin{cases} \infty, & \text{если } \alpha \leqslant 1 - p_n, \\ \dfrac{(1-\alpha)^2}{\alpha + p_n - 1} + \dfrac{(1-\alpha)^2}{1 + p_{n-1} - \alpha}, & \text{если } \alpha > 1 - p_n; \end{cases} \tag{30}$$

- *Если заданы распределение вероятностей $Q = \{q_i, i \in \mathcal{N}\}$, $q_1 \geqslant q_2 \geqslant \ldots \geqslant q_n > 0$, и число α, $0 \leqslant \alpha \leqslant 1$, то*

$$\chi^2_{\max}(Q, \alpha) = \begin{cases} \dfrac{(1 + \alpha - q_n)^2}{q_n} + \dfrac{(q_n - \alpha)^2}{q_{n-1}} - 1, & \text{если } \alpha \leqslant q_n, \\ \dfrac{(1-\alpha)^2}{q_n} + \dfrac{(1-\alpha)^2}{q_{n-1}}, & \text{если } \alpha \geqslant 1 - q_n; \end{cases} \tag{31}$$

- *Для всех α, $q_n < \alpha < 1 - q_n$, справедлива верхняя граница*

$$\chi^2_{\max}(Q, \alpha) \leqslant \frac{(1-\alpha)^2}{q_n} + 1 - \alpha, \tag{32}$$

причем эта верхняя граница достигается, т.е. в (32) имеет место знак равенства, если $\alpha = q_n + \sum\limits_{i=1}^{n-1} a_i q_i$ при некоторых $a_i \in \{0, 1\}$.

Из этой теоремы также можно вывести приведенное ниже следствие (подобное следствию 1) для величин $\chi^2_{\max}(p_{\min}, \alpha)$ и $\chi^2_{\max}(q_{\min}, \alpha)$, определяемых равенствами

$$\chi^2_{\max}(p_{\min}, \alpha) = \max_{(P,Q):\, s(P,Q)=\alpha,\, \min\limits_{i \in \mathcal{N}} p_i = p_{\min}} \chi^2(P \,\|\, Q), \tag{33}$$

$$\chi^2_{\max}(q_{\min}, \alpha) = \max_{(P,Q):\, s(P,Q)=\alpha,\, \min\limits_{i \in \mathcal{N}} q_i = q_{\min}} \chi^2(P \,\|\, Q), \tag{34}$$

где максимумы в (33), (34) берутся по всевозможным распределениям $P = \{p_i, i \in \mathcal{N}\}$ и $Q = \{q_i,\, i \in \mathcal{N}\}$ с заданными параметрами $p_{\min} > 0$ в (33) и $q_{\min} > 0$ в (34), таким что $s(P, Q) = \alpha$.

Следствие 2. *Для величин $\chi^2_{\max}(p_{\min}, \alpha)$ и $\chi^2_{\max}(q_{\min}, \alpha)$, определенных в (33) и (34), в случае $|\mathcal{N}| = n \geqslant 3$ справедливы следующие утверждения*:

- *Для всех $p_{\min} > 0$ и α, $0 \leqslant \alpha \leqslant 1$, справедливо равенство*

$$\chi^2_{\max}(p_{\min}, \alpha) = \begin{cases} \infty, & \text{если } \alpha \leqslant 1 - p_{\min}, \\ \dfrac{2p_{\min}(1-\alpha)^2}{p^2_{\min} - (1-\alpha)^2}, & \text{если } \alpha > 1 - p_{\min}; \end{cases} \tag{35}$$

- *Для всех* $q_{\min} > 0$ *справедливо равенство*

$$\chi^2_{\max}(q_{\min}, \alpha) = \begin{cases} \dfrac{(1+\alpha-q_{\min})^2 + (q_{\min}-\alpha)^2}{q_{\min}} - 1, & \text{если } \alpha \leqslant q_{\min}, \\ \dfrac{2(1-\alpha)^2}{q_{\min}}, & \text{если } \alpha \geqslant 1 - q_{\min}; \end{cases} \tag{36}$$

- *Для всех* $q_{\min} > 0$ *и* α, $q_{\min} < \alpha < 1 - q_{\min}$, *справедлива верхняя граница*

$$\chi^2_{\max}(q_{\min}, \alpha) \leqslant \frac{(1-\alpha)^2}{q_{\min}} + 1 - \alpha, \tag{37}$$

причем эта верхняя граница достигается, т.е. в (37) *имеет место знак равенства, если* $2q_{\min} \leqslant \alpha < 1 - q_{\min}$ *и* $q_{\min} \leqslant \dfrac{1}{n+1}$, *а также если* $q_{\min} \leqslant \dfrac{1}{n}$ *и* $\alpha = kq_{\min}$, *где* k – *любое целое, такое что* $2 \leqslant k \leqslant n-1$.

Доказательство этого следствия вполне аналогично приведенному выше доказательству следствия 1 и поэтому здесь не приводится.

§ 2. Доказательства

Доказательство теоремы 1. Доказательство равенств (5) и (6) проводится вполне аналогично. Поэтому докажем, например, первое из них. Для доказательства того, что $D_f^{\min}(P, \alpha) = 0$ при $\alpha \geqslant 2p_{\max} - 1$ воспользуемся следующим утверждением (см. [3, теорема 1]): если $P = \{p_i,\ i \in \mathcal{N}\}$ и $Q = \{q_i,\ i \in \mathcal{N}\}$ – два распределения вероятностей, а α, $0 \leqslant \alpha \leqslant 1$, – некоторое действительное число, то α-склеивание P и Q (т.е. такое, что $s(P, Q) = \alpha$) существует тогда и только тогда, когда

$$\max_{i \in \mathcal{N}} [p_i + q_i - 1]^+ \leqslant \alpha \leqslant \sum_{i \in \mathcal{N}} \min\{p_i, q_i\}, \quad \text{где } [x]^+ = \begin{cases} x, & \text{если } x \geqslant 0, \\ 0, & \text{если } x \leqslant 0. \end{cases}$$

Из этого сразу следует, что $D_f^{\min}(P, \alpha) = 0$, если $p_{\max} \leqslant 1/2 + \alpha/2$, так как в этом случае существует α-склеивание распределения P с собой, а $D_f(P \,\|\, P) = 0$, так как по предположению $f(1) = 0$.

Поэтому надо доказать лишь второе из равенств в (5), когда предполагается, что $0 \leqslant \alpha \leqslant 2p_{\max} - 1$. Для этого вначале заметим, что для любых распределений вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$ и $Q = \{q_i,\ i \in \mathcal{N}\}$ справедливо неравенство

$$D_f(P \,\|\, Q) \geqslant d_f(p_i \,\|\, q_i) \quad \text{для любых } i \in \mathcal{N}, \tag{38}$$

где $d_f(\cdot \,\|\, \cdot)$ определено в (4). Действительно, пользуясь свойством выпуклости функции $f(t)$, имеем

$$\begin{aligned} D_f(P \,\|\, Q) &= q_i f\left(\frac{p_i}{q_i}\right) + \sum_{j:\, j \neq i} q_j f\left(\frac{p_j}{q_j}\right) = \\ &= q_i f\left(\frac{p_i}{q_i}\right) + (1 - q_i) \sum_{j:\, j \neq i} \frac{q_j}{1 - q_i} f\left(\frac{p_j}{q_j}\right) \geqslant \\ &\geqslant q_i f\left(\frac{p_i}{q_i}\right) + (1 - q_i) f\left(\sum_{j:\, j \neq i} \frac{p_j}{1 - q_i}\right) = d_f(p_i \,\|\, q_i). \end{aligned}$$

Предположим теперь, что $Q = \{q_i,\ i \in \mathcal{N}\}$ – некоторое распределение вероятностей, для которого при заданном α, $0 \leqslant \alpha \leqslant 2p_{\max} - 1$, существует его α-склеивание с

распределением $P = \{p_i,\ i \in \mathcal{N}\}$, у которого, для определенности, $p_{\max} = p_1$. Пусть также матрица $M = \|p_{ij}\|_{i,j=1}^n$ задает совместное распределение, осуществляющее это α-склеивание P и Q, т.е. $\sum\limits_{j=1}^n p_{ij} = p_i$ для всех $i \in \mathcal{N}$, $\sum\limits_{i=1}^n p_{ij} = q_j$ для всех $j \in \mathcal{N}$ и $\sum\limits_{i=1}^n p_{ii} = \alpha$. Тогда, воспользовавшись неравенством (38), получаем

$$D_f(P \,\|\, Q) \geqslant d_f(p_1 \,\|\, q_1) \geqslant d_f(p_{\max} \,\|\, 1 - p_{\max} + \alpha). \tag{39}$$

Второе неравенство в (39) следует из того, что функция $d_f(p_1 \,\|\, q_1)$ убывает по q_1 при $q_1 \leqslant p_1$, а в нашем случае $q_1 \leqslant \alpha + 1 - p_1 \leqslant p_1$, так как

$$q_1 \leqslant p_{11} + \sum_{i=2}^n p_i \leqslant \alpha + 1 - p_1 \leqslant p_1,$$

поскольку $0 \leqslant \alpha \leqslant 2p_1 - 1$.

Поэтому для доказательства второго равенства в (5) достаточно найти распределение вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$, для которого существует его α-склеивание (при $0 \leqslant \alpha \leqslant 2p_{\max} - 1$) с заданным распределением $P = \{p_i,\ i \in \mathcal{N}\}$, и такое что

$$D_f(P \,\|\, Q) = d_f(p_{\max} \,\|\, 1 - p_{\max} + \alpha).$$

Действительно, легко убедиться, что такое распределение $Q = \{q_i,\ i \in \mathcal{N}\}$ является маргинальным для совместного распределения P и Q, осуществляющего их α-склеивание и задаваемого матрицей $M = \|p_{ij}\|_{i,j=1}^n$ с компонентами

$$p_{ij} = \begin{cases} \alpha & \text{при } i = j = 1, \\ cp_j & \text{при } i = 1 \text{ и } j \in \mathcal{N} \setminus \{1\}, \\ p_i & \text{при } i \in \mathcal{N} \setminus \{1\} \text{ и } j = 1, \\ 0 & \text{в остальных случаях,} \end{cases}$$

где параметр $c = \dfrac{p_1 - \alpha}{1 - p_1}$. ▲

Доказательство теоремы 2. Прежде всего заметим, что в рассматриваемом случае, когда задано распределение вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$ и предполагается, что $\min\limits_i p_i = p_n > 0$, то из определения (1) следует, что для любого распределения $Q = \{q_i,\ i \in \mathcal{N}\}$, которое имеет хотя бы одно $q_i = 0$, справедливо равенство

$$D_f(P \,\|\, Q) = \sum_{i:\, q_i > 0} q_i f\left(\frac{p_i}{q_i}\right) + f^* \sum_{i:\, q_i = 0} p_i, \tag{40}$$

где $f^* = \lim\limits_{t \to \infty} \dfrac{f(t)}{t}$. Поэтому, если существует матрица $M = \|p_{ij}\|_{i,j=1}^n$, осуществляющая α-склеивание распределения P с некоторым распределением Q, у которой имеется столбец, целиком состоящий из нулей (т.е. некоторое $q_i = 0$), а $f^* = \infty$, то в этом случае $D_f^{\max}(P, \alpha) = \infty$. Очевидно, что такая матрица всегда существует, если $\alpha \leqslant 1 - p_n$, т.е. в этом случае справедливо первое равенство в (11). Поэтому в дальнейшем при доказательстве теоремы 1 всегда будет предполагаться, что либо $f^* < \infty$, либо, если $f^* = \infty$, то $\alpha > 1 - p_n$.

Для доказательства формулы (10) нужно показать, что существует *оптимальная матрица* $M = \|p_{ij}\|_{i,j=1}^n$ (т.е. матрица, для которой $D_f(M) = D_f^{\max}(P, \alpha)$), осуществляющая α-склеивание заданного распределения вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$

с некоторым распределением $Q = \{q_i,\ i \in \mathcal{N}\}$ и принадлежащая множеству $\mathcal{M}(P, I)$ для некоторого допустимого (P, I)-представления заданного числа α.

В дальнейшем, для краткости, когда речь идет о некоторой матрице, будем всегда считать, что эта матрица осуществляет α-склеивание заданного распределения вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$ с некоторым распределением $Q = \{q_i,\ i \in \mathcal{N}\}$. Докажем вначале, что существует оптимальная матрица, у которой все ненулевые элементы (за исключением, возможно, лишь одного) расположены в некотором (главном) столбце и на (главной) диагонали.

Пусть k-й столбец матрицы $M = \|p_{ij}\|_{i,j=1}^{n}$ таков, что $\dfrac{q_k}{p_k} = \max\limits_{i \in \mathcal{N}} \dfrac{q_i}{p_i}$. Покажем, что $D_f(M)$ можно увеличить, если к каждому элементу (кроме диагонального) этого k-го столбца прибавить все элементы соответствующей строки, кроме диагонального. Действительно, для этого достаточно доказать, что $D_f(M(x)) > D_f(M)$, где $M(x) = \|p_{ij}(x)\|_{i,j=1}^{n}$ – матрица с элементами

$$p_{ij}(x) = \begin{cases} p_{\ell\,k} + x & \text{при } i = \ell \text{ и } j = k, \\ p_{\ell\,m} - x & \text{при } i = \ell \text{ и } j = m, \\ p_{ij} & \text{в остальных случаях,} \end{cases}$$

где $0 < x \leqslant p_{\ell\,m}$, а ℓ и m – любые индексы, такие что $\ell \neq m$, $\ell \neq k$ и $m \neq k$. Имеем

$$[D_f(M(x)]'_x = [f(u) - uf'(u)] - [f(v) - vf'(v)],$$

где

$$u = \frac{p_k}{q_k + x}, \quad v = \frac{p_m}{q_m - x}.$$

Замечая теперь, что $u < v$, так как $x > 0$, а $\dfrac{p_k}{q_k} \leqslant \dfrac{p_m}{q_m}$ по условию, мы видим, что $f(u) - uf'(u)$ убывает по u (так как $f(\cdot)$ – выпуклая функция), а поэтому $D_f(M(x))$ возрастает по x, и значит, $D_f(M(x)) > D_f(M(0)) = D_f(M)$.

Аналогично доказывается, что $D_f(M)$ можно увеличить, если все элементы k-й строки (когда $\dfrac{q_k}{p_k} = \max\limits_{i \in \mathcal{N}} \dfrac{q_i}{p_i}$), кроме диагонального, прибавить к одному из них. Очевидно, что без ограничения общности всегда можно считать, что если k-й столбец матрицы $M = \|p_{ij}\|_{i,j=1}^{n}$ является главным, то $\dfrac{q_k}{p_k} = \max\limits_{i \in \mathcal{N}} \dfrac{q_i}{p_i}$.

Чтобы доказать, что существует оптимальная матрица, принадлежащая некоторому множеству $\mathcal{M}(P, I)$, остается лишь показать, что существует оптимальная матрица, у которой на диагонали стоят некоторые числа p_i, $i \in \mathcal{N}$, а также, возможно, одно число β, $0 < \beta < p_j$, для некоторого $j \in \mathcal{N}$, и нули (последнее возможно, лишь если $\alpha \leqslant 1 - p_n$). Для этого достаточно доказать, что любая матрица, у которой на диагонали стоят по крайней мере два элемента, отличные от нуля и некоторых p_i, $i \in \mathcal{N}$, не может быть оптимальной.

Действительно, пусть $M = \|p_{ij}\|_{i,j=1}^{n}$ – некоторая матрица, у которой на диагонали стоят два элемента $p_{\ell\ell}$ и p_{mm}, $\ell \neq m$, такие что $0 < p_{\ell\ell} < p_\ell$ и $0 < p_{mm} < p_m$. Покажем, что в этом случае существует другая матрица $M(x)$, такая что $D_f(M(x)) > D_f(M)$. Для этого необходимо рассмотреть два различных случая: когда ни $p_{\ell\ell}$, ни p_{mm} не принадлежат главному столбцу матрицы M и когда либо $p_{\ell\ell}$, либо p_{mm} принадлежат ему. Оба случая анализируются вполне аналогично. Поэтому рассмотрим, например, первый из них, когда в матрице M главным столбцом является k-й, а $\ell \neq k$ и $m \neq k$. Пусть для определенности $\dfrac{q_\ell}{p_\ell} \geqslant \dfrac{q_m}{p_m}$. В этом случае рассмотрим

матрицу $M(x) = \|p_{ij}(x)\|_{i,j=1}^n$ с элементами

$$p_{ij}(x) = \begin{cases} p_{\ell\ell} + x & \text{при } i = j = \ell, \\ p_{mm} - x & \text{при } i = j = m, \\ p_{\ell k} - x & \text{при } i = \ell \text{ и } j = k, \\ p_{mk} + x & \text{при } i = m \text{ и } j = k, \\ p_{ij} & \text{в остальных случаях,} \end{cases}$$

где $x > 0$ достаточно мало. Тогда, очевидно, имеем

$$\frac{q_\ell(x)}{p_\ell(x)} = \frac{q_\ell + x}{p_\ell} > \frac{q_m(x)}{p_m(x)} = \frac{q_m - x}{p_m} \quad \text{и} \quad \frac{q_i(x)}{p_i(x)} = \frac{q_i}{p_i} \quad \text{для всех } i \neq \ell \text{ и } i \neq m.$$

Поэтому, как мы видели выше, $D_f(M(x))$ возрастает по x, и значит, $D_f(M(x)) > > D_f(M)$. Таким образом, мы доказали, что существует оптимальная матрица, принадлежащая множеству $\mathcal{M}(P, I)$ при некотором допустимом (P, I)-представлении числа α. Отсюда сразу следует справедливость формулы (10).

Для доказательства второго из равенств в (11) заметим, что в данном случае предполагается, что компоненты p_i распределения $P = \{p_i,\ i \in \mathcal{N}\}$ упорядочены по убыванию и $\alpha > 1 - p_n$. Поэтому из формулы (10) сразу следует, что оптимальную матрицу следует искать среди матриц $M = \|p_{ij}\|_{i,j=1}^n$, у которых на диагонали стоят числа p_i, $i \in \mathcal{N} \setminus \{k\}$, и $p_k - (1 - \alpha)$ при некотором k, вне диагонали в некотором j-м $(j \neq k)$ столбце стоит число $1 - \alpha$, а все остальные элементы матрицы равны нулю. Для такой матрицы

$$D_f(M) = (p_k + \alpha - 1) f\left(\frac{p_k}{p_k + \alpha - 1}\right) + (1 - \alpha + p_j) f\left(\frac{p_j}{1 - \alpha + p_j}\right).$$

Замечая теперь, что, как нетрудно убедиться, функции

$$(p_k + \alpha - 1) f\left(\frac{p_k}{p_k + \alpha - 1}\right) \quad \text{и} \quad (1 - \alpha + p_j) f\left(\frac{p_j}{1 - \alpha + p_j}\right)$$

убывают по p_k и p_j соответственно (здесь существенно, что в соответствии с определением f-дивергенции выпуклая функция $f(\cdot)$ такова, что $f(1) = 0$), мы видим, что для максимума $D_f(M)$ среди подобных матриц M, т.е. для $D_f^{\max}(P, \alpha)$, справедливо второе из равенств (11), где K_P определено в (12). ▲

Отметим, что хотя в общем случае нельзя сказать, какое из двух выражений в определении K_P является максимальным, однако во многих частных случаях f-дивергенции это можно сделать. В частности, это удается сделать для дивергенции Кульбака – Лейблера и χ^2-дивергенции (см. доказательства теорем 4 и 5 ниже).

Доказательство теоремы 3. Прежде всего заметим, что в рассматриваемом случае, когда задано распределение вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$ и предполагается, что $\min\limits_i q_i = q_n > 0$, то вместо (40) из определения (1) следует, что для любого распределения $P = \{p_i,\ i \in \mathcal{N}\}$, которое имеет хотя бы одно $p_i = 0$, имеет место равенство

$$D_f(P \,\|\, Q) = \sum_{i:\, p_i > 0} q_i f\left(\frac{p_i}{q_i}\right) + f(0) \sum_{i:\, p_i = 0} q_i, \tag{41}$$

а тогда снова очевидно (как и при доказательстве теоремы 2), что справедливо первое из равенств в (14). Дальнейшее доказательство этой теоремы вполне аналогично приведенному выше доказательству теоремы 2 и поэтому здесь не приводится. ▲

Доказательство теоремы 4. **1.** Докажем вначале равенство (20). Так как дивергенция Кульбака – Лейблера $D(P\,\|\,Q)$ является f-дивергенцией при $f(t) = t\log t$, то равенство (20) является следствием соотношения (11), поскольку в данном случае $f^* = \infty$, а величина K_P (см. (12)), как нетрудно убедиться, равна

$$p_n \log \frac{p_n}{p_n - 1 + \alpha} + p_{n-1} \log \frac{p_{n-1}}{p_{n-1} + 1 - \alpha}.$$

Действительно, для этого следует лишь заметить, что разность первого и второго выражений в (12) при $f(t) = t\log t$ убывает по α, а при $\alpha = 1$ она равна нулю.

2. Докажем теперь равенства (21) и (22). Из общей формулы (13) теоремы 3 следует, что в случае, когда $\alpha \leqslant q_n$, существует оптимальная матрица (осуществляющая α-склеивание заданного распределения вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$ с некоторым распределением $P = \{p_i,\ i \in \mathcal{N}\}$), находящаяся среди матриц

$$M_1(k,\ell) = \left\|p_{ij}^{(1)}\right\|_{i,j=1}^{n}, \quad M_2(k,\ell) = \left\|p_{ij}^{(2)}\right\|_{i,j=1}^{n}, \quad M_3(k,\ell,m) = \left\|p_{ij}^{(3)}\right\|_{i,j=1}^{n}$$

(где k, ℓ и m – всевозможные различные между собой числа, принадлежащие множеству $\mathcal{N}$) с элементами

$$p_{ij}^{(1)} = \begin{cases} \alpha & \text{при } i = j = k, \\ q_i & \text{при } i \in \mathcal{N} \setminus \{k\} \text{ и } j = k, \\ q_k - \alpha & \text{при } i = k \text{ и } j = \ell, \\ 0 & \text{в остальных случаях,} \end{cases} \tag{42}$$

$$p_{ij}^{(2)} = \begin{cases} q_i & \text{при } i \in \mathcal{N} \setminus \{k,\ell\} \text{ и } j = k, \\ q_\ell - \alpha & \text{при } i = \ell \text{ и } j = k, \\ q_k & \text{при } i = k \text{ и } j = \ell, \\ \alpha & \text{при } i = j = \ell, \\ 0 & \text{в остальных случаях,} \end{cases} \tag{43}$$

$$p_{ij}^{(3)} = \begin{cases} q_i & \text{при } i \in \mathcal{N} \setminus \{k,m\} \text{ и } j = k, \\ q_m - \alpha & \text{при } i = m \text{ и } j = k, \\ q_k & \text{при } i = k \text{ и } j = \ell, \\ \alpha & \text{при } i = j = m, \\ 0 & \text{в остальных случаях.} \end{cases} \tag{44}$$

Заметим, что в каждой из этих матриц k-й столбец является главным. Таким образом, имеем

$$D^{\max}(Q,\alpha) = \max_{k,\ell,m}\{D(M_1(k,\ell)), D(M_2(k,\ell)), D(M_3(k,\ell,m))\},$$

где

$$D(M_1(k,\ell)) = (1 + \alpha - q_k)\log\frac{1+\alpha-q_k}{q_k} + (q_k - \alpha)\log\frac{q_k-\alpha}{q_\ell},$$

$$D(M_2(k,\ell)) = (1 - \alpha - q_k)\log\frac{1-\alpha-q_k}{q_k} + (q_k + \alpha)\log\frac{q_k+\alpha}{q_\ell},$$

$$D(M_3(k,\ell,m)) = (1 - \alpha - q_k)\log\frac{1-\alpha-q_k}{q_k} + q_k\log\frac{q_k}{q_\ell} + \alpha\log\frac{\alpha}{q_m}.$$

Очевидно, что

$$\max_{k,\ell,m} D(M_3(k,\ell,m)) \leqslant \max_{k,\ell} D(M_2(k,\ell)),$$

и поскольку $D(M_1(k,\ell))$ и $D(M_2(k,\ell))$ убывают по q_ℓ и являются выпуклыми функциями от q_k, то

$$D^{\max}(Q,\alpha) = \max\{D(M_i(n-1,n)), D(M_i(1,n)), D(M_i(n,n-1)),\ i=1,2\}.$$

Легко видеть, что

$$D(M_1(1,n)) \leqslant \max\{D(M_1(n-1,n)), D(M_2(n,n-1))\},$$
$$D(M_2(1,n)) \leqslant \max\{D(M_2(n-1,n)), D(M_1(n,n-1))\},$$

а поэтому для доказательства равенства (21) (правая часть которого совпадает с выражением для $D(M_1(n,n-1))$) необходимо доказать, что каждая из трех величин $D(M_1(n-1,n))$, $D(M_2(n-1,n))$ и $D(M_2(n,n-1))$ не превосходит $D(M_1(n,n-1))$.

Неравенство $D(M_1(n,n-1)) \geqslant D(M_1(n-1,n))$ является следствием того, что разность $D(M_1(n,n-1)) - D(M_1(n-1,n))$, как легко проверить, возрастает по α, а при $\alpha = 0$ она положительна. Действительно, нетрудно убедиться, что эта последняя разность $[D(M_1(n,n-1)) - D(M_1(n-1,n))]\big|_{\alpha=0}$ является убывающей функцией q_n, а при максимальном значении q_n, равном q_{n-1}, она равна нулю.

Доказательство двух оставшихся неравенств $D(M_1(n,n-1)) \geqslant D(M_2(n-1,n))$ и $D(M_1(n,n-1)) \geqslant D(M_2(n,n-1))$ проводится вполне аналогично. Таким образом, равенство (21) доказано.

Справедливость равенства (22) легко следует из соотношения (14) теоремы 3, так как в рассматриваемом случае, когда $f(t) = t\log t$, величина K_Q (см. (15)) равна

$$(q_n - 1 + \alpha)\log\frac{q_n - 1 + \alpha}{q_n} + (1 - \alpha + q_{n-1})\log\frac{1-\alpha+q_{n-1}}{q_{n-1}}.$$

Действительно, нетрудно убедиться, что разность первого и второго выражений в (15) убывает по α, а при $\alpha = 1$ она равна нулю.

3. Докажем теперь верхнюю границу (23). Для этого необходимо рассмотреть три типа матриц $M = \|p_{ij}\|_{i,j=1}^n$, принадлежащих одному из множеств $\mathcal{M}(Q,I)$, когда:

а) в главном столбце матрицы на диагонали стоит некоторое q_k, $k \in I$, входящее в одно из допустимых (Q,I)-представлений α в виде $\alpha = \sum\limits_{i\in I} q_i + \beta$;

б) в главном столбце матрицы на диагонали стоит ноль;

в) в главном столбце матрицы на диагонали стоит число β, входящее в одно из допустимых (Q,I)-представлений α в виде $\alpha = \sum\limits_{i\in I} q_i + \beta$.

Согласно общей формуле (13) среди таких матриц находится оптимальная, и нам надо показать, что для всех таких матриц M справедлива верхняя граница

$$D(M) \leqslant (1 - \alpha + q_n)\log\frac{1-\alpha+q_n}{q_n}$$

при всех α, $q_n \leqslant \alpha \leqslant 1 - q_n$. Рассмотрим вкратце доказательства этой границы для каждого из этих трех типов матриц.

а) Если в главном столбце матрицы на диагонали стоит некоторое q_k, $k \in I$, входящее в одно из допустимых (Q,I)-представлений α в виде $\alpha = \sum\limits_{i\in I} q_i + \beta$, а β стоит на диагонали в j-м столбце, то для такой матрицы

$$D(M) = (1-\alpha+q_k)\log\frac{1-\alpha+q_k}{q_k} + \beta\log\frac{\beta}{q_j} \leqslant (1-\alpha+q_n)\log\frac{1-\alpha+q_n}{q_n}. \qquad (45)$$

Действительно, неравенство в этом соотношении следует из того, что функция

$$(1-\alpha+q_k)\log\frac{1-\alpha+q_k}{q_k}$$

убывает по q_k, а $\beta \log \dfrac{\beta}{q_j} \leqslant 0$, так как $0 \leqslant \beta < q_j$ по условию (Q,I)-допустимого представления α. Заметим сразу, что в (45) вместо неравенства справедливо равенство (а значит, и равенство в формуле (23)), если $k = n$ и $\beta = 0$, т.е. если существует (Q,I)-представление α вида $\alpha = q_n + \sum\limits_{i=1}^{n-1} a_i q_i$ при некоторых $a_i \in \{0,1\}$.

б) Если в главном (k-м) столбце матрицы M на диагонали стоит ноль, а число β, входящее в одно из допустимых (Q,I)-представлений α, стоит на диагонали в j-м столбце, то нетрудно видеть, что при любом расположении элемента q_k в матрице M величину $D(M)$ можно оценить сверху следующим образом:

$$D(M) \leqslant \max_{(k,j)\colon k \neq j} \left\{ (1-\alpha-q_k) \log \frac{1-\alpha-q_k}{q_k} + (q_k+q_j) \log \frac{q_k+q_j}{q_j} \right\}. \tag{46}$$

Полагая

$$g(\alpha, q_k, q_j) = (1-\alpha-q_k) \log \frac{1-\alpha-q_k}{q_k} + (q_k+q_j) \log \frac{q_k+q_j}{q_j},$$

заметим, что разность

$$(1-\alpha+q_n) \log \frac{1-\alpha+q_n}{q_n} - g(\alpha, q_k, q_j)$$

является убывающей функцией α при любых q_k и q_j, а при максимальном значении α (если фиксировано любое q_k), равном $1-q_k$, имеем

$$\left[(1-\alpha+q_n) \log \frac{1-\alpha+q_n}{q_n} - g(\alpha, q_k, q_j) \right] \Bigg|_{\alpha = 1-q_k} =$$
$$= (q_n+q_k) \log \frac{q_n+q_k}{q_n} - (q_j+q_k) \log \frac{q_j+q_k}{q_j} \geqslant 0,$$

так как $(q_j+q_k) \log \dfrac{q_j+q_k}{q_j}$ является убывающей функцией q_j. Поэтому из (46) следует, что для рассматриваемого класса матриц M (у которых в главном столбце на диагонали стоит ноль) также справедливо доказываемое неравенство

$$D(M) \leqslant (1-\alpha+q_n) \log \frac{1-\alpha+q_n}{q_n}.$$

в) Наконец, если в главном (k-м) столбце матрицы M на диагонали стоит число β, входящее в одно из допустимых (Q,I)-представлений α, то снова нетрудно видеть, что при любом расположении элемента $q_k - \beta$ в матрице M величину $D(M)$ можно оценить сверху следующим образом:

$$D(M) \leqslant \max_{(k,j)\colon k \neq j} \left\{ (1-\alpha-q_k+2\beta) \log \frac{1-\alpha-q_k+2\beta}{q_k} + \right.$$
$$\left. + (q_k+q_j-\beta) \log \frac{q_k+q_j-\beta}{q_j} \right\}. \tag{47}$$

Замечая теперь, что максимизируемая в правой части (47) функция является выпуклой относительно β, приходим к выводу, что максимум правой части (47) достигается либо при $\beta = 0$, либо при $\beta = q_k$, что сводит задачу к рассмотренным выше случаям а) и б). На этом доказательство верхней границы (23) заканчивается. ▲

Доказательство теоремы 5. **1.** Равенство (30) и второе из равенств в (31) (где $\alpha \geqslant 1 - q_n$) являются прямыми следствиями формул (11), (12) и (14), (15) для рассматриваемого случая $f(t) = (t-1)^2$.

2. Доказательство первого из равенств в (31) (где $\alpha \leqslant q_n$) в основном следует схеме доказательства формулы (21) теоремы 4, и поэтому мы опишем его лишь вкратце.

Оптимальную матрицу, осуществляющую α-склеивание заданного распределения вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$ с некоторым распределением $P = \{p_i,\ i \in \mathcal{N}\}$, снова следует искать среди матриц

$$M_1(k,\ell) = \left\|p_{ij}^{(1)}\right\|_{i,j=1}^{n}, \quad M_2(k,\ell) = \left\|p_{ij}^{(2)}\right\|_{i,j=1}^{n}, \quad M_3(k,\ell,m) = \left\|p_{ij}^{(3)}\right\|_{i,j=1}^{n}$$

с элементами, заданными равенствами (42)–(44), которые определяют χ^2-дивергенции следующих трех типов:

$$\chi^2(M_1(k,\ell)) = \frac{(1+\alpha-q_k)^2}{q_k} + \frac{(q_k-\alpha)^2}{q_\ell} - 1,$$
$$\chi^2(M_2(k,\ell)) = \frac{(1-\alpha-q_k)^2}{q_k} + \frac{(q_k+\alpha)^2}{q_\ell} - 1,$$
$$\chi^2(M_3(k,\ell,m)) = \frac{(1-\alpha-q_k)^2}{q_k} + \frac{q_k^2}{q_\ell} + \frac{\alpha^2}{q_m} - 1,$$

где k, ℓ и m – всевозможные различные между собой числа, принадлежащие множеству $\mathcal{N}$. Так как очевидно, что

$$\max_{k,\ell,m} \chi^2(M_3(k,\ell,m)) \leqslant \max_{k,\ell} \chi^2(M_2(k,\ell)),$$

а $\chi^2(M_1(k,\ell))$ и $\chi^2(M_2(k,\ell))$ являются выпуклыми функциями относительно q_k и убывающими относительно q_ℓ, то рассуждения, приведенные при доказательстве в пункте 2 теоремы 4, здесь полностью сохраняются (с соответствующей заменой величин $D(M_i(\cdot\,,\cdot))$ на $\chi^2(M_i(\cdot\,,\cdot))$) и показывают, что в рассматриваемом случае $\alpha \leqslant q_n$ имеем

$$\chi^2_{\max}(Q,\alpha) = \max\bigl\{\chi^2(M_i(n,n-1)), \chi^2(M_i(n-1,n)),\ i=1,2\bigr\} =$$
$$= \chi^2(M_1(n,n-1)),$$

что и доказывает первое из равенств в (31).

3. Доказательство верхней границы (32) также в основном следует схеме доказательства верхней границы (23) в теореме 4. Снова нам необходимо доказать, что для трех типов матриц $M = \|p_{ij}\|_{i,j=1}^{n}$, принадлежащих одному из множеств $\mathcal{M}(Q,I)$ и введенных в пункте 3 доказательства теоремы 4, справедлива верхняя граница (32), т.е. для всех таких матриц M справедливо неравенство

$$\chi^2(M) \leqslant \frac{(1-\alpha)^2}{q_n} + 1 - \alpha,$$

если $q_n \leqslant \alpha \leqslant 1 - q_n$. Докажем это утверждение.

а) Если в главном столбце матрицы M на диагонали стоит некоторое q_k, $k \in I$, входящее в одно из допустимых (Q,I)-представлений α в виде $\alpha = \sum\limits_{i\in I} q_i + \beta$, а β стоит

на диагонали в j-м столбце, то для такой матрицы

$$\chi^2(M) = \sum_{i=1}^{n} \frac{p_i^2}{q_i} - 1 = \frac{(1-\alpha+q_k)^2}{q_k} + \frac{\beta^2}{q_j} + \sum_{i:\, p_i=q_i} q_i - 1 =$$
$$= \frac{(1-\alpha)^2}{q_k} + 1 - \alpha + \frac{\beta^2}{q_j} - \beta \leqslant \frac{(1-\alpha)^2}{q_n} + 1 - \alpha,$$

так как $0 \leqslant \beta < q_j$ по условию (Q, I)-допустимого представления α. Снова замечаем, что вместо вышеприведенного неравенства имеет место равенство, если $\beta = 0$ и $k = n$, т.е. если существует (Q, I)-представление α вида $\alpha = q_n + \sum\limits_{i=1}^{n-1} a_i q_i$ при любых $a_i \in \{0, 1\}$.

б) Если в главном (k-м) столбце матрицы M на диагонали стоит ноль, а число β, входящее в одно из допустимых (Q, I)-представлений α, стоит на диагонали в j-м столбце, то нетрудно видеть, что при любом расположении элемента q_k в матрице M величину $\chi^2(M)$ можно оценить сверху следующим образом:

$$\chi^2(M) \leqslant \max_{(k,j):\, k \neq j} \left\{ \frac{(1-\alpha)^2}{q_k} + \frac{q_k^2}{q_j} - 3(1-\alpha-q_k) \right\} \leqslant \frac{(1-\alpha)^2}{q_n} + 1 - \alpha. \tag{48}$$

Действительно, справедливость второго неравенства в (48) следует из того, что разность

$$\frac{(1-\alpha)^2}{q_n} + 1 - \alpha - \frac{(1-\alpha)^2}{q_k} - \frac{q_k^2}{q_j} + 3(1-\alpha-q_k),$$

как легко убедиться, является убывающей функцией α при любых q_k и q_j, а при максимальном значении $\alpha = 1 - q_k$ (так как на диагонали в главном k-м столбце матрицы стоит ноль) эта разность неотрицательна.

в) Если в главном (k-м) столбце матрицы M на диагонали стоит число β, входящее в одно из допустимых (Q, I)-представлений α, то снова нетрудно видеть, что при любом расположении элемента $q_k - \beta$ в матрице M величину $\chi^2(M)$ можно оценить сверху следующим образом:

$$\chi^2(M) \leqslant \max_{(k,j):\, k \neq j} \left\{ \frac{(1-\alpha-q_k+2\beta)^2}{q_k} + \frac{(q_k+q_j-\beta)^2}{q_j} + \alpha - \beta - q_j - 1 \right\}. \tag{49}$$

Поскольку максимизируемая в правой части (49) функция является выпуклой относительно β, то максимум правой части (49) достигается либо при $\beta = 0$, либо при $\beta = q_k$, что, как нетрудно убедиться, сводит задачу к рассмотренным выше случаям а) и б). ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Csiszár I.* Information-type Measures of Difference of Probability Distributions and Indirect Observations // Studia Sci. Math. Hungar. 1967. V. 2. P. 299–318.
2. *Ali S.M., Silvey S.D.* A General Class of Coefficients of Divergence of One Distribution from Another // J. Roy. Statist. Soc. Ser. B. 1966. V. 28. № 1. P. 131–142. https://www.jstor.org/stable/2984279
3. *Sason I., Verdú S.* f-Divergence Inequalities // IEEE Trans. Inform. Theory. 2016. V. 62. № 11. P. 5973–6006. https://doi.org/10.1109/TIT.2016.2603151
4. *Макур А., Чжен Л.* Сравнение коэффициентов сжатия для f-дивергенций // Пробл. передачи информ. 2020. Т. 56. № 2. С. 3–62. https://doi.org/10.1134/S0134347520020011

5. *Прелов В.В.* О склеивании вероятностных распределений и оценивании дивергенции через вариацию // Пробл. передачи информ. 2017. Т. 53. № 3. С. 16–22. http://mi.mathnet.ru/ppi2239
6. *Прелов В.В.* О некоторых оптимизационных задачах для дивергенции Реньи // Пробл. передачи информ. 2018. Т. 54. № 3. С. 36–53. http://mi.mathnet.ru/ppi2271
7. *Gilardoni G.L.* On the Minimum f-Divergence for Given Total Variation // C. R. Math. Acad. Sci. Paris. 2006. V. 343. № 11–12. P. 763–766. https://doi.org/10.1016/j.crma.2006.10.027
8. *Gilardoni G.L.* On Pinsker's and Vajda's Type Inequalities for Csiszár's f-Divergences // IEEE Trans. Inform. Theory. 2010. V. 56. № 11. P. 5377–5386. https://doi.org/10.1109/TIT.2010.2068710
9. *Прелов В.В.* О максимальных значениях f-дивергенции и дивергенции Реньи при заданном вариационном расстоянии // Пробл. передачи информ. 2020. Т. 56. № 1. С. 3–15. https://doi.org/10.1134/S0134347520010015

Прелов Вячеслав Валерьевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
prelov@iitp.ru

Поступила в редакцию
17.11.2020
После доработки
04.01.2021
Принята к публикации
11.01.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 1**

УДК 621.391 : 519.725

© 2021 г. **В.А. Зиновьев, Д.В. Зиновьев**

ОБ ОБОБЩЕННОЙ КАСКАДНОЙ КОНСТРУКЦИИ КОДОВ В МОДУЛЬНОЙ МЕТРИКЕ И МЕТРИКЕ ЛИ[1,2]

Рассмотрена обобщенная каскадная конструкция кодов над q-ичным алфавитом в модульной метрике L_1 и метрике Ли L. Результирующие коды имеют произвольную длину, произвольное расстояние (независимо от размера алфавита) и могут исправлять как независимые ошибки, так и пакеты ошибок в обеих метриках. В частности, для любой длины 2^m построены коды над $\mathbb{Z}_4$ с расстоянием Ли, равным 4, которые при отображении Грея приводят к расширенным двоичным совершенным кодам длины 2^{m+1} (с кодовым расстоянием 4). Построены коды над $\mathbb{Z}_4$ длины n с расстоянием Ли, равным n, которые при отображении Грея приводят к матрицам Адамара порядка $2n$ (при дополнительном условии, что существует матрица Адамара порядка n). Построенные новые коды в метрике Ли часто лучше по своим параметрам, чем ранее известные коды, в частности, значительно лучше, чем ранее построенные коды Астолы.

Ключевые слова: блоковый корректирующий код, корректирующий код в метрике Ли, корректирующий код в модульной метрике, обобщенная каскадная конструкция, корректирующий код над $\mathbb{Z}_4$.

DOI: 10.31857/S0555292321010046

§ 1. Введение

Пусть $E = \{0, 1, \ldots, q-1\}$. Блоковым q-ичным кодом C называется любое подмножество множества E^n. Будем называть такой код $(n, N, d)_q$-кодом, где n – *длина* кода, N – число кодовых слов, т.е. *мощность* кода C, а d – *минимальное расстояние Хэмминга*

$$d = d(C) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \neq \boldsymbol{y},\ \boldsymbol{x}, \boldsymbol{y} \in C\},$$

где для $\boldsymbol{x} = (x_1, \ldots, x_n)$ и $\boldsymbol{y} = (y_1, \ldots, y_n)$ из E^n

$$d(\boldsymbol{x}, \boldsymbol{y}) = |\{j : x_j \neq y_j,\ j = 1, \ldots, n\}|.$$

Для случая, когда q – степень простого числа, а q-ичный $(n, N = q^k, d)_q$-код C является линейным пространством размерности k над $\mathbb{F}_q$, используется стандартное обозначение $[n, k, d]_q$. В случае $q = 2$ символ q в обозначениях $(n, N, d)_q$ и $[n, k, d]_q$ опускается.

Расстоянием Ли $d_L(i, j)$ между символами i и j из E мы называем минимальную разность между этими символами:

$$d_L(i, j) = \min\{|j - i|, q - |j - i|\}.$$

[1] Исследование выполнено в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364).

[2] Результаты статьи были доложены на конференции ACCT'2018 и опубликованы в ее трудах [1].

Это расстояние симметрично, т.е. $d_L(i,j) = d_L(j,i)$, и продолжается на векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ из E^n стандартным образом:

$$d_L(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n} d_L(x_i, y_i).$$

Нам понадобится еще одно расстояние, а именно *модульное расстояние* d_{L_1}, равное для символов x_i и x_j из E модулю разности между этими элементами: $d_{L_1}(x_i, x_j) = |x_i - x_j|$, и доопределяемое на векторы над E аналогичным образом:

$$d_{L_1}(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n} d_{L_1}(x_i, y_i).$$

Коды, исправляющие ошибки, для обеих метрик являются важным случаем корректирующих кодов и имеют применения в системах связи и системах хранения информации (см., например, работы [2–8] и библиографию в них).

Цель настоящей работы – описать обобщенную каскадную конструкцию для кодов в метриках L и L_1. Этот подход позволяет построить широкий класс кодов с хорошей корректирующей способностью (с точки зрения таких существующих кодов) для исправления как независимых ошибок, так и пакетов ошибок. Метод построения кодов основан на хорошо известном обобщенном каскадном методе построения корректирующих кодов для евклидовой метрики [9] и метрики Хэмминга [10], который мы применили для метрик L и L_1. Для случая $q = 4$ наша конструкция дает коды над $\mathbb{Z}_4$ произвольной длины и с произвольным расстоянием, которые часто лучше, чем известные коды. В частности, для длины $n = 2^m$ мы получаем коды с расстоянием Ли $d_L = 4$, так что преобразование Грея приводит к двоичным расширенным совершенным кодам длины $2n$ с кодовым расстоянием (уже в хэмминговой метрике), равным 4. Таким образом, мы получаем, что каждый двоичный расширенный совершенный код длины $n = 2^m$ индуцирует $\mathbb{Z}_4$-код той же длины n с расстоянием Ли $d_L = 4$, который дает (при преобразовании Грея) двоичный расширенный совершенный код длины $2n$. Тем самым мы получаем дважды экспоненциальное число взаимно не эквивалентных расширенных двоичных совершенных кодов с $d = 4$, имеющих $\mathbb{Z}_4$-представление. Эта же конструкция дает коды над $\mathbb{Z}_4$ с расстоянием Ли, равным n, которые при отображении Грея приводят к (двоичным) матрицам Адамара порядка $2n$, имеющих $\mathbb{Z}_4$-представление (при дополнительном условии, что существует матрица Адамара порядка n). Как показывают сравнения построенных кодов с уже существующими кодами конечной длины, новые коды в метрике Ли лучше по своим параметрам, чем ранее известные коды.

Статья организована следующим образом. Построение кодов рассмотрено в § 2. Комбинаторные свойства таких кодов приведены в § 3. Следующий § 4 посвящен важному частному случаю кодов, а именно $\mathbb{Z}_4$-кодам. В § 5 рассмотрены коды над $\mathbb{Z}_q$, где $q = p^s$, с фиксированным расстоянием, а § 6 посвящен сравнению новых кодов небольшой длины с ранее построенными кодами в метрике Ли.

§ 2. Построение кодов

Перенумеруем элементы алфавита $E = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ размера q. Предположим, что q можно представить в виде произведения $q = q_1 q_2 \ldots q_s$, где все q_i – произвольные натуральные числа, упорядоченные произвольным образом. Это разложение на множители мы используем для нумерации элементов множества E, а именно: каждому элементу a ставится во взаимно-однозначное соответствие его номер, или *индексный вектор*, $L(a) = (i_1, \ldots, i_s)$ длины s над $\mathbb{Z}_{q_1}, \mathbb{Z}_{q_2}, \ldots, \mathbb{Z}_{q_s}$ (сим-

волы j-й позиции принимают значения из $\mathbb{Z}_{q_j}$). Определим числа Q_j, $j = 1, \ldots, s$:

$$q = q_1 \ldots q_j \times Q_j, \quad j = 1, \ldots, s, \quad \text{где} \quad Q_s = 1.$$

Сначала разобьем E на q_1 подмножеств E_i размера Q_1:

$$E = E_0 \cup \ldots \cup E_{q_1 - 1},$$

где

$$E_i = \{i + jq_1 : \ j = 0, 1, \ldots, Q_1 - 1\}.$$

Затем сделаем то же самое для каждого множества E_i, т.е. каждое E_i разобьем на q_2 подмножеств $E_{i,j}$ размера Q_2:

$$E_i = E_{i,0} \cup E_{i,1} \cup \ldots \cup E_{i,q_2 - 1},$$

где

$$E_{i,j} = \{i + jq_1 + kq_1q_2 : \ k = 0, 1, \ldots, Q_2 - 1\},$$

и так далее. На ℓ-м шаге будем иметь

$$E_{i_1,\ldots,i_{\ell-1}} = E_{i_1,\ldots,i_{\ell-1},0} \cup \ldots \cup E_{i_1,\ldots,i_{\ell-1},q_\ell - 1},$$

где $E_{i_1,\ldots,i_{\ell-1},j}$ – следующее множество:

$$E_{i_1,\ldots,i_{\ell-1},j} = \\ = \{i_1 + i_2q_1 + \ldots + i_{\ell-1}q_1 \ldots q_{\ell-2} + jq_1 \ldots q_{\ell-1} + kq_1 \ldots q_\ell : \ k = 0, 1, \ldots, Q_\ell - 1\}$$

для $j = 0, 1, \ldots, q_\ell - 1$. Эту процедуру мы повторяем в течение s шагов, в результате которых получаем подмножества $E_{i_1,\ldots,i_{s-1}}$ размера $Q_{s-1} = q_s$, а именно получаем следующее разбиение:

$$E = \bigcup_{i_1=0}^{q_1-1} \ldots \bigcup_{i_{s-1}=0}^{q_{s-1}-1} E_{i_1,\ldots,i_{s-1}}, \tag{1}$$

так что каждое множество $E_{i_1,\ldots,i_{s-1}}$ содержит q_s элементов. Каждому элементу a из алфавита E размера q с разложением $q = q_1q_2 \ldots q_s$ приписывается номер, а именно его индексный вектор $L(a)$, определяемый следующим образом: если элемент a принадлежит подмножеству $E_{i_1,\ldots,i_{s-1}}$ и имеет индекс i_s в множестве $E_{i_1,\ldots,i_{s-1}}$, то a имеет индексный вектор $L(a) = (i_1, i_2, \ldots, i_{s-1}, i_s)$. Индекс i_s элемента a – это его номер в множестве элементов $E_{i_1,\ldots,i_{s-1}}$, когда эти элементы упорядочены обычным образом по возрастанию (индекс i_s элемента a растет с ростом a). Если $E_{i_1,\ldots,i_{s-1}} = \{a_1, a_2, \ldots, a, \ldots, a_{q_s}\}$, где

$$a_1 < a_2 < \ldots < a = a_j < \ldots < a_{q_s},$$

то в множестве $E_{i_1,\ldots,i_{s-1}}$ элемент a имеет индекс j.

Таким образом, каждому элементу из E ставится в соответствие его номер, представляющий собой целочисленный вектор $(i_1, \ldots, i_s)$ длины s, обладающий следующим свойством: *j-й индекс i_j принадлежит множеству* $\{0, 1, \ldots, q_j - 1\}$. Легко видеть, что вектор $L(a)$ является $(q_1, \ldots, q_s)$-разложением числа a, а именно: если $L(a)$ – индексный вектор a, т.е.

$$L(a) = (i_1, i_2, \ldots, i_s),$$

то

$$a = i_1 + i_2 q_1 + i_3 q_1 q_2 + \ldots + i_s q_1 \ldots q_{s-1}. \tag{2}$$

В случае, когда $q = p^s$ является степенью простого числа p, а элементами E_q являются элементы конечного поля $\mathbb{F}_q$, условимся, что элементы E_q упорядочиваются лексикографически, используя естественное представление элементов поля $\mathbb{F}_q$ как элементов векторного пространства размерности s над $\mathbb{F}_p$.

Следующее простое утверждение необходимо нам в дальнейшем.

Лемма 1. *Пусть E – алфавит размера q, где q представлено в виде произведения чисел $q = q_1 q_2 \ldots q_s$. Пусть a и b из E имеют номера $L(a) = (i_1, \ldots, i_s)$ и $L(b) = (j_1, \ldots, j_s)$. Пусть*

$$\ell = \min\{h : \ h = 1, \ldots, s, \ i_h \neq j_h\}.$$

Тогда

$$d_L(a,b) \geqslant q_1 \ldots q_{\ell-1} \min\Big\{|i_\ell - j_\ell|, \ \frac{q}{q_1 \ldots q_{\ell-1}} - |i_\ell - j_\ell|\Big\} \geqslant q_1 \ldots q_{\ell-1}$$

и

$$d_{L_1}(a,b) \geqslant q_1 \ldots q_{\ell-1} |i_\ell - j_\ell| \geqslant q_1 \ldots q_{\ell-1},$$

где $q_0 = 1$.

Доказательство. Предположим, что два разных элемента a и b принадлежат множеству $E_{i_1,\ldots,i_{\ell-1}}$, где ℓ – максимально возможное для заданных a и b число, обладающее этим свойством. Из выражения (2) получаем, что

$$a - b = (i_1 - j_1) + (i_2 - j_2) q_1 + (i_3 - j_3) q_1 q_2 + \ldots + (i_s - j_s) q_1 \ldots q_{s-1}. \tag{3}$$

Так как a и b принадлежат множеству $E_{i_1,\ldots,i_{\ell-1}}$, то $i_h = j_h$ для $h = 1, \ldots, \ell - 1$, и мы заключаем, что a и b сравнимы по модулю $q_1 \ldots q_{\ell-1}$. Так как $i_\ell \neq j_\ell$, для модульного расстояния получаем

$$d_{L_1}(a,b) \geqslant q_1 \ldots q_{\ell-1} |i_\ell - j_\ell| \geqslant q_1 \ldots q_{\ell-1}.$$

Аналогично для расстояния Ли получаем

$$d_L(a,b) = q_1 \ldots q_{\ell-1} \min\Big\{|i_\ell - j_\ell|, \frac{q}{q_1 \ldots q_{\ell-1}} - |i_\ell - j_\ell|\Big\} \geqslant q_1 \ldots q_{\ell-1}.$$

Обе оценки для произвольных a и b, принадлежащих множеству $E_{i_1,\ldots,i_{\ell-1}}$, очевидно, не улучшаемы, так как обе достигаются. Конечно, они могут быть улучшены в условиях леммы с помощью выражения (3), если мы знаем какие-то из индексов i_h и j_h для значений $h \geqslant \ell + 1$. ▲

Опишем построение кодов обобщенным каскадным методом. Пусть задан алфавит E (который мы называем *внутренним кодом*) размера q, где $q = q_1 q_2 \ldots q_s$ и где все элементы алфавита E перенумерованы, так что каждому элементу a сопоставлен его индексный вектор $L(a)$. Предположим, что имеется s кодов A_j, $j = 1, \ldots, s$ (одной и той же длины), где код A_j над алфавитом $E_{q_j} = \{0, 1, \ldots, q_j - 1\}$ размера q_j имеет параметры (n, N_j, d_j). Коды A_j мы называем *внешними кодами*. Из каждого кода A_j выберем по произвольному кодовому слову $\boldsymbol{a}^{(j)} = (a_1^{(j)}, \ldots, a_n^{(j)})$. По s выбранным словам $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)}$ построим матрицу B размера $s \times n$, выбирая в качестве j-й строки выбранное нами слово $\boldsymbol{a}^{(j)}$ кода A_j. Пусть $\boldsymbol{b}_i$ обозначает i-й столбец матрицы B. По построению этой матрицы элемент $b_{i,j}$, стоящий в j-й позиции вектора-столбца $\boldsymbol{b}_i$, принадлежит алфавиту E_{q_j} размера q_j, т.е. $b_{i,j} \in \{0, 1, \ldots, q_j - 1\}$.

Отсюда следует, что каждый столбец $\boldsymbol{b}_i$ является индексным вектором $L(a)$ некоторого элемента a из множества E, т.е.

$$L(a) = (i_1, \ldots, i_s) = (b_{i,1}, \ldots, b_{i,s}), \quad i_j \in \{0, 1, \ldots, q_j - 1\}, \quad j = 1, \ldots, s.$$

С помощью полученной матрицы B мы задаем кодовое слово $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ над алфавитом E нового результирующего кода C, заменяя каждый i-й вектор-столбец $\boldsymbol{b}_i$ элементом $a = a(\boldsymbol{b}_i)$, индексным вектором которого является вектор-столбец $\boldsymbol{b}_i$. Это означает, что на i-й позиции кодового слова $\boldsymbol{c} = (c_1, \ldots, c_n)$ стоит элемент a, т.е. что $c_i = a = a(\boldsymbol{b}_i)$. Тем самым, каждому выбору $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)}$ слов по одному из каждого внешнего кода A_j соответствует одно слово $\boldsymbol{c}$ результирующего кода C. Когда все кодовые слова $\boldsymbol{a}^{(j)}$ пробегают все внешние коды A_j для всех $j = 1, \ldots, s$, соответствующие кодовые слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ пробегают весь код C.

Теорема 1. *Пусть задано множество $E = \{0, 1, \ldots, q-1\}$ размера q, где q представимо в виде произведения s натуральных чисел $q = q_1 q_2 \ldots q_s$. Предположим, что имеется s внешних q_j-ичных кодов A_j, $j = 1, \ldots, s$, с параметрами $(n, N_j, d_j)_{q_j}$. Тогда описанная выше конструкция приводит к q-ичному коду C над алфавитом E с параметрами*

$$n, \quad N = \prod_{j=1}^{s} N_j, \quad d_{L_1} \geqslant d_L \geqslant \min\{d_1,\, q_1 d_2,\, q_1 q_2 d_3,\, \ldots,\, q_1 q_2 \ldots q_{s-1} d_s\}.$$

Доказательство. Значения параметров q, n и N нового кода вполне очевидны по построению кода. Докажем, что результирующий код C имеет расстояние Ли d_L и модульное расстояние d_{L_1}, указанные в утверждении теоремы. Пусть $\boldsymbol{c}^{(1)} = (c_1^{(1)}, \ldots, c_n^{(1)})$ и $\boldsymbol{c}^{(2)} = (c_1^{(2)}, \ldots, c_n^{(2)})$ – два различных кодовых слова, и пусть $\boldsymbol{a}^{(j,1)} = (a_1^{(j,1)}, \ldots, a_n^{(j,1)})$ и $\boldsymbol{a}^{(j,2)} = (a_1^{(j,2)}, \ldots, a_n^{(j,2)})$, $j = 1, \ldots, s$, – кодовые слова внешних кодов, на которых основаны соответствующие слова кода C. Так как $\boldsymbol{c}^{(1)}$ и $\boldsymbol{c}^{(2)}$ различны, то имеется ℓ, такое что слова $\boldsymbol{a}^{(\ell,1)}$ и $\boldsymbol{a}^{(\ell,2)}$ различны, но все предыдущие слова $\boldsymbol{a}^{(j,1)}$ и $\boldsymbol{a}^{(j,2)}$, где $j = 1, \ldots, \ell - 1$, совпадают. Далее, $\boldsymbol{a}^{(\ell,1)}$ и $\boldsymbol{a}^{(\ell,2)}$ (как кодовые слова A_ℓ) находятся друг от друга на расстоянии (Хэмминга) d_ℓ или больше. Это означает, что имеется по крайней мере d_ℓ позиций с номерами $r \in \{1, \ldots, n\}$, в которых индексные векторы $L^{(1)}(c_r^{(1)}) = (i_1, \ldots, i_s)$ и $L^{(2)}(c_r^{(2)}) = (j_1, \ldots, j_s)$ элементов $c_r^{(1)}$ и $c_r^{(2)}$ совпадают в первых $\ell - 1$ позициях и отличаются в ℓ-й позиции. Поэтому в силу леммы 1 элементы $c_r^{(1)}$ и $c_r^{(2)}$ находятся друг от друга на расстоянии Ли

$$d_L(c_r^{(1)}, c_r^{(2)}) \geqslant q_1 \ldots q_{\ell-1}.$$

Учитывая, что число таких позиций не менее d_ℓ, а кодовые слова $\boldsymbol{c}^{(1)}$ и $\boldsymbol{c}^{(2)}$ находятся друг от друга на расстоянии не менее чем $(q_1 \ldots q_{\ell-1})d_\ell$, получаем требуемое выражение для минимального расстояния d_L кода C. Тот же результат, очевидно, справедлив и для модульного расстояния, которое всегда не меньше расстояния Ли. ▲

Замечание 1. Заметим, что код, полученный по теореме 1, может быть декодирован алгоритмом, предложенным в работе [11], который реализует минимальное расстояние кода, а также допускает мягкое декодирование. Построенные обобщенные каскадные коды в метриках d_L и d_{L_1}, так же как и для метрики Хэмминга (см. [10–12]) и евклидовой метрики [9], позволяют исправлять как независимые ошибки, так и пакеты ошибок. Кроме того, они обладают важным свойством неравной защиты информационных символов [13]. Все эти свойства реализуются одним и

тем же алгоритмом декодирования по минимуму обобщенного расстояния, предложенным в указанной работе [11].

§ 3. Комбинаторные и алгебраические свойства

Пусть S_n обозначает полную группу всех перестановок на множестве из n элементов. Два кода C и C' в E_q^n с одними и теми же параметрами эквивалентны, если найдутся вектор $\boldsymbol{x} \in E_q^n$ и перестановка $\sigma \in S_n$ (которая действует на координатных позициях множества E_q^n), такие что

$$C + \boldsymbol{x} = \sigma(C').$$

Теорема 2. *Пусть коды C и C' над алфавитом E получены по теореме* 1 *из внешних кодов $A_1, A_2, \ldots, A_s$ и $A'_1, A'_2, \ldots, A'_s$ соответственно. Пусть найдется по крайней мере одно i, такое что коды A_i и A'_i не эквивалентны. Тогда результирующие коды C и C' также не эквивалентны.*

Доказательство. Предположим, что коды $A_1, A_2, \ldots, A_s$ эквивалентны кодам $A'_1, A'_2, \ldots, A'_s$, т.е. существует перестановка $\pi \in S_n$ и векторы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s$, такие что $A_i + \boldsymbol{x}_i = \pi(A'_i)$ для $i = 1, \ldots, s$. По построению кодов это означает, что множество матриц B под действием сдвига каждой i-й строки на вектор $\boldsymbol{x}_i$, $i = 1, \ldots, s$, и перестановки π на столбцы матриц B переходит в множество матриц B' (определяющих слова кода C'). Но это означает, что коды C и C' эквивалентны. Наоборот, пусть код C' эквивалентен коду C, т.е. существует перестановка $\pi \in S_n$ и вектор $\boldsymbol{x} \in E_q^n$, такие что $C + \boldsymbol{x} = \pi(C')$. Тогда $\pi(A'_i) = A_i + \boldsymbol{x}_i$ (здесь $\boldsymbol{x}_i$ индуцируются вектором $\boldsymbol{x}$) для всех $i = 1, \ldots, s$, т.е. коды A_i и A'_i эквивалентны. Если же коды A_i и A'_i не эквивалентны хотя бы для одного i, то результирующие коды C и C' не могут быть эквивалентны. ▲

Для произвольного кода C обозначим через $\mathrm{Sym}(C)$ множество перестановок, стабилизирующих этот код. Два кода C и C' назовем *симметрично эквивалентными*, если найдется перестановка $\tau \in \mathrm{Sym}(C)$, такая что $C = \tau(C') = \{\tau(\boldsymbol{v}) : \boldsymbol{v} \in C'\}$. Скажем, что код $C \subset E_q^n$ *симметрично транзитивен*, если для любых двух слов $\boldsymbol{u}$ и $\boldsymbol{v}$ кода C, имеющих одну и ту же композицию, существует перестановка $\tau \in \mathrm{Sym}(C)$, такая что $\tau(\boldsymbol{u}) = \boldsymbol{v}$.

Теорема 3. *Пусть $q = q_1 q_2$ и заданы коды A_1 и A_2. Пусть код C над алфавитом E_q получен по теореме* 1 *из кодов A_1 и A_2. Предположим, что код A_1 симметрично транзитивен, а код A_2 таков, что $\mathrm{Sym}(A_2) = S_n$. Тогда код C также симметрично транзитивен.*

Доказательство. Пусть $\boldsymbol{c}_1$ и $\boldsymbol{c}_2$ – произвольные кодовые слова из C, имеющие одну и ту же композицию, и пусть слово $\boldsymbol{c}_1$ получено из $\boldsymbol{a}_1 \in A_1$ и $\boldsymbol{b}_1 \in A_2$, а $\boldsymbol{c}_2$ – из $\boldsymbol{a}_2 \in A_1$ и $\boldsymbol{b}_2 \in A_2$. Так как по построению

$$\boldsymbol{c}_j = \boldsymbol{a}_j + q_1 \boldsymbol{b}_j, \quad j = 1, 2,$$

то слова $\boldsymbol{b}_1$ и $\boldsymbol{b}_2$ (а также $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$) имеют одну и ту же композицию и поэтому могут быть переставлены некоторой перестановкой из S_n. Поскольку код A_1 симметрично транзитивен, найдется перестановка $\pi \in \mathrm{Sym}(A_1)$, такая что $\pi(\boldsymbol{a}_1) = \boldsymbol{a}_2$. Так как заведомо $\pi \in S_n$, положим $\pi(b_1) = b_2$, и тогда получим

$$\pi(\boldsymbol{c}_1) = \pi(\boldsymbol{a}_1 + q_1 \boldsymbol{b}_1) = \pi(\boldsymbol{a}_1) + q_1 \pi(\boldsymbol{b}_1) = \boldsymbol{a}_2 + q_1 \boldsymbol{b}_2 = \boldsymbol{c}_2. \quad ▲$$

Код $C \subseteq E_q^n$ имеет радиус покрытия $\rho = \rho(C)$, если ρ – минимальное число, такое что шары радиуса ρ с центрами в кодовых словах кода C покрывают все пространство E_q^n.

Теорема 4. *Пусть код C получен конструкцией теоремы 1 из s внешних кодов A_i, $i = 1, \dots, s$. Если код A_i для каждого i имеет радиус покрытия ρ_i, то результирующий код C имеет радиус покрытия*

$$\rho(C) \geqslant \max\{\rho_1, q_1\rho_2, \dots, q_1 \dots q_{s-1}\rho_s\}.$$

Доказательство. Заметим, что все слова кода A_1 являются словами кода C (это слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)})$, построенные только из A_1 выбором нулевых слов из всех других кодов A_i с $i \geqslant 2$). Покажем, что вектор $\boldsymbol{x}_1$, который находится на расстоянии ρ_1 от кода A_1, находится от кода C на расстоянии, не меньшем чем ρ_1, т.е. что $d(\boldsymbol{x}_1, C) \geqslant d(\boldsymbol{x}_1, A_1)$. Пусть, например, слово $\boldsymbol{c} \in C$ построено по словам $\boldsymbol{a}^{(1)} = (a_1^{(1)}, \dots, a_n^{(1)})$-кода A_1 и $\boldsymbol{a}^{(2)} = (a_1^{(2)}, \dots, a_n^{(2)})$-кода A_2. Индексные векторы компонент слова $\boldsymbol{c}$ имеют вид $(a_i^{(1)}, a_i^{(2)}, 0, \dots, 0)$, $i = 1, 2, \dots, n$. Пусть $j_1, \dots, j_{\rho_1}$ – номера позиций, в которых $\boldsymbol{x}_1$ и $\boldsymbol{a}^{(1)}$ различаются. В наихудшем для нас случае все ненулевые символы слова $\boldsymbol{a}^{(2)}$ расположены в тех же позициях, что и ненулевые символы слова $\boldsymbol{a}^{(1)}$. Но индексные векторы элементов $\boldsymbol{x}_1$ имеют только первую ненулевую компоненту (а все остальные равны нулю). Поэтому любая компонента j_h, в которой $\boldsymbol{x}_1$ и $\boldsymbol{a}^{(1)}$ различаются и в которой $a_{j_h}^{(2)} \neq 0$, увеличивает расстояние Ли между $\boldsymbol{x}_1$ и $\boldsymbol{c}$ (по крайней мере на q_1) по сравнению с расстоянием Хэмминга между $\boldsymbol{x}_1$ и $\boldsymbol{a}^{(1)}$, равным ρ_1. Тем самым мы доказали, что $\rho(C) \geqslant \rho_1$.

Следующее неравенство $\rho(C) \geqslant \max\{\rho_1, q_1\rho_2\}$ доказывается совершенно аналогично. Рассмотрим все слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(2)})$, полученные выбором ненулевого слова $\boldsymbol{a}^{(2)} = (a_1^{(2)}, \dots, a_n^{(2)})$ кода A_2, а всех остальных слов – нулевыми. Индексные векторы компонент таких слов $\boldsymbol{c}$ имеют вид $(0, a_i^{(2)}, 0, \dots, 0)$, $i = 1, 2, \dots, n$. Если вектор $\boldsymbol{x}_2$ находится на расстоянии ρ_2 от кода A_2, то он находится на расстоянии, не меньшем чем $q_1\rho_2$, от всех слов $\boldsymbol{c}$ кода C указанного вида (действительно, координатные позиции таких слов кратны q_1). Можем ли мы приблизиться к $\boldsymbol{x}_2$, рассматривая слова $\boldsymbol{c}$ другого типа? Ясно, что это невозможно при выборе ненулевыми слов $\boldsymbol{a}^{(3)}$. Соответствующие слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(2)}, \boldsymbol{a}^{(2)})$ (полученные выбором ненулевых слов $\boldsymbol{a}^{(2)}$ и $\boldsymbol{a}^{(3)}$) имеют новые координатные позиции, которые не пересекаются с позициями слов $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(2)})$ и которые кратны уже q_1q_2. Тем самым, расстояние между $\boldsymbol{x}_2$ и кодом C только увеличивается. Если же выбирать ненулевыми слова $\boldsymbol{a}^{(1)}$, то мы окажемся в условиях предыдущего случая, для которого $\rho(C) \geqslant \rho_1$. Это дает оценку $\rho(C) \geqslant \max\{\rho_1, q_1\rho_2\}$.

Следующее неравенство $\rho(C) \geqslant \max\{\rho_1, q_1\rho_2, q_1q_2\rho_3\}$ устанавливается аналогичным образом, и так далее. ▲

§ 4. $\mathbb{Z}_4$-коды

Пусть $E = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, т.е. $q = 4 = 2 \cdot 2$. Любой элемент a из E имеет индексный вектор (i_1, i_2), являющийся двоичным представлением a, т.е. $a = i_1 + 2i_2$. Положим $n = 2^m$ и выберем следующие два внешних кода: двоичный расширенный совершенный $(n, 2^{n-m-1}, 4)$-код в качестве кода A_1 и $(n, 2^{n-1}, 2)$-код, полученный проверкой на четность или на нечетность по модулю 2, в качестве кода A_2. Пусть

$$\boldsymbol{a}^{(1)} = \left(a_1^{(1)}, a_2^{(1)}, \dots, a_n^{(1)}\right) \in A_1 \quad \text{и} \quad \boldsymbol{a}^{(2)} = \left(a_1^{(2)}, a_2^{(2)}, \dots, a_n^{(2)}\right) \in A_2.$$

Тогда

$$\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \boldsymbol{a}^{(2)}) = (c_1, c_2, \dots, c_n) \in C,$$

где

$$L(c_i) = \big(a_i^{(1)}, a_i^{(2)}\big), \quad \text{так что} \quad c_i = a_i^{(1)} + 2a_i^{(2)} \in \mathbb{Z}_4.$$

Результирующий $(n, N, d_L)_4$-код C над $\mathbb{Z}_4$ имеет следующие параметры:

$$n = 2^m, \quad N = 2^{2n-m-2}, \quad d_L = \min\{4 \cdot 1, 2 \cdot 2\} = 4, \quad q = 4.$$

Напомним отображение Грея φ из $\mathbb{Z}_4$ на $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$$\varphi(0) = (0,0), \quad \varphi(1) = (1,0), \quad \varphi(2) = (1,1), \quad \varphi(3) = (0,1),$$

которое продолжается на векторы над $\mathbb{Z}_4$ очевидным образом:

$$\varphi(c_1, \ldots, c_n) = (\varphi(c_1), \ldots, \varphi(c_n)).$$

Определим теперь новый код $\mathcal{C}$ как образ кода C с помощью отображения Грея:

$$\mathcal{C} = \{\varphi(\boldsymbol{c}) : \ \boldsymbol{c} \in C\}.$$

Так как при отображении Грея из $\mathbb{Z}_4$ в $\mathbb{Z}_2 \times \mathbb{Z}_2$ расстояние Ли переходит в расстояние Хэмминга [14], так что

$$d_L(\boldsymbol{x}, \boldsymbol{y}) = d(\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})),$$

то заключаем, что новый $(n', N', d')_2$-код $\mathcal{C}$ имеет параметры

$$n' = 2^{m+1}, \quad N' = 2^{n'-m-2}, \quad d' = 4.$$

Таким образом, $\mathcal{C}$ представляет собой двоичный расширенный совершенный код, допускающий $\mathbb{Z}_4$-представление, иначе говоря, $\mathbb{Z}_4$-код. Это означает, что произвольный двоичный расширенный совершенный код A_1 длины n индуцирует двоичный расширенный совершенный $\mathbb{Z}_4$-код C длины $2n$.

Итак, с учетом теоремы 2 имеет место следующая

Теорема 5. *Двоичный расширенный совершенный код A_1 длины n индуцирует двоичный расширенный совершенный $\mathbb{Z}_4$-код C длины $2n$. При этом, если два таких кода A_1 и A_1' не эквивалентны (соответственно, различны), то результирующие $\mathbb{Z}_4$-коды C и C' длины $2n$ также не эквивалентны (соответственно, различны).*

Напомним, что все $\mathbb{Z}_4$-линейные совершенные коды перечислены в [15].

Следствие 1. *Число взаимно неэквивалентных расширенных двоичных совершенных кодов длины $n = 2^m$, имеющих $\mathbb{Z}_4$-представление, не меньше $2^{2^{n/4}}$.*

Доказательство. Этот результат непосредственно вытекает из известной конструкции удвоения Васильева [16], из которой следует, что число взаимно неэквивалентных расширенных двоичных совершенных кодов длины $n = 2^m$ не меньше $2^{2^{n/2}}$. ▲

Снова рассмотрим алфавит $E = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, т.е. $q = 4 = 2 \cdot 2$. Пусть n – натуральное число, такое что существует матрица Адамара порядка n. Таким образом, в качестве A_1 мы берем $(n, 2, n)$-код с повторением, а в качестве кода A_2 – $(n, 2n, n/2)$-код Адамара.

Тогда результирующий $(n, N, d_L)_4$-код C над $\mathbb{Z}_4$ имеет параметры

$$n, \quad N = 4n, \quad d_L = \min\Big\{n \cdot 1, 2 \cdot \frac{n}{2}\Big\} = n, \quad q = 4.$$

Теперь, если определить новый код длины $2n$ как образ кода C под действием отображения Грея, мы получим двоичный $(2n, 4n, n)$-код Адамара. Таким образом, каждый код Адамара длины n порождает код Адамара длины $2n$, имеющий $\mathbb{Z}_4$-представление. Коды Адамара, имеющие $\mathbb{Z}_{2^s}$-представления, активно изучаются (см., например, работу [17] и библиографию в ней).

Теорема 6. *Пусть A_2 – двоичный код Адамара длины n, т.е. код с параметрами $(n, 2n, n/2)$. Тогда этот код вместе с $(n, 2, n)$-кодом A_1 индуцирует двоичный $(2n, 4n, n)$-код Адамара C, имеющий $\mathbb{Z}_4$-представление. При этом, если два таких кода A_2 и A_2' не эквивалентны (соответственно, различны), то результирующие $\mathbb{Z}_4$-коды C и C' длины $2n$ также не эквивалентны (соответственно, различны).*

Из этого утверждения непосредственно вытекает

Следствие 2. *Число взаимно неэквивалентных двоичных $(n, 2n, n/2)$-кодов Адамара длины n, имеющих $\mathbb{Z}_4$-представление, не меньше числа взаимно неэквивалентных двоичных $(n/2, n, n/4)$-кодов Адамара.*

§ 5. Коды над $\mathbb{Z}_{p^s}$

Рассмотрим алфавит $E_q = \mathbb{Z}_q$, где $q = p^s$, а $p \geqslant 2$ – простое. Если использовать в качестве внешних кодов A_i двоичные расширенные примитивные (в узком смысле) коды БЧХ, то имеет место следующая

Теорема 7. *Пусть m, s, u – произвольные натуральные числа, такие что $m \geqslant 3$, $s \geqslant 2$, $u \geqslant 2$. Тогда конструкция теоремы 1 дает (n, N, d_L)-код C над $\mathbb{Z}_q$ с параметрами $n = 2^m$, $N = 2^k$, $d_L = d_{L_1} = 2^u$, $q = 2^s$, где*

$$k \geqslant \begin{cases} sn - s - m(2^u - 2^{u-s} - s), & \text{если } q \leqslant d, \\ sn - u - m(2^u - u - 1), & \text{если } q > d. \end{cases} \tag{4}$$

Доказательство. Как известно, для любых натуральных m и t, таких что $tm \leqslant 2^m - 2$ и $t \leqslant 2^{m-2} - 1$, существует расширенный двоичный примитивный $[n, k, d]$-код БЧХ (в узком смысле), такой что

$$n = 2^m, \quad k \geqslant n - 1 - mt, \quad d \geqslant 2t + 2.$$

В описанной выше конструкции выберем в качестве i-го внешнего кода A_i расширенный двоичный примитивный код БЧХ (в узком смысле) с параметрами

$$n = 2^m, \quad d_i = 2^{u-i+1}, \quad k_i \geqslant n - 1 - m(2^{u-i} - 1), \quad i = 1, 2, \ldots, s.$$

В зависимости от соотношения между s и u непосредственно из теоремы 1 получаем следующие два выражения для нижней оценки числа информационных символов $k = k_1 + \ldots + k_s$ результирующего кода: если $s \leqslant u$, то

$$k \geqslant (n - 1 - m(2^{u-1} - 1)) + (n - 1 - m(2^{u-2} - 1)) + \ldots + (n - 1 - m(2^{u-s} - 1)),$$

а если $s \geqslant u + 1$, то

$$k \geqslant (n - 1 - m(2^{u-1} - 1)) + (n - 1 - m(2^{u-2} - 1)) + \ldots + (n - 1) + n(s - u).$$

Учитывая, что

$$\sum_{i=u-s}^{u-1} (2^i - 1) = 2^u - 2^{u-s} - s$$

и

$$\sum_{i=1}^{u-1}(2^i-1)=2^u-u-1,$$

получаем две соответствующие оценки на число k, приведенные в утверждении теоремы. ▲

Покажем теперь как можно построить код C с произвольными параметрами q, n и d_L, где $q=p^s$ – произвольная степень простого числа $p\geqslant 2$, а n и d_L – натуральные числа, удовлетворяющие следующему условию: найдется целое число i, $1\leqslant i\leqslant s$, такое что

$$\frac{d_L}{p^{i-1}}\leqslant n. \tag{5}$$

Обозначим через $h=h(s,p,n,d_L)$ минимальное i, для которого имеет место неравенство (5). Параметр h – это индекс начала нетривиальных внешних кодов A_i. Построим $s-h+1$ внешних $(n,N_i,d_i)_p$-кодов A_i над $\mathbb{F}_p$ для $i=h,\ldots,s$. Положим $d_1=d_L$. Для каждого $i=h,\ldots,s$ определим параметр ℓ_i, а именно натуральное число, которое задает параметры внешнего кода A_i (и которое надо оптимизировать). Код A_i строится с помощью (простой) каскадной конструкции из двух кодов: внешнего $(n_{v,i},k_{v,i},d_{v,i})$-кода V_i над $\mathbb{F}_{q^{\ell_i}}$, где $d_{v,i}=n_{v,i}+1-k_{v,i}$, являющегося МДР-кодом, и внутреннего $(n_{u,i},N_{u,i},d_{u,i})_p$-кода U_i над $\mathbb{F}_p$, мощность которого определяется размером алфавита внешнего кода V_i, т.е. $N_{u,i}=q^{\ell_i}$, длина которого $n_{u,i}$ должна удовлетворять условию $n_{v,i}n_{u,i}\geqslant n$ для всех $i=h,\ldots,s$. Для каждого $i=h,\ldots,s$ введем еще один параметр, а именно целое неотрицательное число $\chi_i=n_{v,i}n_{u,i}-n$. Длины $n_{v,i}$ и $n_{u,i}$ должны выбираться так, чтобы χ_i было минимальным. Каждый символ каждого кодового слова V_i заменяем на кодовое слово кода U_i, которое поставлено ему во взаимно-однозначное соответствие. В результате получаем внешний (уже для обобщенной каскадной конструкции теоремы 1) код A_i над $\mathbb{F}_p$ с параметрами (n,N_i,d_i):

$$n=n_{v,i}n_{u,i}-\chi_i,\quad N_i=p^{k_i},\quad d_i=d_{v,i}d_{u,i}-\chi_i^{(d)}, \tag{6}$$

где

$$k_i=s\ell_i(n_{v,i}+1-d_{v,i})-\chi_i^{(k)}, \tag{7}$$

а целочисленные (неотрицательные) параметры $\chi_i^{(d)}$ и $\chi_i^{(k)}$ выбираются произвольно так, чтобы выполнялось равенство

$$\chi_i=\chi_i^{(k)}+\chi_i^{(d)}.$$

Используя построенные коды A_i для всех $i=h,\ldots,s$, в соответствии с теоремой 1 получаем код C над $\mathbb{F}_q$ с параметрами $(n,N,d_L)_q$, где

$$n,\quad N=p^k,\quad k=\sum_{i=h}^{s}k_i,\quad d_L=\min\bigl\{p^{i-1}d_{v,i}d_{u,i}:\ i=h,\ldots,s\bigr\}. \tag{8}$$

При $i\leqslant h-1$ код A_i представляет собой формально тривиальный код (т.е. одно кодовое слово), не дающий вклада в мощность результирующего кода C. В этих случаях в алфавите E_q размера q можно использовать только числа, кратные p^{h-1}.

В частном случае, когда $\ell_i=\ell$ для всех $i=h,\ldots,s$ для некоторого $\ell\geqslant 1$, все внешние коды V_i имеют одинаковую длину n_v, все внутренние коды U_i имеют одни

и те же параметры $(n_u, p^{s\ell}, d_u)_p$, и когда $\chi_i = 0$ для всех $i = h, \ldots, s$, параметры n, $N = p^k$ и d_L кода C принимают следующий вид:

$$n = n_v n_u, \quad k = s\ell \sum_{i=h}^{s} (n_v + 1 - d_{v,i}) \tag{9}$$

и

$$d_L = d_u \min\bigl\{p^{i-1} d_{v,i} : \ i = h, \ldots, s\bigr\}. \tag{10}$$

Таким образом, имеет место следующая

Теорема 8. *Пусть $q = p^s$ – произвольная степень простого числа p, и пусть m, d_L – натуральные числа, причем m – любое, а d_L – такое, что имеется число h в диапазоне $1 \leqslant h \leqslant s-1$, для которого справедливо неравенство* (5), *не справедливое при этом для $h-1$. Тогда теорема* 1 *гарантирует построение указанным выше способом (n, k, d_L)-кода C над $\mathbb{F}_q$ с параметрами, удовлетворяющими соотношениям* (9), (10).

Чтобы написать явные выражения для параметров q, n, d_L и $N = p^k$, нужно выбрать конкретный внутренний код U. Как показывают приводимые ниже примеры кодов, удобно использовать код с проверкой на четность, т.е. код U с параметрами $n_u = s\ell + 1$, $N_u = p^{s\ell}$ и $d_u = 2$. Для этого очень частного (вообще говоря, не всегда оптимального) выбора кода U справедливо

Следствие 3. *Пусть $q = p^s$ – произвольная степень простого числа p, а числа n, d_L и h удовлетворяют условиям теоремы* 8. *Тогда теорема* 1 *гарантирует, что (n, N, d_L)-код C над $\mathbb{F}_q$, построенный указанным выше способом, имеет следующие параметры*:

$$N = q^k = p^{sk}, \quad \text{где} \quad k \geqslant n\frac{2(s-h+1)}{2s+1} - d_L \frac{p^{s-h}-1}{(p-1)p^{s-1}}. \tag{11}$$

Доказательство. Из (9), учитывая, что $n = n_v(\ell s+1)$ и $d_L = d_{v,1} d_{u,1} = 2d_{v,1}$, имеем

$$\begin{aligned} k &= \ell \sum_{i=h}^{s} (n_v + 1 - d_{v,i}) = \ell \sum_{i=h}^{s} \left(n_v + 1 - \left\lceil \frac{d_{v,1}}{p^{i-1}} \right\rceil \right) \geqslant \ell \sum_{i=h}^{s} \left(n_v - \frac{d_{v,1}}{p^{i-1}} \right) = \\ &= \ell(s-h+1)n_v - \frac{\ell d_{v,1}}{p^{s-1}} \frac{(p^{s-h}-1)}{p-1} = \ell(s-h+1)\frac{n}{\ell s+1} - \frac{\ell d_{v,1}}{p^{s-1}} \frac{(p^{s-h}-1)}{p-1} = \\ &= n\frac{\ell(s-h+1)}{\ell s+1} - \frac{d_L}{2} \frac{\ell(p^{s-h}-1)}{(p-1)p^{s-1}}. \end{aligned}$$

Результирующий код C над $\mathbb{F}_q$ имеет минимальное расстояние

$$d_L = 2 \min \left\{ p^{i-1} \left\lceil \frac{d_{v,1}}{p^{i-1}} \right\rceil : \ i = 1, \ldots, s \right\} = 2d_{v,1}.$$

Получаем следующее выражение для k, которое зависит от выбора ℓ:

$$k \geqslant \max \left\{ n\frac{\ell(s-h+1)}{\ell s+1} - d_L \frac{\ell(p^{s-h}-1)}{2(p-1)p^{s-1}} : \ \ell \geqslant 1 \right\}. \quad \blacktriangle \tag{12}$$

§ 6. Сравнения с каскадными кодами

Как упоминалось, Астола [5] предложил каскадную конструкцию для кодов в метрике Ли, в которой он использовал известные идеи Юстесена для построения

Таблица 1

$(n_a, k_a, d_a)_q$ [5]	$(n_a, k, d)_q$ (теорема 8)	ℓ	h	$A_i(n, k_i, d_i)_p$	$V_i(n_{v,i}, k_{v,i}, d_{v,i})_{q^\ell}$	$U_i(n_{u,i}, k_{u,i}, d_{u,i})_p$
$(48, 2, 80)_{5^2}$	$(48, 2, 200)_{5^2}$	1	2	$A_2(48, 2, 40)_5$		
$(48, 2, 80)_{5^2}$	$(48, 21, 80)_{5^2}$	1	2	$A_2(48, 21, 16)_5$		
$(48, 4, 70)_{5^2}$	$(48, 4, 180)_{5^2}$	2	2	$A_2(48, 4, 36)_5$		
$(48, 4, 70)_{5^2}$	$(48, 24, 75)_{5^2}$	2	2	$A_2(48, 24, 15)_5$		
$(48, 8, 54)_{5^2}$	$(48, 8, 150)_{5^2}$	2	2	$A_2(48, 8, 30)_5$		
$(48, 8, 54)_{5^2}$	$(48, 28, 55)_{5^2}$	2	2	$A_2(48, 28, 11)_5$		
$(2496, 62, 2696)_{5^2}$	$(2496, 63, 6040)_{5^2}$	3	2	$A_2(2496, 63, 1208)_5$	$V_2(624, 21, 604)_{5^6}$	$U_2(4, 3, 2)_5$
$(2496, 62, 2696)_{5^2}$	$(2496, 474, 2700)_{5^2}$	2	2	$A_2(2496, 948, 540)_5$	$V_2(416, 237, 180)_{5^4}$	$U_2(6, 4, 3)_5$
$(2496, 124, 2510)_{5^2}$	$(2496, 126, 5830)_{5^2}$	3	2	$A_2(2496, 126, 1166)_5$	$V_2(624, 42, 583)_{5^6}$	$U_2(4, 3, 2)_5$
$(2496, 124, 2510)_{5^2}$	$(2496, 498, 2520)_{5^2}$	2	2	$A_2(2496, 996, 504)_5$	$V_2(416, 249, 168)_{5^4}$	$U_2(6, 4, 3)_5$
$(160, 4, 412)_{3^4}$	$(160, 4, 2268)_{3^4}$	1	4	$A_4(160, 4, 84)_3$		
$(160, 4, 412)_{3^4}$	$(160, 161/4, 414)_{3^4}$	1 1 1	2 2 2	$A_2(160, 1, 160)_3$ $A_3(160, 49, 46)_3$ $A_4(160, 111, 16)_3$		
$(160, 20, 300)_{3^4}$	$(160, 20, 864)_{3^4}$	1 1	3 3	$A_3(160, 10, 96)_3$ $A_4(160, 70, 33)_3$		
$(160, 20, 300)_{3^4}$	$(160, 201/4, 306)_{3^4}$	1 1 1	2 2 2	$A_2(160, 7, 102)_3$ $A_3(160, 69, 34)_3$ $A_4(160, 125, 12)_3$		
$(160, 40, 174)_{3^4}$	$(160, 40, 405)_{3^4}$	1 1 1	2 2 2	$A_2(160, 1, 480)_3$ $A_3(160, 45, 48)_3$ $A_4(160, 114, 15)_3$		
$(160, 40, 174)_{3^4}$	$(160, 275/4, 174)_{3^4}$	1 1 1	2 2 2	$A_2(160, 36, 58)_3$ $A_3(160, 99, 20)_3$ $A_4(160, 140, 7)_3$		
$(26240, 656, 49810)_{3^4}$	$(26240, 656, 212706)_{3^4}$	2	4	$A_4(26240, 2624, 7878)_3$	$V_4(1640, 328, 1313)_{3^8}$	$U_4(16, 8, 6)_3$
$(26240, 656, 49810)_{3^4}$	$(26240, 11045/2, 49815)_{3^4}$	2 2	3 3	$A_3(26250, 6142, 5535)_3$ $A_4(26244, 15348, 1846)_3$	$V_3(1875, 769, 1107)_{3^8}$ $V_4(2916, 1994, 923)_{3^8}$	$U_3(14, 8, 5)_3$ $U_4(9, 8, 2)_3$

Таблица 1 (продолжение)

$(n_a, k_a, d_a)_q$ [3]	$(n_a, k, d)_q$ (теорема 8)	ℓ	h	$A_i(n, k_i, d_i)_p$	$V_i(n_{v,i}, k_{v,i}, d_{v,i})_{q^\ell}$	$U_i(n_{u,i}, k_{u,i}, d_{u,i})_p$
$(26240, 5248, 28154)_{3^4}$	$(26240, 5250, 43304)_{3^4}$	2	3	$A_3(26244, 4080, 4812)_3$	$V_3(2916, 510, 2406)_{3^8}$	$U_3(9, 8, 2)_3$
		2	3	$A_4(26244, 16920, 1604)_3$	$V_4(2916, 2115, 802)_{3^8}$	$U_4(9, 8, 2)_3$
$(26240, 5248, 28154)_{3^4}$	$(26240, 8032, 28157)_{3^4}$	2	2	$A_2(26240, 2160, 9387)_3$	$V_2(1312, 270, 1043)_{3^8}$	$U_3(20, 8, 9)_3$
		2	2	$A_3(26244, 10812, 3130)_3$	$V_3(2916, 1352, 1565)_{3^8}$	$U_3(9, 8, 2)_3$
		2	2	$A_4(26244, 19156, 1044)_3$	$V_4(2916, 2395, 522)_{3^8}$	$U_4(9, 8, 2)_3$
$(484, 12, 1942)_{3^5}$	$(484, 12, 6318)_{3^5}$	2	5	$A_5(484, 60, 78)_3$	$V_5(44, 6, 39)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 12, 1942)_{3^5}$	$(484, 84, 1942)_{3^5}$	2	5	$A_3(495, 20, 224)_3$	$V_3(9, 2, 8)_{3^{10}}$	$U_3(55, 10, 28)_3$
		2	5	$A_4(486, 160, 72)_3$	$V_4(27, 16, 12)_{3^{10}}$	$U_4(18, 10, 6)_3$
		2	5	$A_5(486, 240, 24)_3$	$V_5(27, 24, 4)_{3^{10}}$	$U_5(18, 10, 6)_3$
$(484, 60, 1394)_{3^5}$	$(484, 60, 2430)_{3^5}$	2	5	$A_5(484, 300, 30)_3$	$V_5(44, 30, 15)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 60, 1394)_{3^5}$	$(484, 591/5, 1404)_{3^5}$	2	2	$A_2(484, 1, 484)_3$		
		2	2	$A_3(484, 40, 168)_3$	$V_3(11, 4, 8)_{3^{10}}$	$U_3(44, 10, 21)_3$
		2	2	$A_4(484, 190, 52)_3$	$V_4(44, 19, 26)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	2	$A_5(484, 360, 18)_3$	$V_5(44, 36, 9)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 120, 796)_{3^5}$	$(484, 120, 1188)_{3^5}$	2	4	$A_4(484, 230, 44)_3$	$V_4(44, 23, 22)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	4	$A_5(484, 370, 16)_3$	$V_5(44, 37, 8)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(484, 120, 796)_{3^5}$	$(484, 851/5, 798)_{3^5}$	2	2	$A_2(484, 16, 270)_3$		
		2	2	$A_3(486, 130, 90)_3$	$V_3(27, 13, 15)_{3^{10}}$	$U_3(18, 10, 6)_3$
		2	2	$A_4(484, 300, 30)_3$	$V_4(44, 30, 15)_{3^{10}}$	$U_4(11, 10, 2)_3$
		3	2	$A_5(496, 405, 10)_3$	$V_5(31, 27, 5)_{3^{15}}$	$U_5(16, 15, 2)_3$
$(236192, 5904, 768402)_{3^5}$	$(236192, 5904, 3000402)_{3^5}$	2	5	$A_5(236192, 29520, 37042)_3$	$V_5(21472, 2952, 18521)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(236192, 5904, 768402)_{3^5}$	$(236192, 49923, 768442)_{3^5}$	2	3	$A_3(236192, 12500, 85383)_3$	$V_3(10736, 1250, 9487)_{3^{10}}$	$U_3(22, 10, 9)_3$
		2	3	$A_4(236197, 86830, 28461)_3$	$V_4(18169, 8683, 9487)_{3^{10}}$	$U_4(13, 10, 3)_3$
		2	3	$A_5(236192, 150285, 9488)_3$	$V_5(14762, 10019, 4744)_{3^{15}}$	$U_5(16, 15, 2)_3$
$(236192, 59046, 344430)_{3^5}$	$(236192, 59046, 543618)_{3^5}$	2	4	$A_4(236192, 29520, 37042)_3$	$V_4(21472, 2952, 18521)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	4	$A_5(236192, 181170, 6712)_3$	$V_5(21472, 18117, 3356)_{3^{10}}$	$U_5(11, 10, 2)_3$
$(236192, 59046, 344430)_{3^5}$	$(236192, 411856/5, 344462)_{3^5}$	2	4	$A_2(236192, 16, 114810)_3$		
		2	4	$A_3(236196, 67440, 38274)_3$	$V_3(13122, 6744, 6379)_{3^{10}}$	$U_3(18, 10, 6)_3$
		2	4	$A_4(236192, 150940, 12758)_3$	$V_4(21472, 15094, 6379)_{3^{10}}$	$U_4(11, 10, 2)_3$
		2	4	$A_5(236192, 193460, 4254)_3$	$V_5(21472, 19346, 2127)_{3^{10}}$	$U_5(11, 10, 2)_3$

каскадных кодов в метрике Хэмминга. Кроме того, Астола привел в [5] таблицу параметров каскадных кодов в метрике Ли для значений $q \in \{25, 81, 243\}$. Коды были построены каскадным способом на основе известной конструкции Юстесена (см. ссылки в [5]). В табл. 1 приведены параметры кодов из [5], а также параметры кодов, построенных с помощью теоремы 8. Для построения внешних кодов A_i использовались либо коды с наилучшими известными параметрами [18], либо коды A_i, построенные простой каскадной конструкцией из внешних кодов V_i с параметрами $(n_{v,i}, N_{v,i}, d_{v,i})_{q^\ell}$ и внутренних кодов U_i с параметрами $(n_{u,i}, k_{u,i}, d_{u,i})_p$. Под простой каскадной конструкцией на основе $(n_v, N_v, d_v)_{q_v}$-кода V и $(n_u, N_u, d_u)_{q_u}$-кода U понимается замена в каждом слове кода V каждого символа алфавита кода V на слово кода U, которое поставлено ему во взаимно-однозначное соответствие. В результате получается новый код A над алфавитом кода U мощности $N = N_v$ и длины $n = n_v n_u$ с минимальным расстоянием (Хэмминга) $d \geqslant d_v d_u$. В табл. 1 для построения внешних кодов A_i в основном использовались МДР-коды и коды из [18]. Для каждого кода Астолы [5] с параметрами $(n_a, N_a = q^{k_a}, d_a)_q$ мы строим два кода: код с параметрами $(n_a, k_a, d)_q$, фиксируя k_a при заданном n_a, и код с параметрами $(n_a, k, d_a)_q$, фиксируя d_a при заданном n_a. Для всех новых кодов приведены все внешние коды A_i, а также коды V_i и U_i, на основе которых строятся эти коды A_i. В случаях, когда $n_v n_u$ больше, чем нужное нам n, мы используем общеизвестные методы укорочения кодов: выбрасывание лишних позиций (уменьшая n и d) или укорочение фиксированием символов выбранных позиций (уменьшая n и k). Если результирующий код C над $\mathbb{F}_{p^s}$ имеет мощность $N = p^k$, где k не делится на s, то для удобства сравнения с кодами из [5] в табл. 1 используются дробные числа k/s для числа информационных символов кода C.

СПИСОК ЛИТЕРАТУРЫ

1. *Zinoviev D.V., Zinoviev V.A.* On Generalized Concatenated Construction of Codes in Metrics Lee L and L_1 // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2018). Svetlogorsk, Kaliningrad region, Russia. Sept. 2–8, 2018. P. 62–65. Available at https://www.dropbox.com/s/h7u89lh8vyirww9.
2. *Berlekamp E.R.* Negacyclic Codes for the Lee Metric // Proc. Conf. on Combinatorial Mathematics and Its Applications. Chapel Hill, NC. Apr. 10–14, 1967. Chapel Hill: Univ. of North Carolina Press, 1968. Ch. 17. P. 298–316. Reprinted in: *Berlekamp E.R.* Algebraic Coding Theory. Rev. Ed. Singapore: World Sci., 2015. Ch. 9. P. 207–217. https://doi.org/10.1142/9789814635905_0009
3. *Chiang J.C., Wolf J.K.* On Channels and Codes for the Lee Metric // Inform. Control. 1971. V. 19. № 2. P. 159–174. https://doi.org/10.1016/S0019-9958(71)90791-1
4. *Мазур Л.Е.* Коды, исправляющие ошибки большого веса в метрике Ли // Пробл. передачи информ. 1973. Т. 9. № 4. С. 11–16. http://mi.mathnet.ru/ppi917
5. *Astola J.* Concatenated Codes for the Lee Metric // IEEE Trans. Inform. Theory. 1982. V. 28. № 5. P. 778–779. https://doi.org/10.1109/TIT.1982.1056550
6. *Racsmány A.* On Constructing Codes with Given Distance in Lee-Metric // Probl. Control Inform. Theory. 1986. V. 15. № 5. P. 377–384.
7. *Давыдов В.А.* Коды, исправляющие ошибки в модульной метрике, метрике Ли и ошибки оператора // Пробл. передачи информ. 1993. Т. 29. № 3. С. 10–20. http://mi.mathnet.ru/ppi184
8. *Давыдов В.А.* О применении модульной метрики к решению задачи декодирования по минимуму евклидового расстояния // Пробл. передачи информ. 2019. Т. 55. № 2. С. 50–57. https://doi.org/10.1134/S0134347519020037
9. *Ericson T., Zinoviev V.* Spherical Codes Generated by Binary Partitions of Symmetric Pointsets // IEEE Trans. Inform. Theory. 1995. V. 41. № 1. P. 107–129. https://doi.org/10.1109/18.370114
10. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670

11. *Dumer I., Zinoviev V., Zyablov V.* Concatenated Decoding According to Minimal Generalized Distance // Probl. Control Inform. Theory. 1981. V. 10. № 1. P. 3–19.
12. *Зиновьев В.А., Зяблов В.В.* Исправление пакетов ошибок и независимых ошибок обобщенными каскадными кодами // Пробл. передачи информ. 1979. Т. 15. № 2. С. 58–70. http://mi.mathnet.ru/ppi1488
13. *Зиновьев В.А., Зяблов В.В.* Коды с неравной защитой информационных символов // Пробл. передачи информ. 1979. Т. 15. № 3. С. 50–60. http://mi.mathnet.ru/ppi1499
14. *Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319. https://doi.org/10.1109/18.312154
15. *Krotov D.S.* Z_4-Linear Hadamard and Extended Perfect Codes // Electron. Notes Discrete Math. 2001. V. 6. P. 107–112. https://doi.org/10.1016/S1571-0653(04)00161-1
16. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
17. *Krotov D.S., Villanueva M.* Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-Linear Hadamard Codes and Their Automorphism Groups // IEEE Trans. Inform. Theory. 2015. V. 61. № 2. P. 887–894. https://doi.org/10.1109/TIT.2014.2379644
18. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available online at http://www.codetables.de (accessed on Oct. 9, 2018).

Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
28.12.2019
После доработки
10.02.2021
Принята к публикации
10.02.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 2021 Вып. 1

УДК 621.391 : 519.725 : 512.772.7

© 2021 г. **Н. Патанкер, С.К. Сингх**

АФФИННЫЕ ЭВАЛЮАЦИОННЫЕ КОДЫ ПО ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Оценивается минимальное расстояние примарных мономиальных аффинных эвалюационных кодов, построенных по гиперэллиптической кривой $x^5 + x - y^2$ над $\mathbb{F}_7$. Для оценки минимального расстояния этих кодов применяются символьные вычисления на основе техники, предложенной Гейлом и Озбудаком. Для некоторых из этих кодов также вычислено расстояние по парам символов. Кроме того, получены нижние границы на обобщенные веса Хэмминга построенных кодов. Предложенный метод вычисления обобщенных весов Хэмминга можно применять к любым примарным мономиальным аффинным эвалюационным кодам.

Ключевые слова: аффинные эвалюационные коды, базис Грёбнера, гиперэллиптическая кривая, обобщенные веса Хэмминга, расстояние по парам символов.

DOI: 10.31857/S0555292321010058

§ 1. Введение

Аффинные эвалюационные коды (affine variety codes) являются специальным классом кодов, исправляющих ошибки. Они получаются с помощью вычисления значений (эвалюации) элементов координатного кольца аффинного многообразия в $\mathbb{F}_q$-рациональных точках этого многообразия. В [1] было показано, что любой линейный код над $\mathbb{F}_q$ можно представить как аффинный эвалюационный код. Таким образом, класс аффинных эвалюационных кодов содержит в себе весь класс линейных кодов.

Длина и размерность аффинного эвалюационного кода определяются очень легко, однако не существует общего простого метода, который позволил бы определить минимальное расстояние таких кодов. В работе [2] для оценки минимального расстояния аффинных эвалюационных кодов были переформулированы граница Фенга – Рао и граница из [3]. Там же с помощью техники базисов Грёбнера и понятия правильно устроенного (well-behaving) базиса и односторонне правильно устроенной (ОПУ) упорядоченной пары мономов была получена нижняя граница на минимальное расстояние аффинных эвалюационных кодов. В [4] Гейл и Озбудак рассматривали примарные мономиальные аффинные эвалюационные коды по кварткe Клейна с фиксированным взвешенным лексикографическим порядком. Для таких кодов с помощью некоторых компонентов алгоритма Бухбергера и полного перебора некоторых специальных случаев были получены более точные оценки минимального расстояния. Авторы предположили, что такой метод можно применять к любым примарным мономиальным аффинным эвалюационным кодам, причем основной упор был сделан на поиск новых семейств хороших аффинных эвалюационных кодов с хорошими параметрами. Также авторы предложили обобщить их

метод на вычисление высших весов. В настоящей статье мы применяем процедуру, предложенную в [4], для оценки минимального расстояния и обобщенных весов Хэмминга примарных кодов по гиперэллиптической кривой. Для заданной размерности k некоторые полученные таким образом коды являются наилучшими. В [5] с помощью подобной процедуры исследовались примарные коды по кривой типа Клейна $x^2y + y^2 + x$ над $\mathbb{F}_4$.

Важными параметрами кода являются его обобщенные веса Хэмминга [6]. Эти параметры полностью характеризуют поведение кода в канале с подслушиванием типа II. В настоящей статье техника Гейла и Озбудака из [4] распространяется на вычисление обобщенных весов Хэмминга построенных кодов. Еще одним параметром кода является его расстояние по парам символов (symbol-pair distance). Кодирование для пар символов было введено для работы с каналами, на выходе которых появляются перекрывающиеся пары символов. Для некоторых из построенных кодов мы вычисляем точное значение расстояния по парам символов.

Статья организована следующим образом. В § 2 напоминаются определения следа (footprint) идеала и примарных аффинных эвалюационных кодов, а также некоторые относящиеся к этому результаты. В § 3 процедура, предложенная в [4], применяется для вычисления веса Хэмминга различных возможных кодовых слов любого примарного мономиального аффинного эвалюационного кода, построенного по гиперэллиптической кривой $x^5 + x - y^2$ над полем $\mathbb{F}_7$. Получаемые таким образом границы лучше границ, получаемых методами работы [2]. В § 4 строятся примарные мономиальные аффинные эвалюационные коды над $\mathbb{F}_7$. Кроме того, для некоторых из этих кодов вычисляется расстояние по парам символов. В § 5 выводятся нижние границы на обобщенные веса Хэмминга построенных кодов. За исключением нескольких случаев получаемые таким образом границы нетривиальны.

§ 2. Предварительные сведения

Всюду далее через q будем обозначать степень простого числа p.

В этом параграфе дается определение примарных мономиальных аффинных эвалюационных кодов и напоминается известный результат о минимальном расстоянии аффинных эвалюационных кодов. Начнем с определения следа идеала кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

Пусть $\prec$ – фиксированный порядок на мономах из кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, и пусть $I \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ – идеал этого кольца. Через $\mathcal{M}(x_1, x_2, \ldots, x_m)$ обозначим множество всех мономов от $x_1, x_2, \ldots, x_m$ над полем $\mathbb{F}_q$.

О п р е д е л е н и е 1 [2, определение 4.2]. Следом идеала I относительно порядка $\prec$ называется множество

$$\Delta_\prec(I) := \{M \in \mathcal{M}(x_1, x_2, \ldots, x_m) \mid M \text{ не является старшим мономом никакого многочлена из } I\}.$$

Всюду далее будем обозначать через $\mathrm{LM}(P)$ старший моном многочлена P. Имеется следующий результат о следе идеала кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

П р е д л о ж е н и е 1 [2, предложение 4.4] или [4, теорема 1]. *Множество*

$$\{M + I \mid M \in \Delta_\prec(I)\}$$

образует базис кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ как векторного пространства над $\mathbb{F}_q$.

Д о к а з а т е л ь с т в о. Пусть $S := \{M + I \mid M \in \Delta_\prec(I)\}$. Рассмотрим произвольное конечное подмножество $B \subset S$, тогда

$$f := \sum_{M_\alpha + I \in B} a_\alpha (M_\alpha + I) = 0,$$

где $a_\alpha \in \mathbb{F}_q$. Тогда $\mathrm{LM}(f) \in \langle \mathrm{LM}(I)\rangle$, откуда следует, что $a_\alpha = 0$ для всех α. Таким образом, множество S линейно независимо над $\mathbb{F}_q$. Кроме того, пусть G – базис Грёбнера идеала I, а $g \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$. Тогда согласно алгоритму деления имеем $g = h + r$, где $h \in I$ и $r = 0$ или $r \in \Delta_\prec(I)$. Если $r = 0$, то $g + I = 0 + I \in \mathrm{Span}_{\mathbb{F}_q} S$. Если же $r \neq 0$, то $g - r = h \in I$. Таким образом, $g + I = r + I \in \mathrm{Span}_{\mathbb{F}_q} S$, что и доказывает предложение. ▲

Как следствие этого предложения, получаем следующий результат.

Следствие 1 [2, следствие 4.5]. *Пусть $f_1, f_2, \ldots, f_s \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$. Количество общих нулей многочленов $f_1, f_2, \ldots, f_s$ над $\mathbb{F}_q$ равно*

$$\#\Delta_\prec(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle).$$

Доказательство. Пусть $I_q := \langle f_1, \ldots, f_s, x_1^q - x_1, \ldots, x_m^q - x_m\rangle$. Положим $R := \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I_q$. Пусть $Q_1, Q_2, \ldots, Q_z$ – общие нули многочленов $f_1, f_2, \ldots, f_s$ в поле $\mathbb{F}_q$. Рассмотрим отображение

$$\varphi\colon R \to \mathbb{F}_q^z, \quad \varphi(g + I_q) = (g(Q_1), g(Q_2), \ldots, g(Q_z)).$$

Тогда φ является изоморфизмом векторных пространств над $\mathbb{F}_q$. Так как изоморфные векторные пространства имеют одинаковую размерность, то из предложения 1 вытекает, что $z = \#\Delta_\prec(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, \ldots, x_m^q - x_m\rangle)$. ▲

Предложение 2 [4, следствие 1]. *Пусть $I_q := I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle$. Тогда размер (мощность) многообразия, соответствующего I_q, равен $\#\Delta_\prec(I_q)$.*

Пусть $\boldsymbol{V}_{\mathbb{F}_q}(I_q) := \{P_1, P_2, \ldots, P_n\}$, где $P_i \neq P_j$ при $i \neq j$.

Определение 2 [4, определение 2]. *В тех же обозначениях, что и выше, выберем $L \subseteq \Delta_\prec(I_q)$. Тогда*

$$C(I, L) := \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(M + I_q) := (M(P_1), M(P_2), \ldots, M(P_n)) \mid M \in L\}$$

называется примарным мономиальным аффинным эвалюационным кодом.

Из вышесказанного немедленно видно, что $C(I, L)$ является линейным кодом над полем $\mathbb{F}_q$ длины $n := \#\boldsymbol{V}_{\mathbb{F}_q}(I_q) = \#\Delta_\prec(I_q)$ и размерности $k = \#L$.

2.1. Граница на минимальное расстояние аффинных эвалюационных кодов. В работе [2] минимальное расстояние аффинных эвалюационных кодов оценивалось с помощью понятия односторонне правильно устроенной пары мономов, которое будет определено ниже. Вначале напомним определение аффинного эвалюационного кода.

Определение 3. Для тех же I_q и $P_1, P_2, \ldots, P_n$, что и в определении 2, и для подпространства $L' \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ аффинным эвалюационным кодом $C(I, L')$ назовем множество

$$C(I, L') := \{\mathrm{ev}(f + I_q) = (f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L'\}.$$

Всюду далее через $P \operatorname{rem} G$ будем обозначать остаток от деления многочлена P на G.

Определение 4 [2, определение 4.6]. Базис $\{b_1 + I_q, b_2 + I_q, \ldots, b_{\dim(L')} + I_q\}$ подпространства $L' \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, такой что $\mathrm{supp}(b_i) \subseteq \Delta_\prec(I_q)$ для $i = 1, 2, \ldots, \dim(L')$ и $\mathrm{LM}(b_1) \prec \mathrm{LM}(b_2) \prec \ldots \prec \mathrm{LM}(b_{\dim(L')})$, будем называть правильно устроенным относительно порядка $\prec$.

Определение 5 [2, определение 4.8]. Пусть G – базис Грёбнера для I_q относительно порядка $\prec$. Упорядоченная пара мономов (M_1, M_2), где $M_1, M_2 \in \Delta_\prec(I_q)$,

называется односторонне правильно устроенной (ОПУ), если $\forall\, h \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, такого что $\operatorname{supp}(h) \subseteq \Delta_\prec(I_q)$ и $\operatorname{LM}(h) = M_1$, выполняется

$$\operatorname{LM}(M_1 M_2 \operatorname{rem} G) = \operatorname{LM}(hM_2 \operatorname{rem} G).$$

Следующий результат задает границу на минимальное расстояние аффинного эвалюационного кода.

Т е о р е м а 1 [2, теорема 4.9]. *Пусть порядок $\prec$ фиксирован. Минимальное расстояние кода $C(I, L')$ не меньше, чем*

$$\min\bigl\{\#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q),\ \textit{такое что } (P, N) \textit{ – ОПУ пара}\\ \textit{и } \operatorname{LM}(PN \operatorname{rem} G) = K\} \mid P \in \{\operatorname{LM}(b_1), \operatorname{LM}(b_2), \ldots, \operatorname{LM}(b_{\dim(L')})\}\bigr\},$$

где $\{b_1 + I_q, \ldots, b_{\dim(L')} + I_q\}$ – любой правильно устроенный базис подпространства L'.

Д о к а з а т е л ь с т в о. Пусть $\boldsymbol{x} = \operatorname{ev}(f + I_q) \in C(I, L')$ для некоторого $f \in L'$. Положим $P := \operatorname{LM}(f) \in \{\operatorname{LM}(b_1), \operatorname{LM}(b_2), \ldots, \operatorname{LM}(b_{\dim(L')})\}$. Далее, если существует $N \in \Delta_\prec(I_q)$, такое что (P, N) – ОПУ пара и $\operatorname{LM}(PN \operatorname{rem} G) = K$, то

$$K \in \Delta_\prec(I_q) \setminus \Delta_\prec(\langle f\rangle + I_q).$$

Тогда согласно следствию 1

$$w_H(\boldsymbol{x}) = n - \#\Delta_\prec(\langle f\rangle + I_q) = \#\Delta_\prec(I_q) - \#\Delta_\prec(\langle f\rangle + I_q) \geqslant\\ \geqslant \{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q),\ \text{такое что } (P, N) \text{ – ОПУ пара}\\ \text{и } \operatorname{LM}(PN \operatorname{rem} G) = K\},$$

откуда следует требуемый результат. ▲

§ 3. Веса кодовых слов примарных мономиальных аффинных эвалюационных кодов

В начале этого параграфа напомним технику, использовавшуюся в [4] для определения весов кодовых слов примарного мономиального аффинного эвалюационного кода, построенного по кривой Клейна над $\mathbb{F}_8$. Затем применим эту технику для нахождения весов кодовых слов примарных мономиальных аффинных эвалюационных кодов, построенных по конкретной гиперэллиптической кривой над $\mathbb{F}_7$.

Пусть $C(I, L)$ – примарный мономиальный аффинный эвалюационный код, определенный в § 2. Для кодового слова $\boldsymbol{c} := \operatorname{ev}(f + I_q) \in C(I, L)$, где $f \in \operatorname{Span}_{\mathbb{F}_q} L$, из следствия 1 известно, что вес Хэмминга слова $\boldsymbol{c}$ равен

$$w_H(\boldsymbol{c}) = n - \#\Delta_\prec(\langle f\rangle + I_q) = \#\Delta_\prec(I_q) \cap \operatorname{LM}(\langle f\rangle + I_q) =: \#\square_\prec(f),$$

где $\operatorname{LM}(g)$ – старший моном многочлена g относительно порядка $\prec$. Техника из [4] состоит в том, что нижнюю границу на $w_H(\boldsymbol{c})$ можно получить, добавляя мономы в множество $\square_\prec(f)$.

По теореме 1, если $P := \operatorname{LM}(f)$ и $N, K \in \Delta_\prec(I_q)$ удовлетворяют условию

$$(P, N) \text{ – ОПУ пара и } \operatorname{LM}(PN \operatorname{rem} G) = K,$$

то $K \in \square_\prec(f)$.

В настоящей статье мы сперва находим ОПУ пары и получаем элементы множества $\square_\prec(f)$ для различных выборов многочлена $f \in \operatorname{Span}_{\mathbb{F}_q} L$. Затем мы пытаемся добавить в $\square_\prec(f)$ больше мономов, используя технику из [4]. Получаемая таким

образом граница на минимальное расстояние кодовых слов кода $C(I, L)$ иногда оказывается строго лучше, чем граница из теоремы 1.

Прежде чем приступить к этому, введем понятие взвешенного лексикографического порядка на мономах из кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

Определение 6 [2, определение 4.17]. Пусть $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}$ заданы. Определим вес монома $x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}$ как

$$w(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) := i_1 w(x_1) + i_2 w(x_2) + \ldots + i_m w(x_m).$$

Взвешенный лексикографический порядок $\prec_w$ на мономах из $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ определяется следующим образом: $x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \prec_w x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}$, если либо

$$w(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) < w(x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}),$$

либо

$$w(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) = w(x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}), \quad \text{но} \quad x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \prec_{\text{lex}} x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m},$$

где $\prec_{\text{lex}}$ – обычный лексикографический порядок, такой что $x_m \prec_{\text{lex}} \ldots \prec_{\text{lex}} x_1$.

3.1. Веса кодовых слов по гиперэллиптической кривой. Пусть $I = \langle x^5 + x - y^2 \rangle$ – идеал кольца $\mathbb{F}_7[x, y]$, и следовательно, $I_7 = \langle x^5 + x - y^2, x^7 - x, y^7 - y \rangle$. Соответствующее множество $\mathbb{F}_7$-рациональных точек этого многообразия имеет вид

$$\{(0,0), (1,3), (1,4), (3,1), (3,6), (5,1), (5,6)\}.$$

Зафиксируем порядок на мономах из кольца $\mathbb{F}_7[x, y]$ как взвешенный лексикографический порядок $\prec_w$, в котором $w(x) = 2$, $w(y) = 5$, причем $y \prec_{\text{lex}} x$ в обычном лексикографическом порядке. С помощью системы компьютерной алгебры SageMath находим базис Грёбнера идеала I_7 относительно порядка $\prec_w$:

$$\{x^3y - 2x^2y + 2xy - y, y^2 - 2x^3 + 3x^2 - 3x, x^4 - 2x^3 + 2x^2 - x\}.$$

Элементы следа $\Delta_{\prec_w}(I_7)$ и соответствующие им веса перечислены в следующей таблице:

1	y	x	xy	x^2	x^2y	x^3
0	5	2	7	4	9	6

.

В дальнейших пунктах мы будем оценивать мощность множества $\square_{\prec_w}(f)$, следуя технике из [4]. По очереди рассмотрим шесть различных возможных кодовых слов, получаемых из многочленов со старшими мономами из $\Delta_{\prec_w}(I_7)$.

Перед этим зафиксируем одно обозначение. Рассмотрим многочлены $a(x, y)$, $b(x, y)$ и $c(x, y)$. Запись

$$a(x, y) \xrightarrow{b(x,y)} c(x, y)$$

будет означать, что $c(x, y) = a(x, y) - s(x, y)b(x, y)$ для некоторого многочлена $s(x, y)$.

3.1.1. Старший моном, равный x: Рассмотрим слово $\boldsymbol{c} = \text{ev}(f + I_7)$, где $f = x + a_0$, $a_0 \in \mathbb{F}_7$. Проверка показывает, что $\{(x, 1), (x, x), (x, x^2), (x, y), (x, xy)\}$ – ОПУ пары. Таким образом,

$$\{x, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 5$. При этом слово $\text{ev}((x - 1) + I_7)$ имеет вес 5. Значит, в этом случае граница точна.

3.1.2. Старший моном, равный x^2: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = x^2 + a_1x + a_0$, $a_1, a_0 \in \mathbb{F}_7$. Проверка показывает, что $\{(x^2, 1), (x^2, x), (x^2, y)\}$ – ОПУ пары. Таким образом,

$$\{x^2, x^3, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 3$. При этом слово $\mathrm{ev}((x-1)(x-3))$ имеет вес 3. Значит, в этом случае граница точна.

3.1.3. Старший моном, равный y: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = y + a_1x^2 + a_2x + a_3$, $a_1, a_2, a_3 \in \mathbb{F}_7$. Проверка показывает, что $\{(y, 1), (y, x), (y, x^2), (y, x^3)\}$ – ОПУ пары. Таким образом,

$$\{y, xy, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 3$. Теперь рассмотрим редукцию

$$yf \xrightarrow{y^2 - 2x^3 + 3x^2 - 3x} a_1x^2y + a_2xy + 2x^3 + a_3y - 3x^2 + 3x.$$

Если $a_1 \neq 0$, то

$$a_1x^2y + a_2xy + 2x^3 + a_3y - 3x^2 + 3x \xrightarrow{x^2 f}$$
$$\xrightarrow{x^2 f} -a_1^2x^4 + a_2xy + (2 - a_1a_2)x^3 + a_3y + (-3 - a_1a_3)x^2 + 3x \xrightarrow{x^4 - 2x^3 + 2x^2 - x}$$
$$\xrightarrow{x^4 - 2x^3 + 2x^2 - x} a_2xy + (2 - a_1a_2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2)x^2 + (3 - a_1^2)x.$$

Если $a_2 \neq 0$, то

$$a_2xy + (2 - a_1a_2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2)x^2 + (3 - a_1^2)x \xrightarrow{f}$$
$$\xrightarrow{f} (2 - 2a_1a_2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2 - a_2^2)x^2 + (3 - a_1^2 - a_2a_3)x.$$

Если $1 - a_1a_2 - a_1^2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $a_2 = a_1^{-1} - a_1$, и тогда остается

$$a_3y + (-1 - a_1a_3 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2 - a_1^{-1}a_3 + a_1a_3)x.$$

Теперь, если $a_3 \neq 0$, то

$$a_3y + (-1 - a_1a_3 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2 - a_1^{-1}a_3 + a_1a_3)x \xrightarrow{f}$$
$$\xrightarrow{f} (-1 - 2a_1a_3 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2 - 2a_1^{-1}a_3 + 2a_1a_3)x - a_3^2.$$

Если при этом $a_3 \neq 4a_1 - 4a_1^{-3} - 4a_1^{-1}$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $(1 + a_1^{-4})x - a_3^2$, тогда $\{x, x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

А если $a_3 = 0$, то остается $(-1 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2)x$, и $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

Если же $a_2 = 0$, то остается $(2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2)x^2 + (3 - a_1^2)x$. Если $a_1^2 \neq 1$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $a_1 \in \{1, 6\}$, и тогда имеется два случая:

Если $a_1 = 1$, то остается $a_3y + (-1 - a_3)x^2 + 2x$. Если $a_3 \neq 0$, то с помощью f получаем $(-1 - 2a_3)x^2 + 2x - a_3^2$. Теперь, если $a_3 \neq 3$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $2x - 2$, и таким образом, $\{x, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Но если $a_3 = 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

Если же $a_1 = 6$, то остается $a_3y + (-1 - 6a_3)x^2 + 2x$. Если $a_3 \neq 0$, то с помощью f получаем $(-1 - 5a_3)x^2 + 2x - a_3^2$. Теперь, если $a_3 \neq 4$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $2x - 2$, и таким образом, $\{x, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Но если $a_3 = 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

Далее, если $a_1 = 0$, то остается $a_2xy + 2x^3 + a_3y - 3x^2 + 3x$. Если $a_2 \neq 0$, то применяем редукцию

$$a_2xy + 2x^3 + a_3y - 3x^2 + 3x \xrightarrow{f} 2x^3 + a_3y + (-3 - a_2^2)x^2 + (3 - a_2a_3)x.$$

Таким образом, $x^3 \in \square_{\prec_w}(f)$. В противном случае, если $a_2 = 0$, то $x^3 \in \square_{\prec_w}(f)$.

Из всех этих вычислений следует, что в множестве $\square_{\prec_w}(f)$ содержится по крайней мере $3 + \min\{2, 3, 4, 2, 1, 2, 1, 1\} = 4$ элемента. Следовательно, $w_H(\boldsymbol{c}) \geqslant 4$.

3.1.4. Старший моном, равный $\boldsymbol{x^3}$: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = x^3 + a_3y + a_2x^2 + a_1x + a_0$, $a_3, a_2, a_1, a_0 \in \mathbb{F}_7$. Проверка показывает, что $\{(x^3, 1)\}$ – ОПУ пара. Таким образом,

$$\{x^3\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 1$. При этом слово $\mathrm{ev}((x-1)(x-3)(x-5) + I_7)$ имеет вес 1. Значит, в этом случае граница точна.

3.1.5. Старший моном, равный $\boldsymbol{xy}$: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = xy + a_4x^3 + a_3y + a_2x^2 + a_1x + a_0$, $a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_7$. Проверка показывает, что $\{(xy, 1), (xy, x)\}$ – ОПУ пары. Таким образом,

$$\{xy, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 2$. При этом слово $\mathrm{ev}((xy + 3x^3 + 2y + 6x^2 + I_7))$, как и некоторые другие кодовые слова, имеет вес 2. Значит, в этом случае граница точна.

3.1.6. Старший моном, равный $\boldsymbol{x^2y}$: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = x^2y + a_5xy + a_4x^3 + a_3y + a_2x^2 + a_1x + a_0$, $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_7$. Проверка показывает, что $\{(x^2y, 1)\}$ – ОПУ пара. Таким образом,

$$\{x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 1$. Теперь попробуем добавить в множество $\square_{\prec_w}(f)$ больше мономов при различных условиях на коэффициенты многочлена f.

Рассмотрим многочлен $xf = x^3y + a_5x^2y + a_4x^4 + a_3xy + a_2x^3 + a_1x^2 + a_0x$. Применим редукцию

$$xf \xrightarrow{x^3y - 2x^2y + 2xy - y} (a_5 + 2)x^2y + a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x.$$

Если $a_5 \neq 5$, то, продолжая редукцию, получаем

$$\begin{aligned}&(a_5 + 2)x^2y + a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x \xrightarrow{f}\\ &\xrightarrow{f} a_4x^4 + (a_3 - 2 - a_5^2 - 2a_5)xy + (a_2 - a_4a_5 - 2a_4)x^3 + (1 - a_3a_5 - 2a_3)y +\\ &+ (a_1 - a_2a_5 - 2a_2)x^2 + (a_0 - a_1a_5 - 2a_1)x - (a_5 + 2)a_0.\end{aligned}$$

Если при этом $a_4 \neq 0$, то, продолжая редукцию, получаем

$$\begin{aligned}&a_4x^4 + (a_3 - 2 - a_5^2 - 2a_5)xy + (a_2 - a_4a_5 - 2a_4)x^3 + (1 - a_3a_5 - 2a_3)y +\\ &+ (a_1 - a_2a_5 - 2a_2)x^2 + (a_0 - a_1a_5 - 2a_1)x - (a_5 + 2)a_0 \xrightarrow{x^4 - 2x^3 + 2x^2 - x}\\ &\xrightarrow{x^4 - 2x^3 + 2x^2 - x} (a_3 - 2 - a_5^2 - 2a_5)xy + (a_2 - a_4a_5)x^3 + (1 - a_3a_5 - 2a_3)y +\\ &+ (a_1 - a_2a_5 - 2a_2 - 2a_4)x^2 + (a_0 - a_1a_5 - 2a_1 + a_4)x - (a_5 + 2)a_0.\end{aligned}$$

Теперь рассмотрим различные случаи в зависимости от значения коэффициента a_5:

Если $a_5 = 0$, то остается

$$(a_3 - 2)xy + a_2x^3 + (1 - 2a_3)y + (a_1 - 2a_2 - 2a_4)x^2 + (a_0 - 2a_1 + a_4)x - 2a_0.$$

Если $a_3 \neq 2$, то $\{xy\} \subseteq \square_{\prec_w}(f)$. В противном случае остается

$$a_2x^3 + 4y + (a_1 - 2a_2 - 2a_4)x^2 + (a_0 - 2a_1 + a_4)x - 2a_0.$$

Если теперь $a_2 \neq 0$, то $\{x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае $\{y\} \subseteq \square_{\prec_w}(f)$.

Если $a_5 = 1$, то остается

$$(a_3 - 5)xy + (a_2 - a_4)x^3 + (1 - 3a_3)y + (a_1 - 3a_2 - 2a_4)x^2 + (a_0 - 3a_1 + a_4)x - 3a_0.$$

Если теперь $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 - a_4)x^3 + (a_1 - 3a_2 - 2a_4)x^2 + (a_0 - 3a_1 + a_4)x - 3a_0.$$

Если при этом $a_2 \neq a_4$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае остается $(a_1 - 5a_2)x^2 + + (a_0 - 3a_1 + a_2)x - 3a_0$. Тогда, если $a_1 \neq 5a_2$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$, а в противном случае остается $a_0x - 3a_0$. Если $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 1$.

Если $a_5 = 2$, то остается

$$(a_3 - 3)xy + (a_2 - 2a_4)x^3 + (1 - 4a_3)y + (a_1 - 4a_2 - 2a_4)x^2 + \\ + (a_0 - 4a_1 + a_4)x - 4a_0.$$

Если теперь $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 - 2a_4)x^3 + 3y + (a_1 - 4a_2 - 2a_4)x^2 + (a_0 - 4a_1 + a_4)x - 3a_0.$$

Если при этом $a_2 \neq 2a_4$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если $a_5 = 3$, то остается

$$(a_3 - 3)xy + (a_2 - 3a_4)x^3 + (1 - 5a_3)y + (a_1 - 5a_2 - 2a_4)x^2 + \\ + (a_0 - 5a_1 + a_4)x - 5a_0.$$

Если $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 - 3a_4)x^3 + (a_1 - 5a_2 - 2a_4)x^2 + (a_0 - 5a_1 + a_4)x - 5a_0.$$

Тогда $x^3 \in \square_{\prec_w}(f)$, если $a_2 \neq 3a_4$. А если $a_2 = 3a_4$, то остается

$$(a_1 - 3a_4)x^2 + (a_0 - 5a_1 + a_4)x - 5a_0.$$

Если при этом $a_1 \neq 3a_4$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $a_0x - 5a_0$. Если $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 1$.

Если $a_5 = 4$, то

$$(a_3 - 5)xy + (a_2 - 4a_4)x^3 + (1 + a_3)y + (a_1 - 6a_2 - 2a_4)x^2 + (a_0 - 6a_1 + a_4)x + a_0.$$

Если $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае, если к тому же $a_2 \neq 4a_4$, то $x^3 \in \square_{\prec_w}(f)$, а в противном случае $\{y, xy\} \subseteq \square_{\prec_w}(f)$.

Наконец, если $a_5 = 6$, то остается

$$(a_3 - 1)xy + (a_2 - 6a_4)x^3 + (1 - a_3)y + (a_1 - a_2 - 2a_4)x^2 + (a_0 - a_1 + a_4)x - a_0.$$

Если $a_3 \neq 1$, то $xy \in \square_{\prec_w}(f)$. В противном случае, если $a_2 \neq 6a_4$, то $x^3 \in \square_{\prec_w}(f)$. В случае $a_2 = 6a_4$, если $a_1 \neq a_4$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. А если $a_1 = a_4$ и $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае $w_H(c) \geqslant 1$.

Если же $a_4 = 0$, то остается

$$(a_3 - 2 - a_5^2 - 2a_5)xy + a_2x^3 + (1 - a_3a_5 - 2a_3)y + (a_1 - a_2a_5 - 2a_2)x^2 + \\ + (a_0 - a_1a_5 - 2a_1)x - (a_5 + 2)a_0.$$

Теперь рассмотрим различные случаи в зависимости от значения коэффициента a_5:

Если $a_5 = 0$, то остается

$$(a_3 - 2)xy + a_2x^3 + (1 - 2a_3)y + (a_1 - 2a_2)x^2 + (a_0 - 2a_1)x - 2a_0.$$

Если $a_3 \neq 2$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 2$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если $a_5 = 1$, то остается

$$(a_3 - 5)xy + a_2x^3 + (1 - 3a_3)y + (a_1 - 3a_2)x^2 + (a_0 - 3a_1)x - 3a_0.$$

Если $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 5$, и если при этом $a_2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. Если же $a_2 = 0$ и $a_1 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$, а в противном случае остается $a_0x - 3a_0$. Если теперь $a_0 \neq 0$, то $\{x, xy, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 2$.

Если $a_5 = 2$, то остается

$$(a_3 - 3)xy + a_2x^3 + (1 - 4a_3)y + (a_1 - 4a_2)x^2 + (a_0 - 4a_1)x - 4a_0.$$

Если $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 5$, и если при этом $a_2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если $a_5 = 3$, то остается

$$(a_3 - 3)xy + a_2x^3 + (1 - 5a_3)y + (a_1 - 5a_2)x^2 + (a_0 - 5a_1)x - 5a_0.$$

Если $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 3$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $a_2 = 0$, и если при этом $a_1 \neq 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Если же $a_1 = 0$ и $a_0 \neq 0$, то $\{x, xy, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 2$.

Если $a_5 = 4$, то остается

$$(a_3 - 5)xy + a_2x^3 + (1 - 6a_3)y + (a_1 - 6a_2)x^2 + (a_0 - 6a_1)x + a_0.$$

Если $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 5$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $\{y, xy\} \subseteq \square_{\prec_w}(f)$.

Наконец, если $a_5 = 6$, остается

$$(a_3 - 1)xy + a_2x^3 + (1 - a_3)y + (a_1 - a_2)x^2 + (a_0 - a_1)x - a_0.$$

Если $a_3 \neq 1$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 1$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $a_2 = 0$, и если при этом $a_1 \neq 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Если же $a_1 = 0$ и $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 2$.

Если же в самом начале было $a_5 = 5$, то остается

$$a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x.$$

Если $a_4 \neq 0$, то продолжим редукцию:

$$a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x \xrightarrow{x^4-2x^3+2x^2-x}$$
$$\xrightarrow{x^4-2x^3+2x^2-x} (a_3 - 2)xy + (a_2 + 2a_4)x^3 + y + (a_1 - 2a_4)x^2 + (a_0 + a_4)x.$$

Если $a_3 \neq 2$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 + 2a_4)x^3 + y + (a_1 - 2a_4)x^2 + (a_0 + a_4)x.$$

Если $a_2 \neq 5a_4$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если же $a_4 = 0$, то остается $(a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x$. Если $a_3 \neq 2$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 2$, и остается $a_2x^3 + y + a_1x^2 + a_0x$. Если при этом $a_2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Из сделанных вычислений мы заключаем, что если $a_5 \neq 5$ и $a_4 \neq 0$, то $w_H(c) \geqslant 1$, а в противном случае $w_H(c) \geqslant 2$.

В результате всех проделанных вычислений получаем следующую таблицу, в которой первая строка состоит из старших мономов различных кодовых слов $\mathrm{ev}(f)$, а во второй строке приведены границы на $\#\square_{\prec_w}(f)$:

1	x	x^2	y	x^3	xy	x^2y
7	5	3	4	1	2	1

.

§ 4. Построение кода

Для $1 \leqslant s \leqslant n$, следуя [4], определим код

$$C := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(M + I_7) \mid M \in \Delta_{\prec_w}(I_7),\ \delta(M) \geqslant s\},$$

где $\delta(M)$ – полученная выше оценка на $\#\square_{\prec_w}(M)$, приведенная в таблице. Параметры кодов с наилучшим возможным минимальным расстоянием таковы:

$$[7, 1, \geqslant 7], \qquad [7, 2, \geqslant 5], \qquad [7, 3, \geqslant 4], \qquad [7, 4, \geqslant 3], \qquad [7, 5, \geqslant 2], \qquad [7, 6, \geqslant 2].$$

Во всех этих случаях для заданного значения кодовой размерности оценка на минимальное расстояние получаемого таким образом кода либо равна наилучшему известному значению согласно таблице из [7], либо лишь на единицу меньше.

4.1. Расстояние по парам символов. Кодирование для пар символов было введено для работы с каналами, на выходе которых появляются перекрывающиеся пары символов. Тем самым, появился новый параметр кодов, называемый расстоянием по парам символов. Расстояние по парам символов для кода определяется следующим образом.

Пусть A – алфавит объема q. Для $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in A^n$ определим его вектор пар символов как

$$\pi_{\mathrm{sp}}(\boldsymbol{x}) := [(x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n), (x_n, x_1)] \in (A^2)^n.$$

Тогда вес вектора $\boldsymbol{x}$ по парам символов определяется как

$$w_{\mathrm{sp}}(\boldsymbol{x}) := w_H(\pi_{\mathrm{sp}}(\boldsymbol{x})) = \#\{1 \leqslant i \leqslant n \mid (x_i, x_{i+1}) \neq (0, 0),\ x_{n+1} = x_1\}.$$

Для двух векторов $\boldsymbol{x}, \boldsymbol{y} \in A^n$ расстояние по парам символов между ними определяется как

$$d_{\mathrm{sp}}(\boldsymbol{x}, \boldsymbol{y}) := d(\pi_{\mathrm{sp}}(\boldsymbol{x}), \pi_{\mathrm{sp}}(\boldsymbol{y})) =$$
$$= \#\{1 \leqslant i \leqslant n \mid (x_i, x_{i+1}) \neq (y_i, y_{i+1}),\ x_{n+1} = x_1,\ y_{n+1} = y_1\}.$$

Пусть C – линейный код над полем $\mathbb{F}_q$. Тогда расстояние по парам символов для кода C определяется как

$$d_{\mathrm{sp}}(C) := \min\{w_{\mathrm{sp}}(\boldsymbol{x}) \mid \boldsymbol{x} \in C,\ \boldsymbol{x} \neq 0\}.$$

Взаимосвязь между минимальным расстоянием Хэмминга кода C и его расстоянием по парам символов описывает следующее

Предложение 3 [8, предложение 1]. *Для $\boldsymbol{x}, \boldsymbol{y} \in A^n$ пусть $0 < d_H(\boldsymbol{x}, \boldsymbol{y}) < n$ – расстояние Хэмминга между $\boldsymbol{x}$ и $\boldsymbol{y}$. Тогда*

$$d_{\mathrm{sp}}(\boldsymbol{x}, \boldsymbol{y}) \geqslant d(\boldsymbol{x}, \boldsymbol{y}) + 1.$$

Доказательство. Положим

$$\mathcal{A}_H := \{1 \leqslant i \leqslant n \mid x_i \neq y_i\}, \quad \mathcal{A}_{\mathrm{sp}} := \{1 \leqslant i \leqslant n \mid (x_i, x_{i+1}) \neq (y_i, y_{i+1})\}.$$

Каждый индекс $i \in \mathcal{A}_H$ принадлежит $\mathcal{A}_{\mathrm{sp}}$. Таким образом, $d_{\mathrm{sp}}(\boldsymbol{x}, \boldsymbol{y}) \geqslant d(\boldsymbol{x}, \boldsymbol{y})$. Поскольку $d(\boldsymbol{x}, \boldsymbol{y}) < n$, найдется по крайней мере одна пара индексов $(i, i+1)$, такая что ровно один из индексов i и $i+1$ принадлежит $\mathcal{A}_H$, пусть это будет, скажем, i. Тогда $(i-1, i)$ и $(i, i+1)$ принадлежат $\mathcal{A}_{\mathrm{sp}}$, откуда вытекает требуемый результат. ▲

Подробнее о расстоянии по парам символов для кодов см. в [8].

Используя предложение 3, получаем следующие результаты о кодах, построенных по гиперэллиптической кривой над полем $\mathbb{F}_7$.

Предложение 4. *Пусть $P_1 := (0, 0)$, $P_2 := (1, 3)$, $P_3 := (1, 4)$, $P_4 := (3, 1)$, $P_5 := (3, 6)$, $P_6 := (5, 1)$ и $P_7 := (5, 6)$ – порядок точек, в которых вычисляются значения для построения кодов. Тогда*

1. *Если*

$$C_1 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1 + I_7), \mathrm{ev}(x + I_7), \mathrm{ev}(x^2 + I_7), \mathrm{ev}(y + I_7)\},$$

то $d_{\mathrm{sp}}(C_1) = 4$;

2. *Если*

$$C_2 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1 + I_7), \mathrm{ev}(x + I_7), \mathrm{ev}(x^2 + I_7), \mathrm{ev}(y + I_7), \mathrm{ev}(xy + I_7), \mathrm{ev}(x^2 y + I_7)\},$$

то $d_{\mathrm{sp}}(C_2) = 3$.

Доказательство. Имеем $d_{\mathrm{sp}}(C_1) \geqslant d(C_1) + 1 = 4$. Для доказательства противоположного неравенства рассмотрим кодовое слово $\mathrm{ev}((x-1)(x-3) + I_7) \in C_1$. Его вес по парам символов равен 4. Таким образом, $d_{\mathrm{sp}}(C_1) \leqslant 4$, откуда следует утверждение 1.

Имеем $d_{\mathrm{sp}}(C_2) \geqslant d(C_2) + 1 = 3$. Далее, кодовое слово $\mathrm{ev}(y(x-1)(x-3) + I_7) \in C_2$ имеет вес по парам символов, равный 3. Таким образом, $d_{\mathrm{sp}}(C_2) \leqslant 3$, откуда следует утверждение 2. ▲

§ 5. Обобщенные веса Хэмминга кодов

Пусть C – $[n, k]$-код над полем $\mathbb{F}_q$. Обобщенные веса Хэмминга для линейных кодов были введены в [9, 10], а затем их независимо переоткрыл Вэй в [6]. Изучение этих параметров мотивировалось некоторыми приложениями в криптографии. Обобщенные веса Хэмминга линейных кодов определяются следующим образом.

Носителем линейного $[n, k]$-кода C над полем $\mathbb{F}_q$ называется множество

$$\mathrm{Supp}\, C := \{i \mid x_i \neq 0 \text{ для некоторого } \boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in C\}.$$

Для $1 \leqslant r \leqslant k$ назовем *r-м обобщенным весом Хэмминга* кода C величину

$$d_r(C) := \min\{\#\operatorname{Supp} D \mid D \text{ является линейным подкодом кода } C \text{ размерности } \dim_{\mathbb{F}_q}(D) = r\}.$$

Важное свойство обобщенных весов Хэмминга кода C описывает следующая

Теорема 2 [6, теорема 1]. *Для линейного $[n,k]$-кода C, такого что $k > 0$, справедливы неравенства*

$$1 \leqslant d_1(C) < d_2(C) < \ldots < d_k(C) \leqslant n.$$

Доказательство. Из определения следует, что $d_{r-1}(C) \leqslant d_r(C)$. Остается показать, что это неравенство строгое. Пусть D – линейный подкод кода C, имеющий размерность r, такой что $d_r(C) = \#\operatorname{Supp}(D)$. Пусть $i \in \operatorname{Supp}(D)$. Рассмотрим множество $D_i := \{(x_1, x_2, \ldots, x_n) \in D \mid x_i = 0\}$. Тогда $\dim_{\mathbb{F}_q}(D_i) = r-1$. Таким образом, $d_{r-1}(C) \leqslant \#\operatorname{Supp} D_i < \#\operatorname{Supp} D = d_r(C)$. ▲

В этом параграфе мы выведем нижние границы на обобщенные веса Хэмминга для кодов, построенных в § 4. Основная идея состоит в следующем.

Пусть C – $[n,k]$-код над полем $\mathbb{F}_q$. Для любого подкода D кода C, имеющего размерность r, $1 \leqslant r \leqslant k$, с базисом над $\mathbb{F}_q$ вида $\operatorname{ev}(g_1 + I_q), \operatorname{ev}(g_2 + I_q), \ldots, \operatorname{ev}(g_r + I_q)$, т.е. $D = \operatorname{Span}_{\mathbb{F}_q}\{\operatorname{ev}(g_1 + I_q), \operatorname{ev}(g_2 + I_q), \ldots, \operatorname{ev}(g_r + I_q)\}$, согласно следствию 1 имеем

$$\begin{aligned}&\#\operatorname{Supp} D = n - \#\Delta_{\prec_w}(\langle g_1, g_2, \ldots, g_r\rangle + I_q) = \\ &= \#\Delta_{\prec_w}(I_q) \cap \operatorname{LM}(\langle g_1, g_2, \ldots, g_r\rangle + I_q) =: \#\square_{\prec_w}(D).\end{aligned}$$

Поскольку $g_1, g_2, \ldots, g_r$ линейно независимы, всегда можно считать, что их старшие коэффициенты равны единице, а старшие мономы различны.

Предложение 5. *Пусть* $C_1 := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(1 + I_7), \operatorname{ev}(x + I_7), \operatorname{ev}(x^2 + I_7), \operatorname{ev}(y + I_7)\}$. *Тогда*

1. *C_1 является $[7, 4, \geqslant 3]$-кодом*;
2. $d_2(C_1) \geqslant 5$;
3. $d_3(C_1) \geqslant 6$.

Доказательство. Утверждение 1 следует из результатов § 4. Далее, рассмотрим следующие многочлены:

$$f_1 := y + a_1x^2 + a_2x + a_3, \quad f_2 := x^2 + b_1x + b_2, \quad f_3 := x + c_1, \quad f_4 := 1,$$

где $a_1, a_2, a_3, b_1, b_2, c_1 \in \mathbb{F}_7$. Пусть D – подкод размерности 2 кода C_1, тогда при различных выборах D получаем следующее:

- Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7)\}$, то $\{x^2, x^3, y, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 5$;
- Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то $\{x, y, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 6$;
- Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то $\{x, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 5$.
- Во всех остальных случаях $\#\operatorname{Supp} D \geqslant 7$.

Следовательно, $d_2(C_1) \geqslant 5$. Это доказывает утверждение 2. Пусть D' – подкод размерности 3 кода C_1, тогда при различных выборах D' получаем следующее:

- Если $D' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то $\{x, x^2, x^3, y, xy, x^2y\} \subseteq \square_{\prec_w}(D')$. Таким образом, $\#\operatorname{Supp} D' \geqslant 6$;
- Во всех остальных случаях $\#\operatorname{Supp} D' \geqslant 7$.

Следовательно, $d_3(C_1) \geqslant 6$. Это доказывает утверждение 3. ▲

Аналогично, имеют место следующие результаты.

Предложение 6. *Пусть* $C_2 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1+I_7), \mathrm{ev}(x+I_7), \mathrm{ev}(y+I_7)\}$. *Тогда*
1. C_2 *является* $[7, 3, \geqslant 4]$-*кодом*;
2. $d_2(C_2) \geqslant 6$.

Предложение 7. *Пусть* $C_3 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1+I_7), \mathrm{ev}(x+I_7), \mathrm{ev}(x^2+I_7), \mathrm{ev}(y+I_7), \mathrm{ev}(xy+I_7), \mathrm{ev}(x^2y+I_7)\}$. *Тогда*
1. C_3 *является* $[7, 6, \geqslant 2]$-*кодом*;
2. $d_2(C_3) \geqslant 3$;
3. $d_3(C_3) \geqslant 4$;
4. $d_4(C_3) \geqslant 5$.

Доказательство. Утверждение 1 следует из результатов § 4. Далее, рассмотрим следующие многочлены:

$$f_1 := x^2y + a_1xy + a_2y + a_3x^2 + a_4x + a_5, \quad f_2 := xy + b_1y + b_2x^2 + b_3x + b_4,$$
$$f_3 := y + c_1x^2 + c_2x + c_3, \quad f_4 := x^2 + d_1x + d_2, \quad f_5 := x + e_1, \quad f_6 := 1,$$

где $a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, c_1, c_2, c_3, d_1, d_2, e_1 \in \mathbb{F}_7$. Пусть D – подкод размерности 2 кода C_3, тогда при различных выборах D получаем следующее.

Если $D := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(f_1 + I_7), \mathrm{ev}(f_2 + I_7)\}$, то $\{xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Применим редукцию

$$x^2 f_2 \xrightarrow{x^3y - 2x^2y + 2xy - y} (b_1 + 2)x^2y + b_2x^4 - 2xy + b_3x^3 + y + b_4x^2.$$

Если $b_1 \neq 5$, то продолжаем редукцию:

$$(b_1 + 2)x^2y + b_2x^4 - 2xy + b_3x^3 + y + b_4x^2 \xrightarrow{f_2}$$
$$\xrightarrow{f_2} b_2x^4 + (-2 - b_1^2 - 2b_1)xy + (b_3 - b_2b_1 - 2b_2)x^3 + y +$$
$$+ (b_4 - b_3b_1 - 2b_3)x^2 - b_4(b_1 + 2)x.$$

Если $b_2 \neq 0$, то продолжаем редукцию:

$$b_2x^4 + (-2 - b_1^2 - 2b_1)xy + (b_3 - b_2b_1 - 2b_2)x^3 + y +$$
$$+ (b_4 - b_3b_1 - 2b_3)x^2 - b_4(b_1 + 2)x \xrightarrow{x^4 - 2x^3 + 2x^2 - x}$$
$$\xrightarrow{x^4 - 2x^3 + 2x^2 - x} (-2 - b_1^2 - 2b_1)xy + (b_3 - b_2b_1)x^3 + y +$$
$$+ (b_4 - b_3b_1 - 2b_3 - 2b_2)x^2 + (-b_4b_1 - 2b_4 + b_2)x \xrightarrow{f_2}$$
$$\xrightarrow{f_2} (b_3 - b_1b_2)x^3 + (1 + 2b_1 + b_1^3 + 2b_1^2)y + (b_4 - b_1b_3 - 2b_3 + b_2b_1^2 + 2b_2b_1)x^2 +$$
$$+ (-b_4b_1 - 2b_4 + b_2 + 2b_3 + b_3b_1^2 + 2b_1b_3)x + b_4(2 + b_1^2 + 2b_1).$$

Если $b_3 \neq b_1b_2$, то $x^3 \in \square_{\prec_w}(D)$. В противном случае остается

$$(1 + 2b_1^2 + 2b_1 + b_1^3)y + b_4x^2 + (-b_1b_4 - 2b_4 + b_2 + 2b_1b_2 + b_2b_1^3 + 2b_2b_1^2)x +$$
$$+ b_4(2 + b_1^2 + 2b_1).$$

Если теперь $b_1 \notin \{2, 4, 6\}$, то $\{y\} \subseteq \square_{\prec_w}(D)$. В противном случае, продолжая редукцию с помощью f_1, получаем $\#\,\mathrm{Supp}\,D \geqslant 3$.

Если же $b_2 = 0$, то после редукции с помощью f_2 остается

$$b_3x^3 + (1 + 2b_1 + b_1^3 + 2b_1^2)y + (b_4 - b_1b_3 - 2b_3)x^2 +$$
$$+ (-b_1b_4 - 2b_4 + 2b_3 + b_3b_1^2 + 2b_1b_3)x + b_4(2 + b_1^2 + 2b_1).$$

Если $b_3 \neq 0$, то $x^3 \in \square_{\prec_w}(D)$. В противном случае, если $b_3 = 0$ и $b_1 \notin \{2, 4, 6\}$, то $y \in \square_{\prec_w}(D)$. В противном случае, продолжая редукцию, получаем $\#\operatorname{Supp} D \geqslant 3$.

Если же $b_1 = 5$, то остается $b_2x^4 - 2xy + b_3x^3 + y + b_4x^2$. Если $b_2 \neq 0$, то, продолжая редукцию, получаем, что если $b_3 \neq 5b_2$, то $x^3 \in \square_{\prec_w}(D)$, а в противном случае $y \in \square_{\prec_w}(D)$. А если $b_2 = 0$, то в случае $b_3 \neq 0$ имеем $x^3 \in \square_{\prec_w}(D)$, а в противном случае $y \in \square_{\prec_w}(D)$.

Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_4 + I_7)\}$, то $\{x^2, x^3, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 3$.

Во всех остальных случаях $\#\operatorname{Supp} D \geqslant 4$.

Следовательно, $d_2(C_3) \geqslant 3$. Это доказывает утверждение 2. Аналогично, пусть D' – подкод размерности 3 кода C_3, тогда при различных выборах D' получаем следующее:

- Если $D' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то получаем $\{y, xy, x^2y\} \subseteq \subseteq \square_{\prec_w}(D')$. При этом согласно п. 3.1.3 имеем $x^3 \in \square_{\prec_w}(D')$. Таким образом, $\#\operatorname{Supp} D' \geqslant 4$.
- Если $D' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_4 + I_7)\}$, то $\{x^2, x^3, xy, x^2y\} \subseteq \subseteq \square_{\prec_w}(D')$. Таким образом, $\#\operatorname{Supp} D' \geqslant 4$.
- Во всех остальных случаях $\#\operatorname{Supp} D' \geqslant 5$.

Следовательно, $d_3(C_3) \geqslant 4$. Это доказывает утверждение 3. Аналогично, пусть D'' – подкод размерности 4 кода C_3, тогда при различных выборах D'' получаем следующее:

- Если $D'' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7), \operatorname{ev}(f_4 + I_7)\}$, то получаем $\{x^2, x^3, y, xy, x^2y\} \subseteq \square_{\prec_w}(D'')$. Таким образом, $\#\operatorname{Supp} D'' \geqslant 5$.
- Если $D'' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_4 + I_7), \operatorname{ev}(f_5 + I_7)\}$, то получаем $\{x, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(D'')$. Таким образом, $\#\operatorname{Supp} D'' \geqslant 5$.
- Во всех остальных случаях $\#\operatorname{Supp} D'' \geqslant 6$.

Следовательно, $d_4(C_3) \geqslant 5$. Это доказывает утверждение 4. ▲

Предложение 8. *Пусть* $C_4 := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(1+I_7), \operatorname{ev}(x+I_7), \operatorname{ev}(x^2+I_7), \operatorname{ev}(y+I_7), \operatorname{ev}(xy + I_7)\}$. *Тогда*

1. C_4 *является* $[7, 5, \geqslant 2]$-*кодом*;
2. $d_2(C_4) \geqslant 4$;
3. $d_3(C_4) \geqslant 5$;
4. $d_4(C_4) \geqslant 6$.

Предложение 9. *Пусть* $C_5 := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(1+I_7), \operatorname{ev}(x+I_7), \operatorname{ev}(x^2+I_7), \operatorname{ev}(y+I_7), \operatorname{ev}(x^2y + I_7)\}$. *Тогда*

1. C_5 *является* $[7, 5, \geqslant 2]$-*кодом*;
2. $d_2(C_5) \geqslant 4$;
3. $d_3(C_5) \geqslant 5$;
4. $d_4(C_5) \geqslant 6$.

Доказательство. Утверждение 1 следует из результатов § 4. Далее, рассмотрим следующие многочлены:

$$f_1 := x^2y + a_1y + a_2x^2 + a_3x + a_4, \quad f_2 := y + b_1x^2 + b_2x + b_3,$$
$$f_3 := x^2 + c_1x + c_2, \quad f_4 := x + d_1 \quad f_5 := 1,$$

где $a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1, c_2, d_1 \in \mathbb{F}_7$. Пусть D – подкод размерности 2 кода C_5, тогда при различных выборах D получаем следующее.

Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7)\}$, то $\{y, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. При этом согласно п. 3.1.3 имеем $x^3 \in \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 4$.

Если $D := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(f_1 + I_7), \mathrm{ev}(f_3 + I_7)\}$, то $\{x^2, x^3, x^2y\} \subseteq \square_{\prec_w}(D)$. Далее,

$$yf_3 \xrightarrow{f_1} c_1xy + (c_2 - a_1)y - a_2x^2 - a_3x - a_4.$$

Если $c_1 \neq 0$, то $xy \in \square_{\prec_w}(D)$. В противном случае остается $(c_2-a_1)y-a_2x^2-a_3x-a_4$. Если $c_2 \neq a_1$, то $\{y, xy\} \subseteq \square_{\prec_w}(D)$. В противном случае остается $-a_2x^2 - a_3x - a_4$. Если $a_2 \neq 0$, то

$$-a_2x^2y - a_3xy - a_4y \xrightarrow{f_1} -a_3xy + (-a_4 + a_1a_2)y + a_2^2x^2 + a_2a_3x + a_2a_4.$$

Если $a_3 \neq 0$, то $xy \in \square_{\prec_w}(D)$. В противном случае остается $(-a_4+a_1a_2)y+a_2^2x^2+a_2a_4$. Если $a_4 \neq a_1a_2$, то $\{y, xy\} \subseteq \square_{\prec_w}(D)$. В противном случае

$$a_2^2x^2 + a_2^2a_1 \to x^3y + a_1xy \xrightarrow{x^3y-2x^2y+2xy-y} 2x^2y + (a_1 - 2)xy + y \xrightarrow{f_1}$$
$$\xrightarrow{f_1} (a_1 - 2)xy + (1 - 2a_1)y - 2a_2x^2 - 2a_1a_2.$$

Если $a_1 \neq 2$, то $xy \in \square_{\prec_w}(D)$. В противном случае $y \in \square_{\prec_w}(D)$.

Если же $a_2 = 0$, то в случае $a_3 \neq 0$ имеем $\{x, xy\} \subseteq \square_{\prec_w}(D)$. В противном случае, если $a_3 = 0$, то $\{1, x, y, xy\} \subseteq \square_{\prec_w}(D)$. Если теперь $a_4 = 0$, то непосредственными вычислениями убеждаемся, что $\#\,\mathrm{Supp}\,D \geqslant 4$.

Таким образом, $\#\,\mathrm{Supp}\,D \geqslant 4$.

Во всех остальных случаях $\#\,\mathrm{Supp}\,D \geqslant 5$.

Следовательно, $d_2(C_5) \geqslant 4$. Это доказывает утверждение 2. Остальные утверждения доказываются аналогично. ▲

§ 6. Заключение

В статье получено несколько кодов с наилучшими возможными параметрами, построенных по гиперэллиптической кривой над полем $\mathbb{F}_7$ с помощью техники из работы [4]. Также вычислены обобщенные веса Хэмминга этих кодов. Кроме того, для некоторых кодов установлено расстояние по парам символов. За исключением нескольких обобщенных весов Хэмминга, которые можно получить с помощью теоремы 2, полученные нижние границы нетривиальны.

Для построения классов хороших кодов этот метод можно также применять к примарным мономиальным аффинным эвалюационным кодам, построенным по другим кривым.

Авторы выражают благодарность рецензенту за замечания и предложения, способствовавшие улучшению изложения.

СПИСОК ЛИТЕРАТУРЫ

1. *Fitzgerald J., Lax R.F.* Decoding Affine Variety Codes Using Gröbner Bases // Des. Codes Cryptogr. 1998. V. 13. № 2. P. 147–158. https://doi.org/10.1023/A:1008274212057
2. *Geil O.* Evaluation Codes from an Affine Variety Code Perspective // Advances in Algebraic Geometry Codes. Singapore: World Sci., 2008. P. 153–180. https://doi.org/10.1142/9789812794017_0004
3. *Andersen H.E., Geil O.* Evaluation Codes from Order Domain Theory // Finite Fields Appl. 2008. V. 4. № 1. P. 92–123. https://doi.org/10.1016/j.ffa.2006.12.004
4. *Geil O., Özbudak F.* On Affine Variety Codes from the Klein Quartic // Cryptogr. Commun. 2019. V. 11. № 2. P. 237–257. https://doi.org/10.1007/s12095-018-0285-6
5. *Patanker N., Singh S.K.* Quaternary Affine Variety Codes over a Klein-like Curve. Preprint, 2020.

6. *Wei V.K.* Generalized Hamming Weights for Linear Codes // IEEE Trans. Inform. Theory. 1991. V. 37. № 5. P. 1412–1418. https://doi.org/10.1109/18.133259
7. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available online at http://www.codetables.de.
8. *Cassuto Y., Blaum M.* Codes for Symbol-Pair Read Channels // IEEE Trans. Inform. Theory. 2011. V. 57. № 12. P. 8011–8020. https://doi.org/10.1109/TIT.2011.2164891
9. *Helleseth T., Kløve T., Mykkelveit J.* The Weight Distribution of Irreducible Cyclic Codes with Block Lengths $n_1((q^l-1)/N)$ // Discrete Math. 1977. V. 18. № 2. P. 179–211. https://doi.org/10.1016/0012-365X(77)90078-4
10. *Kløve T.* The Weight Distribution of Linear Codes over $GF(q^l)$ Having Generator Matrix over $GF(q)$ // Discrete Math. 1978. V. 23. № 2. P. 159–168. https://doi.org/10.1016/0012-365X(78)90114-0

Патанкер Нупур
Сингх Санджай Кумар
Индийский институт науки, образования
и исследований, Бхопал, Индия
nupurp@iiserb.ac.in
sanjayks@iiserb.ac.in

Поступила в редакцию
11.09.2020
После доработки
14.01.2021
Принята к публикации
19.01.2021

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*
по контракту с ООО «Объединённая редакция»

Москва
ООО «Объединённая редакция»