РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

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

Том 57, 2021 **Вып. 2**

Апрель–Май–Июнь

М о с к в а

С О Д Е Р Ж А Н И Е

CONTENTS

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 2**

УДК 621.391 : 519.72 : 519.832

© 2021 г. **А.С. Вора, А.А. Кулкарни**[1]

ТЕОРЕМЫ О МИНИМАКСЕ ДЛЯ СОВМЕСТНОГО КОДИРОВАНИЯ ИСТОЧНИКА И КАНАЛА С ПОТЕРЯМИ ПРИ КОНЕЧНОЙ ДЛИНЕ БЛОКА В ПРОИЗВОЛЬНО МЕНЯЮЩЕМСЯ КАНАЛЕ

Задача о передаче информации при конечной длине блока в присутствии источника целенаправленных помех, мотивированная приложениями, связанными с безопасностью киберфизических систем, рассматривается как игра с нулевой суммой между командой, состоящей из кодера и декодера, и источником помех, где как этой команде, так и источнику помех разрешается использовать лишь локально рандомизированные стратегии. При использовании локально рандомизированных кодов задача для устанавливающей связь команды является невыпуклой, и поэтому в общем случае теорема о минимаксе для такой игры может не выполняться. Тем не менее показана справедливость *приближенных теорем о минимаксе* в том смысле, что минимакс и максимин для этой игры асимптотически сходятся друг к другу. В частности, для скоростей, строго меньших некоторого порогового значения, *обе* эти величины стремятся к нулю, а для скоростей, строго больших этого порога, – к единице. Затем доказана теорема о минимаксе *для вторых приближений*, т.е. показано, что для скоростей, стремящихся в точности к этому пороговому значению по определенному закону, как минимакс, так и максимин сходятся к некоторому постоянному значению, не равному ни нулю, ни единице. Ключевую роль для этих результатов играют полученные границы на минимакс и максимин игры при конечной длине блока и границы второго порядка, основанные на дисперсии.

Ключевые слова: произвольно меняющиеся каналы, игра с нулевой суммой, невыпуклость, стохастические коды.

DOI: 10.31857/S0555292321020017

§ 1. Введение

Киберфизические системы состоят из физических объектов, дистанционно управляемых по каналам связи. Примерами таких систем являются инфраструктура “умного города”, современные автомобили, электросети и атомные электростанции, где для передачи срочной информации используется вспомогательный кибернетический уровень [2]. Эффективная и безопасная передача информации через этот кибернетический уровень является основополагающим фактором для функционирования таких систем. Чтобы гарантировать надежную связь в парадигме блокового кодирования, обычно требуется все большее число обращений к каналу, что приводит к задержкам при передаче. Поскольку вышеуказанные системы чувствительны к задержкам, крайне важно исследовать эти системы в режиме конечной длины блока. С другой стороны, наличие кибернетического уровня в этих системах делает их уязвимыми для атак противника, которые могут иметь катастрофические последствия [3, 4]. С учетом важности этих двух факторов – ограниченности задержки и

[1] Предварительная версия настоящей статьи была представлена в [1].

возможности целенаправленных помех – в данной статье изучается задача прямой передачи с потерями при конечной длине блока в присутствии источника помех.

Мы рассматриваем постановку задачи, в которой передатчик и приемник осуществляют связь по каналу, состояние которого контролируется активным источником помех. Источник помех может изменять состояние канала *произвольным образом*, т.е. в любой момент передачи, с целью нарушить связь. Стандартная формулировка этой задачи рассматривает эту ситуацию только с точки зрения осуществляющей связь команды путем поиска стратегий кодирования, устойчивых к *любому* действию источника помех. Однако поскольку возможность применять стратегии имеют как осуществляющая связь команда, так и источник помех, будет логично принять нейтральную точку зрения, позволяющую и команде, и источнику помех действовать стратегически. С этой целью мы формулируем вышеуказанную проблему как игру с нулевой суммой, в которой команда, состоящая из передатчика и приемника, стремится минимизировать потери при передаче путем построения соответствующих кодов, а источник помех пытается максимизировать их, выбирая состояния канала.

Ключевым для наших результатов является определение допустимых стратегий для осуществляющей связь команды и источника помех, в частности, понятие рандомизации, которую мы допускаем. Мы предполагаем, что стратегией для осуществляющей связь команды, т.е. для пары кодер–декодер, является *стохастический код* или коды только с *локальной* рандомизацией. Как правило, для задачи передачи информации интерес представляет нахождение детерминированных кодов. В теоретико-игровой терминологии это соответствует *чистым* стратегиям для осуществляющей связь команды. Однако по причинам, которые мы обсудим далее, нахождение детерминированного кода для этой задачи требует анализа, выходящего за рамки настоящей статьи. Поэтому мы будем искать рандомизированные стратегии. Теория игр предоставляет два возможных типа рандомизации чистых стратегий (см., например, [5]). *Смешанная* стратегия – это случайный выбор чистой стратегии; в терминологии теории связи это соответствует случайно выбранной паре кодер–декодер, или *случайному коду*. Однако реализация такого кода требует *совместной* случайности между кодером и декодером, что может оказаться невыполнимым в киберфизических системах, где кодер и декодер децентрализованы, а канал является единственным средством связи. Другим типом рандомизации в теории игр являются *поведенческие* стратегии – при такой стратегии действие выбирается случайным образом с учетом информации, имеющейся на данный момент времени. В литературе по теории информации такие стратегии называются *стохастическими кодами*. При такой стратегии кодер и декодер применяют локальную рандомизацию, используя свой собственный личный источник случайности. В настоящей статье мы используем именно этот тип рандомизации для осуществляющей связь команды. Однако при этом для нас достаточно, чтобы локально случайную стратегию использовал только передатчик. Декодирование может по-прежнему быть детерминированной функцией. Таким образом, под стохастическим кодом в этой статье мы понимаем пару, состоящую из стохастического кодера и детерминированного декодера. Мы предполагаем, что источник помех может применять рандомизированный выбор последовательностей состояний канала.

К сожалению, при рассмотрении стохастических кодов в дальнейшем анализе возникают значительные трудности. Во-первых, сформулировав задачу как игру с нулевой суммой, ее приходится анализировать, используя понятие *седловой точки* [5]. Говорят, что игра имеет седловую точку, если минимальные потери по всем стратегиям источника помех, которые осуществляющая связь команда может понести в худшем случае (называемые *верхней ценой* игры), равны максимальным потерям по всем стратегиям осуществляющей связь команды, которые источник помех может понести в худшем случае (называемые *нижней ценой* игры). Однако

для каждого фиксированного действия источника помех задача оптимизации для осуществляющей связь команды при использовании стохастических кодов с необходимостью *невыпукла* из-за неклассической структуры информации [6]. Как следствие, седловая точка не обязательно существует для получающейся игры с нулевой суммой. Этот факт ставит под вопрос любой дальнейший теоретико-игровой анализ.

Кроме того, построение стохастического кода сопряжено с определенными неотъемлемыми трудностями. Для вычисления границы сверху на верхнюю цену игры требуется схема достижимости для совместного кодирования источника и канала. Однако для построения детерминированного кода для совместного кодирования источника и канала может потребоваться установление существования детерминированного кода в произвольно меняющемся канале при критерии максимальной вероятности ошибки. Эта последняя задача в общем случае не решена, а в некоторых случаях эквивалентна нахождению пропускной способности при нулевой ошибке для дискретного канала без памяти [7].

Наши основные результаты показывают, что, несмотря на вышеуказанную невыпуклость, для этой игры справедливы теоремы, близкие к минимаксным, в том смысле, что при возрастании длины блока верхняя и нижняя цена игры становятся сколь угодно близкими. В частности, мы показываем, что существует такой порог, что если асимптотическая скорость строго ниже него, то верхняя и нижняя цена стремится к нулю, а для скоростей, строго превышающих порог, верхняя и нижняя цена стремятся к единице. Затем мы рассматриваем более тонкий режим, при котором асимптотическая скорость в точности равна порогу, но допускается отклонение от порога, *изменяющееся* в зависимости от длины блока по некоторому специальному закону. В этом случае верхняя и нижняя цена стремятся к одной и той же константе, не равной ни нулю, ни единице. Это показывает, что теорема о минимаксе справедлива даже в этом новом, более тонком режиме.

Верхняя цена игры соответствует совместному кодированию источника и канала с потерями в *произвольно меняющемся канале* (ПМК). С другой стороны, нижняя цена соответствует нахождению распределения вероятностей на последовательностях состояний, такого что минимальные потери в получающемся канале (не обязательно без памяти) максимальны. Наши результаты получены с помощью обращения теоремы кодирования для этой задачи, дающего границу снизу на нижнюю цену игры, и построения схемы достижимости для ПМК, дающей границу сверху на верхнюю цену. Эти границы приводят к границам второго порядка, основанным на дисперсии, для скорости передачи, которые вызвали значительный интерес в недавнем прошлом (см., например, [8, 9] и многочисленные последующие работы). В нашем контексте границы, основанные на дисперсии, дают вышеупомянутую более тонкую теорему о минимаксе (теорему "второго порядка").

В нашей схеме достижимости используется стохастическое кодирование, доступное для совместного кодирования источника и канала. Отдельную схему кодирования для источника и канала в постановке задачи кодирования источника и канала без потерь можно построить как композицию кода для источника и кода для канала, построенных независимо друг от друга. Хотя эта схема достаточна для теорем о минимаксе с классическими скоростями передачи, она недостаточно точна для получения искомой минимаксной теоремы второго порядка. Мы разработали схему совместного кодирования источника и канала, используя идеи из [9, 10], дающую стохастический код, приводящий к желаемой теореме. Для построения этой схемы достижимости мы сперва получаем редуцированный случайный код, являющийся кодом с равномерным распределением на меньшем количестве детерминированных кодов. Используя детерминированный код для канала при критерии средней вероятности ошибки и вышеупомянутый редуцированный случайный код, мы строим совместный код для источника и канала, требующий только локальной случайности на

передающем конце, получая таким образом стохастический код. Для этой конструкции мы используем детерминированный код для канала, представленный в [11].

Для нижней граница используется метод ослабления, основанного на линейном программировании, (ЛП-ослабления) из [12], где было показано, что хотя задача прямой передачи (без помех) и невыпукла в пространстве стохастических кодов, она тем не менее обладает некоторой скрытой выпуклостью. В частности, было показано, что для больших длин блоков задачу можно сколь угодно точно аппроксимировать методом ЛП-ослабления. Это позволяет предположить, что в нашей задаче может быть справедлива *приближенная* теорема о минимаксе. Наши результаты подтверждают эту догадку. Они показывают, что ЛП-ослабление является точным даже в постановке задачи с преднамеренными помехами, расширяя тем самым список случаев, когда метод ЛП-ослабления дает точные результаты [12, 13].

Насколько нам известно, постановка задачи, рассматриваемая здесь, ранее не изучалась. Конечно, теоретико-игровая формулировка задачи передачи информации при наличии помех изучалась на самом деле и ранее, но в несколько ином смысле. Например, в [14, 15] рассматривалась взаимная информация как функция выигрыша и было доказано существование стратегий с седловой точкой. В теории управления изучались подобные задачи для непрерывного алфавита, например, в [16] рассматривался вопрос о передаче последовательности гауссовских случайных величин при наличии помех и формулировалась задача об игре с нулевой суммой со среднеквадратической ошибкой в качестве функции выигрыша. В контексте ПМК теоремы кодирования для гауссовских ПМК при ограничениях на пиковую и среднюю мощности на входе и для источника помехе были доказаны в [17]. В этих теоремах кодирования неявно предполагалась приближенная теорема о минимаксе для игры с нулевой суммой. Формулировка для игры с нулевой суммой, аналогичная нашей, обсуждалась также в [10, гл. 12], где рассматривались и формулировались различные случаи передачи по ПМК как игры с нулевой суммой. Наиболее близкой к нашей постановке является задача, изучавшаяся в [18, 19] вторым автором настоящей статьи, где рассматривалась только задача кодирования канала, а действие источника помех было фиксировано на протяжении всей передачи, что делало вопрос о верхней цене игры эквивалентным кодированию для *составного канала*; кроме того, в [18, 19] не рассматривались минимаксные теоремы второго порядка.

Совместное кодирование источника и канала без потерь в ПМК было рассмотрено нами в предварительной версии данной статьи, представленной на конференции [1]. Настоящая статья отличается от [1] в следующих аспектах. Здесь мы рассматриваем совместное кодирование источника и канала с потерями, в отличие от [1], где рассматривалось только кодирование без потерь. Кроме того, мы выводим основанные на дисперсии границы на скорость, открывающие дорогу к минимаксной теореме второго порядка. Для этого нам нужна характеризация дисперсии ПМК. Далее, для получения членов высшего порядка, учитывающих дисперсию, нам требуется более сложный совместный стохастический код для совместного кодирования источника и канала. Отдельные коды для источника и для канала, использованные в [1], достаточны для получения минимаксных теорем первого порядка. Однако такое раздельное кодирование не позволяет получить точные члены высшего порядка.

Статья имеет следующую структуру. Формулировка задачи приведена в § 3. Нижняя граница выводится в § 4, а верхняя – в § 5. Соответствующий асимптотический анализ производится в § 6, а § 7 содержит заключительные замечания.

§ 2. Предварительные сведения

2.1. Обозначения. Все случайные величины в этой статье дискретны и заданы на соответствующем вероятностном пространстве с мерой $\mathbf{P}$. Случайные величины обозначаются прописными буквами X, а их реализации – строчными буквами x;

если это не оговаривается специально, они являются векторами, длины которых ясны из контекста. Ажурными буквами типа $\mathbb{X}, \mathbb{Y}$ и т.д. обозначаются соответствующие однократные случайные величины, а пространства таких случайных величин обозначаются рукописными буквами $\mathcal{X}, \mathcal{Y}$ и т.д. Множество всех распределений вероятностей на пространстве $\mathcal{X}$ обозначается через $\mathcal{P}(\mathcal{X})$, а одно такое конкретное распределение – через $P_{\mathbb{X}}$.

Типом последовательности $x \in \mathcal{X}^n$ называется эмпирическое распределение $T_x \in \in \mathcal{P}(\mathcal{X})$ вида $T_x(\cdot) \equiv |\{i : x_i = \cdot\}|/n$. Совместный тип величин x, y обозначается через $T_{x,y}$. Через $\mathcal{P}_n(\mathcal{X}) \subseteq \mathcal{P}(\mathcal{X})$ обозначается множество всех типов последовательностей в $\mathcal{X}^n$. Множество последовательностей с типом P обозначается через $T(P)$.

Для любого выражения $\mathcal{B}$ индикаторная функция $\mathbb{I}\{\mathcal{B}\}$ равна единице, когда выражение истинно, и нулю в противном случае. Вероятность события A по мере, индуцированной распределением P, обозначается через $P\{A\} := \sum\limits_x \mathbb{I}_{x\in A} P(x)$. Дисперсия случайной величины $X \in \mathcal{X}$ обозначается через $\mathrm{Var}(X) := \mathbf{E}[X - \mathbf{E}[X]]^2$. Для любых распределений P_X и $P_{Y|X}$ полагаем $(P_X \times P_{Y|X})(x, y) := P_X(x)P_{Y|X}(y\,|\,x)$ и $(P_X P_{Y|X})(y) := \sum\limits_x P_X(x)P_{Y|X}(y\,|\,x)$. Функция, дополнительная к гауссовской функции распределения, обозначается через Q (не путать с условными функциями распределения $Q_{X|Y}$ для случайных величин X, Y – такие функции будут вводиться и использоваться в соответствующих контекстах). Все экспоненты и логарифмы (exp и log) рассматриваются по основанию 2.

2.2. Произвольно меняющийся канал. Произвольно меняющийся канал (ПМК) был впервые введен в [20], где рассматривался канал, закон в котором может произвольным образом изменяться при каждой передаче. ПМК можно моделировать следующим образом. Рассмотрим семейство каналов $\mathbb{V} := \{P_{\mathbb{Y}|\mathbb{X},\,\Theta=\theta} \in \mathcal{P}(\mathcal{Y}\,|\,\mathcal{X}),\ \theta \in \mathcal{T}\}$ с одинаковыми пространствами входов и выходов, являющихся конечными множествами $\mathcal{X}$ и $\mathcal{Y}$ соответственно, где каждый канал индексируется параметром θ, называемым состоянием канала и выбираемым из конечного множества $\mathcal{T}$. Предполагается, что канал не имеет памяти. Тогда получаемый канал можно моделировать как следующий дискретный ПМК без памяти: вероятность получения последовательности $y \in \mathcal{Y}^n$ при передаче последовательности $x \in \mathcal{X}^n$ и при последовательности состояний $\theta \in \mathcal{T}^n$ равна $P_{Y|X,\boldsymbol{\Theta}}(y\,|\,x, \theta) = \prod\limits_{i=1}^{n} P_{\mathbb{Y}|\mathbb{X},\Theta}(y_i\,|\,x_i, \theta_i)$.

Детерминированный код для канала – это пара функций $(f_{\mathrm{C}}, \varphi_{\mathrm{C}})$ вида

$$f_{\mathrm{C}} \colon \mathcal{W} \to \mathcal{X}^n, \quad \varphi_{\mathrm{C}} \colon \mathcal{Y}^n \to \mathcal{W},$$

где $\mathcal{W} = \{1, \ldots, M\}$ для $M \in \mathbb{N}$. Вероятность ошибки для каждого сообщения $m \in \mathcal{W}$ и последовательности состояний $\theta \in \mathcal{T}^n$ при использовании детерминированного кода для канала $(f_{\mathrm{C}}, \varphi_{\mathrm{C}})$ имеет вид

$$e_{m,\theta}(f_{\mathrm{C}}, \varphi_{\mathrm{C}}) := \sum_{y\in\mathcal{Y}^n} \mathbb{I}\{\varphi(y) \neq m\} P_{Y|X,\boldsymbol{\Theta}}(y\,|\,f_{\mathrm{C}}(m), \theta).$$

Максимальная и средняя вероятности ошибки по всем сообщениям для такого кода определяются как

$$e(f_{\mathrm{C}}, \varphi_{\mathrm{C}}) := \max_{\theta\in\mathcal{T}^n} \max_{m\in\{1,\ldots,M\}} e_{m,\theta}(f_{\mathrm{C}}, \varphi_{\mathrm{C}}), \quad \bar{e}(f_{\mathrm{C}}, \varphi_{\mathrm{C}}) := \max_{\theta\in\mathcal{T}^n} \frac{1}{M} \sum_{m=1}^{M} e_{m,\theta}(f_{\mathrm{C}}, \varphi_{\mathrm{C}})$$

соответственно.

В отличие от обычного дискретного канала без памяти (ДКБП), пропускная способность ПМК зависит от критерия ошибки и от типов кодов, используемых кодером и декодером. Кроме того, в некоторых случаях для пропускной способности

ПМК не известно никакое выражение в замкнутом виде. В частности, в [7] было показано, что вычисление пропускной способности детерминированного кодирования для определенного класса ПМК при критерии максимальной вероятности ошибки сводится к вычислению пропускной способности ДКБП при нулевой ошибке, что является весьма сложной задачей. Однако пропускную способность ПМК при критериях как максимальной, так и средней вероятности ошибки можно вычислить, если кодеру и декодеру разрешено рандомизировать свои действия.

Стохастический код определяется как пара условных распределений $Q_{X\,|\,W} \in \in \mathcal{P}(\mathcal{X}^n\,|\,\mathcal{W})$, $Q_{\widehat{W}\,|\,Y} \in \mathcal{P}(\mathcal{W}\,|\,\mathcal{Y}^n)$. Максимальная и средняя вероятности ошибки для стохастического кода $(Q_{X\,|\,W}, Q_{\widehat{W}\,|\,Y})$ определяются как

$$
\begin{aligned}
&e(Q_{X\,|\,W}, Q_{\widehat{W}\,|\,Y}) := \\
&:= \max_{\theta\in\mathcal{T}^n} \max_{w\in\{1,\ldots,M\}} \sum_{x,y,\widehat{w}} \mathbb{I}\{\widehat{w}\neq w\} Q_{X\,|\,W}(x\,|\,w) P_{Y\,|\,X,\boldsymbol{\Theta}}(y\,|\,x,\theta) Q_{\widehat{W}\,|\,Y}(\widehat{w}\,|\,y), \\
&\bar{e}(Q_{X\,|\,W}, Q_{\widehat{W}\,|\,Y}) := \\
&:= \max_{\theta\in\mathcal{T}^n} \frac{1}{M} \sum_{w=1}^{M} \sum_{x,y,\widehat{w}} \mathbb{I}\{\widehat{w}\neq w\} Q_{X\,|\,W}(x\,|\,w) P_{Y\,|\,X,\boldsymbol{\Theta}}(y\,|\,x,\theta) Q_{\widehat{W}\,|\,Y}(\widehat{w}\,|\,y).
\end{aligned}
$$

Пусть e_n – критерий вероятности ошибки (максимальной или средней). Пусть $R_n = \log M/n$ – скорость передачи. Скорость R называется достижимой, если существует последовательность (M, n)-кодов со скоростями R_n (детерминированных или случайных), такая что вероятность ошибки $e_n \to 0$ и $R_n \to R$ при n, стремящемся к бесконечности. Точная верхняя грань всех таких скоростей называется пропускной способностью канала и обозначается через C.

В случае ПМК пропускная способность C может оказаться нулевой для определенных типов кодов и критериев ошибки. Приведем условия, при которых пропускная способность ПМК положительна. ПМК называется несимметризуемым, если не существует распределения $P_{\Theta\,|\,\mathbb{X}} \in \mathcal{P}(\mathcal{T}\,|\,\mathcal{X})$, такого что $\forall x \in \mathcal{X}$, $x' \in \mathcal{X}$, $y \in \mathcal{Y}$ выполняется равенство

$$
\sum_{\theta\in\mathcal{T}} P_{\Theta\,|\,\mathbb{X}}(\theta\,|\,x) P_{\mathbb{Y}\,|\,\mathbb{X},\Theta}(y\,|\,x',\theta) = \sum_{\theta\in\mathcal{T}} P_{\Theta\,|\,\mathbb{X}}(\theta\,|\,x') P_{\mathbb{Y}\,|\,\mathbb{X},\Theta}(y\,|\,x,\theta).
$$

В настоящей статье все рассматриваемые ПМК предполагаются несимметризуемыми. Для несимметризуемого ПМК пропускная способность стохастического кодирования при критерии максимальной (и средней) вероятности ошибки имеет вид [21]

$$
C = \max_{P_{\mathbb{X}}\in\mathcal{P}(\mathcal{X})} \min_{q_\Theta\in\mathcal{P}(\mathcal{T})} I(\mathbb{X}; \mathbb{Y}_{q_\Theta}), \tag{1}
$$

где $I(\mathbb{X}; \mathbb{Y}_{q_\Theta})$ – взаимная информация между $\mathbb{X}$ и $\mathbb{Y}_{q_\Theta}$, а $\mathbb{Y}_{q_\Theta}$ – выход усредненного канала $(q_\Theta P_{\mathbb{Y}\,|\,\mathbb{X},\Theta}) := \sum\limits_{\theta\in\mathcal{T}} q_\Theta(\theta) P_{\mathbb{Y}\,|\,\mathbb{X},\Theta=\theta}$ при входе $\mathbb{X}$. Более подробные сведения о ПМК содержатся в [10, гл. 12; 22].

2.3. Скорость как функция искажения. Пусть $\mathcal{S}$ – пространство сообщений, и пусть $d_{\mathrm{S}}\colon \mathcal{S}\times\mathcal{S} \to [0,\infty)$ – функция искажения. Рассмотрим задачу, в которой требуется выразить наборы длины k из $\mathcal{S}^k$ с помощью M сообщений таким образом, чтобы среднее искажение удовлетворяло неравенству $\mathbf{E}[d_{\mathrm{S}}(\mathbb{S}, \widehat{\mathbb{S}})] \leqslant \boldsymbol{d}$ для некоторого фиксированного уровня искажения $\boldsymbol{d} > 0$.

Детерминированный код для источника определяется как пара функций $(f_{\mathrm{S}}, \varphi_{\mathrm{S}})$ вида

$$f_{\mathrm{S}}\colon \mathcal{S}^k \to \mathcal{W}, \quad \varphi_{\mathrm{S}}\colon \mathcal{W} \to \mathcal{S}^k,$$

где $\mathcal{W} = \{1, \ldots, M\}$ для $M \in \mathbb{N}$.

Искажением для последовательностей длины k называется величина $d(S, \widehat{S}) := \sum\limits_{i=1}^{k} d_{\mathrm{S}}(\mathbb{S}_i, \widehat{\mathbb{S}}_i)/k$. Скорость определяется как $R_k = \log M/k$. Скорость R называется достижимой для заданного уровня искажения $\boldsymbol{d}$, если существует код, такой что $\lim\limits_{k\to\infty} \mathbf{E}[d(S, \widehat{S})] \leqslant \boldsymbol{d}$ и $R_k \to R$. Точная нижняя грань всех таких скоростей носит название "скорость как функция искажения" и имеет вид

$$R(\boldsymbol{d}) = \min_{P_{\widehat{\mathbb{S}}\,|\,\mathbb{S}},\, \mathbf{E}[d_{\mathrm{S}}(\mathbb{S},\widehat{\mathbb{S}})] \leqslant \boldsymbol{d}} I(\mathbb{S}, \widehat{\mathbb{S}}), \tag{2}$$

где $\mathbb{S} \in \mathcal{S}$ имеет распределение $P_{\mathbb{S}} \in \mathcal{P}(\mathcal{S})$, а $\widehat{\mathbb{S}} \in \mathcal{S}$ – распределение $P_{\widehat{\mathbb{S}}\,|\,\mathbb{S}} \in \mathcal{P}(\mathcal{S}\,|\,\mathcal{S})$. Подробнее о теории скорости как функции искажения см. в [23, гл. 10].

2.4. Информационные величины. В этом пункте приводятся определения некоторых информационных величин, которые будут использоваться в настоящей статье. Информационная плотность определяется как

$$i_{\mathbb{X};\mathbb{Y}_{q_\Theta}}(x; y) = \log \frac{(q_\Theta P_{\mathbb{Y}\,|\,\mathbb{X},\Theta})(y\,|\,x)}{(P_{\mathbb{X}} q_\Theta P_{\mathbb{Y}\,|\,\mathbb{X},\Theta})(y)}, \quad x \in \mathcal{X}, \quad y \in \mathcal{Y}, \tag{3}$$

где

$$(q_\Theta P_{\mathbb{Y}\,|\,\mathbb{X},\Theta})(y\,|\,x) = \sum_{\theta\in\mathcal{T}} q_\Theta(\theta) P_{\mathbb{Y}\,|\,\mathbb{X},\Theta}(y\,|\,x,\theta),$$
$$(P_{\mathbb{X}} q_\Theta P_{\mathbb{Y}\,|\,\mathbb{X},\Theta})(y) = \sum_{x\in\mathcal{X},\,\theta\in\mathcal{T}} P_{\mathbb{X}}(x) q_\Theta(\theta) P_{\mathbb{Y}\,|\,\mathbb{X},\Theta}(y\,|\,x,\theta).$$

Информационная плотность для векторнозначных случайных величин (X, Y) обозначается через $i_{X;Y_q}$ и определяется аналогично. Определим $\boldsymbol{d}$-скошенную информацию как

$$j_{\mathrm{S}}(s, \boldsymbol{d}) = \log \frac{1}{\mathbf{E}\big[\exp(\lambda^* \boldsymbol{d} - \lambda^* d(s, \widehat{\mathbb{S}}))\big]}, \quad s \in \mathcal{S}, \tag{4}$$

где математическое ожидание вычисляется относительно безусловного распределения $P_{\widehat{\mathbb{S}}^*}$, на котором достигается минимум в (2), и $\lambda^* = -R'(\boldsymbol{d})$. Далее, $\boldsymbol{d}$-скошенная информация для векторнозначных случайных величин $(S, \widehat{S})$ определяется как

$$R_S(\boldsymbol{d}) = \inf_{P_{\widehat{S}\,|\,S}\colon\, \mathbf{E}[d(S,\widehat{S})] \leqslant \boldsymbol{d}} I(S; \widehat{S}), \tag{5}$$

где $d(s, \widehat{s})$ – функция искажения, определенная выше. Аналогично, $\boldsymbol{d}$-скошенная информация для случайных величин S определяется как

$$j_S(s, \boldsymbol{d}) := \log \frac{1}{\mathbf{E}\big[\exp(\lambda^* \boldsymbol{d} - \lambda^* d(s, \widehat{S}))\big]},$$

где математическое ожидание берется относительно распределения $P_{\widehat{S}^*}$, на котором достигается инфимум в (5), и $\lambda^* = -R'_S(\boldsymbol{d})$. Дальнейшие сведения о $\boldsymbol{d}$-скошенной информации можно найти в [24].

Определим следующее множество распределений, на которых достигается пропускная способность:

$$\Pi_\Theta = \Big\{ q_\Theta \in \mathcal{P}(\mathcal{T}) : \max_{P_\mathbb{X}} I(\mathbb{X}; \mathbb{Y}_{q_\Theta}) = C \Big\},$$
$$\Pi_\mathbb{X} = \Big\{ P_\mathbb{X} \in \mathcal{P}(\mathcal{X}) : \min_{q_\Theta} I(\mathbb{X}; \mathbb{Y}_{q_\Theta}) = C \Big\}.$$

Дисперсии источника и канала определяются следующим образом:

$$V_\mathrm{S} = \mathrm{Var}(j_\mathrm{S}(\mathbb{S}, \boldsymbol{d})), \tag{6}$$
$$V_\mathrm{C}^+ = \min_{P_\mathbb{X} \in \Pi_\mathbb{X}} \max_{q_\Theta \in \Pi_\Theta} \mathrm{Var}\big(i_{\mathbb{X};\mathbb{Y}_{q_\Theta}}(\mathbb{X};\mathbb{Y})\big), \quad V_\mathrm{C}^- = \max_{q_\Theta \in \Pi_\Theta} \min_{P_\mathbb{X} \in \Pi_\mathbb{X}} \mathrm{Var}\big(i_{\mathbb{X};\mathbb{Y}_{q_\Theta}}(\mathbb{X};\mathbb{Y})\big), \tag{7}$$

где $\mathbb{S}$ имеет распределение $P_\mathbb{S}$, а $(\mathbb{X}, \mathbb{Y})$ – распределение $P_\mathbb{X} \times (q_\Theta P_{\mathbb{Y}|\mathbb{X},\Theta})$. Для вычисления асимптотики будем предполагать, что существует единственное распределение состояний $q_\Theta^* \in \Pi_\Theta$, на котором достигается пропускная способность. В этом случае определенные выше дисперсии канала равны между собой: $V_\mathrm{C}^- = V_\mathrm{C}^+ =: V_\mathrm{C}$.

§ 3. Постановка задачи

Рассмотрим конечное семейство каналов $\mathbb{V} := \{P_{\mathbb{Y}|\mathbb{X},\Theta=\theta} \in \mathcal{P}(\mathcal{Y}|\mathcal{X}),\ \theta \in \mathcal{T}\}$. Пусть $\mathcal{S}$ – конечное пространство. Пусть требуется передать случайное исходное сообщение $S \in \mathcal{S}^k$, $k \in \mathbb{N}$, порождаемое независимо от других сообщений согласно одному и тому же распределению $P_\mathbb{S} \in \mathcal{P}(\mathcal{S})$, по этому семейству каналов, где источник помех может выбирать канал из множества $\mathbb{V}$ в каждый момент передачи. Передатчик (кодер) кодирует сообщение S во входную последовательность $X \in \mathcal{X}^n$, $n \in \mathbb{N}$, согласно закону $Q_{X|S} \in \mathcal{P}(\mathcal{X}^n | \mathcal{S}^k)$, а декодер декодирует последовательность $Y \in \mathcal{Y}^n$ на выходе канала в сообщение $\widehat{S} \in \mathcal{S}^k$ согласно закону $Q_{\widehat{S}|Y} \in \mathcal{P}(\widehat{\mathcal{S}}^k | \mathcal{Y}^n)$. Пара $(Q_{X|S}, Q_{\widehat{S}|Y})$ называется стохастическим кодом. Говорят, что произошла ошибка, если искажение между декодированной последовательностью и исходной последовательностью источника превышает заранее определенный уровень $\boldsymbol{d}$, т.е. если $d(S, \widehat{S}) := \sum_{i=1}^{k} d_\mathrm{S}(\mathbb{S}_i, \widehat{\mathbb{S}}_i)/k > \boldsymbol{d}$, где d_S – функция искажения, определенная в п. 2.3, а $\boldsymbol{d} \in [0, \infty)$ – максимальный допустимый уровень искажения. Источник помех выбирает каналы, которые будут использованы при передаче, путем выбора случайной последовательности состояний $\boldsymbol{\Theta} \in \mathcal{T}^n$ с распределением $q \in \mathcal{P}(\mathcal{T}^n)$; через $\Theta \in \mathcal{T}$ обозначаем соответствующую однократную случайную величину. Мы предполагаем, что кодеру и декодеру не известны действия источника помех и что источник помех также не имеет никакой информации ни о кодере и декодере, ни об исходном сообщении.

Предполагается, что память в канале отсутствует. Таким образом, получающийся канал описывается уравнением $P_{Y|X,\boldsymbol{\Theta}}(y|x,\theta) = \prod_{i=1}^{n} P_{\mathbb{Y}|\mathbb{X},\Theta}(y_i|x_i,\theta_i)$, задающим вероятность получения последовательности на выходе $y = (y_1, \ldots, y_n)$ при последовательности на входе $x = (x_1, \ldots, x_n)$ и последовательности состояний $\theta = (\theta_1, \ldots, \theta_n)$. Скорость передачи в такой постановке определяется как $R = k/n$.

Вероятность ошибки имеет вид

$$\mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\big) =$$
$$= \sum_{s,x,y,\widehat{s},\theta} \mathbb{I}\{d(s,\widehat{s}) > \boldsymbol{d}\} q(\theta) P_S(s) Q_{X|S}(x|s) P_{Y|X,\boldsymbol{\Theta}}(y|x,\theta) Q_{\widehat{S}|Y}(\widehat{s}|y). \tag{8}$$

Предполагается, что кодер и декодер стремятся минимизировать вероятности ошибки, выбирая для этого стохастические коды $(Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y})$, а источник помех – максимизировать ее путем выбора распределения q. Таким образом, для каждой пары (k,n) получается игра с нулевой суммой между командой, состоящей из кодера и декодера, и источником помех, выигрышем в которой служит вероятность ошибки. Необходимые сведения об играх с нулевой суммой можно найти в [5, гл. 4].

Минимаксом, или *верхней ценой* игры, называется величина

$$\overline{\nu}(k,n) = \min_{Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y}} \max_{q} \mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\big)$$

$$\text{при условиях} \quad Q_{X\,|\,S} \in \mathcal{P}(\mathcal{X}^n \,|\, \mathcal{S}^k), \quad Q_{\widehat{S}\,|\,Y} \in \mathcal{P}(\mathcal{S}^k \,|\, \mathcal{Y}^n), \quad q \in \mathcal{P}(\mathcal{T}^n),$$

а максимином, или *нижней ценой* игры, – величина

$$\underline{\nu}(k,n) = \max_{q} \min_{Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y}} \mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\big)$$

$$\text{при условиях} \quad Q_{X\,|\,S} \in \mathcal{P}(\mathcal{X}^n \,|\, \mathcal{S}^k), \quad Q_{\widehat{S}\,|\,Y} \in \mathcal{P}(\mathcal{S}^k \,|\, \mathcal{Y}^n), \quad q \in \mathcal{P}(\mathcal{T}^n).$$

Очевидно, $\overline{\nu}(k,n) \geqslant \underline{\nu}(k,n)$.

Можно заметить, что задача о минимаксе – это задача совместного кодирования источника и канала с потерями при передаче по ПМК с помощью стохастических кодов, поскольку кодеру и декодеру нужно найти стохастические коды, минимизирующие вероятность ошибки в наихудшем случае. Далее, оптимальным выбором для источника помех будет детерминированная последовательность состояний, поскольку вероятность ошибки, задаваемая формулой (8), линейна по распределению q. В задаче совместного кодирования источника и канала при передаче по ДКБП *без* источника помех асимптотически стремящейся к нулю вероятности ошибки можно достичь для скоростей, меньших $C'/R(\boldsymbol{d})$, где C' – пропускная способность ДКБП, а $R(\boldsymbol{d})$ – скорость как функция искажения. При этом для скоростей, больших $C'/R(\boldsymbol{d})$, вероятность ошибки стремится к единице [25]. В настоящей статье мы покажем, что эти результаты распространяются и на нашу игру, где $\overline{\nu}(k,n)$ и $\underline{\nu}(k,n)$ приближаются друг к другу при $k,n \to \infty$, а значение, к которому они стремятся, зависит от асимптотического значения скорости k/n.

Основными результатами статьи являются следующие две теоремы о минимаксе. Как показывает первая из них, и верхняя, и нижняя цена игры стремятся к нулю, если $\lim\limits_{k,n\to\infty} k/n < C/R(\boldsymbol{d})$.

Теорема 1. *Рассмотрим последовательность* (k,n), *такую что* $\lim\limits_{k,n\to\infty} k/n < C/R(\boldsymbol{d})$. *Тогда*

$$\lim_{k,n\to\infty} \underline{\nu}(k,n) = \lim_{k,n\to\infty} \overline{\nu}(k,n) = 0.$$

Если же $\lim\limits_{k,n\to\infty} k/n > C/R(\boldsymbol{d})$, то и верхняя, и нижняя цена игры стремятся к единице, как показывает

Теорема 2. *Рассмотрим последовательность* (k,n), *такую что* $\lim\limits_{k,n\to\infty} k/n > C/R(\boldsymbol{d})$. *Тогда*

$$\lim_{k,n\to\infty} \underline{\nu}(k,n) = \lim_{k,n\to\infty} \overline{\nu}(k,n) = 1.$$

Далее рассмотрим более тонкий режим. Пусть последовательность (k,n) такова, что $k/n \to C/R(\boldsymbol{d})$ по некоторому специально выбранному закону. В частности,

пусть последовательность параметризована величиной $\rho \in \mathbb{R}$ следующим образом:

$$\frac{k}{n} = \frac{C}{R(\boldsymbol{d})} + \frac{\rho}{\sqrt{n}}. \tag{9}$$

Для такой последовательности имеет место следующий результат.

Теорема 3. *Пусть* $V_{\mathrm{C}}^{+} = V_{\mathrm{C}}^{-} = V_{\mathrm{C}}$. *Тогда для последовательности* (k, n), *удовлетворяющей* (9), *справедливы равенства*

$$\lim_{k,n\to\infty} \underline{\nu}(k,n) = \lim_{k,n\to\infty} \overline{\nu}(k,n) = \mathrm{Q}\left(\frac{-\rho R(\boldsymbol{d})}{\sqrt{V_{\mathrm{C}} + \dfrac{C}{R(\boldsymbol{d})} V_{\mathrm{S}}(\boldsymbol{d})}}\right).$$

Этот результат показывает, что в отличие от теорем 1 и 2 верхняя и нижняя цена игры стремятся к промежуточному значению между нулем и единицей. Это неэкстремальное значение достигается при выборе последовательности с пределом $C/R(\boldsymbol{d})$, являющимся пороговым значением для надежной передачи в постановке совместного кодирования источника и канала. Такое понимание более тонкой асимптотики возможно исключительно благодаря основанным на дисперсии границам высших порядков, которые выводятся в последующих параграфах.

§ 4. Нижняя граница на максимин

Приступая к выводу вышеуказанных результатов, установим границы на $\overline{\nu}(k,n)$ и $\underline{\nu}(k,n)$ при конечной длине блока. В этом параграфе мы выведем нижнюю границу на $\underline{\nu}(k,n)$ путем ослабления внутренней минимизации по $(Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y})$ в задаче о максимине. Для каждого $q \in \mathcal{P}(\mathcal{T}^n)$ задачу минимизации можно представить в виде

$$\mathrm{SC}(q)\colon \quad \min_{Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y}} \sum_{s,x,y,\widehat{s}} \mathbb{I}\{d(s,\widehat{s}) > \boldsymbol{d}\} Q(s,x,y,\widehat{s})$$

$$\text{при условиях} \quad Q(s,x,y,\widehat{s}) \equiv P_S(s) Q_{X\,|\,S}(x\,|\,s) P_{Y_q\,|\,X}(y\,|\,x) Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y),$$

$$\sum_{x} Q_{X\,|\,S}(x\,|\,s) = 1 \quad \forall s,$$

$$\sum_{\widehat{s}} Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y) = 1 \quad \forall y,$$

$$Q_{X\,|\,S}(x\,|\,s), Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y) \geqslant 0 \quad \forall s,x,y,\widehat{s},$$

где $P_{Y_q\,|\,X}(y\,|\,x) := \sum\limits_{\theta\in\mathcal{T}^n} q(\theta) P_{Y\,|\,X,\boldsymbol{\Theta}}(y\,|\,x,\theta)$.

Эта задача невыпукла в пространстве распределений $(Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y})$ [6]. Возможным подходом к таким задачам является получение выпуклого ослабления путем включения невыпуклой области допустимых решений в некоторое выпуклое множество. Рассмотрим ослабление, основанное на линейном программировании (ЛП-ослабление), которое было представлено в [12] и получено методом типа подъема и проекции.

В этом методе целевая функция и ограничения линеаризуются путем замены произведений $Q_{X\,|\,S}(x\,|\,s) Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y)$ на вспомогательную переменную $V(s,x,y,\widehat{s})$. Затем добавляются ограничения, обеспечивающие тождественное равенство $V(s,x,y,\widehat{s}) \equiv$ $\equiv Q_{X\,|\,S}(x\,|\,s) Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y)$. Наконец, для получения ослабления задачи $\mathrm{SC}(q)$ условие $V(s,x,y,\widehat{s}) \equiv Q_{X\,|\,S}(x\,|\,s) Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y)$ опускается. Фактически невыпуклая область допустимых решений в задаче $\mathrm{SC}(q)$ аппроксимируется многогранником, тем самым

задавая *поднятие* задачи в пространство большей размерности. Результатом этого являются следующая задача линейного программирования:

$$\mathrm{LP}(q)\colon \quad \min_{Q_{X\,|\,S},Q_{\widehat{S}\,|\,Y},V} \sum_{s,x,y,\widehat{s}} \mathbb{I}\{d(s,\widehat{s}) > \boldsymbol{d}\}\bar{Q}(s,x,y,\widehat{s})$$

$$\text{при условиях} \quad \bar{Q}(s,x,y,\widehat{s}) \equiv P_S(s)P_{Y_q\,|\,X}(y\,|\,x)V(s,x,y,\widehat{s}),$$

$$\sum_x Q_{X\,|\,S}(x\,|\,s) = 1 \,:\gamma_q^{\mathrm{S}}(s) \quad \forall s,$$

$$\sum_{\widehat{s}} Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y) = 1 \,:\gamma_q^{\mathrm{C}}(y) \quad \forall y,$$

$$\sum_x V(s,x,y,\widehat{s}) - Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y) = 0 \,:\lambda_q^{\mathrm{S}}(s,\widehat{s},y) \quad \forall s,\widehat{s},y,$$

$$\sum_{\widehat{s}} V(s,x,y,\widehat{s}) - Q_{X\,|\,S}(x\,|\,s) = 0 \,:\lambda_q^{\mathrm{C}}(x,s,y) \quad \forall x,s,y,$$

$$Q_{X\,|\,S}(x\,|\,s), Q_{\widehat{S}\,|\,Y}(\widehat{s}\,|\,y) \geqslant 0 \quad \forall s,x,y,\widehat{s},$$

$$V(s,x,y,\widehat{s}) \geqslant 0 \quad \forall s,x,y,\widehat{s},$$

где функции $\gamma_q^{\mathrm{S}}\colon \mathcal{S}^k \to \mathbb{R}$, $\gamma_q^{\mathrm{C}}\colon \mathcal{Y}^n \to \mathbb{R}$, $\lambda_q^{\mathrm{S}}\colon \mathcal{S}^k \times \mathcal{S}^k \times \mathcal{Y}^n \to \mathbb{R}$ и $\lambda_q^{\mathrm{C}}\colon \mathcal{S}^k \times \mathcal{X}^n \times \mathcal{Y}^n \to \mathbb{R}$ – множители Лагранжа.

Любая допустимая точка для задачи $\mathrm{LP}(q)$ задается тройкой $(Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y}, V)$, а соответствующая допустимая точка задачи $\mathrm{SC}(q)$ получается проекцией этой тройки на пространство пар $(Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y})$. Последовательно повторяя эту процедуру, получаем все более точные выпуклые реализации исходной задачи. Дальнейшие подробности о методе поднятия и проекции можно найти в [26, гл. 5].

Очевидно, справедливо неравенство

$$\mathrm{OPT}(\mathrm{SC}(q)) \geqslant \mathrm{OPT}(\mathrm{LP}(q)), \quad \forall q \in \mathcal{P}(\mathcal{T}^n).$$

Теперь сформулируем двойственную задачу для $\mathrm{LP}(q)$ и, используя слабую двойственность, оценим оптимальное значение для $\mathrm{LP}(q)$, получая тем самым границу на $\mathrm{OPT}(\mathrm{SC}(q))$. Соответствующая двойственная задача выглядит следующим образом:

$$\mathrm{DP}(q)\colon \quad \max_{\gamma_q^{\mathrm{S}},\gamma_q^{\mathrm{C}},\lambda_q^{\mathrm{S}},\lambda_q^{\mathrm{C}}} \sum_s \gamma_q^{\mathrm{S}}(s) + \sum_y \gamma_q^{\mathrm{C}}(y)$$

$$\text{при условиях} \quad \gamma_q^{\mathrm{S}}(s) - \sum_y \lambda_q^{\mathrm{C}}(x,s,y) \leqslant 0 \quad \forall x,s,$$

$$\gamma_q^{\mathrm{C}}(y) - \sum_s \lambda_q^{\mathrm{S}}(s,\widehat{s},y) \leqslant 0 \quad \forall \widehat{s},y,$$

$$\lambda_q^{\mathrm{S}}(s,\widehat{s},y) + \lambda_q^{\mathrm{C}}(x,s,y) \leqslant \Pi(s,x,y,\widehat{s}) \quad \forall s,x,y,\widehat{s},$$

где $\Pi(s,x,y,\widehat{s}) \equiv \mathbb{I}\{d(s,\widehat{s}) > \boldsymbol{d}\}P_S(s)P_{Y_q\,|\,X}(y\,|\,x)$. Из слабой двойственности следует, что $\mathrm{OPT}(\mathrm{SC}(q)) \geqslant \mathrm{OPT}(\mathrm{LP}(q)) = \mathrm{OPT}(\mathrm{DP}(q))$ $\forall q$, и согласно результатам [18] получаем

$$\underline{\nu}(k,n) = \max_q \mathrm{OPT}(\mathrm{SC}(q)) \geqslant \max_q \mathrm{OPT}(\mathrm{LP}(q)) =$$
$$= \max_q \mathrm{OPT}(\mathrm{DP}(q)) \geqslant \mathrm{FEAS}(\mathrm{DP}(q)), \tag{10}$$

где $\mathrm{FEAS}(\mathrm{DP}(q))$ – значение целевой функции для $\mathrm{DP}(q)$, вычисленное в допустимой точке. Таким образом, для вывода нижней границы на минимакс и максимин нашей игры с нулевой суммой достаточно получить допустимое решение задачи $\mathrm{DP}(q)$. В следующей теореме приводится одна такая конструкция и вычисляется целевая функция двойственной задачи $\mathrm{DP}(q)$ для этого допустимого решения, давая тем самым нижнюю границу на максимин.

Т е о р е м а 4. *Значение $\underline{\nu}(k,n)$ ограничено снизу следующим образом*:

$$\begin{aligned}
&\underline{\nu}(k,n) \geqslant \max_q \mathrm{OPT}(\mathrm{DP}(q)) \geqslant \\
&\geqslant \max_{q, P_{\overline{Y}_q}, \mathrm{U}} \sup_{\gamma>0} \Bigg[\sum_s P_S(s) \min_x \Bigg[\mathbf{P}\Big(j_S(s,\boldsymbol{d}) - i_{X;\overline{Y}_q|U}(x;Y\,|\,U) \leqslant \gamma \Big) + \\
&+ \exp(j_S(s,\boldsymbol{d}) - \gamma) \sum_{u=1}^{\mathrm{U}} \sum_y P_{U|X}(u\,|\,x) P_{\overline{Y}_q|U}(y\,|\,u) \times \\
&\times \mathbb{I}\Big\{ j_S(s,\boldsymbol{d}) - i_{X;\overline{Y}_q|U}(x;y\,|\,u) > \gamma \Big\} \Bigg] - \frac{\mathrm{U}}{\exp(\gamma)} \Bigg],
\end{aligned} \tag{11}$$

где $U \in \mathcal{U} := \{1,\dots,\mathrm{U}\}$, $\mathrm{U} \in \mathbb{N}$, $P_{\overline{Y}_q} \in \mathcal{P}(\mathcal{Y}^n)$, $i_{X;\overline{Y}_q|U}(x;y\,|\,u) = \dfrac{\log P_{Y_q|X,U}(y\,|\,x,u)}{P_{\overline{Y}_q|U}(y\,|\,u)}$, *а* $j_S(s,\boldsymbol{d})$ – $\boldsymbol{d}$*-скошенная информация, определенная в п.* 2.4.

Д о к а з а т е л ь с т в о. Определим случайную величину U, принимающую значения в множестве $\mathcal{U} := \{1,\dots,\mathrm{U}\}$, такую что

$$P_{Y_q|X}(y\,|\,x) = \sum_{u=1}^{\mathrm{U}} P_{U|X}(u\,|\,x) P_{Y_q|X,U}(y\,|\,x,u).$$

Рассмотрим следующие двойственные переменные для $\mathrm{DP}(q)$:

$$\begin{aligned}
&\lambda_q^{\mathrm{S}}(s,\widehat{s},y) \equiv -\mathbb{I}\{d(s,\widehat{s}) \leqslant \boldsymbol{d}\} \frac{P_S(s) \sum\limits_{u=1}^{\mathrm{U}} P_{\overline{Y}_q|U}(y\,|\,u)}{\exp(\gamma - j_S(s,\boldsymbol{d}))}, \\
&\lambda_q^{\mathrm{C}}(x,s,y) \equiv P_S(s) \sum_{u=1}^{\mathrm{U}} P_{U|X}(u\,|\,x) \min\Big\{ P_{Y_q|X,U}(y\,|\,x,u), \frac{P_{\overline{Y}_q|U}(y\,|\,u)}{\exp(\gamma - j_S(s,\boldsymbol{d}))} \Big\}, \\
&\gamma_q^{\mathrm{S}}(s) \equiv \min_x \sum_y \lambda_q^{\mathrm{C}}(x,s,y), \quad \gamma_q^{\mathrm{C}}(y) \equiv -\exp(-\gamma) \sum_{u=1}^{\mathrm{U}} P_{\overline{Y}_q|U}(y\,|\,u),
\end{aligned}$$

где $\gamma > 0$, $P_{\overline{Y}_q|U}(y\,|\,u) := \sum\limits_\theta q(\theta) P_{\overline{Y}|\boldsymbol{\Theta},U}(y\,|\,\theta,u)$, а $P_{\overline{Y}|\boldsymbol{\Theta},U}$ – произвольное распределение из $\mathcal{P}(\mathcal{Y}^n\,|\,\mathcal{T}^n,\mathcal{U})$.

Из доказательства теоремы 5.3 работы [12] следует, что такой выбор двойственных переменных является допустимым для задачи $\mathrm{DP}(q)$. При этом целевая функция двойственной задачи имеет вид

$$\begin{aligned}
&\sum_s \min_x \sum_y \lambda_q^{\mathrm{C}}(x,s,y) + \sum_y - \exp(-\gamma) \sum_{u=1}^{\mathrm{U}} P_{\overline{Y}_q|U}(y\,|\,u) \geqslant \\
&\geqslant \sum_s \min_x \sum_y P_S(s) \sum_{u=1}^{\mathrm{U}} P_{U|X}(u\,|\,x) \min\Big\{ P_{Y_q|X,U}(y\,|\,x,u), \frac{P_{\overline{Y}_q|U}(y\,|\,u)}{\exp(\gamma - j_S(s,\boldsymbol{d}))} \Big\} -
\end{aligned}$$

$$- \frac{\sum\limits_{y}\sum\limits_{u=1}^{\mathrm{U}} P_{\overline{Y}_q|U}(y\,|\,u)}{\exp(\gamma)} = \sum_s P_S(s) \min_x \Bigg[\sum_{u=1}^{\mathrm{U}} \sum_y P_{U|X}(u\,|\,x) P_{Y_q|X,U}(y\,|\,x,u) \times$$

$$\times \mathbb{I}\Big\{ \frac{P_{Y_q|X,U}(y\,|\,x,u)}{P_{\overline{Y}_q|U}(y\,|\,u)} \leqslant \frac{\exp(j_S(s,\boldsymbol{d}))}{\exp(\gamma)} \Big\} + \frac{1}{\exp(\gamma - j_S(s,\boldsymbol{d}))} \sum_{u=1}^{\mathrm{U}} \sum_y P_{U|X}(u\,|\,x) \times$$

$$\times P_{\overline{Y}_q|U}(y\,|\,u) \mathbb{I}\Big\{ \frac{P_{Y_q|X,U}(y\,|\,x,u)}{P_{\overline{Y}_q|U}(y\,|\,u)} > \frac{\exp(j_S(s,\boldsymbol{d}))}{\exp(\gamma)} \Big\} \Bigg] - \frac{\mathrm{U}}{\exp(\gamma)}.$$

Полагая $i_{X;\overline{Y}_q|U}(x;y\,|\,u) = \log P_{Y_q|X,U}(y\,|\,x,u)/P_{\overline{Y}_q|U}(y\,|\,u)$, получаем

$$\sum_s \min_x \sum_y \lambda_q^{\mathrm{C}}(x,s,y) + \sum_y - \exp(-\gamma) \sum_{u=1}^{\mathrm{U}} P_{\overline{Y}_q|U}(y\,|\,u) =$$

$$= \sum_s P_S(s) \min_x \Bigg[\mathbf{P}\Big(i_{X;\overline{Y}_q|U}(x;Y\,|\,U) - j_S(s,\boldsymbol{d}) \leqslant -\gamma \Big) +$$

$$+ \exp(j_S(s,\boldsymbol{d}) - \gamma) \sum_{u=1}^{\mathrm{U}} \sum_y P_{U|X}(u\,|\,x) P_{\overline{Y}_q|U}(y\,|\,u) \times$$

$$\times \mathbb{I}\Big\{ i_{X;\overline{Y}_q|U}(x;y\,|\,u) - j_S(s,\boldsymbol{d}) > -\gamma \Big\} \Bigg] - \frac{\mathrm{U}}{\exp(\gamma)}.$$

Переходя к супремуму по γ и максимуму по U, $P_{\overline{Y}_q}$ и q в этом равенстве, получаем выражение в правой части формулы (11). Требуемая граница вытекает из соотношений (10). ▲

ЛП-ослабление дает границу снизу на верхнюю и нижнюю цену игры. Таким образом, эта граница определяет также обращение теоремы кодирования для задачи совместного кодирования источника и канала с потерями в произвольно меняющемся канале. Эта нижняя граница справедлива для всех стратегий источника помех и не требует предположения о том, что стратегия является н.о.р.

Известно, что такая техника ослабления, основанного на линейном программировании, предложенная в [12], дает точные и улучшенные обращения теоремы кодирования для множества задач кодирования, как указано в [12, 13, 19]. Для больших длин блока этот метод приводит к достаточно близкому выпуклому ослаблению задачи кодирования, подчеркивая тем самым ее почти выпуклую природу. Получение границы снизу на вероятность ошибки основывается только на построении подходящих переменных в двойственной задаче, и поэтому метод ослабления представляет собой структурный подход к выводу границ.

Теперь перейдем к выводу верхней границы с помощью построения кода, достигающего пропускной способности, в задаче совместного кодирования источника и канала.

§ 5. Верхняя граница на минимакс

Для вывода верхней границы на величину минимакса $\overline{\nu}(k,n)$ построим стохастический код для задачи совместного кодирования источника и канала. Напомним, что стохастический код для совместного кодирования источника и канала – это пара распределений $(Q_{X|S}, Q_{\widehat{S}|Y})$, где $Q_{X|S} \in \mathcal{P}(\mathcal{X}^n\,|\,\mathcal{S}^k)$ и $Q_{\widehat{S}|Y} \in \mathcal{P}(\mathcal{S}^k\,|\,\mathcal{Y}^n)$.

В настоящей статье мы рассматриваем стохастический код со стохастическим кодированием и детерминированным декодированием. Для построения такого стоха-

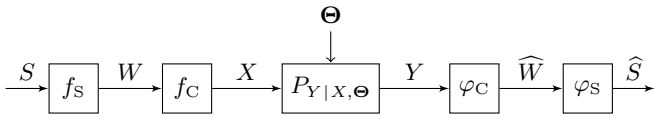

Рис. 1. Совместное кодирование источника и канала

стического кода будем рассматривать случайный код для совместного кодирования источника и канала, а также детерминированный код для канала. Применяя идеи редукции случайных кодов, построим другой случайный код с равномерным распределением на меньшем количестве кодов. Кодер случайным образов выбирает код из этого ансамбля для передачи сообщения, а затем использует детерминированный код для передачи декодеру номера этого кода из ансамбля. Декодер восстанавливает этот номер с помощью детерминированного кода, а затем использует код с этим номером для декодирования исходного сообщения.

Чтобы построить стохастический код для совместного кодирования источника и канала, вначале рассмотрим детерминированный код для канала, дающий гарантированную среднюю вероятность ошибки.

5.1. Детерминированный код для канала для заданной средней вероятности ошибки. Вначале рассмотрим детерминированный код для канала, не зависящий от кода, выбираемого для передачи сообщений. Пусть $(f_{\mathrm{c}}, \varphi_{\mathrm{c}})$ – код для канала, определенный в п. 2.2.

Известен следующий результат [11, теорема 1], обеспечивающий существование детерминированного кода для заданной средней вероятности ошибки.

Теорема 5. *Пусть* $P_X \in \mathcal{P}(\mathcal{X}^n)$, *пусть* $Z(x, \bar{x}, y) \in \{0, 1\}$ – *функция, такая что*

$$Z(x, \bar{x}, y)Z(\bar{x}, x, y) = 0 \quad \forall x \in \mathcal{X}^n,\ \bar{x} \in \mathcal{X}^n,\ y \in \mathcal{Y}^n, \tag{12}$$

и пусть $\mathcal{A} \subset \mathcal{X}^n \times \mathcal{Y}^n$ – *типичное множество. Пусть* $(X, \bar{X}, Y) \sim P_X \times P_X \times P_{Y\,|\,X,\boldsymbol{\Theta}}$. *Тогда существует детерминированный код* $(f_{\mathrm{c}}, \varphi_{\mathrm{c}})$ *для канала, такой что*

$$\begin{aligned}\bar{e}(f_{\mathrm{c}}, \varphi_{\mathrm{c}}) \leqslant \sqrt{\frac{2\ln(3|\mathcal{T}|^n)}{M}} + \min_{P_X} \max_{\theta \in \mathcal{T}^n} \Big(& \mathbf{P}\big((X, Y) \notin \mathcal{A} \,|\, \theta\big) + \\ & + 2\log 3|\mathcal{T}|^n \max_{\bar{x} \in \mathcal{X}^n} \mathbf{P}\big(Z(X, \bar{x}, Y) = 0,\ (X, Y) \in \mathcal{A} \,|\, \theta\big) + \\ & + 2M \log e\, \mathbf{P}\big(Z(X, \bar{X}, Y) = 0,\ (X, Y) \in \mathcal{A} \,|\, \theta\big)\Big).\end{aligned} \tag{13}$$

Таким образом, имеется детерминированный код для канала, дающий верхнюю границу на среднюю вероятность ошибки. Теперь построим случайный код для совместного кодирования источника и канала.

5.2. Случайный код для совместного кодирования источника и канала. Схема совместного кодирования источника и канала представлена на рис. 1. Пусть $W \in \in \mathcal{W} = \{1, \ldots, M\}$ – случайная величина на выходе кодера, где $M \in \mathbb{N}$, а $\widehat{W} \in \mathcal{W}$ – случайная величина на входе декодера. Код для источника – это пара функций $(f_{\mathrm{S}}, \varphi_{\mathrm{S}})$, определенная в п. 2.3. Код для канала – это пара функций $(f_{\mathrm{C}}, \varphi_{\mathrm{C}})$, определенная в п. 2.2. Композиция этих двух кодов задает код (f, φ) для совместного кодирования источника и канала вида

$$f := (f_{\mathrm{C}} \circ f_{\mathrm{S}})\colon \mathcal{S}^k \to \mathcal{X}^n, \quad \varphi := (\varphi_{\mathrm{S}} \circ \varphi_{\mathrm{C}})\colon \mathcal{Y}^n \to \mathcal{S}^k.$$

Случайный код для совместного кодирования источника и канала – это пара случайных величин (F, Φ), принимающих значения в множестве $\{(f,\varphi) \mid f\colon \mathcal{S}^k \to \mathcal{X}^n, \varphi\colon \mathcal{Y}^n \to \mathcal{S}^k\}$. Вероятность ошибки для детерминированного кода для совместного кодирования источника и канала имеет вид $e_{\boldsymbol{d},\theta}(f,\varphi) := \sum\limits_{s,y} \mathbb{I}\{d(s,\varphi(y)) > \boldsymbol{d}\} P_S(s) \times$ $\times\, P_{Y\,|\,X,\boldsymbol{\Theta}}(y\,|\,f(s),\theta)$. Соответственно, ошибка для случайного кода $(F,\Phi) \sim \psi$ для совместного кодирования источника и канала определяется следующим образом:

$$e_{\boldsymbol{d},\theta}(\psi) := \mathbf{E}[e_{\boldsymbol{d},\theta}(F,\Phi)], \quad e_{\boldsymbol{d}}(\psi) := \max_{\theta\in\mathcal{T}^n} \mathbf{E}[e_{\boldsymbol{d},\theta}(\psi)].$$

Теперь построим случайный код для совместного кодирования источника и канала подобно тому, как в [9] был построен детерминированный код для задачи совместного кодирования источника и канала для ДКБП без преднамеренных помех.

Теорема 6. *Существует случайный код ψ, такой что для его вероятности ошибки справедлива оценка сверху*

$$e_{\boldsymbol{d}}(\psi) \leqslant \min_{P_{L\,|\,S}} \max_{\theta\in\mathcal{T}^n} \Big(\mathbf{E}\Big[\exp\Big(-\big|i_{X;Y_{q^*}}(X;Y) - \log L\big|^+\Big)\,|\,\theta\Big] + \mathbf{E}\Big[\big(1 - P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))\big)^L\Big]\Big),$$

где $(S, L, \widehat{S}, X, Y) \sim P_S \times P_{L\,|\,S} \times P_{\widehat{S}} \times P_X \times P_{Y\,|\,X,\boldsymbol{\Theta}=\theta}$,

$$i_{X;Y_{q^*}}(x;y) = \log \frac{(q^* P_{Y\,|\,X,\boldsymbol{\Theta}})(y\,|\,x)}{(P_X q^* P_{Y\,|\,X,\boldsymbol{\Theta}})(y)},$$

причем $(X,Y) \sim P_X \times P_{Y\,|\,X,\boldsymbol{\Theta}=\theta}$, $q^*(\theta) = \prod\limits_{i=1}^n q^*_\Theta(\theta_i)$, $q^*_\Theta \in \Pi_\Theta$ *и* $\mathcal{B}_{\boldsymbol{d}}(s) := \big\{\widehat{s} \in \mathcal{S}^k : d(s,\widehat{s}) \leqslant \boldsymbol{d}\big\}$.

Доказательство. Случайный код ψ будем строить следующим образом. Вначале построим случайный код $(F_{\mathrm{S}}, \Phi_{\mathrm{S}})$ для источника сообщений. Затем для конкретной реализации кода $(f_{\mathrm{S}}, \varphi_{\mathrm{S}})$ для источника построим случайный код $(F_{\mathrm{C}}, \Phi_{\mathrm{C}})$ для канала.

Кодирование для источника: Порождаются M кодовых слов из множества $\mathcal{S}^k$ согласно распределению $P_{\widehat{S}} \in \mathcal{P}(\mathcal{S}^k)$ каждое. Обозначим i-е кодовое слово через $\widehat{S}_i$. Далее для заданного исходного сообщения источника $s \in \mathcal{S}^k$ порождается случайная величина $L \sim P_{L\,|\,S=s} \in \mathcal{P}(\mathbb{N}\,|\,\mathcal{S}^k)$, где $L \leqslant M$. Кодер кодирует сообщение s как

$$F_{\mathrm{S}}(s) = \begin{cases} \min\{m, L\}, & d(s,\widehat{S}_m) \leqslant \boldsymbol{d} < \min\limits_{i<m} d(s,\widehat{S}_i), \\ L, & \boldsymbol{d} < \min\limits_{i=1,\ldots,L} d(s,\widehat{S}_i), \end{cases}$$

где d – функция искажения, а $\boldsymbol{d}$ – максимальный уровень искажения, определенные в п. 2.3.

Декодирование для источника: Декодер сообщений декодирует выход m декодера канала как $\Phi_{\mathrm{S}}(m) = \widehat{S}_m$.

Теперь для заданной реализации кода $(F_{\mathrm{S}}, \Phi_{\mathrm{S}}) = (f_{\mathrm{S}}, \varphi_{\mathrm{S}})$ для источника построим случайный код для канала.

Кодирование для канала: Определим M случайных величин $\{X_m\}_{m=1}^M$ с распределением $P_X \in \mathcal{P}(\mathcal{X}^n)$ каждая. Для заданного выхода m кодера источника кодер канала кодирует его как $F_{\mathrm{C}}(m) = X_m$.

Декодирование для канала: Для функции декодирования канала определим случайную величину $U \in \{1,\ldots,M+1\}$ следующим образом:

$$U = \begin{cases} f_{\mathrm{S}}(S), & d(S, \varphi_{\mathrm{S}} \circ f_{\mathrm{S}}(S)) \leqslant \boldsymbol{d}, \\ M+1 & \text{в противном случае.} \end{cases}$$

Положим $P_{Y_{q^*}|X}(y\,|\,x) := \sum\limits_{\theta\in\mathcal{T}^n} q^*(\theta)P_{Y|X,\boldsymbol{\Theta}}(y\,|\,x,\theta)$, где $q^*(\theta) = \prod\limits_{i=1}^{n} q^*_\Theta(\theta_i)$, $q^*_\Theta \in \Pi_\Theta$. Для наблюдаемого выхода канала y декодер канала декодирует его следующим образом:

$$\Phi_{\mathrm{C}}(y) = m \in \operatorname*{arg\,max}_{j\in\{1,\dots,M\}} P_{U|\widehat{S}^M}\big(j\,|\,\widehat{s}^M\big)P_{Y_{q^*}|X}(y\,|\,X_j),$$

где $P_{U|\widehat{S}^M} \in \mathcal{P}\big(\{1,\dots,M+1\}\,|\,(\mathcal{S}^k)^M\big)$.

Пусть ψ – распределение, индуцированное распределением $P_{\widehat{S}}$ кодовой книги источника и распределением P_X кодовой книги канала, на множестве кодов для совместного кодирования источника и канала $\{(f,\varphi) \mid f\colon \mathcal{S}^k \to \mathcal{X}^n,\ \varphi\colon \mathcal{Y}^n \to \mathcal{S}^k\}$. Теперь вычислим вероятность ошибки для этого случайного кода ψ при фиксированном $\theta \in \mathcal{T}^n$. Пусть $\widehat{s}^M = (\widehat{s}_1,\dots,\widehat{s}_M) \in \mathcal{S}^k$ и $x^M = (x_1,\dots,x_M) \in \mathcal{X}^n$ – кодовые книги источника и канала. Вероятность ошибки оценивается сверху как

$$\begin{aligned}&\mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\,|\,\widehat{s}^M, x^M, \theta\big) \leqslant \mathbf{P}\big(d(S,\varphi_{\mathrm{S}}\circ f_{\mathrm{S}}(S)) > \boldsymbol{d}\,|\,\widehat{s}^M\big) + \\ &+ \mathbf{P}\big(\varphi_{\mathrm{C}}(Y) \neq f_{\mathrm{S}}(S)\,|\,\widehat{s}^M, x^M, \theta, d(S,\varphi_{\mathrm{S}}\circ f_{\mathrm{S}}(S)) \leqslant \boldsymbol{d}\big),\end{aligned} \tag{14}$$

где первое слагаемое – это ошибка кодирования источника, а второе – ошибка декодирования в канале при отсутствии ошибки кодирования источника. Ошибку кодирования можно представить в виде $\mathbf{P}\big(d(S,\varphi_{\mathrm{S}}\circ f_{\mathrm{S}}(S)) > \boldsymbol{d}\,|\,\widehat{s}^M\big) = \mathbf{P}\big(U > L\,|\,\widehat{s}^M\big)$, так как $\{d(S,\varphi_{\mathrm{S}}\circ f_{\mathrm{S}}(S)) > \boldsymbol{d}\} = \{U > L\}$. Ошибку декодирования в канале можно вычислить следующим образом:

$$\begin{aligned}&\mathbf{P}\big(\varphi_{\mathrm{C}}(Y) \neq f_{\mathrm{S}}(S)\,|\,\widehat{s}^M, x^M, \theta, d(S,\varphi_{\mathrm{S}}\circ f_{\mathrm{S}}(S)) \leqslant \boldsymbol{d}\big) = \\ &= \mathbf{P}\big(\varphi_{\mathrm{C}}(Y) \neq U\,|\,\widehat{s}^M, x^M, \theta\big) = \\ &= \sum_{m=1}^{M} P_{U|\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big)\,\mathbf{P}\big(\varphi_{\mathrm{C}}(Y) \neq m\,|\,x^M,\theta\big) = \\ &= \sum_{m=1}^{M} P_{U|\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big)\,\mathbf{P}\left(\bigcup_{m'=1}^{M} \frac{P_{U|\widehat{S}^M}\big(m'\,|\,\widehat{s}^M\big)P_{Y_{q^*}|X}(Y\,|\,X_{m'})}{P_{U|\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big)P_{Y_{q^*}|X}(Y\,|\,X_m)} \geqslant 1\,|\,x^M,\theta\right),\end{aligned} \tag{15}$$

где (15) следует из того факта, что $d(S,\varphi_{\mathrm{S}}\circ f_{\mathrm{S}}(S)) \leqslant \boldsymbol{d}$ влечет $f_{\mathrm{S}}(S) = U$.

Усредняя по кодовым книгам $(\widehat{s}^M, x^M)$, получаем

$$\sum_{\widehat{s}^M, x^M} P_{\widehat{S}^M}\big(\widehat{s}^M\big)P_{X^M}\big(x^M\big)\,\mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\,|\,\widehat{s}^M, x^M, \theta\big) = \mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\,|\,\theta\big) = e_{\boldsymbol{d},\theta}(\psi),$$

где $P_{\widehat{S}^M}(\widehat{s}^M) = \prod\limits_{i=1}^{M} P_{\widehat{S}}(\widehat{s}_i)$, $\widehat{s}_i \in \mathcal{S}^k$, и $P_{X^M}(x^M) = \prod\limits_{i=1}^{M} P_X(x_i)$, $x_i \in \mathcal{X}^n$. Тогда получаем $\mathbf{P}\big(d(S,\widehat{S}) > \boldsymbol{d}\,|\,\theta\big) = e_{\boldsymbol{d},\theta}(\psi)$, поскольку рассматриваемый случайный код индуцирован распределениями P_{X^M} и $P_{\widehat{S}^M}$.

Подставляя это в (14), получаем

$$\begin{aligned}&e_{\boldsymbol{d},\theta}(\psi) \leqslant \mathbf{P}(U > L) + \sum_{\widehat{s}^M} P_{\widehat{S}^M}\big(\widehat{s}^M\big) \sum_{m=1}^{M} P_{U|\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big) \times \\ &\times \mathbf{P}\left(\bigcup_{m'=1}^{M} \frac{P_{U|\widehat{S}^M}\big(m'\,|\,\widehat{s}^M\big)P_{Y_{q^*}|X}(Y\,|\,X_{m'})}{P_{U|\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big)P_{Y_{q^*}|X}(Y\,|\,X_m)} \geqslant 1\,|\,\theta\right).\end{aligned} \tag{16}$$

Повторяя рассуждения из доказательства [9, теорема 7], получаем

$$\sum_{\widehat{s}^M} P_{\widehat{S}^M}\big(\widehat{s}^M\big) \sum_{m=1}^{M} P_{U\,|\,\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big) \times$$
$$\times\, \mathbf{P}\left(\bigcup_{m'=1}^{M} \frac{P_{U\,|\,\widehat{S}^M}\big(m'\,|\,\widehat{s}^M\big) P_{Y_{q^*}\,|\,X}(Y\,|\,X_{m'})}{P_{U\,|\,\widehat{S}^M}\big(m\,|\,\widehat{s}^M\big) P_{Y_{q^*}\,|\,X}(Y\,|\,X_m)} \geqslant 1\,|\,\theta \right) \leqslant$$
$$\leqslant \mathbf{E}\Big[\exp\big(-|i_{X;Y_{q^*}}(X;Y) - \log L|^+\big)\,|\,\theta\Big]$$

и $\mathbf{P}(U > L) = \mathbf{E}\big[(1 - \mathbf{P}(\mathcal{B}_{\boldsymbol{d}}(S)))^L\big]$. Подставляя это в (16), получаем

$$e_{\boldsymbol{d},\theta}(\psi) \leqslant \mathbf{E}\Big[\exp\big(-|i_{X;Y_{q^*}}(X;Y) - \log L|^+\,|\,\theta\big)\Big] + \mathbf{E}\Big[\big(1 - P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))\big)^L\Big].$$

Переходя к минимуму по распределениям $P_{L\,|\,S}$ и максимуму по состояниям θ, получаем требуемую оценку. ▲

Теперь сформулируем более слабую оценку, полагая $L = \lfloor \gamma / P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S)) \rfloor$, где $\gamma > 0$ выбирается произвольным образом согласно [9, теорема 8].

Теорема 7. *Существует случайный код ψ для совместного кодирования источника и канала, такой что*

$$e_{\boldsymbol{d}}(\psi) \leqslant \inf_{\gamma>0} \max_{\theta\in\mathcal{T}^n} \left(\mathbf{E}\left[\exp\left(-\left| i_{X;Y_{q^*}}(X;Y) - \frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))} \right|^+ \right) |\,\theta \right] + e^{1-\gamma} \right),$$

где величины $(S, \widehat{S}, X, Y)$ описаны в теореме 6.

Теперь, используя детерминированный код для канала и случайный код для совместного кодирования источника и канала, построим стохастический код для совместного кодирования источника и канала.

5.3. Стохастический код для совместного кодирования источника и канала и верхняя граница. Изложим подход к построению стохастического кода для совместного кодирования источника и канала. Для этого рассмотрим следующий вариант леммы о редукции случайного кода, приведенной в [10, гл. 4] (доказательство приведено в Приложении).

Лемма 1. *Пусть задано $\varepsilon > 0$. Рассмотрим случайный код $(F, \Phi) \sim \psi$, и пусть $e_{\boldsymbol{d}}(\psi) < \varepsilon$. Пусть $K \in \mathbb{N}$ и ε' таковы, что*

$$\varepsilon' > \varepsilon + \sqrt{\frac{\log|\mathcal{T}^n|}{2K}}. \tag{17}$$

Тогда существуют K детерминированных кодов $(f_i, \varphi_i)_{i=1}^K$ для совместного кодирования источника и канала, таких что

$$\frac{1}{K}\sum_{i=1}^{K} e_{\boldsymbol{d},\theta}(f_i, \varphi_i) < \varepsilon' \quad \forall\theta \in \mathcal{T}^n. \tag{18}$$

Предпочтительно иметь ε' как можно более близким к ε. Для этого достаточно взять $K = n^2$ и $\varepsilon' = \varepsilon + \sqrt{(\log|\mathcal{T}^n| + \varepsilon_0)/2K}$, где $\varepsilon_0 > 0$ сколь угодно мало. Таким образом можно добиться $\varepsilon' \sim \varepsilon$ при достаточно больших n.

Теперь построим код $(Q_{X\,|\,S}, \varphi)$ для совместного кодирования источника и канала, где $Q_{X\,|\,S}$ – стохастический кодер, а φ – детерминированный декодер. Конструкция та же, что в [10, теорема 12.13]. Рассматриваем K детерминированных

кодов $(f_i, \varphi_i)_{i=1}^K$, где $f_i\colon \mathcal{S}^k \to \mathcal{X}^n$ и $\varphi_i\colon \mathcal{Y}^n \to \mathcal{S}^k$ удовлетворяют условию (18). Случайно выбранный код из этого ансамбля используется для передачи сообщений из множества $\mathcal{S}^k$. Далее рассматриваем детерминированный код $(\widehat{f}, \widehat{\varphi})$, у которого $\widehat{f}\colon \{1, \dots, K\} \to \mathcal{X}^{d_n}$ и $\widehat{\varphi}\colon \mathcal{Y}^{d_n} \to \{1, \dots, K\}$ удовлетворяют условию (13), где d_n является функцией от n. Код $(\widehat{f}, \widehat{\varphi})$ используется для передачи номера i выбранного кода. Рассмотрим случайную величину $\boldsymbol{i} \in \{1, \dots, K\}$, распределенную равномерно и не зависящую от остальных случайных величин. Для заданного $s \in \mathcal{S}^k$ кодер выбирает входную последовательность $X \in \mathcal{X}^{d_n+n}$ случайным образом как $X = (\widehat{f}(\boldsymbol{i}), f_{\boldsymbol{i}}(s))$. Декодер $\varphi\colon \mathcal{Y}^{d_n+n} \to \mathcal{S}^k$ декодирует $y = (\widehat{y}, \bar{y}) \in \mathcal{Y}^{d_n+n}$ как

$$\varphi(y) = \begin{cases} s, & \text{если } (\widehat{\varphi}(\widehat{y}), \varphi_i(\bar{y})) = (i, s) \text{ для некоторого } i, \\ 0 & \text{в противном случае,} \end{cases}$$

где $\widehat{y} \in \mathcal{Y}^{d_n}$ и $\bar{y} \in \mathcal{Y}^n$.

Используя этот стохастический код для совместного кодирования источника и канала, оценим теперь нижнюю цену рассматриваемой игры с нулевой суммой. Отметим, что поскольку номер выбранного кода кодируется в виде последовательности длины d_n, то скорость передачи равна $k/(d_n + n)$.

Теорема 8. *Значение минимакса игры $\overline{v}(k, n)$ ограничено сверху следующим образом*:

$$\begin{aligned}
\overline{v}(k,n) &= \min_{Q_{X\,|\,S}, Q_{\widehat{S}\,|\,Y}} \max_q \mathbf{P}(d(S, \widehat{S}) > \boldsymbol{d}) \leqslant \\
&\leqslant \sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}} + \min_{P_{X_a}} \max_{\theta_a} \Big[\mathbf{P}\big((X_a, Y_a) \notin \mathcal{A}\,|\,\theta_a\big) + \\
&+ 2K \log e\, \mathbf{P}\big(Z(X_a, \bar{X}_a, Y_a) = 0, (X_a, Y_a) \in \mathcal{A}\,|\,\theta_a\big) + \\
&+ \max_{\bar{x}_a \in \mathcal{X}^{d_n}} 2\log 3|\mathcal{T}|^{d_n}\, \mathbf{P}\big(Z(X_a, \bar{x}_a, Y_a) = 0, (X_a, Y_a) \in \mathcal{A}\,|\,\theta_a\big) \Big] + \\
&+ \inf_{\gamma > 0} \max_{\theta_b} \left[\mathbf{E}\left[\exp\left(- \left| i_{X;Y_{q^*}}(X_b; Y_b) - \frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))} \right|^+ \right) | \, \theta_b \right] + e^{1-\gamma} \right] + \\
&+ \sqrt{\frac{\log|\mathcal{T}^n| + \varepsilon_0}{2K}}, \qquad (19)
\end{aligned}$$

где $\mathcal{X}^{d_n} \ni \bar{X}_a \sim P_{X_a}$, $\mathcal{X}^{d_n} \times \mathcal{Y}^{d_n} \ni (X_a, Y_a) \sim P_{X_a} P_{Y\,|\,X, \boldsymbol{\Theta}=\theta_a}$ для $\theta_a \in \mathcal{T}^{d_n}$, $\mathcal{X}^n \times \mathcal{Y}^n \ni (X_b, Y_b) \sim P_{X_b} P_{Y\,|\,X, \boldsymbol{\Theta}=\theta_b}$ для $\theta_b \in \mathcal{T}^n$, а $P_{X_a} \in \mathcal{P}(\mathcal{X}^{d_n})$ и $P_{X_b} \in \mathcal{P}(\mathcal{X}^n)$ – произвольные распределения. Величина $\varepsilon_0 > 0$ постоянна.

Доказательство. Максимальную вероятность ошибки оценим следующим образом:

$$\begin{aligned}
&\max_{\theta \in \mathcal{T}^{n+d_n}} \mathbf{P}\big(d(S, \widehat{S}) > \boldsymbol{d}\,|\,\boldsymbol{\Theta} = \theta\big) = \max_{\theta \in \mathcal{T}^{n+d_n}} \frac{1}{K} \sum_{i=1}^K \mathbf{P}\big(d(S, \widehat{S}) > \boldsymbol{d}\,|\,\boldsymbol{i} = i,\, \boldsymbol{\Theta} = \theta\big) = \\
&= \max_{\theta \in \mathcal{T}^{n+d_n}} \left(\frac{1}{K} \sum_{i=1}^K \mathbf{P}\big(d(S, \widehat{S}) > \boldsymbol{d},\, \widehat{\varphi}(Y_a) \neq i\,|\,\boldsymbol{i} = i,\, \boldsymbol{\Theta} = \theta\big) + \right. \\
&\left. + \frac{1}{K} \sum_{i=1}^K \mathbf{P}\big(d(S, \widehat{S}) > \boldsymbol{d},\, \widehat{\varphi}(Y_a) = i\,|\,\boldsymbol{i} = i,\, \boldsymbol{\Theta} = \theta\big) \right) \leqslant \\
&\leqslant \max_{\theta \in \mathcal{T}^{n+d_n}} \left(\frac{1}{K} \sum_{i=1}^K \mathbf{P}\big(\widehat{\varphi}(Y_a) \neq i\,|\,\boldsymbol{i} = i, \boldsymbol{\Theta} = \theta\big)' + \right.
\end{aligned}$$

$$+\frac{1}{K}\sum_{i=1}^{K}\mathbf{P}\big(d(S,\varphi_i(Y_b))>\boldsymbol{d}\,|\,\boldsymbol{i}=i,\ \boldsymbol{\Theta}=\theta\big)\Bigg)\leqslant$$

$$\leqslant\max_{\theta_a\in\mathcal{T}^{d_n}}\frac{1}{K}\sum_{i,y_a}\mathbb{I}\{\widehat{\varphi}(y_a)\neq i\}P_{Y\,|\,X,\boldsymbol{\Theta}}\big(y_a\,|\,\widehat{f}(i),\,\theta_a\big)+$$

$$+\max_{\theta_b\in\mathcal{T}^{n}}\frac{1}{K}\sum_{i,s,y_b}\mathbb{I}\{d(s,\varphi_i(y_b))>\boldsymbol{d}\}P_S(s)P_{Y\,|\,X,\boldsymbol{\Theta}}(y_b\,|\,f_i(s),\,\theta_b)=$$

$$=\max_{\theta_a\in\mathcal{T}^{d_n}}\frac{1}{K}\sum_{i,y_a}\mathbb{I}\{\widehat{\varphi}(y_a)\neq i\}P_{Y\,|\,X,\boldsymbol{\Theta}}\big(y_a\,|\,\widehat{f}(i),\,\theta_a\big)+\max_{\theta_b\in\mathcal{T}^{n}}\frac{1}{K}\sum_{i=1}^{K}e_{\boldsymbol{d},\theta_b}(f_i,\varphi_i).$$

Вначале оценим второе слагаемое. Возьмем $\varepsilon'=e_{\boldsymbol{d}}(\psi)+\sqrt{(\log|\mathcal{T}^n|+\varepsilon_0)/2K}$, где $\varepsilon_0>0$. Тогда по лемме 1 второе слагаемое можно оценить как

$$\frac{1}{K}\sum_{i}e_{\boldsymbol{d},\theta}(f_i,\varphi_i)\leqslant e_{\boldsymbol{d}}(\psi)+\sqrt{\log|\mathcal{T}^n|/2K}+\varepsilon_0\leqslant$$

$$\leqslant\inf_{\gamma>0}\max_{\theta_b}\left[\mathbf{E}\left[\exp\left(-\left|i_{X;Y_{q^*}}(X_b;Y_b)-\frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))}\right|^{+}\right)|\,\theta_b\right]+e^{1-\gamma}\right]+$$

$$+\sqrt{\frac{\log|\mathcal{T}^n|+\varepsilon_0}{2K}}. \tag{20}$$

Первый член оценим с помощью соотношения (13) из теоремы 5, и с учетом (20) получим

$$\max_{\theta\in\mathcal{T}^{n+d_n}}\mathbf{P}\big(d(S,\widehat{S})>\boldsymbol{d}\,|\,\boldsymbol{\Theta}=\theta\big)\leqslant\sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}}+$$

$$+\min_{P_{X_a}}\max_{\theta_a}\Big[\mathbf{P}\big((X_a,Y_a)\notin\mathcal{A}\,|\,\theta_a\big)+$$

$$+\max_{\bar{x}_a\in\mathcal{X}^{d_n}}2\log 3|\mathcal{T}|^{d_n}\,\mathbf{P}\big(Z(X_a,\bar{x}_a,Y_a)=0,(X_a,Y_a)\in\mathcal{A}\,|\,\theta_a\big)+$$

$$+2K\log e\,\mathbf{P}\big(Z(X_a,\bar{X}_a,Y_a)=0,(X_a,Y_a)\in\mathcal{A}\,|\,\theta_a\big)\Big]+$$

$$+\inf_{\gamma>0}\max_{\theta_b}\left[\mathbf{E}\left[\exp\left(-\left|i_{X;Y_{q^*}}(X_b;Y_b)-\frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))}\right|^{+}\right)|\,\theta_b\right]+e^{1-\gamma}\right]+$$

$$+\sqrt{\frac{\log|\mathcal{T}^n|+\varepsilon_0}{2K}}. \tag{21}$$

Используя равенство $\max\limits_{\theta\in\mathcal{T}^{d_n+n}}\mathbf{P}\big(d(S,\widehat{S})>\boldsymbol{d}\,|\,\boldsymbol{\Theta}=\theta\big)=\max\limits_{q\in\mathcal{P}(\mathcal{T}^{d_n+n})}\mathbf{P}\big(d(S,\widehat{S})>\boldsymbol{d}\big)$, получаем требуемый результат. ▲

Верхнюю границу в рассматриваемой задаче мы получили путем построения стохастического кода для совместного кодирования источника и канала. В отличие от случайных кодов, для которых требуется совместная случайность у кодера и декодера, для этого стохастического кода нужна лишь локальная случайность у кодера. Такой тип кодов допустим в нашей задаче, поскольку мы не предполагаем наличия никакой среды для передачи между передатчиком и приемником, кроме самого канала.

Получив границы на нижнюю и верхнюю цену игры, перейдем к оценке скорости их сходимости для рассматриваемой игры с нулевой суммой.

§ 6. Асимптотика и теоремы о минимаксе

Теперь применим выведенные в предыдущих параграфах границы для вычисления пределов верхней и нижней цены игры. На протяжении этого параграфа будем предполагать, что существует единственное распределение состояний $q^*_\Theta \in \Pi_\Theta$, на котором достигается пропускная способность, благодаря чему $V_{\mathrm{C}}^- = V_{\mathrm{C}}^+ =: V_{\mathrm{C}}$ и $V_{\mathrm{C}} > 0$.

Пусть $(\mathbb{X}, \mathbb{Y}) \sim P_{\mathbb{X}} \times \sum\limits_{\theta\in\mathcal{T}} q_\Theta(\theta) P_{\mathbb{Y}|\mathbb{X},\Theta=\theta}$, где $q_\Theta \in \mathcal{P}(\mathcal{T})$. Далее, пусть для всех таких распределений $P_{\mathbb{X}} \in \mathcal{P}(\mathcal{X})$ выполнено неравенство

$$i_{\mathbb{X};\mathbb{Y}_{q^*_\Theta}}(x;\mathbb{Y}) < \infty, \tag{22}$$

где

$$i_{\mathbb{X};\mathbb{Y}_{q^*_\Theta}}(x;y) = \log \frac{(q^*_\Theta P_{\mathbb{Y}|\mathbb{X},\Theta})(y\,|\,x)}{(P_{\mathbb{X}} q^*_\Theta P_{\mathbb{Y}|\mathbb{X},\Theta})(y)}, \quad x \in \mathcal{X}, \quad y \in \mathcal{Y},$$

для $q^*_\Theta \in \Pi_\Theta$. Кроме того, предположим также, что

$$j_{\mathrm{S}}(s, \boldsymbol{d}) < \infty, \quad \forall s \in \mathcal{S}, \tag{23}$$

где $j_{\mathrm{S}}(s, \boldsymbol{d})$ определено в п. 2.4.

6.1. Асимптотика второго порядка для верхней границы. Здесь мы вычислим предел нижней границы с помощью теоремы 8. Вначале оценим члены в (19), отвечающие за среднюю вероятность ошибки.

Средняя ошибка. Пусть $P^*_{\mathbb{X}} \in \Pi_{\mathbb{X}}$, и положим $P^*_X(x) := \prod\limits_{i=1}^{d_n} P^*_{\mathbb{X}}(x_i)$ для $x \in \mathcal{X}^{d_n}$. Чтобы применить теорему 8, определим множество $\mathcal{A} \subseteq \mathcal{X}^{d_n} \times \mathcal{Y}^{d_n}$ следующим образом. Пусть $T^n_\theta(\theta') := \prod\limits_{i=1}^{d_n} T_\theta(\theta'_i)$ для $T_\theta \in \mathcal{P}_n(\mathcal{T})$. Положим

$$i_{X^*;Y_{T^n_\theta}}(x;y) = \log \frac{(T^n_\theta P_{Y\,|\,X,\boldsymbol{\Theta}})(y\,|\,x)}{(P^*_X T^n_\theta P_{Y\,|\,X,\boldsymbol{\Theta}})(y)}, \quad x \in \mathcal{X}^n, \quad y \in \mathcal{Y}^n.$$

Теперь зададим множество $\mathcal{A}$ следующим образом:

$$\mathcal{A} = \Big\{(x,y) \in \mathcal{X}^{d_n} \times \mathcal{Y}^{d_n} : i_{X^*;Y_{T^n_\theta}}(x;y) > \gamma \text{ для некоторого } T_\theta \in \mathcal{P}_n(\mathcal{T})\Big\}. \tag{24}$$

Далее, пусть

$$\mathrm{V}_0 := \sup_{q_\Theta \in \mathcal{P}(\mathcal{T})} \mathrm{Var}\big(i_{\mathbb{X}^*;\mathbb{Y}_{q_\Theta}}(\mathbb{X};\mathbb{Y})\big), \tag{25}$$

где $(\mathbb{X}, \mathbb{Y}) \sim P^*_{\mathbb{X}} \times \sum\limits_{\theta\in\mathcal{T}} q_\Theta(\theta) P_{\mathbb{Y}|\mathbb{X},\Theta=\theta}$.

Следующая лемма, которая вытекает из [11, лемма 6], дает необходимое условие несимметризуемости ПМК.

Лемма 2. *Пусть $\mathbb{X}, \mathbb{X}' \sim P_{\mathbb{X}}$, и пусть $P_{\mathbb{X}}(x) > 0$ для всех $x \in \mathcal{X}$. Рассмотрим множество*

$$D_\eta = \big\{Q_{\mathbb{X}\mathbb{X}'\Theta\mathbb{Y}} \in \mathcal{P}(\mathcal{X}\times\mathcal{X}\times\mathcal{T}\times\mathcal{Y}) : D(Q_{\mathbb{X}\mathbb{X}'\Theta\mathbb{Y}} \,\|\, P_{\mathbb{X}} \times Q_{\mathbb{X}'\Theta} \times P_{\mathbb{Y}|\mathbb{X},\Theta}) \leqslant \eta\big\},$$

где $(P_{\mathbb{X}} \times Q_{\mathbb{X}'\Theta} \times P_{\mathbb{Y}|\mathbb{X},\Theta})(x,x',\theta,y) = P_{\mathbb{X}}(x) Q_{\mathbb{X}'\Theta}(x',\theta) P_{\mathbb{Y}|\mathbb{X},\Theta}(y\,|\,x,\theta)$, $Q_{\mathbb{X}'\Theta}$ – маргинальное распределение для $Q_{\mathbb{X}\mathbb{X}'\Theta\mathbb{Y}}$, а $D(Q_{\mathbb{X}\mathbb{X}'\Theta\mathbb{Y}} \,\|\, P_{\mathbb{X}} \times Q_{\mathbb{X}'\Theta} \times P_{\mathbb{Y}|\mathbb{X},\Theta})$ – относитель-

ная энтропия между $Q_{\mathbb{X}\mathbb{X}'\Theta\mathbb{Y}}$ *и* $P_{\mathbb{X}} \times Q_{\mathbb{X}'\Theta} \times P_{\mathbb{Y}|\mathbb{X},\Theta}$. *Положим*

$$\eta^* = \inf\bigl\{\eta:\ Q_{\mathbb{X}\mathbb{X}'\Theta\mathbb{Y}} \in D_\eta,\ Q_{\mathbb{X}'\mathbb{X}\Theta'\mathbb{Y}} \in D_\eta$$
$$\text{для некоторого } Q_{\mathbb{X}\mathbb{X}'\Theta\Theta'\mathbb{Y}} \in \mathcal{P}(\mathcal{X}\times\mathcal{X}\times\mathcal{T}\times\mathcal{T}\times\mathcal{Y})\bigr\}.$$

Если ПМК несимметризуем, то $\eta^* > 0$.

Теперь с помощью этой леммы построим функцию $Z\colon \mathcal{X}^{d_n}\times\mathcal{X}^{d_n}\times\mathcal{Y}^{d_n}\to\{0,1\}$ следующим образом. Так как ПМК несимметризуем, то по лемме 2 имеем $\eta^* > 0$. Выберем η таким, что $0 < \eta < \eta^*$. Положим

$$Z(x_a,\bar{x}_a,y_a) = \begin{cases} 1, & \text{если } (x_a,y_a)\in\mathcal{A} \text{ и либо } (\bar{x}_a,y_a)\notin\mathcal{A},\\ & \text{либо } \exists\,\theta_a\in\mathcal{T}^{d_n},\ \text{такое что } T_{x_a,\bar{x}_a,\theta_a,y_a}\in D_\eta,\\ 0 & \text{в противном случае,}\end{cases} \tag{26}$$

где, напомним, $T_{x_a,\bar{x}_a,\theta_a,y_a}$ – совместный тип для $x_a,\bar{x}_a,\theta_a,y_a$. Таким образом, функция Z удовлетворяет условию (12) и при этом $Z(x_a,\bar{x}_a,y_a)Z(\bar{x}_a,x_a,y_a) = 0\ \forall x_a,\ \bar{x}_a\in\mathcal{X}^{d_n},\ y_a\in\mathcal{Y}^{d_n}$, поскольку в противном случае найдутся $(x_a,\bar{x}_a,y_a)\in\mathcal{X}^{d_n}\times$ $\times\,\mathcal{X}^{d_n}\times\mathcal{Y}^{d_n}$, такие что $Z(x_a,\bar{x}_a,y_a)Z(\bar{x}_a,x_a,y_a)=1$. Отсюда $(x_a,y_a)\in\mathcal{A}$ и $(\bar{x}_a,y_a)\in$ $\in\mathcal{A}$, и значит, существуют совместные типы $T_{x_a,\bar{x}_a,\theta_a,y_a}\in D_\eta$ и $T_{\bar{x}_a,x_a,\theta'_a,y_a}\in D_\eta$ для некоторых $\theta_a,\theta'_a\in\mathcal{T}^{d_n}$. Таким образом, по определению η^* получаем $\eta^*\leqslant\eta$. Но это дает противоречие, поскольку η выбрано строго меньшим η^*. С помощью этой функции Z получаем следующую оценку сверху (доказательство приведено в Приложении).

Теорема 9. *При вышеуказанном выборе* $\mathcal{A}$, Z, K *и* d_n *получаем*

$$\begin{aligned}
&\sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}} + \min_{P_{X_a}}\max_{\theta_a\in\mathcal{T}^{d_n}}\Bigl[\mathbf{P}\bigl((X_a,Y_a)\notin\mathcal{A}\,|\,\theta_a\bigr) +\\
&+ 2K\log e\,\mathbf{P}\bigl(Z(X_a,\bar{X}_a,Y_a)=0,(X_a,Y_a)\in\mathcal{A}\,|\,\theta_a\bigr) +\\
&+ \max_{\bar{x}_a\in\mathcal{X}^{d_n}} 2\log 3|\mathcal{T}|^{d_n}\,\mathbf{P}\bigl(Z(X_a,\bar{x}_a,Y_a)=0,(X_a,Y_a)\in\mathcal{A}\,|\,\theta_a\bigr)\Bigr]\leqslant\\
&\leqslant\sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}} + \frac{\mathrm{V}_0}{d_n\Bigl(\delta-\dfrac{\log\sqrt{d_n}}{d_n}\Bigr)^2} + \frac{2\log e}{\sqrt{d_n}} +\\
&+ \frac{2\log 3|\mathcal{T}|^{d_n}(d_n+1)^{|\mathcal{X}|^2|\Theta||\mathcal{Y}|}}{\exp(d_n(\eta))}.
\end{aligned} \tag{27}$$

Ошибка для случайного кода. Оценим отвечающие за вероятность ошибки члены в (19), соответствующие случайному коду для совместного кодирования источника и канала (доказательство дано в Приложении).

Теорема 10. *Вероятность ошибки для случайного кода в* (19) *оценивается как*

$$\begin{aligned}
&\inf_{\gamma>0}\max_{\theta_b\in\mathcal{T}^n}\left[\mathbf{E}\left[\exp\left(-\left|i_{X;Y_{q^*}}(X_b;Y_b)-\log\frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))}\right|^+\right)|\,\theta_b\right]+e^{1-\gamma}\right]\ \leqslant\\
&\leqslant \mathrm{Q}\left(\frac{nC-kR(\boldsymbol{d})-\Gamma(k)}{\sqrt{nV_{\mathrm{C}}+kV_{\mathrm{S}}(\boldsymbol{d})}}\right)+\frac{B}{n+k}+\frac{K_0+2}{\sqrt{k}},
\end{aligned} \tag{28}$$

где $B,K_0,\varepsilon_0>0$ – *константы, а* $\Gamma(k)=\bar{c}\log k+c+\log\Bigl(\dfrac{1}{2}\log k+1\Bigr)$, $\bar{c},c>0$.

Объединяя результаты двух последних теорем, получаем следующий результат.

Теорема 11. *Для верхней цены игры справедлива оценка*

$$\overline{\nu}(k,n) \leqslant \mathrm{Q}\biggl(\frac{nC - kR(\boldsymbol{d}) - \Gamma(k)}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}}\biggr) + \frac{B}{\sqrt{n+k}} + \frac{K_0+2}{\sqrt{k}} + \sqrt{\frac{\log|\mathcal{T}^n| + \varepsilon_0}{2K}} +$$
$$+ \sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}} + \frac{2\log e}{\sqrt{d_n}} + \frac{\mathrm{V}_0}{d_n\Bigl(\delta - \dfrac{\log\sqrt{d_n}}{d_n}\Bigr)^2} +$$
$$+ \frac{2\log 3|\mathcal{T}|^{d_n}(d_n+1)^{|\mathcal{X}|^2|\Theta||\mathcal{Y}|}}{\exp(d_n(\eta))}, \tag{29}$$

где $\Gamma(k)$, B, K_0 *и* ε_0 *описаны в теореме* 10.

Доказательство. Этот результат получается подстановкой в (19) оценки (27) из теоремы 9 и оценки (28) из теоремы 10. ▲

Теперь рассмотрим последовательность пар (k,n), для которой верхняя и нижняя цена игры стремятся к нулю. Возьмем

$$K = c_0 n^2, \quad d_n = \left\lceil \frac{\log K}{C - \delta} \right\rceil, \tag{30}$$

где $c_0 \in \mathbb{N}$, а $\lceil\cdot\rceil$ – функция округления до ближайшего целого в большую сторону.

Границу второго порядка на скорость передачи описывает

Следствие 1 (граница достижимости второго порядка). *Пусть* $\varepsilon > 0$. *Рассмотрим последовательность пар* (k,n), *для которой*

$$nC - kR(\boldsymbol{d}) \geqslant \sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}\,\mathrm{Q}^{-1}(\varepsilon) + O\biggl(\sqrt{\frac{n}{\log n}}\biggr).$$

Тогда $\underline{\nu}(k,n) \leqslant \overline{\nu}(k,n) \leqslant \varepsilon$.

Доказательство. Возьмем последовательность пар (k,n), для которой выполнено $nC - kR(\boldsymbol{d}) \geqslant \sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}\mathrm{Q}^{-1}(\varepsilon - \Delta(k,n)) + \Gamma(k)$, где

$$\Delta(k,n) = \frac{B}{\sqrt{n+k}} + \sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}} + \frac{2\log e}{\sqrt{d_n}} + \frac{\mathrm{V}_0}{d_n\Bigl(\delta - \dfrac{\log\sqrt{d_n}}{d_n}\Bigr)^2} +$$
$$+ \frac{2\log 3|\mathcal{T}|^{d_n}(d_n+1)^{|\mathcal{X}|^2|\Theta||\mathcal{Y}|}}{\exp(d_n(\eta))} + \sqrt{\frac{\log|\mathcal{T}^n| + \varepsilon_0}{2K}},$$

а K, d_n удовлетворяют (30). Подставляя это в (29), получаем

$$\mathrm{Q}\biggl(\frac{nC - kR(\boldsymbol{d}) - \Gamma(k)}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}}\biggr) + \frac{B}{\sqrt{n+k}} + \sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}} + \frac{2\log e}{\sqrt{d_n}} +$$
$$+ \frac{\mathrm{V}_0}{d_n\Bigl(\delta - \dfrac{\log\sqrt{d_n}}{d_n}\Bigr)^2} + \frac{2\log 3|\mathcal{T}|^{d_n}(d_n+1)^{|\mathcal{X}|^2|\Theta||\mathcal{Y}|}}{\exp(d_n(\eta))} + \sqrt{\frac{\log|\mathcal{T}^n| + \varepsilon_0}{2K}} \leqslant \varepsilon.$$

Требуемый результат получается рассмотрением ряда Тейлора для $\mathrm{Q}^{-1}(\varepsilon - \Delta(k,n))$. Остаточный член $O(\sqrt{n/\log n})$ возникает как произведение члена $O(1/\sqrt{\log n})$ из ряда Тейлора для $\mathrm{Q}^{-1}(\varepsilon - \Delta(k,n))$ и члена $O(\sqrt{n})$. ▲

6.2. Асимптотика второго порядка для нижней границы. В этом пункте вычислим предел нижней границы на вероятность ошибки (доказательство приведено в Приложении).

Теорема 12. *Для нижней цены игры* $\underline{\nu}(k,n)$ *справедлива оценка*

$$\begin{aligned}\underline{\nu}(k,n) \geqslant \max_{q,P_{\overline{Y}_q},\mathrm{U}} \sup_{\gamma>0}\Bigg[\sum_s P_S(s)\min_x\Bigg[\mathbf{P}\big(j_S(s,\boldsymbol{d}) - i_{X;\overline{Y}_q|U}(x;Y\,|\,U)\leqslant\gamma\big) + \\ + \exp(j_S(s,\boldsymbol{d})-\gamma)\sum_{u=1}^{\mathrm{U}}\sum_y P_{U|X}(u\,|\,x)P_{\overline{Y}_q|U}(y\,|\,u)\times \\ \times\,\mathbb{I}\big\{j_S(s,\boldsymbol{d}) - i_{X;\overline{Y}_q|U}(x;y\,|\,u)>\gamma\big\}\Bigg] - \frac{\mathrm{U}}{\exp(\gamma)}\Bigg] \geqslant \\ \geqslant \mathrm{Q}\Bigg(\frac{nC - kR(\boldsymbol{d}) + \gamma(n)}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d}) - K_3}}\Bigg) - \frac{K_1}{k} - \frac{K_2}{\sqrt{n}} - \frac{B'}{\sqrt{n+k}} - \frac{1}{\sqrt{n+1}},\end{aligned} \tag{31}$$

где $K_1, K_2, K_3, B' > 0$ *– константы, а* $\gamma(n) = K_4\log(n+1)$, $K_4 > 0$.

Справедливо также следующее утверждение, дающее границу второго порядка на скорость передачи.

Следствие 2 (обращение теоремы кодирования второго порядка). *Пусть* $\varepsilon > 0$. *Рассмотрим последовательность пар* (k,n), *такую что*

$$nC - kR(\boldsymbol{d}) \leqslant \sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}\,\mathrm{Q}^{-1}(\varepsilon) - O(\log n).$$

Тогда $\overline{\nu}(k,n) \geqslant \underline{\nu}(k,n) \geqslant \varepsilon$.

Доказательство. Возьмем последовательность пар (k,n), для которой выполнено $nC - kR(\boldsymbol{d}) + \gamma(n) \leqslant \sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}\mathrm{Q}^{-1}(\varepsilon + \Delta(k,n))$, где

$$\Delta(k,n) = \frac{K_1}{k} + \frac{K_2}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} + \frac{B'}{\sqrt{n+k}}.$$

Подставляя это в (31), получаем

$$\mathrm{Q}\Bigg(\frac{nC - kR(\boldsymbol{d}) + \gamma(n)}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d}) - K_3}}\Bigg) - \frac{K_1}{k} - \frac{K_2}{\sqrt{n}} - \frac{1}{\sqrt{n+1}} - \frac{B'}{\sqrt{n+k}} \geqslant \varepsilon.$$

Требуемый результат получается рассмотрением ряда Тейлора для $\mathrm{Q}^{-1}(\varepsilon+\Delta(k,n))$. Остаточный член $O(\log n)$ возникает за счет члена $\gamma(n)$. ▲

С использованием полученных границ опишем теперь дисперсию для заданных ε и $k,n\in\mathbb{N}$.

Теорема 13. *Для* $\varepsilon > 0$ *и* $k,n\in\mathbb{N}$ *дисперсия для стохастического совместного кодирования источника и канала при передаче по ПМК имеет вид*

$$\sqrt{V_{\mathrm{C}} + \frac{k}{n}V_{\mathrm{S}}}\,\mathrm{Q}^{-1}(\varepsilon),$$

где V_{C} *и* V_{S} *– соответствующие дисперсии канала и источника.*

6.3. Доказательство минимаксных теорем. Теперь мы готовы к выводу асимптотических результатов, приведенных в § 3. Мы рассматриваем последовательности пар (k,n) и изучаем предельное поведение границ при конечной длине блока для таких последовательностей. Вначале докажем теорему 1.

Доказательство теоремы 1. Рассмотрим границу из теоремы 10. Выберем последовательность $(k,n)\uparrow\infty$, такую что $\lim k/n < C/R(\boldsymbol{d})$. Тогда

$$\lim_{k,n\to\infty} \mathrm{Q}\left(\sqrt{n}\left(\frac{C-\frac{k}{n}R(\boldsymbol{d})+\frac{\Gamma(k)}{n}}{\sqrt{V_{\mathrm{C}}+\frac{k}{n}V_{\mathrm{S}}(\boldsymbol{d})}}\right)\right)=0.$$

Далее, при $k,n\to\infty$ и для K и d_n, выбранных согласно (30), имеем

$$\frac{B}{n+k}+\frac{K_0+2}{\sqrt{k}}+\sqrt{\frac{2\ln(3|\mathcal{T}|^{d_n})}{K}}+\frac{2\log e}{\sqrt{d_n}}+\frac{\mathrm{V}_0}{d_n\Big(\delta-\frac{\log\sqrt{d_n}}{d_n}\Big)^2}+$$
$$+\frac{2\log 3|\mathcal{T}|^{d_n}(d_n+1)^{|\mathcal{X}|^2|\Theta||\mathcal{Y}|}}{\exp(d_n(\eta))}+\sqrt{\frac{\log|\mathcal{T}^n|+\varepsilon_0}{2K}}\to 0.$$

Таким образом, $\overline{\nu}(k,n)\to 0$, и следовательно, $\underline{\nu}(k,n)\to 0$. ▲

Теперь перейдем к доказательству теоремы 2.

Доказательство теоремы 2. Рассмотрим границу из теоремы 12. Выберем последовательность $(k,n)\uparrow\infty$, такую что $\lim k/n > C/R(\boldsymbol{d})$. Тогда

$$\lim_{k,n\to\infty} \mathrm{Q}\left(\sqrt{n}\left(\frac{C-\frac{k}{n}R(\boldsymbol{d})+\frac{\gamma(n)}{n}}{\sqrt{V_{\mathrm{C}}+\frac{k}{n}V_{\mathrm{S}}(\boldsymbol{d})-\frac{K_3}{n}}}\right)\right)=1.$$

Далее, при $k,n\to\infty$

$$-\frac{K_1}{k}-\frac{K_2}{\sqrt{n}}-\frac{1}{\sqrt{n+1}}-\frac{B'}{\sqrt{n+k}}\to 0.$$

Таким образом, $\underline{\nu}(k,n)\to 1$, и следовательно, $\overline{\nu}(k,n)\to 1$. ▲

Заметим, что совпадение верхней и нижней цены, указанных в теоремах 1 и 2, можно показать и без границ второго порядка (см., например, рассуждения в [1]). Следовательно, эти утверждения справедливы, даже когда распределение состояний, на котором достигается пропускная способность, не единственно.

Для доказательства теоремы 3 рассмотрим уточненное определение скорости передачи, отличающееся на $O(1/\sqrt{n})$ от $C/R(\boldsymbol{d})$. Напомним, что в (9) последовательность дана в виде

$$\frac{k}{n}=\frac{C}{R(\boldsymbol{d})}+\frac{\rho}{\sqrt{n}}, \tag{32}$$

где $\rho\in\mathbb{R}$ фиксировано. Выведенные нами неасимптотические формулы позволяют оценивать верхнюю и нижнюю цену игры при таком уточненном определении скорости. Для такой последовательности и верхняя, и нижняя цена теперь стремятся к одному и тому же значению, зависящему от ρ. В общем случае это значение не равно ни 0, ни 1. Такое совпадение в более тонкой асимптотике зависит от существования единственного распределения, на котором достигается пропускная способность, для источника помех. Мы обсудим это в следующем пункте.

Доказательство теоремы 3. Подставляя (32) в нижнюю оценку (31), получаем следующий гауссовский член в неравенстве:

$$\mathrm{Q}\biggl(\frac{nC - kR(\boldsymbol{d}) + \gamma(n)}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d}) - K_3}}\biggr) = \mathrm{Q}\left(\frac{-\rho R(\boldsymbol{d}) + \dfrac{\gamma(n)}{\sqrt{n}}}{\sqrt{V_{\mathrm{C}} + \Bigl(\dfrac{C}{R(\boldsymbol{d})} + \dfrac{\gamma(n)}{\sqrt{n}}\Bigr)V_{\mathrm{S}}(\boldsymbol{d}) - \dfrac{K_3}{n}}}\right).$$

Переходя к пределу при $k, n \to \infty$, получаем

$$\lim_{k,n\to\infty} \underline{\nu}(k,n) \geqslant \mathrm{Q}\left(\frac{-\rho R(\boldsymbol{d})}{\sqrt{V_{\mathrm{C}} + \dfrac{C}{R(\boldsymbol{d})}V_{\mathrm{S}}(\boldsymbol{d})}}\right),$$

так как остальные члены в (31) асимптотически стремятся к нулю.

Аналогично, подставляя (32) в (29), получаем следующий гауссовский член в неравенстве:

$$\mathrm{Q}\biggl(\frac{nC - kR(\boldsymbol{d}) - \Gamma(k)}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}}\biggr) = \mathrm{Q}\left(\frac{-\rho R(\boldsymbol{d}) - \dfrac{\Gamma(k)}{\sqrt{n}}}{\sqrt{V_{\mathrm{C}} + \Bigl(\dfrac{C}{R(\boldsymbol{d})} + \dfrac{\rho}{\sqrt{n}}\Bigr)V_{\mathrm{S}}(\boldsymbol{d})}}\right).$$

Переходя к пределу при $k, n \to \infty$, получаем

$$\lim_{k,n\to\infty} \underline{\nu}(k,n) \geqslant \mathrm{Q}\left(\frac{-\rho R(\boldsymbol{d})}{\sqrt{V_{\mathrm{C}} + \dfrac{C}{R(\boldsymbol{d})}V_{\mathrm{S}}(\boldsymbol{d})}}\right),$$

так как остальные члены в (29) асимптотически стремятся к нулю, что и завершает доказательство. ▲

6.4. Неединственность дисперсии канала. В общей постановке задачи передачи по ПМК может существовать несколько пар распределений $(P_{\mathbb{X}}, q_\Theta)$, на которых достигается пропускная способность в (1), и поэтому множества $\Pi_{\mathbb{X}}$ и Π_Θ могут не состоять из одного элемента. Когда распределение на входе и распределение состояний, на которых достигается пропускная способность, не единственны, дисперсии канала V_{C}^+ и V_{C}^-, определенные в п. 2.4, могут быть не равны между собой. Они равны, когда любое одно из этих распределений (на входе или распределение состояний), на которых достигается пропускная способность, единственно.

В настоящей статье вычислены основанные на дисперсии границы для стохастического совместного кодирования источника и канала при передаче по ПМК в предположении, что распределение состояний, на котором достигается пропускная способность, единственно. Недавно в [11, 27] были получены границы второго порядка на скорость передачи по ПМК для детерминированных и случайных кодов соответственно. Было показано, что в случае неединственного распределения, на котором достигается пропускная способность, скорость достижимости и скорость в обращении теоремы кодирования не равны между собой. Таким образом, естественно предположить, что в случае неединственных распределений, на которых достигается пропускная способность, "более тонкая" теорема о минимаксе может не выполняться, и тем самым граница достижимости и обратная граница на скорость в задаче совместного кодирования источника и канала могут не совпадать. Подтверждение этого факта потребует улучшения стратегий для совместного кодирования источника и канала, что является предметом будущей работы.

§ 7. Заключение

Задача передачи информации при наличии целенаправленных помех рассмотрена в статье как игра с нулевой суммой между командой, состоящей из кодера и декодера, и источником помех, в которой эта команда старается минимизировать вероятность ошибки, а источник помех – максимизировать ее. Эта задача невыпукла в пространстве стратегий команды кодера–декодера, и поэтому теорема о минимаксе может не выполняться. Однако мы показали, что для этой игры справедлива приближенная теорема о минимаксе. Мы вывели верхнюю и нижнюю границы на значения минимакса и максимина игры при конечной длине блока и показали, что асимптотическая теорема о минимаксе имеет место, когда длина блока стремится к бесконечности. В частности, для скоростей выше порогового значения $C/R(\boldsymbol{d})$ верхняя и нижняя цена игры стремится к нулю, а для скоростей выше $C/R(\boldsymbol{d})$ эти величины стремятся к единице. Для скоростей, стремящихся в точности к $C/R(\boldsymbol{d})$ с отклонением не более $O(1/n^{\delta})$, где $0 < \delta < 1$, эти величины стремятся к одной и той же константе при предположении технического характера о единственности распределений, на которых достигается пропускная способность.

Авторы благодарны рецензенту за внимательное прочтение первоначального варианта статьи и конструктивные замечания.

ПРИЛОЖЕНИЕ

Начнем со следующей центральной предельной теоремы, принадлежащей Берри и Эссеену (см. [8]).

Теорема 14 (ЦПТ Берри–Ессеена). *Зафиксируем $n \in \mathbb{N}$. Пусть W_i – независимые случайные величины. Тогда для $t \in \mathbb{R}$ справедливо неравенство*

$$\left|\mathbf{P}\left(\frac{1}{n}\sum_{i=1}^{n} W_i > D_n + t\sqrt{\frac{V_n}{n}}\right) - \mathrm{Q}(t)\right| \leqslant \frac{B_n}{\sqrt{n}},$$

где Q *– функция, дополнительная к гауссовской функции распределения,*

$$D_n = \frac{1}{n}\sum_{i=1}^{n}\mathbf{E}[W_i], \qquad V_n = \frac{1}{n}\sum_{i=1}^{n}\mathrm{Var}[W_i],$$

$$A_n = \frac{1}{n}\sum_{i=1}^{n}\mathbf{E}\big[|W_i - \mathbf{E}[W_i]|^3\big], \qquad B_n = \frac{c_0 A_n}{V_n^{3/2}}, \quad c_0 > 0.$$

Доказательство леммы 1. Зафиксируем $\theta \in \mathcal{T}^n$ и рассмотрим K независимых копий случайного кода $\{F_i, \Phi_i\}_{i=1}^{K}$. Применяя неравенство Хёффдинга, получаем

$$\mathbf{P}\left(\frac{1}{K}\sum_i e_{\boldsymbol{d},\theta}(F_i,\Phi_i) \geqslant \varepsilon'\right) \leqslant \exp\Big(-2K\big(\varepsilon' - \mathbf{E}[e_{\boldsymbol{d},\theta}(F,\Phi)]^2\big)\Big).$$

Так как $e_{\boldsymbol{d}}(\psi) = \max\limits_{\theta\in\mathcal{T}^n}\mathbf{E}[e_{\boldsymbol{d},\theta}(F,\Phi)] < \varepsilon$, то $e_{\boldsymbol{d},\theta}(F,\Phi) < \varepsilon\ \forall\theta \in \mathcal{T}^n$. Используя это неравенство и ε' из (18), получаем, что для всех $\theta \in \mathcal{T}^n$

$$\varepsilon' - \mathbf{E}[e_{\boldsymbol{d},\theta}(F,\Phi)] > \varepsilon' - \varepsilon > \sqrt{\log|\mathcal{T}^n|/2K},$$

откуда

$$\mathbf{P}\left(\frac{1}{K}\sum_i e_{\boldsymbol{d},\theta}(F_i,\Phi_i) \geqslant \varepsilon'\right) \leqslant \exp\Big(-2K^2\big(\varepsilon' - \mathbf{E}[e_{\boldsymbol{d},\theta}(F,\Phi)]^2\big)\Big) <$$

$$< \exp\left(-2K\frac{\log|\mathcal{T}^n|}{2K}\right) = \frac{1}{|\mathcal{T}^n|}.$$

Таким образом,

$$\mathbf{P}\left(\frac{1}{K}\sum_i e_{\boldsymbol{d},\theta}(F_i,\Phi_i) < \varepsilon' \ \forall\theta\in\mathcal{T}^n\right) =$$

$$= 1 - \mathbf{P}\left(\frac{1}{K}\sum_i e_{\boldsymbol{d},\theta}(F_i,\Phi_i) \geqslant \varepsilon' \text{ для некоторого } \theta\in\mathcal{T}^n\right) \geqslant$$

$$\geqslant 1 - \sum_{\theta\in\mathcal{T}^n}\mathbf{P}\left(\frac{1}{K}\sum_i e_{\boldsymbol{d},\theta}(F_i,\Phi_i) \geqslant \varepsilon'\right) > 1 - \frac{|\mathcal{T}^n|}{|\mathcal{T}^n|} > 0.$$

Следовательно, событие $\left\{\sum\limits_i e_{\boldsymbol{d},\theta}(F_i,\Phi_i)/K < \varepsilon' \ \forall\theta\in\mathcal{T}^n\right\}$ имеет ненулевую вероятность, и поэтому существует K детерминированных кодов $\{f_i,\varphi_i\}_{i=1}^K$, таких что для всех $\theta\in\mathcal{T}^n$ справедливо

$$\frac{1}{K}\sum_i e_{\boldsymbol{d},\theta}(f_i,\varphi_i) < \varepsilon',$$

где $\varepsilon' > \varepsilon + \sqrt{\log|\mathcal{T}^n|/2K}$. ▲

Доказательство теоремы 9. Ослабим оценку в (19), выбирая $P_{X_a}(x_a) = \prod\limits_{i=1}^{d_n} P^*_{\mathbb{X}}(x_i)$, $P^*_{\mathbb{X}}\in\Pi_{\mathbb{X}}$. Пусть $\mathcal{A}$, Z, K и d_n определены в (24), (26) и (30) соответственно. Положим $U_i := i_{\mathbb{X}^*;\mathbb{Y}_{T_\theta}}(X_{ai};Y_{ai})$, где $(X_{ai},Y_{ai})\sim P^*_{\mathbb{X}}\times\sum\limits_{\theta\in\mathcal{T}} T_\theta(\theta)P_{\mathbb{Y}|\mathbb{X},\Theta=\theta}$ $\forall i$. Так как память в канале отсутствует, то $i_{X^*;Y_{q^*}}(X_a;Y_a) = \sum\limits_{i=1}^{d_n} U_i$. Таким образом, выбирая $\gamma = \log(\sqrt{d_n}K)$, получаем $\mathbf{P}\big(i_{X^*;Y_{q^*}}(X_a;Y_a)\leqslant\gamma\big) = \mathbf{P}\left(\sum\limits_{i=1}^{d_n} U_i \leqslant \log(\sqrt{d_n}K)\right)$. Согласно [10, лемма 12.10] имеем $C\leqslant\mathbf{E}\big[i_{\mathbb{X};\mathbb{Y}_{T^n_\theta}}(X_{ai};Y_{ai})\big] = E[U_i]$ для всех $T_\theta\in\mathcal{P}_n(\mathcal{T})$, и поэтому $d_nC\leqslant\sum\limits_{i=1}^{d_n}\mathbf{E}[U_i]$. Кроме того, подставляя $\log K$ из условия (30), получаем

$$\mathbf{P}\left(\sum_{i=1}^{d_n}U_i\leqslant\log\sqrt{d_n}+\log K\right)\leqslant\mathbf{P}\left(\sum_{i=1}^{d_n}U_i\leqslant\log\frac{\sqrt{d_n}}{\exp d_n\delta}+\sum_{i=1}^{d_n}\mathbf{E}[U_i]\right)\leqslant$$

$$\leqslant\mathbf{P}\left(\left|\sum_{i=1}^{d_n}(U_i-\mathbf{E}[U_i])\right|\geqslant\log\frac{\exp d_n\delta}{\sqrt{d_n}}\right),$$

где последнее неравенство вытекает из неравенства треугольника. Применяя неравенство Чебышева и переходя к супремуму по θ_a, получаем

$$\sup_{\theta_a\in\mathcal{T}^{d_n}}\mathbf{P}\left(\left|\sum_{i=1}^{d_n}(U_i-\mathbf{E}[U_i])\right|\geqslant d_n\delta-\log\sqrt{d_n}\right)\leqslant$$

$$\leqslant\sup_{\theta_a\in\mathcal{T}^{d_n}}\frac{d_n}{(d_n\delta-\log\sqrt{d_n})^2}\operatorname{Var}\big(i_{\mathbb{X}^*;\mathbb{Y}_{T_{\theta_a}}}(\mathbb{X}_a;\mathbb{Y}_a)\big)\leqslant$$

$$\leqslant\frac{V_0}{d_n\Big(\delta-\dfrac{\log\sqrt{d_n}}{d_n}\Big)^2}, \tag{33}$$

где неравенство (33) следует из соотношения (25).

Оценки для остальных двух слагаемых $\mathbf{P}(Z(X_a, \bar{X}_a, Y_a) = 0, (X_a, Y_a) \in \mathcal{A} \,|\, \theta_a) \leqslant$ $\leqslant 1/\sqrt{d_n}K$ и $\mathbf{P}(Z(X_a, \bar{x}_a, Y_a) = 0, (X_a, Y_a) \in \mathcal{A} \,|\, \bar{X}_a = \bar{x}_a, \theta_a) \leqslant (d_n+1)^{|\mathcal{X}|^2|\Theta||\mathcal{Y}|} \times$ $\times \exp(-d_n\eta)$ следуют из доказательства теоремы 4 работы [11]. Из (33) и этих оценок вытекает требуемая граница. ▲

Доказательство теоремы 10. Для вывода этой границы построим случайный код (F, Φ) для совместного кодирования источника и канала, т.е. распределение ψ на множестве кодов $\{(f, \varphi) \mid f\colon \mathcal{S}^k \to \mathcal{X}^n,\ \varphi\colon \mathcal{Y}^n \to \mathcal{S}^k\}$. По теореме 6 достаточно выбрать распределения P_X и $P_{\widehat{S}}$. Пусть $P^*_{\mathbb{X}}$ – распределение из множества $\Pi_{\mathbb{X}}$. Положим $P_X(x) := \prod\limits_{i=1}^{n} P^*_{\mathbb{X}}(x_i)$ для $x \in \mathcal{X}^n$. Далее, возьмем $P_{\widehat{S}}(\widehat{s}) = \prod\limits_{i=1}^{k} P^*_{\widehat{\mathbb{S}}}(\widehat{s}_i)$, $\widehat{s} \in \mathcal{S}^k$, где $P^*_{\widehat{\mathbb{S}}}$ достигает оптимума в (2). Очевидно, что при таком выборе распределений

$$i_{X^*;Y_{q^*}}(X;Y) = \sum_{i=1}^{n} i_{\mathbb{X}^*;\mathbb{Y}_{q^*_\Theta}}(X_i;Y_i), \quad j_S(S, \boldsymbol{d}) = \sum_{j=1}^{k} j_{\mathrm{S}}(S_j, \boldsymbol{d}).$$

Рассмотрим слагаемые, составляющие вероятность ошибки случайного кода в теореме 8. Записывая максимизацию по $\theta_b \in \mathcal{T}^n$ как максимизацию по $q \in \mathcal{P}(\mathcal{T}^n)$, можно представить границу в виде

$$\max_{q \in \mathcal{P}(\mathcal{T}^n)} \left[\mathbf{E}\left[\exp\left(-\left| i_{X^*;Y_{q^*}}(X_b;Y_b) - \log \frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))} \right|^+ \right) \right] + e^{1-\gamma} \right],$$

где $q(\theta) = \prod\limits_{i=1}^{n} q_i(\theta_i)$ для $q_i \in \mathcal{P}(\mathcal{T})$, $\theta \in \mathcal{T}^n$. Пусть $h(X_b, Y_b, S) := \sum\limits_{j=1}^{n} i_{\mathbb{X}^*;\mathbb{Y}_{q^*_\Theta}}(X_{bj};Y_{bj}) -$ $- \log(\gamma / P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S)))$. Далее, зададим множество

$$\mathcal{D} := \left\{ s \in \mathcal{S}^k :\ \log \frac{1}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(s))} \leqslant \sum_{i=1}^{k} j_{\mathrm{S}}(s_i, \boldsymbol{d}) + \left(\bar{c} - \frac{1}{2}\right) \log k + c \right\},$$

где $\bar{c}, c$ – константы, определенные в [9, лемма 5]. Определим случайную величину

$$W_\ell = W_\ell(n,k) := \begin{cases} i_{\mathbb{X}^*;\mathbb{Y}_{q^*_\Theta}}(X_{b\ell};Y_{b\ell}), & \text{если } \ell \leqslant n, \\ -j_{\mathrm{S}}(S_{\ell-n}, \boldsymbol{d}), & \text{если } n < \ell \leqslant n+k. \end{cases} \tag{34}$$

Математическое ожидание $\mathbf{E}[\exp(-|h(X_b, Y_b, S)|^+)]$ можно представить в виде

$$\begin{aligned} &\mathbf{E}\big[\exp(-|h(X_b, Y_b, S)|^+)\mathbb{I}\{S \in \mathcal{D}\}\big] + \mathbf{E}\big[\exp(-|h(X_b, Y_b, S)|^+)\mathbb{I}\{S \notin \mathcal{D}\}\big] \ \leqslant \\ &\leqslant \mathbf{E}\left[\exp\left(-\left| \sum_{\ell=1}^{n+k} W_\ell - \log\big(k^{(\bar{c}-\frac{1}{2})} \exp(c)\gamma\big) \right|^+ \right) \right] + \frac{K_0}{\sqrt{k}}, \end{aligned} \tag{35}$$

где первое слагаемое в (35) вытекает из определения множества $\mathcal{D}$, а второе получается из неравенства $\mathbf{E}\big[\exp(-|h(X_b, Y_b, S)|^+)\mathbb{I}\{S \notin \mathcal{D}\}\big] \leqslant \mathbf{P}(S \notin \mathcal{D})$ и леммы 5 работы [9].

Введем следующие моменты, которые будут использоваться для оценки первого слагаемого в (35) с помощью ЦПТ Берри – Эссеена:

$$
\begin{aligned}
&D_{n+k}(q) = \frac{1}{n+k}\sum_{\ell=1}^{n+k}\mathbf{E}[W_\ell], && V_{n+k}(q) = \frac{1}{n+k}\sum_{\ell=1}^{n+k}\operatorname{Var}[W_\ell],\\
&A_{n+k}(q) = \frac{1}{n+k}\sum_{\ell=1}^{n+k}\mathbf{E}\big[|W_\ell - \mathbf{E}[W_\ell]|^3\big], && B_{n+k}(q) = \frac{c_0 A_{n+k}(q)}{V_{n+k}^{3/2}(q)}, \quad c_0 > 0.
\end{aligned}
\tag{36}
$$

Отметим, что эти моменты вычисляются относительно распределения $P_X \times \times \sum\limits_\theta q(\theta) P_{Y\,|\,X,\mathbf{\Theta}=\theta} \times P_S$. Далее, определим следующее множество:

$$
\mathcal{H} = \left\{(x,y,s) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{S}^k : \frac{1}{n+k}\sum_{\ell=1}^{n+k} W_\ell > D_{n+k}(q) - t_{k,n}\sqrt{\frac{V_{n+k}(q)}{n+k}}\right\},
$$

где $t_{k,n} > 0$ будет выбрано позже. Для краткости введем следующие обозначения:

$$
g(X_b, Y_b, S) = \sum_{\ell=1}^{n+k} W_\ell - \log\big(k^{(\bar{c}-\frac{1}{2})}\exp(c)\gamma\big), \tag{37}
$$

$$
\Gamma_{n+k}(q) = (n+k)\left(D_{n+k}(q) - t_{k,n}\sqrt{\frac{V_{n+k}(q)}{n+k}}\right) - \log\big(k^{(\bar{c}-\frac{1}{2})}\exp(c)\log\gamma\big). \tag{38}
$$

Тогда член с экспонентой в (35) можно записать в виде $\mathbf{E}[\exp(-|g(X_b,Y_b,S)|^+)]$, что можно представить как

$$
\begin{aligned}
&\mathbf{E}\big[\exp(-|g(X_b,Y_b,S)|^+)\mathbb{I}\{(X_b,Y_b,S)\in\mathcal{H}\}\big] +\\
&+\mathbf{E}\big[\exp(-|g(X_b,Y_b,S)|^+)\mathbb{I}\{(X_b,Y_b,S)\notin\mathcal{H}\}\big] \leqslant\\
&\leqslant \mathbf{E}\big[\exp(-|\Gamma_{n+k}(q)|^+)\mathbb{I}\{(X_b,Y_b,S)\in\mathcal{H}\}\big] + \mathbf{E}\big[\mathbb{I}\{(X_b,Y_b,S)\notin\mathcal{H}\}\big],
\end{aligned}
\tag{39}
$$

где первое слагаемое в (39) вытекает из определения множества $\mathcal{H}$, а второе получается с помощью неравенства $\exp(-|\cdot|^+) \leqslant 1$. Из этого с учетом (35) получаем следующую оценку:

$$
\begin{aligned}
&\max_{q\in\mathcal{P}(\mathcal{T}^n)}\left[\mathbf{E}\left[\exp\left(-\left|i_{X^*;Y_{q^*}}(X_b;Y_b) - \log\frac{\gamma}{P_{\widehat{S}}(\mathcal{B}_{\boldsymbol{d}}(S))}\right|^+\right)\right] + e^{1-\gamma}\right] \leqslant\\
&\leqslant \max_{q\in\mathcal{P}(\mathcal{T}^n)}\mathbf{E}\big[\exp(-|\Gamma_{n+k}(q)|^+)\mathbb{I}\{(X_b,Y_b,S)\in\mathcal{H}\}\big] +\\
&+ \max_{q\in\mathcal{P}(\mathcal{T}^n)}\mathbf{P}((X_b,Y_b,S)\notin\mathcal{H}) + e^{1-\gamma} + \frac{K_0}{\sqrt{k}}.
\end{aligned}
\tag{40}
$$

Чтобы оценить сверху первое слагаемое в (40), вычислим максимум величины $\exp(-|\Gamma_{n+k}(q)|^+)$ по всем распределениям. Так как функция $\exp(-|\cdot|^+)$ убывает по $\Gamma_{n+k}(q)$, получаем

$$
\max_{q\in\mathcal{P}(\mathcal{T}^n)}\exp(-|\Gamma_{n+k}(q)|^+) \leqslant \exp\Big(-\Big|\min_{q\in\mathcal{P}(\mathcal{T}^n)}\Gamma_{n+k}(q)\Big|^+\Big).
$$

Для вычисления последнего минимума рассмотрим следующие величины:

$$
D_{n+k}(q) = \frac{1}{n+k}\sum_{i=1}^{n}\mathbf{E}'\big[i_{\mathbb{X}^*;\mathbb{Y}_{q^*_\Theta}}(\mathbb{X}_{bi};\mathbb{Y}_{bi})\big] - \frac{k}{n+k}R(\boldsymbol{d}),
$$

$$V_{n+k}(q) = \frac{1}{n+k}\sum_{i=1}^{n}\mathrm{Var}\big(i_{\mathbb{X}^*;\mathbb{Y}_{q^*_\Theta}}(\mathbb{X}_{bi};\mathbb{Y}_{bi})\big) + \frac{k}{n+k}V_{\mathrm{S}}(\boldsymbol{d}),$$

где моменты берутся относительно распределения $P^*_{\mathbb{X}} \times \sum\limits_{\theta\in\mathcal{T}} q_i(\theta)P_{\mathbb{Y}|\mathbb{X},\Theta=\theta}$. Таким образом, этот минимум имеет вид

$$\min_{q\in\mathcal{P}(\mathcal{T}^n)}(n+k)\left(D_{n+k}(q) - t_{k,n}\sqrt{\frac{V_{n+k}(q)}{n+k}}\right) =$$
$$= nC - kR(\boldsymbol{d}) - (n+k)\max_{q_i\in\Pi_\Theta} t_{k,n}\sqrt{\frac{V_{n+k}(q)}{n+k}} + O(1), \tag{41}$$

где максимум в (41) ограничен на множество Π_Θ согласно [8, леммы 63 и 64]. Так как $P^*_{\mathbb{X}} \in \Pi_{\mathbb{X}}$ и $q^*_\Theta \in \Pi_\Theta, |\Pi_\Theta| = 1$, то $\max\limits_{q_i\in\Pi_\Theta} V_{n+k}(q) = nV_{\mathrm{C}}$. Таким образом,

$$\min_{q\in\mathcal{P}(\mathcal{T}^n)}(n+k)\left(D_{n+k}(q) - t_{k,n}\sqrt{\frac{V_{n+k}(q)}{n+k}}\right) =$$
$$= nC - kR(\boldsymbol{d}) - t_{k,n}\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})} + O(1),$$

Выберем $t_{k,n}$ в виде $t_{k,n} = (nC - kR(\boldsymbol{d}) - \bar{c}\log k - \log\gamma - c)/\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d})}$. Тогда получаем $\min\limits_{q\in\mathcal{P}(\mathcal{T}^n)} \Gamma_{n+k}(q) \geqslant \frac{1}{2}\log k + O(1)$. Подставляя это в (40), получаем следующую оценку сверху:

$$\max_{q\in\mathcal{P}(\mathcal{T}^n)} \frac{1}{\sqrt{k}}\,\mathbf{P}((X_b,Y_b,S)\in\mathcal{H}) + \max_{q\in\mathcal{P}(\mathcal{T}^n)}\mathbf{P}((X_b,Y_b,S)\notin\mathcal{H}) + e^{1-\gamma} + \frac{K_0}{\sqrt{k}} \leqslant$$
$$\leqslant \mathrm{Q}(t_{k,n}) + \max_{q\in\mathcal{P}(\mathcal{T}^n)}\frac{B_{n+k}(q)}{\sqrt{n+k}} + \frac{K_0+2}{\sqrt{k}}, \tag{42}$$

где (42) получается в результате выбора $\gamma = (\log_e k)/2 + 1$ и оценивания вероятности $\mathbf{P}((X_b,Y_b,S)\notin\mathcal{H})$ с помощью ЦПТ Берри – Эссеена.

Напомним, что $B_{n+k}(q)$ имеет вид $B_{n+k}(q) = c_0 A_{n+k}(q)/V^{3/2}_{n+k}(q)$. Предполагая, что $\min\limits_{\ell\in\{1,\ldots,n+k\}} \mathrm{Var}[W_\ell] \neq 0$, можно оценить $B_{n+k}(q)$ с помощью определений $A_{n+k}(q)$ и $V_{n+k}(q)$ как

$$B_{n+k}(q) \leqslant \frac{c_0 \max\limits_{\ell}\mathbf{E}\big[|W_\ell - \mathbf{E}[W_\ell]|^3\big]}{\Big(\min\limits_{\ell}\mathrm{Var}[W_\ell]\Big)^{3/2}}. \tag{43}$$

Из (22) и (23) следует, что правая часть конечна при всех q и не зависит от k, n. Таким образом, $\max\limits_{q\in\mathcal{P}(\mathcal{T}^n)} B_{n+k}(q)$ является конечной константой. Подставляя указанные выше значения $t_{k,n}$, выбирая $\max\limits_{q\in\mathcal{P}(\mathcal{T}^n)} B_{n+k}(q) \leqslant B$, где $B > 0$, и используя (42), получаем требуемую границу. ▲

Доказательство теоремы 12. В силу (11) для получения границы снизу на $\underline{\nu}(k,n)$ достаточно построить q, $P_{\bar{Y}_q}$, случайную величину U и γ. Возьмем $q(\theta) = q^*(\theta) = \prod\limits_{i=1}^{n} q^*_\Theta(\theta_i)$, где $q^*_\Theta \in \Pi_\Theta$. Пусть U – число типов в $\mathcal{P}_n(\mathcal{X})$, и пусть $\mathcal{U} = \{1,\ldots,\mathrm{U}\}$ – номера каждого из этих типов, т.е. для данной последовательности $x\in\mathcal{X}^n$ функция U задает ее тип, описываемый некоторым номером $u\in\mathcal{U}$. Далее,

определим $P_{\overline{Y}_q|U}$ как

$$P_{\overline{Y}_q|U}(y\,|\,u) = (P_X q^* P_{Y|X,\mathbf{\Theta}})(y) = \sum_{x,\theta} P_X(x) q^*(\theta) P_{Y|X,\mathbf{\Theta}}(y\,|\,x,\theta),$$

где $P_X(x) = \prod\limits_{i=1}^{n} T_x(x_i)$, $x \in \mathcal{X}^n$, а $T_x \in \mathcal{P}_n(\mathcal{X})$ – тип, соответствующий номеру u. Таким образом, $i_{X;\overline{Y}_q|U}(x;Y\,|\,u) = \sum\limits_{i=1}^{n} i_{\mathbb{X};\mathbb{Y}_{q^*}}(x_i;Y_i)$, где

$$i_{\mathbb{X};\mathbb{Y}_{q^*}}(x';y) := \log \frac{(q^*_{\mathbf{\Theta}} P_{\mathbb{Y}|\mathbb{X},\Theta})(y\,|\,x')}{(T_x q^*_{\mathbf{\Theta}} P_{\mathbb{Y}|\mathbb{X},\Theta})(y)}, \quad x' \in \mathcal{X}, \quad y \in \mathcal{Y},$$

и $j_S(s,\boldsymbol{d}) = \sum\limits_{j=1}^{k} j_{\mathrm{S}}(s_j,\boldsymbol{d})$.

Поскольку q выбираются как н.о.р. величины, по существу имеется канал, в котором $Y \sim \prod\limits_{i=1}^{n} \sum\limits_{\theta_i \in \mathcal{T}} q^*_{\mathbf{\Theta}}(\theta_i) P_{\mathbb{Y}|\mathbb{X}=x_i,\Theta=\theta_i}$ при входе $x = (x_1,\ldots,x_n)$. Таким образом, левая часть неравенства (31) представляет собой обращение теоремы кодирования для стандартного ДКБП без целенаправленных помех, где каналом является такой усредненный канал. Повторяя рассуждения из [9, Приложение C], приходим к следующему неравенству:

$$\begin{aligned}
&\max_{q,P_{\overline{Y}_q},\mathrm{U}} \sup_{\gamma>0} \Bigg[\sum_s P_S(s) \min_x \Bigg[\mathbf{P}\big(j_S(s,\boldsymbol{d}) - i_{X;\overline{Y}_q|U}(x;Y\,|\,U) \leqslant \gamma\big) + \\
&+ \exp\big(j_S(s,\boldsymbol{d}) - \gamma\big) \sum_{u=1}^{\mathrm{U}} \sum_y P_{U|X}(u\,|\,x) P_{\overline{Y}_q|U}(y\,|\,u) \times \\
&\times \mathbb{I}\big\{ j_S(s,\boldsymbol{d}) - i_{X;\overline{Y}_q|U}(x;y\,|\,u) > \gamma \big\} \Bigg] - \frac{\mathrm{U}}{\exp(\gamma)} \Bigg] \geqslant \\
&\geqslant \mathbf{P}\left(\sum_{i=1}^{n} i_{\mathbb{X};\mathbb{Y}_{q^*_{\mathbf{\Theta}}}}(x_i^*;Y_i) - \sum_{j=1}^{k} j_{\mathrm{S}}(S_j,\boldsymbol{d}) \leqslant -\gamma \right) - \frac{K_1}{k} - \frac{K_2}{\sqrt{n}} - \\
&- (n+1)^{|\mathcal{X}|-1} \exp(-\gamma),
\end{aligned} \tag{44}$$

где второе слагаемое в левой части ограничивается снизу нулем, K_1 и K_2 – некоторые константы, а $x^* = (x_1^*,\ldots,x_n^*)$ – последовательность, тип которой T_{x^*} доставляет

$$\min_{T_x \in \mathcal{P}_n(\mathcal{X})} |T_x - P^*_{\mathbb{X}}|, \tag{45}$$

где $P^*_{\mathbb{X}} \in \Pi_{\mathbb{X}}$. Пусть

$$W_\ell = W_\ell(n,k) := \begin{cases} i_{\mathbb{X};\mathbb{Y}_{q^*_{\mathbf{\Theta}}}}(x_\ell^*;Y_\ell), & \text{если } \ell \leqslant n, \\ j_{\mathrm{S}}(S_{n-\ell},\boldsymbol{d}), & \text{если } n < \ell \leqslant n+k. \end{cases}$$

Определим следующие моменты случайной величины W_ℓ:

$$D_{n+k} = \frac{1}{n+k} \sum_{\ell=1}^{n+k} \mathbf{E}[W_\ell], \qquad V_{n+k} = \frac{1}{n+k} \sum_{\ell=1}^{n+k} \mathrm{Var}[W_\ell],$$

$$A_{n+k} = \frac{1}{n+k} \sum_{\ell=1}^{n+k} \mathbf{E}\big[|W_\ell - \mathbf{E}[W_\ell]|^3\big], \qquad B'_{n+k} = \frac{c_0 A_{n+k}}{V_{n+k}^{3/2}}, \quad c_0 > 0.$$

Согласно ЦПТ Берри – Эссеена имеем

$$\mathbf{P}\left(\sum_{\ell=1}^{n+k} W_\ell \leqslant -\gamma\right) \geqslant \mathrm{Q}\left(\frac{D_{n+k} + \dfrac{\gamma}{n+k}}{\sqrt{\dfrac{V_{n+k}}{n+k}}}\right) - \frac{B'_{n+k}}{\sqrt{n+k}}. \tag{46}$$

Справедливы также следующие неравенства из [9, Приложение C]:

$$D_{n+k} \leqslant \frac{n}{n+k} C - \frac{k}{n+k} R(\boldsymbol{d}), \tag{47}$$

$$V_{n+k} \geqslant \frac{n}{n+k} V_{\mathrm{C}} + \frac{k}{n+k} V_{\mathrm{S}}(\boldsymbol{d}) - \frac{K_3}{n+k}, \tag{48}$$

где $K_3 > 0$ – некоторая константа. Далее, с учетом (22) и (23) можно показать, что величина A_{n+k} ограничена, и поэтому B'_{n+k} ограничено некоторой константой $B' > 0$. Используя (47) и (48), получаем

$$\mathrm{Q}\left(\frac{D_{n+k} + \dfrac{\gamma}{n+k}}{\sqrt{\dfrac{V_{n+k}}{n+k}}}\right) \geqslant \mathrm{Q}\Big(\frac{nC - kR(\boldsymbol{d}) + \gamma}{\sqrt{nV_{\mathrm{C}} + kV_{\mathrm{S}}(\boldsymbol{d}) - K_3}}\Big).$$

Подставляя это в (46), выбирая $\gamma = (|\mathcal{X}| - 1/2)\log(n+1)$ и применяя (44), получаем требуемую границу. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Vora A.S., Kulkarni A.A.* A Minimax Theorem for Finite Blocklength Joint Source-Channel Coding over an AVC // 2019 National Conf. on Communications (NCC 2019). Bangalore, India. Feb. 20–23, 2019. P. 1–6. https://doi.org/10.1109/NCC.2019.8732205
2. *Humayed A., Lin J., Li F., Luo B.* Cyber-Physical Systems Security—A Survey // IEEE Internet of Things J. 2017. V. 4. № 6. P. 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172
3. *Slay J., Miller M.* Lessons Learned from the Maroochy Water Breach // Critical Infrastructure Protection (Proc. Int. Conf. ICCIP'2007. Hanover, NH, USA. Mar. 19–21, 2007). Boston: Springer, 2008. https://doi.org/10.1007/978-0-387-75462-8_6
4. *Langner R.* Stuxnet: Dissecting a Cyberwarfare Weapon // IEEE Secur. Priv. 2011. V. 9. № 3. P. 49–51. https://doi.org/10.1109/MSP.2011.67
5. *Maschler M., Solan E., Zamir S.* Game Theory. Cambridge: Cambridge Univ. Press, 2013.
6. *Kulkarni A.A., Coleman T.P.* An Optimizer's Approach to Stochastic Control Problems with Nonclassical Information Structures // IEEE Trans. Autom. Control. 2015. V. 60. № 4. P. 937–949. https://doi.org/10.1109/TAC.2014.2362596
7. *Ahlswede R.* A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity // Ann. Math. Statist. 1970. V. 41. № 3. P. 1027–1033. https://doi.org/10.1214/aoms/1177696979
8. *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
9. *Kostina V., Verdú S.* Lossy Joint Source-Channel Coding in the Finite Blocklength Regime // IEEE Trans. Inform. Theory. 2013. V. 59. № 5. P. 2545–2575. https://doi.org/10.1109/TIT.2013.2238657
10. *Csiszár I., Körner J.* Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge, UK: Cambridge Univ. Press, 2011.

11. *Kosut O., Kliewer J.* Finite Blocklength and Dispersion Bounds for the Arbitrarily-Varying Channel // Proc. 2018 IEEE Int. Symp. on Information Theory (ISIT'2018). Vail, CO, USA. June 17–22, 2018. P. 2007–2011. https://doi.org/10.1109/ISIT.2018.8437724
12. *Jose S.T., Kulkarni A.A.* Linear Programming-Based Converses for Finite Blocklength Lossy Joint Source-Channel Coding // IEEE Trans. Inform. Theory. 2017. V. 63. № 11. P. 7066–7094. https://doi.org/10.1109/TIT.2017.2738634
13. *Jose S.T., Kulkarni A.A.* Improved Finite Blocklength Converses for Slepian–Wolf Coding via Linear Programming // IEEE Trans. Inform. Theory. 2019. V. 65. № 4. P. 2423–2441. https://doi.org/10.1109/TIT.2018.2873623
14. *Borden J.M., Mason D.M., McEliece R.J.* Some Information Theoretic Saddlepoints // SIAM J. Control Optim. 1985. V. 23. № 1. P. 129–143. https://doi.org/10.1137/0323011
15. *Hegde M.V., Stark W.E., Teneketzis D.* On the Capacity of Channels with Unknown Interference // IEEE Trans. Inform. Theory. 1989. V. 35. № 4. P. 770–783. https://doi.org/10.1109/18.32154
16. *Başar T., Wu Y.-W.* A Complete Characterization of Minimax and Maximin Encoder-Decoder Policies for Communication Channels with Incomplete Statistical Description // IEEE Trans. Inform. Theory. 1985. V. 31. № 4. P. 482–489. https://doi.org/10.1109/TIT.1985.1057076
17. *Hughes B., Narayan P.* Gaussian Arbitrarily Varying Channels // IEEE Trans. Inform. Theory. 1987. V. 33. № 2. P. 267–284. https://doi.org/10.1109/TIT.1987.1057288
18. *Jose S.T., Kulkarni A.A.* On a Game Between a Delay-Constrained Communication System and a Finite State Jammer // Proc. 2018 IEEE Conf. on Decision and Control (CDC'2018). Miami, FL, USA. Dec. 17–19, 2018. P. 5063–5068. https://doi.org/10.1109/CDC.2018.8618987
19. *Jose S.T., Kulkarni A.A.* Shannon Meets von Neumann: A Minimax Theorem for Channel Coding in the Presence of a Jammer // IEEE Trans. Inform. Theory. 2020. V. 66. № 5. P. 2842–2859. https://doi.org/10.1109/TIT.2020.2971682
20. *Blackwell D., Breiman L., Thomasian A.J.* The Capacities of Certain Channel Classes under Random Coding // Ann. Math. Statist. 1960. V. 31. № 3. P. 558–567. https://doi.org/10.1214/aoms/1177705783
21. *Ahlswede R.* Elimination of Correlation in Random Codes for Arbitrarily Varying Channels // Z. Wahrsch. Verw. Gebiete. 1978. V. 44. № 2. P. 159–175. https://doi.org/10.1007/BF00533053
22. *Lapidoth A., Narayan P.* Reliable Communication under Channel Uncertainty // IEEE Trans. Inform. Theory. 1998. V. 44. № 6. P. 2148–2177. https://doi.org/10.1109/18.720535
23. *Cover T.M., Thomas J.A.* Elements of Information Theory. Hoboken, NJ: Wiley, 2012.
24. *Kostina V., Verdú S.* Fixed-Length Lossy Compression in the Finite Blocklength Regime // IEEE Trans. Inform. Theory. 2012. V. 58. № 6. P. 3309–3338. https://doi.org/10.1109/TIT.2012.2186786
25. *Shannon C.E.* Coding Theorems for a Discrete Source with a Fidelity Criterion // IRE Nat. Conv. Rec. 1959. Part 4. P. 142–163.
26. *Conforti M., Cornuéjols G., Zambelli G.* Integer Programming. New York: Springer, 2014.
27. *Kosut O., Kliewer J.* Dispersion of the Discrete Arbitrarily-Varying Channel with Limited Shared Randomness // Proc. 2017 IEEE Int. Symp. on Information Theory (ISIT'2017). Aachen, Germany. June 25–30, 2017. P. 1242–1246. https://doi.org/10.1109/ISIT.2017.8006727

Вора Анудж Самиркумар
Кулкарни Анкур Ачют
Индийский технологический институт Бомбея,
Мумбаи, Индия
anujvora@iitb.ac.in
kulkarni.ankur@iitb.ac.in

Поступила в редакцию
20.06.2019
После доработки
17.12.2020
Принята к публикации
05.03.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 2**

УДК 621.391 : 519.724

© 2021 г. **В.С. Лебедев**[1], **Н.А. Полянский**[2]

КОДИРОВАНИЕ В Z-КАНАЛЕ ПРИ БОЛЬШОМ ЧИСЛЕ ОШИБОК

Доказано, что максимальное число слов в коде, исправляющем долю $1/4+\varepsilon$ асимметричных ошибок в Z-канале, равно $\Theta(\varepsilon^{-3/2})$ при $\varepsilon \to 0$.

Ключевые слова: Z-канал, минимальное расстояние, равновесный код.

DOI: 10.31857/S0555292321020029

§ 1. Введение

В теории кодирования для моделирования некоторых асимметричных систем передачи и хранения информации используется Z-канал. В этом двоичном канале символ 0 передается всегда безошибочно. При передаче символа 1 может возникнуть ошибка, поэтому на приеме может быть получен как символ 1, так и 0. Мы рассмотрим модель передачи информации, когда число ошибок при передаче n символов ограничено числом τn для некоторого действительного числа τ, $0 \leqslant \tau \leqslant 1$.

Для данного двоичного слова $\boldsymbol{x} \in \{0,1\}^n$ определим Z-шар с центром в $\boldsymbol{x}$ и относительным радиусом τ, куда включим всевозможные слова, которые могут быть получены при передаче $\boldsymbol{x}$ по Z-каналу с не более чем τn ошибками. Для фиксированных параметров τ и n задача кодирования состоит в том, чтобы найти код $\mathcal{C} \subseteq \{0,1\}^n$, такой что для любых различных $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ соответствующие Z-шары с центрами в $\boldsymbol{x}$ и $\boldsymbol{y}$ и относительными радиусами τ не пересекались. При выполнении этого условия будем говорить, что код может исправить долю τ (асимметричных) ошибок в Z-канале. Отметим, что параметры кодов, исправляющих ошибки в Z-канале, исследовались в большом количестве работ. В частности, известно [1, 2], что асимптотическая скорость кодов, исправляющих долю τ асимметричных ошибок, равна асимптотической скорости кодов, исправляющих ту же самую долю τ ошибок в двоичном симметричном канале. Под двоичным симметричным каналом мы будем понимать канал, в котором при передаче как символа 0, так и символа 1 может произойти ошибка.

Из границы Плоткина [3] следует, что мощность кода, исправляющего долю $1/4+\varepsilon$ симметричных ошибок, ограничена сверху величиной $1+1/(4\varepsilon)$. Таким образом, можно сделать вывод, что асимптотическая скорость кодов, исправляющих долю $1/4+\varepsilon$ ошибок в Z-канале, равна нулю. Однако остаются и другие вопросы, касающиеся границ существования таких кодов. В частности, можно ли утверждать, что мощность кода $\mathcal{C} \subseteq \{0,1\}^n$, исправляющего долю $1/4+\varepsilon$ ошибок в Z-канале, ограничена некоторой функцией от ε, т.е. оценка $|C| \leqslant f(\varepsilon)$ не зависит от длины кода n.

[1] Исследование выполнено в ИППИ РАН при частичной финансовой поддержке Российского фонда фундаментальных исследований (номера проектов 19-01-00364 и 20-51-50007).

[2] Исследование выполнено в Техническом университете Мюнхена и Сколковском институте науки и технологий при частичной поддержке гранта немецкого научно-исследовательского сообщества (номер проекта WA3907/1-1).

В работе [2] утверждалось, что подобная граница выполнена лишь при $\varepsilon > 1/12$. При доказательстве этого утверждения автор [2] допустил ошибку при упрощении задачи линейного программирования, решение которой дает максимальное количество слов в коде, исправляющем долю $1/4 + \varepsilon$ ошибок в Z-канале. В данной статье мы покажем, что максимальное число слов в коде, исправляющем долю $1/4 + \varepsilon$ асимметричных ошибок, равно $\Theta(\varepsilon^{-3/2})$ при $\varepsilon \to 0$. Таким образом, в теореме 1 мы докажем верхнюю границу $|\mathcal{C}| \leqslant \varepsilon^{-3/2}(1 + o(1))$, а в теореме 2 построим код длины $\exp(O(\varepsilon^{-3/2}))$ и объема $|\mathcal{C}| \geqslant \dfrac{3\sqrt{3}}{128}\varepsilon^{-3/2}(1+o(1))$. Отметим, что подобный вопрос для двоичного симметричного канала был ранее разрешен в более строгой форме. Из результатов работ [3–5] следует, что максимальное число слов в коде, исправляющем долю $1/4 + \varepsilon$ симметричных ошибок, равно $(4\varepsilon)^{-1}(1 + o(1))$ при $\varepsilon \to 0$.

§ 2. Обозначения, определения и вспомогательные результаты

Множество целых чисел $\{i, i + 1, \ldots, j\}$ для некоторых целых чисел i и j, для которых выполнено $i \leqslant j$, будем обозначать через $[i, j]$. Если $i = 1$, то будем использовать сокращение $[j]$. Для обозначения векторов будем использовать полужирные символы, например, $\boldsymbol{x}$, а i-ю координату вектора $\boldsymbol{x}$ будем записывать как x_i. Вектор, состоящий из всех нулей, будем обозначать через $\mathbf{0}$. Пусть асимметричная функция $\Delta(\boldsymbol{x}, \boldsymbol{y})$, зависящая от двух векторов $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$, равна числу координат $i \in [n]$, таких что $x_i = 1$ и $y_i = 0$. Расстояние Хэмминга между двумя векторами $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ равно $d_H(\boldsymbol{x}, \boldsymbol{y}) = \Delta(\boldsymbol{x}, \boldsymbol{y}) + \Delta(\boldsymbol{y}, \boldsymbol{x})$. Весом вектора $\boldsymbol{x} \in \{0,1\}^n$ будем называть величину $\mathrm{wt}(\boldsymbol{x}) = d_H(\boldsymbol{x}, \mathbf{0})$, а относительным весом $\boldsymbol{x}$ – величину $\mathrm{wt}(\boldsymbol{x})/n$. Определим *Z-шар* и *S-шар* с центром в $\boldsymbol{x} \in \{0,1\}^n$ и радиусом t следующим образом:

$$B_t^{\mathrm{Z}}(\boldsymbol{x}) = \{\boldsymbol{y} \in \{0,1\}^n : \ y_i \leqslant x_i \ \forall i \in [n],\ \Delta(\boldsymbol{x}, \boldsymbol{y}) \leqslant t\},$$
$$B_t^{\mathrm{S}}(\boldsymbol{x}) = \{\boldsymbol{y} \in \{0,1\}^n : \ d_H(\boldsymbol{x}, \boldsymbol{y}) \leqslant t\}.$$

Кодом $\mathcal{C} \subseteq \{0,1\}^n$ будем называть произвольное подмножество двоичных векторов одной длины. *Мощность* (число слов) кода $\mathcal{C}$ будем обозначать через $|\mathcal{C}|$. Код $\mathcal{C} \subseteq \{0,1\}^n$ назовем *w-равновесным*, если вес всякого слова $\boldsymbol{x} \in \mathcal{C}$ равен $\mathrm{wt}(\boldsymbol{x}) = w$. Будем говорить, что код $\mathcal{C}$ *исправляет* t асимметричных (симметричных) ошибок, если для любых различных $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ соответствующие Z-шары (S-шары) с центрами в $\boldsymbol{x}$ и $\boldsymbol{y}$ и радиусами t не пересекаются, т.е. $B_t^{\mathrm{Z}}(\boldsymbol{x}) \cap B_t^{\mathrm{Z}}(\boldsymbol{y}) = \varnothing$ ($B_t^{\mathrm{S}}(\boldsymbol{x}) \cap B_t^{\mathrm{S}}(\boldsymbol{y}) = \varnothing$). Заметим, что код $\mathcal{C}$ исправляет t асимметричных ошибок тогда и только тогда, когда для любых различных $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ выполнено неравенство $\max(\Delta(\boldsymbol{x}, \boldsymbol{y}), \Delta(\boldsymbol{y}, \boldsymbol{x})) > t$. Код $\mathcal{C} \subseteq \{0,1\}^n$ исправляет *долю* τ асимметричных (симметричных) ошибок, если он исправляет t асимметричных (симметричных) ошибок для $t = \lceil \tau n \rceil$. В следующей лемме отметим очевидный, но важный результат [6].

Лемма 1. *Пусть код $\mathcal{C} \subseteq \{0,1\}^n$ является w-равновесным. Код $\mathcal{C}$ исправляет t асимметричных ошибок тогда и только тогда, когда он исправляет t симметричных ошибок.*

Далее напомним два известных результата, доказанных в работах [3] и [1] соответственно.

Лемма 2. *Пусть код $\mathcal{C} \subseteq \{0,1\}^n$ исправляет t, $t > n/4$, симметричных ошибок. Тогда мощность кода $\mathcal{C}$ ограничена следующим образом*:

$$|\mathcal{C}| \leqslant 2\left\lfloor \frac{2t+2}{4t+3-n} \right\rfloor.$$

Лемма 3. *Пусть код $\mathcal{C} \subseteq \{0,1\}^n$ является w-равновесным и исправляет t симметричных ошибок. Если выполнено соотношение $t + 1 \leqslant w \leqslant (n - \sqrt{n^2 - 4tn})/2$,*

то мощность кода $\mathcal{C}$ ограничена следующим образом:

$$|\mathcal{C}| \leqslant \left\lfloor \frac{tn}{w^2-(w-t)n} \right\rfloor .$$

§ 3. Верхняя граница

В следующем утверждении мы получим верхнюю границу на мощность кода, исправляющего долю $1/4+\varepsilon$ асимметричных ошибок. Идея доказательства этой верхней границы состоит в том, чтобы специальным образом разбить код на $O(\varepsilon^{-1/2})$ подкодов (слоев). Каждый слой будет содержать слова близкого веса. Тогда, удлиняя кодовые слова внутри одного слоя так, чтобы все они стали одинакового веса, мы сводим задачу к оценке мощности равновесного кода, решение которой известно (см. леммы 1–3).

Т е о р е м а 1. *Пусть $n > 36$ и код $\mathcal{C} \subseteq \{0,1\}^n$ исправляет долю асимметричных ошибок, равную $1/4+\varepsilon$ для некоторого $0 < \varepsilon < 1/12 - 3/n$. Тогда мощность кода ограничена следующим образом*: $|\mathcal{C}| \leqslant \dfrac{1+7/n+2\sqrt{\varepsilon}+4\varepsilon+16\sqrt{\varepsilon}/n}{\varepsilon^{3/2}} + 10$.

Д о к а з а т е л ь с т в о. Без ограничения общности можно считать, что число кодовых слов веса, меньшего $n/2$, не меньше, чем число кодовых слов веса, превосходящего $n/2$ (иначе можно рассмотреть код той же мощности, в котором кодовые слова получаются заменой нулей на единицы и наоборот). Для целого неотрицательного числа i обозначим $\rho_i := \dfrac{i}{2i+1}$. Определим подкод

$$\mathcal{A}_i := \{\boldsymbol{x} \in \mathcal{C} : \lfloor \rho_i n \rfloor < \mathrm{wt}(\boldsymbol{x}) \leqslant \lfloor \rho_{i+1} n \rfloor\}.$$

Удлиним все кодовые слова кода $\mathcal{A}_i$ путем добавления $\lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1$ координат так, чтобы все полученные слова имели вес $\lfloor \rho_{i+1} n \rfloor$. Заметим, что это можно сделать несколькими способами. Из леммы 1 следует, что получившийся код $\mathcal{A}'_i \subseteq \{0,1\}^{n+\lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1}$ содержит слова веса $\lfloor \rho_{i+1} n \rfloor$ и исправляет $\lceil (1/4+\varepsilon)n \rceil$ симметричных ошибок. Из леммы 3 (при $\varepsilon < 1/12 - 3/n$ условия леммы выполнены) получаем, что

$$|\mathcal{A}_i| = |\mathcal{A}'_i| \leqslant \frac{\lceil (1/4+\varepsilon)n \rceil (n + \lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1)}{\lfloor \rho_{i+1} n \rfloor^2 - (\lfloor \rho_{i+1} n \rfloor - \lceil (1/4+\varepsilon)n \rceil)(n + \lfloor \rho_{i+1} n \rfloor - \lfloor \rho_i n \rfloor - 1)} \leqslant$$
$$\leqslant \frac{(1/4+\varepsilon+1/n)(1+\rho_{i+1}-\rho_i)}{\rho_{i+1}^2 - (\rho_{i+1} - 1/4 - \varepsilon)(1+\rho_{i+1}-\rho_i)}.$$

В последнем неравенстве воспользовались тем, что $w^2-(w-t)n$ является монотонно убывающей функцией по w при $w \leqslant (n - \sqrt{n^2-4tn})/2$. Заметим, что

$$\rho_{i+1}^2 - (\rho_{i+1} - 1/4)(1+\rho_{i+1}-\rho_i) = 0,$$

поскольку $\rho_i = \dfrac{i}{2i+1}$. Значит, $|\mathcal{A}'_i| \leqslant 1 + (1/4+1/n)\varepsilon^{-1}$.

Пусть $i_0 := \lfloor 1/(2\sqrt{\varepsilon}) \rfloor$, и следовательно, $\rho_{i_0} \geqslant \dfrac{1-2\sqrt{\varepsilon}}{2+2\sqrt{\varepsilon}}$. Для неотрицательного целого числа j рассмотрим подкод

$$\mathcal{B}_j := \{\boldsymbol{x} \in \mathcal{C} : \lfloor \rho_{i_0} n \rfloor + j\lceil 2\varepsilon n \rceil < \mathrm{wt}(\boldsymbol{x}) \leqslant \lfloor \rho_{i_0} n \rfloor + (j+1)\lceil 2\varepsilon n \rceil\}.$$

Как и ранее, удлиним все слова кода $\mathcal{B}_j$ путем добавления $\lceil 2\varepsilon n \rceil$ координат так, чтобы полученные слова имели одинаковый вес. Получившийся код $\mathcal{B}'_j \subseteq \{0,1\}^{n+\lceil 2\varepsilon n \rceil}$ содержит слова веса $\lfloor \rho_{i_0} n \rfloor + (j+1)\lceil 2\varepsilon n \rceil$ и исправляет $\lceil (1/4+\varepsilon)n \rceil$ симметричных

ошибок. Используя лемму 2, можем оценить

$$|\mathcal{B}_j| = |\mathcal{B}'_j| \leqslant \frac{n + 4\varepsilon n + 8}{n + 4\varepsilon n + 3 - n - 2\varepsilon n - 1} \leqslant (1/2 + 4/n + 2\varepsilon)\varepsilon^{-1}.$$

Для того чтобы каждое слово кода $\mathcal{C}$, имеющее вес в интервале $[1, n/2]$, вошло в $\mathcal{A}_i$ для $i \in [0, i_0 - 1]$ или в $\mathcal{B}_j$ для $j \in [0, j_0 - 1]$, достаточно взять $j_0 := \lfloor 3/(4\sqrt{\varepsilon}) + 2 \rfloor$, так как

$$\frac{n/2 - \lfloor \rho_{i_0} n \rfloor}{\lceil 2\varepsilon n \rceil} \leqslant \frac{n/2 - \dfrac{1 - 2\sqrt{\varepsilon}}{2 + 2\sqrt{\varepsilon}} n}{2\varepsilon n} + 1 \leqslant \left\lfloor \frac{3}{4\sqrt{\varepsilon}} + 2 \right\rfloor.$$

Поскольку число кодовых слов с весом из интервала $[1, n/2]$ не меньше числа кодовых слов с весом из интервала $[n/2, n - 1]$, получаем

$$\begin{aligned}
|\mathcal{C}| &\leqslant 2\left(\sum_{i=0}^{i_0 - 1} |\mathcal{A}_i| + \sum_{j=0}^{j_0 - 1} |\mathcal{B}_j| \right) + 2 \leqslant \\
&\leqslant \frac{1}{\varepsilon^{3/2}}(\varepsilon + 1/4 + 1/n + 3/4 + 6/n + 3\varepsilon + 2\sqrt{\varepsilon} + 16\sqrt{\varepsilon}/n + 8\varepsilon^{3/2}) + 2 = \\
&= \frac{1 + 7/n + 4\varepsilon + 2\sqrt{\varepsilon} + 16\sqrt{\varepsilon}/n}{\varepsilon^{3/2}} + 10. \quad \blacktriangle
\end{aligned}$$

§ 4. Нижняя граница

В следующем утверждении мы докажем, что существует код длины $\exp(\Theta(\varepsilon^{-3/2}))$ и мощности $\Omega(\varepsilon^{-3/2})$, исправляющий долю $1/4 + \varepsilon$ асимметричных ошибок при $\varepsilon \to 0$. Мы воспользуемся соображениями, которые использовали при доказательстве теоремы 1, а именно: для построения кода большой мощности мы сначала найдем $\Omega(\varepsilon^{-1/2})$ равновесных кодов, таких что j-й код $\mathcal{C}_j$ содержит слова с относительным весом $1/2 - j\varepsilon$ и исправляет долю $1/4 + \Omega(\varepsilon)$ симметричных ошибок. Отметим, что конструкция такого кода при $j = 0$ была впервые предложена в работе [4], в которой авторы исследовали коды для списочного декодирования. Затем мы рассмотрим код $\widetilde{\mathcal{C}}_j$, являющийся многократным повторением кода $\mathcal{C}_j$, и случайно переставим координаты в этом коде. Эта операция не изменяет корректирующую способность кода. Итоговый код является объединением кодов $\widetilde{\mathcal{C}}_j$. Случайная перестановка координат внутри каждого из равновесных кодов гарантирует, что значение функции $\Delta(\boldsymbol{x}, \boldsymbol{y})$ для $\boldsymbol{x} \in \widetilde{\mathcal{C}}_j$ и $\boldsymbol{y} \in \widetilde{\mathcal{C}}_i$ при $j < i$ достаточно велико с большой вероятностью.

Теорема 2. *Существует код длины* $\exp(O(\varepsilon^{-3/2}))$, *исправляющий долю* $\dfrac{1}{4} + \varepsilon$ *асимметричных ошибок и содержащий не менее чем* $\dfrac{3\sqrt{3}}{128}\varepsilon^{-3/2}(1 + o(1))$ *кодовых слов при* $\varepsilon \to 0$.

Доказательство. Рассмотрим целое положительное $m := \lfloor 3/(32\varepsilon) \rfloor$ и определим константу $c := 2^{-3/2}$. Для всякого $j \in \{-\lfloor c\sqrt{m} \rfloor, \ldots, \lfloor c\sqrt{m} \rfloor\}$ обозначим $f_j := \binom{2m}{m - j}$. Рассмотрим двоичную матрицу A_j размера $2m \times f_j$, столбцы которой составляют множество всевозможных двоичных векторов длины $2m$ и веса $m - j$. Для двух произвольных различных строк $\boldsymbol{x}$ и $\boldsymbol{y}$ матрицы A_j подсчитаем число координат, в которых они различаются:

$$\Delta(\boldsymbol{x}, \boldsymbol{y}) = \Delta(\boldsymbol{y}, \boldsymbol{x}) = \binom{2m - 2}{m - j - 1}.$$

Значит, код, кодовыми словами которого являются строки матрицы A_j, исправляет долю ρ_j асимметричных ошибок, где

$$\rho_j := \frac{\binom{2m-2}{m-j-1}-1}{\binom{2m}{m-j}} = \frac{(m-j)(m+j)}{2m(2m-1)} - \frac{1}{\binom{2m}{m-j}} = \frac{1}{4} + \frac{m/2-j^2}{4m^2-2m} - \frac{1}{\binom{2m}{m-j}}.$$

Проверим, что для достаточно малого ε это выражение не меньше $\frac{1}{4}+\varepsilon$:

$$\frac{m/2-j^2}{4m^2-2m} - \frac{1}{\binom{2m}{m-j}} \geqslant \frac{m/2-c^2m}{4m^2-2m} - \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}} =$$
$$= \frac{3}{32m-16} - \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}} = \frac{3}{32m} + \frac{3}{2m(32m-16)} - \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}} \geqslant \varepsilon.$$

В последнем неравенстве были использованы соотношения $m = \lfloor 3/(32\varepsilon)\rfloor$, $c = 2^{-3/2}$, а также тот факт, что для достаточно большого m (малого ε) верно неравенство

$$\frac{3}{64m^2} > \frac{1}{\binom{2m}{m-\lfloor c\sqrt{m}\rfloor}}.$$

Действительно, правая часть последнего неравенства равна $2^{-2m(1+o(1))}$ при $m\to\infty$.

Для всякого целого положительного числа z определим матрицу $A_j^{(z)}$ размера $2m \times zf_j$, составленную из z копий матрицы A_j. Копии матрицы A_j записываются справа, т.е. удлиняются строки $A_j^{(z)} = (A_j, A_j, \ldots, A_j)$. Через $\widetilde{A}_j^{(z)}$ обозначим матрицу, полученную из $A_j^{(z)}$ случайной перестановкой ее столбцов. Подразумевается, что из всех возможных перестановок случайным образом выбирается одна, причем выбор равновероятен для всех перестановок. Заметим, что код, кодовыми словами которого являются строки матрицы $\widetilde{A}_j^{(z)}$, исправляет ту же долю асимметричных ошибок, что и код, полученный из A_j. Определим целые числа

$$z_j := \prod_{\substack{i=-\lfloor c\sqrt{m}\rfloor,\\ i\neq j}}^{\lfloor c\sqrt{m}\rfloor} \binom{2m}{m-i}, \quad N := \prod_{i=-\lfloor c\sqrt{m}\rfloor}^{\lfloor c\sqrt{m}\rfloor} \binom{2m}{m-i}, \quad M := 2m(2\lfloor c\sqrt{m}\rfloor+1).$$

Рассмотрим матрицу A размера $M\times N$, содержащую в качестве подматриц матрицы $\widetilde{A}_j^{(z_j)}$ для всех $j\in\{-\lfloor c\sqrt{m}\rfloor,\ldots,\lfloor c\sqrt{m}\rfloor\}$. Для определенности будем считать, что матрицы $\widetilde{A}_j^{(z_j)}$ записаны друг под другом в естественном порядке увеличения параметра j, начиная с $j=-\lfloor c\sqrt{m}\rfloor$. Используя параметр ε, стремящийся к нулю, число строк M и число столбцов N в матрице A оцениваются как

$$M = \frac{3\sqrt{3}}{128\varepsilon\sqrt{\varepsilon}}(1+o(1)), \quad N = \exp(\Theta(\varepsilon^{-3/2})).$$

Покажем, что для произвольных различных строк $\widetilde{\boldsymbol{x}}$ и $\widetilde{\boldsymbol{y}}$ матрицы A значение функции $\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}),\Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}}))$ достаточно велико с большой вероятностью при $\varepsilon\to 0$. Последнее условие гарантирует, что код исправит нужную долю асимметричных ошибок. Более формально, пусть $\widetilde{\boldsymbol{x}}$ и $\widetilde{\boldsymbol{y}}$ являются строками из $\widetilde{A}_j^{(z_j)}$ и $\widetilde{A}_i^{(z_i)}$, где $j<i$. Ясно, что $\mathrm{wt}(\widetilde{\boldsymbol{x}}) = \frac{m-j}{2m}N > \frac{m-i}{2m}N = \mathrm{wt}(\widetilde{\boldsymbol{y}})$ и $\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}),\Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}})) = \Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}})$.

Пусть $T = \{\mathrm{wt}(\widetilde{\boldsymbol{x}}) - \mathrm{wt}(\widetilde{\boldsymbol{y}}), \ldots, \min(\mathrm{wt}(\widetilde{\boldsymbol{x}}), N - \mathrm{wt}(\widetilde{\boldsymbol{y}}))\}$. Распределение вероятностей для случайной величины $\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}})$ выглядит следующим образом:

$$\Pr\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) = t\} = \begin{cases} \dfrac{\binom{\mathrm{wt}(\widetilde{\boldsymbol{x}})}{t}\binom{N - \mathrm{wt}(\widetilde{\boldsymbol{x}})}{\mathrm{wt}(\widetilde{\boldsymbol{y}}) - \mathrm{wt}(\widetilde{\boldsymbol{x}}) + t}}{\binom{N}{\mathrm{wt}(\widetilde{\boldsymbol{y}})}} & \text{для } t \in T, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Оценим вероятность того события, что $\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}})$ недостаточно велико:

$$\Pr\left\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) \leqslant N\left(\frac{1}{4} + \varepsilon\right)\right\} \leqslant N \max_{t \in [0, \lfloor N(\frac{1}{4}+\varepsilon)\rfloor]} \Pr\left\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) = t\right\}. \tag{1}$$

Пусть целое число t равно αN для некоторого действительного числа $\alpha \in \left[\frac{i-j}{2m}, \min\left(\frac{m-j}{2m}, \frac{m+i}{2m}\right)\right]$. Заметим, что N и m являются функциями от ε. Определим функцию

$$g_{i,j}(\alpha, \varepsilon) := \frac{1}{N}\log\left(\Pr\left\{\Delta(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{y}}) = t\right\}\right).$$

Для произвольных целых чисел $u > v \geqslant 1$ биномиальный коэффициент $\binom{u}{v}$ удовлетворяет неравенству

$$\sqrt{\frac{u}{8v(u-v)}}\,2^{uh(v/u)} \leqslant \binom{u}{v} \leqslant 2^{uh(v/u)},$$

где $h(x) := -x\log x - (1-x)\log(1-x)$. Значит, для $\alpha \in \left(\frac{i-j}{2m}, \min\left(\frac{m-j}{2m}, \frac{m+i}{2m}\right)\right)$ выполнена оценка

$$g_{i,j}(\alpha, \varepsilon) \leqslant \frac{m-j}{2m}h\left(\frac{2\alpha m}{m-j}\right) + \frac{m+j}{2m}h\left(\frac{j-i+2\alpha m}{m+j}\right) - h\left(\frac{m-i}{2m}\right) -$$
$$- \frac{\log\left(\frac{m^2}{2(m-i)(m+i)N}\right)}{2N} \leqslant r_{i,j}(\alpha, \varepsilon) + \delta(\varepsilon),$$

где функции $r_{i,j}(\alpha, \varepsilon)$ и $\delta_{i,j}(\varepsilon)$ определены следующим образом:

$$r_{i,j}(\alpha, \varepsilon) := \frac{m-j}{2m}h\left(\frac{2\alpha m}{m-j}\right) + \frac{m+j}{2m}h\left(\frac{j-i+2\alpha m}{m+j}\right) - h\left(\frac{m-i}{2m}\right),$$
$$\delta(\varepsilon) := \frac{\log(2N)}{2N}.$$

Используя соотношение $\dfrac{\partial h(x)}{\partial x} = \log\left(\dfrac{1-x}{x}\right)$, посчитаем производную функции $r_{i,j}(\alpha, \varepsilon)$:

$$q_{i,j}(\alpha, \varepsilon) := \frac{\partial r_{i,j}(\alpha, \varepsilon)}{\partial \alpha} = \log\left(\frac{m-j-2\alpha m}{2\alpha m}\right) + \log\left(\frac{m+i-2\alpha m}{j-i+2\alpha m}\right).$$

Пусть $\alpha_{i,j} = \alpha_{i,j}(\varepsilon) := \dfrac{(m-j)(m+i)}{4m^2}$. Несложно видеть, что функция $q_{i,j}(\alpha, \varepsilon)$ строго положительна при $\alpha < \alpha_{i,j}$, и функция $r_{i,j}(\alpha, \varepsilon) \leqslant 0$ для всех допустимых α, причем $r_{i,j}(\alpha_{i,j}, \varepsilon) = 0$. В силу выбора $m = \lfloor 3/(32\varepsilon)\rfloor$ и ограничений на i и j, т.е.

$-\lfloor c\sqrt{m}\rfloor \leqslant j < i \leqslant \lfloor c\sqrt{m}\rfloor$, получаем, что $\alpha_{i,j}(\varepsilon) - (1/4+\varepsilon) > 0$, а также

$$\alpha_{i,j}(\varepsilon) - \left(\frac{1}{4}+\varepsilon\right) = \frac{(m-j)(m+i)}{4m^2} - \left(\frac{1}{4}+\varepsilon\right) = \frac{(i-j)m - ij - 4\varepsilon m^2}{4m^2}.$$

Поскольку производная функции $r_{i,j}(\alpha,\varepsilon)$ положительна при $\alpha \leqslant 1/4+\varepsilon$, можем заключить, что

$$\sup_{\frac{i-j}{2m}<\alpha\leqslant\frac{1}{4}+\varepsilon} g_{i,j}(\alpha,\varepsilon) \leqslant r_{i,j}(1/4+\varepsilon,\varepsilon) + \delta(\varepsilon). \tag{2}$$

Заметим, что выполнено частичное разложение Тейлора с остаточным членом в форме Лагранжа:

$$\begin{aligned} &r_{i,j}(\alpha_{i,j},\varepsilon) = r_{i,j}(1/4+\varepsilon,\varepsilon) + (\alpha_{i,j} - 1/4 - \varepsilon) q_{i,j}(1/4+\varepsilon,\varepsilon) + \\ &+ (\alpha_{i,j} - 1/4 - \varepsilon)^2 \frac{\sigma_{i,j}(\theta,\varepsilon)}{2}, \end{aligned} \tag{3}$$

где $\sigma_{i,j}(\alpha,\varepsilon) := \dfrac{\partial q_{i,j}(\alpha,\varepsilon)}{\partial\alpha}$, а θ – некоторая точка между $1/4+\varepsilon$ и $\alpha_{i,j}$. Далее найдем вид функции $\sigma_{i,j}(\alpha,\varepsilon)$ и покажем ее ограниченность снизу на интервале $(1/4+\varepsilon, \alpha_{i,j})$:

$$\frac{\sigma_{i,j}(\alpha,\varepsilon)}{\log e} = \frac{j-m}{\alpha(m-j-2\alpha m)} - \frac{2m(m+j)}{(j-i+2\alpha m)(m+i-2\alpha m)}.$$

При $\varepsilon \to 0$ имеем $m = \Theta(\varepsilon^{-1})$. Следовательно, $\sigma_{i,j}(\theta,\varepsilon) = -16\log e(1+o(1))$ при $\varepsilon\to 0$, поскольку

$$\lim_{\varepsilon\to 0} \sup_{1/4+\varepsilon<\alpha<\alpha_{i,j}} \sigma_{i,j}(\alpha,\varepsilon) = -16\log e, \quad \lim_{\varepsilon\to 0} \inf_{1/4+\varepsilon<\alpha<\alpha_{i,j}} \sigma_{i,j}(\alpha,\varepsilon) = -16\log e.$$

Теперь оценим $q_{i,j}(1/4+\varepsilon,\varepsilon)$ при $\varepsilon\to 0$:

$$\begin{aligned} &q_{i,j}(1/4+\varepsilon,\varepsilon) = \log\left(1 + \frac{mi - 4\varepsilon m^2 - jm - ji}{(m/2+2\varepsilon m)(m/2+j-i+2\varepsilon m)}\right) = \\ &= 4\log e \frac{m(i-j) - 4\varepsilon m^2 - ji}{m^2}(1+o(1)). \end{aligned}$$

Также напомним, что $r_{i,j}(\alpha_{i,j},\varepsilon) = 0$. Подставляя вышеуказанные оценки в (3), имеем

$$\begin{aligned} &r_{i,j}(1/4+\varepsilon,\varepsilon) = -\left(\alpha_{i,j} - \frac{1}{4} - \varepsilon\right)\left(\frac{m(i-j) - 4\varepsilon m^2 - ji}{m^2}(4\log e - 2\log e)\right) \times \\ &\times (1+o(1)) \leqslant -\lambda\varepsilon^2 + o(\varepsilon^2) \end{aligned}$$

для некоторой константы $\lambda > 0$ и $\varepsilon\to 0$. Используя это неравенство, оценку $\delta(\varepsilon) = o(\varepsilon^2)$ и неравенство (2), оценим левую часть (1) следующим образом:

$$\Pr\left\{\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}) \leqslant N\left(\frac{1}{4}+\varepsilon\right)\right\} \leqslant N 2^{-\lambda\varepsilon^2 N + o(\varepsilon^2 N)} = o(1),$$

поскольку $\varepsilon^2 N = \exp(\Omega(\varepsilon^{-3/2}))$. Вероятность того, что $\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}), \Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}})) \leqslant N(1/4+\varepsilon)$ хотя бы для какой-то пары строк $\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}$ из матрицы A, оценим сверху величиной

$$\binom{M}{2} \max_{\substack{\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}\in A \\ \widetilde{\boldsymbol{x}}\neq\widetilde{\boldsymbol{y}}}} \Pr\left\{\max(\Delta(\widetilde{\boldsymbol{x}},\widetilde{\boldsymbol{y}}), \Delta(\widetilde{\boldsymbol{y}},\widetilde{\boldsymbol{x}})) \leqslant N\left(\frac{1}{4}+\varepsilon\right)\right\} = o(1).$$

Это означает, что при $\varepsilon \to 0$ с большой вероятностью строки случайной матрицы A могут служить кодом, исправляющим долю $1/4 + \varepsilon$ асимметричных ошибок. ▲

§ 5. Заключение

Из теорем 1 и 2 вытекает следующее утверждение.

Следствие. *Максимальное число слов в коде, исправляющем долю* $1/4 + \varepsilon$ *асимметричных ошибок, равно* $\Theta(\varepsilon^{-3/2})$ *при* $\varepsilon \to 0$.

Отметим, что длина предъявленной случайной конструкции в теореме 2 достаточно велика. Было бы интересно найти существенно более короткий код, имеющий ту же по порядку мощность.

СПИСОК ЛИТЕРАТУРЫ

1. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. http://mi.mathnet.ru/ppi762
2. *Borden J.M.* A Low-Rate Bound for Asymmetric Error-Correcting Codes // IEEE Trans. Inform. Theory. 1983. V. 29. № 4. P. 600–602. https://doi.org/10.1109/TIT.1983.1056708
3. *Plotkin M.* Binary Codes with Specified Minimum Distance // IRE Trans. Inform. Theory. 1960. V. 6. № 4. P. 445–450. https://doi.org/10.1109/TIT.1960.1057584
4. *Alon N., Bukh B., Polyanskiy Y.* List-Decodable Zero-Rate Codes // IEEE Trans. Inform. Theory. 2018. V. 65. № 3. P. 1657–1667. https://doi.org/10.1109/TIT.2018.2868957
5. *Левенштейн В.И.* Применение матриц Адамара к одной задаче кодирования // Проблемы кибернетики. Вып. 5. М.: Физматгиз, 1961. С. 123–136.
6. *Варшамов Р.Р.* К теории несимметрических кодов // Докл. АН СССР. 1965. Т. 164. № 4. С. 757–760. http://mi.mathnet.ru/dan31642

Лебедев Владимир Сергеевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
lebedev37@mail.ru
Полянский Никита Андреевич
Сколковский институт науки и технологий (Сколтех)
Технический университет Мюнхена, Германия
nikitapolyansky@gmail.com

Поступила в редакцию
14.12.2020
После доработки
25.03.2021
Принята к публикации
26.03.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 2**

УДК 621.391 : 519.174.7

© 2021 г. **А.В. Бердников, А.М. Райгородский**

ОЦЕНКИ ЧИСЕЛ БОРСУКА ПО ДИСТАНЦИОННЫМ ГРАФАМ СПЕЦИАЛЬНОГО ВИДА[1]

В 1933 г. Борсук сформулировал ставшую классической гипотезу о том, что минимальное число частей меньшего диаметра, на которые может быть разбито произвольное множество диаметра 1 в $\mathbb{R}^n$, равно $n+1$. В 1993 г. гипотеза была опровергнута с помощью совокупностей точек с координатами 0 и 1. Позже вторым автором статьи были получены более сильные контрпримеры, основанные на семействах точек с координатами $-1, 0, 1$. В настоящей статье устанавливаются новые нижние оценки для чисел Борсука в семействах такого типа.

Ключевые слова: проблема Борсука, $(0,1)$-векторы, разбиения, графы диаметров, раскраски.

DOI: 10.31857/S0555292321020030

§ 1. Введение и формулировки результатов

Настоящая статья посвящена одному важному аспекту классической проблемы Борсука о разбиении множеств на части меньшего диаметра (см. [1–3]). Напомним, что *число Борсука* – это величина $f(d)$, равная минимальному количеству частей меньшего диаметра, на которые может быть разбито произвольное множество $\Omega \subset \mathbb{R}^d$, имеющее диаметр 1. Долгое время большинство специалистов верило, что $f(d) = d+1$. Однако в 1993 г. эта гипотеза была опровергнута, и сейчас известно, что хотя $f(1) = 2$, $f(2) = 3$, $f(3) = 4$, уже $f(64) > 65$ (см. [1, 4]), и более того,

$$\left(\left(\frac{2}{\sqrt{3}}\right)^{\sqrt{2}} + o(1)\right)^{\sqrt{d}} \leqslant f(d) \leqslant \left(\sqrt{\frac{3}{2}} + o(1)\right)^{d} \tag{1}$$

(см. нижнюю оценку в [1], а верхнюю – в [5, 6]). При малых d множество смежных результатов и ссылок можно найти в [7–9].

В дальнейшем нас будут интересовать нижние оценки величины $f(d)$ при $d \to \infty$. Пусть $\Omega \subset \mathbb{R}^d$ – конечное множество точек. Граф $G = G_\Omega = (\Omega, E)$ называется его *графом диаметров*, если $(x, y) \in E$ тогда и только тогда, когда расстояние $|x - y|$ между точками x, y равно диаметру $\operatorname{diam}\Omega$ множества Ω. Напомним, что *хроматическое число* произвольного графа H – это минимальное число цветов $\chi(H)$, в которые можно так покрасить вершины H, чтобы концы каждого ребра имели разные цвета. Нетрудно видеть, что для конечных множеств разбиение на части меньшего диаметра и раскраска графа диаметров суть одно и то же. Поэтому имеет место оценка $f(d) \geqslant \chi(G_\Omega)$, коль скоро $\Omega \subset \mathbb{R}^d$.

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 18-01-00355) и гранта Президента Российской Федерации для государственной поддержки ведущих научных школ (номер гранта НШ-2540.2020.1).

Напомним, далее, что *дистанционным графом* в $\mathbb{R}^d$ называется любой граф $G = (V, E)$, у которого $V \subset \mathbb{R}^d$, а ребра – всевозможные пары вершин, между которыми одно и то же наперед заданное расстояние (см. [10–13]).

Нижняя оценка в неравенстве (1) получается следующим образом. Сперва в $\mathbb{R}^n$ берется дистанционный граф G, у которого вершины являются $(-1, 0, 1)$-векторами с равными (общими для всех) количествами отрицательных и положительных координат, а ребра порождаются парами ортогональных вершин. Затем ищется граф диаметров H, изоморфный G и расположенный в $\mathbb{R}^d$ с $d \leqslant \dfrac{n(n+1)}{2}$. В итоге оказывается, что

$$\chi(G) \geqslant \left(\frac{2}{\sqrt{3}} + o(1)\right)^n,$$

откуда

$$f(d) \geqslant \chi(H) = \chi(G) \geqslant \left(\left(\frac{2}{\sqrt{3}}\right)^{\sqrt{2}} + o(1)\right)^{\sqrt{d}}.$$

Возникает следующая естественная постановка. Пусть $n, k_{-1}, k_0, k_1 \in \mathbb{N}$, причем $k_{-1} + k_0 + k_1 = n$. Пусть $V(n, k_{-1}, k_0, k_1)$ – множество $(-1, 0, 1)$-векторов в $\mathbb{R}^n$, в каждом из которых k_i координат, равных $i \in \{-1, 0, 1\}$. Пусть $\mathcal{G}(k_{-1}, k_0, k_1)$ – множество всех таких дистанционных графов с вершинами $V(n, k_{-1}, k_0, k_1)$, что для каждого из них существует изоморфный ему граф диаметров в $\mathbb{R}^d$ с $d \leqslant \dfrac{n(n+1)}{2}$. Пусть, наконец, $\chi(n, k_{-1}, k_0, k_1)$ – максимум величины $\chi(G)$ по всем $G \in \mathcal{G}(k_{-1}, k_0, k_1)$. Ясно, что сказанное выше означает справедливость неравенства

$$\max_{k_1} \chi(n, k_1, k_0, k_1) \geqslant \left(\frac{2}{\sqrt{3}} + o(1)\right)^n.$$

Вопрос в том, как ведет себя с ростом n исходная величина $\chi(n, k_{-1}, k_0, k_1)$. Растет ли она экспоненциально при $k_{-1} \neq k_1$? Тут важно не забывать, что даже при фиксированных n, k_{-1}, k_1 максимизация ведется по величине расстояния, задающего дистанционный граф из множества $\mathcal{G}(k_{-1}, k_0, k_1)$, с нетривиальным, однако, условием существования изоморфного графа диаметров в пространстве сравнительно малой размерности.

Ответ на поставленные вопросы дает следующая

Теорема 1. *Пусть* $k'_{-1} \leqslant k'_1$, $k'_1 + k'_{-1} \in (0, 1/2)$. *Пусть* $k_{-1} \sim k'_{-1} n$, $k_1 \sim k'_1 n$, *и стало быть,* $k_0 \sim (1 - k'_{-1} - k'_1)n$ *при* $n \to \infty$. *Положим* $p' = k'_{-1} + k'_1 - (k'_1 - k'_{-1})^2$. *Пусть* x' *– меньший корень квадратного уравнения* $x(1 - p' + x) = (p' - 2x)^2$. *Тогда*

$$\chi(n, k_{-1}, k_0, k_1) \geqslant \left(\frac{(x')^{x'}(p' - 2x')^{p'-2x'}(1 - p' + x')^{1-p'+x'}}{(k'_{-1})^{k'_{-1}}(k'_1)^{k'_1}(1 - k'_1 - k'_{-1})^{1-k'_1-k'_{-1}}} + o(1)\right)^n.$$

В табл. 1 приведены значения оснований экспоненты из теоремы 1. В ней по вертикали отмечены значения k'_{-1}, а по горизонтали – значения k'_1. Видно, что во всех клетках числа больше единицы. Таким образом, в условиях теоремы 1 оценка всегда экспоненциальна. С другой стороны, максимум чисел в таблице (как показывает более детальный расчет) равен $2/\sqrt{3} = 1{,}154\ldots$, т.е. оценка в исходной проблеме Борсука остается прежней.

В следующем параграфе мы докажем теорему 1. Отметим, что смежные исследования, связанные с конструкциями на $(-1, 0, 1)$-векторах, можно найти в работах [14–31].

Таблица 1

	0,02	0,04	0,06	0,08	0,10	0,12	0,14	0,16	0,18	0,20	0,22	0,24
0,02	1,026											
0,06	1,044	1,060	1,072									
0,10	1,056	1,076	1,089	1,100	1,109							
0,14	1,068	1,088	1,103	1,113	1,122	1,129	1,135					
0,18	1,078	1,099	1,113	1,124	1,132	1,138	1,144	1,147	1,150			
0,20	1,083	1,104	1,118	1,128	1,136	1,142	1,147	1,150	1,152	1,154		
0,22	1,088	1,108	1,122	1,132	1,139	1,145	1,149	1,152	1,153	1,154	1,154	
0,24	1,092	1,112	1,125	1,135	1,142	1,147	1,150	1,152	1,153	1,154	1,153	1,151
0,26	1,096	1,116	1,128	1,137	1,143	1,148	1,151	1,152	1,153	1,152	1,151	
0,28	1,099	1,119	1,131	1,139	1,144	1,148	1,150	1,151	1,151	1,150		
0,30	1,103	1,121	1,133	1,140	1,145	1,148	1,149	1,149	1,148			
0,32	1,106	1,123	1,134	1,140	1,144	1,146	1,147	1,146				
0,36	1,110	1,126	1,134	1,139	1,141	1,141						
0,40	1,112	1,126	1,132	1,134								
0,44	1,113	1,123										

§ 2. Доказательство теоремы 1

2.1. Построение дистанционного графа. Прежде всего заметим, что максимальное скалярное произведение векторов из множества $V(n, k_{-1}, k_0, k_1)$ равно скалярному квадрату любого из них, т.е. величине $k_1 + k_{-1}$. Напротив, выбор параметров таков, что минимальное скалярное произведение равно $-2k_{-1}$. Пусть p – минимальное простое число, строго большее величины $k_1 + k_{-1} - (k_1 - k_{-1})^2/n$. Согласно известным результатам теории чисел (см. [32]) $p \sim p'n$ при $n \to \infty$. При этом

$$k_1 + k_{-1} - 2p < -2k_{-1}. \tag{2}$$

В самом деле, достаточно проверить, что $k_1 + k_{-1} - p < (k_1 - k_{-1})/2$, т.е. что

$$\frac{(k_1 - k_{-1})^2}{n} < \frac{k_1 - k_{-1}}{2} \iff k_1 - k_{-1} < \frac{n}{2},$$

а это мгновенно следует из условия теоремы.

Соединим ребром две вершины из $V(n, k_{-1}, k_0, k_1)$ тогда и только тогда, когда скалярное произведение соответствующих векторов равно $k_1 + k_{-1} - p$. Возникает дистанционный граф G в $\mathbb{R}^n$. Однако мы пока не знаем, принадлежит ли он множеству $\mathcal{G}(k_{-1}, k_0, k_1)$. Ниже мы докажем это, а также убедимся в том, что для хроматического числа графа G справедлива оценка, фигурирующая в теореме 1. На этом доказательство теоремы 1 будет завершено.

2.2. Принадлежность графа G множеству $\mathcal{G}(k_{-1}, k_0, k_1)$. Пусть λ – корень квадратного уравнения

$$\lambda^2 n - 2\lambda(k_1 - k_{-1}) + k_1 + k_{-1} - p = 0.$$

Он вещественный, поскольку положительность дискриминанта следует из условий, наложенных на величину p.

Пусть $\boldsymbol{x} = (x_1, \ldots, x_n) \in V(n, k_{-1}, k_0, k_1)$. Рассмотрим вектор

$$\boldsymbol{x}^* = \big((x_1 - \lambda)(x_1 - \lambda), (x_1 - \lambda)(x_2 - \lambda), \ldots, (x_1 - \lambda)(x_n - \lambda),$$
$$(x_2 - \lambda)(x_1 - \lambda), \ldots, (x_2 - \lambda)(x_n - \lambda), \ldots, (x_n - \lambda)(x_n - \lambda)\big).$$

Множество таких векторов обозначим через W. Оно лежит в подпространстве размерности $\dfrac{n(n+1)}{2}$ пространства $\mathbb{R}^{n^2}$. Таким образом, остается доказать, что граф диаметров этого множества изоморфен графу G.

Заметим, что

$$(\boldsymbol{x}^*, \boldsymbol{y}^*) = \sum_{i=1}^{n}\sum_{j=1}^{n}(x_i-\lambda)(x_j-\lambda)(y_i-\lambda)(y_j-\lambda) =$$

$$= \left(\sum_{i=1}^{n}(x_i-\lambda)(y_i-\lambda)\right)^2 = \big((\boldsymbol{x},\boldsymbol{y}) - 2\lambda(k_1-k_{-1}) + \lambda^2 n\big)^2.$$

Величина λ подобрана так, чтобы получившийся полный квадрат принимал минимальное по $(\boldsymbol{x},\boldsymbol{y})$ значение (равное нулю) тогда и только тогда, когда $(\boldsymbol{x},\boldsymbol{y}) = k_1 + k_{-1} - p$. Последнее равенство в точности соответствует образованию ребра между вершинами $\boldsymbol{x},\boldsymbol{y}$ графа G. А максимум расстояния между векторами из множества W достигается ровно тогда, когда их скалярное произведение минимально, ведь, как мы видим из формулы для их скалярного произведения, все их скалярные квадраты одинаковы. Следовательно, граф G изоморфен графу диаметров множества W, и эта часть доказательства завершена.

2.3. Оценка хроматического числа графа G. Хорошо известно, что $\chi(G) \geqslant \dfrac{|V|}{\alpha(G)}$, где $\alpha(G)$ – *число независимости* графа, равное максимальной мощности такого множества вершин графа, что никакие две вершины в нем не соединены ребром (сами такие множества называются *независимыми*). Легко видеть, что в нашем случае

$$|V| = C_n^{k_1}C_{n-k_1}^{k_{-1}} = \left(\frac{1}{(k'_{-1})^{k'_{-1}}(k'_1)^{k'_1}(1-k'_1-k'_{-1})^{1-k'_1-k'_{-1}}} + o(1)\right)^n.$$

Соответственно, неравенство в теореме 1 подсказывает, что верхняя оценка числа независимости должна иметь вид

$$\left(\frac{1}{(x')^{x'}(p'-2x')^{p'-2x'}(1-p'+x')^{1-p'+x'}} + o(1)\right)^n,$$

и нам остается обосновать это.

Рассмотрим произвольное независимое множество вершин нашего графа $W = \{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t\}$. Каждому вектору $\boldsymbol{x}_i$ сопоставим многочлен $P_{\boldsymbol{x}_i} \in \mathbb{Z}/p\mathbb{Z}[y_1,\ldots,y_n]$ (здесь p – простое число из формулировки теоремы), задаваемый в виде

$$P_{\boldsymbol{x}_i}(\boldsymbol{y}) = \prod_{j\in J}(j - (\boldsymbol{x}_i,\boldsymbol{y})), \quad \boldsymbol{y} = (y_1,\ldots,y_n),$$

$$J = \{0,1,\ldots,p-1\} \setminus \{k_1 + k_{-1} - p\}.$$

Преобразуем многочлены $P_{\boldsymbol{x}_i}$ следующим образом. Раскроем все скобки в определении и получим некоторую комбинацию одночленов. Степень каждого одночлена не превосходит $p-1$. Если одночлен имеет вид $y_{i_1}^{\alpha_{i_1}}\cdot\ldots\cdot y_{i_q}^{\alpha_{i_q}}$, где

$$q \leqslant p-1, \quad 1 \leqslant \alpha_{i_\nu} \leqslant p-1, \quad 1 \leqslant \nu \leqslant q, \quad \alpha_{i_1} + \ldots + \alpha_{i_q} \leqslant p-1,$$

то заменим в нем все четные α_{i_ν} на двойки, а все нечетные – на единицы. После приведения подобных слагаемых над $\mathbb{Z}/p\mathbb{Z}$ возникает новый многочлен $P'_{\boldsymbol{x}_i}$. Степень каждого такого многочлена по-прежнему не выше $p-1$. При этом все эти многочлены расположены в линейном пространстве, размерность которого не больше величины

$$\sum_{(i,j):\, i+2j\leqslant p-1} C_n^i C_{n-i}^j.$$

Здесь i – число переменных первой степени, а j – число переменных второй степени в мономах, образующих стандартный базис.

Если мы докажем, что многочлены $P'_{\boldsymbol{x}_1}, \ldots, P'_{\boldsymbol{x}_t}$ линейно независимы над $\mathbb{Z}/p\mathbb{Z}$, то мы установим оценку

$$\alpha(G) \leqslant \sum_{(i,j):\ i+2j\leqslant p-1} C_n^i C_{n-i}^j.$$

Предположим, что

$$c_1 P'_{\boldsymbol{x}_1} + \ldots + c_t P'_{\boldsymbol{x}_t} = 0.$$

Тогда для любого $\boldsymbol{y} \in W$ верно

$$c_1 P'_{\boldsymbol{x}_1}(\boldsymbol{y}) + \ldots + c_t P'_{\boldsymbol{x}_t}(\boldsymbol{y}) \equiv 0 \pmod p.$$

Более того, верно и

$$c_1 P_{\boldsymbol{x}_1}(\boldsymbol{y}) + \ldots + c_t P_{\boldsymbol{x}_t}(\boldsymbol{y}) \equiv 0 \pmod p.$$

Дело в том, что для $\boldsymbol{y} \in W$ все $y_i \in \{-1, 0, 1\}$, а на таких значениях переменных значения P и P' просто равны между собой.

Подставим вместо $\boldsymbol{y}$ вектор $\boldsymbol{x}_1$. Мы знаем, что $(\boldsymbol{x}_1, \boldsymbol{x}_1) = k_1 + k_{-1}$. Но в множестве J (см. определение многочлена P) нет вычета $k_1 + k_{-1}$. Значит, $P_{\boldsymbol{x}_1}(\boldsymbol{x}_1) \not\equiv 0 \pmod p$. С другой стороны, для любого другого $\boldsymbol{x}_i$ имеем

$$(\boldsymbol{x}_i, \boldsymbol{x}_1) < k_1 + k_{-1}, \quad (\boldsymbol{x}_i, \boldsymbol{x}_1) \neq k_1 + k_{-1} - p,$$
$$(\boldsymbol{x}_i, \boldsymbol{x}_1) \geqslant -2k_{-1}, \quad k_1 + k_{-1} - 2p < -2k_{-1},$$

где второе неравенство является следствием отсутствия ребер в независимом множестве W, четвертое неравенство – это полученный ранее факт (2), а все вместе говорит о том, что

$$(\boldsymbol{x}_i, \boldsymbol{x}_1) \not\equiv k_1 + k_{-1} - p \pmod p,$$

откуда $P_{\boldsymbol{x}_i}(\boldsymbol{x}_1) \equiv 0 \pmod p$. В итоге видим, что $c_1 \equiv 0 \pmod p$. Действуя аналогично, получаем, что все коэффициенты равны нулю по модулю p, так что многочлены и впрямь линейно независимы.

Для завершения доказательства остается проверить, что

$$\sum_{(i,j):\ i+2j\leqslant p-1} C_n^i C_{n-i}^j = \left(\frac{1}{(x')^{x'}(p'-2x')^{p'-2x'}(1-p'+x')^{1-p'+x'}} + o(1) \right)^n.$$

Это довольно рутинный анализ, и мы опускаем подробности. Во-первых, ясно, что запись $(c+o(1))^n$ при $c > 1$ не чувствительна к домножению и делению на субэкспоненциальные функции – тем более на многочлены. Поэтому достаточно найти c в записи максимального слагаемого в сумме. Разумеется, в этом слагаемом $i+2j = p-1$. Стало быть, мы ищем максимум выражения $C_n^i C_{n-i}^{p-1-2i}$. Отбрасывая субэкспоненциальные величины и вспоминая, что $p \sim p'n$, видим, что максимизирующее i можно искать среди $i \sim xn$, где $x \in (0,1)$ при $n \to \infty$. Тогда

$$C_n^i C_{n-i}^{p-1-2i} = \left(\frac{1}{x^x(p'-2x)^{p'-2x}(1-p'+x)^{1-p'+x}} + o(1) \right)^n.$$

Дифференцируя по x дробь, стоящую в скобках, находим необходимое условие экстремума как раз в виде квадратного уравнения из условия теоремы. Стандартными

выкладками проверяем, что это и есть точка максимума. Заменяем x на x', и теорема доказана. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Raigorodskii A.M.* Cliques and Cycles in Distance Graphs and Graphs of Diameters // Discrete Geometry and Algebraic Combinatorics (AMS Special Session on Discrete Geometry and Algebraic Combinatorics. San Diego, CA, USA. Jan. 11, 2013). Contemp. Math. V. 625. Providence, RI: Amer. Math. Soc., 2014. P. 93–109.
2. *Raigorodskii A.M.* Combinatorial Geometry and Coding Theory // Fund. Inform. 2016. V. 145. № 3. P. 359–369. https://doi.org/10.3233/FI-2016-1365
3. *Райгородский А.М.* Проблема Борсука и хроматические числа некоторых метрических пространств // УМН. 2001. Т. 56. № 1 (337). С. 107–146. https://doi.org/10.4213/rm358
4. *Райгородский А.М.* Вокруг гипотезы Борсука // Геометрия и механика. Современная математика. Фундаментальные направления. Т. 23. М: РУДН, 2007. С. 147–164. http://mi.mathnet.ru/cmfd96
5. *Bourgain J., Lindenstrauss J.* On Covering a Set in $\mathbb{R}^d$ by Balls of the Same Diameter // Geometric Aspects of Functional Analysis: Israel Seminar (GAFA) 1989–90. Lect. Notes Math. V. 1469. Berlin: Springer-Verlag, 1991. P. 138–144. https://doi.org/10.1007/BFb0089220
6. *Schramm O.* Illuminating Sets of Constant Width // Mathematika. 1988. V. 35. № 2. P. 180–189. https://doi.org/10.1112/S0025579300015175
7. *Боголюбский Л.И., Райгородский А.М.* Замечание о нижних оценках хроматических чисел пространств малой размерности с метриками ℓ_1 и ℓ_2 // Матем. заметки. 2019. V. 105. № 2. P. 187–213. https://doi.org/10.4213/mzm11736
8. *Райгородский А.М., Боголюбский Л.И.* Об оценках в проблеме Борсука // Тр. МФТИ. 2019. Т. 11. № 3. С. 20–49.
9. *Филимонов В.П.* О покрытии множеств в $\mathbb{R}^m$ // Матем. сб. 2014. Т. 205. № 8. С. 95–138. https://doi.org/10.4213/sm8316
10. *Райгородский А.М., Кошелев М.М.* Новые оценки клико-хроматических чисел графов Джонсона // Докл. РАН. 2020. Т. 490. № 1. С. 78–80. https://doi.org/10.31857/S268695432001018X
11. *Ипатов М.М., Кошелев М.М., Райгородский А.М.* Модулярность некоторых дистанционных графов // Докл. РАН. 2020. Т. 490. № 1. С. 71–73. https://doi.org/10.31857/S2686954320010142
12. *Raigorodskii A.M., Koshelev M.M.* New Bounds on Clique-Chromatic Numbers of Johnson Graphs // Discrete Appl. Math. 2020. V. 283. P. 724–729. https://doi.org/10.1016/j.dam.2020.01.015
13. *Пушняков Ф.А., Райгородский А.М.* Оценка числа ребер в особых подграфах некоторого дистанционного графа // Матем. заметки. 2020. Т. 107. № 2. С. 286–298. https://doi.org/10.4213/mzm12088
14. *Райгородский А.М., Харламова А.А.* О совокупностях $(-1, 0, 1)$-векторов с запретами на величины попарных скалярных произведений // Труды семинара по векторному и тензорному анализу. Т. 29. М.: Изд-во МГУ, 2013. С. 130–146.
15. *Frankl P., Kupavskii A.* Erdős–Ko–Rado Theorem for $\{0, \pm 1\}$-Vectors // J. Combin. Theory Ser. A. 2018. V. 155. P. 157–179. https://doi.org/10.1016/j.jcta.2017.11.003
16. *Frankl P., Kupavskii A.* Incompatible Intersection Properties // Combinatorica. 2019. V. 39. № 6. P. 1255–1266. https://doi.org/10.1007/s00493-019-4064-6
17. *Kupavskii A.* Degree Versions of Theorems on Intersecting Families via Stability // J. Combin. Theory Ser. A. 2019. V. 168. P. 272–287. https://doi.org/10.1016/j.jcta.2019.06.002
18. *Ihringer F., Kupavskii A.* Regular Intersecting Families // Discrete Appl. Math. 2019. V. 270. P. 142–152. https://doi.org/10.1016/j.dam.2019.07.009
19. *Бобу А.В., Куприянов А.Э., Райгородский А.М.* Об одном обобщении кнезеровских графов // Матем. заметки. 2020. Т. 107. № 3. С. 351–365. https://doi.org/10.4213/mzm12205

20. *Sagdeev A.A., Raigorodskii A.M.* On a Frankl–Wilson Theorem and Its Geometric Corollaries // Acta Math. Univ. Comenian. (N.S.). 2019. V. 88. № 3. P. 1029–1033.
21. *Райгородский А.М., Шишунов Е.Д.* О числах независимости некоторых дистанционных графов с вершинами в $\{-1, 0, 1\}^n$ // ДАН. 2019. V. 485. № 3. P. 269–271. https://doi.org/10.31857/S0869-56524853269-271
22. *Райгородский А.М., Шишунов Е.Д.* О числах независимости дистанционных графов с вершинами в $\{-1, 0, 1\}^n$ // ДАН. 2019. V. 488. № 5. P. 486–487. https://doi.org/10.31857/S0869-56524885486-487
23. *Соколов А.А., Райгородский А.М.* О рациональных аналогах проблем Нелсона – Хадвигера и Борсука // Чебышевский сб. 2018. Т. 19. № 3. С. 270–281. https://doi.org/10.22405/2226-8383-2018-19-3-270-281
24. *Райгородский А.М., Трухан Т.В.* О хроматических числах некоторых дистанционных графов // ДАН. 2018. Т. 482. № 6. С. 648–650. https://doi.org/10.31857/S086956520002950-8
25. *Cherkashin D., Kulikov A., Raigorodskii A.* On the Chromatic Numbers of Small-Dimensional Euclidean Spaces // Discrete Appl. Math. 2018. V. 243. P. 125–131. https://doi.org/10.1016/j.dam.2018.02.005
26. *Райгородский А.М., Сагдеев А.А.* Об одной оценке в экстремальной комбинаторике // ДАН. 2018. Т. 478. № 3. С. 271–273. https://doi.org/10.7868/S0869565218030040
27. *Сагдеев А.А.* Об одной теореме Франкла – Уилсона // Пробл. передачи информ. 2019. Т. 55. № 4. С. 86–106. https://doi.org/10.1134/S0555292319040041
28. *Cherkashin D., Kiselev S.* Independence Numbers of Johnson-type Graphs, arXiv:1907.06752 [math.CO], 2019.
29. *Захаров Д.А.* О хроматических числах некоторых дистанционных графов // Матем. заметки. 2020. Т. 107. № 2. С. 210–220. https://doi.org/10.4213/mzm11349
30. *Zakharov D.* Chromatic Numbers of Kneser-type Graphs // J. Combin. Theory Ser. A. 2020. V. 172. P. 105188 (16 pp.). https://doi.org/10.1016/j.jcta.2019.105188
31. *Просанов Р.И.* Контрпримеры к гипотезе Борсука, имеющие большой обхват // Матем. заметки. 2019. V. 105. № 6. P. 890–898. https://doi.org/10.4213/mzm12000
32. *Baker R.C., Harman G., Pintz J.* The Difference between Consecutive Primes. II // Proc. London Math. Soc. (3). 2001. V. 83. № 3. P. 532–562. https://doi.org/10.1112/plms/83.3.532

Бердников Алексей Викторович
Московский физико-технический институт
(государственный университет),
факультет инноваций и высоких технологий,
кафедра дискретной математики
alexey-berdnikov@yandex.ru
Райгородский Андрей Михайлович
Московский физико-технический институт
(государственный университет),
Физтех-школа прикладной математики и информатики и
лаборатория продвинутой комбинаторики и сетевых приложений
Московский государственный университет им. М.В. Ломоносова,
механико-математический факультет,
кафедра математической статистики и случайных процессов
Кавказский математический центр
Адыгейского государственного университета, Майкоп
Бурятский государственный университет,
институт математики и информатики, Улан-Удэ
mraigor@yandex.ru

Поступила в редакцию
14.07.2020
После доработки
06.11.2020
Принята к публикации
07.11.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 2**

УДК 621.391 : 519.178

© 2021 г. **М.Н. Вялый**[1]

ПОДСЧЕТ ЧИСЛА СОВЕРШЕННЫХ ПАРОСОЧЕТАНИЙ И ОБОБЩЕННЫЕ РАЗРЕШАЮЩИЕ ДЕРЕВЬЯ

Изучается обобщение подхода Пойа – Кастелейна к подсчету числа совершенных паросочетаний в графах, основанное на вычислении символического пфаффиана ориентированной матрицы смежности графа. Трудоемкость алгоритмов, основанных на таком подходе, связана со сложностью функции знака совершенного паросочетания в моделях обобщенных разрешающих деревьев. Получены нижние оценки сложности знака совершенного паросочетания через детерминированную коммуникационную сложность XOR-функции знака паросочетания. Эти оценки показывают ограничения метода символического пфаффиана как для общего случая, так и для случая разреженных графов.

Ключевые слова: совершенное паросочетание, пфаффиан, разрешающее дерево, коммуникационная сложность.

DOI: 10.31857/S0555292321020042

§ 1. Введение

Хорошо известно [1], что задача подсчета числа совершенных паросочетаний в графе алгоритмически трудна; более точно, она является полной в классе $\#\mathbf{P}$.

Самый быстрый из известных на данный момент алгоритмов подсчета числа совершенных паросочетаний работает за время $O^*(2^{n/2})$, где n – число вершин в графе, $O^*(\cdot)$ обозначает асимптотическую оценку с точностью до полиномиального по n множителя [2].

Известно также [3], что в предположении одного из вариантов сильной гипотезы экспоненциального времени не существует алгоритмов подсчета числа совершенных паросочетаний, работающих за время $O^*(2^{o(n)})$.

Большое количество работ посвящено решению задачи подсчета числа совершенных паросочетаний для некоторых классов графов. Известны полиномиальные алгоритмы решения этой задачи для планарных графов, а также для графов ограниченного рода [4–6], графов, не содержащих минора $K_{3,3}$ [7], графов, не содержащих минора K_5 [8]. Для разреженных двудольных графов, в которых количество ребер не более чем в Δ раз превосходит количество вершин, известен алгоритм с временем работы $O^*(2^{(1-1/(5\Delta\log\Delta))n/2})$ [9].

Многие из этих алгоритмов используют предложенные Кастелейном в [4] пфаффовы ориентации графов. Судя по литературе, первым эту идею высказал Пойа [10] применительно к двудольным графам (точнее, к $(0,1)$-матрицам, которые естественным образом задают двудольный граф). Основанные на этой идее алгоритмы сводят подсчет числа совершенных паросочетаний в графе к вычислению детерминанта

[1] Работа выполнена за счет гранта Российского научного фонда (проект № 20-11-20203).

(для двудольных графов) или пфаффиана (в общем случае) ориентированной матрицы смежности графа.

Естественным обобщением идеи Пойа – Кастелейна является использование символических детерминантов и пфаффианов вместо простого присваивания знаков. Под символическим детерминантом (пфаффианом) мы понимаем детерминант (пфаффиан) матрицы, элементы которой принадлежат некоторому кольцу многочленов от вспомогательных переменных. Подсчет числа совершенных паросочетаний в графе сводится к арифметическим операциям с коэффициентами многочленов от вспомогательных переменных.

В работах [11,12] исследовались возможности такого подхода для подсчета числа совершенных паросочетаний в двудольных графах. Для некоторого варианта реализации такого метода в [11] были доказаны нижние оценки времени работы вида $2^{\Omega(n)}$. В [12] эти оценки усилены до оптимальных (с точностью до мультипликативной константы) нижних оценок вида $2^{\Omega(n \log n)}$, а также получены нижние оценки для разреженных двудольных графов вида $2^{\Omega(n)}$.

В настоящей статье мы обобщаем проделанный в [11,12] анализ на случай общих графов. Предлагается вариант метода символического пфаффиана (см. § 3), сложность которого зависит от представления булевой функции знака паросочетания (см. определение (6) в § 4) разрешающим деревом в базисе целочисленных линейных функций. Модель обобщенных разрешающих деревьев подробно описана в § 4. Имея разрешающее дерево T в базисе целочисленных линейных функций, которое вычисляет функцию знака паросочетания для графа G, можно найти количество совершенных паросочетаний в графе G за время $\mathrm{poly}((nL(T))^{h(T)})$, где n – количество вершин в графе, $L(T)$ – максимум модулей коэффициентов линейных функций дерева, $h(T)$ – высота дерева (теорема 1). В частности, при $L = \mathrm{poly}(n)$ и $h = O(1)$ время вычисления ограничено полиномом от n. Это обобщает известные результаты [4, 6].

Получены также нижние оценки для сложности функции знака паросочетания в моделях обобщенных разрешающих деревьев для полного графа K_{2n} (§ 4, теорема 2). Эти оценки имеют вид $\Omega(n \log n)$ и показывают, что предложенный подход неэффективен в случае произвольных графов. Линейные нижние оценки $\Omega(n)$ получены для связных графов на n вершинах, степень каждой вершины равна 3 (§ 7, теорема 3), что показывает неэффективность данного подхода и для произвольных графов ограниченной степени.

Остается открытым вопрос об описании тех классов графов, для которых метод символического пфаффиана дает эффективные алгоритмы.

Основным техническим приемом для построения нижних оценок является анализ коммуникационной сложности XOR-функции знака паросочетания (см. определения в § 5).

Полученные нижние оценки представляют самостоятельный интерес с точки зрения теории сложности булевых функций. Они также показывают, что знаки паросочетаний полного графа в некотором смысле распределены очень равномерно. Этот комбинаторный факт может оказаться полезным в других вопросах теории алгоритмов и теории сложности.

§ 2. Детерминант, перманент, пфаффиан и хафниан

Напомним определения основных многочленов, которые будут использоваться далее, и зафиксируем обозначения.

Пусть x_{ij}, $1 \leqslant i, j \leqslant n$, – набор из n^2 переменных. Их естественно представлять как элементы матрицы переменных X порядка n.

Перманент и детерминант – это два многочлена от таких переменных, которые задаются очень похожими формулами в разложении на мономы:

$$\operatorname{per} X = \sum_{\pi \in S_n} \prod_{i=1}^{n} x_{i\pi(i)}, \tag{1}$$
$$\det X = \sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} x_{i\pi(i)},$$

здесь S_n – группа всех перестановок, $\operatorname{sign}(\pi)$ – знак перестановки π.

Однако сложность этих многочленов резко различается. Детерминант вычислим эффективно. Существуют алгоритмы вычисления детерминанта матрицы с элементами из любого коммутативного кольца, которые требуют выполнения лишь полиномиального количества арифметических операций в кольце [13] (в частности, эти алгоритмы не используют операцию деления).

С другой стороны, вычисление перманента $(0,1)$-матрицы является #**P**-полной задачей [1].

Перманент $(0,1)$-матрицы имеет простую комбинаторную интерпретацию. По двудольному графу G построим $(0,1)$-матрицу B_G, строки которой соответствуют вершинам одной доли, а столбцы – другой. На пересечении i-й строки и j-го столбца стоит 1 тогда и только тогда, когда в G есть ребро из вершины i в вершину j. Это соответствие взаимно однозначно: для любой $(0,1)$-матрицы X существует такой граф G, что $X = B_G$. Из определения перманента (1) сразу видно, что $\operatorname{per} B_G$ равен количеству совершенных паросочетаний в графе G.

В случае произвольной матрицы значение перманента будем понимать как сумму весов совершенных паросочетаний во взвешенном двудольном графе, считая вес паросочетания равным произведению весов входящих в него ребер.

Паросочетаниям в произвольных графах отвечают значения другого многочлена – хафниана – на $(0,1)$-матрицах. Хафниан для симметрической матрицы переменных размера $2n \times 2n$ (т.е. $x_{ij} = x_{ji}$ для всех i, j) определяется так:

$$\operatorname{Hf} X = \sum_{\mathfrak{m} \in \mathcal{M}_{2n}} \prod_{\{i,j\} \in \mathfrak{m}}^{n} x_{ij}. \tag{2}$$

Здесь $\mathcal{M}_{2n}$ – это множество разбиений множества $\{1, 2, \ldots, 2n\}$ на n неупорядоченных пар (и разбиение, и пары неупорядоченные). Другими словами, $\mathcal{M}_{2n}$ – это множество совершенных паросочетаний в полном графе K_{2n}.

Обозначим через X_G симметрическую матрицу с элементами из множества переменных x_e, $e \in E(G)$, и 0, такую что $(X_G)_{i,j} = x_e$, если $e = \{i, j\}$, и $(X_G)_{i,j} = 0$, если $\{i, j\} \notin E(G)$. Через A_G будем обозначать матрицу смежности графа G. Она получается из X_G подстановками $x_e = 1$.

Из (2) видно, что $\operatorname{Hf} A_G$ равен количеству совершенных паросочетаний в графе G. Как и в случае двудольных графов, значение $\operatorname{Hf} X_G$ равно сумме весов совершенных паросочетаний в графе G.

Между перманентом и хафнианом есть простое соотношение (см. [2])

$$\operatorname{per} X = \operatorname{Hf} Y, \quad \text{где } Y = \begin{pmatrix} 0 & X \\ X^T & 0 \end{pmatrix}.$$

Поэтому вычисление хафниана $(0,1)$-матрицы также является #**P**-полной задачей.

Как и у перманента, у хафниана есть эффективно вычислимый компаньон – пфаффиан. Пфаффиан определяется для кососимметрических матриц. В кососимметрической матрице порядка $2n$ выделим *ориентацию* $\varepsilon_{ij} \in \{+1, -1\}$, $\varepsilon_{ij} = -\varepsilon_{ji}$, и симметрическую часть $x_{ij} = x_{ji}$. Ориентация задает направление на ребрах полного графа: если $\varepsilon_{ij} = +1$, то у ребра $\{i, j\}$ считаем началом вершину i, а концом – вершину j. Поэтому паросочетанию $\mathfrak{m}$ отвечает *ориентированное паросочетание* – ориентированный граф $\mathfrak{m}^\varepsilon$ с множеством ребер

$$\{(i_s j_s) : \{i_s j_s\} \in \mathfrak{m},\ \varepsilon_{i_s j_s} = +1\}.$$

Нетрудно видеть, что перестановки S_n, сохраняющие ориентированное паросочетание $\mathfrak{m}^\varepsilon$, четные. Поэтому все ориентированные паросочетания разбиваются на два класса: внутри каждого класса ориентированные паросочетания переводятся друг в друга четными перестановками, а между классами – нечетными.

Присвоив знак $+1$ какому-нибудь ориентированному паросочетанию $\mathfrak{m}_0^{\varepsilon_0}$, определим знаки остальных паросочетаний по правилу: $\operatorname{sign}(\mathfrak{m}^\varepsilon) = +1$, если $\mathfrak{m}^\varepsilon$ лежит в том же классе, что и $\mathfrak{m}_0^{\varepsilon_0}$, а в противном случае $\operatorname{sign}(\mathfrak{m}^\varepsilon) = -1$. Обычно в определении пфаффиана выбирается паросочетание

$$\{(1, 2), (3, 4), \ldots, (2n-1, 2n)\},$$

но выбор другого $\mathfrak{m}_0^{\varepsilon_0}$ разве что изменит знаки всех паросочетаний одновременно.

В этих терминах пфаффиан матрицы $\varepsilon \bullet X = (\varepsilon_{ij} x_{ij})$ равен

$$\operatorname{Pf}(\varepsilon \bullet X) = \sum_{\mathfrak{m} \in \mathcal{M}_{2n}} \operatorname{sign}(\mathfrak{m}^\varepsilon) \prod_{\{i,j\} \in \mathfrak{m}} x_{ij}.$$

Здесь и далее мы обозначаем через $\bullet$ покомпонентное умножение матриц (произведение Адамара, или произведение Шура [14]).

Пфаффиан выражается через детерминант (см., например, [15]):

$$\det X = (\operatorname{Pf} X)^2. \tag{3}$$

Аналогично детерминанту, для вычисления пфаффиана матрицы с элементами из любого коммутативного кольца также существуют алгоритмы, которые требуют выполнения лишь полиномиального количества арифметических операций (сложения, вычитания и умножения) в кольце [16].

Нетрудно проверить следующие свойства знаков ориентированных паросочетаний.

Во-первых, $\operatorname{sign}(\mathfrak{m}^{\varepsilon'}) = \operatorname{sign}(\mathfrak{m}^{\varepsilon''})$, если и только если четное количество ребер $\mathfrak{m}$ имеет разную ориентацию в ε' и ε''.

Во-вторых, $\operatorname{sign}(\mathfrak{m}_1^\varepsilon) \operatorname{sign}(\mathfrak{m}_2^\varepsilon)$ совпадает с произведением *знаков циклов*, на которые разбивается симметрическая разность $\mathfrak{m}_1 \oplus \mathfrak{m}_2$ (все эти циклы имеют четную длину). Знак цикла равен $(-1)^{1+b}$, где b – количество ребер на цикле, ε-ориентированных против направления обхода цикла (выбор направления обхода неважен для цикла четной длины).

Пример 1. Занумеруем вершины графа числами от 1 до $2n$ и ориентируем ребро (i, j) от вершины с меньшим номером к вершине с бóльшим номером.

Будем считать положительным знак паросочетания

$$\{(1, 2), (3, 4), \ldots, (2n-1, 2n)\}.$$

Используя знаки циклов, нетрудно проверить, что знак паросочетания $\mathfrak{m}$ определяется четностью количества пересекающихся пар ребер [6]. По определению ребра $\{a, b\}$, $\{c, d\}$ пересекаются, если $a < c < b < d$.

§ 3. Метод символического пфаффиана

Граф G называется *пфаффовым*, если для некоторой ориентации ε знаки всех ориентированных совершенных паросочетаний $\mathfrak{m}^\varepsilon$ графа G одинаковы. Такая ориентация называется *пфаффовой*.

Для графа G с пфаффовой ориентацией ε выполняется равенство

$$\operatorname{Hf} X_G = |\operatorname{Pf}(\varepsilon \bullet X_G)|.$$

Поэтому хафниан $\operatorname{Hf} X_G$ и, в частности, количество совершенных паросочетаний $\operatorname{Hf} A_G$ в пфаффовом графе с заданной пфаффовой ориентацией вычисляется за полиномиальное время.

Для простоты мы ограничиваемся подсчетом количества совершенных паросочетаний в графе, т.е. вычислением $\operatorname{Hf} A_G$. Заметим, что все последующие рассуждения без труда переносятся на задачу подсчета значения хафниана $\operatorname{Hf} X_G$ при заданных значениях переменных x_e.

Примером пфаффовых графов являются планарные графы. Доказательство существования пфаффовых ориентаций для планарных графов и эффективный алгоритм их построения были предложены Кастелейном [4]. До сих пор не известны ни структурный критерий пфаффовости графов, ни полиномиальный алгоритм проверки пфаффовости. Отметим, что для двудольных графов известны как структурная характеризация (теорема Литтла – см. [17] или альтернативное доказательство в [18]), так и полиномиальный алгоритм проверки пфаффовости двудольного графа [19].

Мы рассматриваем обобщение этого подхода. А именно, вместо задающих ориентацию знаков будем домножать элементы матрицы X_G на мономы из алгебры $\mathcal{R}_h = \mathbb{R}[t_0, \dots, t_{h-1}]$ многочленов от h вспомогательных переменных[2]. Зафиксируем некоторую ориентацию ребер ε^0 и для краткости знаки паросочетаний относительно этой ориентации обозначаем просто через $\operatorname{sign}(\mathfrak{m})$. Через τ обозначим матрицу с многочленами (мономами) из алгебры $\mathcal{R}_h$ (матрица "обобщенных знаков"). Пфаффиан матрицы $A_{\tau,G} = \varepsilon^0 \bullet \tau \bullet A_G$ является многочленом от переменных t_i. Обозначим множество совершенных паросочетаний в графе G через $\mathcal{M}(G)$. Тогда

$$\operatorname{Pf} A_{\tau,G} = \sum_{\mathfrak{m}\in\mathcal{M}(G)} \operatorname{sign}(\mathfrak{m}) \prod_{\{i,j\}\in\mathfrak{m}}^{n} \tau_{ij}(t_1, \dots, t_h) \stackrel{\text{def}}{=} \sum_{\mathfrak{m}\in\mathcal{M}(G)} \operatorname{sign}(\mathfrak{m})\tau(\mathfrak{m}). \tag{4}$$

Суть метода символического пфаффиана состоит в том, чтобы подсчитать количество совершенных паросочетаний, исходя из многочленов вида $\operatorname{Pf} A_{\tau,G}$ (возможно использование нескольких матриц τ). Основная идея состоит в том, чтобы мономы $\tau(\mathfrak{m})$ разделяли знаки паросочетаний из $\mathcal{M}(G)$: если $\operatorname{sign}(\mathfrak{m}_1) \neq \operatorname{sign}(\mathfrak{m}_2)$, то $\tau(\mathfrak{m}_1) \neq \tau(\mathfrak{m}_2)$. В таком случае количество совершенных паросочетаний равно сумме модулей коэффициентов $\operatorname{Pf} A_{\tau,G}$. В следующем § 4 мы опишем более сложный вариант этого метода, в котором используются мономы из многочленов $\operatorname{Pf} A_{\tau,G}$ с разными τ.

Для пфаффовых графов метод символического пфаффиана применим в этом, самом простом, виде. Пусть ε – пфаффова ориентация. Сопоставим ей матрицу τ, где $\tau_{ij} = t$, если $\varepsilon_{ij} = -\varepsilon^0_{ij}$, и $\tau_{ij} = 1$, если $\varepsilon_{ij} = \varepsilon^0_{ij}$. Как уже отмечалось выше, $\operatorname{sign}(\mathfrak{m}^\varepsilon) = \operatorname{sign}(\mathfrak{m}^{\varepsilon^0})$, если и только если четное количество ребер $\mathfrak{m}$ имеет разную ориентацию в ε и ε^0. Это означает, что $\tau(\mathfrak{m}) = t^{2k}$, если $\operatorname{sign}(\mathfrak{m}^\varepsilon) = \operatorname{sign}(\mathfrak{m}^{\varepsilon^0})$, и $\tau(\mathfrak{m}) =$

[2] Конечно, в качестве множителей можно использовать произвольные многочлены. Однако пока не видно способов применить эту более общую конструкцию. Поэтому здесь мы ограничиваемся мономами.

$= t^{2k+1}$, если $\operatorname{sign}(\mathfrak{m}^{\varepsilon}) = -\operatorname{sign}(\mathfrak{m}^{\varepsilon^0})$. Поэтому в (4) знаки всех мономов четной степени одинаковы, как и знаки всех мономов нечетной степени.

Уже Кастелейн отмечал, что хафниан матрицы X_G для графа ограниченного рода g выражается как сумма 4^g пфаффианов. Первое математическое доказательство для случая ориентированного рода появилось, по всей видимости, в работе [5]. Несколько позже Теслер [6] предложил другое доказательство этого факта и доказал аналогичное утверждение для неориентированного рода. В терминах метода символического детерминанта он доказал, что для графов ограниченного рода g существует подходящая матрица мономов τ от $2g$ переменных, которая разделяет знаки паросочетаний. В случае ориентированного рода достаточно учитывать только четность степеней переменных в мономах $\tau(\mathfrak{m})$, в случае неориентированного рода требуется учитывать степени переменных по модулю 4.

Обсудим вычислительную сложность метода символического пфаффиана. Помимо порядка матрицы n, она зависит от количества вспомогательных переменных h, максимума показателей степеней в мономах матрицы τ, который будем обозначать через L, и количества вычислений символических пфаффианов N (в общем случае будет вычисляться несколько пфаффианов). Сложность конкретной реализации метода мы будем измерять величиной $N(nL)^h$ по следующим соображениям.

Алгоритм вычисления пфаффиана [16] выполняет $\Theta(n^4)$ арифметических действий с элементами кольца, где n – порядок матрицы. Алгебраические схемы вычисления пфаффиана из работы [16] устроены так, что все промежуточные результаты вычисления являются суммами произведений матричных элементов с коэффициентами ± 1. Все мономы, возникающие в этих вычислениях, являются произведениями мономов матрицы τ. Поэтому при вычислении пфаффиана матрицы мономов в промежуточных вычислениях и окончательном ответе возникают многочлены, степени мономов в которых ограничены величиной n^2L, а коэффициенты ограничены по модулю 2^{n^2}. Общее количество таких мономов от h вспомогательных переменных равно $(n^2L)^h$. Поэтому время выполнения арифметических операций на таких многочленах составляет $\operatorname{poly}((n^2L)^h)$. Общее время вычисления оказывается ограниченным полиномом от выбранной меры сложности $N(nL)^h$.

В частности, при $L = \operatorname{poly}(n)$ и $h = O(1)$ время вычисления символического пфаффиана ограничено полиномом от n.

Отметим, что верхняя оценка числа мономов может быть улучшена в некоторых случаях. Например, если использовать не алгебру многочленов, а ее факторалгебру $\mathcal{A}_{h,d} = \mathbb{R}[t_1, \ldots, t_{2g}]/(t_i^d - 1 : \ 1 \leqslant i \leqslant h)$, количество мономов будет оцениваться сверху как d^h после приведения монома к стандартному виду. Скажем, для графов ограниченного рода g достаточно проводить вычисления в алгебрах $\mathcal{A}_{2g,2}$ (случай ориентированного рода) и $\mathcal{A}_{2g,4}$ (случай неориентированного рода).

Заметим, что случай алгебры $\mathcal{A}_h = \mathcal{A}_{h,2}$ особенно важен при анализе возможностей метода символического пфаффиана (см. обсуждение в § 5 и лемму 3 там же).

Для вариантов метода символического пфаффиана, использующих алгебры $\mathcal{A}_{h,d}$, более естественной мерой сложности является Nnd^h.

Отметим, что используемая мера сложности не дает абсолютных нижних оценок времени работы. В принципе возможна такая реализация метода, в которой количество мономов в промежуточных многочленах гораздо меньше $(n^2L)^h$. Однако в настоящее время неизвестны способы существенного сокращения количества мономов, и сомнительно, что они вообще существуют.

§ 4. Разрешающие деревья

В этом параграфе мы опишем самую общую известную на данный момент форму метода символического пфаффиана и свяжем анализ возможностей этого метода

с задачами вычисления булевых функций в модели обобщенных разрешающих деревьев.

В стандартной модели разрешающих деревьев вычисление булевой функции происходит в результате последовательности запросов переменных, а сложность вычисления зависит лишь от количества запросов (подробнее см., например, в [20]).

В обобщенной модели возможны запросы не только переменных, но и произвольных функций от булевых переменных из некоторого множества функций B. По аналогии со схемной сложностью это множество будем называть *базисом*.

Разрешающее дерево в базисе B – это корневое дерево. Каждой внутренней вершине v (не листу) разрешающего дерева приписана некоторая функция $l_v(x) \in B$. Потомков вершины столько, сколько значений может принимать функция $l_v(x)$. Каждому потомку присвоено одно из возможных значений этой функции. В листьях дерева дополнительно записаны *результаты* вычисления: значения 0 или 1.

Разрешающее дерево в базисе B вычисляет булеву функцию $f\colon \{0,1\}^n \to \{0,1\}$ по такому правилу. Аргумент x функции f определяет последовательность вершин, которая начинается в корне и заканчивается в листе. Следующим после вершины v является тот ее потомок, которому присвоено значение $l_v(x)$. Результат в листе, на котором заканчивается эта последовательность, и есть $f(x)$.

Разрешающее дерево по определению вычисляет всюду определенную функцию. Далее потребуются частичные функции. Будем считать, что разрешающее дерево вычисляет частичную функцию, если оно вычисляет некоторое всюду определенное продолжение этой функции.

Сложность булевой функции в модели разрешающих деревьев в базисе B – это минимум величины $h(T)\lceil\log_2 b(T)\rceil$ по всем разрешающим деревьям в базисе B, вычисляющим функцию f. Здесь $h(T)$ – высота дерева, а $b(T)$ – максимальное ветвление (количество потомков у одной вершины)[3]. Будем обозначать сложность функции f в модели разрешающих деревьев в базисе B через $\mathbf{D}_B(f)$.

Стандартная модель разрешающих деревьев отвечает базису, состоящему из функций-проекций $(x_1,\ldots,x_n) \mapsto x_i$. Сложность булевой функции в таком базисе обозначаем через $\mathbf{D}(f)$. В этом случае значения функций принадлежат множеству $\{0,1\}$ и разрешающие деревья являются бинарными деревьями, а сложность f совпадает с минимальной высотой разрешающего дерева, которое вычисляет f.

Разрешающие деревья с линейными запросами (или линейные разрешающие деревья – parity decision trees) отвечают базису линейных булевых функций $(x_1,\ldots,x_n) \mapsto x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_k}$ ($\oplus$ обозначает сложение по модулю 2). Сложность булевой функции в базисе линейных разрешающих деревьев обозначается через $\mathbf{D}_{\oplus}(f)$. В этом случае множество значений функций также $\{0,1\}$, и линейное разрешающее дерево – бинарное.

Отметим одно существенное различие между сложностью (частичной) функции в стандартной модели разрешающих деревьев и в модели линейных разрешающих деревьев.

Очевидной верхней оценкой сложности $\mathbf{D}(f)$ является количество переменных (при известных значениях всех аргументов значение функции однозначно определено). Для сложности в стандартной модели разрешающих деревьев известны примеры тотальных функций от n переменных сложности ровно n. Например, такой функцией является дизъюнкция переменных. Применением метода противника (adversary method) [20] нетрудно проверить, что также равна n сложность частичной функции, которая определена на $n+1$ наборе значений аргументов $(0,\ldots,0)$, $(1,0,\ldots,0)$, $(0,1,0,\ldots,0)$, $\ldots$, $(0,0,\ldots,0,1)$ и совпадает с дизъюнкцией на области

[3] Неформально смысл логарифмического множителя в том, чтобы свести общую модель к модели с запросами, допускающими бинарный ответ.

определения. Стратегия противника остается той же самой, что и для обычной (всюду определенной) дизъюнкции.

Для сложности в модели линейных разрешающих деревьев такой пример невозможен. Через $\mathrm{Dom}\, f$ обозначаем область определения f.

Лемма 1. $\mathbf{D}_{\oplus}(f) = O(\log|\mathrm{Dom}\, f|)$ *для любой функции* f.

Доказательство. Докажем, что для любого множества $D \subseteq \mathbb{F}_2^n$ существуют $k = O(\log|D|)$ линейных функционалов (линейных однородных функций) $s_1, \ldots, s_k$ на $\mathbb{F}_2^n$, разделяющих точки D. Это означает, что для любой пары $x \in D$, $y \in D$, $x \neq y$, существует такое i, что $s_i(x) \neq s_i(y)$.

Для двух различных точек $x \neq y$ есть ровно 2^{n-1} линейных функционалов, которые не разделяют x, y (т.е. равны 0 на $x \oplus y$, здесь $\oplus$ обозначает покомпонентное сложение векторов). Поэтому k случайных линейных функционалов, выбранных независимо, не различают эту пару с вероятностью 2^{-k}. Всего есть $|D|(|D|-1)/2$ пар точек из D. Поэтому при $2^{-k}|D|(|D|-1)/2 < 1$ найдутся k функционалов, которые разделяют все пары (оценка объединения). Это условие выполняется для некоторого $k = O(\log|D|)$.

Имея набор из $k = O(\log|\mathrm{Dom}\, f|)$ линейных функционалов, разделяющих точки из $\mathrm{Dom}\, f$, легко построить разрешающее дерево, которое вычисляет f. Это полное бинарное дерево высоты k. На уровне i этого дерева вычисляется функционал s_i (запросы неадаптивные, не зависят от ответов). В каждом листе, отвечающем (ровно одной) точке из $\mathrm{Dom}\, f$, записываем значение функции, в остальных листах пишем произвольный результат вычисления. ▲

Обобщая, можно рассмотреть базис S, состоящий из всех симметрических функций от некоторого подмножества переменных. В этот базис входят не только линейные функции, но функции сложения по произвольному модулю q, а также функции голосования. Сложность булевой функции в таком базисе обозначаем через $\mathbf{D}_S(f)$.

Из определений очевидны неравенства

$$\mathbf{D}_S(f) \leqslant \mathbf{D}_{\oplus}(f) \leqslant \mathbf{D}(f).$$

Для метода символического пфаффиана важен базис целочисленных линейных функций. В целочисленном разрешающем дереве вершинам приписаны линейные функционалы $\ell_v(x_1, \ldots, x_n)$ с целыми неотрицательными коэффициентами. Значения таких функционалов лежат на отрезке $[0, nL]$, где L – максимум коэффициентов линейных функционалов в разрешающем дереве. Сложность булевой функции f в этом базисе обозначаем через $\mathbf{D}_{\mathbb{Z}}(f)$.

Предложение 1. $\mathbf{D}_{\mathbb{Z}}(f) \leqslant \mathbf{D}_S(f)\lceil\log_2(n+1)\rceil$ *для любой булевой функции* f *от* n *переменных.*

Доказательство. Значение симметрической булевой функции зависит только от количества единиц среди ее аргументов $y_1, \ldots, y_k$, т.е. от значения линейной функции $y_1 + \ldots + y_k$.

По дереву T в базисе симметрических булевых функций построим дерево $z(T)$ в базисе целочисленных линейных функций по следующему правилу.

Если T имеет высоту 0, то корень является листом. Дерево $z(T)$ в таком случае также имеет высоту 0 и в его корне записан тот же результат, что и в корне дерева T.

Если T имеет высоту > 0 и в корне вычисляется симметрическая функция $s(y)$ от k переменных $y_1, \ldots, y_k$, то дерево $z(T)$ имеет ветвление $k+1$ в корне. Корню дерева $z(T)$ присваивается функция $y_1 + \ldots + y_k$, а потомок корня, которому присвоено значение j, является корнем дерева $z(T_\alpha)$, где $\alpha = s(z)$, а в z ровно j единиц.

Индукцией по построению дерева доказывается, что оба дерева вычисляют одну и ту же функцию.

Высота деревьев T и $z(T)$ одинакова, а максимальное ветвление дерева $z(T)$ не превосходит $n+1$. ▲

Для сложности разрешающих деревьев в базисе целочисленных функций выполняется аналог леммы 1.

Лемма 2. *Для любой функции f справедлива оценка $\mathbf{D}_{\mathbb{Z}}(f) = O(\log|\mathrm{Dom}\, f|)$.*

Доказательство. Рассуждение повторяет доказательство леммы 1. Но теперь разделяем точки целочисленными функционалами.

Для применения вероятностной оценки оценим количество целочисленных функционалов с коэффициентами в отрезке $[1, L]$, которые не различают некоторый фиксированный вектор $x - y \in \{\pm 1, 0\}^n$. Выберем первые $n-1$ коэффициентов произвольно. Тогда из условия неразличения получаем линейное уравнение на последний коэффициент (не все решения таких уравнений годятся, они могут лежать вне $[1, L]$; нам достаточно верхней оценки). Поэтому неразличающих функционалов не более чем L^{n-1}, их доля среди всех линейных функционалов с коэффициентами из отрезка $[1, L]$ не более L^{-1}.

Аналогично доказательству леммы 1 при выполнении неравенства

$$L^{-k} D(D-1)/2 < 1$$

k линейных функционалов, выбранных случайно и независимо, разделяют множество из D точек с положительной вероятностью. Поэтому для существования k разделяющих линейных функционалов, коэффициенты которых лежат в отрезке $[1, L]$, достаточно выполнения условия

$$k \log L > 2 \log D. \tag{5}$$

Выберем $L = n$. Тогда ветвление разрешающего дерева, неадаптивно вычисляющего k разделяющих функционалов, равно $b = nL = L^2$. Выбирая как можно меньшее k, при котором выполняется (5), получаем верхнюю оценку на сложность разрешающего дерева $k \log b = 2k \log L = O(\log|\mathrm{Dom}\, f|)$. ▲

Нас будет интересовать вычисление знака паросочетания в модели разрешающих деревьев. Для определения этой (частичной) булевой функции перейдем от ориентаций ребер к булевым переменным. Рассмотрим координатное векторное пространство $\mathbb{F}_2^{\binom{2n}{2}}$, индексированное парами $\{i, j\}$, $i \neq j$, $1 \leqslant i, j \leqslant 2n$, т.е. ребрами полного графа на $2n$ вершинах (вершины перенумерованы числами от 1 до $2n$). Графам на этом множестве вершин, в том числе и паросочетаниям, сопоставляются векторы пространства $\mathbb{F}_2^{\binom{n}{2}}$. Через $\mathbb{F}_2^{E(G)}$ будем обозначать координатное подпространство, натянутое на базисные векторы, отвечающие ребрам графа G. Зафиксируем некоторую ориентацию ребер полного графа ε_0 (скажем, выбранную в примере 1), знак паросочетания $\mathfrak{m}$ относительно этой ориентации обозначаем через $\mathrm{sign}(\mathfrak{m})$.

Для каждого графа G определим частичную функцию знака паросочетаний этого графа $\mathrm{sign}_G\colon \mathbb{F}_2^{E(G)} \to \{0, 1\}$ как

$$\mathrm{sign}_G(X) = \begin{cases} 0, & \text{если } X = \mathfrak{m} \in \mathcal{M}(G) \text{ и } \mathrm{sign}(\mathfrak{m}) = 1, \\ 1, & \text{если } X = \mathfrak{m} \in \mathcal{M}(G) \text{ и } \mathrm{sign}(\mathfrak{m}) = -1, \\ \text{не определена} & \text{в противном случае.} \end{cases} \tag{6}$$

Пример 2. Для цикла четной длины C_{2k} область определения функции $\mathrm{sign}_{C_{2k}}$ состоит из двух векторов, отвечающих двум совершенным паросочетаниям, на которые разбивается цикл. Хотя граф C_{2n} пфаффовый, функция $\mathrm{sign}_{C_{2k}}$ не обязательно постоянна на области определения, это зависит от выбора ориентации ε_0.

Однако для любого пфаффова графа эта функция линейна на области определения (поскольку знак паросочетания $\mathfrak{m}$ относительно пфаффовой ориентации отличается от знака относительно ориентации ε_0 на четность количества ребер в $\mathfrak{m}$, различно ориентированных в этих ориентациях).

Теорема 1. *Пусть дано разрешающее дерево T в базисе целочисленных линейных функций, вычисляющее функцию sign_G графа G на n вершинах. Количество листьев в этом дереве обозначим через $s(T)$, высоту – через $h(T)$, максимум коэффициентов в линейных функциях разрешающего дерева T – через $L(T)$. Тогда количество совершенных паросочетаний в графе G вычисляется за время $\operatorname{poly}(n)$ по результатам вычисления $s(T)$ символических пфаффианов, мономы в матрицах которых зависят от $h(T)$ вспомогательных переменных, а степени переменных в мономах ограничены величиной $L(T)$. В частности, общее время вычисления составляет $\operatorname{poly}((n^2L(T))^{h(T)}, n)$.*

Доказательство. Пусть вычисление функции sign_G на векторе $X \in \mathbb{F}_2^{E(G)}$ порождает последовательность вершин $v_0, \ldots, v_h$ дерева T, от корня к листу. Через

$$\ell_k(X) = \sum_{e \in E(G)} \lambda_e^{(k)} x_e, \quad 0 \leqslant k < h,$$

обозначим линейные функции, приписанные вершинам этого пути, а через α_k – значения этих функций на векторе X.

Поскольку дерево вычисляет функцию sign_G, все совершенные паросочетания графа G, удовлетворяющие соотношениям

$$\ell_k(\mathfrak{m}) = \alpha_k, \tag{7}$$

имеют одинаковый знак.

Зададим матрицу "обобщенных знаков" τ по правилу

$$\tau_{i,j} = \prod_{k=0}^{h-1} t_k^{\lambda_e^{(k)}}, \quad \{i,j\} = e \in E(G), \qquad \tau_{i,j} = 0, \quad \{i,j\} \notin E(G),$$

мономы в этой матрице зависят от $h(T)$ вспомогательных переменных, степени переменных ограничены величиной $L(T)$.

Коэффициент m_α при мономе $\prod\limits_{k=0}^{h-1} t_k^{\alpha_k}$ в разложении $\operatorname{Pf} A_{\tau,G}$ равен $\pm 1 \cdot P_{v_h}$, где P_{v_h} – количество совершенных паросочетаний графа G, удовлетворяющих (7).

Суммируя модули коэффициентов m_α по всем листьям дерева, получаем общее количество совершенных паросочетаний в графе G.

Каждый из этих коэффициентов вычисляется за время $\operatorname{poly}((nL(T))^{h(T)})$. Ветвление дерева в базисе целочисленных линейных функций ограничено сверху $nL(T)$, поэтому количество листьев $s(T)$ не превосходит $(nL(T))^{h(T)}$. Отсюда следует указанная в теореме оценка времени работы. ▲

Замечание 1. Для базиса линейных разрешающих деревьев оценку теоремы можно улучшить до $\operatorname{poly}(2^{h(T)}, n)$. В этом случае можно проводить вычисления в алгебре $\mathcal{A}_{h(T)}$, размерность которой равна $2^{h(T)}$.

Для применения теоремы 1 нужно уметь строить разрешающие деревья для sign_G в базисе целочисленных линейных функций небольшой высоты. Здесь возникают вопросы, аналогичные вопросам о пфаффовых графах: структурная характеризация графов, для которых возможны разрешающие деревья небольшой высоты, и алгоритмы построения таких деревьев. Эти вопросы далеки от разрешения.

Подсчет совершенных паросочетаний в графе является $\#\mathbf{P}$-полной задачей и даже возможность вычисления за время $2^{o(n)}$ противоречит популярным гипотезам теории сложности [3]. Противоречат ли верхние оценки времени работы алгоритма из теоремы 1 этим гипотезам? Мы дадим отрицательный ответ на этот вопрос.

Пусть T – разрешающее дерево в базисе целочисленных линейных функций, вычисляющее функцию $\operatorname{sign}_{K_{2n}}$ для полного графа K_{2n}. Используем те же обозначения для параметров дерева, что и в формулировке теоремы 1. Так как $b(T) \leqslant nL(T)$, то $2^{\mathbf{D}_{\mathbb{Z}}(\operatorname{sign}_G)} \leqslant (nL(T))^{h(T)}$, т.е. логарифм меры сложности алгоритма из теоремы 1 ограничен снизу величиной $\mathbf{D}_{\mathbb{Z}}(\operatorname{sign}_G)$.

Мы докажем сильные нижние оценки на эту сложность.

Теорема 2. *Справедливы оценки* $\mathbf{D}_{\mathbb{Z}}(\operatorname{sign}_{K_{2n}}) = \Omega(n \log n)$ *и* $\mathbf{D}_{\oplus}(\operatorname{sign}_{K_{2n}}) = \Omega(n \log n)$.

Всего совершенных паросочетаний в полном графе $2^{O(n \log n)}$. В силу лемм 1 и 2 оценки теоремы оптимальны с точностью до мультипликативной константы.

Доказательство теоремы 2 см. ниже в § 6.

Замечание 2. Первая часть теоремы 2 и предложение 1 дают лишь линейную по n нижнюю оценку для $\mathbf{D}_S(\operatorname{sign}_{K_{2n}})$ и $\mathbf{D}_{\oplus}(\operatorname{sign}_{K_{2n}})$. Как уже отмечалось, в случае линейных разрешающих деревьев возможно вычисление в факторалгебре $\mathcal{A}_h$, которое быстрее общего алгоритма теоремы 1. Второе утверждение теоремы 2 показывает, что использование этой факторалгебры не дает существенного выигрыша в общем случае. Для разрешающих деревьев в базисе симметрических функций такого ускорения вычислений неизвестно.

Вопрос о сложности знака паросочетания в модели разрешающих деревьев в базисе симметрических функций представляется также интересным с точки зрения теории сложности булевых функций. В настоящее время этот вопрос остается открытым.

Для получения нижних оценок сложности знака паросочетания в моделях обобщенных разрешающих деревьев мы свяжем эту сложность с оценками сложности коммуникационных задач.

§ 5. Коммуникационная сложность для знака паросочетания

Кратко напомним основные понятия коммуникационной сложности, использованные в этой статье, и зафиксируем обозначения. Подробное изложение этой дисциплины читатель может найти в учебниках, скажем, в классическом учебнике [21] или в уже упомянутой книге [20]. Весьма подробный обзор методов построения нижних оценок в коммуникационной сложности содержится в [22].

Коммуникационная задача для двух участников (их по традиции именуют Алиса и Боб) задается функцией $F\colon A \times B \to Z$. Обычно функция предполагается всюду определенной, но все даваемые ниже определения имеют точно тот же смысл для частично определенных функций; использованные в статье результаты рутинно переносятся на случай частично определенных функций.

Задача состоит в следующем: Алиса знает первый аргумент x функции F, а Боб – второй аргумент y. Участникам нужно вычислить значение $F(x, y)$, обменявшись как можно меньшим количеством информации. Протокол коммуникации Алисы и Боба – это корневое бинарное дерево, каждому внутреннему узлу которого приписан участник и функция выбора потомка в зависимости от известного данному участнику аргумента функции. Листьям дерева приписаны элементы множества Z. Пара аргументов x, y функции F порождает путь по дереву протокола из корня в лист, а листу сопоставлен какой-то элемент из Z. Так определяется функция, вычисляемая протоколом.

Протокол всегда вычисляет всюду определенную функцию. Поэтому протоколом вычисления частичной функции называется протокол вычисления всюду определенного продолжения этой функции.

Детерминированной коммуникационной сложностью $\mathbf{C}(F)$ функции F называется наименьшая высота протокола, вычисляющего F.

Обозначим через $M_{2n}(\pm 1, 0)$ множество симметрических матриц порядка $2n$ с матричными элементами ± 1, 0. Определим аддитивную функцию знака совершенного паросочетания в графе G как

$$\operatorname{sign}_G^{\mathbb{Z}}(X,Y) = \begin{cases} \operatorname{sign}(\mathfrak{m}), & \text{если } X+Y = A_{\mathfrak{m}},\ \mathfrak{m} \in \mathcal{M}(G), \\ \text{не определена} & \text{в противном случае.} \end{cases} \tag{8}$$

Здесь $X, Y \in M_{2n}(\pm 1, 0)$, а сложение обычное, целочисленное. Мы считаем, что вершины графа нумеруются числами от 1 до $2n$.

Пример 3. Пусть $G = K_4$ – полный граф на четырех вершинах, занумерованных числами от 1 до 4, и фиксированная ориентация ε_0 та же, что и в примере 1. Тогда для

$$X_1 = \begin{pmatrix} +1 & 0 & 0 & 0 \\ -1 & 0 & +1 & 0 \\ -1 & 0 & -1 & -1 \\ 0 & 0 & 0 & +1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} -1 & 0 & 0 & +1 \\ +1 & 0 & 0 & 0 \\ +1 & +1 & +1 & +1 \\ +1 & 0 & 0 & -1 \end{pmatrix},$$

$$X_3 = \begin{pmatrix} +1 & 0 & +1 & -1 \\ -1 & 0 & 0 & +1 \\ 0 & -1 & -1 & -1 \\ -1 & +1 & 0 & +1 \end{pmatrix}$$

получаем $\operatorname{sign}_G^{\mathbb{Z}}(X_1, X_2) = +1$, $\operatorname{sign}_G^{\mathbb{Z}}(X_2, X_3) = -1$, а $\operatorname{sign}_G^{\mathbb{Z}}(X_1, X_3)$ не определена.

Предложение 2. *Справедливо неравенство* $\mathbf{C}(\operatorname{sign}_G^{\mathbb{Z}}) \leqslant 2\mathbf{D}_{\mathbb{Z}}(\operatorname{sign}_G)$.

Доказательство. Алиса и Боб могут имитировать вычисление по оптимальному разрешающему дереву T в базисе целочисленных линейных функций, обмениваясь значениями функций в вершинах разрешающего дерева на своих матрицах. В силу линейности это позволяет восстановить значение функции на сумме этих матриц. Для передачи одного значения нужно $\lceil \log b(T) \rceil$ битов, а общее количество переданной информации будет как раз $2h(T)\log b(T) = 2\mathbf{D}_{\mathbb{Z}}(\operatorname{sign}_G)$. Двойка возникает из-за того, что для корректного выбора пути по дереву коммуникационного протокола каждый участник должен знать значение функции в текущей вершине. ▲

Коммуникационная сложность $\mathbf{C}(\operatorname{sign}_G^{\mathbb{Z}})$ дает нижнюю оценку $\mathbf{D}_{\mathbb{Z}}(\operatorname{sign}_G)$. Поэтому для построения нижних оценок сложности функции знака паросочетания в модели разрешающих деревьев можно использовать хорошо развитую технику построения нижних оценок в коммуникационной сложности.

Функция (8) является обобщением хорошо известных XOR-функций. Для булевой функции $f(x)$, $x \in \{0,1\}^m$, XOR-функция $f \circ \oplus$ является булевой функцией от $2m$ булевых переменных, она задается равенством $f \circ \oplus(x,y) = f(x \oplus y)$. XOR-функции были предложены в работе [23] и оказались полезными для анализа нескольких важных вопросов в коммуникационной сложности (см., например, [23–25]).

Для сложности $\mathbf{D}_{\oplus}(\operatorname{sign}_G)$ есть аналогичная оценка через XOR-функцию знака паросочетания $\operatorname{sign}_G \circ \oplus$, определенную на множестве $\operatorname{Sym}_{2n}(\mathbb{F}_2)$ симметрических матриц порядка $2n$ над полем $\mathbb{F}_2$ из двух элементов:

$$\operatorname{sign}_G \circ \oplus\,(X,Y) = \begin{cases} \operatorname{sign}_G(\mathfrak{m}), & \text{если } X \oplus Y = A_{\mathfrak{m}},\ \mathfrak{m} \in \mathcal{M}(G), \\ \text{не определена} & \text{в противном случае.} \end{cases}$$

Здесь мы допускаем неоднозначность в обозначениях, используя $A_{\mathfrak{m}}$ и для целочисленной матрицы смежности, и для соответствующей матрицы над полем $\mathbb{F}_2$. Смысл этого обозначения всюду ясен из контекста.

Предложение 3. *Справедливо неравенство* $\mathbf{C}(f \circ \oplus) \leqslant 2\mathbf{D}_{\oplus}(f)$.

Доказательство по сути то же самое, что для предложения 2.

Замечание 3. Верхняя оценка сложности $\mathbf{D}_{\oplus}(f)$ функции f в модели линейных разрешающих деревьев через коммуникационную сложность XOR-функции $f \circ \oplus$ оказывается более трудной задачей. Известна верхняя оценка $O(\mathbf{C}(f \circ \oplus)^6)$, см. [26]. Ее точность остается открытым вопросом.

Нам потребуются сравнительно простые нижние оценки коммуникационной сложности. Напомним их формулировки.

Подмножества $S \subseteq A$, $Q \subseteq B$ задают *комбинаторный прямоугольник* $S \times Q$ (далее для краткости – прямоугольник). Прямоугольник называется монохроматическим для функции $F\colon A \times B \to Z$, если F постоянна на этом прямоугольнике (для частичных функций – на пересечении области определения с прямоугольником). Наименьшее количество монохроматических прямоугольников в покрытии области определения F обозначается $\mathrm{Cov}(F)$ и называется *величиной покрытия*. Каждый протокол вычисления порождает покрытие матричных элементов монохроматическими прямоугольниками. Наименьшее количество прямоугольников в покрытиях, порождаемых коммуникационными протоколами, обозначается через $\mathrm{Cov}^P(F)$.

Величины покрытий используются в нижних оценках коммуникационной сложности в силу следующего простого неравенства.

Предложение 4 [20, 21]. *Справедливы неравенства* $\mathrm{Cov}(F) \leqslant \mathrm{Cov}^P(F) \leqslant 2^{\mathbf{C}(F)}$.

Заметим, что в [20, 21], как и в большинстве источников, это предложение доказано для всюду определенных функций. Однако доказательство без труда переносится на случай частичных функций: любое покрытие монохроматическими прямоугольниками всюду определенного продолжения F' частичной функции является покрытием монохроматическими прямоугольниками самой функции, т.е. $\mathrm{Cov}(F) \leqslant \mathrm{Cov}(F')$. Выбрав то продолжение F', которое отвечает оптимальному протоколу для F, получаем

$$\mathrm{Cov}(F) \leqslant \mathrm{Cov}(F') \leqslant 2^{\mathbf{C}(F')} = 2^{\mathbf{C}(F)}.$$

Нижние оценки коммуникационной сложности удобнее получать не для $\mathrm{sign}_G^{\mathbb{Z}}$, а для варианта XOR-функции $\mathrm{sign}_G^{\oplus} = (-1)^{\mathrm{sign}_G \circ \oplus}$, в которой множество значений изменено на $\{+1, -1\}$.

Напрямую сравнить коммуникационные сложности $\mathbf{C}(\mathrm{sign}_G^{\mathbb{Z}})$ и $\mathbf{C}(\mathrm{sign}_G^{\oplus})$ затруднительно. Однако нетрудно сравнить величины покрытий монохроматическими прямоугольниками для функций $\mathrm{sign}_G^{\mathbb{Z}}$ и $\mathrm{sign}_G^{\oplus}$.

Лемма 3. *Справедливо неравенство* $\mathrm{Cov}(\mathrm{sign}_G^{\mathbb{Z}}) \geqslant \mathrm{Cov}(\mathrm{sign}_G^{\oplus})$.

Доказательство. Определим отображение стирания знака $\sigma\colon \{-1, 0, 1\} \to \mathbb{F}_2$

$$\sigma(-1) = \sigma(1) = 1, \quad \sigma(0) = 0$$

и продолжим его на матрицы поэлементно. Докажем, что отображение стирания знака переводит матрицы из области определения $\mathrm{sign}_G^{\mathbb{Z}}$ в матрицы из области определения $\mathrm{sign}_G^{\oplus}$, т.е.

$$\sigma\big(\mathrm{Dom}(\mathrm{sign}_G^{\mathbb{Z}})\big) = \mathrm{Dom}(\mathrm{sign}_G^{\oplus}).$$

Пусть $(X, Y) \in \mathrm{Dom}(\mathrm{sign}_G^{\mathbb{Z}})$, т.е. $X + Y = A_{\mathfrak{m}}$, $\mathfrak{m} \subseteq E(G)$. Если $\{i, j\} \in \mathfrak{m}$, то из двух матричных элементов $X_{i,j}$ и $Y_{i,j}$ ровно один равен 1, а второй равен 0; остальные матричные элементы либо равны нулю в обеих матрицах X и Y, либо имеют разные знаки. Но это означает, что $\sigma(X) \oplus \sigma(Y) = A_{\mathfrak{m}}$.

И обратно: если $X^\sigma \oplus Y^\sigma = A_{\mathfrak{m}}$, то возможно приписать знак минус тем матричным элементам $Y^\sigma(i, j)$, которые равны 1 и $\{i, j\} \notin \mathfrak{m}$. Получим матрицу Y, а матрицу X возьмем равной X^σ (отождествляя 0 и 1 в целых числах и в поле $\mathbb{F}_2$). И тогда $X + Y = A_{\mathfrak{m}}$, где сложение уже целочисленное.

Проверим, что монохроматический для $\mathrm{sign}_G^{\mathbb{Z}}$ прямоугольник $S \times Q$ переводится отображением стирания знака в монохроматический для $\mathrm{sign}_G^{\oplus}$ прямоугольник $\sigma(S) \times \sigma(Q)$. Действительно, если $(X, Y) \in \mathrm{Dom}(\mathrm{sign}_G^{\mathbb{Z}})$, то

$$\mathrm{sign}_G^{\mathbb{Z}}(X, Y) = \mathrm{sign}_G^{\oplus}(\sigma(X), \sigma(Y)).$$

Поэтому любое покрытие монохроматическими для $\mathrm{sign}_G^{\mathbb{Z}}$ прямоугольниками является также покрытием монохроматическими для $\mathrm{sign}_G^{\oplus}$ прямоугольниками. ▲

Для оценки величины покрытия используем оценку отклонения (discrepancy) $\mathrm{disc}_U(f)$ (частичной) функции $f\colon A \times B \to \{-1, +1\}$ относительно равномерного распределения на области определения f. *Вес прямоугольника* $S \times Q$ относительно функции f равен сумме значений функции на пересечении прямоугольника с областью определения функции:

$$\delta_f(S, Q) = \sum_{\substack{x \in S,\, y \in Q \\ (x,y) \in \mathrm{Dom}\, f}} f(x, y).$$

Отклонение f по отношению к равномерному распределению U на области определения f задается как

$$\mathrm{disc}_U(f) = \frac{1}{\mathrm{Dom}\, f} \max_{S \subseteq A,\, Q \subseteq B} |\delta_f(S, Q)|.$$

Отклонение ограничивает сверху меру монохроматического прямоугольника относительно равномерного распределения на области определения f, поэтому

$$\mathrm{Cov}(F) \geqslant \frac{1}{\mathrm{disc}_U(f)}. \tag{9}$$

В свою очередь, отклонение частичной симметрической функции $f\colon A \times A \to \{-1, +1\}$, $f(x, y) = f(y, x)$, если $(x, y) \in \mathrm{Dom}\, f$, будем оценивать спектральным методом. Продолжим функцию f до всюду определенной функции f_0 нулями:

$$f_0(x, y) = \begin{cases} f(x, y), & (x, y) \in \mathrm{Dom}\, f, \\ 0 & \text{в противном случае.} \end{cases}$$

Функцию f_0 можно рассматривать как матрицу симметрического линейного оператора F на пространстве $\mathbb{R}^A$ функций с действительными значениями и областью определения A. Через $\|F\|$ обозначаем спектральную норму оператора F.

Лемма 4. *Для любого прямоугольника $S \times Q$ выполняется*

$$|\delta_f(S, Q)| \leqslant \sqrt{|S||Q|}\, \|F\|.$$

Доказательство. Обозначим через $\mathbb{1}_S, \mathbb{1}_Q$ индикаторные функции подмножеств S, Q:

$$\mathbb{1}_S(x) = \begin{cases} 1, & \text{если } x \in S, \\ 0 & \text{в противном случае.} \end{cases}$$

Запишем вес прямоугольника $S \times Q$ как

$$\delta_f(S,Q) = \sum_{x,y \in A} f(x,y)\mathbb{1}_S(X)\mathbb{1}_Q(Y) = \sum_{x \in A} \mathbb{1}_S(x)(F\mathbb{1}_Q)(x) = \langle \mathbb{1}_S, F\mathbb{1}_Q \rangle,$$

где $\langle \cdot, \cdot \rangle$ – стандартное скалярное произведение в координатном базисе.

Применяя неравенство Коши – Шварца, получаем

$$|\langle \mathbb{1}_S, F\mathbb{1}_Q \rangle| \leqslant \|\mathbb{1}_S\|_2 \|\mathbb{1}_Q\|_2 \|F\| = \sqrt{|S|}\sqrt{|Q|}\,\|F\|,$$

где $\|\cdot\|_2$ обозначает ℓ_2-норму. ▲

§ 6. Спектральные нижние оценки

Применим спектральный метод для получения нижних оценок коммуникационной сложности XOR-функции $\operatorname{sign}_G^{\oplus} = (-1)^{\operatorname{sign}_G \circ \oplus}$ знака паросочетания.

Обозначим через P_G оператор, отвечающий продолжению функции $\operatorname{sign}_G^{\oplus}$ нулями вне области определения. Чтобы использовать лемму 4, нам нужна оценка его спектральной нормы.

Оператор P_G действует на пространстве V функций $\operatorname{Sym}_{2n}(\mathbb{F}_2) \to \mathbb{R}$, размерность этого пространства равна $\binom{2n+1}{2}$. Спектральную норму этого оператора можно оценить сверху следующим образом.

Лемма 5. *Справедливо неравенство $\|P_G\| \leqslant D(G)$, где $D(G)$ – максимальное значение модуля пфаффиана $|\operatorname{Pf}(\varepsilon \bullet A_G)|$ по всем ориентациям ребер графа G.*

Доказательство. Выразим P_G как сумму

$$P_G = \sum_{\mathfrak{m} \in \mathcal{M}(G)} \operatorname{sign}(\mathfrak{m}) P_{\mathfrak{m}}, \quad \text{где} \quad P_{\mathfrak{m}}(X,Y) = \begin{cases} 1, & \text{если } X \oplus Y = A_{\mathfrak{m}}, \\ 0 & \text{в противном случае.} \end{cases}$$

Матрицы $P_{\mathfrak{m}}$ одновременно диагонализуются в базисе Фурье (базисе характеров). Напомним, что характеры χ_T индексируются симметрическими матрицами T размера $n \times n$ над $\mathbb{F}_2$ и задаются следующим образом:

$$\chi_T(X) = (-1)^{\sum\limits_{i \leqslant j} T_{i,j} X_{i,j}}.$$

Сумма в показателе определена корректно, так как существенна лишь четность этой суммы. Более подробно о преобразовании Фурье на булевом кубе см. [27].

Напомним, что спектральная норма симметрического оператора равна максимуму модулей собственных чисел этого оператора. Собственные числа $P_{\mathfrak{m}}$ легко вычисляются. Подействуем $P_{\mathfrak{m}}$ на базисный вектор (характер):

$$(P_{\mathfrak{m}}\chi_T)(X) = \sum_Y P_{\mathfrak{m}}(X,Y)\chi_T(Y) = \chi_T(X \oplus A_{\mathfrak{m}})) = \chi_T(A_{\mathfrak{m}})\chi_T(X).$$

В последнем равенстве использована мультипликативность характеров.

Собственное число оператора P_G на характере χ_T является суммой собственных чисел $P_{\mathfrak{m}}$:

$$\lambda_T = \sum_{\mathfrak{m}\in\mathcal{M}(G)} \chi_T(A_{\mathfrak{m}})\operatorname{sign}(\mathfrak{m}) = \sum_{\mathfrak{m}\in\mathcal{M}(G)} (-1)^{\sum\limits_{i\leqslant j} T_{i,j}(A_{\mathfrak{m}})_{i,j}} \operatorname{sign}(\mathfrak{m}) =$$
$$= \sum_{\mathfrak{m}\in\mathcal{M}(G)} \operatorname{sign}(\mathfrak{m}) \prod_{\{i,j\}\in\mathfrak{m}} (-1)^{T_{i,j}} = \operatorname{Pf}(\varepsilon \bullet A_G),$$

где ε отличается от фиксированной по умолчанию ориентации ε^0 в точности на тех ребрах, на которых $T(i,j) = 1$.

Но это и означает, что максимальное по модулю собственное число оператора P_G равно $D(G)$. ▲

Используя эти факты, уже нетрудно получить верхнюю оценку отклонения для функции $\operatorname{sign}_G^{\oplus}$ и тем самым нижнюю оценку коммуникационной сложности XOR-функции знака паросочетания.

Следствие 1. *Справедливы неравенства*

$$\operatorname{disc}_U(\operatorname{sign}_G^{\oplus}) \leqslant D(G)/|\mathcal{M}(G)|, \quad \mathbf{C}(\operatorname{sign}_G^{\oplus}) \geqslant \log_2 |\mathcal{M}(G)|/D(G).$$

Доказательство. Для каждого $X \in \operatorname{Sym}_{2n}(\mathbb{F}_2)$ есть ровно $|\mathcal{M}(G)|$ таких матриц Y, что $(X,Y) \in \operatorname{Dom}\operatorname{sign}_G^{\oplus}$. Это в точности матрицы вида $X \oplus A_{\mathfrak{m}}$ для всех $\mathfrak{m} \in \mathcal{M}(G)$. Поэтому область определения функции $\operatorname{sign}_G^{\oplus}$ имеет размер $|\mathcal{M}(G)|N$, где $N = 2^{\dim V} = 2^{\binom{2n+1}{2}}$.

Из лемм 4, 5 получаем

$$\operatorname{disc}_U(\operatorname{sign}_G^{\oplus}) = \frac{1}{N|\mathcal{M}(G)|} \max_{\substack{S\subseteq M_n(\mathbb{F}_2)\\ Q\subseteq M_n(\mathbb{F}_2)}} |\delta_{\operatorname{sign}_G^{\oplus}}(S,Q)| \leqslant \frac{1}{N|\mathcal{M}(G)|}\sqrt{|S||Q|}\,\|P_G\| \leqslant$$
$$\leqslant \sqrt{\frac{|S|}{N}\,\frac{|Q|}{N}}\,\frac{D(G)}{|\mathcal{M}(G)|} \leqslant \frac{D(G)}{|\mathcal{M}(G)|},$$

что и требовалось.

Второе неравенство следует из первого в силу предложения 4 и неравенства (9). ▲

Отсюда следуют оценки $\Omega(n\log n)$ на коммуникационную сложность XOR-функции $\operatorname{sign}_{K_{2n}}^{\oplus}$ знака паросочетания для полного графа и тем самым на сложность функции $\operatorname{sign}_{K_{2n}}$ в модели линейных разрешающих деревьев (теорема 2).

Доказательство теоремы 2. Для применения следствия 1 нужно оценить отношение количества совершенных паросочетаний в полном графе на $2n$ вершинах $|\mathcal{M}(K_{2n})|$ и максимума модуля пфаффиана ориентированной матрицы смежности полного графа $D(K_{2n})$.

Оценим первую величину как

$$|\mathcal{M}(K_{2n})| = (2n-1)!! \geqslant (2n-2)!! = (2n-2)(2n-4)\ldots 2 = 2^{n-1}(n-1)!.$$

Оценим $D(K_{2n})$. Из формулы (3) и неравенства Адамара [14, следствие 7.8.2, с. 565] для матриц порядка $2n$ с матричными элементами $0, \pm 1$ получаем

$$|\operatorname{Pf}(\varepsilon \bullet A_G)| \leqslant \sqrt{\det(\varepsilon \bullet A_G)} \leqslant (2n)^{n/2}.$$

Это означает, что $D(G) \leqslant (2n)^{n/2}$, и потому

$$\mathrm{Cov}\big(\mathrm{sign}^{\oplus}_{K_{2n}}\big) \geqslant \frac{2^{n-1}(n-1)!}{(2n)^{n/2}} = \frac{1}{2n}\frac{2^n n!}{(2n)^{n/2}} \geqslant \frac{1}{2n}2^{n/2}\frac{(n/3)^n}{n^{n/2}} =$$
$$= \frac{1}{2}\left(\frac{\sqrt{2}}{3}\right)^n n^{n/2-1}.$$

После логарифмирования и применения предложения 4 и леммы 3 отсюда получаются нижние оценки коммуникационной сложности $\Omega(n\log n)$ для XOR-функций знака паросочетания. Указанные в теореме 2 нижние оценки сложности в моделях разрешающих деревьев для функции знака паросочетания следуют из предложений 2 и 3. ▲

§ 7. Оценки для разреженных графов

Следствие 1 дает нижнюю оценку $\log_2 |\mathcal{M}_G|/D(G)$ коммуникационной сложности XOR-функции знака паросочетания в любом графе. Из этой оценки следует также нижняя оценка на высоту разрешающего дерева в базисе линейных функций для функции sign_G.

Точность соотношения между коммуникационной сложностью и высотой разрешающих деревьев остается открытым вопросом. Заметим, что техника, использованная в работе [26] для оценки сложности в модели линейных разрешающих деревьев полиномом от коммуникационной сложности XOR-функции, не применима к частично определенным функциям.

Однако в предельном случае $|\mathcal{M}(G)| = D(G)$ оценка точна. Действительно, это равенство означает, что $|\mathrm{Pf}(\varepsilon \bullet A_G)| = |\mathcal{M}(G)|$ для некоторой ориентации ε. Поскольку вклад каждого паросочетания в $\mathrm{Pf}(\varepsilon \bullet A_G)$ по модулю равен 1, знаки всех паросочетаний при такой ориентации должны быть одинаковы, т.е. ε – пфаффова ориентация графа G. Но тогда значение линейной функции на матричных элементах, отвечающее оптимальному (пфаффову) выбору знаков, позволяет определить знак паросочетания. Это, в свою очередь, означает, что линейное разрешающее дерево высоты 1 вычисляет функцию знака паросочетания.

Любой непфаффовый граф H с $|\mathcal{M}(H)| > D(H)$ позволяет получать линейные по числу вершин оценки коммуникационной сложности XOR-функции знака паросочетания.

Заметим, что коммуникационная сложность XOR-функции знака паросочетания монотонна по увеличению ребер графа: если $E(G') \subset E(G)$, то $\mathbf{C}(\mathrm{sign}^{\oplus}_{G'}) \leqslant \mathbf{C}(\mathrm{sign}^{\oplus}_{G})$. Действительно, любой протокол для большего графа легко модифицируется для меньшего (на отсутствующих ребрах полагаем значения матриц X и Y равными нулю).

Подграф H графа G называется *центральным*, если подграф, индуцированный дополнением к вершинам H, содержит совершенное паросочетание.

Рассмотрим такую последовательность графов $H_1, \ldots H_s$, для которых

$$|\mathcal{M}(H_i)|/D(H_i) \geqslant \alpha > 1.$$

Лемма 6. *Пусть в графе G есть центральный подграф H, связные компоненты которого – графы H_i, $1 \leqslant i \leqslant s$. Тогда* $\mathbf{D}_{\oplus}(\mathrm{sign}_G) \geqslant \frac{1}{2}s\log_2\alpha$.

Доказательство. Из предложения 3 и монотонности коммуникационной сложности по ребрам имеем

$$\mathbf{D}_{\oplus}(\mathrm{sign}_G) \geqslant \frac{1}{2}\mathbf{C}(\mathrm{sign}^{\oplus}_G) \geqslant \frac{1}{2}\mathbf{C}(\mathrm{sign}^{\oplus}_H).$$

Поэтому достаточно доказать неравенство $|\mathcal{M}(H)|/D(H) \geqslant \alpha^s$. Матрица смежности H распадается на блоки, отвечающие компонентам связности H_i.

Количество совершенных паросочетаний в графе H выражается как произведение $|\mathcal{M}(H)| = |\mathcal{M}(H_1)||\mathcal{M}(H_2)| \dots |\mathcal{M}(H_s)|$.

Пфаффиан матрицы $\varepsilon \bullet A_H$ также разбивается на произведение пфаффианов матриц $\varepsilon \bullet A_{H_i}$. Значит, $D(H) = D(H_1) \dots D(H_s)$.

Так как $|\mathcal{M}(H_i)|/D(H_i) \geqslant \alpha$, получаем искомое неравенство. ▲

Следствие 2. *Пусть H – непфаффовый граф, $|\mathcal{M}(H)| = h$. Тогда для графа, содержащего центральный подграф sH (несвязная сумма s копий H), выполняется неравенство*

$$\mathbf{D}_{\oplus}(\mathrm{sign}_G) \geqslant \frac{s}{2} \log_2 \left(1 + \frac{2}{h-2}\right).$$

Доказательство. Для любой ориентации ε непфаффова графа H выполняется неравенство $|\mathrm{Pf}(\varepsilon \bullet H)| \leqslant h - 2$. Теперь применим лемму 6. ▲

Используя эти утверждения, можно доказать, что сложность разрешающих деревьев велика для функции знака паросочетания уже для связных графов, все вершины которых имеют степень 3. Это значительно сужает возможности метода символического пфаффиана.

Теорема 3. *Существует последовательность графов G_i, в которой все графы связные, степени вершин в каждом равны* 3, *и $\mathbf{D}_{\oplus}(\mathrm{sign}_{G_i}) = \Omega(n_i)$, где n_i – количество вершин в G_i, а константа, скрытая в Ω, не зависит от i.*

Доказательство. *Гекс* – это граф, полученный из полного двудольного графа $K_{3,3}$ подразбиением ребер. В гексе естественным образом выделяются девять путей, каждый получен в результате подразбиений одного ребра $K_{3,3}$. Будем называть эти пути *отрезками гекса*. Назовем гекс *нечетным*, если каждый отрезок состоит из нечетного количества ребер. Нечетный гекс является непфаффовым графом [17].

Заметим, что покрыть все внутренние вершины отрезка в нечетном гексе можно двумя паросочетаниями: одно содержит концевые вершины отрезка, другое – нет. Каждая из шести вершин, отвечающих графу $K_{3,3}$, из которого получен гекс, содержится ровно в одном паросочетании первого типа. Таким образом, выбор паросочетаний первого типа задает совершенное паросочетание на исходном графе $K_{3,3}$. Очевидно, верно и обратное. Поэтому совершенных паросочетаний в нечетном гексе столько же, сколько в $K_{3,3}$, т.е. шесть.

Возьмем граф sH, где H – нечетный гекс, в котором есть два отрезка длины 3, а остальные отрезки имеют длину 1. Граф G_s имеет те же вершины, что и sH, поэтому sH – центральный в G_s. Обозначим внутренние вершины первого отрезка длины 3 в i-й копии H_i гекса H через $u_i^{(1)}, v_i^{(1)}$, аналогично внутренние вершины второго отрезка длины 3 в H_i обозначим через $u_i^{(2)}, v_i^{(2)}$. Множество ребер графа G_s содержит все ребра гексов H_i, а также ребра $(u_i^{(1)}, u_{i-1}^{(2)}), (v_i^{(1)}, v_{i-1}^{(2)})$ (вычитание по модулю s). Других ребер нет. Из построения ясно, что граф G_s связный и степень каждой вершины равна 3.

Количество вершин в графе G_s равно $n_s = 10s$, а $\mathbf{D}_{\oplus}(G_s) \geqslant s \log_2(\sqrt{3/2})$ по следствию 2. Получаем оценку теоремы. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Valiant L.G.* The Complexity of Computing the Permanent // Theoret. Comput. Sci. 1979. V. 8. № 2. P. 189–201. https://doi.org/10.1016/0304-3975(79)90044-6

2. *Björklund A.* Counting Perfect Matchings as Fast as Ryser // Proc. 23rd Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'2012). Kyoto, Japan. Jan. 17–19, 2012. P. 914–921. https://dl.acm.org/doi/10.5555/2095116.2095189
3. *Dell H., Husfeldt T., Marx D., Taslaman N., Wahlén M.* Exponential Time Complexity of the Permanent and the Tutte Polynomial // ACM Trans. Algorithms. 2014. V. 10. № 4. Art. 21 (32 pp.). https://doi.org/10.1145/2635812
4. *Kasteleyn P.* Graph Theory and Crystal Physics // Graph Theory and Theoretical Physics. London: Academic, 1967. P. 43–110.
5. *Galluccio A., Loebl M.* On the Theory of Pfaffian Orientations. I: Perfect Matchings and Permanents // Electron. J. Combin. 1999. V. 6. Art. R6 (18 pp.). https://doi.org/10.37236/1438
6. *Tesler G.* Matchings in Graphs on Non-orientable Surfaces // J. Combin. Theory Ser. B. 2000. V. 78. № 2. P. 198–231. https://doi.org/10.1006/jctb.1999.1941
7. *Little C.H.C.* An Extension of Kasteleyn's Method of Enumerating the 1-Factors of Planar Graphs // Combinatorial Mathematics II. Lect. Notes Math. V. 403. Berlin: Springer, 1974. P. 63–72. https://doi.org/10.1007/BFb0057377
8. *Straub S., Thierauf T., Wagner F.* Counting the Number of Perfect Matchings in K_5-Free Graphs // Theory Comput. Syst. 2016. V. 59. № 3. P. 416–439. https://doi.org/10.1007/s00224-015-9645-1
9. *Izumi T., Wadayama T.* A New Direction for Counting Perfect Matchings // Proc. 2012 IEEE 53rd Annu. Symp. on Foundations of Computer Science (FOCS'2012). New Brunswick, NJ, USA. Oct. 20–23, 2012. P. 591–598. https://doi.org/10.1109/FOCS.2012.28
10. *Pólya G.* Aufgabe 424 // Arch. Math. Phys. (3). 1913. V. 20. P. 271.
11. *Бабенко А.В., Вялый М.Н.* О линейной классификации четных и нечетных перестановочных матриц и сложности вычисления перманента // Ж. вычисл. матем. и матем. физ. 2017. Т. 57. № 2. С. 362–372. https://doi.org/10.7868/S004446691702003X
12. *Вялый М.Н.* Сложность вычисления знака перестановки в модели разрешающих деревьев и подсчет совершенных паросочетаний в двудольных графах // Тр. X междунар. конф. "Дискретные модели в теории управляющих систем". Москва и Подмосковье, 23–25 мая 2018 г. / Отв. ред. Алексеев В., Романов Д., Данилов Б. М.: МАКС Пресс, 2018. С. 94–97.
13. *Mahajan M., Vinay V.* Determinant: Old Algorithms, New Insights // SIAM J. Discrete Math. 1999. V. 12. № 4. P. 474–490. https://doi.org/10.1137/S0895480198338827
14. *Хорн Р., Джонсон Ч.* Матричный анализ. М.: Мир, 1989.
15. *Винберг Э.Б.* Курс алгебры. М.: Факториал, 1999.
16. *Mahajan M., Subramanya P.R., Vinay V.* A Combinatorial Algorithm for Pfaffians // Proc. 5th Annu. Int. Conf. on Computing and Combinatorics (COCOON'99). Tokyo, Japan. July 26–28, 1999. Lect. Notes Comput. Sci. V. 1627. Berlin: Springer, 1999. P. 134–143. https://doi.org/10.1007/3-540-48686-0_13
17. *Little C.H.C.* A Characterization of Convertible $(0,1)$-Matrices // J. Combin. Theory Ser. B. 1975. V. 18. № 3. P. 187–208. https://doi.org/10.1016/0095-8956(75)90048-9
18. *Thomas R., Whalen P.* Odd $k_{3,3}$ Subdivisions in Bipartite Graphs // J. Combin. Theory Ser. B. 2016. V. 118. P. 76–87. https://doi.org/10.1016/j.jctb.2016.01.005
19. *Robertson N., Seymour P.D., Thomas R.* Permanents, Pfaffian Orientations, and Even Directed Circuits // Ann. of Math. (2). 1999. V. 150. № 3. P. 929–975. https://doi.org/10.2307/121059
20. *Jukna S.* Boolean Function Complexity: Advances and Frontiers. Heidelberg: Springer, 2012.
21. *Kushilevitz E., Nisan N.* Communication Complexity. Cambridge: Cambridge Univ. Press, 1997.
22. *Lee T., Shraibman A.* Lower Bounds in Communication Complexity // Found. Trends Theor. Comput. Sci. 2009. V. 3. № 4. P. 263–399. http://doi.org/10.1561/0400000040
23. *Zhang Z., Shi Y.* On the Parity Complexity Measures of Boolean Functions // Theoret. Comput. Sci. 2010. V. 411. № 26–28. P. 2612–2618. https://doi.org/10.1016/j.tcs.2010.03.027

24. *Lee T., Zhang S.* Composition Theorems in Communication Complexity // Proc. 37th Int. Colloq. on Automata, Languages and Programming (ICALP'2010). Bordeaux, France. July 6–10, 2010. Part I. Lect. Notes Comput. Sci. V. 6198. Berlin: Springer, 2010. P. 475–489. https://doi.org/10.1007/978-3-642-14165-2_41

25. *Tsang H.Y., Wong C.H., Xie N., Zhang S.* Fourier Sparsity, Spectral Norm, and the Log-Rank Conjecture // Proc. 2013 IEEE 54th Annu. Symp. on Foundations of Computer Science (FOCS'2013). Berkeley, CA, USA. Oct. 26–29, 2013. P. 658–667. https://doi.org/10.1109/FOCS.2013.76

26. *Hatami H., Hosseini K., Lovett S.* Structure of Protocols for XOR Functions // Proc. 2016 IEEE 57th Annu. Symp. on Foundations of Computer Science (FOCS'2016). New Brunswick, NJ, USA. Oct. 9–11, 2016. P. 282–288. https://doi.org/10.1109/FOCS.2016.38

27. *O'Donnell R.* Analysis of Boolean Functions. New York: Cambridge Univ. Press, 2014.

Вялый Михаил Николаевич
Национальный исследовательский университет
"Высшая школа экономики"
vyalyi@gmail.com

Поступила в редакцию
19.09.2020
После доработки
17.12.2020
Принята к публикации
17.12.2020

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 2**

УДК 621.391 : 519.175.4 : 519.214

© 2021 г. **Т. Константопулос[1], А.В. Логачёв[2], А.А. Могульский[2], С.Г. Фосс[1,2]**

ПРЕДЕЛЬНЫЕ ТЕОРЕМЫ ДЛЯ МАКСИМАЛЬНОГО ВЕСА ПУТИ В НАПРАВЛЕННОМ ГРАФЕ НА ЦЕЛОЧИСЛЕННОЙ ПРЯМОЙ СО СЛУЧАЙНЫМИ ВЕСАМИ РЕБЕР

Рассматривается бесконечный направленный граф, вершины которого занумерованы целыми числами $\dots, -2, -1, 0, 1, 2, \dots$, а любая пара вершин $j < k$ соединена ребром (j, k) между ними, направленным из j в k и имеющим случайный вес $v_{j,k} \in [-\infty, \infty)$, где $\{v_{j,k},\ j < k\}$ – семейство независимых и одинаково распределенных случайных величин, которые принимают либо конечные значения (любого знака), либо значение $-\infty$. Путь в таком графе – это последовательность связанных между собой ребер $(j_0, j_1), (j_1, j_2), \dots, (j_{m-1}, j_m)$ (где $j_0 < j_1 < \dots < j_m$), а его вес – сумма весов этих ребер $\sum_{s=1}^{m} v_{j_{s-1},j_s} \geqslant -\infty$. Пусть $w_{0,n}$ – максимальный вес среди всех путей из 0 в n. В предположениях, что $\mathbf{P}(v_{0,1} > 0) > 0$, условное распределение $\mathbf{P}(v_{0,1} \in \cdot \mid v_{0,1} > 0)$ невырождено и $\mathbf{E}\exp(Cv_{0,1}) < \infty$ при некотором $C = \mathrm{const} > 0$, изучается асимптотическое поведение случайной последовательности $w_{0,n}$ при стремлении $n \to \infty$. В области нормальных и умеренно больших уклонений получена локальная предельная теорема в случае, когда распределение случайных величин $v_{i,j}$ является арифметическим, и интегро-локальная предельная теорема, если это распределение является нерешетчатым.

Ключевые слова: направленный граф, максимальный вес пути, осевые и стержневые вершины, нормальные и умеренно большие уклонения, (интегро-)локальная предельная теорема.

DOI: 10.31857/S0555292321020054

§ 1. Введение, основные обозначения и формулировка основного результата

Мы рассматриваем бесконечный направленный граф $G(\mathbb{Z}, E)$, множество вершин которого – все целые числа $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, а множество направленных ребер $E = \{e = (j, k),\ j < k,\ j, k \in \mathbb{Z}\}$ – все ребра, направленные из меньших вершин в большие. Предполагается, что в графе нет ребер из больших вершин в меньшие и нет петель вида (j, j).

Каждому ребру $e \in E$ сопоставляется его "вес" v_e, который может быть либо числом (положительным или отрицательным), либо принимать значение $-\infty$. Будем предполагать, что случайные величины $\{v_{j,k},\ j < k\}$ независимы и одинаково распределены с некоторой случайной величиной v, принимающей значения в $[-\infty, \infty)$.

[1] Работа выполнена при частичной финансовой поддержке совместного российско-французского гранта Российского фонда фундаментальных исследований и Национального центра научных исследований Франции (номера проектов РФФИ-НЦНР 19-51-15001 и CNRS 193-382).

[2] Работа выполнена в рамках Международного Центра в Академгородке (соглашение 075-15-2019-1675 с Министерством науки и высшего образования).

Пусть $p = \mathbf{P}(v > -\infty)$ и $p^+ = \mathbf{P}(v > 0)$. Пусть v^+ – случайная величина с распределением

$$\mathbf{P}(v^+ < t) = \mathbf{P}(v < t \,|\, v > 0), \quad t > 0. \tag{1.1}$$

В этой статье мы будем предполагать выполнение следующих условий:

$$\begin{aligned} &p^+ > 0, \quad \mathbf{P}(v^+ = c) < 1 \quad \text{при любом } c > 0, \\ &\mathbf{E}\, e^{Cv^+} < \infty \quad \text{при некотором } C > 0, \end{aligned} \tag{1.2}$$

т.е. случайная величина v принимает положительные значения с положительной вероятностью, ее распределение на положительной полуоси невырождено и правый хвост ее распределения относительно тонок.

В литературе используется и такая интерпретация этой модели: если $v_e = -\infty$, то считается, что ребро e отсутствует, а если $v_e > -\infty$, то ребро существует и его вес равен v_e. При таком задании появляются две независимые "случайности": ребро может существовать или нет, и если ребро существует, то его вес – независимая ни от чего случайная величина, имеющая распределение $\mathbf{P}(v \in \cdot \,|\, v > -\infty)$.

Назовем *путем* π длины $L(\pi) = m$ последовательность m связанных ребер $e_1 = (j_0, j_1)$, $e_2 = (j_1, j_2)$, $\ldots$, $e_m = (j_{m-1}, j_m)$, где конечная вершина каждого ребра совпадает с начальной вершиной следующего и $j_0 < j_1 < \ldots < j_m$, и будем говорить, что это путь из j_0 в j_m и писать $e_i \in \pi$, $i = 1, \ldots, L(\pi)$. Вес $w(\pi)$ этого пути определим как сумму весов входящих в него ребер, т.е.

$$w(\pi) = \sum_{s=1}^{L(\pi)} v_{j_{s-1}, j_s} = \sum_{e \in \pi} v_e.$$

Ясно, что путь имеет конечный вес тогда и только тогда, когда конечны веса всех его ребер.

При $j < k$ обозначим через $\Pi_{j,k}$ множество всех путей из j в k с конечными весами (т.е. $w(\pi) > -\infty$ для $\pi \in \Pi_{j,k}$), а через $w_{j,k}$ – максимальный из весов всех путей из j в k. Тогда

$$w_{j,k} = \max_{\pi \in \Pi_{j,k}} w(\pi)$$

с вероятностью единица, так как используется соглашение, что максимум по пустому множеству равен $-\infty$. Положим также $w_{j,j} = 0$ при всех j.

Рассматриваемые нами графы со случайными весами могут возникать естественным образом в различных приложениях. Скажем, если вес ребра принимает только два значения, 1 (ребро есть) и $-\infty$ (ребра нет), т.е.

$$p = \mathbf{P}(v = 1) = 1 - \mathbf{P}(v = -\infty), \tag{1.3}$$

то такой граф может описывать порядок работы некоторой вычислительной сети (см., например, [1, 2]), где под вершинами понимаются выполняемые работы, а ребра описывают их временные ограничения (если $v_{j,k} = 1$, то выполнение работы k не может начаться до завершения выполнения работы j), или функционирование биологических моделей (см., например, [3, 4]), где вершины – это виды животных, а пути описывают "пищевые цепочки" (food chains): если $v_{j,k} = 1$, то вид k может быть пищей для вида j).

Введем следующие два взаимоисключающих условия:

[**R**] *Распределение случайной величины v является нерешетчатым*, т.е. при любых a и $h > 0$ вероятность того, что v принимает значения на решетке шага h, сдвинутой на a, строго меньше единицы: $\sum\limits_{s=-\infty}^{\infty} \mathbf{P}(v = a + sh) < 1$;

[**Z**] *Распределение случайной величины v является арифметическим*, т.е. имеет место равенство $\sum\limits_{s=-\infty}^{\infty} \mathbf{P}(v = sh) = 1$ при некотором $h > 0$. Не ограничивая общности рассуждений, мы дополнительно предположим, что шаг решетки равен $h = 1$, т.е. значения v целочислены и наибольший общий делитель множества $\{k \geqslant 1 : \mathbf{P}(v = k) > 0\}$ равен единице[3].

Отметим, что мы исключаем из рассмотрения случай $v^+ = \text{const}$ (см. (1.2)) и случай неарифметического, но решетчатого распределения.

Нас интересует асимптотическое поведение случайной последовательности $w_{0,n}$ при $n \to \infty$. Мы рассмотрим область нормальных и умеренно больших уклонений и докажем локальную предельную теорему при выполнении условия [**Z**] и интегролокальную предельную теорему при выполнении условия [**R**].

Доказательство этих утверждений разбито на два шага. На первом шаге (приведенном в § 2) мы сначала построим вложенную регенерирующую последовательность с соответствующими "весами" (воспользовавшись методами, предложенными в работах [5,6]), а затем покажем, что как длины циклов регенерации τ_k, так и соответствующие им веса циклов ζ_k имеют конечные показательные моменты (точные определения этих величин даны в § 3). Отметим, что последовательность $\{(\tau_k, \zeta_k)\}_{k=1}^{\infty}$ состоит из независимых при $k \geqslant 1$ и одинаково распределенных при $k \geqslant 2$ двумерных случайных векторов, имеющих при $k \geqslant 2$ общее распределение с вектором (τ, ζ), координаты которого, как правило, зависят друг от друга.

На втором шаге доказательства (в § 3) мы отметим, что векторы (τ_k, ζ_k) определяют стационарный обобщенный процесс восстановления (о.п.в.), при изучении которого применимы методы и результаты работы [7]. После этого мы докажем, что асимптотика в предельных теоремах для последовательности $w_{0,n}$ совпадает с такой же асимптотикой для построенного о.п.в., что завершит доказательство требуемых результатов.

Для формулировки результатов нам осталось ввести функцию уклонений для о.п.в., управляемого случайным вектором $(\tau, \zeta) \stackrel{d}{=} (\tau_2, \zeta_2)$. Для $(\lambda, \mu) \in \mathbb{R}^2$ обозначим

$$A(\lambda, \mu) := \ln \mathbf{E} e^{\lambda\tau + \mu\zeta}. \tag{1.4}$$

Рассмотрим выпуклое множество

$$\mathcal{A}^{\leqslant 0} := \{(\lambda, \mu) : \ A(\lambda, \mu) \leqslant 0\}$$

и положим

$$D(\alpha) := \sup_{(\lambda,\mu) \in \mathcal{A}^{\leqslant 0}} \{\lambda + \mu\alpha\}.$$

Функция $D(\alpha)$ играет определяющую роль в описании логарифмической асимптотики вероятностей больших уклонений о.п.в., определяемого вектором (τ, ζ), и она достаточно полно изучена (см., например, [8]). Отметим, что это выпуклая функция, принимающая неотрицательные значения и обращающаяся в 0 в единственной

[3] Условия [**R**] и [**Z**] можно также сформулировать в терминах характеристической функции $f(z) = \mathbf{E}\, e^{izv}$ случайной величины v, а именно:
[**R**] $|f(2\pi z)| < 1$ для всех $z \neq 0$;
[**Z**] $f(2\pi z) = 1$ для всех $z \in \mathbb{Z}$ и $|f(2\pi z)| < 1$ для всех $z \in \mathbb{R} \setminus \mathbb{Z}$.

точке $\alpha = a$, где

$$a = \frac{\mathbf{E}\,\zeta}{\mathbf{E}\,\tau} > 0. \tag{1.5}$$

В наших условиях функция $D(\alpha)$ аналитична в некоторой окрестности точки минимума $\alpha = a$ и при этом

$$D(a) = 0, \quad D'(a) = 0, \quad D''(a) = \frac{1}{\sigma^2},$$

где

$$\sigma^2 := \frac{\mathbf{E}(\zeta - a\tau)^2}{\mathbf{E}\,\tau}. \tag{1.6}$$

Приведем основное утверждение данной статьи.

Теорема 1. *Пусть выполнены условия* (1.2).

I. *Если случайная величина ν удовлетворяет условию* [**Z**], *то для любой последовательности $x = x_n \in \mathbb{Z}$, такой что $\alpha := x/n \to a$ при $n \to \infty$, имеет место асимптотическое соотношение*

$$\mathbf{P}(w_{0,n} = x) \sim \frac{1}{\sigma\sqrt{2\pi n}} e^{-nD(\alpha)}. \tag{1.7}$$

Если при этом $y_n := x - an = o(n^{2/3})$, то справедливо

$$\mathbf{P}(w_{0,n} = x) \sim \frac{1}{\sigma\sqrt{2\pi n}} e^{-\frac{y_n^2}{2n\sigma^2}}.$$

II. *Если случайная величина ν удовлетворяет условию* [**R**], *то для некоторой последовательности положительных чисел $\Delta_n^{(0)} = o(1)$ и для любой последовательности $x = x_n \in \mathbb{R}$, такой что $\alpha := x/n \to a$ при $n \to \infty$, имеет место асимптотическое соотношение*

$$\mathbf{P}(w_{0,n} \in [x, x + \Delta_n)) \sim \frac{\Delta_n}{\sigma\sqrt{2\pi n}} e^{-nD(\alpha)}, \tag{1.8}$$

в котором последовательность $\Delta_n = o(1)$ удовлетворяет неравенству $\Delta_n \geqslant \geqslant \Delta_n^{(0)}$ (т.е. сходится к 0 достаточно медленно).
Если при этом $y_n := x - an = o(n^{2/3})$, то справедливо

$$\mathbf{P}(w_{0,n} \in [x, x + \Delta_n)) \sim \frac{\Delta_n}{\sigma\sqrt{2\pi n}} e^{-\frac{y_n^2}{2n\sigma^2}}.$$

Замечание 1. Можно несколько усилить утверждения теоремы 1, рассмотрев наряду с нормальными и умеренно большими уклонениями вида $\alpha := x/n \to a$ большие уклонения вида $|\alpha - a| \leqslant \delta$ при некотором (вообще говоря, малом) $\delta > 0$. При этом в правых частях соотношений (1.7), (1.8) множители $\dfrac{1}{\sigma\sqrt{2\pi}}$ (константы) следует заменить на более сложные, зависящие от параметра $\alpha = x/n$ функции. Однако для вычисления этих функций необходимы дополнительные довольно громоздкие построения, поэтому мы ограничились в теореме 1 рассмотрением нормальных и умеренно больших уклонений.

Замечание 2. Утверждение теоремы 1 формулируется в терминах функции уклонений $D(\alpha)$, строящейся по распределению случайного вектора (τ, ζ), которое задается неявно и зависит от двух параметров c_1 и c_2, выбираемых произвольно из неко-

торого интервала (см. лемму 1). Однако в теореме 3 мы докажем, что результаты теоремы 1 не зависят от того, какими эти константы выбраны.

Асимптотические свойства последовательности $w_{0,n}$ при стремлении $n \to \infty$ изучались ранее в работах [5,6,9,10]. В работе [9] рассмотрен случай, когда $\mathbf{P}(v > 0) = 1$ и доказаны закон больших чисел и центральная предельная теорема при условии конечности третьего момента случайной величины v, а также получены другие предельные теоремы при отсутствии этого условия. Центральная предельная теорема для случая, когда случайная величина v может иметь произвольный знак, доказана в работе [10]. В более ранних работах [5, 6] изучались модели с весами вида (1.3). Отметим также работу [11], в которой изучаются асимптотики длины *минимального* пути из 0 в n при $n \to \infty$ для случая, когда веса постоянны, но вероятность существования ребра зависит от расстояния между вершинами и убывает к нулю при его возрастании.

Оставшаяся часть статьи включает три параграфа: в §§ 2, 3 мы доказываем основную теорему по схеме, изложенной выше, а в § 4 приводим один вспомогательный результат.

§ 2. Построение регенерирующей последовательности, изучение ее свойств

В этом параграфе мы предложим конструкцию, позволяющую задать п.н. бесконечное случайное множество вершин $\{\Gamma_i\}_{i\in\mathbb{Z}}$ (называемых нами в дальнейшем *стержневыми вершинами* – см. определение 3 ниже), где $\ldots < \Gamma_{-2} < \Gamma_{-1} < 0 \leqslant \leqslant \Gamma_0 < \Gamma_1 < \ldots$, обладающих следующими свойствами:

1. Последовательность двумерных векторов

$$(\Gamma_n - \Gamma_{n-1}, w_{\Gamma_{n-1},\Gamma_n}), \quad n \neq 0, \tag{2.1}$$

состоит из независимых и одинаково распределенных элементов, которые в совокупности не зависят от $(\Gamma_{-1}, \Gamma_0, w_{\Gamma_{-1},0}, w_{0,\Gamma_0})$. Используя язык случайных точечных процессов, можно сказать, что последовательность пар $\{(\Gamma_n, w_{\Gamma_{n-1},\Gamma_n})\}$ образует стационарный в дискретном времени маркированный точечный процесс с марками $\{w_{\Gamma_{n-1},\Gamma_n}\}$, определяющий стационарный о.п.в.

2. При некотором $C > 0$ все четыре экспоненциальных момента

$$\mathbf{E}\exp(C\Gamma_0), \quad \mathbf{E}\exp(C(\Gamma_1 - \Gamma_0)), \quad \mathbf{E}\exp(Cw_{0,\Gamma_0}), \quad \mathbf{E}\exp(Cw_{\Gamma_0,\Gamma_1}) \tag{2.2}$$

конечны. При этом для $C_1 = C/2$ с необходимостью конечны и моменты

$$\mathbf{E}\exp(C_1(\Gamma_0 + w_{0,\Gamma_0})) \quad \text{и} \quad \mathbf{E}\exp(C_1(\Gamma_1 - \Gamma_0 + w_{\Gamma_0,\Gamma_1})). \tag{2.3}$$

3. При любых $0 \leqslant m \leqslant n$, если $\Gamma_m \leqslant n$, то

$$w_{0,n} = w_{0,\Gamma_0} + w_{\Gamma_0,\Gamma_1} + \ldots + w_{\Gamma_{m-1},\Gamma_m} + w_{\Gamma_m,n} \tag{2.4}$$

(напомним, что мы полагаем $w_{j,j} = 0$ при любом $j \in \mathbb{Z}$).

Приведем также ряд вспомогательных утверждений. Мы будем частично использовать схему доказательства из работы [9], где рассматривались веса, принимающие только положительные значения либо значение $-\infty$, и изучались вопросы существования первых и вторых степенных моментов у величин Γ_0 и w_{0,Γ_0}.

2.1. Построение осевых и стержневых вершин. Мы последовательно введем в рассмотрение четыре случайных подмножества множества вершин $\mathbb{Z}$: множество осевых вершин $\mathcal{S}$, осевых-плюс $\mathcal{S}^+$, стержневых $\mathcal{R}$ и стержневых-плюс $\mathcal{R}^+$.

О п р е д е л е н и е 1. Назовем вершину $x \in \mathbb{Z}$ *осевой*, если она связана путями конечного веса с каждой из других вершин, т.е. для любых $j < x$ и $k > x$ выполнены

неравенства $w_{j,x} > -\infty$ и $w_{x,k} > -\infty$. Обозначим через $\mathcal{S}$ случайное множество осевых точек.

Если $p = \mathbf{P}(v > -\infty) = 1$, то любая точка $x \in \mathbb{Z}$ является осевой. Если p – любое число из интервала $(0, 1)$, то, как следует из лемм 5–7 работы [6], верны следующие пять утверждений.

1. Вероятность того, что вершина x является осевой, строго положительна и одна и та же при всех $x \in \mathbb{Z}$.
2. Последовательность событий $\{x \in \mathcal{S}\}$, $x = \ldots, -2, -1, 0, 1, 2, \ldots$, является стационарной эргодической, и поэтому с вероятностью единица существует почти наверное бесконечно много осевых вершин $\{t_i\}$.
3. Последовательность $\{t_i\}$ (где $\ldots t_{-2} < t_{-1} < 0 \leqslant t_0 < t_1 < \ldots$) образует стационарный процесс восстановления (в дискретном времени), и в частности, длительности интервалов между соседними точками $\{t_i - t_{i-1},\ i \in \mathbb{Z},\ i \neq 0\}$ являются независимыми и одинаково распределенными случайными величинами и не зависят от пары случайных величин (t_{-1}, t_0), а эти величины зависят друг от друга, и t_0 имеет то же распределение, что и $|t_{-1}| - 1$. При этом $\mathbf{P}(t_{-1} = -i) = \mathbf{P}(t_1 - t_0 \geqslant i)/\,\mathbf{E}(t_1 - t_0)$, $i = 1, 2, \ldots$
4. При некотором $C > 0$

$$\mathbf{E}\, e^{Ct_0} < \infty, \quad \text{и следовательно,} \quad \mathbf{E}\, e^{C(t_1 - t_0)} < \infty. \tag{2.5}$$

5. Для любых $j < k$ обозначим через

$$L_{j,k} = \max_{\pi \in \Pi_{j,k}} L(\pi) \quad (\text{где максимум по пустому множеству равен } -\infty)$$

максимальную длину пути среди всех путей из $\Pi_{j,k}$. Тогда при каждом $n > 0$, если $L_{0,n} > 0$, то любой путь длины $L_{0,n}$ из 0 в n должен проходить через все промежуточные осевые точки (если таковые имеются). А именно пусть $0 \leqslant t_0 < t_1 < \ldots < t_m \leqslant n < t_{m+1}$ при некотором $m \geqslant 0$. Тогда любой путь максимальной длины из 0 в n, принадлежащий множеству $\Pi_{0,n}$, должен проходить через каждую из вершин $t_0, \ldots, t_m$. При этом с необходимостью все значения $L_{t_0,t_1}, \ldots, L_{t_{m-1},t_m}$ строго положительны и

$$L_{0,n} = L_{0,t_0} + L_{t_0,t_1} + \ldots + L_{t_{m-1},t_m} + L_{t_m,n}.$$

Наряду с введенным в § 1 классом путей $\Pi_{j,k}$, использующих только ребра с конечными весами, введем также множество путей $\Pi^+_{j,k}$ из j в k, использующих только ребра с положительными весами (т.е. $v_e > 0$ для всех $e \in \pi$, если $\pi \in \Pi^+_{j,k}$), и положим

$$w^+_{j,k} := \max_{\pi \in \Pi^+_{j,k}} w(\pi).$$

Определение 2. Назовем вершину $x \in \mathbb{Z}$ *осевой-плюс*, если она связана с каждой из других вершин путями, использующими только ребра положительного веса, т.е. для любых $j < x$ и $k > x$ найдутся путь π из j в x и путь $\widetilde{\pi}$ из x в k, такие что $v_e > 0$ при всех $e \in \pi$ и всех $e \in \widetilde{\pi}$ и, в частности, выполнены неравенства $w^+_{j,x} > 0$ и $w^+_{x,k} > 0$. Обозначим через $\mathcal{S}^+ = \{t^+_i\}$ множество осевых-плюс точек.

Отметим, что так как мы предполагаем, что $p^+ > 0$, то результаты работы [6] применимы и к множеству $\mathcal{S}^+$, и в частности, (2.5) остается справедливым при замене $\{t_i\}$ на $\{t^+_i\}$.

Теперь мы определим множества $\mathcal{R}$ *стержневых* и $\mathcal{R}^+$ *стержневых-плюс* вершин. Пусть $c_1 \geqslant c_2 > 0$ – фиксированные числа. Для $x \in \mathbb{Z}$ определим следующие

события:

$$A_x^r(c_1) = \bigcap_{i=1}^{\infty}\{w_{x,x+i} \geqslant c_1 i\},$$

$$A_x^0(c_2) = \bigcap_{j,i=1}^{\infty}\{v_{x-j,x+i} < c_2(j+i)\},$$

$$A_x^l(c_1) = \bigcap_{j=1}^{\infty}\{w_{x-j,x} \geqslant c_1 j\}.$$

Здесь событие $A_x^r(c_1)$ означает, что вершина x соединена путями конечного веса со всеми вершинами, находящимися справа от нее, и более того, все соответствующие максимальные веса путей строго положительны и растут по крайней мере линейно (со скоростью не меньшей c_1) с ростом расстояния от вершины x. Аналогично, событие $A_x^l(c_1)$ означает, что вершина x соединена путями конечного веса со всеми вершинами, находящимися слева от нее, и более того, все соответствующие максимальные веса путей строго положительны и растут по крайней мере линейно с ростом расстояния от вершины x. В частности, если происходят оба события $A_x^r(c_1)$ и $A_x^l(c_1)$, то вершина x является с необходимостью осевой, и к тому же $w_{x-j,x+i} \geqslant c_1(j+i)$ при всех $j, i \geqslant 0$. А если к тому же происходит и событие $A_x^0(c_2)$, то так как $c_2 \leqslant c_1$, то с необходимостью при любых $j, i \geqslant 0$ любой путь максимального веса из вершины $x-j$ в вершину $x+i$ обязан проходить через вершину x.

Определение 3. Назовем вершину x *стержневой*, если происходят все три события $A_x^l(c_2)$, $A_x^0(c_1)$ и $A_x^r(c_2)$, и пусть $\mathcal{R} = \{\Gamma_i\}$ – случайное множество стержневых вершин.

Так как события $\{x \in \mathcal{R}\}$ образуют стационарную эргодическую последовательность, то выполнен "закон нуля или единицы": либо с вероятностью единица множество $\mathcal{R}$ бесконечно, либо с вероятностью единица пусто. Предположим, что это множество бесконечно на некотором элементарном исходе. Тогда его элементы можно упорядочить:

$$\ldots < \Gamma_{-1} < 0 \leqslant \Gamma_0 < \Gamma_1 < \ldots,$$

и имеет место представление (2.4). Именно это свойство помогает нам в изучении асимптотики последовательности $w_{0,n}$ при стремлении n к бесконечности.

Введем по аналогии события

$$A_x^{r+}(c_1) = \bigcap_{i=1}^{\infty}\{w^+_{x,x+i} \geqslant c_1 i\},$$

$$A_x^{0+}(c_2) \equiv A_x^0(c_2) = \bigcap_{j,i=1}^{\infty}\{v_{x-j,x+i} < c_2(j+i)\},$$

$$A_x^{l+}(c_1) = \bigcap_{j=1}^{\infty}\{w^+_{x-j,x} \geqslant c_1 j\}.$$

Здесь событие $A_x^{r+}(c_1)$ означает, что вершина x соединена путями, использующими только ребра с положительными весами, со всеми вершинами, находящимися справа от нее, и более того, все соответствующие максимальные веса путей строго положительны и растут по крайней мере линейно с ростом расстояния от вершины x. Аналогично, событие $A_x^{l+}(c_1)$ означает, что вершина x соединена путями, использующими только ребра с положительными весами, со всеми вершинами, находящимися

слева от нее, и более того, все соответствующие максимальные веса путей строго положительны и растут по крайней мере линейно с ростом расстояния от вершины x. С необходимостью $A_x^{l+}(c_1) \subseteq A_x^l(c_1)$ и $A_x^{r+}(c_1) \subseteq A_x^r(c_1)$ при любом $c_1 > 0$.

Определение 4. Назовем вершину x *стержневой-плюс*, если происходит событие $A_x^{l+}(c_1) \cap A_x^{0+}(c_2) \cap A_x^{r+}(c_1)$, и обозначим через $\mathcal{R}^+$ множество всех стержневых-плюс вершин. Это множество также либо п.н. бесконечно, либо п.н. пусто.

Отметим, что имеют место соотношения

$$\mathcal{R}^+ \subseteq \mathcal{R} \subseteq \mathcal{S} \quad \text{и} \quad \mathcal{R}^+ \subseteq \mathcal{S}^+ \subseteq \mathcal{S}. \tag{2.6}$$

Кроме этого, множества $\mathcal{R}$ и $\mathcal{R}^+$ монотонно возрастают с ростом c_2 и убыванием c_1.

2.2. Регенерирующая структура и существование показательных моментов. Для формулировки следующего утверждения нам понадобится распределение случайной величины v^+, заданное в (1.1). Пусть $\operatorname{ess\,inf} v^+ = \inf\{t > 0 : \mathbf{P}(v^+ < t) > 0\}$ и $V = \mathbf{E} \min\limits_{t_0^+ \leqslant i < j \leqslant t_1^+} v_{i,j}^+$. Ясно, что $\operatorname{ess\,inf} v^+ < V$, если распределение случайной величины v^+ невырождено. Положим $\gamma^+ = \dfrac{1}{\mathbf{E}(t_1^+ - t_0^+)}$. Из лемм 5–7 работы [6] вытекает следующее утверждение.

Лемма 1. *Пусть выполнено условие* (1.2). *Тогда если*

$$\gamma^+ \operatorname{ess\,inf} v^+ < c_2 \leqslant c_1 < \gamma^+ V, \tag{2.7}$$

то для любого $x \in \mathbb{Z}$ *выполнено неравенство* $\mathbf{P}(A_x^{l+}(c_1) \cap A_x^0(c_2) \cap A_x^{r+}(c_1)) > 0$ *и множество* $\mathcal{R}^+$ *бесконечно с вероятностью* 1. *Следовательно, и множество* $\mathcal{R}$ *также бесконечно с вероятностью* 1.

Замечание 3. В работе [6] стержневые точки вводились при $c_1 = c_2$ и соответствующие утверждения формулировались только в этом случае. Однако их доказательства не претерпевают никаких изменений (кроме небольших изменений в обозначениях) при выполнении более общих условий (2.7).

Определим циклы

$$\mathcal{C}_k^+ := \Big(\Gamma_k^+ - \Gamma_{k-1}^+;\ \Big\{v^+_{\Gamma^+_{k-1+j},\Gamma^+_{k-1+i}},\ 0 \leqslant j < i \leqslant \Gamma_k^+ - \Gamma_{k-1}^+\Big\}\Big), \quad k \in \mathbb{Z},$$

и

$$\mathcal{C}_k := \big(\Gamma_k - \Gamma_{k-1};\ \{v_{\Gamma_{k-1+j},\Gamma_{k-1+i}},\ 0 \leqslant j < i \leqslant \Gamma_k - \Gamma_{k-1}\}\big), \quad k \in \mathbb{Z}.$$

Имеет место следующая

Лемма 2. *При выполнении условий* (1.2) *и* (2.7) *справедливы следующие два утверждения*:

(I) *Случайные элементы* $\{\mathcal{C}_k^+,\ k \in \mathbb{Z}\}$ *независимы в совокупности, причем элементы* $\{\mathcal{C}_k^+,\ k \in \mathbb{Z} \setminus \{0\}\}$ *одинаково распределены. Процесс* $\Big(\Gamma_k^+, w^+_{\Gamma^+_{k-1},\Gamma^+_k}\Big)$, $k \in \mathbb{Z}$, *является стационарным маркированным точечным процессов в дискретном времени, порождающим стационарный о.п.в., т.е. его первые координаты* Γ_k^+ *образуют стационарный точечный процесс с соответствующими метками* $w^+_{\Gamma^+_{k-1},\Gamma^+_k}$.

(II) *Утверждение* (I) *остается верным для циклов* $\mathcal{C}_k$ *при естественной замене* Γ_k^+ *на* Γ_k *и* $w^+_{\Gamma^+_{k-1},\Gamma^+_k}$ *на* $w_{\Gamma_{k-1},\Gamma_k}$.

Отметим, что утверждение (I) является прямым следствием леммы 3.8 работы [9] и что схемы доказательств утверждений (I) и (II) идентичны.

Докажем теперь первое из основных утверждений этого параграфа.

Лемма 3. *Пусть выполнены условия* (1.2) *и* (2.7). *Тогда найдется константа* $C > 0$, *такая что*

$$\mathbf{E}\, e^{C\Gamma_0^+} < \infty, \quad \textit{и следовательно,} \quad \mathbf{E}\, e^{C(\Gamma_1^+ - \Gamma_0^+)} < \infty. \tag{2.8}$$

Так как последовательность $\{\Gamma_n^+\}$ *является подпоследовательностью последовательности* $\{\Gamma_n\}$, *то утверждение* (2.8) *остается верным и при замене* Γ_0^+ *и* Γ_1^+ *на, соответственно,* Γ_0 *и* Γ_1, *т.е. при некотором* $C > 0$ *конечны два первых математических ожидания в* (2.2).

Доказательство. Мы позаимствуем из работы [9] ряд вспомогательных построений. Определим множество $\mathcal{U} = \{x \in \mathbb{Z} :\ \mathbf{I}(A_x^{l+}(c_1)) = 1\}$. Нетрудно видеть, что $\mathcal{R}^+ \subseteq \mathcal{U}$. Обозначим через $\ldots, \rho_{-1}, \rho_0, \rho_1, \ldots$ возрастающую последовательность точек множества $\mathcal{U}$, где ρ_0 – его наименьший неотрицательный элемент. Зададим новую последовательность циклов: при $k \in \mathbb{Z}$

$$\mathcal{D}_k = \big(\rho_k - \rho_{k-1};\ \big\{v^+_{\rho_{k-1}+j,\rho_{k-1}+i},\ 0 \leqslant j < i \leqslant \rho_k - \rho_{k-1}\big\}\big).$$

Из леммы 3.10 работы [9] вытекает следующее утверждение.

Лемма 4. *Пусть выполнены условия* (1.2) *и* (2.7). *Тогда циклы* $(\mathcal{D}_k,\ k \in \mathbb{Z})$ *независимы, причем* $(\mathcal{D}_k,\ k \in \mathbb{Z} \setminus \{0\})$ *одинаково распределены, а последовательность* ρ_n, $n \in \mathbb{Z}$, *образует стационарный точечный процесс, порождающий стационарный процесс восстановления.*

Утверждение леммы 4 несложно пояснить “на пальцах”. Введем для этого при $d > 0$ события

$$A^{l+}_{x,d}(c_1) := \bigcap_{j=1}^{d} \big\{w^+_{x-j,x} \geqslant c_1 j\big\}.$$

Отметим, что при любых целых $k \geqslant 0$ и $0 \leqslant s_0 < s_1 < \ldots < s_k$ событие $\{\rho_0 = s_0, \ldots, \rho_k = s_k\}$ однозначно определяется набором случайных величин $\mathcal{B}_{s_k} := \{v_{i,j},\ i < j \leqslant s_k\}$, и на этом событии равенство $\rho_{k+1} - \rho_k = m$ выполняется тогда и только тогда, когда $m = \min\big\{d > 0 :\ \mathbf{I}\big(A^{l+}_{s_k,s_k+d}(c_1)\big) = 1\big\}$, что определяется случайными величинами $\mathcal{B}_{s_k,s_k+m} := \{v^+_{i,j},\ s_k \leqslant i < j \leqslant m\}$. Нетрудно видеть, что семейства $\mathcal{B}_{s_k}$ и $\mathcal{B}_{s_k,s_k+m}$ не зависят друг от друга и к тому же распределение величин $\mathcal{B}_{s_k,s_k+m}$ не зависит от k и s_k, – это, по сути, и влечет утверждение леммы 4.

Введем также при $d > 0$ вспомогательные события

$$A^{r+}_{x,d}(c_1) := \bigcap_{i=1}^{d} \{w^+_{x,x+i} \geqslant c_1 i\},$$

$$A^{0+}_{x,d}(c_2) := \bigcap_{1 \leqslant i \leqslant d,\ j \geqslant 1}^{\infty} \{v_{x-j,x+i} < c_2(j+i)\}.$$

Положим $\mu = \inf\big\{d > 0 :\ \mathbf{I}\big(A^{0+}_{0,d}(c_2) \cap A^{r+}_{0,d}(c_1)\big) = 0\big\}$. Отметим, что $\mathbf{P}(\mu = \infty) = \mathbf{P}(A^{0+}_0(c_2) \cap A^{r+}_0(c_1)) > 0$. Зададим теперь последовательно случайные величины $\sigma_0, \mu_0, \ldots, \sigma_K, \mu_K$, где $K = \min\{k \geqslant 0 :\ \mu_k = \infty\}$. Положим

$$\sigma_0 = \rho_0, \quad \mu_0 = \inf\Big\{d > 0 :\ \mathbf{I}\big(A^{0+}_{\sigma_0,\sigma_0+d}(c_2) \cap A^{r+}_{\sigma_0,\sigma_0+d}(c_1)\big) = 0\Big\},$$

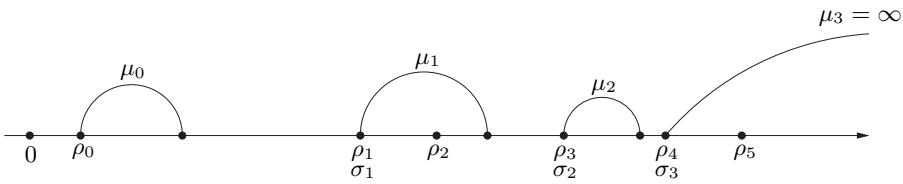

Рис. 1. Процесс построения последовательности σ_k. Изображен случай, когда $K = 3$; в изображенном случае $\sigma_3 = \rho_4$ – момент регенерации, который является оценкой сверху для Γ_0

и при $k = 0, 1, \ldots$, если $\mu_k < \infty$, то

$$\sigma_{k+1} = \inf\{x \in \mathcal{U} :\ x \geqslant \sigma_k + \mu_k\},$$
$$\mu_{k+1} = \inf\Big\{d > 0 :\ \mathbf{I}\big(A^{0+}_{\sigma_k,\sigma_k+d}(c_2) \cap A^{r+}_{\sigma_k,\sigma_k+d}(c_1)\big) = 0\Big\}.$$

Более наглядно процесс построения этой последовательности приведен на рис. 1.

Как следует из построения, $\sigma_k \in \mathcal{U}$ при $k \leqslant K$ и $\sigma_K \in \mathcal{R}^+$, и значит, $\sigma_K \geqslant \Gamma_0^+$ п.н. Кроме того, случайные величины $\{\mu_k\}$ образуют последовательность независимых и одинаково распределенных случайных величин, имеющих то же распределение, что и μ. Поэтому случайная величина K имеет геометрическое распределение с параметром q, и в частности, ее показательные моменты $\mathbf{E}\, e^{CK} < \infty$ конечны при $C < -1/\ln q$. Кроме этого, при любом $k \geqslant 1$ при условии $\{K = k\}$ случайные величины $\mu_0, \ldots, \mu_{k-1}$ условно независимы и распределены как $\mathbf{P}(\mu_0 \in \cdot \,|\, \mu_0 < \infty)$.

В силу того, что $\rho_k - \rho_{k-1} \geqslant 1$,

$$\sigma_K \leqslant \rho_M = \rho_0 + \sum_{k=1}^{M} (\rho_k - \rho_{k-1}), \tag{2.9}$$

где $M := \sum\limits_{j=0}^{K-1} \mu_j$.

Поэтому если мы покажем, что выражение в правой части (2.9) имеет конечный показательный момент, то конечный показательный момент будет иметь также и σ_K, и из этого будет следовать утверждение леммы 3. С учетом леммы 9 из § 4 и элементарного неравенства $e^{x+y} < e^{2x} + e^{2y}$ при $x, y \geqslant 0$ нам достаточно показать, что, во-первых, случайная величина $\rho_1 - \rho_0$ имеет конечный показательный момент (поэтому конечный показательный момент будет существовать и у ρ_0), и во-вторых, вероятности $\mathbf{P}(\mu_0 = m \,|\, \mu_0 < \infty)$ убывают экспоненциально быстро по m.

В силу независимости ρ_0 и $\rho_1 - \rho_0$ и в силу того, что при каждом целом $n > 0$ при выполнении события $A_0^{l+}(c_1)$ события $A_n^{l+}(c_1)$ и $A_{n,n}^{l+}(c_1)$ либо происходят, либо не происходят одновременно, мы получаем, что распределения случайных величин $\rho_1 - \rho_0$ и $\nu := \min\{n :\ \mathbf{I}(A_{n,n}^{l+}(c_1)) = 1\}$ совпадают:

$$\mathbf{P}(\rho_1 - \rho_0 = m) = \mathbf{P}(\rho_1 - \rho_0 = m \,|\, \rho_0 = 0) = \mathbf{P}(\nu = m \,|\, \rho_0 = 0) = \mathbf{P}(\nu = m),$$
$$m = 1, 2, \ldots,$$

а существование показательного момента у случайной величины ν следует из предложения 3.12 работы [9].

Далее,

$$\mathbf{P}(\mu = d) = \mathbf{P}\Big(\big(A^{0+}_{0,d}(c_2) \cap A^{r+}_{0,d}(c_1)\big)^c \cap \big(A^{0+}_{0,d-1}(c_2) \cap A^{r+}_{0,d-1}(c_1)\big)\Big) \leqslant$$

$$\leqslant \mathbf{P}\Big(\big(A^{0+}_{0,d}(c_2)\big)^c \cap A^{0+}_{0,d-1}(c_2)\Big) + \mathbf{P}\Big(\big(A^{r+}_{0,d}(c_1)\big)^c \cap A^{r+}_{0,d-1}(c_1)\Big) \leqslant$$
$$\leqslant \mathbf{P}\Big(\sup_{j\geqslant 1}\big(v^+_{-j,d} - c_2 j\big) > c_2 d\Big) + \mathbf{P}(w^+_{0,d} < c_1 d) \leqslant$$
$$\leqslant \sum_{j=1}^{\infty} \mathbf{P}\big(v > c_2(d+j)\big) + \mathbf{P}\big(w^+_{0,d} < c_1 d\big).$$

В последнем выражении сумма вероятностей $\sum\limits_{j=1}^{\infty} \mathbf{P}(v > c_2(d+j))$ убывает по d экспоненциально быстро в силу (1.2). Чтобы показать, что последняя вероятность также убывает экспоненциально быстро, мы найдем $\varepsilon > 0$, такое что $\widetilde{c} := c_1(1+3\varepsilon)$ также удовлетворяет (2.7). Положим $\eta(d) = \max\{k : t^+_k \leqslant d\}$ (где максимум по пустому множеству полагается равным $-\infty$). Тогда при $r = \gamma^+(1+\varepsilon)^{-1}$

$$\mathbf{P}\big(w^+_{0,d} < c_1 d\big) \leqslant \mathbf{P}(t^+_0 > d) + \mathbf{P}\Big(w^+_{t^+_0, t^+_{\eta(d)}} < c_1 d,\ t^+_0 \leqslant d\Big) \leqslant$$
$$\leqslant \mathbf{P}(t^+_0 > d) + \mathbf{P}\big(\eta(d) < [rd]\big) + \mathbf{P}\left(\sum_{i=1}^{[rd]} w^+_{t_{i-1},t_i} < c_1 d\right) \leqslant$$
$$\leqslant \mathbf{P}(t^+_0 > d) + \mathbf{P}\left(\sum_{1}^{[rd]} (t^+_i - t^+_{i-1}) > d\right) + \mathbf{P}\left(\sum_{i=1}^{[rd]} w^+_{t_{i-1},t_i} < c_1 d\right),$$

где $[rd]$ – целая часть числа rd. В последней строке все слагаемые убывают экспоненциально быстро по d: первое слагаемое потому, что t^+_0 имеет конечный показательный момент, а второе слагаемое – потому, что $t^+_i - t^+_{i-1}$ имеют конечный показательный момент, $\mathbf{E}(t^+_1 - t^+_0)r < 1$, и следовательно, по экспоненциальному неравенству Чебышева при $h > 0$

$$\mathbf{P}\left(\sum_{i=1}^{[rd]} (t^+_i - t^+_{i-1}) > d\right) \leqslant \Big(\big(\mathbf{E}\exp\big(h(t^+_1 - t^+_0)\big)\big)^r e^{-h}\Big)^d,$$

где правая часть неравенства убывает экспоненциально быстро по d, если взять h достаточно малым. Наконец, третье слагаемое убывает экспоненциально быстро, потому что, как хорошо известно, для любой последовательности независимых одинаково распределенных положительных случайных величин $X, X_1, X_2, \ldots$ с конечным средним $\mathbf{E}\,X$ и для любого $\delta \in (0,1)$ вероятности $\mathbf{P}\Big(\sum\limits_{i=1}^{n} X_i < (1-\delta)n\,\mathbf{E}\,X\Big)$ убывают экспоненциально быстро с ростом n. В нашем случае $n = [rd] \geqslant rd - 1$, $X_i = w_{t^0_{i-1},t^0_i}$, $\mathbf{E}\,w_{t^+_0,t^+_1} \geqslant V$ и $c_1 d \leqslant c_1(1+n)(1+\varepsilon)/\gamma^+ \leqslant c_1(1+2\varepsilon)nV/\gamma^+ < (1-\delta)nV$ при достаточно больших n, где $\delta = \varepsilon/(1+3\varepsilon)$.

Значит, вероятности $\mathbf{P}(\mu = d)$, а следовательно, и $\mathbf{P}(\mu = d \,|\, \mu < \infty)$ убывают экспоненциально быстро с ростом d. Это завершает доказательство леммы 3. ▲

Приведем теперь доказательство конечности последних двух математических ожиданий в (2.2).

Лемма 5. *Пусть выполнены условия* (1.2) *и* (2.7). *Тогда* $\mathbf{E}\exp(Cw_{0,\Gamma_0})$, *и следовательно,* $\mathbf{E}\exp(Cw_{\Gamma_0,\Gamma_1})$ *конечны при некотором* $C > 0$.

Доказательство. Выберем произвольный путь π из вершины 0 в вершину Γ_0 и предположим, что он включает в себя $d+1$ вершину, $0 = x_0 < x_1 < \ldots < x_d = \Gamma_0$.

Так как $\sum\limits_{k=1}^{d}(x_k - x_{k-1}) = \Gamma_0$, то

$$w_{0,\Gamma_0} = \sum_{k=1}^{d} v_{x_{k-1},x_k} \leqslant \Gamma_0 + \sum_{k=1}^{d}(v_{x_{k-1},x_k} - (x_k - x_{k-1}))^+ \leqslant$$
$$\leqslant \Gamma_0 + \sum_{0\leqslant x<y\leqslant\Gamma_0}(v_{x,y} - (y-x))^+ \leqslant \Gamma_0 + \sum_{x=0}^{\Gamma_0-1} Z_x, \tag{2.10}$$

где $\{Z_x := \max\limits_{y>x}(v_{x,y} - (y-x))^+\}_{x\in\mathbb{Z}}$ – последовательность независимых и одинаково распределенных неотрицательных случайных величин. В силу условия (1.2) хвост распределения

$$\mathbf{P}(Z_0 > m) \leqslant \sum_{k=1}^{\infty}\mathbf{P}(v > m+k)$$

убывает экспоненциально быстро с ростом m. Для завершения доказательства осталось опять воспользоваться элементарным неравенством $e^{x+y} < e^{2x} + e^{2y}$ и леммой 9. ▲

Мы завершим § 2 коротким доказательством одного простого факта, который понадобится нам в следующем параграфе.

Лемма 6. *Пусть* $p \in (0,1]$, *и пусть выполнены условия* (1.2) *и* (2.7). *Тогда* $\mathbf{P}(\Gamma_1 - \Gamma_0 = 1,\ w_{\Gamma_0,\Gamma_1} \geqslant y) > 0$ *для* $y \in (c_2, \operatorname{ess\,sup} v^+)$.

Доказательство. Следующие два события совпадают:

$$\{\Gamma_0 = 0,\ \Gamma_1 - \Gamma_0 = 1,\ w_{\Gamma_0,\Gamma_1} \geqslant y\} =$$
$$= A_0^l(c_1) \cap A_{0,1}^{0+}(c_2) \cap \{v_{0,1} \geqslant y\} \cap B_{1,1}(c_2) \cap A_1^r(c_1), \tag{2.11}$$

где

$$B_{1,1}(c_2) = \bigcap_{j=1}^{\infty}\{v_{0,1+j} < c_2(1+j)\},$$

при этом все пять событий в правой части представления (2.11) взаимно независимы и каждое имеет положительную вероятность. ▲

§ 3. Изучение обобщенного процесса восстановления и доказательство основной теоремы

В этом параграфе мы изучим о.п.в., порожденный стационарным маркированным точечным процессом $(\Gamma_k, w_{\Gamma_{k-1},\Gamma_k})$, $k \in \mathbb{Z}$. Используя результаты предыдущего параграфа и работы [7], а также классическую теорему Стоуна [12], мы покажем, что построенный для произвольных фиксированных допустимых констант c_1, c_2 о.п.в. и последовательность $w_{0,n}$ имеют одинаковую точную асимптотику в области нормальных и умеренно больших уклонений (результат теоремы 1). При этом, чтобы убрать "недоскок" о.п.в., будет произведено преобразование исходной меры. Утверждение о том, что характеристики α, σ^2 и $D(\alpha)$ в теореме 1 на самом деле не зависят от выбора констант c_1 и c_2, завершает нашу статью.

Далее нам будет удобно использовать краткие обозначения, унифицированные с обозначениями работы [7]:

$$(\tau_k, \boldsymbol{u}_k) := (\tau_k, (u_{k,1}, \dots, u_{k,\tau_k})), \quad k = 1, 2, \dots, \tag{3.1}$$

где

$$(\tau_1, (u_{1,1}, \dots, u_{1,\tau_1})) := (\Gamma_0, (w_{0,1}, \dots, w_{0,\Gamma_0})),$$
$$(\tau_k, (u_{k,1}, \dots, u_{k,\tau_k})) := (\Gamma_{k-1} - \Gamma_{k-2}, (w_{\Gamma_{k-2},\Gamma_{k-2}+1}, \dots, w_{\Gamma_{k-2},\Gamma_{k-1}})) \quad \text{при } k \geqslant 2.$$

Как было показано в § 2, векторы $(\tau_k, \boldsymbol{u}_k)$, $k \geqslant 2$, имеют одинаковое распределение, и мы будем использовать обозначение

$$(\tau, \boldsymbol{u}) := (\tau,\ (u_1, \dots, u_\tau)) \tag{3.2}$$

для любого вектора с этим распределением. Положим также $\zeta = u_\tau$ и $\zeta_k = u_{\tau_k}$, $k \geqslant 1$. Тогда, в частности, $\{(\tau_k, \zeta_k)\}$ – последовательность независимых случайных векторов, имеющих при $k \geqslant 2$ общее распределение с вектором (τ, ζ).

Перечислим утверждения из § 2 (основанные на леммах 2, 3, 5 и 6), которые нам сейчас потребуются. Пусть $p \in (0, 1]$ и c_1, c_2 удовлетворяют условию (2.7).

S_{I}. Последовательность (3.1) является последовательностью независимых векторов; при $k \geqslant 2$ векторы $(\tau_k, \boldsymbol{u}_k)$ имеют общее распределение.

S_{II}. Случайные величины u_{1,τ_1} и $u_1, \dots, u_\tau$ положительны, и при этом

$$\max\{u_1, \dots, u_{\tau-1}\} \leqslant u_\tau.$$

S_{III}. Найдется $C > 0$, такое что

$$\mathbf{E}\, e^{C\tau_1} < \infty, \quad \mathbf{E}\, e^{C\tau} < \infty, \quad \mathbf{E}\, e^{Cu_{1,\tau_1}} < \infty, \quad \mathbf{E}\, e^{Cu_\tau} < \infty.$$

S_{IV}. Вероятность $\mathbf{P}(\tau = 1, u_\tau \geqslant y)$ строго положительна при $y \in (c_2, \operatorname{ess\,sup} v^+)$.

Обозначим

$$(\tau, \zeta) := (\tau, u_\tau), \quad (\tau_k, \zeta_k) := (\tau_k, u_{k,\tau_k}), \quad k = 1, 2, \dots \tag{3.3}$$

Тогда последовательность $\{(\tau_k, \zeta_k)\}$ – это последовательность независимых случайных векторов, имеющих при $k \geqslant 2$ общее распределение с вектором (τ, ζ).

Из перечисленных утверждений вытекает

Следствие 1. *Пусть выполнены условия* (1.2) *и* (2.7). *Тогда справедливы следующие утверждения.*

(I) *Если для случайной величины v выполнено условие* [**Z**], *то для случайного вектора (τ, ζ) выполнено условие*

[**ZZ**] *Распределение случайного вектора является арифметическим и сосредоточено на решетке с шагом* 1 *по каждой из координат.*

(II) *Если для случайной величины v выполнено условие* [**R**], *то для случайного вектора (τ, ζ) выполнено условие*

[**ZR**] *Маргинальное распределение первой координаты вектора является арифметическим с шагом* 1, *а маргинальное распределение второй координаты – нерешетчатым*[4].

Перейдем теперь к доказательству основного результата.

Доказательство теоремы 1. Рассмотрим последовательность $\{(\tau_k, \zeta_k)\}_{k=1}^{\infty}$ независимых случайных векторов, имеющих при $k \geqslant 2$ общее распределение с вектором (τ, ζ) (см. формулу (3.2) и обозначения после нее). Введем последовательности

[4] В терминах характеристической функции $f(z, l) := \mathbf{E}\, e^{iz\tau + il\zeta}$ случайного вектора (τ, ζ) эти два условия имеют следующий вид:
[**ZZ**] $f(2\pi z, 2\pi t) = 1$ для любого $(z, t) \in \mathbb{Z}^2$, $|f(z, t)| < 1$ для любого $(z, t) \notin \mathbb{Z}^2$.
[**ZR**] $f(2\pi z, 0) = 1$ для любого $z \in \mathbb{Z}$, $|f(2\pi z, 0)| < 1$ для любого $z \notin \mathbb{Z}$ и $|f(0, t)| < 1$ для любого $t \neq 0$.

частичных сумм

$$T_n := \sum_{k=0}^{n} \tau_k, \quad Z_n := \sum_{k=0}^{n} \zeta_k, \quad n \geqslant 0,$$

где $(\tau_0, \zeta_0) := (0, 0)$. Пусть

$$\eta_+(n) := \min\{k \geqslant 1 : \, T_k > n\}, \quad \nu_+(n) := \max\{k \geqslant 0 : \, T_k \leqslant n\} = \eta_+(n) - 1,$$
$$\gamma_+(n) := n - \nu_+(n).$$

Определим о.п.в. (так называемый "первый о.п.в."), положив

$$Z_+(n) := \sum_{k=0}^{\nu_+(n)} \zeta_k.$$

Поясним, что здесь мы используем обозначение $Z_+(n)$ с нижним индексом $+$ исключительно для того, чтобы согласовать наши обозначения с обозначениями работы [7], в которой наряду с обозначениями $Z_+(n)$, $\nu_+(n)$, $\gamma_+(n)$ использовались обозначения $Z(n)$, $\nu(n)$, $\gamma(n)$, т.е. этот индекс никак не связан с $w^+_{j,m}$.

Используя введенные обозначения, получаем представление

$$w_{0,n} = Z_+(n) + w_{n-\gamma_+(n),n} = Z_{\nu_+(n)} + w_{\nu_+(n),n}.$$

Рассмотрим случайный вектор (случайной длины), заданный формулой (3.2):

$$(\tau, (u_1, u_2, \cdots, u_\tau)),$$

координаты которого по определению удовлетворяют соотношениям

$$\tau \geqslant 1, \quad \min_{1 \leqslant i \leqslant \tau} u_i \geqslant c_1 > 0, \quad \max_{1 \leqslant i \leqslant \tau} u_i \leqslant u_\tau.$$

Определим далее случайный вектор (τ^*, ζ^*), принимающий значения $(i, y) \in \mathbb{Z} \times \mathbb{R}$, $i \geqslant 0$, $y \geqslant 0$, задав его распределение (и считая $u_0 = 0$ с вероятностью 1)

$$\mathbf{P}(\tau^* = i, \, \zeta^* \in dy) := \frac{1}{Q} \, \mathbf{P}(\tau \geqslant i + 1, \, u_i \in dy),$$

где

$$Q := \sum_{i=0}^{\infty} \int_0^{\infty} \mathbf{P}(\tau \geqslant i + 1, \, u_i \in dy) = \sum_{i=0}^{\infty} \mathbf{P}(\tau \geqslant i + 1) = \mathbf{E}\tau.$$

Из условия S_{III} следует, что найдется константа $C > 0$, такая что

$$\mathbf{E}\, e^{C\tau^*} < \infty, \quad \mathbf{E}\, e^{C\zeta^*} < \infty.$$

Наряду с последовательностью $\{(\tau_k, \zeta_k)\}$, которая определяет о.п.в. $Z_+(n)$ и функционалы $\nu_+(n)$, $\gamma_+(n)$, определим последовательность $\{(\tau^*_k, \zeta^*_k)\}$, положив

$$(\tau^*_1, \zeta^*_1) := (\tau_1, \zeta_1) + (\tau^*, \zeta^*), \quad (\tau^*_k, \zeta^*_k) := (\tau_k, \zeta_k) \quad \text{при } k \geqslant 2,$$

где вектор (τ^*, ζ^*) и последовательность $\{(\tau_k, \zeta_k)\}$ независимы. Новая последовательность $\{(\tau^*_k, \zeta^*_k)\}$ определяет новый о.п.в. $Z^*_+(n)$ и новые функционалы $\nu^*_+(n)$ и $\gamma^*_+(n)$.

Лемма 7. *Пусть выполнены условия* S_{I}–S_{IV}. *Тогда для любых целых* $n \geqslant 2$ *и любых вещественных* $x \geqslant c_1$ *и* $\Delta > 0$ *справедливо равенство*

$$\begin{aligned}&\mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} \in [x, x+\Delta),\ \tau_1 \leqslant n\big) = \\ &= Q\,\mathbf{P}\big(Z^*_+(n) \in [x, x+\Delta),\ \gamma^*_+(n) = 0\big).\end{aligned} \tag{3.4}$$

Доказательство. Имеем

$$\begin{aligned}P_n &:= \mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} \in [x, x+\Delta),\ \tau_1 \leqslant n\big) = \\ &= \sum_{k=1}^{\infty} \mathbf{P}\big(T_k = n,\ Z_k \in [x, x+\Delta)\big) + \\ &+ \sum_{k=1}^{\infty}\sum_{i=1}^{n}\int_0^{\infty} \mathbf{P}\big(T_k = n-i,\ Z_k + y \in [x, x+\Delta),\ \tau_{k+1} \geqslant i+1,\ u_{k+1,i} \in dy\big).\end{aligned}$$

Поскольку событие $\mathbf{P}(\tau \geqslant 1,\ u_0 = 0) = 1$ и векторы $(\tau_{k+1}, u_{k+1,i})$ и (T_k, Z_k) независимы, то

$$\begin{aligned}P_n &= \sum_{k=1}^{\infty} \mathbf{P}\big(T_k = n,\ Z_k \in [x, x+\Delta)\big)\,\mathbf{P}(\tau \geqslant 1,\ u_0 = 0) + \\ &+ \sum_{k=1}^{\infty}\sum_{i=1}^{n}\int_0^{\infty} \mathbf{P}\big(T_k = n-i,\ Z_k + y \in [x, x+\Delta)\big)\,\mathbf{P}(\tau \geqslant i+1,\ u_i \in dy) = \\ &= Q\sum_{k=1}^{\infty}\sum_{i=0}^{n}\int_0^{\infty} \mathbf{P}\big(T_k = n-i,\ Z_k + y \in [x, x+\Delta)\big)\frac{1}{Q}\,\mathbf{P}(\tau \geqslant i+1,\ u_i \in dy) = \\ &= Q\sum_{k=1}^{\infty}\sum_{i=0}^{n}\int_0^{\infty} \mathbf{P}\big(T_k = n-i,\ Z_k + y \in [x, x+\Delta)\big)\,\mathbf{P}(\tau^* = i,\ \zeta^* \in dy) = \\ &= Q\sum_{k=1}^{\infty} \mathbf{P}\big(T^*_k = n,\ Z^*_k \in [x, x+\Delta)\big) = \\ &= Q\,\mathbf{P}\big(Z^*_+(n) \in [x, x+\Delta),\ \gamma^*_+(n) = 0,\ \nu^*_+(n) \geqslant 1\big) = \\ &= Q\,\mathbf{P}\big(Z^*_+(n) \in [x, x+\Delta),\ \gamma^*_+(n) = 0\big) - \\ &- Q\,\mathbf{P}\big(Z^*_+(n) \in [x, x+\Delta),\ \gamma^*_+(n) = 0,\ \nu^*_+(n) = 0\big) = \\ &= Q\,\mathbf{P}\big(Z^*_+(n) \in [x, x+\Delta),\ \gamma^*_+(n) = 0\big),\end{aligned}$$

где последнее равенство является следствием того, что при $x > 0$ выполняется

$$\mathbf{P}(Z^*_+(n) \in [x, x+\Delta), \nu^*_+(n) = 0) = 0. \quad \blacktriangle$$

В частном случае, когда v имеет арифметическое распределение, полагая $\Delta = 1$ в лемме 7 и выбирая $x \in \mathbb{Z}$, получаем в качестве следствия леммы 7 следующее утверждение.

Лемма 8. *Пусть выполнены условия* S_{I}–S_{IV}, *и пусть* v *удовлетворяет условию* [**Z**]. *Тогда при любых целых* $n \geqslant 2$ *и* $x \geqslant 1$ *справедливо соотношение*

$$\mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} = x,\ \tau_1 \leqslant n\big) = Q\,\mathbf{P}\big(Z^*_+(n) = x,\ \gamma^*_+(n) = 0\big). \tag{3.5}$$

Продолжим доказательство теоремы 1.

I. Обратимся сначала к арифметическому случаю. Для того чтобы воспользоваться результатами работы [7], нам придется наряду с о.п.в. $Z_+(n)$ определить о.п.в. $Z(n)$ (основные утверждения работы [7] произведены для о.п.в. $Z(n)$).

Пусть для $n \geqslant 1$

$$\nu(n) := \max\{k \geqslant 1 : T_k < n\}, \quad \gamma(n) := n - \nu(n).$$

Тогда

$$Z(n) := Z_{\nu(n)}.$$

Легко видеть (считая, что процессы $Z(n)$, $Z_+(n)$ построены на одном вероятностном пространстве по общей последовательности $\{(\tau_k, \zeta_k)\}$), что для $n \geqslant 1$

$$\nu_+(n) = \nu(n+1), \quad Z_+(n) = Z(n+1), \quad \gamma_+(n) = \gamma(n) - 1. \tag{3.6}$$

В частности, величина недоскока $\gamma(n)$ принимает значения $\{1, 2, \ldots\}$, а величина недоскока $\gamma_+(n)$ – значения $\{0, 1, 2, \ldots\}$. О.п.в., построенный по последовательности $\{(\tau_k^*, \zeta_k^*)\}$, и соответствующие ему функционалы обозначим теми же символами, снабдив их верхним индексом $*$, например:

$$\nu^*(n), \quad \nu_+^*(n), \quad Z^*(n), \quad Z_+^*(n), \quad \gamma^*(n), \quad \gamma_+^*(n) \quad \text{и т.д.}$$

В силу формул (3.6) из утверждений теоремы 2.1, следствия 2.1 и теоремы 2.1^* работы [7] без труда выводим следующие два соотношения в области нормальных и умеренно больших уклонений, когда $x \in \mathbb{N}$, $x - na = o(n)$: при $n \to \infty$

$$\begin{aligned} &\mathbf{P}(Z(n) = x) \sim \mathbf{P}(Z_+(n) = x) \sim \mathbf{P}(Z^*(n) = x) \sim \mathbf{P}(Z_+^*(n) = x) \sim \\ &\sim \frac{1}{\sigma\sqrt{2\pi n}} e^{-nD(\frac{x}{n})}, \end{aligned} \tag{3.7}$$

$$\mathbf{P}\big(Z_+^*(n) = x,\, \gamma_+^*(n) = 0\big) \sim \mathbf{P}\big(Z_+(n) = x,\, \gamma_+(n) = 0\big) \sim \frac{1}{\mathbf{E}\tau}\, \mathbf{P}(Z_+^*(n) = x). \tag{3.8}$$

Соотношения (3.7) показывают, что в наших условиях для локальных теорем в области нормальных и умеренно больших уклонений "нивелируются" различия между процессами $Z(n)$ и $Z_+(n)$, равно как и различия, связанные с неоднородностью.

Привлекая далее утверждение леммы 8 и замечая, что $Q = \mathbf{E}\tau$ и для некоторого $h > 0$

$$\begin{aligned} &\mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} = x\big) = \\ &= \mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} = x,\, \tau_1 > n\big) + \mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} = x,\, \tau_1 \leqslant n\big) = \\ &= \mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} = x,\, \tau_1 \leqslant n\big) + O(e^{-nh}), \end{aligned}$$

получаем из (3.7) и (3.8) утверждение части I теоремы 1:

$$\mathbf{P}\big(Z_+(n) + w_{n-\gamma_+(n),n} = x\big) \sim \frac{1}{\sigma\sqrt{2\pi n}} e^{-nD(\frac{x}{n})}.$$

II. В основе доказательства части II лежит интегро-локальная теорема в областях нормальных, умеренно больших и больших уклонений, полученная в работе Стоуна [12]. Приведем формулировку этой теоремы в удобных для нас обозначениях. Функцию уклонений для случайного вектора (τ, ζ) определим как

$$\Lambda(\theta, \alpha) := \sup_{\lambda,\mu}\{\lambda\theta + \mu\alpha - A(\lambda, \mu)\}.$$

Определитель матрицы $\Lambda''(\theta,\alpha)$ вторых производных функции уклонений $\Lambda(\theta,\alpha)$ обозначим через $|\Lambda''(\theta,\alpha)|$.

Теорема 2 [12]. *Пусть распределение вектора (τ_1,ζ_1) совпадает с распределением (τ,ζ) и выполнены условия $S_{\rm III}$ и [**ZR**]. Тогда для некоторого $\delta>0$ и некоторой последовательности $\Delta^{(0)}:=\Delta_n^{(0)}>0$, сходящейся к нулю при $n\to\infty$, для любых $(x,y)\in\mathbb{Z}\times\mathbb{R}$, таких что $|\theta-a_\tau|+|\alpha-a_\zeta|\leqslant\delta$, где $(\theta,\alpha):=\left(\frac{x}{n},\frac{y}{n}\right)$, имеет место соотношение*

$$\mathbf{P}\big(T_n=x,\ Z_n\in[y,y+\Delta)\big)=\frac{\Delta\sqrt{|\Lambda''(\theta,\alpha)|}}{2\pi n}\exp\{-n\Lambda(\theta,\alpha)\}(1+o(1)),$$

в котором $\Delta:=\Delta_n\geqslant\Delta_n^{(0)}$, $\Delta_n\to0$ при $n\to\infty$, а остаточный член $o(n)=\varepsilon_n(x,y)$ удовлетворяет соотношению

$$\lim_{n\to\infty}\sup_{\substack{(x,y)\in\mathbb{Z}\times\mathbb{R}\\ |\theta-a_\tau|+|\alpha-a_\zeta|\leqslant\delta}}|\varepsilon_n(x,y)|=0.$$

Используя утверждения $S_{\rm I}$–$S_{\rm IV}$ и повторяя все этапы доказательства теорем 2.1, 2.1^* и следствия 2.1 работы [7], можно получить аналоги этих утверждений, в которых символы $=x$ заменены на $\in[x,x+\Delta)$, а в правых частях появляется множитель Δ. Далее доказательство части II полностью повторяет соответствующее доказательство части I. ▲

Покажем теперь, что справедлива

Теорема 3. *Характеристики a, σ и $D(\alpha)$, в терминах которых приведены результаты теоремы* 1, *не зависят от выбора констант c_1 и c_2.*

Доказательство. Мы доказали, что локальные теоремы в областях нормальных и умеренно больших уклонений для процессов $w_{0,n}$ и $Z_+(n)$ выглядят одинаково, и формулировка этого утверждения содержит характеристики a, σ и $D(\alpha)$, которые однозначно определяются по вектору (τ,ζ) (см. (1.4)–(1.6)), "управляющему" о.п.в. $Z_+(n)$. А поскольку в построении вектора (τ,ζ) заняты произвольные константы c_1 и c_2, удовлетворяющие условию (2.7), то естественно ожидать, что и характеристики a, σ и $D(\alpha)$ будут зависеть от этих констант. Покажем, что это не так, т.е. покажем, что для любых других констант $\widetilde{c}_2\leqslant\widetilde{c}_1$, удовлетворяющих (2.7), характеристики $\widetilde{a}$, $\widetilde{\sigma}$ и $\widetilde{D}(\alpha)$, построенные для вектора $(\widetilde{\tau},\widetilde{\zeta})$, совпадают с характеристиками a, σ и $D(\alpha)$.

В силу уже доказанного для процессов $w_{0,n}$ и $\widetilde{Z}_+(n)$ справедлива такая же локальная теорема, в формулировке которой используются характеристики $\widetilde{a}$, $\widetilde{\sigma}$ и $\widetilde{D}(\alpha)$. Таким образом, для процесса $w_{0,n}$ справедливы две локальные теоремы, формулировки которых отличаются только характеристиками $a,\sigma,D(\alpha)$ и $\widetilde{a},\widetilde{\sigma},\widetilde{D}(\alpha)$. Из локальных теорем в области нормальных уклонений очевидным образом вытекают соответствующие законы больших чисел: для любого $\varepsilon>0$ справедливы соотношения

$$\lim_{n\to\infty}\mathbf{P}(|w_{0,n}-an|\leqslant n\varepsilon)=1,\quad \lim_{n\to\infty}\mathbf{P}(|w_{0,n}-\widetilde{a}n|\leqslant n\varepsilon)=1.$$

Следовательно, с необходимостью $\widetilde{a}=a$.

Далее, если переписать формулировки двух локальных теорем с учетом равенства $\widetilde{a}=a$, то придем к соотношению

$$\frac{1}{\sigma\sqrt{n}}e^{-nD(\frac{x}{n})}\sim\frac{1}{\widetilde{\sigma}\sqrt{n}}e^{-n\widetilde{D}(\frac{x}{n})},$$

которое выполняется для любых $x = x_n \in \mathbb{Z}$ в зоне $\left|\frac{x}{n} - a\right| = o(1)$. Тогда с необходимостью из этого соотношения вытекают равенство констант $\sigma = \widetilde{\sigma}$ и равенство аналитических (в некоторой окрестности точки $\alpha = a$) функций $\widetilde{D}(\alpha) = D(\alpha)$. Таким образом, мы доказали, что характеристики a, σ и $D(\alpha)$ не зависят от выбора констант, по которым построен о.п.в. ▲

§ 4. Вспомогательный результат

Мы используем в доказательствах приводимый ниже результат, который не претендует на новизну. Так как его доказательство очень коротко, то мы решили привести и его.

Лемма 9. *Пусть* $S_n = \sum\limits_{i=1}^{n} X_i$, $n = 1, 2, \ldots$, – *последовательность частичных сумм независимых и одинаково распределенных неотрицательных случайных величин* $\{X_i\}$, *и пусть* N – *неотрицательная целочисленная случайная величина. Предположим, что*

$$\mathbf{E}\, e^{CX_1} < \infty, \quad \mathbf{E}\, e^{CN} < \infty \quad \textit{для некоторого } C > 0.$$

Тогда найдется константа $b > 0$, *такая что*

$$\mathbf{E}\, e^{bS_N} < \infty.$$

Доказательство. Возьмем любое $a > \mathbf{E}\, X_1$. Тогда

$$S_N = \sum_{i=1}^{N} (X_i - a) + aN \leqslant \sup_{n \geqslant 0} (S_n - na) + aN \equiv R + aN, \tag{4.1}$$

где мы считаем $S_0 = 0$. В силу (4.1) и элементарного неравенства $e^{x+y} \leqslant e^{2x} + e^{2y}$ при любом $b > 0$ будем иметь

$$e^{bS_N} \leqslant e^{2bR} + e^{2baN} \leqslant 1 + \sum_{n=1}^{\infty} e^{2b(S_n - na)} + e^{2baN},$$

и следовательно,

$$\mathbf{E}\, e^{bS_N} \leqslant 1 + \sum_{n=1}^{\infty} \left(\mathbf{E}\, e^{2b(X_1 - a)}\right)^n + \mathbf{E}\, e^{2baN}. \tag{4.2}$$

Так как $a > \mathbf{E}\, X_1$, то найдется достаточно малое $b > 0$, такое что $2b \max(1, a) < C$ и $\mathbf{E}\, e^{2b(X_1 - a)} < 1$. При таком b и правая часть в неравенстве (4.2) оказывается конечным числом. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Cohen J.E., Briand F., Newman C.M.* Community Food Webs: Data and Theory. Berlin: Springer, 1990.
2. *Newman C.M.* Chain Lengths in Certain Random Directed Graphs // Random Structures Algorithms. 1992. V. 3. № 3. P. 243–253. https://doi.org/10.1002/rsa.3240030304
3. *Gelenbe E., Nelson R., Philips T., Tantawi A.* An Approximation of the Processing Time for a Random Graph Model of Parallel Computation // Proc. 1986 ACM Fall Joint Computer Conf. (ACM'86). Los Alamitos, CA: IEEE Computer Society Press, 1986. P. 691–697. https://dl.acm.org/doi/proceedings/10.5555/324493

4. *Isopi M., Newman C.M.* Speed of Parallel Processing for Random Task Graphs // Comm. Pure Appl. Math. 1994. V. 47. № 3. P. 361–376. https://doi.org/10.1002/cpa.3160470307
5. *Foss S., Konstantopoulos T.* Extended Renovation Theory and Limit Theorems for Stochastic Ordered Graphs // Markov Process. Related Fields. 2003. V. 9. № 3. P. 413–468.
6. *Denisov D., Foss S., Konstantopoulos T.* Limit Theorems for a Random Directed Slab Graph // Ann. Appl. Probab. 2012. V. 22. № 2. P. 702–733. https://doi.org/10.1214/11-AAP783
7. *Могульский А.А., Прокопенко Е.И.* Локальные предельные теоремы для арифметических многомерных обобщенных процесов восстановления при выполнении условия Крамера // Матем. тр. 2019. Т. 22. № 2. С. 106–133. https://doi.org/10.33048/mattrudy.2019.22.207
8. *Могульский А.А., Прокопенко Е.И.* Функция уклонений и базовая функция для многомерного обобщенного процесса восстановления // Сиб. электрон. матем. изв. 2019. Т. 16. С. 1449–1463. https://doi.org/10.33048/semi.2019.19.100
9. *Foss S., Martin J.B., Schmidt P.* Long-Range Last-Passage Percolation on the Line // Ann. Appl. Probab. 2014. V. 24. № 1. P. 198–234. https://doi.org/10.1214/13-AAP920
10. *Foss S., Konstantopoulos T.* Limiting Properties of Random Graph Models with Vertex and Edge Weights // J. Stat. Phys. 2018. V. 173. № 3–4. P. 626–643. https://doi.org/10.1007/s10955-018-2080-3
11. *Тесемников П.И.* Об асимптотике кратчайшего расстояния между крайними вершинами в обобщенном графе Барака – Эрдеша // Сиб. электрон. матем. изв. 2018. Т. 15. С. 1556–1565. https://doi.org/10.33048/semi.2018.15.129
12. *Stone C.* On Local and Ratio Limit Theorems // Proc. 5th Berkeley Symp. on Mathematical Statitics and Probability. Univ. of California, Berkeley, 1965–66. Berkeley, CA: Univ. of California Press, 1967. V. 2: Contributions to Probability Theory. Part 2. P. 217–224. https://doi.org/10.1525/9780520325340-017

Константопулос Такис
Отделение математических наук, Ливерпульский университет,
Ливерпуль, Великобритания
T.Konstantopoulos@liverpool.ac.uk
Логачёв Артём Васильевич
Институт математики им. С.Л. Соболева СО РАН, Новосибирск
Новосибирский государственный университет
Сибирский государственный университет геосистем
и технологий, Новосибирск
omboldovskaya@mail.ru
Могульский Анатолий Альфредович
Институт математики им. С.Л. Соболева СО РАН, Новосибирск
Новосибирский государственный университет
mogul@math.nsc.ru
Фосс Сергей Георгиевич
Институт математики им. С.Л. Соболева СО РАН, Новосибирск
Новосибирский государственный университет
Школа математических наук, Университет Хериот-Ватта,
Эдинбург, Великобритания
sergueiorfoss25@gmail.com

Поступила в редакцию
19.11.2020
После доработки
01.02.2021
Принята к публикации
08.02.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 2021 Вып. 2

УДК 621.391 : 519.72

© 2021 г. **Е.Е. Егорова, Г.А. Кабатянский**

РАЗДЕЛИМЫЕ КОДЫ ДЛЯ ЗАЩИТЫ МУЛЬТИМЕДИА ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ КОАЛИЦИЯМИ[1]

Дается обзор известных результатов о кодах, способных защитить мультимедийный контент от нелегального перераспределения коалициями недобросовестных пользователей.

Ключевые слова: разделимый код, разделяющий код, дизъюнктивный код, мультимедийный код цифровых отпечатков пальцев, канал множественного доступа, сигнатурный код, целенаправленный шум.

DOI: 10.31857/S0555292321020066

§ 1. Введение

Развитие Интернета и мультимедийных технологий сделало актуальной задачу разработки методов защиты цифровых авторских прав и предотвращения нелегальной перепродажи мультимедийного контента коалициями недобросовестных пользователей. Впервые математическая модель этой проблемы была сформулирована около двадцати лет назад в статье [1], а затем и в монографии [2]. Ключевым моментом предложенной модели было использование шумоподобных сигналов для построения уникальных меток, называемых цифровыми водяными знаками и внедряемых в распространяемые копии мультимедийного файла без потери качества (звука, изображения и т.д.). Вслед за этим последовал ряд работ, в которых эта модель получила свое дальнейшее развитие. В том числе, в работах [3,4] было введено понятие *разделимого* (separable) *кода*, который позволяет безошибочно находить по нелегальной копии *всех членов коалиции*. Проблему защиты мультимедийного контента от коалиционных атак можно рассматривать как обобщение на непрерывный случай другой известной задачи – о кодах цифровых отпечатков пальцев, устойчивых к коалиционным атакам (см. [5–13]). Отметим существенное различие разделимых кодов от кодов цифровых отпечатков пальцев, так как первые гарантируют нахождение всей коалиции, тогда как последние позволяют найти только одного члена коалиции (см. обзор [14]).

Построенные в [3] первые разделимые коды позволяли по нелегальной копии находить целиком коалицию недобросовестных пользователей, однако основной недостаток этих кодов был в том, что их скорость стремилась к нулю с ростом длины кода, т.е. эти коды не обеспечивали защиту мультимедийной информации с экспоненциальным от длины цифровых водяных знаков, т.е. от длины кода, числом пользователей. Этот недостаток был впервые преодолен в работе [15], где были построены разделимые коды с экспоненциальным числом пользователей, в том числе разделимые коды с простым “декодированием”, т.е. нахождением всех участников коалиции. Эти результаты были получены с помощью установленной связи между разделимы-

[1] Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (номера проектов 20-17-50013 и 20-51-50007).

ми кодами и сигнатурными кодами для специального типа канала множественного доступа, известного как A-канал [16]. В дальнейшем эта связь была расширена на другие модели защиты мультимедийной информации и соответствующие им каналы множественного доступа и стала основным теоретико-информационным методом в исследовании разделимых кодов. В частности, в работе [17] была предложена более общая математическая модель построения цифровых водяных знаков, названная авторами взвешенным двоичным суммирующим каналом множественного доступа, который обобщает как обычный двоичный суммирующий канал (см. [18]), так и его расширение, предложенное в [19]. Возникающие в этой более общей модели задачи оказались весьма близки к задачам "сжатия отсчетов" (compressed sensing), см. [20–22].

Следует отметить, что модель цифровых водяных знаков, предложенная в [1, 2], довольно чувствительна к шуму, и вопрос о том, чтобы разделимые коды были способны находить членов коалиции и в условиях шума, ставился уже в [1]. Решения для вероятностной модели были предложены в [23], а для целенаправленного шума – в [17, 24]. Отметим хорошо известную связь между кодами для каналов множественного доступа и различными вариациями комбинаторных задач поиска (см. [25]), в частности, с задачами поиска в присутствии шума, например, с игрой Реньи – Улама [26,27], известной также как задача о "поиске со лжецом". Впервые эту задачу сформулировал А. Реньи [26], но популярной она стала после книги С. Улама [27], где он задал вопрос, чему равно минимальное число вопросов, достаточное, чтобы найти неизвестное целое число в диапазоне от 1 до миллиона, если среди ответов ДА/НЕТ на вопросы один может быть ложным. Точный ответ для игры Реньи – Улама при адаптивном поиске был получен в [28]. В случае фиксированного числа L ложных ответов известна асимптотика минимального числа вопросов, а именно $(\log_2 N + L \log_2 \log_2 N)(1 + o(1))$ неадаптивных вопросов, где N – число "предметов", из которых ищется один "загаданный".

Коды по определению дискретны, а исходная постановка задачи непрерывна. Чтобы перейти в дискретную область, используется простая двоичная модуляция. А что можно улучшить, если рассмотреть более общие типы модуляции? Этот вопрос был задан и частично решен в недавней работе [29].

Наконец, в качестве лингвистического курьеза отметим, что основным инструментом для построения эффективных *разделимых* (separable) кодов стали хорошо известные в теории кодирования *разделяющие* (separating) коды, исследованию которых были посвящены многочисленные работы Ю.Л. Сагаловича и Ж. Коэна (см. их обзоры [30, 31]).

Все вышеперечисленные и некоторые другие известные результаты будут отражены в данном обзоре.

§ 2. Математические модели кодов для защиты мультимедийной информации

Математическая постановка задачи защиты цифрового контента от нелегального копирования и перераспределения возникла в конце прошлого века, см. [5–7]. Первой появилась математическая модель, наиболее известная как коды поиска пиратов [7] или коды цифровых отпечатков пальцев [11]. В этой модели имеется код над некоторым конечным алфавитом, каждому пользователю на этапе инициализации системы передается соответствующее ему кодовое слово, позволяющее получить доступ к передаваемой информации, которая зашифрована. Коалиция из не более чем t недобросовестных пользователей на основе имеющихся у ее членов кодовых слов может создать новое, ложное слово, которое тоже позволит получить доступ к зашифрованной информации. При этом имеется ограничение на то, какие слова может создавать коалиция, известное как marking assumption и существующее в двух вариациях, под названием (в терминах [12]) узкая [9] и широкая [11] выпуклые обо-

лочки. В обеих вариациях, если все члены коалиции имеют в данной позиции один и тот же символ алфавита, то он же будет стоять и в ложном слове. Если же в данной позиции не все члены коалиции одинаковы, то в случае широкой выпуклой оболочки коалиция может поставить в данной позиции ложного слова любой символ алфавита, а в случае узкой выпуклой оболочки – только один из символов, имеющихся у членов коалиции в этой позиции. Краткое изложение того, как в этой модели используется широковещательное шифрование на базе различных схем разделения секрета [32,33], можно найти в [34, Приложение]. Известные модели кодов цифровых отпечатков пальцев являются дискретными, и непрерывная модель впервые возникла в задачах защиты мультимедийного контента (изображения, музыка и т.д.) [1,2].

Рассмотрим математическую модель защиты мультимедийного контента от нелегального перераспределения. Мультимедийное сообщение представляется как N-мерный вещественный вектор $\boldsymbol{x} \in \mathbb{R}^N$. Это сообщение одновременно передается (продается) многим (M) пользователям системы. Перед передачей система уникально для каждого пользователя видоизменяет $\boldsymbol{x}$ таким образом, что если коалиция недобросовестных пользователей подделает $\boldsymbol{x}$, то система может найти всех членов коалиции. Для этого выбираются m ортонормированных векторов $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ в $\mathbb{R}^N$, которые *не известны пользователям*. Затем система формирует для j-го пользователя свой *цифровой водяной знак* $\boldsymbol{w}_j$ как линейную комбинацию векторов $\boldsymbol{f}_i$ с двоичными коэффициентами $h_{ij} \in \{0, 1\}$:

$$\boldsymbol{w}_j = \sum_{i=1}^{m} h_{ij} \boldsymbol{f}_i. \tag{1}$$

Вложение цифровых водяных знаков осуществляется аддитивно, т.е. система выдает j-му пользователю вектор

$$\boldsymbol{y}_j = \boldsymbol{x} + \boldsymbol{w}_j \tag{2}$$

как копию $\boldsymbol{x}$, где предполагается, что длина вектора $\boldsymbol{x}$ много больше длины $\boldsymbol{w}_j$, для того чтобы копия $\boldsymbol{y}_j$ мало отличалась от оригинала $\boldsymbol{x}$.

Отметим, что известен и другой вариант “модуляции”, когда в качестве коэффициентов h_{ij} используются $+1$ и -1.

Пусть среди M пользователей системы, которым присвоены номера $1, \ldots, M$, имеется коалиция $A \subset \{1, \ldots, M\}$ недобросовестных пользователей. *Линейная атака* состоит в том, что коалиция A генерирует поддельную копию $\boldsymbol{y}$ как линейную комбинацию имеющихся у нее копий $\boldsymbol{y}_j$ с вещественными коэффициентами $\lambda_1, \ldots, \lambda_M$, такими что $\sum\limits_{j=1}^{M} \lambda_j = 1$, $\lambda_j > 0$ для всех $j \in A$ и $\lambda_j = 0$ для $j \notin A$, т.е.

$$\boldsymbol{y} = \sum_{j=1}^{M} \lambda_j \boldsymbol{y}_j = \sum_{a \in A} \lambda_a \boldsymbol{y}_a, \tag{3}$$

Так как $\sum\limits_{j=1}^{M} \lambda_j = 1$, то $\boldsymbol{y} = \boldsymbol{x} + \sum\limits_{j=1}^{M} \lambda_j \boldsymbol{w}_j$, при этом все $\lambda_j \geqslant 0$, и поэтому в силу неравенства треугольника (для нормы)

$$\|\boldsymbol{y} - \boldsymbol{x}\| = \left\| \sum_{j=1}^{M} \lambda_j \boldsymbol{w}_j \right\| \leqslant \sum_{j=1}^{M} \lambda_j \|\boldsymbol{w}_j\| \leqslant \max_j \|\boldsymbol{w}_j\| \ll \|\boldsymbol{x}\|, \tag{4}$$

где здесь и ниже $\|\boldsymbol{a}\| := \sqrt{\sum\limits_{i=1}^{N} a_i^2}$ обозначает евклидову норму вектора $\boldsymbol{a}$.

Следовательно, $\boldsymbol{y}$ является достаточно хорошей копией оригинала $\boldsymbol{x}$. Отметим, что общепринято рассматривать только линейные атаки, так как для известных примеров нелинейных атак [35] $\boldsymbol{y}$ не является достаточно хорошей копией оригинала $\boldsymbol{x}$.

Так как система знает значение $\boldsymbol{x}$, то для определения того, что $\boldsymbol{y}$ – нелегальная копия, и нахождения всех участников коалиции, которые создали $\boldsymbol{y}$, система вычисляет скалярные произведения

$$s_k = (\boldsymbol{y} - \boldsymbol{x}, \boldsymbol{f}_k) = \left(\sum_{j=1}^{M} \lambda_j \sum_{i=1}^{m} h_{ij} \boldsymbol{f}_i, \boldsymbol{f}_k \right) = \sum_{j=1}^{M} \lambda_j h_{kj} = \sum_{j \in A} \lambda_j h_{kj}, \tag{5}$$

из которых формирует вектор-*синдром*

$$\boldsymbol{S} = \boldsymbol{S}(\Lambda) = (s_1, \ldots, s_m), \tag{6}$$

где $\Lambda = (\lambda_1, \ldots, \lambda_M)$. Отметим, что носитель $\operatorname{supp}(\Lambda) := \{j : \lambda_j \neq 0\}$ вектора Λ – это и есть коалиция A.

Введем векторы $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M$, где $\boldsymbol{h}_j = (h_{1j}, \ldots, h_{mj})$. Тогда (5) можно переписать в виде

$$\boldsymbol{S}(\Lambda) = \sum_{j=1}^{M} \lambda_j \boldsymbol{h}_j = \sum_{a \in A} \lambda_a \boldsymbol{h}_a. \tag{7}$$

Это уравнение, в свою очередь, можно записать как матричное уравнение

$$\boldsymbol{S}(\Lambda) = H\Lambda^T, \tag{8}$$

где H – $(m \times M)$-матрица, составленная из векторов-столбцов $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M$.

Так как векторы $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ ортонормированные, а векторы $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M$ выражаются в базисе $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m$ как $\boldsymbol{w}_j = \sum\limits_{i=1}^{m} h_{ij} \boldsymbol{f}_i$, где $h_{ij} \in \{0, 1\}$, то множества $\mathcal{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M\} \subset \mathbb{R}^N$ и $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M\} \subset \{0, 1\}^m \subset \mathbb{R}^m$ изометричны. Поэтому далее мы будем оба множества называть мультимедийным кодом, а если по синдрому $\boldsymbol{S}$ можно однозначно найти носитель $\operatorname{supp}(\Lambda)$, т.е. коалицию A, то будем называть такой код *мультимедийным кодом со свойством полного поиска t-коалиций*, сокращенно – t-МППК-кодом [24] (английский эквивалент этого названия – complete traceability code [36]).

Определение 1. Двоичный код $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M\} \subset \{0, 1\}^m := B^m$ длины m называется *t-МППК-кодом*, если для любых двух вещественных векторов $\Lambda = (\lambda_1, \ldots, \lambda_M)$ и $\Lambda' = (\lambda'_1, \ldots, \lambda'_M)$, таких что все λ_j и λ'_j неотрицательны, $\sum\limits_{j=1}^{M} \lambda_j = \sum\limits_{j=1}^{M} \lambda'_j = 1$ и $|\operatorname{supp}(\Lambda)|, |\operatorname{supp}(\Lambda')| \leqslant t$, из $\operatorname{supp}(\Lambda) \neq \operatorname{supp}(\Lambda')$ следует, что $H\Lambda^T \neq H\Lambda'^T$.

Замечание 1. В данном определении условие $\operatorname{supp}(\Lambda) \neq \operatorname{supp}(\Lambda')$ можно заменить на $\operatorname{supp}(\Lambda) \cap \operatorname{supp}(\Lambda') = \varnothing$, т.е. ограничиться случаем, когда соответствующие коалиции не пересекаются.

Чтобы показать справедливость этого замечания, предположим противное, т.е. что определение выполнено для всех векторов, таких что их носители не пересекаются, но тем не менее существуют два вектора Λ и Λ', удовлетворяющие условиям определения, такие что их синдромы равны $H\Lambda^T = H\Lambda'^T$, хотя $\operatorname{supp}(\Lambda) \neq \operatorname{supp}(\Lambda')$.

Обозначим $\operatorname{supp}\Lambda = U$, $\operatorname{supp}\Lambda' = V$, $W = U \cap V$, $W_U = \{w \in W : \lambda_w > \lambda'_w\}$ и $W_V = \{w \in W : \lambda'_w > \lambda_w\}$. Условие $H\Lambda^T = H\Lambda'^T$ представимо в виде

$$\sum_{\boldsymbol{u}\in U} \lambda_u \boldsymbol{u} = \sum_{\boldsymbol{v}\in V} \lambda'_v \boldsymbol{v}. \tag{9}$$

С помощью множеств W_U и W_V перепишем (9) в виде

$$\sum_{\boldsymbol{u}\in U\setminus W} \lambda_u \boldsymbol{u} + \sum_{\boldsymbol{u}\in W_U} (\lambda_u - \lambda'_u)\boldsymbol{u} = \sum_{\boldsymbol{v}\in V\setminus W} \lambda'_v \boldsymbol{v} + \sum_{\boldsymbol{v}\in W_V} (\lambda'_v - \lambda_v)\boldsymbol{v}. \tag{10}$$

Обозначим через σ_L и σ_R суммы коэффициентов в левой и правой частях равенства (10) соответственно. Легко проверить, что $\sigma_L = \sigma_R := \sigma \leqslant 1$ и что все коэффициенты в (10) положительны. Следовательно, пронормировав коэффициенты, поделив их на σ, получим два вектора, синдромы которых совпадают, тогда как их носители, равные $(U \setminus W) \cup W_U$ и $(V \setminus W) \cup W_V$, не пересекаются, в противоречии с исходным предположением.

Пример. Проверим, что код $\mathcal{H} = \{\boldsymbol{h}_1 = (1,0), \boldsymbol{h}_2 = (0,1), \boldsymbol{h}_3 = (1,1)\}$ является 2-МППК-кодом. Заметим, что у вектора, полученного как линейная комбинация векторов $\boldsymbol{h}_1$ и $\boldsymbol{h}_2$, сумма координат равна 1, а у двух других линейных комбинаций $\lambda_i \boldsymbol{h}_i + \lambda_3 \boldsymbol{h}_3$, где $i \in \{1,2\}$, сумма координат равна $1 + \lambda_3$. Осталось проверить, возможно ли, что $\lambda_1 \boldsymbol{h}_1 + \lambda_3 \boldsymbol{h}_3 = \lambda'_2 \boldsymbol{h}_2 + \lambda'_3 \boldsymbol{h}_3$. В этом случае, как только что было отмечено, $1 + \lambda_3 = 1 + \lambda'_3$, т.е. $\lambda_3 = \lambda'_3$. Следовательно, $\lambda_1 \boldsymbol{h}_1 = \lambda'_2 \boldsymbol{h}_2$, откуда $\lambda_1 = \lambda'_2 = 0$, что противоречит предположению, что все λ положительны.

Обозначим через $M(t,m)$ максимальную мощность двоичного t-МППК-кода длины m. Из примера следует, что $M(2,2) \geqslant 3$, а так как полный код, очевидно, не является 2-МППК-кодом, то $M(2,2) = 3$.

Для оценки асимптотического поведения максимальной мощности $M(t,m)$ двоичного t-МППК-кода длины m рассмотрим, как обычно, соответствующую скорость кода $R(m,t) := m^{-1}\log_2 M(m,t)$. Будем обозначать через $R^*(t)$ и $R_*(t)$, соответственно, верхний и нижний пределы величины $R(m,t)$ при $m \to \infty$. Возьмем в определении 1 в качестве Λ и Λ' векторы, у которых координаты носителя вектора одинаковы и равны $1/t$ (такая линейная атака называется атакой усреднения, и мы ее обсудим чуть ниже). Отсюда следует, что для любого t-МППК-кода все суммы по t векторов кода (как вещественных векторов) различны и поэтому справедлив следующий аналог границы Хэмминга:

$$C^t_{M(m,t)} \leqslant (t+1)^m.$$

Тем самым, $R^*(t) \leqslant t^{-1}\log_2(t+1)$. Отметим, что при больших t эту границу можно в два раза улучшить, см. [37].

С другой стороны, в [17] была доказана конструктивно следующая нижняя граница:

$$M(m,t) \geqslant 2^{\lfloor m/t \rfloor}, \tag{11}$$

из которой очевидно следует, что $R_*(t) \geqslant t^{-1}$. Явное построение в [17] t-МППК-кодов основано на простом замечании из линейной алгебры, что если некоторые двоичные векторы $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_L$ линейно независимы над полем $GF(2)$ из двух элементов, то эти векторы линейно независимы и над полем $\mathbb{R}$ вещественных чисел. Следовательно, множество столбцов проверочной матрицы любого двоичного кода с расстоянием $d \geqslant 2t+1$ является t-МППК-кодом. Такой t-МППК-код по известному "синдрому" $S(\Lambda)$ позволяет найти вектор Λ целиком, а не только его носитель. Граница (11)

получается, если взять в качестве двоичного кода неприводимый код Гоппы длины $n = 2^\ell$ с избыточностью $r = t\ell$ и расстоянием $d \geqslant 2t + 1$, см. [38].

Замечание 2. Приведенное выше построение t-МППК-кодов не использует неотрицательности коэффициентов λ, так как в результате построения получается подмножество вершин булева куба, таких что любые $2t$ из них линейно независимы над $\mathbb{R}$. В связи с этим в [17] был задан следующий вопрос: чему равна максимально возможная мощность $M^*(t, m)$ подмножеств вершин булева куба $B^m \subset \mathbb{R}^m$, таких что любые $2t$ из них линейно независимы над $\mathbb{R}$, и какова асимптотика величины $M^*(t, m)$ при фиксированном t и $m \to \infty$? Очевидно, что $M(t, m) \geqslant M^*(t, m)$. Оказалось, что логарифмическая асимптотика $M^*(t, m)$ известна благодаря работе [39]. Обозначим через $r(n, t)$ минимальную размерность евклидова пространства, в котором существует n двоичных векторов, таких что любые t из них линейно независимы. В [39] было доказано, что $r(n, t) = O\Big(t + \dfrac{t \log(t^{-1} n)}{\log t}\Big)$, откуда, в частности, следует, что

$$c_1 \frac{\log t}{t} \leqslant R_*(t) \leqslant R^*(t) \leqslant c_2 \frac{\log t}{t}, \tag{12}$$

где $0 < c_1 < c_2$ – некоторые константы.

Среди всех линейных атак принято особо выделять *атаку усреднения*, для которой $\lambda_j = |A|^{-1}$ при $j \in A$ и $\lambda_j = 0$ в противном случае, где A – коалиция недобросовестных пользователей. Начиная с первых работ по этой тематике (см. [1, 2]), считалось, что это самая эффективная из всех линейных атак, которой можно "заменить" все остальные линейные атаки. Так, например, в [3] написано: "атака усреднения является наиболее справедливой для участников коалиции, чтобы избежать обнаружения", и поэтому в подавляющем большинстве работ ограничивались рассмотрением только атаки усреднения. Довольно очевидно, что такое утверждение неверно, так как выбор какой-то одной стратегии задания коэффициентов λ_j из всех возможных линейных атак существенно упрощает задачу поиска коалиции. Сейчас мы покажем, что в случае $t > 2$ атака усреднения не является оптимальной и среди фиксированных линейных атак.

Начнем с рассмотрения случая $t = 2$, когда, как мы сейчас покажем, *кроме атаки усреднения, нет других нетривиальных атак*. Более точно, покажем, что для любых четырех различных двоичных векторов $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a}', \boldsymbol{b}'$ из того, что

$$\lambda_a \boldsymbol{a} + \lambda_b \boldsymbol{b} = \lambda'_a \boldsymbol{a}' + \lambda'_b \boldsymbol{b}' := \boldsymbol{S} = (s_1, \ldots, s_m),$$

следует, что все λ равны $1/2$. Введем следующие множества координат: $N_{\alpha,\beta} = \{i : a_i = \alpha,\ b_i = \beta\}$ и $N'_{\alpha,\beta} = \{i : a'_i = \alpha,\ b'_i = \beta\}$, где $\alpha, \beta \in \{0, 1\}$. Очевидно, что $s_i = 0$ для $i \in N_{0,0}$ и $s_i = 1$ для $i \in N_{1,1}$, так как $\lambda_a + \lambda_b = 1$. Аналогично, $s_i = 0$ для $i \in N'_{0,0}$ и $s_i = 1$ для $i \in N'_{1,1}$. Следовательно, $N_{0,0} = N'_{0,0}$ и $N_{1,1} = N'_{1,1}$. Далее, $s_i = \lambda_a$ для $i \in N_{1,0}$ и $s_i = \lambda_b$ для $i \in N_{0,1}$. Аналогично, $S_i = \lambda'_a$ для $i \in N'_{1,0}$ и $S_i = \lambda'_b$ для $i \in N'_{0,1}$. Напомним, что $0 < \lambda_a, \lambda_b < 1$, и пусть $\lambda_a \neq \lambda_b$. Если среди значений S_i есть два значения, отличных от 0 и 1, то эти значения равны λ_a и λ_b и, аналогично, равны λ'_a и λ'_b. Следовательно, множества $\{\lambda_a, \lambda_b\}$ и $\{\lambda'_a, \lambda'_b\}$ совпадают. Пусть для простоты $\lambda_a = \lambda'_a$, $\lambda_b = \lambda'_b$, и значит, совпадают и соответствующие множества координат $N_{\alpha,\beta}$ и $N'_{\alpha,\beta}$ при всех $\alpha, \beta \in \{0, 1\}$. Тем самым, пары векторов $\boldsymbol{a}, \boldsymbol{b}$ и $\boldsymbol{a}', \boldsymbol{b}'$ совпадают. Аналогично рассматривается и случай, когда среди значений S_i имеется только одно значение, отличное от 0 и 1.

Замечание 3. Доказанное выше утверждение можно сформулировать геометрически следующим образом: любые два отрезка с вершинами в точках булева куба B^m пересекаются либо в вершинах, либо в серединах отрезков.

Приведем пример, что для больших t это уже не так. Рассмотрим $t = 3$ и двоичный код $\mathcal{H}$, состоящий из векторов $a = (1,0,0,0)$, $b = (0,1,0,1)$, $c = (0,1,1,0)$, $a' = (0,1,0,0)$, $b' = (1,0,0,1)$, $c' = (1,0,1,0)$, и две коалиции $I = \{a,b,c\}$ и $I' = \{a',b',c'\}$. Тогда при атаке усреднения система различает коалиции I и I', так как у коалиций получаются разные синдромы: $S_I = (1/3, 2/3, 1/3, 1/3)$ и $S_{I'} = (2/3, 1/3, 1/3, 1/3)$. С другой стороны, выборы $\lambda_a = 1/2$, $\lambda_b = 1/4$, $\lambda_c = 1/4$ и $\lambda_{a'} = 1/2$, $\lambda_{b'} = 1/4$, $\lambda_{c'} = 1/4$ дают один и тот же синдром $S = (1/2, 1/2, 1/4, 1/4)$. Следовательно, при такой атаке система не может различить коалиции I и I'.

Перейдем теперь к *дискретной* версии описанной выше модели. Вся полезная информация, которую система имеет о ложном векторе, содержится в скалярных произведениях s_k, см. (5). Из последнего равенства в уравнении (5) и того, что $\lambda_j > 0$ для всех $j \in A$, следует, что

$s_k = 0$, если $h_{kj} = 0$ для всех $j \in A$,

$s_k = 1$, если $h_{kj} = 1$ для всех $j \in A$,

$0 < s_k < 1$ в противном случае.

В работах [1, 3] было предложено рассматривать следующую дискретную модель, при которой системе известно не точное значение s_k, а только то, что $s_k = 0$, $s_k = 1$, или $0 < s_k < 1$. Это равносильно тому, что системе известно, что либо все k-е координаты векторов коалиции равны 0, что соответствует случаю $s_k = 0$, либо все k-е координаты векторов коалиции равны 1 (случай $s_k = 1$), либо среди значений k-й координаты встречаются как 0, так и 1.

Обозначим через $F(\cdot)$ следующее отображение отрезка $[0,1]$ на троичный алфавит, состоящий из символов $0, 1$ и $*$:

$$F(x) = \begin{cases} x, & \text{если } x \in \{0,1\}, \\ *, & \text{если } 0 < x < 1, \end{cases}$$

где $*$ используется для краткости как символ, заменяющий множество $\{0,1\}$.

Для произвольного множества A вершин булева куба B^m определим его проекцию на i-ю координату как $P_i(A) := \{a_i : \boldsymbol{a} \in A\}$ и его полную проекцию как

$$P(A) = \{(a_1, \ldots, a_m) : \ a_1 \in P_1(A), \ldots, a_m \in P_m(A)\}, \tag{13}$$

т.е. $P(A) = P_1(A) \times \ldots \times P_m(A)$.

Для произвольного множества (коалиции) A его *дискретный синдром* $F(S) = (F(s_1), \ldots, F(s_m)) = F(A)$ *не зависит от выбора коэффициентов* λ_a *в* (5), так как $F(s_i) = P_i(A)$ в силу того, что $\lambda_a > 0$ при $a \in A$ и $\lambda_a = 0$ в противном случае. Тем самым, задачей системы становится восстановить коалицию по ее дискретному синдрому или, что то же самое, по ее полной проекции. Это приводит к определению разделимого (separable) кода.

О п р е д е л е н и е 2 [3, 4]. Двоичный код C называется *t-разделимым кодом*, если для любых двух различных кодовых подмножеств (коалиций) $U, V \subset C$, $|U| \leqslant t$, $|V| \leqslant t$, их полные проекции различны:

$$P(U) \neq P(V). \tag{14}$$

Сравним определения 1 и 2. Так как для любой коалиции ее дискретный синдром не зависит от коэффициентов λ, то t-разделимый код является t-МППК-кодом. Обратное в общем случае неверно, так как нижняя оценка (12) для скорости t-МППК-кодов превышает верхнюю оценку (23) на скорость t-разделимых кодов для больши́х t. Отметим также, что в определении 2 нельзя заменить условие "различные подмножества" на "непересекающиеся", как можно было сделать в определении 1.

Однако для $t = 2$ эти два понятия совпадают. Для этого покажем, что 2-МППК-код является 2-разделимым. Рассмотрим четыре произвольных кодовых вектора $\boldsymbol{a} \neq \boldsymbol{b} \neq \boldsymbol{c} \neq \boldsymbol{d}$ и соответствующие две коалиции $U = \{\boldsymbol{a}, \boldsymbol{b}\}$ и $V = \{\boldsymbol{c}, \boldsymbol{d}\}$ и применим к ним атаку усреднения. Так как код 2-МППК, то $\boldsymbol{a}+\boldsymbol{b} \neq \boldsymbol{c}+\boldsymbol{d}$, что в силу двоичности векторов равносильно тому, что $P(V) \neq P(U)$, что и требовалось доказать.

Определение 2 показывает и сходство, и различие между разделимыми кодами и идентифицирующими кодами [14], также известными как коды со свойством отождествления родителей, или IPP-коды [9]. Напомним, что q-ичный код C называется *t-IPP-кодом*, если для любого вектора $\boldsymbol{z}$ либо

$$\bigcap_{U\colon \boldsymbol{z}\in P(U),\, U\subset C,\, |U|\leqslant t} U \neq \varnothing, \tag{15}$$

либо не существует кодового подмножества U (коалиции), такого что $\boldsymbol{z} \in P(U)$ и $|U| \leqslant t$. Таким образом, в случае IPP-кодов по любой точке $\boldsymbol{z}$ из полной проекции $P(U)$ коалиции U система может гарантированно найти хотя бы одного члена коалиции. Отметим, что в такой постановке задачи *найти коалицию целиком невозможно*, за исключением случая тривиальных кодов, мощность которых не более мощности алфавита. Действительно, рассмотрим произвольный q-ичный код C мощности $|C| > q$. Пусть i – некоторая координата, такая что $|P_i(C)| > 1$. Так как $|C| > q$, то существуют векторы $\boldsymbol{b}, \boldsymbol{b}' \in C$, такие что $b_i = b'_i$. Так как $|P_i(C)| > 1$, то существует вектор $\boldsymbol{a} \in C$, такой что $a_i \neq b_i$. Тогда вектор $\boldsymbol{z}$, который совпадает с вектором $\boldsymbol{a}$ во всех координатах, кроме i, где $z_i = b_i$, порождается двумя разными коалициями: $\{\boldsymbol{a}, \boldsymbol{b}\}$ и $\{\boldsymbol{a}, \boldsymbol{b}'\}$.

Очень важным является следующий факт, впервые отмеченный в [15], что понятие разделимых кодов совпадает с известным в теории информации понятием сигнатурных кодов для А-канала множественного доступа. Напомним соответствующие определения.

Мы будем рассматривать детерминированные каналы множественного доступа без памяти (сокращенно, MAC – multiple access channel) с дискретным временем и частичной активностью (см. [18]). MAC задается входным и выходным алфавитами X и Y и функцией выхода $f\colon X^M \to Y$, такой что выход MAC равен $y = f(x_1, \ldots, x_M)$, где $x_j \in X \cup \varnothing$ – символ, подаваемый на вход канала j-м пользователем, причем $x_j = \varnothing$ означает, что j-й пользователь ничего не подал на вход MAC, т.е. был не активен.

Нас будут особо интересовать *t-сигнатурные* коды, когда каждому пользователю сопоставлено только одно кодовое слово, а именно j-му пользователю сопоставлено слово $\boldsymbol{c}_j$, и не более чем t пользователей активны, т.е. передают в канал свои кодовые слова. Если при этом по выходу канала можно однозначно восстановить, какие пользователи были активны, при условии, что их было не более t, то код $C = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\}$ называется *t-сигнатурным*. Далее мы будем отождествлять пользователя и соответствующее ему кодовое слово. Для активного множества пользователей U будем обозначать через S_U соответствующий выход MAC.

О п р е д е л е н и е 3. Код C называется *t-сигнатурным*, если для любых двух различных подмножеств $U, V \subset C$, таких что $|U|, |V| \leqslant t$, справедливо $S_U \neq S_V$.

Наиболее важными для нас примерами MAC являются А-канал, $\vee$-канал и двоичный суммирующий канал, см. [18].

Для булева суммирующего канала, сокращенно $\vee$-канала, $X = Y = \{0, 1\}$ и $f(x_1, \ldots, x_t) = x_1 \vee \ldots \vee x_t$.

Для двоичного суммирующего канала, сокращенно Σ-канала, $X = \{0, 1\}$, $Y = \{0, 1, 2, \ldots\}$ и

$$f(x_1, \ldots, x_t) = x_1 + \ldots + x_t \in \mathbb{Z}.$$

Для А-канала вход X – произвольное конечное множество, $Y = 2^X$ – множество всех подмножеств X и $f(x_1, \ldots, x_t) = \{x_1, \ldots, x_t\}$. Например, для $X = \{0, 1, 2\}$ имеем $f(0, 1, 1, 0) = \{0, 1\}$. Тем самым, в А-канале для любого множества $U \subset C$ справедливо $S_U = P(U)$, и следовательно, t-разделимый код – это то же самое, что t-сигнатурный код для А-канала. Этот факт впервые был отмечен в [15], и начиная с этой работы, сигнатурные коды стали интенсивно использоваться при изучении кодов для защиты мультимедийной информации.

Модель А-канала была введена в работе [16] вместе с В-каналом, выходом которого является не только множество символов, переданных активными пользователями, но и кратности, с которыми эти символы были использованы.

Введем *частичный порядок на каналах множественного доступа*. Пусть каналы $\mathcal{A}$ и $\mathcal{B}$ задаются одним и тем же входным алфавитом X, множествами выходов $Y_{\mathcal{A}}$ и $Y_{\mathcal{B}}$ и функциями выхода $f_{\mathcal{A}}$ и $f_{\mathcal{B}}$. Будем говорить, что канал $\mathcal{A}$ меньше, чем канал $\mathcal{B}$, и обозначать $\mathcal{A} \prec \mathcal{B}$, если существует отображение $g\colon Y_{\mathcal{B}} \to Y_{\mathcal{A}}$, такое что для любого набора $x_1, \ldots, x_m$ справедливо

$$g(f_{\mathcal{B}}(x_1, \ldots, x_m)) = f_{\mathcal{A}}(x_1, \ldots, x_m). \tag{16}$$

Соотношение (16) говорит, что "больший" канал $\mathcal{B}$ дает "больше информации", чем канал $\mathcal{A}$, а именно что по выходу канала $\mathcal{B}$ можно однозначно восстановить выход канала $\mathcal{A}$. Отсюда следует, что если $\mathcal{A} \prec \mathcal{B}$ и код $C \subset X^n$ является t-сигнатурным кодом для канала $\mathcal{A}$, то он является t-сигнатурным кодом и для канала $\mathcal{B}$.

В двоичном случае, т.е. при $X = \{0, 1\}$, имеет место следующее упорядочение: $\vee$-канал $\prec$ A-канал $\prec$ B-канал.

Отметим, что в работе [3] было показано, что t-дизъюнктивные (t-superimposed) коды, введенные в [40], являются t-разделимыми кодами. Действительно, t-дизъюнктивный код является t-сигнатурным кодом для $\vee$-канала, а так как $\vee$-канал "меньше" А-канала, то t-дизъюнктивный код является t-сигнатурным кодом для А-канала, т.е. является t-разделимым кодом. Поэтому условие дизъюнктивности является достаточным для разделимости, но не необходимым. Мы обсудим это подробнее в следующем параграфе.

§ 3. Разделимые, разделяющие и дизъюнктивные коды

Как было объяснено в предыдущем параграфе, разделимые коды – это то же самое, что сигнатурные коды для *двоичного* А-канала множественного доступа. Так как А-канал определен для любого конечного алфавита, то естественно обобщить определение 3 разделимого кода на случай произвольного алфавита.

Пусть X – конечный алфавит мощности q. Для произвольного множества $A \subset X^m$ обозначим через

$$P(A) = \{(x_1, \ldots, x_m) \in X^m : \; x_1 \in P_1(A), \; \ldots, \; x_m \in P_m(A)\} \tag{17}$$

его полную проекцию, где $P_i(A) := \{a_i : \boldsymbol{a} \in A\}$ – это проекция множества A на i-ю координату. Таким образом, $P(A) = P_1(A) \times \ldots \times P_m(A)$.

О п р е д е л е н и е 4. Код $C \subset X^m$ называется *t-разделимым*, если для любых двух различных подмножеств $U, V \subset C$, таких что $|U|, |V| \leqslant t$, справедливо $P(U) \neq P(V)$.

Таким образом, для разделимого кода любое его подмножество мощности не более t может быть однозначно найдено по своей полной проекции. Как уже отмечалось, свойство t-разделимости кода совпадает со свойством кода быть t-сигнатурным для А-канала, т.е. позволяет по выходу А-канала однозначно восстановить, какие пользователи были активны.

Исторически еще раньше, в 60-е годы прошлого века [41], появилось понятие *разделяющего* кода, см. [30].

Определение 5. q-ичный код C называется (t_1, t_2)-разделяющим, если для любых двух непересекающихся подмножеств $U, V \subset C$, таких что $|U| \leqslant t_1$, $|V| \leqslant t_2$, существует координата i, которая их разделяет, т.е. $P_i(U) \cap P_i(V) = \varnothing$.

Следующее утверждение, доказанное в [3], показывает, что понятия t-разделимого кода и $(1, t)$-разделяющего кода близки.

Предложение 1. *$(1, t)$-разделяющий код является t-разделимым, а t-разделимый код является $(1, t-1)$-разделяющим.*

Доказательство. Очевидно, что для любого $(1, t)$-разделяющего кода C его произвольное подмножество (коалиция) $U \subset C : |U| \leqslant t$ может быть найдено по своей полной проекции $P(U)$ следующим образом:

$$U = \{\boldsymbol{c} \in C : \boldsymbol{c} \in P(U)\}. \tag{18}$$

Покажем теперь, что t-разделимый код C является $(1, t-1)$-разделяющим. Рассмотрим произвольное кодовое подмножество U мощности не более $t-1$ и произвольное кодовое слово $\boldsymbol{a} \notin U$ и сформируем кодовое множество $V = U \cup \boldsymbol{a}$. Тогда в силу t-разделимости кода должно быть $P(U) \neq P(V)$, и следовательно, существует координата i, такая что $a_i \notin P_i(U)$, что и требовалось доказать. ▲

Замечание 4. Частные случаи разделяющих кодов были переоткрыты в работах по кодам цифровых отпечатков пальцев: $(1, t)$-разделяющие коды под именем t-frameproof codes, а (t, t)-разделяющие коды – под именем t-secure frameproof codes [11]. Новая терминология не принесла новых результатов, за исключением исследования нетрадиционного для теории кодирования случая, когда мощность алфавита растет, а длина кода фиксирована (см., например, [42]).

Обозначим через $A^q_{\text{sep}}(t, n)$ максимально возможную мощность q-ичного t-разделимого кода длины n, а через $A^q_s(t, n)$ – максимально возможную мощность q-ичного $(1, t)$-разделяющего кода длины n. Тогда из предложения 1 следует, что

$$A^q_s(t, n) \leqslant A^q_{\text{sep}}(t, n) \leqslant A^q_s(t-1, n).$$

Как обычно, мы будем опускать символ q, когда речь идет о двоичных кодах. Также будем рассматривать асимптотическое поведение мощности наилучших кодов в виде их скорости, определяемой как

$$R_{\text{sep}}(t) = \lim_{n\to\infty} n^{-1} \log_2 A_{\text{sep}}(t, n)$$

и

$$R_s(t) = \lim_{n\to\infty} n^{-1} \log_2 A_s(t, n)$$

соответственно. Мы здесь допускаем некую вольность записи, так как мы не доказываем существования соответствующих пределов (хотя вероятно, что это можно сделать аналогично тому, как это было сделано для обычных кодов в [43]). Поэтому нижеследующие границы надо рассматривать как оценки на нижний и верхний пределы соответственно.

При малых t известные результаты относительно этих двух классов кодов заметно различаются. Например, для скорости $R_s(t)$ лучших двоичных $(1, 2)$-разделяющих кодов известно, что

$$0{,}207565 \leqslant R_s(2) \leqslant 1/2, \tag{19}$$

где нижняя граница получена сравнительно недавно в [44] с помощью алгеброгеометрических кодов, что позволило улучить известный задолго до этого аналог гра-

ницы Варшамова – Гилберта (или случайного кодирования)

$$R_s(2) \geqslant 1 - 2^{-1}\log_2 3 = 0{,}207518.$$

Покажем, что при числе активных пользователей не более двух асимптотика скорости наилучших сигнатурных кодов для двоичных суммирующего канала и А-канала асимптотически совпадают. Легко проверить, что если априори известно число активных пользователей и оно не больше чем 2, то двоичные А-канал и суммирующий канал эквивалентны (т.е. совпадают при соответствующей перенумерации выходов каналов). Пусть C – это 2-сигнатурный код для суммирующего канала. Так как все слова кода C различны, то среди координат выхода А-канала для пары слов обязательно есть символ $*$, которого нет в случае одного активного пользователя, следовательно, C различает случай одного или двух активных пользователей и поэтому является 2-сигнатурным кодом и для А-канала. Пусть C – это 2-сигнатурный код для А-канала. Удлиним C на одну координату, сделав ее равной 1 для всех кодовых слов. Тогда новый код различает случай одного или двух активных пользователей в суммирующем канале и поэтому является 2-сигнатурным кодом и для суммирующего канала.

Поэтому известные границы для скорости 2-сигнатурных кодов в суммирующем канале справедливы и для двоичных 2-разделимых кодов:

$$1/2 \leqslant R_{\mathrm{sep}}(2) \leqslant 0{,}5753, \tag{20}$$

где нижняя граница – это стандартная граница случайного кодирования, а верхняя граница получена в [45].

Имеется хорошо известная связь между двоичными $(1,t)$-разделяющими кодами и t-дизъюнктивными [40] кодами.

Определение 6. Двоичный код C называется *t-дизъюнктивным*, если для любого кодового подмножества $U \subset C$ мощности не более t и произвольного кодового слова $\boldsymbol{a} \notin U$ существует координата i, такая что $a_i = 1$, тогда как $u_i = 0$ для всех $\boldsymbol{u} \in U$ (т.е. $P_i(U) = 0$).

Дизъюнктивные коды были переоткрыты в экстремальной комбинаторике под названием семейства множеств без t-покрытий [46, 47], т.е. таких семейств, что ни одно множество семейства не покрывается объединением t других множеств этого семейства.

Очевидно, что t-дизъюнктивный код C является t-сигнатурным кодом для $\vee$-канала, т.е. для любых двух различных подмножеств $U, V \subset C$, таких что $|U|, |V| \leqslant t$, справедливо

$$\bigvee_{\boldsymbol{u}\in U} \boldsymbol{u} \neq \bigvee_{\boldsymbol{v}\in V} \boldsymbol{v}. \tag{21}$$

Это следует, например, из того, что если выход $\vee$-канала при использовании t-дизъюнктивного кода C равен $\boldsymbol{S}(U) = \boldsymbol{S} = (s_1, \ldots, s_m)$, то на вход были поданы векторы $\boldsymbol{c} \in C$, такие что $u_i \leqslant s_i$ для всех i, ср. (18).

Тем самым, t-дизъюнктивные коды играют для $\vee$-канала ту же роль, что $(1,t)$-разделяющие коды для А-канала. Очевидно, что t-дизъюнктивный код является двоичным $(1,t)$-разделяющим кодом. С другой стороны, пусть C – это двоичный $(1,t)$-разделяющий код длины n. Легко видеть, что код C^* длины $2n$, состоящий из слов вида $(\boldsymbol{x}, \overline{\boldsymbol{x}})$, где $\overline{\boldsymbol{x}}$ – двоичный вектор, полученный из вектора $\boldsymbol{x}$ инвертированием всех координат, является t-дизъюнктивным кодом. Поэтому если обозначить через $R_\vee(t)$ максимальную скорость t-дизъюнктивных кодов, то выполнено следу-

ющее соотношение:

$$R_\vee(t) \leqslant R_s(t) \leqslant 2R_\vee(t). \tag{22}$$

Для больших t известны следующие асимптотические границы, которые мы приведем для двоичного случая, а общий случай подробно исследован в [48]. Итак, при больших t

$$\Theta\Big(\frac{1}{t^2}\Big) \leqslant R_s(t) \leqslant R_{\mathrm{sep}}(t) \leqslant O\Big(\frac{\log t}{t^2}\Big). \tag{23}$$

Нижняя граница в (23) была получена в [30] стандартным методом случайного кодирования с выбрасыванием (см. [49]), тогда как верхняя граница была сначала получена для дизъюнктивных кодов в [46,47,50] и только затем перенесена на $(1,t)$-разделяющие коды с помощью (22).

§ 4. Разделимые и разделяющие коды с простым декодированием и исправлением ошибок

Так как нижняя граница в (23) – это граница существования, то возникает традиционный вопрос о кодах с "простыми" (т.е. со сложностью, полиномиальной от длины кода) алгоритмами построения кода, его кодирования и декодирования. Такой класс кодов, основанный на каскадной конструкции и "мягком" декодировании каскадных кодов [51, 52], был предложен в [15].

Дадим описание каскадной конструкции, следуя [53]. Имеются два кода: q-ичный код C длины m и мощности Q, называемый внутренним кодом, и Q-ичный код W длины N и мощности M, называемый внешним кодом, и взаимно-однозначное отображение $\varphi\colon GF(Q) \to C$. Каскадный код V состоит из слов вида $\boldsymbol{v} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N) = \Phi(\boldsymbol{w})$, где $\boldsymbol{v}_i = \varphi(w_i) \in C$ и $\boldsymbol{w} = (w_1, \ldots, w_N) \in W$. Этот код q-ичный, длины Nm и мощности M. В каскадной конструкции свойства внутреннего и внешнего кодов часто "наследуются". Так, нам понадобится хорошо известный (и просто проверяемый) факт (см. [30]), что *каскадный код, у которого и внутренний и внешний коды являются* $(1,t)$*-разделяющими, также является* $(1,t)$*-разделяющим.*

Также будет полезно следующее простое замечание.

Предложение 2. *Если расстояние кода больше чем* $n(1-t^{-1})$*, где* n *– его длина, то код является* $(1,t)$*-разделяющим.*

Действительно, пусть это не так и существует кодовое слово $\boldsymbol{c}$ и подмножество кода $U : |U| \leqslant t$, которые не разделяются. Тогда число совпадений координат между $\boldsymbol{c}$ и словами из U не менее n, а с другой стороны, из неравенства на расстояние кода следует, что любые два кодовых слова совпадают менее чем в nt^{-1} позициях, а так как слов в U не более чем t, то число совпадений координат между $\boldsymbol{c}$ и словами из U меньше n. Это рассуждение применялось многократно, видимо, начиная с [54], в том числе для доказательства существования IPP-кодов [7].

Опишем конструкцию из [15]. В качестве внутреннего кода берется двоичный $(1,t)$-разделяющий код C длины m и мощности Q, а в качестве внешнего – код Рида – Соломона W над полем $GF(Q)$ длины $N = Q$ и размерности $K = N/t$, т.е. код со скоростью $R = 1/t$. Каскадный код V состоит из слов вида $\boldsymbol{v} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N) = \Phi(\boldsymbol{w})$, где $\boldsymbol{v}_i = \varphi(w_i) \in C$ и $\boldsymbol{w} = (w_1, \ldots, w_N) \in W$. Из сказанного выше следует, что этот каскадный код является двоичным $(1,t)$-разделяющим кодом длины Nm и мощности $Q^{N/t}$. Для его декодирования в A-канале мы будем использовать алгоритм Гуруcвами – Судана "мягкого" списочного декодирования кодов Рида – Соломона, предложенный в [51, 52].

Пусть символам α конечного поля $GF(Q)$ приписаны неотрицательные веса ("надежности") $r_i(\alpha)$ в зависимости от координаты $i \in \{1, \ldots, N\}$. Определим вес ("надежность") кодового вектора $\boldsymbol{w}$ как

$$r(\boldsymbol{w}) = \sum_{i=1}^{N} r_i(w_i).$$

Алгоритм [51, 52] позволяет найти за полиномиальное от N время список всех слов кода Рида – Соломона, таких что

$$r(\boldsymbol{w}) \geqslant r_{\text{crit}} = \sqrt{NR\sigma}, \tag{24}$$

где $\sigma = \sum\limits_{i=1}^{N} \sum\limits_{\alpha \in GF(Q)} r_i^2(\alpha)$, а $R = K/N$ – скорость кода Рида – Соломона.

Опишем работу алгоритма декодирования в A-канале. Пусть на вход A-канала поступили кодовые векторы $\boldsymbol{v}^1 = \Phi(\boldsymbol{w}^1)$, ..., $\boldsymbol{v}^{t'} = \Phi(\boldsymbol{w}^{t'})$, где $t' \leqslant t$. Пусть

$$\mathbf{s} = (s_{11}, \ldots, s_{1m}, s_{21}, \ldots, s_{2m}, \ldots, s_{N1}, \ldots, s_{Nm}) = (\boldsymbol{s}_1, \ldots, \boldsymbol{s}_N)$$

– соответствующий выход A-канала. Первый шаг алгоритма состоит в декодировании векторов $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_N$ внутренним $(1, t)$-разделяющим кодом C длины m, например, полным перебором всех слов кода C, что потребует $O(Qm)$ операций. В результате будут получены некоторые подмножества $A_1, \ldots, A_N$ слов кода C, $|A_i| := t_i \leqslant t$ для всех i, и соответствующие им подмножества $H_i = \varphi^{-1}(A_i)$ символов поля $GF(Q)$.

Зададим веса следующим образом: $r_i(\alpha) = 1$, если $\alpha \in H_i$, и $r_i(\alpha) = 0$ в противном случае. Из свойства $(1, t)$-разделимости кода C следует, что i-е координаты векторов $\boldsymbol{w}^1, \ldots, \boldsymbol{w}^{t'}$ принадлежат множеству H_i при всех i, и следовательно, $r(\boldsymbol{w}^j) = N$ для всех $j = 1, \ldots, t'$. С другой стороны, так как данный код Рида – Соломона является $(1, t)$-разделяющим (в силу того, что его расстояние $d = N - K + 1 > N(1 - t^{-1})$), то для любого другого кодового слова $\boldsymbol{w}$ существует как минимум одна координата, не принадлежащая соответствующему множеству H_i, и следовательно, $r(\boldsymbol{w}) \leqslant N - 1$.

В силу (24) алгоритм Гурусвами – Судана выдаст все слова $\boldsymbol{w}^1, \ldots, \boldsymbol{w}^{t'}$ в составе списка, но, возможно, и некоторые "лишние", которые будут затем отброшены как не прошедшие проверку $r(\boldsymbol{w}) = N$. Полиномиальность построения кода, его кодирования и декодирования следует, как обычно, из того, что мощность внутреннего кода Q растет экспоненциально от длины m, следовательно, длина итогового (каскадного) кода, равная Qm, растет так же, и основной вклад в сложность декодирования составляет сложность декодирования кода Рида – Соломона, а она полиномиальна от Q.

Замечание 5. Для дизъюнктивных кодов известна другая конструкция кодов с полиномиальной сложностью построения, кодирования и декодирования кода [55]. Достоинством предложенной здесь каскадной конструкции является то, что она легко обобщается на случай, когда синдром может быть ошибочным, см. ниже.

Как мы уже отмечали, переход от непрерывной модели мультимедийных кодов, находящих коалицию недобросовестных пользователей целиком, т.е. t-МППК-кодов (см. определение 1), к дискретной модели мультимедийных кодов, также находящих коалицию целиком, т.е. к разделимым кодам (см. определения 2 и 4), неминуемо ведет к ошибкам дискретизации в силу неточности измерений. Другой возможный источник ошибок – это недобросовестные пользователи (участники коалиции). Среди возможных моделей ошибок в этом параграфе мы уделим основное внимание комбинаторной модели ошибок, когда любой из символов на выходе A-канала может быть изменен, но число изменений-ошибок заранее ограничено сверху некоторой величи-

ной T. Этот класс ошибок также часто называют целенаправленными (adversarial), имея в виду ситуацию, когда некто пытается обмануть систему и вносит произвольные ошибки, но число вносимых ошибок заранее ограничено сверху.

Ясно, что комбинаторная модель ошибок применима к любому каналу множественного доступа. Введем следующее

Определение 7. Код C называется *t-сигнатурным кодом, исправляющим T ошибок в канале множественного доступа*, если по выходу канала, искаженному не более чем в T координатах, однозначно восстанавливается множество активных пользователей мощности не более t.

Эквивалентное этому определению условие таково:

Для любых двух различных кодовых подмножеств U и V мощности не более t каждое справедливо

$$d_H(S_U, S_V) > 2T, \tag{25}$$

где d_H – расстояние Хэмминга.

Дадим соответствующее определение для разделяющих кодов, обобщающее определение 5.

Определение 8. q-ичный код C называется *(t_1, t_2)-разделяющим с исправлением T ошибок*, если для любых двух непересекающихся подмножеств $U, V \subset C$, таких что $|U| \leqslant t_1$, $|V| \leqslant t_2$, число разделяющих их координат больше $2T$, т.е.

$$|\{i:\ P_i(U) \cap P_i(V) = \varnothing\}| > 2T. \tag{26}$$

В частности, код C является *$(1, t)$-разделяющим кодом с исправлением T ошибок*, если для любого кодового вектора $\boldsymbol{c} \in C$ и любого t-множества кода U: $\boldsymbol{c} \notin U$ имеется больше чем $2T$ разделяющих их координат. Очевидно, что такой код является t-сигнатурным кодом, исправляющим T ошибок в A-канале.

Отметим, что определение 8 появилось в работе [56] из других соображений (см. также [57]). А именно было показано, как из (t_1, t_2)-разделяющего кода получить $(t_1 - 1, t_2 - 1)$-разделяющий код с довольно большим расстоянием Хэмминга, что привело к новым верхним границам на мощность (t_1, t_2)-разделяющих кодов. Эта техника получения верхних границ для мощности (t_1, t_2)-разделяющих кодов была независимо переоткрыта в [58]. Заметим, что, к сожалению, эта техника не применима к $(1, t)$-разделяющим кодам.

Обобщим предложение 2 на случай исправления ошибок.

Предложение 3. *Если расстояние кода больше чем $n(1 - t^{-1}(1 - 2\tau))$, где n – его длина, то код является $(1, t)$-разделяющим кодом с исправлением $T = \tau n$ ошибок.*

Доказательство. Рассмотрим произвольное подмножество кода $U : |U| \leqslant t$ и любое кодовое слово $\boldsymbol{c}$ не из U. Тогда число совпадений координат между $\boldsymbol{c}$ и любым словом из U меньше чем $n\dfrac{1 - 2\tau}{t}$, следовательно, общее число совпадений координат между $\boldsymbol{c}$ и U меньше чем $n(1 - 2\tau)$. Тем самым, число координат, разделяющих $\boldsymbol{c}$ и U, больше $2n\tau$. ▲

Обобщим описанные выше конструкцию и алгоритм декодирования из [15] так, чтобы исправлять $T = \tau N$ ошибок. Внутренний код оставим без изменений, т.е. возьмем двоичный $(1, t)$-разделяющий код C длины m и мощности Q, а в качестве внешнего возьмем код Рида – Соломона W над полем $GF(Q)$ длины $N = Q$ и скорости $R = \dfrac{1 - 2\tau}{t}$.

Как и в исходном алгоритме, применимом к А-каналу без ошибок, первый шаг состоит в декодировании векторов $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_N$ внутренним $(1, t)$-разделяющим кодом C.

Результатом декодирования являются подмножества $A_1, \dots, A_N$ слов кода C и соответствующие им подмножества $H_i = \varphi^{-1}(A_i)$ символов поля $GF(Q)$. Веса для декодирования внешнего кода оставим прежними, т.е. $r_i(\alpha) = 1$, если $\alpha \in H_i$, и $r_i(\alpha) = 0$ в противном случае.

Из свойства $(1,t)$-разделимости кода C следует, что i-я координата любого из векторов $\boldsymbol{w}^1, \dots, \boldsymbol{w}^{t'}$ принадлежит множеству H_i, если в векторе $\boldsymbol{s}_i$ не было ошибок в A-канале. Следовательно, для любого $\boldsymbol{w}^j$ справедливо $r(\boldsymbol{w}^j) \geqslant N - T = T(1-\tau)$, так как без ошибок $r(\boldsymbol{w}^j) = N$. С другой стороны, в силу предложения 3 для любого кодового слова $\boldsymbol{w}$ не из коалиции число координат, разделяющих это слово и коалицию, больше чем $2T$, а так как ошибки могли уменьшить это число максимум на T, то $r(\boldsymbol{w}) < N - T = N(1-\tau)$. При этом алгоритм декодирования Гурусвами – Судана выдаст все слова кода, для которых $r(\boldsymbol{w}) \leqslant r_{\mathrm{crit}}$, где

$$r_{\mathrm{crit}} = \sqrt{NR\sigma} \leqslant \sqrt{N\frac{1-2\tau}{t}Nt} = N\sqrt{1-2\tau} < N(1-\tau). \tag{27}$$

Следовательно, алгоритм выдаст все слова коалиции, а возможные лишние слова будут отсеяны неравенством $r(\boldsymbol{w}) \geqslant N - T = N(1-\tau)$.

§ 5. МППК-коды с исправлением ошибок

Мы уже отмечали, что при переходе от непрерывной модели t-МППК-кодов к дискретной модели разделимых кодов неточность измерений ведет к ошибкам в соответствующем дискретном канале MAC (A-канале). Сейчас нам будет важно, что неточность измерений вносит ошибки и для t-МППК-кодов. Другой возможный источник ошибок для t-МППК-кодов – это недобросовестные пользователи (участники коалиции). Мы ограничимся рассмотрением t-МППК-кодов, способных исправлять ошибки, у которых ограничена сверху норма вектора ошибки в евклидовой метрике [24]. В [17] была рассмотрена другая модель ошибок – *разреженные ошибки*, т.е. когда ошибки могут изменить не более заранее заданного числа координат в векторе-синдроме $\boldsymbol{S}(\Lambda)$ (см. уравнения (5), (7)), но зато нет никаких ограничений на величину ошибки в изменяемых координатах. Конструкция соответствующих кодов, предложенная в [17] (см. также [59,60]), по существу излагается ниже как часть построения t-ДЕД-кодов.

Будем, следуя [36], рассматривать атаку коалиции A, которая не только создает ложную копию $\boldsymbol{y} = \boldsymbol{x} + \sum\limits_{j\in A} \lambda_j \boldsymbol{w}_j \in \mathbb{R}^N$ в соответствии с моделью линейной атаки, но еще целенаправленно добавляет вектор шума $\boldsymbol{e} \in \mathbb{R}^N$, такой что $\|\boldsymbol{e}\| \leqslant \delta$, где $\|\cdot\|$ – евклидова норма на $\mathbb{R}^N$. В результате коалиция A перераспределяет копию

$$\widehat{\boldsymbol{y}} = \boldsymbol{x} + \sum_{j\in A} \lambda_j \boldsymbol{w}_j + \boldsymbol{e}, \tag{28}$$

где $\boldsymbol{w}_j = \sum\limits_{i=1}^{m} h_{ij}\boldsymbol{f}_i$ (см. (1)). Координаты синдрома $\boldsymbol{S} = \boldsymbol{S}(\Lambda) = (s_1, \dots, s_m)$ равны

$$s_k = \left(\boldsymbol{e} + \sum_{j=1}^{M} \lambda_j \sum_{i=1}^{m} h_{ij}\boldsymbol{f}_i, \boldsymbol{f}_k\right) = (\boldsymbol{e}, \boldsymbol{f}_k) + \sum_{j=1}^{M} \lambda_j h_{kj} = \varepsilon_k + \sum_{j\in A} \lambda_j h_{kj} \tag{29}$$

(см. (5)), где $\varepsilon_k = (\boldsymbol{e}, \boldsymbol{f}_k)$, и длина вектора $\varepsilon = (\varepsilon_1, \dots, \varepsilon_m)$, равная $\|\varepsilon\| = \sqrt{\sum\limits_{i=1}^{m} \varepsilon_i^2}$, не превышает длины вектора $\boldsymbol{e}$ в силу неравенства Бесселя.

Как отмечалось в начале § 2, множество $\mathcal{W} = \{\boldsymbol{w}_1, \dots, \boldsymbol{w}_M\} \subset \mathbb{R}^N$ и двоичный код $\mathcal{H} = \{\boldsymbol{h}_1, \dots, \boldsymbol{h}_M\} \subset B^m$ изометричны, и далее мы будем рассматривать код $\mathcal{H}$. Двоичный код $\mathcal{H}$ естественно называть (t,δ)-*МППК-кодом со свойством полного поиска*

t-коалиций и устойчивым к δ-шуму, если по любой ложной копии $\widehat{\boldsymbol{y}} = \sum\limits_{j\in A} \lambda_j \boldsymbol{y}_j + \boldsymbol{e}$ можно однозначно найти коалицию A.

Это условие равносильно тому, что для любых двух вещественных векторов $\Lambda = (\lambda_1, \ldots, \lambda_M)$ и $\Lambda' = (\lambda'_1, \ldots, \lambda'_M)$, таких что все λ_j и λ'_j неотрицательны, $\sum\limits_{j=1}^{M} \lambda_j = \sum\limits_{j=1}^{M} \lambda'_j = 1$ и $|\operatorname{supp}(\Lambda)|, |\operatorname{supp}(\Lambda')| \leqslant t$, из $A = \operatorname{supp}(\Lambda) \neq B = \operatorname{supp}(\Lambda')$ следует, что

$$\left\| \sum_{j\in A} \lambda_j \boldsymbol{h}_j - \sum_{j\in B} \lambda'_j \boldsymbol{h}_j \right\| > 2\delta. \tag{30}$$

В [36] было показано, что такие коды не существуют. Действительно, в качестве контрпримера положим $A = \{1, 2, \ldots, t\}$, $B = \{1, 2, \ldots, t-1, t+1\}$ и

$$\lambda_t = \lambda'_{t+1} = \lambda < \frac{\delta}{\|\boldsymbol{h}_t\| + \|\boldsymbol{h}_{t+1}\|}.$$

Выберем положительные $\lambda_j = \lambda'_j$ для $j = 1, \ldots, t-1$ такими, что $\lambda + \sum\limits_{j=1}^{t-1} \lambda_j = 1$. Тогда

$$\left\| \sum_{j\in A} \lambda_j \boldsymbol{h}_j - \sum_{j\in B} \lambda'_j \boldsymbol{h}_j \right\| = \|\lambda(\boldsymbol{h}_t - \boldsymbol{h}_{t+1})\| < \delta,$$

и неравенство (30) не выполнено.

В [24] было предложено ограничиться только атакой усреднения и исследовать коды, находящие коалицию целиком в этом случае.

Определение 9. Двоичный код $\mathcal{H}$ называется (t, δ)-*мультимедийным кодом со свойством полного поиска коалиций, устойчивым к атаке усреднения и δ-шуму* ((t, δ)-МППК-кодом), если для любых двух различных подмножеств кода $A, B \subset \mathcal{H}$, таких что $|A|, |B| \leqslant t$, справедливо неравенство

$$\left\| \frac{1}{|A|} \sum_{j\in A} \boldsymbol{h}_j - \frac{1}{|B|} \sum_{j\in B} \boldsymbol{h}_j \right\| > 2\delta. \tag{31}$$

Обозначим через $\mathcal{M}(m, t, \delta)$ максимальную мощность (t, δ)-МППК-кода и определим соответствующую максимальную скорость

$$\mathcal{R}(m, t, \delta) := m^{-1} \log_2 \mathcal{M}(m, t, \delta).$$

Основным результатом [24] стало доказательство существования (t, δ)-мультимедийных кодов со скоростью, отделенной от нуля. А именно: для фиксированных t и δ

$$\liminf_m \mathcal{R}(m, t, \delta) \geqslant \frac{\gamma_t \log_2 e}{t(1 + \gamma_t \log_2 e)} > \frac{\log_2 e}{t(e + \log_2 e)} > \frac{0{,}346}{t}, \tag{32}$$

где $\gamma_t = (1 - t^{-1})^{t-1}$.

Построение таких кодов в [24] было разбито на две подзадачи: первая – построение (t, δ)-МППК-кодов для случая, когда мощность коалиции заранее известна, а вторая – построение кодов, которые позволяют найти мощность коалиции по ложной копии.

Решение первой подзадачи заключается в построении двоичного кода $\mathcal{C} = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\}$, такого что для любых двух различных подмножеств кода $A, B \subset \mathcal{C}$,

таких что $|A| = |B| \leqslant t$, справедливо неравенство

$$\left\| \sum_{\boldsymbol{c} \in A} \boldsymbol{c} - \sum_{\boldsymbol{c}' \in B} \boldsymbol{c}' \right\| > 2\Delta. \tag{33}$$

Действительно, такой код $\mathcal{C}$ позволит однозначно найти всю коалицию при атаке усреднения и δ-шуме, где $\delta = \Delta/t$, если мощность коалиции заранее известна и не превышает t.

Отметим, вслед за [24], что если в определении 9 неравенство

$$\left\| \frac{1}{|A|} \sum_{j \in A} \boldsymbol{h}_j - \frac{1}{|B|} \sum_{j \in B} \boldsymbol{h}_j \right\| > 2\delta$$

заменить на неравенство

$$\left\| \sum_{j \in A} \boldsymbol{h}_j - \sum_{j \in B} \boldsymbol{h}_j \right\| > 2\delta,$$

то получится определение *двоичных* евклидовых дизъюнктивных кодов, тогда как в задаче о евклидовых дизъюнктивных кодах в качестве $\boldsymbol{h}_j$ рассматривались *произвольные* векторы евклидова пространства, см. [61, 62]. Тем самым, рассматриваемая нами подзадача – это задача о двоичных евклидовых дизъюнктивных кодах с одинаковой мощностью коалиций. Будем такие коды сокращенно называть t-ДЕД-кодами. Опишем построение таких кодов, которое навеяно конструкцией [63] (см. также [59, 60, 64]).

Построение t-ДЕД-кодов. Выберем, как мы уже делали при построении t-МППК-кодов, в качестве кода $\widehat{\mathcal{H}}$ столбцы проверочной $(m \times M)$-матрицы линейного двоичного кода V, исправляющего t ошибок. Закодируем слова $\widehat{\boldsymbol{h}}_1, \ldots, \widehat{\boldsymbol{h}}_M \in \widehat{\mathcal{H}}$ двоичным кодом U длины n, с m информационными символами и минимальным кодовым расстоянием d в метрике Хэмминга. Полученные векторы $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M$ и образуют искомый код $\mathcal{H} = \{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M\}$ с $\Delta = \sqrt{d}/2$, см. [24].

Действительно, для двух произвольных различных подмножеств A, B кода $\mathcal{H}$ одинаковой мощности не более t рассмотрим векторы $\boldsymbol{h}^{(A)} = \sum\limits_{\boldsymbol{h} \in A} \boldsymbol{h}$ и $\boldsymbol{h}^{(B)} = \sum\limits_{\boldsymbol{h} \in B} \boldsymbol{h}$. Так как различные суммы *по модулю* 2 из t и менее векторов $\widehat{\boldsymbol{h}}_j$ различны, то $\boldsymbol{h}^{(A)} \bmod 2 \neq \boldsymbol{h}^{(B)} \bmod 2$. Так как векторы $\boldsymbol{h}^{(A)} \bmod 2$ и $\boldsymbol{h}^{(B)} \bmod 2$ принадлежат коду U (в силу линейности кода) и различны, то

$$d_H\big(\boldsymbol{h}^{(A)} \bmod 2, \boldsymbol{h}^{(B)} \bmod 2\big) \geqslant d,$$

где d_H – расстояние Хэмминга, Применив неравенство

$$\|\boldsymbol{a} - \boldsymbol{b}\|^2 \geqslant d_H(\boldsymbol{a} \bmod 2, \boldsymbol{b} \bmod 2),$$

справедливое для любых двух целочисленных векторов $\boldsymbol{a}$ и $\boldsymbol{b}$, получим искомое утверждение.

Перейдем теперь к построению кодов, которые могут найти мощность коалиции. Как ни странно, эта подзадача оказалась несколько сложнее первой подзадачи.

О п р е д е л е н и е 10. Будем говорить, что двоичный код C *определяет мощность коалиции вплоть до t в условиях δ-шума*, если для любых двух его под-

множеств A и B различной мощности не более t справедливо неравенство

$$\left\| \frac{1}{|A|} \sum_{c \in A} \boldsymbol{c} - \frac{1}{|B|} \sum_{c' \in B} \mathbf{c}' \right\| > 2\delta. \tag{34}$$

С помощью такого кода система сформирует итоговый код, приписывая к словам кода $\mathcal{H}$, построенного выше, в качестве "хвостов" слова кода, определяющего мощность. По "хвостам" система найдет мощность коалиции, а затем с помощью кода $\mathcal{H}$ найдет и саму коалицию.

С этой целью в [24] были введены коды, названные авторами слабыми дизъюнктивными кодами. Оказалось, что такие коды исследуются уже довольно давно, видимо, начиная с работы [65], и под разными именами. Наиболее часто они называются *селекторами* (см. [66–68]) или *t-локально тонкими семействами множеств* (см. [69]).

Будем говорить, перефразируя [66–68], что вектор $\boldsymbol{a} \in A \subset B^n$ *выделяется* из множества A, если существует координата i, такая что $a_i = 1$ и $a'_i = 0$ для всех $\boldsymbol{a}' \in A \setminus \{\boldsymbol{a}\}$. Если для двоичного кода C длины n в любом кодовом подмножестве мощности не более t выделяется не менее r векторов, то такой код называется (n, t, r)-селектором. При $r = 1$ получаем определение слабого t-дизъюнктивного кода из [24], или, если заменить двоичные векторы длины n на соответствующие подмножества, то получим определение t-локально тонкого семейства подмножеств множества из n элементов. Отметим, что при $r = t$ получается определение $(t-1)$-дизъюнктивного кода.

В действительности для построения кодов, определяющих мощность коалиции, в [24] использовалось более общее (и сильное) понятие слабого дизъюнктивного кода с исправлением ошибок. Это определение аналогично определению 8.

Определение 11. Двоичный код называется *слабым (t, T)-дизъюнктивным кодом*, если для любого кодового подмножества A, такого что $2 \leqslant |A| \leqslant t$, существует не менее T координат i, таких что $\pi_i(A) = 1$, где $\pi_i(A) := |\{\boldsymbol{a} \in A : \ a_i = 1\}|$.

В качестве примера заметим, что слабый $(2, T)$-дизъюнктивный код – это двоичный код с минимальным кодовым расстоянием в метрике Хэмминга не менее T.

В [24] методом случайного кодирования была доказана следующая нижняя граница для скорости $R(t, T)$ слабых (t, T)-дизъюнктивных кодов при фиксированных t, T:

$$R(t, T) \geqslant \frac{1}{t}\Big(1 - \frac{1}{t}\Big)^{t-1} \log_2 e > \frac{\log_2 e}{et}. \tag{35}$$

Заметим, что эта асимптотическая граница не зависит от фиксированного T.

В [24] был предложен алгоритм линейной от n сложности, который позволяет найти мощность коалиции с помощью произвольного слабого (t, T)-дизъюнктивного кода, если длина шума

$$\|\boldsymbol{e}\| \leqslant \delta = \frac{\sqrt{T}}{2\sqrt{2}} t^{-2}.$$

Естественно выбрать параметры d и T, возникающие при решении первой и второй подзадач, таким образом, чтобы обеспечиваемый уровень шума δ совпадал, что достигается при $T = 2dt^2$. А далее прямые вычисления дают границу (32) (подробнее см. [24]).

§ 6. Заключение

В статье рассмотрены коды, способные полностью обнаружить коалицию пользователей по сделанной ими нелегальной копии мультимедийного контента. Эти коды исследовались как для исходной непрерывной модели, так и для ее дискретной версии. Возникающие коды есть не что иное, как сигнатурные коды для соответствующих каналов множественного доступа, а именно, взвешенного суммирующего канала и A-канала соответственно. Как нам представляется, исследование непрерывной модели оказывается проще в силу аддитивной структуры соответствующего канала множественного доступа. Так, для этой модели известно, что скорость наилучших кодов имеет порядок $t^{-1}\log t$, тогда как для A-канала верхняя и нижняя границы скорости наилучших кодов R_A различаются по порядку в $t^{-1}\log t$ раз (см. (23)). Это различие характерно для многих дискретных моделей каналов множественного доступа, начиная с дизъюнктивного канала и кодов (см. [70, 71]).

Авторы считают своим приятным долгом выразить благодарность И.В. Воробьеву за полезные обсуждения и замечания.

СПИСОК ЛИТЕРАТУРЫ

1. *Trappe W., Wu M., Wang Z.J., Liu K.J.R.* Anti-Collusion Fingerprinting for Multimedia // IEEE Trans. Signal Process. 2003. V. 51. № 4. P. 1069–1087. https://doi.org/10.1109/TSP.2003.809378
2. *Liu K.J.R., Trappe W., Wang Z.J., Wu M., Zhao H.* Multimedia Fingerprinting Forensics for Traitor Tracing. Cairo, Egypt: Hindawi, 2005.
3. *Cheng M., Miao Y.* On Anti-Collusion Codes and Detection Algorithms for Multimedia Fingerprinting // IEEE Trans. Inform. Theory. 2011. V. 57. № 7. P. 4843–4851. https://doi.org/10.1109/TIT.2011.2146130
4. *Cheng M., Ji L., Miao Y.* Separable Codes // IEEE Trans. Inform. Theory. 2012. V. 58. № 3. P. 1791–1803. https://doi.org/10.1109/TIT.2011.2146130
5. *Wagner N.R.* Fingerprinting // Proc. 1983 IEEE Symp. on Security and Privacy. Oakland, CA, USA. Apr. 25–27, 1983. P. 18–22. https://doi.org/10.1109/SP.1983.10018
6. *Blakley G.R., Meadows C., Purdy G.B.* Fingerprinting Long Forgiving Messages // Advances in Cryptology—CRYPTO'85 (Proc. Conf. on the Theory and Application of Cryptographic Techniques. Santa Barbara, CA, USA. Aug. 18–22, 1985). Lect. Notes Comp. Sci. V. 218. Berlin: Springer, 1986. P. 180–189. https://doi.org/10.1007/3-540-39799-X_15
7. *Chor B., Fiat A., Naor M.* Tracing Traitors // Advances in Cryptology—CRYPTO'94 (Proc. 14th Annu. Int. Cryptology Conf. Santa Barbara, CA, USA. Aug. 21–25, 1994). Lect. Notes Comp. Sci. V. 839. Berlin: Springer, 1994. P. 257–270. https://doi.org/10.1007/3-540-48658-5_25
8. *Chor B., Fiat A., Naor M., Pinkas B.* Tracing Traitors // IEEE Trans. Inform. Theory. 2000. V. 46. № 3. P. 893–910. https://doi.org/10.1109/18.841169
9. *Hollmann H.D.L., van Lint J.H., Linnartz J.-P., Tolhuizen L.M.G.M.* On Codes with the Identifiable Parent Property // J. Combin. Theory Ser. A. 1998. V. 82. № 2. P. 121–133. https://doi.org/10.1006/jcta.1997.2851
10. *Barg A., Cohen G., Encheva S., Kabatiansky G., Zémor G.* A Hypergraph Approach to the Identifying Parent Property: The Case of Multiple Parents // SIAM J. Discrete Math. 2001. V. 14. № 3. P. 423–431. https://doi.org/10.1137/S0895480100376848
11. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Trans. Inform. Theory. 1998. V. 44. № 5. P. 1897–1905. https://doi.org/10.1109/18.705568
12. *Barg A., Blakley G.R., Kabatiansky G.A.* Digital Fingerprinting Codes: Problem Statements, Constructions, Identification of Traitors // IEEE Trans. Inform. Theory. 2003. V. 49. № 4. P. 852–865. https://doi.org/10.1109/TIT.2003.809570
13. *Tardos G.* Optimal Probabilistic Fingerprint Codes // J. ACM. 2008. V. 55. № 2. Art. 10 (24 pp.). https://doi.org/10.1145/1346330.1346335

14. *Кабатянский Г.А.* Идентифицирующие коды и их обобщения // Пробл. передачи информ. 2019. Т. 55. № 3. С. 93–105. https://doi.org/10.1134/S0555292319030070
15. *Egorova E., Fernandez M., Kabatiansky G., Lee M.H.* Signature Codes for the A-Channel and Collusion-Secure Multimedia Fingerprinting Codes // Proc. 2016 IEEE Int. Symp. on Information Theory (ISIT'2016). Barcelona, Spain. July 10–15, 2016. P. 3043–3047. https://doi.org/10.1109/ISIT.2016.7541858
16. *Chang S.C., Wolf J.K.* On the T-User M-Frequency Noiseless Multiple-Access Channel with and without Intensity Information // IEEE Trans. Inform. Theory. 1981. V. 27. № 1. P. 41–48. https://doi.org/10.1109/TIT.1981.1056304
17. *Egorova E., Fernandez M., Kabatiansky G., Lee M.H.* Signature Codes for Weighted Noisy Adder Channel, Multimedia Fingerprinting and Compressed Sensing // Des. Codes Cryptogr. 2019. V. 87. № 2–3. P. 455–462. https://doi.org/10.1007/s10623-018-0551-9
18. *Györfi L., Győri S., Laczay B., Ruszinkó M.* Lectures on Multiple Access Channels. Book draft, 2005. Available at http://www.szit.bme.hu/~gyori/AFOSR_05/book.pdf.
19. *Mathys P.* A Class of Codes for T Active Users out of N Multiple-Access Communication System // IEEE Trans. Inform. Theory. 1990. V. 36. № 6. P. 1206–1219. https://doi.org/10.1109/18.59923
20. *Donoho D.L.* Compressed Sensing // IEEE Trans. Inform. Theory. 2006. V. 52. № 4. P. 1289–1306. https://doi.org/10.1109/TIT.2006.871582
21. *Candes E.J., Tao T.* Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies? // IEEE Trans. Inform. Theory. 2006. V. 52. № 12. P. 5406–5425. https://doi.org/10.1109/TIT.2006.885507
22. *Кашин Б.С., Темляков В.Н.* Замечание о задаче сжатого измерения // Матем. заметки. 2007. Т. 82. № 6. С. 829–837. https://doi.org/10.4213/mzm4183
23. *Kabatiansky G., Fernandez M., Egorova E.* Multimedia Fingerprinting Codes Resistant against Colluders and Noise // Proc. 8th IEEE Int. Workshop on Information Forensics and Security (WIFS'2016). Abu Dhabi, UAE. Dec. 4–7, 2016. P. 1–5. https://doi.org/10.1109/WIFS.2016.7823904
24. *Егорова Е.Е., Фернандес М., Кабатянский Г.А., Мяо И.* Существование и конструкции мультимедийных кодов, способных находить полную коалицию при атаке усреднения и шуме // Пробл. передачи информ. 2020. Т. 56. № 4. С. 97–108. https://doi.org/10.31857/S0555292320040087
25. *Wolf J.K.* Born Again Group Testing: Multiaccess Communications // IEEE Trans. Inform. Theory. 1985. V. 31. № 2. P. 185–191. https://doi.org/10.1109/TIT.1985.1057026
26. *Rényi A.* On a Problem in Information Theory // Magyar Tud. Akad. Mat. Kutató Int. Közl. 1961. V. 6. P. 505–516.
27. *Ulam S.M.* Adventures of a Mathematician. New York: Scribner, 1976.
28. *Pelc A.* Solution of Ulam's Problem on Searching with a Lie // J. Combin. Theory Ser. A. 1987. V. 44. № 1. P. 129–140. https://doi.org/10.1016/0097-3165(87)90065-3
29. *Kabatiansky G.A., Egorova E.E.* Adversarial Multiple Access Channels and a New Model of Multimedia Fingerprinting Coding // Proc. 2020 IEEE Conf. on Communications and Network Security (CNS'2020). Avignon, France. June 29 – July 1, 2020. P. 1–5. https://doi.org/10.1109/CNS48642.2020.9162248
30. *Сагалович Ю.Л.* Разделяющие системы // Пробл. передачи информ. 1994. Т. 30. № 2. С. 14–35. http://mi.mathnet.ru/ppi228
31. *Cohen G.D., Schaathun H.G.* Asymptotic Overview on Separating Codes // Tech. Rep. № 248. Dept. of Informatics, Univ. of Bergen. Bergen, Norway, 2003. Available at http://www.ii.uib.no/~georg/sci/inf/coding/hyperpdf/cs03rep.pdf.
32. *Blakley G.R.* Safeguarding Cryptographic Keys // Proc. 1979 National Computer Conf.: Int. Workshop on Managing Requirements Knowledge (MARK). New York. June 4–7, 1979. AFIPS Conf. Proceedings, V. 48. Montvale, NJ: AFIPS Press, 1979. P. 313–317. https://doi.org/10.1109/MARK.1979.8817296
33. *Shamir A.* How to Share a Secret // Comm. ACM. 1979. V. 22. № 11. P. 612–613. https://doi.org/10.1145/359168.359176

34. *Егорова Е.Е.* Обобщение IPP-кодов и IPP-систем множеств // Пробл. передачи информ. 2019. Т. 55. № 3. С. 46–59. https://doi.org/10.1134/S0555292319030045
35. *Zhao H.V., Wu M., Wang Z.J., Liu K.J.R.* Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting // IEEE Trans. Image Process. 2005. V. 14. № 5. P. 646–661. https://doi.org/10.1109/TIP.2005.846035
36. *Fan J., Gu Y., Hachimori M., Miao Y.* Signature Codes for Weighted Binary Adder Channel and Multimedia Fingerprinting // IEEE Trans. Inform. Theory. 2021. V. 67. № 1. P. 200–216. https://doi.org/10.1109/TIT.2020.3033445
37. *Djackov A.G.* On a Search Model of False Coins // Topics in Information Theory (Proc. 2nd Colloq. on Information Theory. Keszthely, Hungary. Aug. 25–30, 1975). Colloq. Math. Soc. János Bolyai. V. 16. Amsterdam: Horth Holland, 1977. P. 163–170.
38. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
39. *Bshouty N.H., Mazzawi H.* On Parity Check $(0,1)$-Matrix over $\mathbb{Z}_p$ // Proc. 22nd Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'11). San Francisco, CA. Jan. 23–25, 2011. P. 1383–1394. https://dl.acm.org/doi/10.5555/2133036.2133142
40. *Kautz W., Singleton R.* Nonrandom Binary Superimposed Codes // IEEE Trans. Inform. Theory. 1964. V. 10. № 4. P. 363–377. https://doi.org/10.1109/TIT.1964.1053689
41. *Friedman A.D., Graham R.L., Ullman J.D.* Universal Single Transition Time Asynchronous State Assignments // IEEE Trans. Comput. 1969. V. 18. № 6. P. 541–547. https://doi.org/10.1109/T-C.1969.222707
42. *Blackburn S.R.* Probabilistic Existence Results for Separable Codes // IEEE Trans. Inform. Theory. 2015. V. 61. № 11. P. 5822–5827. https://doi.org/10.1109/TIT.2015.2473848
43. *Manin Yu.I.* What Is the Maximum Number of Points on a Curve over $\mathbf{F}_2$? // J. Fac. Sci. Univ. Tokyo Sect. IA Math. 1981. V. 28. № 3. P. 715–720.
44. *Randriambololona H.* $(2,1)$-Separating Systems beyond the Probabilistic Bound // Israel J. Math. 2013. V. 195. № 1. P. 171–186. https://doi.org/10.1007/s11856-012-0126-9
45. *Cohen G., Litsyn S., Zémor G.* Binary B_2-Sequences: A New Upper Bound // J. Combin. Theory Ser. A. 2001. V. 94. № 1. P. 152–155. https://doi.org/10.1006/jcta.2000.3127
46. *Erdős P., Frankl P., Füredi Z.* Families of Finite Sets in Which No Set Is Covered by the Union of Two Others // J. Combin. Theory Ser. A. 1982. V. 33. № 2. P. 158–166. https://doi.org/10.1016/0097-3165(82)90004-8
47. *Erdős P., Frankl P., Füredi Z.* Families of Finite Sets in Which No Set Is Covered by the Union of r Others // Israel J. Math. 1985. V. 51. № 1–2. P. 79–89. https://doi.org/10.1007/BF02772959
48. *Воробьев И.В.* Границы скоростей разделяющих кодов // Пробл. передачи информ. 2017. Т. 53. № 1. С. 34–46. http://mi.mathnet.ru/ppi2225
49. *Бассалыго Л.А., Гельфанд С.И., Пинскер М.С.* Простые методы получения нижних границ в теории кодов // Пробл. передачи информ. 1991. Т. 27. № 4. С. 3–8. http://mi.mathnet.ru/ppi576
50. *Дьячков А.Г., Рыков В.В.* Границы длины дизъюнктивных кодов // Пробл. передачи информ. 1982. Т. 18. № 3. С. 7–13. http://mi.mathnet.ru/ppi1232
51. *Guruswami V., Sudan M.* Improved Decoding of Reed–Solomon and Algebraic-Geometry Codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 6. P. 1757–1767. https://doi.org/10.1109/18.782097
52. *Guruswami V.* List Decoding of Error-Correcting Codes (Winning Thesis of the 2002 ACM Doct. Diss. Competition) // Lect. Notes Comp. Sci. V. 3282. Berlin: Springer, 2005.
53. *Форни Д.* Каскадные коды. М.: Мир, 1970.
54. *Alon N.* Explicit Construction of Exponential Sized Families of k-Independent Sets // Discrete Math. 1986. V. 58. № 2. P. 191–193. https://doi.org/10.1016/0012-365X(86)90161-5
55. *Indyk P., Ngo H.Q., Rudra A.* Efficiently Decodable Non-adaptive Group Testing // Proc. 21st Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'10). Austin, TX. Jan. 17–19, 2010. P. 1126–1142. https://dl.acm.org/doi/10.5555/1873601.1873692

56. *Сагалович Ю.Л.* Верхняя граница мощности кода состояний автомата // Пробл. передачи информ. 1973. Т. 9. № 1. С. 73–83. http://mi.mathnet.ru/ppi884
57. *Сагалович Ю.Л.* Новые верхние границы мощности разделяющих систем // Пробл. передачи информ. 1993. Т. 29. № 2. С. 109–111. http://mi.mathnet.ru/ppi182
58. *Körner J., Simonyi G.* Separating Partition Systems and Locally Different Sequences // SIAM J. Discrete Math. 1988. V. 1. № 3. P. 355–359. https://doi.org/10.1137/0401035
59. *Kabatiansky G., Vlăduţ S., Tavernier C.* On the Doubly Sparse Compressed Sensing Problem // Cryptography and Coding (Proc. 15th IMA Int. Conf. IMACC'2015. Oxford, UK. Dec. 15–17, 2015). Lect. Notes Comp. Sci. V. 9496. Berlin: Springer, 2015. P. 184–189. https://doi.org/10.1007/978-3-319-27239-9_11
60. *Gritsenko V., Kabatiansky G., Lebedev V., Maevskiy A.* Signature Codes for Noisy Multiple Access Adder Channel // Des. Codes Cryptogr. 2017. V. 82. № 1–2. P. 293–299. https://doi.org/10.1007/s10623-016-0228-1
61. *Ericson T., Györfi L.* Superimposed Codes in $\mathbb{R}^n$ // IEEE Trans. Inform. Theory. 1988. V. 34. № 4. P. 877–880.
62. *Füredi Z., Ruszinkó M.* An Improved Upper Bound of the Rate of Euclidean Superimposed Codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 2. P. 799–802. https://doi.org/10.1109/18.749032
63. *Ericson T., Levenshtein V.I.* Superimposed Codes in the Hamming Space // IEEE Trans. Inform. Theory. 1994. V. 40. № 6. P. 1882–1893. https://doi.org/10.1109/18.340463
64. *Влэдуц С.Г., Кабатянский Г.А., Ломаков В.В.* Об исправлении ошибок при искажениях в канале и синдроме // Пробл. передачи информ. 2015. Т. 51. № 2. С. 50–56. http://mi.mathnet.ru/ppi2169
65. *Komlós J., Greenberg A.G.* An Asymptotically Fast Nonadaptive Algorithm for Conflict Resolution in Multiple-Access Channels // IEEE Trans. Inform. Theory. 1985. V. 31. № 2. P. 302–306. https://doi.org/10.1109/TIT.1985.1057020
66. *Clementi A.E.F., Monti A., Silvestri R.* Selective Families, Superimposed Codes, and Broadcasting on Unknown Radio Networks // Proc. 12th Annu. ACM–SIAM Symp. on Discrete Algorithms (SODA'01). Washington, DC, USA. Jan. 7–9, 2001. P. 709–718. https://dl.acm.org/doi/proceedings/10.5555/365411
67. *Chlebus B.S., Kowalski D.R.* Almost Optimal Explicit Selectors // Fundamentals of Computation Theory (Proc. 15th Int. Symp. FCT'2005. Lübeck, Germany. Aug. 17–20, 2005). Lect. Notes Comp. Sci. V. 3623. Berlin: Springer, 2005. P. 270–280. https://doi.org/10.1007/11537311_24
68. *Cicalese F., Vaccaro U.* Superselectors: Efficient Constructions and Applications // Algorithms (Proc. 18th Annu. European Symp. ESA'2010. Liverpool, UK. Sept. 6–8, 2010. Part I). Lect. Notes Comp. Sci. V. 6346. Berlin: Springer, 2010. P. 207–218. https://doi.org/10.1007/978-3-642-15775-2_18
69. *Alon N., Fachini E., Körner J.* Locally Thin Set Families // Combin. Probab. Comput. 2000. V. 9. № 6. P. 481–488. https://doi.org/10.1017/S0963548300004521
70. *Дьячков А.Г., Воробьев И.В., Полянский Н.А., Щукин В.Ю.* Границы скорости дизъюнктивных кодов // Пробл. передачи информ. 2014. Т. 50. № 1. С. 31–63. http://mi.mathnet.ru/ppi2131
71. *Дьячков А.Г., Воробьев И.В., Полянский Н.А., Щукин В.Ю.* Письмо в редакцию // Пробл. передачи информ. 2016. Т. 52. № 2. С. 111. http://mi.mathnet.ru/ppi2208

Егорова Елена Евгеньевна
Кабатянский Григорий Анатольевич
Сколковский институт науки и технологий (Сколтех)
egorovahelene@gmail.com
g.kabatyansky@skoltech.ru

Поступила в редакцию
03.04.2021
После доработки
15.04.2021
Принята к публикации
15.04.2021

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 «ИКЦ«АКАДЕМКНИГА»

Москва
ООО «Объединённая редакция»