РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

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

Том 57, 2021 **Вып. 4**

Октябрь–Ноябрь–Декабрь

М о с к в а

С О Д Е Р Ж А Н И Е

Теория информации

Теория кодирования

Методы обработки сигналов

Большие системы

CONTENTS

Information Theory

Coding Theory

Methods of Signal Processing

Large Systems

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391 : 519.724

© 2021 г. **А.Г. Дьячков, Д.Ю. Гошкодер**

НОВЫЕ НИЖНИЕ ГРАНИЦЫ ДЛЯ ДОЛИ ИСПРАВЛЯЕМЫХ ОШИБОК ПРИ СПИСОЧНОМ ДЕКОДИРОВАНИИ В КОМБИНАТОРНЫХ ДВОИЧНЫХ КАНАЛАХ СВЯЗИ

Целью данной статьи являются восстановление и развитие результатов неопубликованной рукописи А.Г. Дьячкова. Рассматривается дискретный канал без памяти (ДКБП) и доказывается теорема об экспоненциальной границе выбрасывания при декодировании списком фиксированной длины L. Данный результат является обобщением классической экспоненциальной границы вероятности ошибки оптимальных кодов в ДКБП на модель списочного декодирования в ДКБП. В качестве приложений данного результата рассмотрены двоичный симметричный канал (ДСК) без памяти и двоичный асимметричный канал (Z-канал) без памяти. Для обоих рассматриваемых каналов выведена нижняя граница доли числа исправляемых ошибок при передаче с нулевой скоростью по соответствующим каналам, на выходе которых используется декодирование списком фиксированной длины L. Для Z-канала эта граница получена при произвольном распределении входного алфавита $(1-w, w)$, а также найдено оптимальное значение полученной границы и доказано, что доля числа ошибок, исправляемых оптимальным кодом, стремится к единице при стремлении длины списка L к бесконечности.

Ключевые слова: дискретный канал без памяти, двоичный симметричный канал, Z-канал, доля исправляемых ошибок, граница выбрасывания, декодирование списком.

DOI: 10.31857/S055529232104001X

§ 1. Введение и обзор результатов

Статья состоит из трех частей. В первой части (§ 2) мы приводим формулировку и вывод теоремы об экспоненциальной границе выбрасывания при декодировании списком фиксированной длины L в общем случае ДКБП с произвольными конечными входным и выходным алфавитами (теорема 1), а также исследуем логарифмическую асимптотику границы выбрасывания (теорема 2). Отметим, что во всех известных нам публикациях других авторов (например, [1–5]), в которых изучались коды со списочным декодированием, постановка задачи списочного декодирования рассматривалась лишь для частных случаев двоичных каналов без памяти.

Во второй части статьи (§ 3) мы применяем построенную в первой части границу выбрасывания к частному случаю ДСК, чтобы для соответствующего *комбинаторного двоичного симметричного канала связи* (BS-канала) получить обозначаемую через $f_{\mathrm{bs}}(L)$ нижнюю границу для максимально возможной доли симметричных ошибок, исправляемых при передаче с нулевой скоростью по BS-каналу, на выходе которого используется декодирование списком длины L. Данная нижняя граница $f_{\mathrm{bs}}(L)$ со ссылкой на неопубликованную рукопись [6] как на первоисточник была ранее приведена в работе [5].

В третьей части статьи (§ 4) мы применяем построенную в первой части границу выбрасывания при декодировании списком фиксированной длины L к важному частному случаю ДКБП, называемому вероятностным Z-каналом, а затем к соответствующему *комбинаторному двоичному асимметричному каналу связи* (Z-каналу), в котором ошибки могут происходить при передаче лишь одного из двух возможных двоичных входных символов.

Основным результатом, установленным в третьей части статьи, является обозначаемая нами через $f_{\mathrm{z}}(w, L)$ нижняя граница для максимально возможной доли асимметричных ошибок, исправляемых при передаче с нулевой скоростью по комбинаторному Z-каналу, на выходе которого используется декодирование списком длины L, а на входном алфавите задано распределение вероятностей $\underline{Q}^* = (1 - w, w)$.

При любом натуральном $L \geqslant 1$ и $w \in [0, 1]$ нижняя граница $f_{\mathrm{z}}(w, L)$ вычисляется по формуле

$$f_{\mathrm{z}}(w, L) = w(1 - w^L).$$

Кроме того, нам удалось оптимизировать найденную величину, т.е. найти $f_{\mathrm{z}}(L) = \max\limits_{w \in [0,1]} f_{\mathrm{z}}(w, L)$ и соответствующую ей $w_{\max}(L)$, а также доказать, что

$$\lim_{L \to +\infty} \Big(\max_{w \in [0,1]} f_{\mathrm{z}}(w, L) \Big) = 1.$$

Приведем таблицу значений величин $w_{\max}(L)$ и $f_{\mathrm{z}}(L)$ при различных значениях $L \geqslant 1$:

L	1	2	3	4	5	10	15	20	25	50
$w_{\max}(L)$	0,5	0,58	0,63	0,67	0,70	0,79	0,83	0,86	0,88	0,92
$f_{\mathrm{z}}(L)$	0,25	0,38	0,47	0,53	0,58	0,72	0,78	0,82	0,84	0,91

Отметим, что в классическом случае $L = 1$ значение нижней границы $f_{\mathrm{z}}(1) = 1/4$ совпадает со значением верхней границы, которая является следствием известной нижней границы вероятности ошибки, называемой границей сферической упаковки [7]. Также полученная граница совпадает с результатами работ [8, 9], в которых были выведены аналогичные оценки и доказана их оптимальность.

§ 2. Обозначения, определения, постановка задачи, формулировка и вывод теоремы о границе выбрасывания при декодировании списком фиксированной длины в общем случае ДКБП, свойства экспоненты границы выбрасывания

Пусть на нашем канале входные и выходные слова – это последовательности длины N из элементов конечных алфавитов:

$\underline{x} = (x_1, x_2, \ldots, x_N)$ – входное слово, $x_i \in [K]$;
$\underline{y} = (y_1, y_2, \ldots, y_N)$ – выходное слово, $y_i \in [J]$.

Пусть также для этого канала заданы условные вероятности принятия символа $j \in [J]$ при условии отправки символа $k \in [K]$ в канал. Обозначим эти вероятности через $W(k \,|\, j)$.

Вероятность получения слова $\underline{y}$ при передаче слова $\underline{x}$ задается следующим образом:

$$W_N(\underline{y} \,|\, \underline{x}) = \prod_{i=1}^{N} W(y_i \,|\, x_i).$$

Такой канал и называется дискретным каналом без памяти. Обозначим через X_K^N множество всевозможных слов $\underline{x}$ длины N над алфавитом $[K]$, а через Y_J^N – множество всевозможных слов $\underline{y}$ длины N над алфавитом $[J]$, и пусть $\underline{x}^{(1)}, \ldots, \underline{x}^{(M)}$ – фиксированные слова. Напомним, как в таком случае определяется декодирование по максимуму правдоподобия (МП).

Определение 1 (МП-декодирование). При заданном $\underline{y}$ положим $D_{\text{МП}}(\underline{y}) = m$, где $m \in [M]$ – наименьшее среди всех чисел $m' \in [M]$, для которых достигается

$$\max_{m' \in [M]} W_N(\underline{y} \,|\, \underline{x}^{(m')}) = W_N(\underline{y} \,|\, \underline{x}^{(m)}).$$

Таким образом, при МП-декодировании возвращается статистически наиболее вероятное для получения слово $\underline{x}^{(m)}$.

При этом зачастую однозначно восстановить входное слово довольно сложно, поэтому применяется декодирование списком.

Определение 2. Декодирование списком длины L – один из методов декодирования кодов, при котором вместо одного кодового слова декодер возвращает список из L возможных вариантов.

Определение 3. Декодирование списком фиксированного объема считается успешным, если переданный кодовый вектор принадлежит набору L кодовых слов, возвращаемых декодером, в противном случае считается, что произошла ошибка декодирования списком. Условная вероятность ошибки при передаче слова $\underline{x}^{(m)}$ и использовании декодирования списком длины L по методу максимума правдоподобия обозначим через $\mathcal{P}(m, L)$. Определим набор всевозможных L-подмножеств кода, которые не содержат слова $\underline{x}^{(m)}$:

$$X_{m,L} \stackrel{\text{def}}{=} \left\{ \left(\underline{x}^{(m_1)}, \ldots, \underline{x}^{(m_L)}\right) : \, m_i \in [M'] \setminus \{m\}, \, m_i \neq m_j, \, \forall i, j \in [L], \, i \neq j \right\}.$$

Тогда условная вероятность ошибки в общем случае может быть записана в виде следующей суммы:

$$\mathcal{P}(m, L) = \sum_{\vec{x} \in X_{m,L}} \mathcal{P}_L(m, \vec{x}),$$

где $\mathcal{P}_L(m, \vec{x})$ – вероятность ошибки при передаче слова $\underline{x}^{(m)}$, декодировании списком длины L и возвращении декодером слов из набора $\vec{x}$. Также определим естественным образом максимальную вероятность ошибки:

$$\mathcal{P}_{\max}(L) \stackrel{\text{def}}{=} \max_{m \in [M]} \mathcal{P}(m, L).$$

В данной статье мы будем использовать декодирование списком длины L по методу максимума правдоподобия (т.е. декодер будет возвращать L статистически наиболее вероятных для получения слов).

Определение 4. Скорость кода с M кодовыми словами длины N определяется следующим образом:

$$R \stackrel{\text{def}}{=} \frac{\ln \frac{M}{L}}{N} = \frac{\ln M}{N} - \frac{\ln L}{N}. \tag{1}$$

Для обычного декодирования, где $L = 1$, это стандартное определение скорости кода ($M = \exp(RN)$).

Целью § 2 является формулировка и доказательство теоремы о границе выбрасывания при декодировании списком фиксированной длины в общем случае ДКБП с произвольными конечными входным и выходным алфавитами. Для этого зафиксируем распределение вероятностей $\underline{Q} = (Q(1), Q(2), \ldots, Q(K))$ на входном алфавите канала, такое что $\sum\limits_{i=1}^{K} Q(i) = 1$, и введем следующее множество:

$$\mathcal{K} \stackrel{\text{def}}{=} \big\{\underline{k} = (k_1, k_2, \ldots, k_{L+1}) : \; k_i \in [K],\, i \in [L+1]\big\}, \quad |\mathcal{K}| = K^{L+1}.$$

Теорема 1. *Пусть заданы дискретный канал без памяти с $M' = 2M - 1$ словами длины N и вероятности перехода $W(j \,|\, k)$, $1 \leqslant k \leqslant K$, $1 \leqslant j \leqslant J$. Тогда для любого распределения вероятностей на входном алфавите канала $\underline{Q}$ имеет место следующая экспоненциальная верхняя граница максимальной вероятности ошибки при декодировании списком длины L:*

$$\mathcal{P}_{\max}(L) \leqslant \exp\left\{-NE_{\text{ex}}^{(L)}\left(R + \frac{(L+1)\ln 2}{LN} + \frac{\ln L}{N}, \underline{Q}\right)\right\}, \tag{2}$$

где для любого $R > 0$ функция $E_{\text{ex}}^{(L)}(R, \underline{Q})$, называемая экспонентой границы выбрасывания, определяется следующим образом:

$$E_{\text{ex}}^{(L)}(R, \underline{Q}) \stackrel{\text{def}}{=} \sup_{\rho \geqslant 1}\left\{-\rho RL + E_x^{(L)}(\rho, \underline{Q})\right\}, \tag{3}$$

$$E_x^{(L)}(\rho, \underline{Q}) \stackrel{\text{def}}{=} -\rho \ln\left\{\sum_{\underline{k} \in \mathcal{K}} \prod_{i=1}^{L+1} Q(k_i)\left[\sum_{j=1}^{J} \prod_{\ell=1}^{L+1} W(j \,|\, k_\ell)^{\frac{1}{L+1}}\right]^{\frac{1}{\rho}}\right\}. \tag{4}$$

Доказательство теоремы разбивается на несколько более простых утверждений, из которых в итоге и следует наша граница.

1. Рассмотрим код с $M = L+1$ словами $\underline{x}^{(1)}, \underline{x}^{(2)}, \ldots, \underline{x}^{(M)}$ и схемой декодирования списком длины L. Определим набор Y_L следующим образом:

$$Y_L = \left\{\underline{y} \in Y_J^N : \min_{i \in [L+1],\, i \neq 1} W_N(\underline{y} \,|\, \underline{x}^{(i)}) \geqslant W_N(\underline{y} \,|\, \underline{x}^{(1)})\right\}.$$

Тогда условная вероятность ошибки $\mathcal{P}_L$ при декодировании списком по методу максимума правдоподобия, учитывая, что исходным словом является $\underline{x}^{(1)}$, может быть записана как

$$\mathcal{P}_L = \sum_{\underline{y} \in Y_L} W_N(\underline{y} \,|\, \underline{x}^{(1)}).$$

Лемма 1. *Для любого действительного числа $\sigma \geqslant 0$*

$$\mathcal{P}_L \leqslant \sum_{\underline{y} \in Y_J^N} W_N(\underline{y} \,|\, \underline{x}^{(1)})^{1-L\sigma} \prod_{i=2}^{L+1} W_N(\underline{y} \,|\, \underline{x}^{(i)})^{\sigma}. \tag{5}$$

Доказательство. Заметим, что по определению множества Y_L получаем, что $\forall \underline{y} \in Y_L$ и $i \in [L+1]$, $i \neq 1$, верно неравенство $W_N(\underline{y} \,|\, \underline{x}^{(i)}) \geqslant W_N(\underline{y} \,|\, \underline{x}^{(1)})$. Тогда для любого числа $\sigma > 0$ получаем, что

$$\left(\frac{W_N(\underline{y} \,|\, \underline{x}^{(i)})}{W_N(\underline{y} \,|\, \underline{x}^{(1)})}\right)^{\sigma} \geqslant 1$$

и соответственно

$$\prod_{i=2}^{L+1}\left(\frac{W_N(\underline{y}\,|\,\underline{x}^{(i)})}{W_N(\underline{y}\,|\,\underline{x}^{(1)})}\right)^{\sigma}\geqslant 1.$$

Тогда справедлива следующая цепочка преобразований:

$$\mathcal{P}_L=\sum_{\underline{y}\in Y_L}W_N(\underline{y}\,|\,\underline{x}^{(1)})\leqslant\sum_{\underline{y}\in Y_L}W_N(\underline{y}\,|\,\underline{x}^{(1)})\prod_{i=2}^{L+1}\left(\frac{W_N(\underline{y}\,|\,\underline{x}^{(i)})}{W_N(\underline{y}\,|\,\underline{x}^{(1)})}\right)^{\sigma}\leqslant$$

$$\leqslant\sum_{\underline{y}\in Y_J^N}W_N(\underline{y}\,|\,\underline{x}^{(1)})\prod_{i=2}^{L+1}\left(\frac{W_N(\underline{y}\,|\,\underline{x}^{(i)})}{W_N(\underline{y}\,|\,\underline{x}^{(1)})}\right)^{\sigma}=$$

$$=\sum_{\underline{y}\in Y_J^N}W_N(\underline{y}\,|\,\underline{x}^{(1)})^{1-L\sigma}\prod_{i=2}^{L+1}W_N(\underline{y}\,|\,\underline{x}^{(i)})^{\sigma}.$$

Последнее равенство завершает доказательство леммы. ▲

Отметим, что эта граница формулируется только в терминах заданных переходных вероятностей. Более того, суммирование в правой части идет по всем возможным выходным словам $\underline{y}$ длины N в отличие от определения условной вероятности ошибки при декодировании списком по методу максимального правдоподобия, где суммирование идет только по $\underline{y}$ из Y_L.

2. Рассмотрим ансамбль кодов с независимыми и одинаково распределенными словами, число которых равно $M'=2M-1$, и имеющих распределение $\underline{Q}_N(\underline{x})$, $\underline{x}\in X_K^N$. Для $m\in[M']$ и $L\in[M'-1]$ согласно определению 3 обозначим через $\mathcal{P}(m,L)$ случайную величину в ансамбле, равную вероятности ошибки при передаче слова $\underline{x}^{(m)}$ и использовании декодирования списком по методу максимума правдоподобия. Отметим, что случайные величины $\mathcal{P}(m,L)$ при $m\in[M']$ имеют одинаковое распределение.

Пусть $s>0$ – действительное число. Среднюю по ансамблю кодов с M' словами вероятность ошибки $\mathcal{P}(m,L)$ в степени s будем обозначать через $\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]$. Эта величина равна математическому ожиданию $\mathcal{P}^s(m,L)$ по ансамблю, т.е.

$$\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]=$$

$$=\sum_{\underline{z}^{(1)},\ldots,\underline{z}^{(M')}\in X_K^N}\prod_{r=1}^{M'}\underline{Q}_N(\underline{z}^{(r)})\mathbf{M}\big[\mathcal{P}^s(m,L)\mid\underline{x}^{(1)}=\underline{z}^{(1)},\ \ldots,\ \underline{x}^{(M')}=\underline{z}^{(M')}\big].$$

Отметим, что величина $\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]$ равна некоторому действительному значению при фиксированных L и $\underline{Q}$ и не зависит от m.

Лемма 2. *Для рассматриваемого ансамбля кодов существует хотя бы один подкод с M словами $\widetilde{\underline{x}}^{(1)},\widetilde{\underline{x}}^{(2)},\ldots,\widetilde{\underline{x}}^{(M)}$, а также метод декодирования списком длины L этого кода, такой что для любого $m\in[M]$ и любого $s>0$ условная вероятность ошибочного декодирования $\widetilde{\mathcal{P}}(m,L)$ при передаче слова $\widetilde{\underline{x}}^{(m)}$ удовлетворяет неравенству*

$$\widetilde{\mathcal{P}}(m,L)<\big(2\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]\big)^{\frac{1}{s}},\tag{6}$$

где среднее значение $\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]$ не зависит от выбора значения $m\in[M']$.

Доказательство. Напомним известное следствие из неравенства Маркова для неотрицательной случайной величины с конечным математическим ожиданием:

$$\Pr(\eta \geqslant 2\mathbf{M}\eta) \leqslant \frac{1}{2}.$$

В качестве случайной величины $\eta = \mathcal{P}^s(m, L)$ возьмем случайную величину в ансамбле, равную s-й степени вероятности ошибки при передаче слова $\underline{x}^{(m)}$ и использовании декодирования списком по методу максимума правдоподобия. Тогда можно использовать следствие неравенства Маркова для случайной величины η:

$$\Pr\Big(\mathcal{P}^s(m, L) \geqslant 2\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m, L)]\Big) \leqslant \frac{1}{2},$$

или

$$\Pr\Big(\mathcal{P}(m, L) < 2^{\frac{1}{s}}\big(\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m, L)]\big)^{\frac{1}{s}}\Big) \geqslant \frac{1}{2}.$$

Последнее неравенство означает, что по крайней мере для половины слов ($\frac{M'}{2}$) кода выполняется неравенство, вероятность которого мы оценили.

Другими словами, последнее неравенство означает, что существуют подкод с M кодовыми словами $\widetilde{\underline{x}}^{(1)}, \widetilde{\underline{x}}^{(2)}, \ldots, \widetilde{\underline{x}}^{(M)}$ и схема декодирования списком по методу максимума правдоподобия, где размер списка ограничен величиной L, такие что для любого переданного слова $\widetilde{\underline{x}}^{(m)}$, где $m \in [M]$, условная вероятность ошибки декодирования $\widetilde{\mathcal{P}}(m, L)$ удовлетворяет следующему неравенству для любого $s > 0$:

$$\widetilde{\mathcal{P}}(m, L) < \big(2\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m, L)]\big)^{\frac{1}{s}}. \quad \blacktriangle$$

3. Нашей следующей целью будет получение верхней границы средней вероятности ошибки. Мы рассматриваем ансамбль кодов с $M' = 2M - 1$ независимыми и одинаково распределенными словами. Пусть они имеют распределение $\underline{Q}_N(\underline{x})$. Также мы определили (см. определение 3) набор всевозможных L-подмножеств кода, не содержащих слова $\underline{x}^{(m)}$:

$$X_{m,L} = \Big\{\big(\underline{x}^{(m_1)}, \ldots, \underline{x}^{(m_L)}\big) : m_i \in [M'] \setminus \{m\},\ m_i \neq m_j,\ \forall i, j \in [L],\ i \neq j\Big\}.$$

Заметим, что количество таких L-подмножеств кода равно $\binom{M'-1}{L}$, так как мы выбираем L слов из всех (всего их M'), кроме $\underline{x}^{(m)}$.

Лемма 3. *Для ансамбля кодов с независимыми и одинаково распределенными словами, число которых равно $M' = 2M - 1$, с распределением $\underline{Q}_N(\underline{x})$ и для любого $0 < s \leqslant 1$ имеет место следующая оценка*:

$$\mathcal{P}^s(m, L) \leqslant \sum_{\vec{x} \in X_{m,L}} \left[\sum_{\underline{y} \in Y_J^N} W_N(\underline{y} \,|\, \underline{x}^{(m)})^{1-L\sigma} \left(\prod_{i=1}^{L} W_N(\underline{y} \,|\, \underline{x}^{(m_i)})\right)^{\sigma}\right]^s, \tag{7}$$

Более того, усредняя эту границу по ансамблю, мы получаем верхнюю границу средней вероятности ошибки:

$$\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m, L)] \leqslant$$
$$\leqslant [2(M-1)]^L \sum_{\underline{z}^{(1)}, \ldots, \underline{z}^{(L+1)} \in X_K^N} \prod_{i=1}^{L+1} \underline{Q}_N(\underline{z}^{(i)}) \left[\sum_{\underline{y} \in Y_J^N} \prod_{i=1}^{L+1} W_N(\underline{y} \,|\, \underline{z}^{(i)})^{\frac{1}{1+L}}\right]^s, \tag{8}$$

где суммирование в правой части идет по всем $(L+1)$-подмножествам слов из множества с M' словами.

Доказательство. а) Выберем L слов из ансамбля с $M'-1=2M-2$ словами (т.е. выберем элемент $\vec{x}\in X_{m,L}$) и добавим к ним слово $\underline{x}^{(m)}$. Так мы получим подкод из $L+1$ слова, и будем рассматривать ошибку при передаче одного из этих слов (слова $\underline{x}^{(m)}$). Таким образом, мы попадем в условие леммы 1, и получим верхнюю границу вероятности ошибки декодирования списком по методу максимума правдоподобия при передаче слова $\underline{x}^{(m)}$ из $L+1$ данных (обозначаемую в определении 3 через $\mathcal{P}_L(m,\vec{x})$). Далее, согласно определению 3 вероятность ошибки при передаче слова $\underline{x}^{(m)}$ из M' данных может быть записана в виде следующей суммы:

$$\mathcal{P}(m,L)=\sum_{\vec{x}\in X_{m,L}}\mathcal{P}_L(m,\vec{x}).$$

Применим известное неравенство: для любого $0<s\leqslant 1$

$$\left(\sum_{i\in\mathcal{I}}a_i\right)^s\leqslant\sum_{i\in\mathcal{I}}a_i^s,$$

где мы берем множество $X_{m,L}$ в качестве множества суммирования $\mathcal{I}$, а вероятность ошибки $\mathcal{P}_L(m,\vec{x})$ в качестве слагаемых a_i. Тогда получаем, что

$$\mathcal{P}^s(m,L)\leqslant\sum_{\vec{x}\in X_{m,L}}\mathcal{P}_L^s(m,\vec{x})\leqslant$$
$$\leqslant\sum_{\vec{x}\in X_{m,L}}\left[\sum_{\underline{y}\in Y_J^N}W_N(\underline{y}\,|\,\underline{x}^{(m)})^{1-L\sigma}\left(\prod_{i=1}^{L}W_N(\underline{y}\,|\,\underline{x}^{(m_i)})\right)^{\sigma}\right]^s.$$

Представленная цепочка неравенств завершает доказательство первого утверждения леммы 3.

б) Теперь усредним верхнюю границу условной вероятности ошибки при передаче слова $\underline{x}^{(m)}$ по ансамблю. Мы определяем среднюю вероятность ошибки как математическое ожидание $\mathcal{P}(m,L)$. По определению математического ожидания для дискретной случайной величины и первому утверждению леммы (при $\sigma=\dfrac{1}{1+L}$ и $1-L\sigma=\sigma$)

$$\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]\leqslant$$
$$\leqslant\binom{M'-1}{L}\sum_{\underline{z}^{(1)},\ldots,\underline{z}^{(L+1)}\in X_K^N}\prod_{i=1}^{L+1}\underline{Q}_N(\underline{z}^{(i)})\left[\sum_{\underline{y}\in Y_J^N}\prod_{\ell=1}^{L+1}W_N(\underline{y}\,|\,\underline{z}^{(\ell)})^{\frac{1}{1+L}}\right]^s.$$

Первый множитель равен мощности множества $X_{m,L}$ (количеству вариантов выбрать L слов из набора $M'-1$ слова), а дальнейшая сумма включает вероятность выбора множества из $L+1$ слов (элемента $\vec{x}\in X_{m,L}$ и вектора $\underline{x}^{(m)}$) с распределением $\underline{Q}_N(\underline{x})$ и соответствующие границы вероятности ошибки. Затем, воспользовавшись известным свойством биномиальных коэффициентов ($\binom{n}{m}\leqslant n^m$), можно получить, что

$$\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m,L)]\leqslant$$
$$\leqslant[2(M-1)]^L\sum_{\underline{z}^{(1)},\ldots,\underline{z}^{(L+1)}\in X_K^N}\prod_{i=1}^{L+1}\underline{Q}_N(\underline{z}^{(i)})\left[\sum_{\underline{y}\in Y_J^N}\prod_{\ell=1}^{L+1}W_N(\underline{y}\,|\,\underline{z}^{(\ell)})^{\frac{1}{1+L}}\right]^s,$$

что завершает доказательство леммы 3. ▲

4. Далее покажем, что из лемм 2 и 3 вытекает справедливость теоремы 1. Рассмотрим канал без памяти, т.е. канал, для которого

$$\underline{Q}_N(\underline{x}) = \prod_{i=1}^{N} Q(x_i),$$

где $\underline{x} = (x_1, \ldots, x_N)$ – исходное слово, а $\underline{Q} = (Q(1), Q(2), \ldots, Q(K))$ – заданное распределение вероятностей на входном алфавите канала. Определим теперь максимальную вероятность ошибки следующим естественным образом. Из определения 3 имеем

$$\mathcal{P}_{\max}(L) = \max_{m\in[M]} \widetilde{\mathcal{P}}(m, L).$$

Из оценки в лемме 2 следует, что верно следующее неравенство:

$$\mathcal{P}_{\max}(L) \leqslant \left(2\mathbf{M}_{\underline{Q}}[\mathcal{P}^s(m, L)]\right)^{\frac{1}{s}}.$$

Мы рассматриваем канал без памяти и можем использовать верхнюю границу средней вероятности ошибки из леммы 3 для этого канала, полагая $\rho = \dfrac{1}{s}$ при $\rho \geqslant 1$:

$$\mathcal{P}_{\max}(L) \leqslant \left(2^{L+1}(M-1)^L\right)^{\rho} \times$$
$$\times \left(\sum_{\underline{z}^{(1)},\ldots,\underline{z}^{(L+1)} \in X_K^N} \prod_{i=1}^{L+1} \underline{Q}_N(\underline{z}^{(i)}) \left[\sum_{\underline{y}\in Y_J^N} \prod_{\ell=1}^{L+1} W_N(\underline{y}\,|\,\underline{z}^{(\ell)})^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} \right)^{\rho}.$$

Напомним обозначение $\mathcal{K} = \{\underline{k} = (k_1, k_2 \ldots, k_{L+1}) : k_i \in [K], i \in [L+1]\}$. Рассмотрим следующую цепочку преобразований:

$$\sum_{\underline{z}^{(1)},\ldots,\underline{z}^{(L+1)} \in X_K^N} \prod_{i=1}^{L+1} \underline{Q}_N(\underline{z}^{(i)}) \left[\sum_{\underline{y}\in Y_J^N} \prod_{\ell=1}^{L+1} W_N(\underline{y}\,|\,\underline{z}^{(\ell)})^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} =$$
$$= \sum_{z_1^{(1)},\ldots,z_N^{(1)}\in[K]} \cdots \sum_{z_1^{(L+1)},\ldots,z_N^{(L+1)}\in[K]} \prod_{i=1}^{L+1}\prod_{v=1}^{N} Q(z_v^{(i)}) \times$$
$$\times \left[\sum_{y_1,\ldots,y_N\in[J]} \prod_{\ell=1}^{L+1}\prod_{s=1}^{N} W(y_s\,|\,z_s^{(\ell)})^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} =$$
$$= \sum_{\underline{k}^{(1)}\in\mathcal{K}} \prod_{i_1=1}^{L+1} Q(k_{i_1}^{(1)}) \left[\sum_{j_1=1}^{J} \prod_{\ell_1=1}^{L+1} W(j_1\,|\,k_{\ell_1}^{(N)})^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} \times \ldots \times$$
$$\times \sum_{\underline{k}^{(N)}\in\mathcal{K}} \prod_{i_N=1}^{L+1} Q(k_{i_N}^{(N)}) \left[\sum_{j_N=1}^{J} \prod_{\ell_N=1}^{L+1} W(j_N\,|\,k_{\ell_N}^{(N)})^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} =$$
$$= \left\{ \sum_{\underline{k}\in\mathcal{K}} \prod_{i=1}^{L+1} Q(k_i) \left[\sum_{j=1}^{J} \prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} \right\}^N.$$

Следовательно,

$$\mathcal{P}_{\max}(L) \leqslant \left(2^{L+1}(M-1)^L\right)^{\rho} \left\{ \sum_{\underline{k}\in\mathcal{K}} \prod_{i=1}^{L+1} Q(k_i) \left[\sum_{j=1}^{J} \prod_{\ell=1}^{L+1} W(j \,|\, k_\ell)^{\frac{1}{1+L}} \right]^{\frac{1}{\rho}} \right\}^{\rho N}. \qquad (9)$$

Остается понять, почему границы (2) и (9) эквивалентны. Для этого рассмотрим и преобразуем следующее выражение:

$$\exp\left\{-N\left(-\rho L\left(R+\frac{(L+1)\ln 2}{LN}+\frac{\ln L}{N}\right)\right)\right\} = \exp\{\rho LRN + \rho(L+1)\ln 2 +$$
$$+ \rho L \ln L\} = (\exp\{RN\})^{\rho L}(\exp\{\ln 2\})^{\rho(L+1)}(\exp\{\ln L\})^{\rho L} =$$
$$= \left(\frac{M}{L}\right)^{\rho L} 2^{\rho(L+1)} L^{\rho L} = M^{\rho L} 2^{\rho(L+1)} \geqslant (M-1)^{\rho L} 2^{\rho(L+1)} =$$
$$= (2^{L+1}(M-1)^L)^{\rho},$$

где мы используем тот факт, что $\exp\{RN\} = \dfrac{M}{L}$ для декодирования списком длины L. Таким образом, первый член в $E_{\text{ex}}^{(L)}(R, \underline{Q})$ в экспоненциальной границе (2) соответствует первым двум множителям в границе (9).

Из определения $E_x^{(L)}(\rho, \underline{Q})$ также следует, что выражение $\exp\{-NE_x^{(L)}(\rho, \underline{Q})\}$ в экспоненциальной границе (2) соответствует коэффициенту в фигурных скобках в границе (9). Из описанных рассуждений следует справедливость теоремы, и мы получаем верхнюю границу максимальной вероятности ошибки при использовании декодирования списком по методу максимума правдоподобия. Теорема 1 полностью доказана. ▲

Замечание. В частном случае $L{=}1$ имеет место следующее неравенство (см. [7, с. 170]):

$$E_{\text{ex}}^{(1)}(R, \underline{Q}) \geqslant E_{\text{ran}}^{(1)}(R, \underline{Q}),$$

где

$$E_{\text{ran}}^{(1)}(R, \underline{Q}) \stackrel{\text{def}}{=} \max_{0\leqslant\rho\leqslant 1} \{-\rho R + E_0(\rho, \underline{Q})\}$$

– показатель экспоненты средней по $\underline{Q}$-ансамблю вероятности ошибки при классическом МП-декодировании, когда длина списка $L = 1$, а

$$E_0(\rho, \underline{Q}) \stackrel{\text{def}}{=} -\ln\left\{\sum_{j=1}^{J}\left(\sum_{k=1}^{K} Q(k)W(j \,|\, k)^{\frac{1}{\rho+1}}\right)^{\rho+1}\right\}$$

– функция Галлагера для ДКБП параметра $\rho \geqslant 0$.

Открытой задачей остается доказательство (или опровержение) обобщения этого неравенства на случай произвольного $L \geqslant 2$, т.е. надо доказать или найти противоречащий пример ДКБП для выполнения неравенства

$$E_{\text{ex}}^{(L)}(R, \underline{Q}) \geqslant E_{\text{ran}}^{(L)}(R, \underline{Q}),$$

где функция скорости передачи имеет вид

$$E_{\text{ran}}^{(L)}(R, \underline{Q}) \stackrel{\text{def}}{=} \max_{0\leqslant\rho\leqslant L} \{-\rho R + E_0(\rho, \underline{Q})\}.$$

В частном случае нулевой скорости передачи ($R = 0$) неравенство $E_{\text{ex}}^{(L)}(0, \underline{Q}) \geqslant$ $\geqslant E_{\text{ran}}^{(L)}(0, \underline{Q})$ будет доказано в п. 2 теоремы 2. Решение представленной задачи в общем виде принципиально важно, поскольку в работе [9] было показано, что правая часть предыдущего равенства для любого фиксированного распределения вероятностей Q на входе ДКБП задает точную экспоненту средней по ансамблю вероятности ошибки при декодировании списком длины L.

Опишем свойства полученной в теореме 1 экспоненты границы выбрасывания.

Теорема 2. *Имеют место следующие свойства экспоненты границы выбрасывания*:

1. $E_x^{(L)}(\rho, \underline{Q})$ *является неубывающей функцией параметра* ρ;
2. $E_x^{(L)}(1, \underline{Q}) = E_0(L, \underline{Q})$. *Более того, при нулевой скорости передачи имеет место неравенство*

$$E_{\text{ran}}^{(L)}(0, \underline{Q}) = \max_{0 \leqslant \rho \leqslant L} \{E_0(\rho, \underline{Q})\} \leqslant \sup_{\rho \geqslant 1} \{E_x^{(L)}(\rho, \underline{Q})\} = E_{\text{ex}}^{(L)}(0, \underline{Q});$$

3. $E_{\text{ex}}^{(L)}(R, \underline{Q})$ *принимает бесконечные значения в следующем диапазоне скоростей*:

$$0 < R < \lim_{\rho \to +\infty} \frac{E_x^{(L)}(\rho, \underline{Q})}{\rho L};$$

4. $R_{x,\infty}^{(L)}(\underline{Q}) \stackrel{\text{def}}{=} \lim\limits_{\rho \to +\infty} \frac{E_x^{(L)}(\rho, \underline{Q})}{\rho} = -\ln\left[\sum\limits_{\underline{k} \in \mathcal{K}} \prod\limits_{i=1}^{L+1} Q(k_i)\varphi(\underline{k})\right]$, *где*

$$\varphi(\underline{k}) = \varphi(k_1, \ldots, k_{L+1}) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{если } \sum\limits_{j=1}^{J} \prod\limits_{i=1}^{L+1} W(j \,|\, k_i) \neq 0, \\ 0 & \text{в остальных случаях}; \end{cases}$$

5. $E_{\text{ex}}^{(L)}(0, \underline{Q}) = \lim\limits_{R \to 0} E_{\text{ex}}^{(L)}(R, \underline{Q}) = \lim\limits_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q})$;
6. *Пусть* $\varphi(\underline{k}) = 1$ *для любого* $\underline{k} \in \mathcal{K}$. *Тогда*

$$E_{\text{ex}}^{(L)}(0, \underline{Q}) = -\sum_{\underline{k} \in \mathcal{K}} \prod_{i=1}^{L+1} Q(k_i) \ln\left[\sum_{j=1}^{J} \prod_{\ell=1}^{L+1} W(j \,|\, k_\ell)^{\frac{1}{L+1}}\right].$$

Доказательство. Пункт 1 можно доказать с использованием неравенства

$$\sum_k \left(A_k B_k^{\frac{1}{s}}\right)^s \geqslant \sum_k \left(A_k B_k^{\frac{1}{r}}\right)^r,$$

справедливого при $0 < s \leqslant r$ и $|A_k| \leqslant 1$. Подставим $\prod\limits_{i=1}^{L+1} Q(k_i)$ из определения $E_x^{(L)}(\rho, \underline{Q})$ вместо величин A_k из неравенства, величины $\sum\limits_{j=1}^{J} \prod\limits_{i=1}^{L+1} W(j \,|\, k_i)^{\frac{1}{L+1}}$ подставим вместо величин B_k из неравенства, и затем применим к обеим частям неравенства функцию $-\ln x$. Такое преобразование известного неравенства и даст утверждение о монотонности функции $E_x^{(L)}(\rho, \underline{Q})$. Пункт 1 теоремы доказан.

2. Вычислим значение $E_x^{(L)}(\rho, \underline{Q})$ при $\rho = 1$:

$$E_x^{(L)}(1, \underline{Q}) = -\ln\left\{\sum_{\underline{k}\in\mathcal{K}}\sum_{j=1}^{J}\prod_{i=1}^{L+1}\left(Q(k_i)W(j\,|\,k_i)^{\frac{1}{L+1}}\right)\right\} =$$

$$= -\ln\left\{\sum_{j=1}^{J}\left(\sum_{k=1}^{K}Q(k)W(j\,|\,k)^{\frac{1}{L+1}}\right)^{L+1}\right\} = E_0(L, \underline{Q}).$$

В сделанных преобразованиях величины $E_x^{(L)}(1, \underline{Q})$ стоит обосновать второе равенство. Его проще понять, двигаясь по равенству справа налево: при возведении суммы в степень $L+1$ мы умножаем сумму по k на саму себя $L+1$ раз. При этом умножении из каждой суммы мы выбираем по одному слагаемому, и каждый такой выбор соответствует некоторому элементу $\underline{k} \in \mathcal{K}$, т.е. при возведении суммы в степень мы получаем сумму по всевозможным $\underline{k} \in \mathcal{K}$ произведений $L+1$ элемента, как в левой части рассматриваемого равенства.

Для доказательства неравенства из п. 2 теоремы воспользуемся свойствами монотонности по параметру ρ функции Галлагера $E_0(\rho, \underline{Q})$ и функции $E_x^{(L)}(\rho, \underline{Q})$ (из п. 1). Тогда получаем, что

$$\max_{0\leqslant\rho\leqslant L}\{E_0(\rho, \underline{Q})\} = E_0(L, \underline{Q}) = E_x^{(L)}(1, \underline{Q}) \leqslant \sup_{\rho\geqslant 1}\{E_x^{(L)}(\rho, \underline{Q})\}.$$

Второй пункт теоремы полностью доказан.

3. Для доказательства п. 3 теоремы рассмотрим выражение $-\rho RL + E_x^{(L)}(\rho, \underline{Q}) = F(R)$ как линейную функцию от R с наклоном $-\rho$ при $\rho \geqslant 1$. Координата пересечения такой функции с осью абсцисс равна

$$\frac{E_x^{(L)}(\rho, \underline{Q})}{\rho L}.$$

Следовательно, при $\rho \to +\infty$ наша функция имеет вертикальную асимптоту (коэффициент наклона линейной функции стремится к $-\infty$, а сама наклонная прямая стремится к вертикальной прямой, проходящей через абсциссу пересечения функции $F(R)$ с осью абсцисс):

$$R = \lim_{\rho\to+\infty}\frac{E_x^{(L)}(\rho, \underline{Q})}{\rho L}.$$

А тогда по определению $E_{\text{ex}}^{L}(R, \underline{Q}) = \sup_{\rho\geqslant 1}\{-\rho RL + E_x^{(L)}(\rho, \underline{Q})\}$ принимает бесконечные значения при

$$0 < R < \lim_{\rho\to+\infty}\frac{E_x^{(L)}(\rho, \underline{Q})}{\rho L}.$$

Пункт 3 доказан.

4. Для нахождения предела из п. 4 теоремы введем следующие обозначения:

$$A_{\underline{k}} = \prod_{i=1}^{L+1} Q(k_i), \quad B_{\underline{k}} = \sum_{j=1}^{J}\prod_{i=1}^{L+1} W(j\,|\,k_i)^{\frac{1}{L+1}}.$$

Тогда

$$E_x^{(L)}(\rho, \underline{Q}) = -\rho \ln \left(\sum_{\underline{k} \in \mathcal{K}} A_{\underline{k}} B_{\underline{k}}^{\frac{1}{\rho}} \right).$$

Перепишем искомый предел в новых обозначениях и сократим числитель и знаменатель на ρ:

$$R_{x,\infty}^{(L)}(\underline{Q}) = \lim_{\rho \to +\infty} \frac{E_x^{(L)}(\rho, \underline{Q})}{\rho} = \lim_{\rho \to +\infty} \frac{-\rho \ln \left(\sum\limits_{\underline{k} \in \mathcal{K}} A_{\underline{k}} B_{\underline{k}}^{\frac{1}{\rho}} \right)}{\rho} =$$

$$= \lim_{\rho \to +\infty} \frac{-\ln \left(\sum\limits_{\underline{k} \in \mathcal{K}} A_{\underline{k}} B_{\underline{k}}^{\frac{1}{\rho}} \right)}{1} = \lim_{\rho \to +\infty} \left(-\ln \left(\sum_{\underline{k} \in \mathcal{K}} A_{\underline{k}} B_{\underline{k}}^{\frac{1}{\rho}} \right) \right).$$

Далее заметим, что

$$\lim_{\rho \to +\infty} B_{\underline{k}}^{\frac{1}{\rho}} = \varphi(\underline{k}) = \begin{cases} 1, & \text{если } B_{\underline{k}} \neq 0, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Из этого замечания и следует, что

$$R_{x,\infty}^{(L)}(\underline{Q}) = -\ln \left[\sum_{\underline{k} \in \mathcal{K}} \prod_{i=1}^{L+1} Q(k_i) \varphi(\underline{k}) \right],$$

где

$$\varphi(\underline{k}) = \varphi(k_1, \ldots, k_{L+1}) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{если } \sum\limits_{j=1}^{J} \prod\limits_{i=1}^{L+1} W(j \,|\, k_i) \neq 0, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Пункт 4 доказан.

5. По определению

$$E_{\text{ex}}^{(L)}(R, \underline{Q}) \stackrel{\text{def}}{=} \sup_{\rho \geqslant 1} \left\{ -\rho R L + E_x^{(L)}(\rho, \underline{Q}) \right\} \leqslant \sup_{\rho \geqslant 1} \left\{ E_x^{(L)}(\rho, \underline{Q}) \right\} = \lim_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q}),$$

где последнее равенство вытекает из того, что функция $E_x^{(L)}(\rho, \underline{Q})$ является неубывающей. Таким образом, получаем, что

$$E_{\text{ex}}^{(L)}(R, \underline{Q}) \leqslant \lim_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q})$$

при всех R. Если $\lim\limits_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q})$ конечен, то для любого малого $\varepsilon > 0$ найдется такое ρ, что

$$E_x^{(L)}(\rho, \underline{Q}) \geqslant \lim_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q}) - \varepsilon.$$

Тогда для достаточно малых R также будет выполнено неравенство

$$E_x^{(L)}(\rho, \underline{Q}) - \rho R L \geqslant \lim_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q}) - \varepsilon.$$

Следовательно, при достаточно малых R имеет место двойное неравенство

$$\lim_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q}) \geqslant E_{\text{ex}}^{(L)}(R, \underline{Q}) \geqslant \lim_{\rho \to +\infty} E_x^{(L)}(\rho, \underline{Q}) - \varepsilon.$$

Отсюда и следует необходимое нам равенство пределов

$$\lim_{R\to 0} E_{\text{ex}}^{(L)}(R,\underline{Q}) = \lim_{\rho\to+\infty} E_x^{(L)}(\rho,\underline{Q}).$$

Пункт 5 доказан.

6. В предыдущем пункте теоремы мы доказали, что

$$E_{\text{ex}}^{(L)}(0,\underline{Q}) = \lim_{R\to 0} E_{\text{ex}}^{(L)}(R,\underline{Q}) = \lim_{\rho\to+\infty} E_x^{(L)}(\rho,\underline{Q}).$$

Для доказательства данного пункта, т.е. поиска предела

$$\lim_{\rho\to+\infty} E_x^{(L)}(\rho,\underline{Q}) = \lim_{\rho\to+\infty} -\rho\ln\left\{\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1} Q(k_i)\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]^{\frac{1}{\rho}}\right\},$$

сделаем замену $\rho = \dfrac{1}{\sigma}$ и рассмотрим предел

$$\lim_{\sigma\to 0} \frac{-\ln\left\{\sum\limits_{\underline{k}\in\mathcal{K}}\prod\limits_{i=1}^{L+1} Q(k_i)\left[\sum\limits_{j=1}^{J}\prod\limits_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]^{\sigma}\right\}}{\sigma},$$

который и будет в точности равен $E_{\text{ex}}^{(L)}(0,\underline{Q})$.

Для нахождения этого предела воспользуемся правилом Лопиталя. Для этого найдем (и обозначим через γ) следующую производную:

$$\gamma \stackrel{\text{def}}{=} \left(-\ln\left\{\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1} Q(k_i)\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]^{\sigma}\right\}\right)'_{\sigma} =$$

$$= -\frac{1}{\sum\limits_{\underline{k}\in\mathcal{K}}\prod\limits_{i=1}^{L+1} Q(k_i)\left[\sum\limits_{j=1}^{J}\prod\limits_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]^{\sigma}} \times$$

$$\times\left(\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1} Q(k_i)\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]^{\sigma}\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]\right).$$

Теперь найдем предел этой величины при $\sigma\to 0$:

$$\lim_{\sigma\to 0}\gamma = -\frac{1}{\sum\limits_{\underline{k}\in\mathcal{K}}\prod\limits_{i=1}^{L+1} Q(k_i)\varphi(\underline{k})}\left(\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1} Q(k_i)\varphi(\underline{k})\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]\right).$$

В силу условия $\varphi(\underline{k}) = 1$ для всех $\underline{k}\in\mathcal{K}$ получаем, что

$$\lim_{\sigma\to 0}\gamma = -\frac{1}{\sum\limits_{\underline{k}\in\mathcal{K}}\prod\limits_{i=1}^{L+1} Q(k_i)}\left(\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1} Q(k_i)\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]\right).$$

Далее отметим тот факт, что $\sum\limits_{\underline{k}\in\mathcal{K}}\prod\limits_{i=1}^{L+1} Q(k_i) = 1$, так как это сумма по всевозможным элементам $\mathcal{K}$ вероятностей получить эти элементы, а вероятность наступления

событий, образующих полную группу, равна единице. Тогда получаем

$$\lim_{\sigma\to 0}\gamma = -\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1}Q(k_i)\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1}W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right].$$

Теперь можно перейти уже к нахождению величины $E_{\mathrm{ex}}^{(L)}(0,\underline{Q})$. Напомним, что предел мы считаем по правилу Лопиталя:

$$E_{\mathrm{ex}}^{(L)}(0,\underline{Q}) = \lim_{\sigma\to 0}\frac{-\ln\left\{\sum\limits_{\underline{k}\in\mathcal{K}}\prod\limits_{i=1}^{L+1}Q(k_i)\left[\sum\limits_{j=1}^{J}\prod\limits_{\ell=1}^{L+1}W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right]^{\sigma}\right\}}{\sigma} =$$

$$= \lim_{\sigma\to 0}\frac{\gamma}{1} = \lim_{\sigma\to 0}\gamma = -\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1}Q(k_i)\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1}W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right].$$

Пункт 6 и теорема 2 полностью доказаны. ▲

§ 3. Нижняя граница для максимально возможной доли симметричных ошибок, исправляемых при передаче с нулевой скоростью и декодировании списком длины L в частном случае комбинаторного двоичного симметричного канала связи (BS-канала)

Целью этого параграфа является применение экспоненты границы выбрасывания из теоремы 2 в частном случае ДСК для построения нижней границы для максимально возможной доли симметричных ошибок, исправляемых при передаче с нулевой скоростью и декодировании списком фиксированной длины в частном случае комбинаторного BS-канала связи. Отметим тот факт, что в работе [4] именно в частном случае ДСК построена нижняя граница вероятности ошибки, экспонента которой совпадает с экспонентой границы выбрасывания.

Напомним, что для ДСК с вероятностью ошибки p переходные вероятности имеют вид $W(1\,|\,1) = W(2\,|\,2) = 1-p$, $W(1\,|\,2) = W(2\,|\,1) = p$. Зафиксируем для данного ДСК распределение вероятностей на входном алфавите $\underline{Q}^* = (1/2, 1/2)$, а также введем следующие обозначения:

$$\widetilde{E}_{\mathrm{ex}}(p,L) \stackrel{\mathrm{def}}{=} E_{\mathrm{ex}}^{(L)}(0,\underline{Q}^*),$$

$$f_{\mathrm{bs}}(L) \stackrel{\mathrm{def}}{=} \varliminf_{p\to 0}\frac{\widetilde{E}_{\mathrm{ex}}(p,L)}{-\ln p}.$$

Теорема 3. *Пусть $-N\widetilde{E}_{\mathrm{ex}}(p,L)$ – показатель экспоненты в верхней границе вероятности ошибки при передаче слов длины N с нулевой скоростью по ДСК с вероятностью ошибки p, а $e_{\mathrm{bs}}^{(L)}(R,N)$ – максимально возможное количество ошибок, исправляемых при передаче слов длины N по BS-каналу связи со скоростью R с использованием на выходе BS-канала декодирования списком длины L.*

Тогда при $R=0$ справедливо следующее неравенство:

$$f_{\mathrm{bs}}(L) = \varliminf_{p\to 0}\frac{\widetilde{E}_{\mathrm{ex}}(p,L)}{-\ln p} \leqslant \overline{\lim_{N\to+\infty}}\frac{e_{\mathrm{bs}}^{(L)}(0,N)}{N},$$

где $e_{\mathrm{bs}}^{(L)}(R,N)$ определяется в точке $R=0$ по непрерывности.

Доказательство. Обозначим через $\mathcal{P}^{(L)}(p,R,N)$ минимальную вероятность ошибки при передаче слов длины N по ДСК со скоростью R с использованием

на выходе ДСК декодирования списком длины L для дискретного симметричного канала с нулевой скоростью передачи. Тогда по условию имеем

$$p^{e_{\rm bs}^{(L)}(0,N)+1}(1-p)^{N-e_{\rm bs}^{(L)}(0,N)-1} \leqslant \mathcal{P}^{(L)}(p,0,N) \leqslant \exp^{-N\widetilde{E}_{\rm ex}(p,L)}.$$

Логарифмируя это неравенство, получим

$$\big(e_{\rm bs}^{(L)}(0,N)+1\big)\ln p + \big(N-e_{\rm bs}^{(L)}(0,N)-1\big)\ln(1-p) \leqslant -N\widetilde{E}_{\rm ex}(p,L).$$

Поделим обе части на $N\ln p$, но изменим знак неравенства, так как $\ln p<0$:

$$\frac{\widetilde{E}_{\rm ex}(p,L)}{-\ln p} \leqslant \frac{e_{\rm bs}^{(L)}(0,N)+1}{N} + \frac{N-e_{\rm bs}^{(L)}(0,N)-1}{N}\frac{\ln(1-p)}{\ln p}.$$

Теперь дважды сделаем предельный переход при $p\to 0$ и при $N\to+\infty$, учитывая что $\lim\limits_{p\to 0}\dfrac{\ln(1-p)}{\ln p}=0$. Получаем требуемое неравенство теоремы, а именно

$$\varliminf_{p\to 0}\frac{\widetilde{E}_{\rm ex}(p,L)}{-\ln p} \leqslant \varlimsup_{N\to+\infty}\frac{e_{\rm bs}^{(L)}(0,N)}{N}. \quad \blacktriangle$$

Т е о р е м а 4. *Для любого $k=1,2,\ldots$*

$$f_{\rm bs}(2k-1)=f_{\rm bs}(2k)=\frac{1}{2}\left(1-\frac{(2k-1)!!}{(2k)!!}\right).$$

Д о к а з а т е л ь с т в о. Воспользуемся формулой для $E_{\rm ex}^{(L)}(0,\underline{Q}^*)$ из п. 6 теоремы 2 и найдем $\widetilde{E}_{\rm ex}(p,L)$:

$$\widetilde{E}_{\rm ex}(p,L) \stackrel{\rm def}{=} E_{\rm ex}^{(L)}(0,\underline{Q}^*) = -\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1}Q(k_i)\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1}W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right] =$$

$$= -\sum_{\ell=1}^{L}\binom{L+1}{\ell}2^{-(L+1)}\ln\left[\big(p^\ell(1-p)^{L+1-\ell}\big)^{\frac{1}{L+1}} + \big((1-p)^\ell p^{L+1-\ell}\big)^{\frac{1}{L+1}}\right] =$$

$$= -\sum_{\ell=1}^{L}\binom{L+1}{\ell}2^{-(L+1)}\ln\left[(1-p)\left(\frac{p}{1-p}\right)^{\frac{\ell}{L+1}} + p\left(\frac{1-p}{p}\right)^{\frac{\ell}{L+1}}\right],$$

где суммирование в полученном выражении идет по параметру ℓ, который равен количеству k_i, равных 1. Если $\ell=0$ или $\ell=L+1$, то значение величины под знаком логарифма равно 1. Таким образом, остается суммирование по параметру $\ell\in[L]$. Под знаком суммы множитель $\binom{L+1}{\ell}$ соответствует числу вариантов выбрать элемент $\underline{k}\in\mathcal{K}$, в котором ровно ℓ элементов равны 1, и множитель $2^{-(L+1)}$ равен $\prod\limits_{i=1}^{L+1}Q^*(k_i)$.

Л е м м а 4. *Справедливо равенство*

$$\lim_{p\to 0}\frac{\ln\left[(1-p)\Big(\frac{p}{1-p}\Big)^{\frac{\ell}{L+1}} + p\Big(\frac{1-p}{p}\Big)^{\frac{\ell}{L+1}}\right]}{\ln p} = \min\left(\frac{\ell}{L+1}, 1-\frac{\ell}{L+1}\right).$$

Доказательство. Для нахождения этого предела воспользуемся правилом Лопиталя:

$$\lim_{p\to 0}\frac{\ln\left[(1-p)\Big(\frac{p}{1-p}\Big)^{\frac{\ell}{L+1}}+p\Big(\frac{1-p}{p}\Big)^{\frac{\ell}{L+1}}\right]}{\ln p}=$$

$$=\lim_{p\to 0}\frac{p}{p^{\frac{\ell}{L+1}}(1-p)^{1-\frac{\ell}{L+1}}+(1-p)^{\frac{\ell}{L+1}}p^{1-\frac{\ell}{L+1}}}\left(\frac{\ell}{L+1}p^{\frac{\ell}{L+1}-1}(1-p)^{1-\frac{\ell}{L+1}}-\right.$$

$$-\left(1-\frac{\ell}{L+1}\right)(1-p)^{-\frac{\ell}{L+1}}p^{\frac{\ell}{L+1}}+\left(1-\frac{\ell}{L+1}\right)p^{-\frac{\ell}{L+1}}(1-p)^{\frac{\ell}{L+1}}-$$

$$\left.-\frac{\ell}{L+1}(1-p)^{\frac{\ell}{L+1}-1}p^{1-\frac{\ell}{L+1}}\right)=\lim_{p\to 0}\frac{p}{p^{\frac{\ell}{L+1}}+p^{1-\frac{\ell}{L+1}}}\left(\frac{\ell}{L+1}p^{\frac{\ell}{L+1}-1}-\right.$$

$$\left.-\left(1-\frac{\ell}{L+1}\right)p^{\frac{\ell}{L+1}}+\left(1-\frac{\ell}{L+1}\right)p^{-\frac{\ell}{L+1}}-\frac{\ell}{L+1}p^{1-\frac{\ell}{L+1}}\right)=$$

$$=\lim_{p\to 0}\frac{p}{p^{\frac{\ell}{L+1}}+p^{1-\frac{\ell}{L+1}}}\left(\frac{\ell}{L+1}p^{\frac{\ell}{L+1}-1}+\left(1-\frac{\ell}{L+1}\right)p^{-\frac{\ell}{L+1}}\right)=$$

$$=\lim_{p\to 0}p^{1-\min\left(\frac{\ell}{L+1},1-\frac{\ell}{L+1}\right)}\left(\frac{\ell}{L+1}p^{\frac{\ell}{L+1}-1}+\left(1-\frac{\ell}{L+1}\right)p^{-\frac{\ell}{L+1}}\right)=$$

$$=\min\left(\frac{\ell}{L+1},1-\frac{\ell}{L+1}\right).$$

Лемма 4 доказана. ▲

Найдем значение величины $f_{\rm bs}(2k-1)$, используя симметрию биноминальных коэффициентов и результат леммы 4:

$$f_{\rm bs}(2k-1)=2\sum_{\ell=1}^{k-1}\left(\binom{2k}{\ell}2^{-2k}\frac{\ell}{2k}\right)+\binom{2k}{k}2^{-(2k+1)},$$

где последнее слагаемое соответствует $\ell=k$. Аналогично при $L=2k$ получаем

$$f_{\rm bs}(2k)=2\sum_{\ell=1}^{k}\binom{2k+1}{\ell}2^{-(2k+1)}\frac{\ell}{2k+1}=\frac{1}{2^{2k}}\sum_{\ell=1}^{k}\binom{2k}{\ell-1},$$

где последнее равенство следует из того, что $\dfrac{\ell}{2k+1}\binom{2k+1}{\ell}=\binom{2k}{\ell-1}$.

Затем отметим следующие свойства биномиальных коэффициентов:

1. $2^{2k-1}=\displaystyle\sum_{\ell=0}^{2k-1}\binom{2k-1}{\ell}=2\sum_{\ell=0}^{k-1}\binom{2k-1}{\ell}\ \Rightarrow\ \sum_{\ell=0}^{k-1}\binom{2k-1}{\ell}\left(\frac{1}{2}\right)^{2k-1}=\frac{1}{2}$;
2. $\displaystyle\sum_{\ell=0}^{k-1}\binom{2k}{\ell}=\frac{2^{2k}-\binom{2k}{k}}{2}$;
3. $\displaystyle\binom{2k}{k}=2\binom{2k-1}{k-1}\ \Rightarrow\ 4\binom{2k-1}{k-1}-\binom{2k}{k}=2\binom{2k}{k}-\binom{2k}{k}=\binom{2k}{k}$.

Преобразуем выражение для $f_{\mathrm{bs}}(2k-1)$, используя свойства 1 и 3 биномиальных коэффициентов:

$$f_{\mathrm{bs}}(2k-1) = \sum_{\ell=0}^{k-2} \binom{2k-1}{\ell} \left(\frac{1}{2}\right)^{2k-1} + \binom{2k}{k} \left(\frac{1}{2}\right)^{2k+1} =$$

$$= \frac{1}{2} - \frac{\binom{2k-1}{k-1}}{2^{2k-1}} + \frac{\binom{2k}{k}}{2^{2k+1}} = \frac{1}{2} - \frac{4\binom{2k-1}{k-1} - \binom{2k}{k}}{2^{2k+1}} = \frac{1}{2}\left(1 - \frac{\binom{2k}{k}}{2^{2k}}\right).$$

Теперь применим свойство (2) и получим следующее равенство:

$$f_{\mathrm{bs}}(2k) = \frac{1}{2^{2k}} \sum_{\ell=1}^{k} \binom{2k}{\ell-1} = \frac{1}{2}\left(1 - \frac{\binom{2k}{k}}{2^{2k}}\right) = f_{\mathrm{bs}}(2k-1).$$

Поэтому для любого числа $k = 1, 2, 3, \ldots$ справедливо следующее равенство:

$$f_{\mathrm{bs}}(2k-1) = f_{\mathrm{bs}}(2k) = \frac{1}{2}\left(1 - \frac{\binom{2k}{k}}{2^{2k}}\right) = \frac{1}{2}\left(1 - \frac{(2k)!}{k!\,k!\,2^{2k}}\right) =$$

$$= \frac{1}{2}\left(1 - \frac{(2k)!}{(2k)!!\,(2k)!!}\right) = \frac{1}{2}\left(1 - \frac{(2k-1)!!}{(2k)!!}\right).$$

Теорема 4 полностью доказана. ▲

Таким образом, теорема 3 утверждает, что $f_{\mathrm{bs}}(L)$ является нижней границей для доли симметричных ошибок, исправляемых оптимальным двоичным кодом при декодировании списком фиксированной длины, в частном случае комбинаторного двоичного симметричного канала связи и нулевой скорости передачи, а теорема 4 позволяет точно посчитать эту границу для любого наперед заданного L. Приведем таблицу значений полученной границы:

L	1	2	3	4	5	6	7	8	9	10
$f_{\mathrm{bs}}(L)$	1/4	1/4	5/16	5/16	11/32	11/32	93/256	93/256	193/512	193/512

Также можно отметить, что

$$\lim_{k\to+\infty} f_{\mathrm{bs}}(2k-1) = \lim_{k\to+\infty} f_{\mathrm{bs}}(2k) = \lim_{k\to+\infty} \frac{1}{2}\left(1 - \frac{(2k-1)!!}{(2k)!!}\right) =$$

$$= \frac{1}{2}\left(1 - \prod_{k=1}^{+\infty} \frac{2k-1}{2k}\right) = \frac{1}{2}.$$

§ 4. Нижняя граница для максимальной доли асимметричных ошибок, исправляемых при передаче с нулевой скоростью и декодировании списком длины L в частном случае двоичного асимметричного Z-канала

Целью этого параграфа является применение построенной в § 2 границы выбрасывания при декодировании списком фиксированной длины L к важному частному случаю ДКБП, называемому вероятностным Z-каналом, а затем к соответствующему *комбинаторному двоичному асимметричному каналу связи* (Z-каналу), в которых ошибки могут происходить при передаче лишь одного из двух возможных двоичных входных символов.

Напомним, что для Z-канала с вероятностью ошибки p переходные вероятности имеют вид $W(1\,|\,1) = 1$, $W(1\,|\,2) = p$, $W(2\,|\,1) = 0$, $W(2\,|\,2) = 1 - p$. Рассмотрим для Z-канала более общий случай по сравнению с ДСК, а именно зафиксируем для данного канала распределение вероятностей на входном алфавите $\underline{Q}^* = (1 - w, w)$. Введем дополнительно следующие обозначения:

$$\widetilde{E}_{\text{ex}}(p, w, L) \stackrel{\text{def}}{=} E_{\text{ex}}^{(L)}(0, \underline{Q}^*),$$
$$f_{\text{z}}(w, L) \stackrel{\text{def}}{=} \varliminf_{p \to 0} \frac{\widetilde{E}_{\text{ex}}(p, w, L)}{-\ln p}.$$

Теорема 5. *Пусть $-N\widetilde{E}_{\text{ex}}(p, w, L)$ – показатель экспоненты в верхней границе вероятности ошибки при передаче слов длины N по двоичному асимметричному Z-каналу с вероятностью ошибки p, а $e_z^{(L)}(R, N)$ – максимально возможное количество ошибок, исправляемых при передаче слов длины N по Z-каналу связи со скоростью R с использованием на выходе Z-канала декодирования списком длины L. Тогда при $R = 0$ справедливо следующее неравенство*:

$$f_{\text{z}}(w, L) = \varliminf_{p \to 0} \frac{\widetilde{E}_{\text{ex}}(p, w, L)}{-\ln p} \leqslant \varlimsup_{N \to +\infty} \frac{e_z^{(L)}(0, N)}{N},$$

где $e_z^{(L)}(R, N)$ определяется в точке $R = 0$ по непрерывности.

Доказательство. Обозначим через $\mathcal{P}^{(L)}(p, R, N)$ минимальную вероятность ошибки при передаче слов длины N по Z-каналу со скоростью R с использованием на выходе Z-канала декодирования списком длины L. Для двоичного асимметричного Z-канала с нулевой скоростью передачи по условию имеем

$$p^{e_z^{(L)}(0,N)+1} 1^k (1-p)^{N-k-e_z^{(L)}(0,N)-1} \leqslant \mathcal{P}^{(L)}(p, 0, N) \leqslant \exp^{-N\widetilde{E}_{\text{ex}}(p,w,L)},$$

где k – число единиц, перешедших по каналу в единицы.

Логарифмируя это неравенство, получаем

$$(e_z^{(L)}(0, N) + 1)\ln p + k \ln 1 + (N - k - e_z^{(L)}(0, N) - 1)\ln(1 - p) \leqslant -N\widetilde{E}_{\text{ex}}(p, w, L).$$

Поделим обе части на $N \ln p$, но изменим знак неравенства, так как $\ln p < 0$:

$$\frac{\widetilde{E}_{\text{ex}}(p, w, L)}{-\ln p} \leqslant \frac{e_z^{(L)}(0, N)}{N} + \frac{N - k - e_z^{(L)}(0, N) - 1}{N} \frac{\ln(1-p)}{\ln p}.$$

Теперь дважды сделаем предельный переход при $p \to 0$ и при $N \to +\infty$, учитывая что $\varlimsup\limits_{p \to 0} \dfrac{\ln(1-p)}{\ln p} = 0$. Получаем требуемое неравенство теоремы, а именно

$$\varliminf_{p \to 0} \frac{\widetilde{E}_{\text{ex}}(p, w, L)}{-\ln p} \leqslant \varlimsup_{N \to +\infty} \frac{e_z^{(L)}(0, N)}{N}. \quad \blacktriangle$$

Теорема 6. *Для любого натурального L и любого $w \in [0, 1]$ справедливо*

$$f_{\text{z}}(w, L) = w\left(1 - w^L\right).$$

Более того,

$$f_{\mathrm{z}}(L) = \max_{w\in[0,1]} f_{\mathrm{z}}(w,L) = \left(\frac{1}{L+1}\right)^{\frac{1}{L}}\left(1-\frac{1}{L+1}\right),$$

$$\lim_{L\to+\infty}\left(\max_{w\in[0,1]} f_{\mathrm{z}}(w,L)\right) = 1.$$

Доказательство. 1. Воспользовавшись формулой для $E_{\mathrm{ex}}^{(L)}(0,\underline{Q}^*)$ из п. 6 теоремы 2, вычислим для такого канала следующую величину:

$$\widetilde{E}_{\mathrm{ex}}(p,w,L) \stackrel{\mathrm{def}}{=} E_{\mathrm{ex}}^{(L)}(0,\underline{Q}^*) = -\sum_{\underline{k}\in\mathcal{K}}\prod_{i=1}^{L+1} Q(k_i)\ln\left[\sum_{j=1}^{J}\prod_{\ell=1}^{L+1} W(j\,|\,k_\ell)^{\frac{1}{L+1}}\right] =$$

$$= -\sum_{\ell=0}^{L+1}\binom{L+1}{\ell}(1-w)^{\ell}w^{L+1-\ell}\ln\left[\left(1^{\ell}p^{L+1-\ell}\right)^{\frac{1}{L+1}} + \left(0^{\ell}(1-p)^{L+1-\ell}\right)^{\frac{1}{L+1}}\right],$$

где суммирование идет по параметру ℓ, который равен числу k_i, равных 1, а под знаком суммы множитель $\binom{L+1}{\ell}$ соответствует числу вариантов выбрать элемент $\underline{k}\in\mathcal{K}$, в котором ровно ℓ единиц, а множитель $(1-w)^l w^{L+1-\ell}$ равен $\prod\limits_{i=1}^{L+1} Q^*(k_i)$. Если $\ell = 0$ или $\ell = L+1$, то величина под знаком логарифма равна 1. Поэтому суммирование остается лишь по $\ell\in[L]$:

$$\widetilde{E}_{\mathrm{ex}}(p,w,L) = -\sum_{\ell=1}^{L}\binom{L+1}{\ell}(1-w)^{l}w^{L+1-\ell}\ln\left[p^{\frac{L+1-\ell}{L+1}}\right].$$

Лемма 5. *Справедливо равенство*

$$\lim_{p\to 0}\frac{\ln p^{\frac{L+1-\ell}{L+1}}}{\ln p} = 1-\frac{\ell}{L+1}.$$

Доказательство. Для нахождения этого предела воспользуемся правилом Лопиталя:

$$\lim_{p\to 0}\frac{\ln p^{\frac{L+1-\ell}{L+1}}}{\ln p} = \lim_{p\to 0}\frac{p}{p^{\frac{L+1-\ell}{L+1}}}\frac{L+1-\ell}{L+1}p^{\frac{-\ell}{L+1}} = \frac{L+1-\ell}{L+1} = 1-\frac{\ell}{L+1}.$$

Лемма 5 доказана. ▲

Воспользуемся определением величины $f_{\mathrm{z}}(w,L)$, выражением $\widetilde{E}_{\mathrm{ex}}(p,w,L)$ для асимметричного Z-канала и результатом леммы 5:

$$f_{\mathrm{z}}(w,L) = \sum_{\ell=1}^{L}\binom{L+1}{\ell}(1-w)^{l}w^{L+1-\ell}\frac{L+1-\ell}{L+1} =$$

$$= \sum_{\ell=1}^{L}\frac{(L+1)!}{\ell!(L+1-\ell)!}(1-w)^{l}w^{L+1-\ell}\frac{L+1-\ell}{L+1} =$$

$$= \sum_{\ell=1}^{L}\frac{L!}{\ell!(L-\ell)!}(1-w)^{l}w^{L+1-\ell} = \sum_{\ell=1}^{L}\binom{L}{\ell}(1-w)^{l}w^{L+1-\ell}.$$

Затем рассмотрим хорошо известное свойство биномиальных коэффициентов:

$$1^L = ((1-w)+w)^L = \sum_{\ell=0}^{L} \binom{L}{\ell} (1-w)^\ell w^{L-\ell} =$$

$$= \binom{L}{0} w^L + \sum_{\ell=1}^{L} \binom{L}{\ell} (1-w)^\ell w^{L-\ell} = w^L + \sum_{\ell=1}^{L} \binom{L}{\ell} (1-w)^\ell w^{L-\ell}.$$

Воспользуемся этим свойством, чтобы получить нужное нам выражение для величины $f_{\text{z}}(w, L)$:

$$f_{\text{z}}(w, L) = w \sum_{\ell=1}^{L} \binom{L}{\ell} (1-w)^l w^{L-\ell} = w(1-w^L).$$

Первая часть теоремы доказана.

2. Найдем значение величины $\max\limits_{w\in[0,1]} f_{\text{z}}(w, L)$. Для этого решим уравнение

$$(f_{\text{z}}(w, L))'_w = 1 - (L+1)w^L = 0.$$

Отсюда получаем $w_{\max} = (L+1)^{-\frac{1}{L}}$ и

$$f_{\text{z}}(L) = \max_{w\in[0,1]} f_{\text{z}}(w, L) = f_{\text{z}}(w_{\max}, L) = \left(\frac{1}{L+1}\right)^{\frac{1}{L}} \left(1 - \frac{1}{L+1}\right).$$

Для нахождения $\lim\limits_{L\to+\infty} \left(\max\limits_{w\in[0,1]} f_{\text{z}}(w, L) \right)$ вычислим сначала следующий предел:

$$\lim_{L\to+\infty} \left(\frac{1}{L+1}\right)^{\frac{1}{L}} = \lim_{L\to+\infty} \exp\left\{-\frac{1}{L}\ln(1+L)\right\} = \lim_{L\to+\infty} \exp\left\{-\frac{1}{L+1}\right\} = 1.$$

Тогда искомый предел будет равен

$$\lim_{L\to+\infty} \left(\max_{w\in[0,1]} f_{\text{z}}(w, L) \right) = \lim_{L\to+\infty} \left(\frac{1}{L+1}\right)^{\frac{1}{L}} \cdot \lim_{L\to+\infty} \left(1 - \frac{1}{L+1}\right) = 1 \cdot 1 = 1.$$

Теорема 6 полностью доказана. ▲

Итак, теорема 5 утверждает, что значение $f_{\text{z}}(w, L)$ является нижней границей доли асимметричных ошибок, исправляемых оптимальным кодом при декодировании списком фиксированной длины в Z-канале с нулевой скоростью передачи, а теорема 6 позволяет точно посчитать эту границу для любых наперед заданных значений w и L. Таблица значений величин $w_{\max}$ и $\max\limits_{w\in[0,1]} f_{\text{z}}(w, L)$ (т.е. доли числа ошибок, исправляемых оптимальным кодом) приведена в § 1.

СПИСОК ЛИТЕРАТУРЫ

1. *Elias P.* List Decoding for Noisy Channels // Tech. Rep. № 335. Research Lab. of Electronics, MIT. Cambridge, MA, USA. 1957. (Reprinted from: IRE WESCON Convention Record. Part 2. P. 99–104). Available at `https://dspace.mit.edu/handle/1721.1/4484`
2. *Wozencraft J.M.* List Decoding. Quarterly Progress Report, Research Lab. of Electronics, MIT. Cambridge, MA, USA. 1958. V. 48. P. 90–95.
3. *Elias P.* Error-Correcting Codes for List Decoding // IEEE Trans. Inform. Theory. 1991. V. 37. № 1. P. 5–12. `https://doi.org/10.1109/18.61123`

4. *Блиновский В.М.* Нижняя граница вероятности ошибки декодирования списком фиксированного объема // Пробл. передачи информ. 1991. Т. 27. № 4. С. 17–33. http://mi.mathnet.ru/ppi578
5. *Блиновский В.М.* Границы для кодов при декодировании списком конечного объема // Пробл. передачи информ. 1986. Т. 22. № 1. С. 11–25. http://mi.mathnet.ru/ppi839
6. *Дьячков А.Г.* Граница выбрасывания при декодировании списком фиксированной длины для дискретного канала без памяти. Неопубликованная рукопись, 1982.
7. *Gallager R.G.* Information Theory and Reliable Communication. New York: Wiley, 1968.
8. *Polyanskii N., Zhang Y.* Codes for the Z-Channel, https://arXiv.org/abs/2105.01427 [cs.IT], 2021.
9. *Lebedev A., Lebedev V., Polyanskii N.* Two-Stage Coding over the Z-Channel, https://arXiv.org/abs/2010.16362v2 [cs.IT], 2020.

Дьячков Аркадий Георгиевич
(29.09.1944 – 20.10.2021)
Гошкодер Даниил Юрьевич
Московский государственный университет
им. М.В. Ломоносова, механико-математический
факультет, кафедра теории вероятностей
daniilgoshkoder@mail.ru

Поступила в редакцию
31.05.2021
После доработки
07.11.2021
Принята к публикации
08.11.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391 : 519.72

© 2021 г. **В.В. Прелов**

О МАКСИМУМЕ f-ДИВЕРГЕНЦИИ ВЕРОЯТНОСТНЫХ РАСПРЕДЕЛЕНИЙ ПРИ ЗАДАННОЙ ВЕЛИЧИНЕ ИХ СКЛЕИВАНИЯ[1]

Статья является дополнением к работе автора [1]. Здесь приводятся явные верхние границы, являющиеся в некоторых случаях оптимальными, для максимального значения f-дивергенции $D_f(P\,\|\,Q)$ дискретных распределений вероятностей P и Q при условии, что заданы распределение Q (или его минимальная компонента $q_{\min}$) и величина склеивания P и Q. Получено также явное выражение для максимума дивергенции $D_f(P\,\|\,Q)$ при условии, что задана только величина склеивания распределений P и Q. Результаты [1], относящиеся к дивергенции Кульбака–Лейблера и χ^2-дивергенции, являются частными случаями утверждений, доказанных в данной статье.

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

DOI: 10.31857/S0555292321040021

В данной статье используются обозначения, принятые в [1], однако для удобства читателя мы напомним некоторые из них, а также введем новые, необходимые нам в дальнейшем. Нас будут интересовать величины $D_f^{\max}(Q,\alpha)$, $D_f^{\max}(q_{\min},\alpha)$ и $D_f^{\max}(\alpha)$, определяемые равенствами

$$D_f^{\max}(Q,\alpha) = \max_{P\colon s(P,Q)=\alpha} D_f(P\,\|\,Q), \tag{1}$$

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

$$D_f^{\max}(\alpha) = \sup_{(P,Q)\colon s(P,Q)=\alpha} D_f(P\,\|\,Q), \tag{3}$$

где $D_f(P\,\|\,Q) = \sum\limits_{i\in\mathcal{N}} q_i f\Big(\frac{p_i}{q_i}\Big)$ – f-дивергенция (см., например, [2]) дискретного распределения вероятностей $P=\{p_i,\ i\in\mathcal{N}\}$ относительно другого дискретного распределения $Q=\{q_i,\ i\in\mathcal{N}\}$ с конечным множеством значений $\mathcal{N}=\{1,2,\dots,n\}$, $q_{\min}=\min\limits_{i\in\mathcal{N}} q_i$, q_i – минимальная компонента распределения $Q=\{q_i,\ i\in\mathcal{N}\}$, а $s(P,Q)$ – величина склеивания распределений P и Q (напомним, что $s(P,Q)=\Pr\{X=Y\}$, где X и Y – дискретные случайные величины, имеющие распределения P и Q соответственно (см. [1])). Заметим сразу, что максимумы правых частей в определениях (1) и (2), как будет показано ниже, достигаются. Заметим также, что здесь, как и в [1], всегда предполагается, что функция $f\colon(0,\infty)\to\mathbb{R}$, определяющая f-дивергенцию $D_f(P\,\|\,Q)$, является выпуклой дважды дифференцируемой функцией,

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

такой что $f''(x) > 0$, $x \neq 1$ и $f(1) = 0$. При этом всегда по определению предполагается, что $0 \cdot f\left(\frac{0}{0}\right) = 0$, $f(0) = \lim\limits_{x \downarrow 0} f(x)$ и $0 \cdot f\left(\frac{a}{0}\right) = \lim\limits_{x \downarrow 0} x f\left(\frac{a}{x}\right) = a \lim\limits_{t \to \infty} \frac{f(t)}{t}$, где $a \neq 0$.

Напомним также, что при заданном распределении вероятностей $Q = \{q_i, i \in \mathcal{N}\}$ всякое равенство

$$\alpha = \sum_{i \in I} q_i + \beta, \quad \text{где} \quad I \subseteq \mathcal{N}, \tag{4}$$

называется *допустимым* (Q, I)*-представлением* α, если либо $\beta = 0$, либо существует индекс $j \in \mathcal{N} \setminus I$, такой что $0 < \beta < q_j$.

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

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

Теорема. *Для любого распределения вероятностей* $Q = \{q_i,\ i \in \mathcal{N}\}$, $q_1 \geqslant q_2 \geqslant \ldots \geqslant q_n > 0$, *и любого* α, $0 \leqslant \alpha \leqslant 1$, *справедливо равенство*

$$D_f^{\max}(Q, \alpha) = \max_{(Q,I)} \max_{M \in \mathcal{M}(Q,I)} D_f(M), \tag{5}$$

где первый максимум в правой части (5) *берется по всем допустимым* (Q, I)*-представлениям* α. *При этом*

$$D_f^{\max}(Q, \alpha) = \infty, \quad \text{если } \alpha \leqslant 1 - q_n \text{ и } f(0) = \infty, \tag{6}$$

и если $\alpha > 1 - q_n$, *то при любом значении* $f(0)$ *справедливо равенство*

$$D_f^{\max}(Q, \alpha) = \max\left\{ q_n f\left(\frac{\alpha - 1 + q_n}{q_n}\right) + q_{n-1} f\left(\frac{1 - \alpha + q_{n-1}}{q_{n-1}}\right), \right.$$
$$\left. q_{n-1} f\left(\frac{\alpha - 1 + q_{n-1}}{q_{n-1}}\right) + q_n f\left(\frac{1 - \alpha + q_n}{q_n}\right) \right\}. \tag{7}$$

В настоящей статье мы дополняем эту теорему нижеследующими предложением и следствием из него для величины $D_f^{\max}(q_{\min}, \alpha)$, определенной в (2).

Предложение 1. *Для любого распределения вероятностей* $Q = \{q_i,\ i \in \mathcal{N}\}$, $q_1 \geqslant q_2 \geqslant \ldots \geqslant q_n > 0$, *для* f*-дивергенции* $D_f^{\max}(Q, \alpha)$ *в случае, когда* $f(0) < \infty$ *и* $f'(0) < \infty$, *справедливы следующие утверждения*:

- *Если* $0 \leqslant \alpha \leqslant q_n$, *то*

$$D_f^{\max}(Q, \alpha) = \max\{A_\alpha(q_n, q_{n-1}), A_\alpha(q_{n-1}, q_n), B_\alpha(q_{n-1}, q_n)\}, \tag{8}$$

где

$$A_\alpha(x,y) = xf\left(\frac{1+\alpha-x}{x}\right) + yf\left(\frac{x-\alpha}{y}\right) + (1-x-y)f(0), \tag{9}$$

$$B_\alpha(x,y) = xf\left(\frac{1-\alpha-x}{x}\right) + yf\left(\frac{x+\alpha}{y}\right) + (1-x-y)f(0); \tag{10}$$

- *Если* $q_n \leqslant \alpha \leqslant 1-q_n$, *то*

$$D_f^{\max}(Q,\alpha) \leqslant q_n f\left(\frac{1-\alpha+q_n}{q_n}\right) + (1-\alpha)f(0), \tag{11}$$

причем эта верхняя граница достигается (*т.е. в* (11) *имеет место знак равенства*), *если* $\alpha = q_n + \sum\limits_{i=1}^{n-1} a_i q_i$ *при некоторых* $a_i \in \{0,1\}$.

Следствие 1. *Для величины* $D_f^{\max}(q_{\min},\alpha)$, *определенной в* (2), *в случае, когда* $f(0) < \infty$, $f'(0) < \infty$ *и* $|\mathcal{N}| = n \geqslant 3$, *справедливы следующие утверждения*:

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

$$D_f^{\max}(q_{\min},\alpha) = A_\alpha(q_{\min},q_{\min}), \tag{12}$$

где $A_\alpha(x,y)$ *определено в* (9);

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

$$D_f^{\max}(q_{\min},\alpha) = q_{\min}\left[f\left(\frac{\alpha-1+q_{\min}}{q_{\min}}\right) + f\left(\frac{1-\alpha+q_{\min}}{q_{\min}}\right)\right]; \tag{13}$$

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

$$D_f^{\max}(q_{\min},\alpha) \leqslant q_{\min} f\left(\frac{1-\alpha+q_{\min}}{q_{\min}}\right) + (1-\alpha)f(0), \tag{14}$$

причем эта верхняя граница достигается, т.е. в (14) *имеет место равенство, если* $2q_{\min} \leqslant \alpha < 1-q_{\min}$ *и* $q_{\min} \leqslant \dfrac{1}{n+1}$, *а также если* $q_{\min} \leqslant \dfrac{1}{n}$ *и* $\alpha = kq_{\min}$, *где* k – *любое целое, такое что* $2 \leqslant k \leqslant n-1$.

Предложение 2. *Для величины* $D_f^{\max}(\alpha)$, *определенной в* (3), *и любого* α, $0 \leqslant \alpha < 1$, *справедливо равенство*

$$D_f^{\max}(\alpha) = (1-\alpha)[f(0) + f^*(0)], \tag{15}$$

где $f^*(x) = xf\left(\dfrac{1}{x}\right)$ *и* $f^*(0) = \lim\limits_{x\downarrow 0} f^*(x) = \lim\limits_{t\to\infty} \dfrac{f(t)}{t}$.

Замечание. Отметим, что дивергенция Кульбака – Лейблера

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

(известная также под многими другими названиями, например, *информационная дивергенция*, *относительная энтропия*, *энтропия меры по мере*, *информация для различения* или просто *дивергенция*) и χ^2-дивергенция

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

являются важнейшими частными случаями f-дивергенции, когда $f(t) = t\log t$ и $f(t) = (t-1)^2$ соответственно (см., например, [3, 4]). Результаты в [1], относящиеся к дивергенции Кульбака – Лейблера и χ^2-дивергенции, являются частными случаями результатов, полученных в приведенных выше предложении 1 и следствии 1. Отметим, например, что для дивергенции Кульбака – Лейблера и χ^2-дивергенции в формуле (8) максимальной является величина $A(q_n, q_{n-1})$, откуда и вытекают соответствующие формулы в [1]. В общем же случае для f-дивергенции не удается выяснить, какая из трех величин в (8) является максимальной, поскольку это существенно зависит от вида и свойств функции f.

Отметим также, что аналог равенства (15) в случае, когда вместо условия на величину склеивания распределений P и Q накладывается условие на вариационное расстояние $V(P,Q)$ между ними, был получен в работах [3,5]. А именно, в них было показано, что справедливо равенство

$$\sup_{(P,Q)\colon V(P,Q)=v} D_f(P\,\|\,Q) = \frac{v}{2}[f(0) + f^*(0)].$$

Доказательство предложения 1. **1.** Докажем вначале формулу (8), когда предполагается, что $0 \leqslant \alpha \leqslant q_n$. В этом случае в соответствии с (5) оптимальная матрица M_{opt}, задающая α-склеивание данного распределения вероятностей $Q = \{q_i,\, i \in \mathcal{N}\}$ с некоторым распределением $P = \{p_i,\, i \in \mathcal{N}\}$, для которой $D_f(M_{\text{opt}}) = D_f(P\,\|\,Q) = D_f^{\max}(Q,\alpha)$, находится среди матриц $M = \|p_{ij}\|_{i,j=1}^n$, у которых на диагонали в некотором столбце стоит α, остальные диагональные элементы равны нулю, а главный столбец либо содержит α, либо нет. Поэтому, пользуясь формулой

$$D_f(P\,\|\,Q) = \sum_{i\colon p_i>0} q_i f\left(\frac{p_i}{q_i}\right) + \left(\sum_{i\colon p_i=0} q_i\right) f(0), \tag{16}$$

получаем, что для таких матриц величина $D_f(M)$ может иметь три разных вида:

- Если α стоит на диагонали в k-м (главном) столбце, а $q_k - \alpha$ – в k-й строке и ℓ-м столбце, то

$$D_f(M) = A_\alpha(q_k, q_\ell) = \\ = q_k f\left(\frac{1+\alpha-q_k}{q_k}\right) + q_\ell f\left(\frac{q_k-\alpha}{q_\ell}\right) + (1-q_k-q_\ell) f(0); \tag{17}$$

- Если на диагонали в главном k-м столбце стоит ноль, α стоит на диагонали в ℓ-м столбце и q_k стоит в k-й строке и ℓ-м столбце, то

$$D_f(M) = B_\alpha(q_k, q_\ell) = \\ = q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_\ell f\left(\frac{q_k+\alpha}{q_\ell}\right) + (1-q_k-q_\ell) f(0); \tag{18}$$

- Если на диагонали в главном k-м столбце стоит ноль, q_k стоит в k-й строке и ℓ-м столбце, а α – на диагонали в m-м ($m \neq \ell$) столбце, то

$$D_f(M) = C_\alpha(q_k, q_\ell, q_m) = \\ = q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_\ell f\left(\frac{q_k}{q_\ell}\right) + q_m f\left(\frac{\alpha}{q_m}\right) + (1-q_k-q_\ell-q_m) f(0). \tag{19}$$

Поэтому

$$D_f^{\max}(Q,\alpha) = \max\{A_\alpha, B_\alpha, C_\alpha\}, \tag{20}$$

где

$$A_\alpha = \max_{k,\ell} A_\alpha(q_k, q_\ell), \quad B_\alpha = \max_{k,\ell} B_\alpha(q_k, q_\ell), \quad C_\alpha = \max_{k,\ell,m} C_\alpha(q_k, q_\ell, q_m), \tag{21}$$

а максимумы в (21) берутся по всем различным между собой натуральным числам k, ℓ и m из множества $\mathcal{N}$. Докажем теперь следующее утверждение.

Лемма 1. *Справедливо неравенство $C_\alpha \leqslant B_\alpha$, где B_α и C_α определены в* (21).

Доказательство. Достаточно показать, что при любом фиксированном значении k справедливо неравенство

$$\max_{\ell:\, \ell\neq k} q_\ell f\left(\frac{q_k+\alpha}{q_\ell}\right) \geqslant \max_{(\ell,m):\, \ell\neq k,\, m\neq k} \left[q_\ell f\left(\frac{q_k}{q_\ell}\right) + q_m f\left(\frac{\alpha}{q_m}\right) - q_m f(0)\right]. \tag{22}$$

Для этого заметим, что функция $xf\left(\frac{a}{x}\right) - xf(0)$ убывает по x, если $a = \mathrm{const} > 0$ и $x > 0$. Действительно,

$$\left[xf\left(\frac{a}{x}\right) - xf(0)\right]'_x = f\left(\frac{a}{x}\right) - \left(\frac{a}{x}\right) f'\left(\frac{a}{x}\right) - f(0) < 0,$$

так как функция $f(u) - uf'(u) - f(0)$ убывает по u, а при $u = 0$ она равна нулю. Поэтому, полагая

$$s = \begin{cases} n, & \text{если } k \neq n, \\ n-1, & \text{если } k = n, \end{cases}$$

получаем, что для доказательства (22) достаточно показать, что

$$q_s f\left(\frac{q_k+\alpha}{q_s}\right) - q_s f(0) \geqslant q_s f\left(\frac{q_k}{q_s}\right) - q_s f(0) + q_s f\left(\frac{\alpha}{q_s}\right) - q_s f(0),$$

т.е. что

$$f\left(\frac{q_k+\alpha}{q_s}\right) \geqslant f\left(\frac{q_k}{q_s}\right) + f\left(\frac{\alpha}{q_s}\right) - f(0). \tag{23}$$

Справедливость неравенства (23), а значит, и леммы 1, следует из того, что разность левой и правой частей в (23) возрастает по α, а при $\alpha = 0$ она равна нулю. ▲

Лемма 2. *Справедливо равенство*

$$\max\{A_\alpha, B_\alpha\} = \max\bigl\{A_\alpha(q_n, q_{n-1}), A_\alpha(q_{n-1}, q_n), B_\alpha(q_{n-1}, q_n)\bigr\},$$

где A_α и B_α определены в (21), *а $A_\alpha(x,y)$ и $B_\alpha(x,y)$ – в* (9) *и* (10).

Доказательство. Прежде всего заметим, что $A_\alpha(q_k, q_\ell)$ и $B_\alpha(q_k, q_\ell)$ являются выпуклыми функциями от q_k и убывающими от q_ℓ. Поэтому (см. (21))

$$A_\alpha = \max\bigl\{A_\alpha(q_{n-1}, q_n), A_\alpha(q_1, q_n), A_\alpha(q_n, q_{n-1})\bigr\}, \tag{24}$$

$$B_\alpha = \max\bigl\{B_\alpha(q_{n-1}, q_n), B_\alpha(q_1, q_n), B_\alpha(q_n, q_{n-1})\bigr\}. \tag{25}$$

Покажем теперь, что

$$A_\alpha(q_1, q_n) \leqslant \max\bigl\{A_\alpha(q_{n-1}, q_n), B_\alpha(q_n, q_{n-1})\bigr\}, \tag{26}$$

$$B_\alpha(q_1, q_n) \leqslant \max\bigl\{B_\alpha(q_{n-1}, q_n), A_\alpha(q_n, q_{n-1})\bigr\}. \tag{27}$$

Действительно, для доказательства (26) заметим, что если $[A_\alpha(x, q_n)]'_x\big|_{x=q_1} < 0$, то $A_\alpha(x, q_n)$ убывает по x при всех $0 < x < q_1$, и тогда $A_\alpha(q_1, q_n) < A(q_{n-1}, q_n)$.

Если же $[A_\alpha(x,q_n)]'_x\big|_{x=q_1} > 0$, то $A_\alpha(x,q_n)$ возрастает по x при $x > q_1$, и тогда $A_\alpha(q_1,q_n) < A(1-q_n,q_n)$.

Поэтому для доказательства (26) необходимо только показать, что

$$A_\alpha(1-q_n,q_n) \leqslant B_\alpha(q_n,q_{n-1}). \tag{28}$$

Сравнивая выражения для $A_\alpha(1-q_n,q_n)$ и $B_\alpha(q_n,q_{n-1})$ (см. (9) и (10)), мы видим, что для доказательства (28) достаточно лишь убедиться, что

$$(1-q_n)f\left(\frac{\alpha+q_n}{1-q_n}\right) - (1-q_n)f(0) \leqslant q_{n-1}f\left(\frac{\alpha+q_n}{q_{n-1}}\right) - q_{n-1}f(0).$$

А это неравенство следует из того, что, как было показано выше при доказательстве леммы 1, функция $xf\left(\frac{a}{x}\right) - xf(0)$ убывает по x, если $a = \mathrm{const} > 0$ и $x > 0$. Неравенство (26) доказано. Неравенство (27) доказывается аналогично. Поэтому, учитывая (24)–(27), получаем, что

$$\max\{A_\alpha, B_\alpha\} = \max\big\{A_\alpha(q_{n-1},q_n), A_\alpha(q_n,q_{n-1}), B_\alpha(q_{n-1},q_n), B_\alpha(q_n,q_{n-1})\big\}.$$

Таким образом, для доказательства леммы 2 достаточно лишь показать, что $B_\alpha(q_n,q_{n-1}) \leqslant A_\alpha(q_n,q_{n-1})$. Для доказательства этого последнего неравенства следует лишь убедиться, что производная разности $A_\alpha(q_n,q_{n-1}) - B_\alpha(q_n,q_{n-1})$ по α положительна, а при $\alpha = 0$ эта разность равна нулю. ▲

Наконец, формула (8) теперь следует из (20) и лемм 1 и 2.

2. Докажем теперь верхнюю границу (11) в случае, когда $q_n < \alpha < 1-q_n$. Для этого в соответствии с (5) достаточно показать, что для всех матриц M, осуществляющих α-склеивание заданного распределения вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$ с некоторым распределением $P = \{p_i,\ i \in \mathcal{N}\}$ и принадлежащих множествам $\mathcal{M}(Q,I)$, соответствующих всевозможным допустимым (Q,I)-представлениям α, справедливо неравенство

$$D_f(M) \leqslant q_n f\left(\frac{1-\alpha+q_n}{q_n}\right) + (1-\alpha)f(0). \tag{29}$$

Пусть $\alpha = \sum\limits_{i\in I} q_i + \beta$, где $\beta = 0$ или существует j, такое что $0 < \beta < q_j$ для некоторого $j \in \mathcal{N} \setminus I$, – произвольное допустимое (Q,I)-представление α (отметим, что в случае, когда $I = \varnothing$, считаем, что $\sum\limits_{i\in I} q_i = 0$). Тогда величина $D_f(M)$, соответствующая различным матрицам $M \in \mathcal{M}(Q,I)$, может принимать разные значения в зависимости от расположения главного столбца (диагональным элементом которого является либо некоторое q_k, $k \in I$, либо ноль, либо β) и единственного ненулевого элемента вне главного столбца и диагонали (хотя при некоторых (Q,I)-представлениях α такой элемент может вообще отсутствовать). Рассмотрим каждый из этих случаев в отдельности и покажем, что для каждого из них справедливо неравенство (29).

а) Если диагональным элементом главного (k-го) столбца матрицы $M \in \mathcal{M}(Q,I)$ служит q_k, где $k \in I$, а элемент β расположен на диагонали в j-м столбце, то воспользовавшись формулой (16), получим, что

$$D_f(M) = q_k f\left(\frac{1-\alpha+q_k}{q_k}\right) + q_j f\left(\frac{\beta}{q_j}\right) + (1-\alpha-q_j+\beta)f(0). \tag{30}$$

Справедливость верхней границы (29) в этом случае следует из того, что функция $q_k f\Big(\dfrac{1-\alpha+q_k}{q_k}\Big)$ убывает по q_k, а при любых q_j и β, $0 \leqslant \beta \leqslant q_j$, имеет место неравенство

$$q_j f\left(\frac{\beta}{q_j}\right) - (q_j - \beta) f(0) \leqslant 0. \tag{31}$$

Действительно, неравенство (31) следует из того, что его левая часть является выпуклой функцией β, а при $\beta = 0$ и $\beta = q_j$ она равна нулю (так как по условию $f(1) = 0$).

b1) Если диагональным элементом главного k-го столбца матрицы $M \in \mathcal{M}(Q, I)$ служит ноль, элементы q_k и q_j, где $k \notin I$, $j \in I$, находятся в j-м столбце, а элемент β расположен на диагонали в i-м столбце, то для такой матрицы

$$\begin{aligned} D_f(M) &= q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_j f\left(\frac{q_k+q_j}{q_j}\right) + q_i f\left(\frac{\beta}{q_i}\right) + \\ &+ (1-\alpha+\beta-q_k-q_i) f(0). \end{aligned} \tag{32}$$

Воспользовавшись тем, что $q_i f\Big(\dfrac{\beta}{q_i}\Big) - (q_i - \beta) f(0) \leqslant 0$ (см. (31)), получаем оценку

$$D_f(M) \leqslant q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_j f\left(\frac{q_k+q_j}{q_j}\right) + (1-\alpha) f(0) - q_k f(0). \tag{33}$$

Поэтому для доказательства верхней границы (29) в рассматриваемом случае достаточно показать, что при любых q_k и q_j справедливо неравенство

$$q_n f\left(\frac{1-\alpha+q_n}{q_n}\right) \geqslant q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_j f\left(\frac{q_k+q_j}{q_j}\right) - q_k f(0). \tag{34}$$

Для доказательства неравенства (34) заметим, что разность его левой и правой частей убывает по α, а при максимальном значении $\alpha = 1 - q_k$ (так как в рассматриваемом случае на диагонали в k-м столбце стоит ноль) эта разность, равная $q_n f\Big(\dfrac{q_k+q_n}{q_n}\Big) - q_j f\Big(\dfrac{q_k+q_j}{q_j}\Big)$, положительна, поскольку функция $q_j f\Big(\dfrac{q_k+q_j}{q_j}\Big)$ убывает по q_j.

b2) Если диагональным элементом главного k-го столбца матрицы $M \in \mathcal{M}(Q, I)$ служит ноль, q_k находится в i-м столбце, в котором на диагонали стоит β, то для такой матрицы

$$\begin{aligned} D_f(M) &= q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_i f\left(\frac{q_k+\beta}{q_i}\right) + (1-\alpha+\beta-q_k-q_i) f(0) = \\ &= q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_i f\left(\frac{q_k+\beta}{q_i}\right) + (1-\alpha) f(0) - q_k f(0) - q_i f\left(\frac{\beta}{q_i}\right) + \\ &+ \left[q_i f\left(\frac{\beta}{q_i}\right) - (q_i-\beta) f(0)\right] \leqslant q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_i f\left(\frac{q_k+q_i}{q_i}\right) + \\ &+ (1-\alpha) f(0) - q_k f(0). \end{aligned} \tag{35}$$

Неравенство в (35) следует из (31) и того факта, что

$$q_i f\left(\frac{q_k+q_i}{q_i}\right) \geqslant q_i f\left(\frac{q_k+\beta}{q_i}\right) - q_i f\left(\frac{\beta}{q_i}\right). \tag{36}$$

Действительно, справедливость неравенства (36) является следствием того, что его правая часть является возрастающей функцией β, а при максимальном значении $\beta = q_i$ левая и правая части (36) равны. Теперь заметим, что правая часть неравенства (35) совпадает с выражением правой части в (33), которую мы уже оценили сверху в п. b1), показав, что она не превосходит нужной нам оценки (29).

b3) Если диагональным элементом главного k-го столбца матрицы $M \in \mathcal{M}(Q, I)$ служит ноль, q_k находится в ℓ-м столбце, диагональным элементом которого является ноль, а β находится на диагонали в i-м столбце, то для такой матрицы

$$D_f(M) = q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_i f\left(\frac{\beta}{q_i}\right) + q_\ell f\left(\frac{q_k}{q_\ell}\right) +$$
$$+ (1-\alpha+\beta-q_k-q_i-q_\ell)f(0) \leqslant q_k f\left(\frac{1-\alpha-q_k}{q_k}\right) + q_i f\left(\frac{\beta}{q_i}\right) +$$
$$+ q_\ell f\left(\frac{q_k+q_\ell}{q_\ell}\right) + (1-\alpha+\beta-q_k-q_i)f(0). \tag{37}$$

Неравенство в (37) следует из того, что

$$q_\ell f\left(\frac{q_k}{q_\ell}\right) - q_\ell f(0) \leqslant q_\ell f\left(\frac{q_k+q_\ell}{q_\ell}\right). \tag{38}$$

Действительно, справедливость (38) является следствием того, что ввиду выпуклости функции $f(x)$ и условия $f(1) = 0$ имеет место неравенство $f(1+x) \geqslant f(x) - f(0)$. Правая часть неравенства (37) совпадает с выражением правой части в (32), которую мы уже оценили сверху в п. b1), показав, что она не превосходит оценки (29).

c1) Если диагональным элементом главного k-го столбца матрицы $M \in \mathcal{M}(Q, I)$ служит β, а $q_k - \beta$ находится в j-м столбце, диагональным элементом которого является q_j, $j \in I$, то для такой матрицы

$$D_f(M) =$$
$$= q_k f\left(\frac{1-\alpha-q_k+2\beta}{q_k}\right) + q_j f\left(\frac{q_k+q_j-\beta}{q_j}\right) + (1-\alpha+\beta-q_k)f(0). \tag{39}$$

Так как правая часть (39) является выпуклой функцией β, то ее максимум достигается либо при $\beta = 0$, либо при $\beta = q_k$. В случае $\beta = 0$ правая часть (39) совпадает с правой частью (33), которую мы уже оценивали сверху в п. b1), показав, что она не превосходит оценки (29). Если же $\beta = q_k$, то максимум правой части (39) очевидно совпадает с доказываемой оценкой (29).

c2) Если диагональным элементом главного k-го столбца матрицы $M \in \mathcal{M}(Q, I)$ служит β, а $q_k - \beta$ находится в i-м столбце, диагональным элементом которого является ноль, то для такой матрицы

$$D_f(M) =$$
$$= q_k f\left(\frac{1-\alpha-q_k+2\beta}{q_k}\right) + q_i f\left(\frac{q_k-\beta}{q_i}\right) + (1-\alpha+\beta-q_k-q_i)f(0). \tag{40}$$

Снова очевидно, что правая часть (40) является выпуклой функцией β, а тогда опять все сводится к рассмотренным ранее случаям (см. (37), (39)).

Верхняя граница (11) теперь полностью доказана. Наконец, очевидно, что верхняя граница (11) достигается, если $\alpha = q_n + \sum\limits_{i=1}^{n-1} a_i q_i$ при любых $a_i \in \{0, 1\}$, так как в этом случае $\beta = 0$ и в (30) при $q_k = q_n$ получаем нужное нам равенство. ▲

Доказательство следствия 1. Равенство (12) для случая, когда $0 \leqslant \alpha \leqslant q_n$ и $|\mathcal{N}| = n \geqslant 3$, следует из того, что значение $D_f^{\max}(q_{\min}, \alpha)$ достигается для распределения $Q = \{q_i,\ i \in \mathcal{N}\}$, у которого $q_{n-1} = q_n = q_{\min}$, в чем нетрудно убедиться, просматривая доказательство равенства (8). При этом этот максимум равен $A_\alpha(q_n, q_n)$, где $A_\alpha(x, y)$ определено в (9). Действительно, в случае, когда $q_{n-1} = q_n = q_{\min}$, имеем $A_\alpha(q_n, q_{n-1}) = A_\alpha(q_{n-1}, q_n) = A_\alpha(q_n, q_n)$, и нетрудно видеть, что $A_\alpha(q_n, q_n) \geqslant B_\alpha(q_n, q_n)$, для чего следует лишь заметить, что разность $A_\alpha(q_n, q_n) - B_\alpha(q_n, q_n)$ возрастает по α, а при $\alpha = 0$ эта разность равна нулю.

Равенство (13) также легко доказать, заметив, что максимумы каждого из двух выражений в (7) достигаются при $q_{n-1} = q_n = q_{\min}$, а в этом случае оба этих выражения совпадают.

Наконец, верхняя граница (14) является прямым следствием (11), а справедливость равенства в (14) также следует из утверждения предложения об условиях равенства в (11), поскольку при сформулированных там условиях нетрудно предъявить соответствующие распределения вероятностей $Q = \{q_i,\ i \in \mathcal{N}\}$, при которых имеет место равенство $\alpha = \sum\limits_{i=1}^{n-1} a_i q_i + q_n$ при некоторых $a_i \in \{0, 1\}$ (см. доказательство следствия 1 в [1]). ▲

Доказательство предложения 2. Заметим вначале, что из определения f-дивергенции сразу следует, что $D_f^{\max}(\alpha) = 0$, если $\alpha = 1$. Далее заметим, что в случае, когда $0 \leqslant \alpha < 1$ и либо $f(0) = \infty$, либо $f^*(0) = \infty$, равенство (15) очевидно, так как всегда можно построить матрицу $M = \|p_{ij}\|_{i,j=1}^n$, задающую α-склеивание некоторого распределения вероятностей $P = \{p_i,\ i \in \mathcal{N}\}$ с другим распределением $Q = \{q_i,\ i \in \mathcal{N}\}$, такую что либо некоторое $p_i = 0$, а соответствующее $q_i \neq 0$ (в случае, когда $f(0) = \infty$), либо некоторое $q_i = 0$, а $p_i \neq 0$ (в случае $f^*(0) = \infty$). Поэтому в дальнейшем при доказательстве равенства (15) будем всегда предполагать, что и $f(0) < \infty$, и $f^*(0) < \infty$.

Далее для доказательства (15) воспользуемся следующими неравенствами для выпуклой функции $f(x)$, задающей f-дивергенцию $D_f(P \,\|\, Q)$:

$$f(x) \leqslant \begin{cases} (1-x)f(0), & \text{если } 0 < x < 1, \\ (x-1)f^*(0), & \text{если } x > 1. \end{cases} \tag{41}$$

Действительно, первое неравенство следует из определения выпуклости функции $f(x)$ и условия $f(1) = 0$, второе – из того, что функция $f^*(x) = xf(1/x)$ тоже выпукла и $f^*(1) = 0$.

Теперь, поскольку

$$D_f^{\max}(\alpha) = \sup_{q_{\min}:\, 0 < q_{\min} \leqslant 1/n} D_f^{\max}(q_{\min}, \alpha), \tag{42}$$

то для получения оценки сверху для $D_f^{\max}(\alpha)$ достаточно оценить сверху функции от $q_{\min}$, стоящие в правых частях равенств (12), (13) и неравенства (14) при заданном параметре α, $0 \leqslant \alpha < 1$, и любом возможном значении $q_{\min}$. Замечая, что функции в правых частях равенств (12),(13) являются выпуклыми относительно $q_{\min}$, а функция в правой части неравенства (14) убывает по $q_{\min}$, то очевидно имеем

$$A(q_{\min}, q_{\min}) \leqslant \max\{A_\alpha(\alpha, \alpha), A_\alpha(1, 1)\}, \tag{43}$$

так как в (12) предполагается, что $q_{\min} \geqslant \alpha$,

$$q_{\min}\left[f\left(\frac{\alpha - 1 + q_{\min}}{q_{\min}}\right) + f\left(\frac{1 - \alpha + q_{\min}}{q_{\min}}\right)\right] \leqslant$$
$$\leqslant \max\big\{(1-\alpha)[f(0) + f(2)], f(\alpha) + f(2-\alpha)\big\}, \tag{44}$$

так как в (13) предполагается, что $q_{\min} \geqslant 1-\alpha$, и

$$q_{\min} f\left(\frac{1-\alpha+q_{\min}}{q_{\min}}\right) \leqslant 0 \cdot f\left(\frac{1-\alpha}{0}\right) = (1-\alpha) f^*(0), \tag{45}$$

так как в (14) предполагается, что $q_{\min} \leqslant \alpha$.

Поэтому, воспользовавшись неравенствами (41) для оценивания сверху выражений в (43)–(45) и учитывая (12)–(14) и (42), получаем, что

$$D_f^{\max}(\alpha) \leqslant (1-\alpha)[f(0) + f^*(0)]. \tag{46}$$

Таким образом, для доказательства равенства (15) необходимо показать, что на самом деле знак неравенства в (46) можно заменить на знак равенства при любом α, $0 \leqslant \alpha < 1$. Покажем это. Действительно, если $\alpha = 0$, то из (12) следует, что

$$\lim_{q_{\min}\to 0} D_f^{\max}(q_{\min}, \alpha) = \lim_{x\to 0} A_0(x,x) = \lim_{t\to\infty} \frac{f(t)}{t+1} + f(0) = f^*(0) + f(0).$$

Это означает, что при $\alpha = 0$ в (46) имеет место знак равенства, т.е. равенство (15) доказано для $\alpha = 0$. Если же α, $0 < \alpha < 1$, – любое фиксированное число, то в (14) при достаточно малых $q_{\min}$ имеет место знак равенства, а тогда

$$\lim_{q_{\min}\to 0} D_f^{\max}(q_{\min}, \alpha) = \lim_{x\to 0}\left[x f\left(\frac{1-\alpha+x}{x}\right)\right] + (1-\alpha) f(0) =$$
$$= \lim_{t\to\infty} (1-\alpha)\frac{f(t)}{t-1} + (1-\alpha) f(0) = (1-\alpha)[f^*(0) + f(0)],$$

так что снова в (46) имеет место знак равенства, а значит, равенство (15) справедливо и при любом α, $0 < \alpha < 1$. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Прелов В.В.* f-дивергенция и склеивание вероятностных распределений // Пробл. передачи информ. 2021. Т. 57. № 1. С. 64–80. https://doi.org/10.31857/S0555292321010034
2. *Csiszár I.* Information-type Measures of Difference of Probability Distributions and Indirect Observations // Studia Sci. Math. Hungar. 1967. V. 2. № 3–4. P. 299–318.
3. *Sason I., Verdú S.* f-Divergence Inequalities // IEEE Trans. Inform. Theory. 2016. V. 62. № 11. P. 5973–6006. https://doi.org/10.1109/TIT.2016.2603151
4. *Макур А., Чжен Л.* Сравнение коэффициентов сжатия для f-дивергенций // Пробл. передачи информ. 2020. Т. 56. № 2. С. 3–62. https://doi.org/10.31857/S0555292320020011
5. *Basu A., Shioya Y., Park C.* Statistical Inference: The Minimum Distance Approach. Boca Raton, FL: CRC Press, 2011.

Прелов Вячеслав Валерьевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
prelov@iitp.ru

Поступила в редакцию
12.11.2021
После доработки
16.11.2021
Принята к публикации
16.11.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391.1 : 519.725

© 2021 г. **В.А. Зиновьев, Д.В. Зиновьев**

ОБ ОБОБЩЕННОЙ КАСКАДНОЙ КОНСТРУКЦИИ КОДА НОРДСТРОМА – РОБИНСОНА И ДВОИЧНОГО КОДА ГОЛЕЯ[1]

Показано, что код Нордстрома – Робинсона и двоичный расширенный код Голея являются обобщенными каскадными кодами третьего порядка.

Ключевые слова: обобщенный каскадный код, код Нордстрома – Робинсона, двоичный расширенный код Голея.

DOI: 10.31857/S0555292321040033

§ 1. Введение

Пусть $E_q = \{0, 1, \ldots, q-1\}$ – алфавит размера q. Произвольное подмножество $C \subseteq E_q^n$ называется q-ичным кодом и обозначается через $(n, N, d)_q$, где n – длина кода, N – число его кодовых слов (или мощность), и d – его минимальное расстояние (Хэмминга). Линейный код C с параметрами $(n, N = q^k, d)_q$ обозначается через $[n, k, d]_q$. Для двоичных кодов приняты обозначения (n, N, d) и $[n, k, d]$ (т.е. q опускается). Пусть $J = \{1, 2, \ldots, n\}$ – координатное множество E_q^n. Для вектора $\boldsymbol{x} = (x_1, \ldots, x_n) \in E_q^n$ обозначим через $\operatorname{supp}(\boldsymbol{x})$ его носитель, т.е.

$$\operatorname{supp}(\boldsymbol{x}) = \{i \in J : \ x_i \neq 0\}.$$

Обозначим через $\operatorname{wt}(\boldsymbol{x})$ вес вектора $\boldsymbol{x}$, т.е. размер его носителя: $\operatorname{wt}(\boldsymbol{x}) = |\operatorname{supp}(\boldsymbol{x})|$. Для двоичного вектора $\boldsymbol{x}$ обозначим через $\bar{\boldsymbol{x}}$ дополнительный к нему вектор, т.е. вектор, полученный из $\boldsymbol{x}$ взаимной заменой элементов 0 и 1: $\bar{\boldsymbol{x}} = \boldsymbol{x} + (1, 1, \ldots, 1)$.

Нелинейный код Нордстрома – Робинсона с параметрами

$$n = 16, \quad N = 2^8, \quad d = 6$$

был построен в 1968 г. Нордстромом и Робинсоном [1] и независимо в [2]. Двоичный расширенный совершенный код Голея с параметрами

$$n = 24, \quad N = 2^{12}, \quad d = 8$$

был построен в 1949 г. Голеем [3]. По обоим кодам опубликовано очень много работ, значительная часть которых может быть найдена в монографии [4]. В частности, в [5] установлено, что код Нордстрома – Робинсона и двоичный код Голея единственны с точностью до эквивалентности. Это существенно упрощает нашу задачу (а именно достаточно построить ОК-коды с параметрами этих кодов). Мы только

[1] Работа выполнена в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364) и Национального научного фонда Болгарии (номер проекта 20-51-18002).

еще сошлемся на некоторые более поздние статьи, в основном по коду Нордстрома – Робинсона, в связи с полученными там интересными результатами (см. работы [6–12] и библиографию в них). Отметим, что в [13] (см. библиографию) было дано представление кода Голея как каскадного кода, полученного отображением из построенного в [13] кода длины 12 над $\mathbb{F}_4$ в двоичный код.

§ 2. Построение кода Нордстрома – Робинсона

Пусть B обозначает тривиальный $(4, 16, 1)$-код (т.е. все двоичные векторы длины 4). Этот код B разбивается на два тривиальных подкода: $(4, 8, 2)$-код B_1 с проверкой на четность и $(4, 8, 2)$-код B_2 с проверкой на нечетность, которые, в свою очередь, разбиваются на тривиальные $(4, 2, 4)$-коды $B_{i,j}$. Эти коды мы приводим вместе с нумерацией их слов (вектор с номером $\boldsymbol{b}(i, j, k)$, $k = 1, 2$, принадлежит коду $B_{i,j}$):

$$
\begin{aligned}
B_{1,1} &= \{\boldsymbol{b}(1,1,1) = (0\,0\,0\,0),\ \boldsymbol{b}(1,1,2) = (1\,1\,1\,1)\},\\
B_{1,2} &= \{\boldsymbol{b}(1,2,1) = (1\,1\,0\,0),\ \boldsymbol{b}(1,2,2) = (0\,0\,1\,1)\},\\
B_{1,3} &= \{\boldsymbol{b}(1,3,1) = (1\,0\,1\,0),\ \boldsymbol{b}(1,3,2) = (0\,1\,0\,1)\},\\
B_{1,4} &= \{\boldsymbol{b}(1,4,1) = (1\,0\,0\,1),\ \boldsymbol{b}(1,4,2) = (0\,1\,1\,0)\},\\
B_{2,1} &= \{\boldsymbol{b}(2,1,1) = (1\,0\,0\,0),\ \boldsymbol{b}(2,1,2) = (0\,1\,1\,1)\},\\
B_{2,2} &= \{\boldsymbol{b}(2,2,1) = (0\,1\,0\,0),\ \boldsymbol{b}(2,2,2) = (1\,0\,1\,1)\},\\
B_{2,3} &= \{\boldsymbol{b}(2,3,1) = (0\,0\,1\,0),\ \boldsymbol{b}(2,3,2) = (1\,1\,0\,1)\},\\
B_{2,4} &= \{\boldsymbol{b}(2,4,1) = (0\,0\,0\,1),\ \boldsymbol{b}(2,4,2) = (1\,1\,1\,0)\}.
\end{aligned}
$$

В качестве внешних выберем два МДР-кода A_1 и V_1 с параметрами $(4, 16, 3)_4$, которые разбиваются на подкоды $A_{1,i}$, $i = 1, 2, 3, 4$, и $V_{1,j}$, $j = 1, 2, 3, 4$, с расстоянием 4:

$$
A_{1,1} = \begin{bmatrix}(0\,0\,0\,0)\\(1\,1\,1\,1)\\(2\,2\,2\,2)\\(3\,3\,3\,3)\end{bmatrix},\quad
A_{1,2} = \begin{bmatrix}(0\,3\,2\,1)\\(3\,0\,1\,2)\\(2\,1\,0\,3)\\(1\,2\,3\,0)\end{bmatrix},\quad
A_{1,3} = \begin{bmatrix}(0\,2\,1\,3)\\(2\,0\,3\,1)\\(1\,3\,0\,2)\\(3\,1\,2\,0)\end{bmatrix},\quad
A_{1,4} = \begin{bmatrix}(0\,1\,3\,2)\\(1\,0\,2\,3)\\(3\,2\,0\,1)\\(2\,3\,1\,0)\end{bmatrix} \tag{1}
$$

и

$$
V_{1,1} = \begin{bmatrix}(0\,0\,0\,0)\\(1\,1\,1\,1)\\(2\,2\,2\,2)\\(3\,3\,3\,3)\end{bmatrix},\quad
V_{1,2} = \begin{bmatrix}(0\,1\,2\,3)\\(1\,0\,3\,2)\\(2\,3\,0\,1)\\(3\,2\,1\,0)\end{bmatrix},\quad
V_{1,3} = \begin{bmatrix}(0\,2\,3\,1)\\(2\,0\,1\,3)\\(3\,1\,0\,2)\\(1\,3\,2\,0)\end{bmatrix},\quad
V_{1,4} = \begin{bmatrix}(0\,3\,1\,2)\\(3\,0\,2\,1)\\(1\,2\,0\,3)\\(2\,1\,3\,0)\end{bmatrix}. \tag{2}
$$

Коды A_1 и V_1 пересекаются по подкодам $A_{1,1}$ и $V_{1,1}$, а все другие подкоды $A_{1,i}$, $i = 2, 3, 4$, и $V_{1,j}$, $j = 2, 3, 4$, находятся друг от друга на расстоянии 2 или 3, т.е.

$$
d(A_{1,i}, V_{1,j}) = \begin{cases} 0, & \text{если } i = j = 1,\\ 2, & \text{если } i, j \in \{2, 3, 4\},\\ 3, & \text{если } 1 \in \{i, j\},\ i \neq j. \end{cases} \tag{3}
$$

В качестве внешних кодов A_2 и V_2 возьмем два двоичных $(4, 8, 2)$-кода (т.е. внутренние коды B_1 и B_2): A_2 (с проверкой на четность) и V_2 (с проверкой на нечетность), которые разбиваются на подкоды $A_{2,i}$, где $i = 1, 2$, и $V_{2,j}$, где $j = 1, 2$, с расстоя-

нием 2:

$$A_{2,1} = \begin{bmatrix}(0\,0\,0\,0)\\(1\,1\,0\,0)\\(1\,0\,1\,0)\\(1\,0\,0\,1)\end{bmatrix}, \quad A_{2,2} = \begin{bmatrix}(1\,1\,1\,1)\\(0\,0\,1\,1)\\(0\,1\,0\,1)\\(0\,1\,1\,0)\end{bmatrix} \tag{4}$$

и

$$V_{2,1} = \begin{bmatrix}(1\,0\,0\,0)\\(0\,1\,0\,0)\\(0\,0\,1\,0)\\(0\,0\,0\,1)\end{bmatrix}, \quad V_{2,2} = \begin{bmatrix}(0\,1\,1\,1)\\(1\,0\,1\,1)\\(1\,1\,0\,1)\\(1\,1\,1\,0)\end{bmatrix}. \tag{5}$$

Построим следующие три ОКК-кода [14]:

- код C на основе внешних кодов $A = \{(0\,0\,0\,0), (1\,1\,1\,1)\}$, $A_1 \cup V_1$ (интерпретируя это как множество с повторениями), $A_2 \cup V_2$ и внутреннего кода $B = B_1 \cup B_2$;
- код C_1 на основе внешних кодов A_1 и A_2 и внутреннего кода B_1;
- код C_2 на основе внешних кодов V_1 и V_2 и внутреннего кода B_2.

Поясним построение кода C_1. Выберем два слова: $\boldsymbol{a} = (a_1, a_2, a_3, a_4)$ из кода A_1 и $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$ из кода A_2. Они индуцируют слово $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ кода C_1. В качестве i-го блока $\boldsymbol{c}_i$, $i = 1, 2, 3, 4$, возьмем слово $\boldsymbol{b}$ кода B_1 с номером $\boldsymbol{c}_i = \boldsymbol{b}(1, a_i + 1, x_i + 1)$ (сложение в действительном поле). Когда $\boldsymbol{a}$ и $\boldsymbol{x}$ пробегают все слова кодов A_1 и A_2, слово $\boldsymbol{c}$ пробегает все слова нового кода C_1. Из такой конструкции следует, что C_1 имеет параметры

$$n = 4 \cdot 4 = 16, \quad N = 16 \cdot 8 = 128, \quad d = \min\{2 \cdot 3, 4 \cdot 2\} = 6.$$

Код C_2 строится аналогично из внешних кодов V_1 и V_2 и внутреннего кода B_2 и имеет такие же параметры. Поясним построение C. При выборе слова $(0\,0\,0\,0)$ используются коды A_1 и A_2, а при выборе слова $(1\,1\,1\,1)$ используются V_1 и V_2.

Теперь наша цель доказать, что C_1 и C_2 находятся друг от друга на расстоянии 6. То, что они находятся на расстоянии 4, следует из того, что код C с кодовым расстоянием 4 (по каскадной конструкции) является объединением кодов C_1 и C_2.

Напомним, что все слова $\boldsymbol{c}$ кода C имеют блочный вид: $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$, где блоки $\boldsymbol{c}_i$ являются словами кода B. Так как кодовые слова внутренних кодов B_1 и B_2 не совпадают, то слова кодов C_1 и C_2 отличаются в каждом блоке, откуда, в частности, следует, что для любых слов $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ из кода C_1 и $\boldsymbol{c}' = (\boldsymbol{c}'_1 \,|\, \boldsymbol{c}'_2 \,|\, \boldsymbol{c}'_3 \,|\, \boldsymbol{c}'_4)$ из кода C_2 справедливо неравенство

$$d(\boldsymbol{c}_i, \boldsymbol{c}'_i) \geqslant 1 \quad \text{для каждого } i \in \{1, 2, 3, 4\}. \tag{6}$$

Разбиения (1), (2) и (4) кодов A_1 и V_1 на подкоды $A_{1,i}$, $i = 1, 2, 3, 4$, и $V_{1,j}$, $j = 1, 2, 3, 4$, соответственно, индуцируют разбиения кодов C_1 и C_2 на подкоды $C_{1,i}$ и $C_{2,j}$. Нужные нам свойства кодов C_1 и C_2 дает следующая

Лемма 1. *Пусть* $\boldsymbol{x} = (\boldsymbol{x}_1 \,|\, \boldsymbol{x}_2 \,|\, \boldsymbol{x}_3 \,|\, \boldsymbol{x}_4)$ – *произвольное слово кода* $C_1 \setminus C_{1,1}$, *а* $\boldsymbol{y} = (\boldsymbol{y}_1 \,|\, \boldsymbol{y}_2 \,|\, \boldsymbol{y}_3 \,|\, \boldsymbol{y}_4)$ – *произвольное слово кода* $C_2 \setminus C_{2,1}$. *Тогда* (*блочные*) *векторы* $\boldsymbol{x}_i$ *и* $\boldsymbol{y}_j$ *обладают следующими свойствами*:

(1) *Если* $\mathrm{wt}(\boldsymbol{x}) = 6$, *то имеется индекс* $i_0 \in \{1, 2, 3, 4\}$, *такой что* $i_0 \in \mathrm{supp}(\boldsymbol{x}_i)$ *для всех ненулевых* $\boldsymbol{x}_i$. *Если же индекс* s *отличен от* i_0, *то он покрыт носителем вектора* $\boldsymbol{x}_i$ *ровно один раз*, *т.е. только для одного* i;

(2) *Если* $\mathrm{wt}(\boldsymbol{x}) = 10$, *то имеется индекс* i_0, *такой что* $i_0 \in \mathrm{supp}(\boldsymbol{x}_i)$ *ровно один раз*, *т.е. только для одного* i. *Каждый индекс* i, *отличный от* i_0, *покрыт носителями* $\boldsymbol{x}_i$ *ровно три раза*;

(3) *Если* $\mathrm{wt}(\boldsymbol{y}) = 6$, *то имеется индекс* $j_0 \in \{1,2,3,4\}$, *который ни разу не покрыт ни одним из носителей* $\boldsymbol{y}_j$. *Все другие индексы* $j \neq j_0$ *покрыты два раза носителями* $\boldsymbol{y}_j$;

(4) *Если* $\mathrm{wt}(\boldsymbol{y}) = 10$, *то имеется индекс* j_0, *который покрыт носителями всех векторов* $\boldsymbol{y}_j$. *Все другие индексы* $j \neq j_0$ *покрыты два раза носителями* $\boldsymbol{y}_j$.

Доказательство непосредственно следует из описания приведенных выше внутренних кодов B_1 и B_2 и обоих внешних кодов A_i и V_i, $i = 1, 2$. ▲

Определим следующие три перестановки π_1, π_2 и π_3, действующие на множестве векторов длины 4: для любого вектора $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$ положим

$$\pi_1(\boldsymbol{x}) = (x_2, x_1, x_4, x_3), \quad \pi_2(\boldsymbol{x}) = (x_4, x_3, x_2, x_1), \quad \pi_3(\boldsymbol{x}) = (x_1, x_4, x_2, x_3).$$

Обозначим через $\mathcal{G}$ группу, порожденную перестановками π_1, π_2 и π_3.

Пусть $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ – произвольное слово кода C_1, построенного на основе кодовых слов $\boldsymbol{a} \in A_1$ и $\boldsymbol{x} \in A_2$, что можно записать в виде $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{x})$. Аналогично будем писать $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{v}, \boldsymbol{y})$ для слова $\boldsymbol{c} \in C_2$, построенного из слов $\boldsymbol{v} \in V_1$ и $\boldsymbol{y} \in V_2$.

Определим действие группы $\mathcal{G}$ на $\boldsymbol{c}$: для любого $g \in \mathcal{G}$ положим

$$g(\boldsymbol{c}) = \begin{cases} \boldsymbol{c}(g(\boldsymbol{a}), g(\boldsymbol{x})), & \text{если } \boldsymbol{c} \in C_1, \\ \boldsymbol{c}(g(\boldsymbol{v}), g(\boldsymbol{y})), & \text{если } \boldsymbol{c} \in C_2. \end{cases}$$

Лемма 2. *Справедливы следующие утверждения*:

(1) *Группа* $\mathcal{G}$ *стабилизирует коды* A_i *и* V_i *для* $i = 1, 2$ *и действует транзитивно на подкодах* $A_1 \setminus A_{1,1}$ *и* $V_1 \setminus V_{1,1}$;

(2) *Группа* $\mathcal{G}$ *стабилизирует коды* C_1 *и* C_2 *и действует транзитивно на подкодах* $C_1 \setminus C_{1,1}$ *и* $C_2 \setminus C_{2,1}$;

(3) *Для любых* $\boldsymbol{c} \in C_1$ *и* $\boldsymbol{c}' \in C_2$ *и для любого* $g \in \mathcal{G}$ *имеет место следующее равенство*:

$$d(g(\boldsymbol{c}), g(\boldsymbol{c}')) = d(\boldsymbol{c}, \boldsymbol{c}'); \tag{7}$$

(4) *Коды* C_1 *и* C_2 *инвариантны относительно сдвига на вектор из всех единиц, т.е.*

$$C_i + (1\,1\,\ldots\,1) = C_i, \quad i = 1, 2. \tag{8}$$

Доказательство. Первые два утверждения следуют непосредственно из таблиц кодовых слов (1), (2) и (4). Так как перестановки не меняют расстояния между векторами, а действие группы является автоморфизмом кодов C_1 и C_2, то получаем утверждение (3). Докажем утверждение (4) сначала для кода C_1. Пусть $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ – произвольное слово этого кода. По построению $\boldsymbol{c}_i = \boldsymbol{b}(1, a_i, x_i)$, где $(a_1\, a_2\, a_3\, a_4)$ – слово кода A_1, а $(x_1\, x_2\, x_3\, x_4)$ принадлежит A_2. Но, как легко видеть из всех его слов,

$$A_2 + (1\,1\,1\,1) = A_2.$$

По построению слово $\boldsymbol{x}$ пробегает весь код A_2. Поэтому для любого $\boldsymbol{x} = (x_1\, x_2\, x_3\, x_4)$ дополнительное к нему слово $\boldsymbol{x} + (1\,1\,1\,1)$ также принадлежит A_2. Следовательно, для любого слова

$$\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$$

дополнительное к нему слово также принадлежит коду C_1. Для кода C_2 доказательство совершенно аналогично, так как код V_2 (участвующий в построении C_2) также инвариантен относительно сдвига на слово из всех единиц. ▲

Теорема 1. *Объединение кодов C_1 и C_2, т.е. код*

$$C = C_1 \cup C_2$$

представляет собой $(16, 256, 6)$-код, т.е. код Нордстрома – Робинсона C является ОКК-кодом третьего порядка.

Доказательство. Чтобы доказать утверждение теоремы, надо доказать, что для любых r и s выполнено следующее условие:

$$d(C_{1,r}, C_{2,s}) \geqslant 6, \quad r, s \in \{1, 2, 3, 4\}. \tag{9}$$

Пусть $\boldsymbol{x}$ и $\boldsymbol{y}$ – произвольные слова кодов $C_{1,r}$ и $C_{2,s}$ соответственно, которые можно представить в следующем блочном виде:

$$\boldsymbol{x} = (\boldsymbol{x}_1 \,|\, \boldsymbol{x}_2 \,|\, \boldsymbol{x}_3 \,|\, \boldsymbol{x}_4),$$
$$\boldsymbol{y} = (\boldsymbol{y}_1 \,|\, \boldsymbol{y}_2 \,|\, \boldsymbol{y}_3 \,|\, \boldsymbol{y}_4),$$

где $\boldsymbol{x}_i \in B_1$ и $\boldsymbol{y}_j \in B_2$. В силу леммы 2 для доказательства достаточно рассмотреть четыре разных случая в зависимости от условий $1 \in \{r, s\}$ или $1 \notin \{r, s\}$.

Случай $(r = 1,\ s = 1)$. В этом случае $\boldsymbol{x}_i$ – это одно слово $\boldsymbol{b}_1$ из подкода B_1 для всех $i \in \{1, 2, 3, 4\}$ или одно слово $\boldsymbol{b}_1$ из подкода B_1 и дополнительное к нему слово $\bar{\boldsymbol{b}}_1$, каждое повторенное два раза, а $\boldsymbol{y}_j$ – одно слово $\boldsymbol{b}_2$ из подкода B_2, повторенное три раза, и дополнительное к нему слово $\bar{\boldsymbol{b}}_2$. Предположим сначала, что $\mathrm{wt}(\boldsymbol{y}) = 6$. Если $\mathrm{supp}(\boldsymbol{b}_2) \not\subset \mathrm{supp}(\boldsymbol{b}_1)$, то и доказывать нечего. Поэтому рассмотрим случай $\mathrm{supp}(\boldsymbol{b}_2) \subset \mathrm{supp}(\boldsymbol{b}_1)$. Пусть сначала $\boldsymbol{b}_1$ встречается четыре раза. Тогда условие $\mathrm{supp}(\boldsymbol{b}_2) \subset \mathrm{supp}(\boldsymbol{b}_1)$ выполняется для трех блоковых векторов $\boldsymbol{y}_j$ веса 1 и не выполнено для четвертого блока, где $\boldsymbol{y}_j$ имеет вес 3, который и даст вклад 3 в расстояние между $\boldsymbol{x}$ и $\boldsymbol{y}$. Если же $\boldsymbol{b}_1$ и $\bar{\boldsymbol{b}}_1$ встречаются по два раза, то вклад 3 в расстояние между векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ даст третий блок веса 1. Пусть теперь $\mathrm{wt}(\boldsymbol{y}) = 10$ и $\mathrm{supp}(\boldsymbol{b}_1) \subset \mathrm{supp}(\boldsymbol{b}_2)$. В этом случае, аналогично предыдущему случаю, блок, в котором $\boldsymbol{y}_j$ имеет вес 1, даст вклад 3 в расстояние между $\boldsymbol{x}$ и $\boldsymbol{y}$. Случаи, когда один или более блоков $\boldsymbol{x}_i$ имеют вес 4, исключаются аналогично.

Случай $(r = 1,\ s = 2, 3, 4)$. В этом случае $\boldsymbol{y}_j$, $j = 1, 2, 3, 4$, – это четыре разных слова из кода B_2, а именно либо три слова веса 1 и слово веса 3, дополнительное к четвертому слову веса 1, либо три разных слова веса 3 и одно слово веса 1, дополнительное к четвертому слову веса 3. Ясно, что в случае, когда единица пробегает три разных позиции в трех блоках $\boldsymbol{y}_j$, а $\boldsymbol{x}_i$ – одно и то же слово $\boldsymbol{b}_1$, встречающееся во всех четырех блоках, то слова $\boldsymbol{x}_i$ и $\boldsymbol{y}_i$ по крайней мере в одном блоке будут на расстоянии 3 друг от друга. Пусть теперь слово $\boldsymbol{b}_1$ (веса 2) встречается в двух блоках $\boldsymbol{x}_i$, в которых оно покрывает два разных слова кода B_2 веса 1, скажем, $\boldsymbol{b}_2(i_1)$ и $\boldsymbol{b}_2(i_2)$. Ясно, что при этом $\bar{\boldsymbol{b}}_1$ покроет вектор $\boldsymbol{b}_2(i_3)$ веса 1 кода B_2 (три блока веса 1 кода B_2 имеют непересекающиеся единицы). Поэтому вклад в расстояние 3 даст четвертый блок (веса 3), где $\boldsymbol{y}$ содержит слово $\bar{\boldsymbol{b}}_2(i_4)$, дополнительное к четвертому слову $\boldsymbol{b}_2(i_4)$ кода B_2. Если же три блока $\boldsymbol{y}_j$ имеют вес 3, то те же аргументы остаются в силе с переходом к дополнительным словам.

Случай $(r = 2, 3, 4,\ s = 1)$. Этот случай совершенно аналогичен предыдущему, и поэтому мы не повторяем доказательство.

Случай $(r = 2, 3, 4, s = 2, 3, 4)$. В этом случае блоковые векторы $\boldsymbol{x}_i$ и $\boldsymbol{y}_j$ пробегают все различные слова кодов A_2 и V_2. Согласно лемме 1 для вектора $\boldsymbol{x}$ имеется индекс $i_0 \in \{1, 2, 3, 4\}$, который покрывается векторами из трех блоков $\boldsymbol{x}$, если $\mathrm{wt}(\boldsymbol{x}) = 6$, и покрывается только одним блоком, если $\mathrm{wt}(\boldsymbol{x}) = 10$. Для слова $\boldsymbol{y}_j$ также имеется индекс $j_0 \in \{1, 2, 3, 4\}$, который не покрывается ни одним из векторов всех четырех блоков $\boldsymbol{y}$, если $\mathrm{wt}(\boldsymbol{y}) = 6$, и покрывается четыре раза, если $\mathrm{wt}(\boldsymbol{y}) = 10$. Поэтому мы

проводим доказательство для двух разных случаев – когда индексы i_0 и j_0 равны и когда они не равны.

Предположим сначала, что для двух произвольных слов $\boldsymbol{x}$ и $\boldsymbol{y}$ индексы i_0 и j_0 совпадают, и пусть $\boldsymbol{x}$ и $\boldsymbol{y}$ имеют оба вес 6. В силу (6) в каждом блоке векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ находятся на расстоянии по крайней мере 1. Позиция с индексом $j_0 = i_0$ не покрыта ни одним блоком $\boldsymbol{y}_j$ веса 1. Нулевому блоку $\boldsymbol{x}_i$ будет соответствовать либо блок $\boldsymbol{y}_i$ веса 3 (и это даст вклад 3 в расстояние между $\boldsymbol{x}$ и $\boldsymbol{y}$), либо блок веса 1 (и тогда вклад 3 даст тот блок, в котором $\boldsymbol{y}_i$ имеет вес 3, так как он не может покрывать элемент 1 в позиции i_0 соответствующего блока $\boldsymbol{x}_i$).

Рассмотрим теперь случай, когда $\mathrm{wt}(\boldsymbol{x}) = 10$, а $\mathrm{wt}(\boldsymbol{y}) = 6$. Для этого случая нам понадобятся используемые нами внешние коды. Выберем произвольное слово $\boldsymbol{x}$ кода C_1, полученное, например, из пары $(0\,3\,2\,1)$ и $(1\,0\,0\,1)$:

$$\begin{array}{l}\boldsymbol{x} = (1\,1\,1\,1|\,1\,0\,0\,1|\,1\,0\,1\,0|\,0\,0\,1\,1),\\ \hline \boldsymbol{y} = (1\,0\,1\,1|\,0\,0\,0\,1|\,1\,0\,0\,0|\,0\,0\,1\,0),\\ \boldsymbol{y}' = (1\,0\,1\,1|\,1\,0\,0\,0|\,0\,0\,1\,0|\,0\,0\,0\,1).\end{array}$$

Легко выписать два единственно возможных вектора $\boldsymbol{y}$ и $\boldsymbol{y}'$ веса 6, которые по своей структуре могут быть кодовыми словами C_2 и которые покрываются кодовым словом $\boldsymbol{x}$, т.е. находятся от него на расстоянии 4. Используя таблицы кодов (1), (2) и (4), заключаем, что векторы $\boldsymbol{y}$ и $\boldsymbol{y}'$ получены из пар $(1\,3\,0\,2)$, $(1\,0\,0\,0)$ и $(1\,0\,2\,3)$, $(1\,0\,0\,0)$ соответственно. Но оба вектора $(1\,3\,0\,2)$ и $(1\,0\,2\,3)$ не принадлежат коду V_1, а значит, $\boldsymbol{y}$ и $\boldsymbol{y}'$ не принадлежат коду C_2.

Следующие два случая, когда $\mathrm{wt}(\boldsymbol{x}) = 6$, а $\mathrm{wt}(\boldsymbol{y}) = 10$, и когда $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 10$, доказывать не надо, так как они вытекают из двух предыдущих случаев ($\mathrm{wt}(\boldsymbol{x}) = 10$, $\mathrm{wt}(\boldsymbol{y}) = 6$ и $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 6$) в силу инвариантности обоих кодов C_1 и C_2 относительно сдвига на слово из всех единиц (лемма 2). Действительно, пусть, например, для случая $\mathrm{wt}(\boldsymbol{x}) = 6$, а $\mathrm{wt}(\boldsymbol{y}) = 10$ мы нашли два вектора $\boldsymbol{x}$ и $\boldsymbol{y}$ с меньшим расстоянием $d(\boldsymbol{x}, \boldsymbol{y}) \leqslant 5$. Тогда на этом же расстоянии будут находиться дополнительные к ним векторы $\boldsymbol{x} + (1\,1\,\ldots\,1)$ и $\boldsymbol{y} + (1\,1\,\ldots\,1)$, что противоречит уже доказанному случаю.

Рассмотрим теперь случай, когда индексы векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ не равны: $i_0 \neq j_0$. Доказательство проводится совершенно аналогично, и мы рассмотрим только два случая – когда $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 6$ и когда $\mathrm{wt}(\boldsymbol{x}) = 6$ и $\mathrm{wt}(\boldsymbol{y}) = 10$.

Пусть сначала $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 6$. Выберем произвольное слово $\boldsymbol{x}$ кода C_1, например (индекс $\boldsymbol{x}$ равен $i_0 = 1$),

$$\begin{array}{l}\boldsymbol{x} = (0\,0\,0\,0|\,1\,0\,0\,1|\,1\,0\,1\,0|\,1\,1\,0\,0),\\ \hline \boldsymbol{y} = (0\,1\,0\,0|\,0\,0\,0\,1|\,1\,0\,0\,0|\,1\,1\,0\,1),\\ \boldsymbol{y}' = (0\,0\,0\,1|\,1\,1\,0\,1|\,1\,0\,0\,0|\,0\,1\,0\,0).\end{array}$$

Выпишем два единственно возможных вектора $\boldsymbol{y}$ и $\boldsymbol{y}'$ веса 6 с индексом $j_0 = 3$, которые могут быть кодовыми словами C_2 и которые находятся от $\boldsymbol{x}$ на расстоянии 4. На основе таблиц кодов снова выясняем, что векторы $\boldsymbol{y}$ и $\boldsymbol{y}'$ получены из пар $(1\,3\,0\,2)$, $(0\,0\,0\,1)$ и $(3\,2\,0\,1)$, $(0\,1\,0\,0)$ соответственно. Но $(1\,3\,0\,2)$ и $(3\,2\,0\,1)$ не принадлежат коду V_1, а значит, $\boldsymbol{y}$ и $\boldsymbol{y}'$ не принадлежат коду C_2. Оставшиеся два случая значения индекса $j_0 \in \{2, 4\}$ вектора $\boldsymbol{y}$ исключаются совершенно аналогично.

Пусть теперь $\mathrm{wt}(\boldsymbol{x}) = 6$ и $\mathrm{wt}(\boldsymbol{y}) = 10$. Выберем произвольное слово $\boldsymbol{x}$ кода C_1, например (индекс $\boldsymbol{x}$ равен $i_0 = 1$),

$$\begin{array}{l}\boldsymbol{x} = (0\,0\,0\,0|\,1\,0\,0\,1|\,1\,0\,1\,0|\,1\,1\,0\,0),\\ \hline \boldsymbol{y} = (0\,0\,0\,1|\,1 * \bar{*}1|\,1\,0\,1\,1|\,1\,1\,0\,1).\end{array}$$

Предположим, что индекс $\boldsymbol{y}$ равен $j_0 = 4$. Это означает, что каждый из трех блоков $\boldsymbol{y}_j$ веса 3 должен покрывать позицию с индексом $j_0 = 4$, и кроме того, две ненулевые позиции блоков $\boldsymbol{x}_i$. Легко убедиться, что это сделать невозможно. Действительно, в приведенном выше векторе $\boldsymbol{y}$ блок $\boldsymbol{y}_2$ не может быть достроен до веса 3 (в каждом из двух возможных случаев получим блоковый вектор $\boldsymbol{y}_2$, совпадающий с одним из блоковых векторов $\boldsymbol{y}_3$ или $\boldsymbol{y}_4$). Два оставшихся значения индекса $j_0 \in \{2, 3\}$ исключаются аналогично.

Чтобы завершить доказательство теоремы, напомним лемму 2, согласно которой коды инвариантны относительно действия группы $\mathcal{G}$. Это обосновывает наш выбор только одного вектора $\boldsymbol{x}$. Выбрав другой вектор $\boldsymbol{x}'$, мы получим такое же число возможных претендентов векторов на слова кода C_2, находящихся на расстоянии 4 от $\boldsymbol{x}$. Действительно, предположим, что для $\boldsymbol{x}'$ нашлось три претендента $\boldsymbol{y}$, $\boldsymbol{y}'$ и $\boldsymbol{y}''$ на слова кода C_2, находящихся на расстоянии 4 от $\boldsymbol{x}'$. Пусть $g \in \mathcal{G}_2$ переводит $\boldsymbol{x}'$ в $\boldsymbol{x}$, т.е. $g(\boldsymbol{x}') = \boldsymbol{x}$. При этом (по лемме 2) g переводит все векторы $\boldsymbol{y}$, $\boldsymbol{y}'$ и $\boldsymbol{y}''$ в векторы, находящиеся на расстоянии 4 от $\boldsymbol{x}$, которые также являются претендентами на слова кода C_2. Таким образом, приходим к противоречию, так как слову $\boldsymbol{x}$ соответствуют только два претендента. Это завершает доказательство теоремы. ▲

§ 3. Построение двоичного кода Голея

Построение двоичного расширенного $[24, 12, 8]$-кода Голея аналогично предыдущей конструкции кода Нордстрома – Робинсона. В качестве внутреннего кода берется тот же $[4, 4, 1]$-код B с таким же разбиением на $[4, 3, 2]$-подкоды: $[4, 3, 2]$-код B_0 (с проверкой на четность) и $(4, 8, 2)$-код B_1 (с проверкой на нечетность). При этом мы изменим следующим образом нумерацию их слов, чтобы линеаризовать отображение из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_0 (что нам нужно для доказательства линейности результирующего кода):

$$B_{0,0} = \{\boldsymbol{b}(0,0,0) = (0\,0\,0\,0),\ \boldsymbol{b}(0,0,1) = (1\,1\,1\,1)\},$$
$$B_{0,1} = \{\boldsymbol{b}(0,1,0) = (1\,1\,0\,0),\ \boldsymbol{b}(0,1,1) = (0\,0\,1\,1)\},$$
$$B_{0,2} = \{\boldsymbol{b}(0,2,0) = (1\,0\,1\,0),\ \boldsymbol{b}(0,2,1) = (0\,1\,0\,1)\},$$
$$B_{0,3} = \{\boldsymbol{b}(0,3,0) = (0\,1\,1\,0),\ \boldsymbol{b}(0,3,1) = (1\,0\,0\,1)\}.$$

Для кода B_1 нумерация имеет следующий вид:

$$B_{1,0} = \{\boldsymbol{b}(1,0,0) = (1\,0\,0\,0),\ \boldsymbol{b}(1,0,1) = (0\,1\,1\,1)\},$$
$$B_{1,1} = \{\boldsymbol{b}(1,1,0) = (0\,1\,0\,0),\ \boldsymbol{b}(1,1,1) = (1\,0\,1\,1)\},$$
$$B_{1,2} = \{\boldsymbol{b}(1,2,0) = (0\,0\,1\,0),\ \boldsymbol{b}(1,2,1) = (1\,1\,0\,1)\},$$
$$B_{1,3} = \{\boldsymbol{b}(1,3,0) = (0\,0\,0\,1),\ \boldsymbol{b}(1,3,1) = (1\,1\,1\,0)\}.$$

Определим внешние коды: $A = \{(0\,0\,0\,0\,0\,0),\ (1\,1\,1\,1\,1\,1)\}$ и $[6, 3, 4]_4$-код A_1 над $\mathbb{F}_4$, а также двоичные коды: $[6, 5, 2]$-код A_2 с проверкой на четность и $(6, 32, 2)$-код V_2 с проверкой на нечетность.

Поясним построение $[6, 3, 4]_4$-кода A_1 над $\mathbb{F}_4$. Пусть

$$\mathbb{F}_4 = \{0, 1, \xi, \xi^2\}, \quad \text{где } \xi^2 + \xi + 1 = 0,$$

и пусть $\mathbb{F}_{4^2}$ получено из $\mathbb{F}_4$ с помощью примитивного многочлена

$$f(x) = x^2 + x + \xi.$$

Пусть α – корень этого многочлена, т.е. примитивный элемент поля $\mathbb{F}_{4^2}$. Всюду далее в качестве элементов $0, 1, \xi, \xi^2$ поля $\mathbb{F}_4$ мы для удобства используем элементы

$0, 1, 2, 3$ соответственно, которыми нумеруются слова внутренних кодов. Обозначим через $m_i(x)$ минимальную функцию элемента α^i. Так как

$$x^5 + 1 = (x^2 + 3x + 1)(x^2 + 2x + 1)(x + 1), \tag{10}$$

то можно определить следующий циклический $[5, 3, 3]_4$-МДР-код C, имеющий порождающий многочлен

$$g_a(x) = m_3(x) = x^2 + 3x + 1.$$

Обозначим через A_1 код, полученный из C расширением, т.е. добавлением к каждому кодовому слову $\boldsymbol{a}' = (a_1, a_2, a_3, a_4, a_5)$ кода C еще одной позиции a_6 общей проверки:

$$a_6 = \sum_{i=1}^{5} a_i.$$

При этом получаем $[6, 3, 4]_4$-код A_1, образованный словами $\boldsymbol{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$. Этот код удобно описать с помощью следующих пяти кодовых слов (генераторов):

$$(1\,1\,1\,1\,1\,|\,1), \quad (2\,1\,2\,0\,0\,|\,1), \quad (3\,3\,0\,1\,0\,|\,1), \quad (1\,2\,2\,1\,0\,|\,0), \quad (1\,2\,3\,2\,1\,|\,3). \tag{11}$$

Первый генератор в (11) порождает, очевидно, три кодовых слова. Каждый из четырех остальных генераторов порождает 15 кодовых слов умножением на скаляр (т.е. на ξ и ξ^2) и пятью циклическими сдвигами. Если $\boldsymbol{a} = (a_1, a_2, a_3, a_4, a_5\,|\,a_6)$ – один из таких генераторов, то 15 соответствующих кодовых слов порождаются циклическими сдвигами (первых пяти позиций, позиция же a_6 остается неподвижной) трех векторов $\boldsymbol{a}$, $\xi\boldsymbol{a}$ и $\xi^2\boldsymbol{a}$.

Для удобства читателя приведем все слова кода A_1:

(000000)	(111111)	(222222)	(333333),
(212001)	(330101)	(122100)	(123213),
(021201)	(033011)	(012210)	(112323),
(002121)	(103301)	(101220)	(211233),
(200211)	(010331)	(210120)	(321123),
(120021)	(301031)	(221010)	(232113),
(323002)	(110202)	(233200)	(231321),
(032302)	(011022)	(023320)	(223131),
(003232)	(201102)	(202330)	(322311),
(300322)	(020112)	(320230)	(132231),
(230032)	(102012)	(332020)	(313221),
(131003)	(220303)	(311300)	(312132),
(013103)	(022033)	(031130)	(331212),
(001313)	(302203)	(303110)	(133122),
(100133)	(030223)	(130310)	(213312),
(310013)	(203023)	(113030)	(121332).

Строим три ОКК-кода:

- код G (порядка 3) на основе внутреннего кода B и внешних кодов A, A_1 и $A_2 \cup V_2$ (при выборе слова $(0\,0\,0\,0\,0\,0)$ используется A_2, а при выборе $(1\,1\,1\,1\,1\,1)$ используется V_2);
- код G_1 (порядка 2) на основе внутреннего кода B_0 и двух внешних кодов A_1 и A_2;
- код G_2 (порядка 2) на основе внутреннего кода B_1 и двух внешних кодов A_1 и V_2.

Отображение из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_0 обозначим через φ_0, а в слова кода B_1 – через φ_1:

$$\varphi_i(j,k) = \boldsymbol{b}(i,j,k), \quad i = 0,1.$$

Доопределим естественным образом эти отображения на векторы $\boldsymbol{x} = (x_1, \ldots, x_n)$ над $\mathbb{F}_4 \times \mathbb{F}_2$:

$$\varphi_i(\boldsymbol{x}) = (\varphi_i(x_1), \varphi_i(x_2), \ldots, \varphi_i(x_n)), \quad i = 0,1.$$

Лемма 3. *Справедливы следующие утверждения*:

(1) *Отображение φ_0 из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_0 линейно по обоим индексам, т.е. если $\boldsymbol{b}'$ и $\boldsymbol{b}''$ – слова кода B_0 с номерами $(0,j',k')$ и $(0,j'',k'')$ соответственно, то их сумма $\boldsymbol{b} = \boldsymbol{b}' + \boldsymbol{b}''$ имеет номер*

$$(i,j,k) = (0, j' + j'', k' + k''),$$

где индексы j' и j'' суммируются в поле $\mathbb{F}_4$ (с учетом введенных нами обозначений элементов поля $\mathbb{F}_4$), а индексы k' и k'' – в поле $\mathbb{F}_2$;

(2) *Отображение φ_1 из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_1 линейно по первому индексу, а также линейно по второму с поправочным коэффициентом $k_3 \in \{0,1\}$ (в зависимости от четности числа появлений элемента 3 в множестве $\{j', j''\}$), т.е. если $\boldsymbol{b}'$ и $\boldsymbol{b}''$ – слова кода B_1 с номерами $(1,j',k')$ и $(1,j'',k'')$ соответственно, то их сумма $\boldsymbol{b} = \boldsymbol{b}' + \boldsymbol{b}''$ принадлежит коду B_0 и вектор $\boldsymbol{b}$ имеет номер*

$$(i,j,k) = (0, j' + j'', k' + k'' + k_3),$$

где k_3 – число появлений элемента 3 в множестве $\{j', j''\}$, взятое по модулю 2 и интерпретируемое как элемент поля $\mathbb{F}_2$.

Доказательство. Непосредственная проверка сложения номеров слов кодов B_0 и B_1, которое индуцируется сложением двоичных векторов длины 4. ▲

Лемма 4. *Справедливы следующие утверждения*:

(1) *Коды G_1 и G_2 имеют кодовое расстояние 8, причем $\mathrm{wt}(\boldsymbol{g}) \geqslant 8$ для любого слова $\boldsymbol{g}$ из G_2;*

(2) *Код G_1 является линейным кодом, т.е. $[24, 11, 8]$-кодом;*

(3) *Код G_2 инвариантен относительно сдвига на любое слово кода G_1.*

Доказательство. (1) Минимальные расстояния d_1 и d_2 кодов G_1 и G_2 следуют из обобщенной каскадной конструкции [14]:

$$d_1 = d_2 = \min\{2 \cdot 4, 4 \cdot 2\} = 8.$$

(2) Линейность кода G_1 следует из линейности кодов A_1 и A_2 и линейности отображения φ_0 (лемма 3).

(3) Заметим следующий очевидный факт: *множество всех двоичных векторов нечетного веса длины n инвариантно относительно сдвига на любой двоичный вектор четного веса длины n*. Поэтому код B_1 инвариантен относительно сдвига на любое слово кода B_0, а код V_2 инвариантен относительно сдвига на любое слово кода A_2. Следовательно, для любого слова $\boldsymbol{g} = \varphi_0(\boldsymbol{a}, \boldsymbol{b})$ кода G_1, $\boldsymbol{a} \in A_1$, $\boldsymbol{b} \in A_2$, получаем

$$\begin{aligned}
&\boldsymbol{g} + G_2 = \varphi_0(\boldsymbol{a}, \boldsymbol{b}) + \{\varphi_1(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \in A_1,\ \boldsymbol{y} \in V_2\} = \\
&= \{\varphi_1(\boldsymbol{x} + \boldsymbol{a}, \boldsymbol{y} + \boldsymbol{b}) : \boldsymbol{x} \in A_1,\ \boldsymbol{y} \in V_2\} = \\
&= \{\varphi_1(\boldsymbol{x}', \boldsymbol{y}') : \boldsymbol{x}' \in A_1,\ \boldsymbol{y}' \in V_2\} = G_2. \quad ▲
\end{aligned}$$

Лемма 5. *Коды G_1 и G_2 находятся друг от друга на расстоянии 8.*

Доказательство. Согласно лемме 4 код G_2 инвариантен относительно сдвига на любое слово кода G_1. Ясно, что условие $d(G_1, G_2) \leqslant 7$ означает, что $d(\boldsymbol{g}, G_2) \leqslant 7$ для некоторого слова $\boldsymbol{g} \in G_1$. Но это неравенство противоречит лемме 4, согласно которой код G_2 инвариантен относительно сдвига на любое слово кода G_1, и поэтому должно выполняться неравенство $d(\boldsymbol{g}, G_2) = 8$. ▲

На самом деле, мы уже доказали, что объединение кодов G_1 и G_2 является двоичным кодом Голея, так как известно [5], что любой двоичный код с параметрами $n = 24$, $N = 2^{12}$, $d = 8$ является кодом Голея. Тем не менее мы приведем второе доказательство этого факта через линейность кода.

Лемма 6. *Код G_2 является смежным классом кода G_1.*

Доказательство. Согласно лемме 4 имеем $\boldsymbol{g} + G_2 = G_2$ для любого $\boldsymbol{g} \in G_1$. Это равенство означает, что $\boldsymbol{g} + \boldsymbol{g}_1 = \boldsymbol{g}_2$ для любого $\boldsymbol{g}_1 \in G_2$, где $\boldsymbol{g}_2 \in G_2$, откуда и следует утверждение. ▲

Итак, доказана следующая

Теорема 2. *Объединение кодов G_1 и G_2, т.е. код*

$$G = G_1 \cup G_2$$

представляет собой $(24, 2^{12}, 8)$-код, т.е. ОКК-код третьего порядка G представляет собой двоичный расширенный совершенный $[24, 12, 8]$-код Голея.

Авторы благодарны Д. Кротову за стимулирующую беседу относительно ОКК-конструкции кода Нордстрома – Робинсона, результатом которой и является данная статья, а также рецензенту за полезные замечания, которыми мы воспользовались при подготовке окончательного варианта статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Nordstrom A.W., Robinson J.P.* An Optimum Nonlinear Code // Inform. Control. 1967. V. 11. № 5–6. P. 613–616. https://doi.org/10.1016/S0019-9958(67)90835-2
2. *Семаков Н.В., Зиновьев В.А.* Совершенные и квазисовершенные равновесные коды // Пробл. передачи информ. 1969. Т. 5. № 2. С. 14–18. http://mi.mathnet.ru/ppi1794
3. *Golay M.J.E.* Notes on Digital Coding // Proc. IRE. 1949. V. 37. P. 657. https://doi.org/10.1109/JRPROC.1949.233620
4. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. *Snover S.L.* The Uniqueness of the Nordstrom–Robinson and the Golay Binary Codes. Ph.D. Thesis. Dept. of Mathematics, Michigan State Univ., 1973. https://doi.org/10.25335/M56D5PM3R
6. *Preparata F.P.* A Class of Optimum Nonlinear Double-Error-Correcting Codes // Inform. Control. 1968. V. 13. № 4. P. 378–400. https://doi.org/10.1016/S0019-9958(68)90874-7
7. *Kerdock A.M.* A Class of Low-Rate Nonlinear Binary Codes // Inform. Control. 1972. V. 20. № 2. P. 182–187. https://doi.org/10.1016/S0019-9958(72)90376-2
8. *Vardy A.* The Nordstrom–Robinson Code: Representation over $GF(4)$ and Efficient Decoding // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 1686–1693. https://doi.org/10.1109/18.333895
9. *Forney G.D., Jr., Sloane N.J.A., Trott M.D.* The Nordstrom–Robinson Code Is the Binary Image of the Octacode // Coding and Quantization (Proc. DIMACS/IEEE Workshop. Princeton Univ., NJ, USA. Oct. 19–21, 1992). Providence, RI: Amer. Math. Soc., 1993. P. 19–26.
10. *Bierbrauer J.* Nordstrom–Robinson Code and A_7-Geometry // Finite Fields Appl. 2007. V. 13. № 1. P. 158–170. https://doi.org/10.1016/j.ffa.2005.05.004

11. *Могильных И.Ю.* О продолжении пропелинейных структур кода Нордстрома – Робинсона на код Хэмминга // Пробл. передачи информ. 2016. Т. 52. № 3. С. 97–107. http://mi.mathnet.ru/ppi2215
12. *Gillespie N.I., Praeger C.E.* New Characterisations of the Nordstrom–Robinson Codes // Bull. London Math. Soc. 2017. V. 49. № 2. P. 320–330. https://doi.org/10.1112/blms.12016
13. *Думер И.И., Зиновьев В.А.* Некоторые новые максимальные коды над полем Галуа $GF(4)$ // Пробл. передачи информ. 1978. Т. 14. № 3. С. 24–34. http://mi.mathnet.ru/ppi1543
14. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670

Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
20.12.2020
После доработки
17.11.2021
Принята к публикации
17.11.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391.1 : 519.725

© 2021 г. **Н.А. Полянский**

О СПИСОЧНОМ ДЕКОДИРОВАНИИ НЕКОТОРЫХ $\mathbb{F}_q$-ЛИНЕЙНЫХ КОДОВ[1]

Представлен алгоритм списочного декодирования $\mathbb{F}_q$-линейных кодов, обобщающих s-коды Рида – Соломона.

Ключевые слова: списочное декодирование, s-коды Рида – Соломона, минимальное расстояние.

DOI: 10.31857/S0555292321040045

§ 1. Обозначения, определения и вспомогательные результаты

Множество натуральных чисел обозначим символом $\mathbb{N}$, причем будем считать, что $0 \in \mathbb{N}$. Множество последовательных целых чисел $\{i, i+1, \ldots, j\}$ для некоторых $i, j \in \mathbb{N}$, $i \leqslant j$, будем обозначать через $[i, j]$. Для множества $[1, j]$ будем использовать сокращение $[j]$. Для обозначения векторов будем использовать полужирные символы, например, $\boldsymbol{x}$, а i-ю координату вектора $\boldsymbol{x}$ будем записывать в виде x_i. Для векторов $\boldsymbol{i} = (i_1, \ldots, i_m)$ и $\boldsymbol{j} = (j_1, \ldots, j_m)$ из $\mathbb{N}^m$ определим естественное отношение частичного порядка: $\boldsymbol{i} \leqslant \boldsymbol{j}$, если выполнено $i_k \leqslant j_k$ для всех $k \in [m]$. Через $\binom{\boldsymbol{i}+\boldsymbol{j}}{\boldsymbol{i}}$ для некоторых $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}^m$ будем обозначать произведение $\prod\limits_{k=1}^{m} \binom{i_k + j_k}{i_k}$. Запись $\max\{i_1, \ldots, i_m\}$ обозначает максимум из чисел $i_1, \ldots, i_m$. *Кодом* $\mathcal{C}$ длины n над алфавитом $\mathcal{A}$ будем называть произвольное подмножество множества $\mathcal{A}^n$, т.е. $\mathcal{C} \subseteq \mathcal{A}^n$. Через $|A|$ будем обозначать мощность множества A, например, объем кода равен $|\mathcal{C}|$. *Расстояние Хэмминга* между двумя векторами $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{A}^n$ определим как $d_H(\boldsymbol{x}, \boldsymbol{y}) := |\{i : x_i \neq y_i\}|$. *Минимальное расстояние* в коде $\mathcal{C}$ равно минимуму величины $d_H(\boldsymbol{x}, \boldsymbol{y})$ по всем $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$, $\boldsymbol{x} \neq \boldsymbol{y}$.

В настоящей статье будем рассматривать лишь конечные поля $\mathbb{F}_q$ с характеристикой p, т.е. $q = p^c$ для некоторого $c \in \mathbb{N} \setminus \{0\}$ и простого числа p. Мультипликативную группу поля $\mathbb{F}_q$ будем обозначать через $\mathbb{F}_q^*$. Символом $\mathbf{0}$ будем обозначать вектор из всех нулей, длина которого будет ясна из контекста. Будем использовать прописные символы для обозначения переменных, например, T или $\boldsymbol{X} = (X_1, \ldots, X_m)$. В ходе рассуждений число переменных m будет чаще всего фиксировано. Обозначим через $\mathbb{F}_q[\boldsymbol{X}]$ кольцо многочленов от m переменных $X_1, \ldots, X_m$ над полем $\mathbb{F}_q$. Для вектора $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$ моном $\boldsymbol{X}^{\boldsymbol{v}} \in \mathbb{F}_q[\boldsymbol{X}]$ определяется как $\prod\limits_{j=1}^{m} X_j^{v_j}$. Для многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ и вектора $\boldsymbol{i} \in \mathbb{N}^m$ будем обозначать через $[\boldsymbol{X}^{\boldsymbol{i}}]f(\boldsymbol{X})$ коэффициент перед $\boldsymbol{X}^{\boldsymbol{i}}$ в записи $f(\boldsymbol{X})$. Для вектора $\boldsymbol{x}_0 \in \mathbb{F}_q^m$ значение многочлена $f(\boldsymbol{X})$ в точке $\boldsymbol{x}_0$ будем записывать в виде $f(\boldsymbol{x}_0)$, где $f(\boldsymbol{x}_0) \in \mathbb{F}_q$. Пусть $\boldsymbol{X} = (X_1, \ldots, X_m)$

[1] Работа выполнена в Сколковском институте науки и технологий при поддержке гранта Российского научного фонда (номер проекта 19-71-00137).

и $\boldsymbol{Y} = (Y_1, \ldots, Y_k)$. Тогда для многочлена $f(\boldsymbol{X}, \boldsymbol{Y})$ из $\mathbb{F}_q[\boldsymbol{X}, \boldsymbol{Y}]$ через $\{\boldsymbol{Y}^{\boldsymbol{i}}\}f(\boldsymbol{X}, \boldsymbol{Y})$ будем обозначать многочлен из $\mathbb{F}_q[\boldsymbol{X}]$, определяемый равенством

$$\{\boldsymbol{Y}^{\boldsymbol{i}}\}f(\boldsymbol{X}, \boldsymbol{Y}) := \sum_{\boldsymbol{j} \in \mathbb{N}^m} \big([\boldsymbol{X}^{\boldsymbol{j}}\boldsymbol{Y}^{\boldsymbol{i}}]f(\boldsymbol{X}, \boldsymbol{Y})\big)\boldsymbol{X}^{\boldsymbol{j}}.$$

1.1. Производная Хассе и эквивалентные многочлены.

Определение 1. Пусть $\boldsymbol{X} = (X_1, \ldots, X_m)$ и $\boldsymbol{Y} = (Y_1, \ldots, Y_m)$. Для вектора $\boldsymbol{i} \in \mathbb{N}^m$ определим *$\boldsymbol{i}$-ю производную Хассе* многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ как $\boldsymbol{i}$-й коэффициент "сдвинутого" многочлена $\widetilde{f}(\boldsymbol{X}, \boldsymbol{Y}) := f(\boldsymbol{X} + \boldsymbol{Y})$, т.е.

$$f^{(\boldsymbol{i})}(\boldsymbol{X}) := \{\boldsymbol{Y}^{\boldsymbol{i}}\}\widetilde{f}(\boldsymbol{X}, \boldsymbol{Y}).$$

Иногда для удобства будем использовать эквивалентное обозначение $D^{(\boldsymbol{i})}f(\boldsymbol{X}) := f^{(\boldsymbol{i})}(\boldsymbol{X})$. Таким образом, выполнено соотношение

$$f(\boldsymbol{X} + \boldsymbol{Y}) = \sum_{\boldsymbol{i} \in \mathbb{N}^m} f^{(\boldsymbol{i})}(\boldsymbol{X})\boldsymbol{Y}^{\boldsymbol{i}}.$$

Отметим несколько свойств производной Хассе, доказательство которых можно найти в [1].

Предложение 1. *Пусть* $f(\boldsymbol{X}), g(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$, $\lambda \in \mathbb{F}_q$, *и пусть* $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}^m$. *Тогда справедливы следующие соотношения*:

1. $f^{(\boldsymbol{i})}(\boldsymbol{X}) + g^{(\boldsymbol{i})}(\boldsymbol{X}) = (f + g)^{(\boldsymbol{i})}(\boldsymbol{X})$;
2. $(\lambda f)^{(\boldsymbol{i})}(\boldsymbol{X}) = \lambda f^{(\boldsymbol{i})}(\boldsymbol{X})$;
3. $(fg)^{(\boldsymbol{i})}(\boldsymbol{X}) = \sum\limits_{\boldsymbol{0} \leqslant \boldsymbol{e} \leqslant \boldsymbol{i}} f^{(\boldsymbol{e})}(\boldsymbol{X})g^{(\boldsymbol{i}-\boldsymbol{e})}(\boldsymbol{X})$;
4. $(f^{(\boldsymbol{i})})^{(\boldsymbol{j})}(\boldsymbol{X}) = \binom{\boldsymbol{i}+\boldsymbol{j}}{\boldsymbol{i}} f^{(\boldsymbol{i}+\boldsymbol{j})}(\boldsymbol{X})$.

Определим функцию

$$\deg\colon \mathbb{N}^m \to \mathbb{N}, \quad \deg(\boldsymbol{v}) = \sum_{j=1}^{m} v_j,$$

и функцию

$$\deg_q\colon \mathbb{N}^m \to \mathbb{N}, \quad \deg_q(\boldsymbol{v}) = \sum_{j=1}^{m} \lfloor v_j/q \rfloor.$$

Степень $\deg(f(\boldsymbol{X}))$ многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ определим как максимальное значение $\deg(\boldsymbol{i})$ для вектора $\boldsymbol{i} \in \mathbb{N}^m$, такого что $[\boldsymbol{X}^{\boldsymbol{i}}]f(\boldsymbol{X}) \neq 0$. Следующее утверждение напрямую вытекает из [2, следствие 6.50].

Предложение 2. *Для произвольного числа* $s \in [q-1]$ *определим многочлен от одной переменной* $f(T) := (T^q - T)^s \in \mathbb{F}_q[T]$. *Тогда*

$$f^{(i)}(T) = \begin{cases} (-1)^i \binom{s}{i} (T^q - T)^{s-i} & \text{для } 0 \leqslant i \leqslant s, \\ 0 & \text{для } i > s. \end{cases}$$

Через $f^{(<s)}(\boldsymbol{x}_0) \in \mathbb{F}_q^{\binom{s+m-1}{m}}$ будем обозначать вектор, $\boldsymbol{i}$-я компонента которого равна $f^{(\boldsymbol{i})}(\boldsymbol{x}_0)$ для всех $\boldsymbol{i} \in \mathbb{N}^m$, $\deg(\boldsymbol{i}) < s$.

Определение 2. Два многочлена $f(\boldsymbol{X}), g(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ назовем *s-эквивалентными*, если $f^{(<s)}(\boldsymbol{x}_0) = g^{(<s)}(\boldsymbol{x}_0)$ для всех $\boldsymbol{x}_0 \in \mathbb{F}_q^m$. В таком случае будем также писать $f(\boldsymbol{X}) \equiv_s g(\boldsymbol{X})$.

Доказательства следующего и некоторых последующих утверждений, для которых не указаны ссылки на работы, содержащие доказательства, приведены в § 3.

Предложение 3. *Пусть q – степень простого числа p, и пусть $s \in [q-1]$. Тогда для всякого многочлена от одной переменной $f(T) \in \mathbb{F}_q[T]$ существует единственный многочлен $g(T) \in \mathbb{F}_q[T]$ степени не выше $sq-1$, такой что $f(T) \equiv_s g(T)$. Если s также является степенью p, то*

$$f(T) \equiv g(T) \pmod{T^{qs} + (-T)^s}.$$

В дальнейшем чаще всего будем предполагать, что s является степенью p. Это позволит существенным образом упростить анализ ввиду предложения 3. Определим функцию $\mathrm{Mod}_q^s \colon \mathbb{N} \to [0, qs-1]$ по следующему правилу:

- если $a < s$, то $\mathrm{Mod}_q^s(a) = a$;
- если $a \geqslant s$ и $a \equiv b \pmod{qs-s}$, $b \in [s, qs-1]$, то $\mathrm{Mod}_q^s(a) = b$.

Эта функция имеет смысл благодаря следующему наблюдению. Если s является степенью p, то

$$T^a \equiv_s (-1)^t T^{\mathrm{Mod}_q^s(a)}, \tag{1}$$

где $t = \dfrac{a - \mathrm{Mod}_q^s(a)}{qs-s}$.

1.2. Хорошие мономы и обобщение s-кодов Рида – Соломона. Определим отношение частичного порядка $\leqslant_p$ на множествах $\mathbb{N}$ и $\mathbb{N}^m$ для некоторого простого числа p.

Определение 3. Возьмем целые числа $n, k \in \mathbb{N}$, простое число p и положим $t := \lfloor \log_p(\max\{n,k\}) \rfloor$. Рассмотрим p-ичные представления чисел $n = \sum\limits_{i=0}^{t} n^{(i)} p^i$ и $k = \sum\limits_{i=0}^{t} k^{(i)} p^i$. Определим следующий порядок: $k \leqslant_p n$, если $k^{(i)} \leqslant n^{(i)}$ для всех $i \in [0,t]$. Для вектора $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$ будем писать $\boldsymbol{v} \leqslant_p n$, если $v_j \leqslant_p n$ для всех $j \in [m]$. Для двух векторов одной длины $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{N}^m$ определим порядок $\boldsymbol{v} \leqslant_p \boldsymbol{w}$, если выполнено $v_j \leqslant_p w_j$ для всех $j \in [m]$.

Следующий результат, доказанный в [3], поясняет удобство использования вышеуказанного частичного порядка.

Предложение 4. *Пусть даны целые числа $n > 0$, $k \geqslant 0$, $k \leqslant n$, и простое число p. Определим $t := \lfloor \log_p(n) \rfloor$ и рассмотрим p-ичные представления чисел $n = \sum\limits_{i=0}^{t} n^{(i)} p^i$ и $k = \sum\limits_{i=0}^{t} k^{(i)} p^i$. Тогда для биномиального коэффициента справедливо соотношение*

$$\binom{n}{k} \equiv \prod_{i=0}^{t} \binom{n^{(i)}}{k^{(i)}} \pmod{p}.$$

В частности, равенство $\binom{n}{k} \equiv 0 \pmod{p}$ выполнено в том и только том случае, когда существует хотя бы один индекс $i \in [0,t]$, для которого $k^{(i)} > n^{(i)}$. Другими словами, соотношение $\binom{n}{k} \not\equiv 0 \pmod{p}$ верно тогда и только тогда, когда $k \leqslant_p n$.

Следствие 1. *Пусть даны целые числа* $n, k_j \in \mathbb{N}$, $j \in [m]$, $\sum\limits_{j=1}^{m} k_j = n$, *и простое число* p. *Тогда соответствующий мультиномиальный коэффициент не равен нулю,* $\binom{n}{k_1, \ldots, k_m} \not\equiv 0 \pmod{p}$, *тогда и только тогда, когда отношение порядка* $k_j \leqslant_p n$ *справедливо для всех* $j \in [m]$.

Определение 4. Пусть q и s являются степенью простого p, $s < q$, и пусть даны числа $m \geqslant 1$ и $d \in [sq]$. Будем говорить, что моном $\boldsymbol{X}^{\boldsymbol{v}} \in \mathbb{F}_q[\boldsymbol{X}]$, где $\boldsymbol{v} \in \mathbb{N}^m$, является $(m,d)_q^s$-*хорошим*, если выполнены следующие два условия:

1. $\deg_q(\boldsymbol{v}) \leqslant s-1$;
2. для всякого $\boldsymbol{i} \in \mathbb{N}^m$, такого что $\boldsymbol{i} \leqslant_p \boldsymbol{v}$, выполнено неравенство $\mathrm{Mod}_q^s(\deg(\boldsymbol{i})) < d$.

Заметим, что все мономы $\boldsymbol{X}^{\boldsymbol{v}}$, для которых выполнено первое условие определения 4 и при этом $\deg(\boldsymbol{v}) < d$, являются $(m,d)_q^s$-хорошими. Однако общее число $(m,d)_q^s$-хороших мономов может быть значительно большим. Вышеуказанное определение иллюстрирует следующий

Пример 1. Пусть $m = s = 2$, $d = 7$, $q = 2^2 = 4$; рассмотрим моном $f(X_1, X_2) = X_1^2 X_2^6$, т.е. $f(\boldsymbol{X}) = \boldsymbol{X}^{\boldsymbol{v}}$ для $\boldsymbol{v} = (v_1, v_2) = (2, 6)$ и $\deg(\boldsymbol{v}) = 8 > d$. Проверим, что этот моном является $(m,d)_q^s$-хорошим. Во-первых, выполнено

$$\deg_q(\boldsymbol{v}) = \left\lfloor \frac{v_1}{q} \right\rfloor + \left\lfloor \frac{v_2}{q} \right\rfloor = \left\lfloor \frac{2}{4} \right\rfloor + \left\lfloor \frac{6}{4} \right\rfloor = 1 \leqslant s-1.$$

Для проверки второго условия отметим, что существует несколько различных векторов $\boldsymbol{i} = (i_1, i_2)$, удовлетворяющих соотношению $\boldsymbol{i} \leqslant_2 \boldsymbol{v}$. Подходят все векторы (i_1, i_2), такие что $i_1 \in \{0, 2\}$ и $i_2 \in \{0, 2, 4, 6\}$. Поскольку функция $\mathrm{Mod}_q^s(\cdot)$ не увеличивает аргумент, достаточно проверить условие $\mathrm{Mod}_q^s(\deg(\boldsymbol{i})) < d = 7$ лишь для $\boldsymbol{i} = (2, 6)$. Действительно, для $\boldsymbol{i} = (2, 6)$ выполнено

$$\mathrm{Mod}_q^s(\deg(\boldsymbol{i})) = \mathrm{Mod}_q^s(8) = 2 < d,$$

поскольку $8 \equiv 2 \pmod{qs - s}$ и $2 \in [s, qs-1]$.

Обозначим множество $(m,d)_q^s$-хороших мономов через $G_q^s(m,d) \subseteq \mathbb{F}_q[\boldsymbol{X}]$, а его мощность – через $N_q^s(m,d)$. Заметим, что кольцо $\mathbb{F}_q[\boldsymbol{X}]$ можно рассматривать как $\mathbb{F}_q$-линейное векторное пространство. Пусть $V_q^s(m,d) \subseteq \mathbb{F}_q[\boldsymbol{X}]$ обозначает линейную оболочку множества $G_q^s(m,d)$ над $\mathbb{F}_q$. В следующем утверждении указано важнейшее свойство хороших мономов и пространства $V_q^s(m,d)$.

Предложение 5. *Пусть задан произвольный вектор из линейных многочленов от одной переменной* $\gamma(T) = \boldsymbol{a}T + \boldsymbol{b}$, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^m$, $\boldsymbol{a} \neq \boldsymbol{0}$, *а также произвольный многочлен* $f(\boldsymbol{X}) \in V_q^s(d,m)$. *Тогда многочлен* $g(T)$, *определяемый как композиция* $f \circ \gamma(T)$, s-*эквивалентен некоторому многочлену* $h(T) \in \mathbb{F}_q[T]$ *степени* $\deg(h(T)) < d$.

Замечание 1. Отметим, что в предложении 5 образ отображения вычисления значений функции $\gamma(T)\colon \mathbb{F}_q \to \mathbb{F}_q^m$ соответствует некоторой прямой в пространстве $\mathbb{F}_q^m$. Таким образом, предложение 5 утверждает, что если рассмотреть линейную комбинацию хороших многочленов и ограничить их на произвольную прямую в пространстве, то полученный многочлен от одной переменной может быть эквивалентным образом задан (с точки зрения вычисления значений многочлена и всех его производных до $(s-1)$-го порядка включительно) многочленом от одной переменной невысокой степени.

Обозначим отображение вычисления значений многочлена и всех его производных до $(s-1)$-го порядка включительно во всех точках пространства $\mathbb{F}_q^m$ через

$$\mathrm{Ev}_{q,m}^s \colon \mathbb{F}_q[\boldsymbol{X}] \to \left(\mathbb{F}_q^{\binom{s+m-1}{m}}\right)^{q^m}.$$

Для произвольного многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ его образ равен

$$\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})) = \left(f^{(<s)}(\boldsymbol{x}_0)\right)\big|_{\boldsymbol{x}_0 \in \mathbb{F}_q^m}.$$

Наконец, определим коды, которые будут исследоваться в данной статье.

О п р е д е л е н и е 5 (обобщение s-кодов Рида – Соломона). Пусть q и s – степени простого числа p, $s < q$, и пусть даны положительные числа $m \geqslant 1$ и $d \leqslant sq$. Тогда определим код $\mathcal{C}_q^s(m,d)$ длины q^m над алфавитом $\mathbb{F}_q^{\binom{m+s-1}{m}}$ как

$$\mathcal{C}_q^s(m,d) := \left\{\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})) :\ f(\boldsymbol{X}) \in V_q^s(d,m)\right\}.$$

Определение 5 в указанном виде ранее в литературе не вводилось. Далее мы приведем историческую справку, которая раскрывает мотивацию для изучения обобщений s-кодов Рида – Соломона.

Код Рида – Соломона, один из наиболее исследованных в теории кодирования на данный момент, был изобретен в 1960 г. Ридом и Соломоном. Этот код в частном случае может быть задан как образ отображения вычисления значений многочленов от одной переменной степени не выше $d-1$ во всех точках поля $\mathbb{F}_q$. Отметим очевидное и при этом важное свойство, что при $d < q$ произвольная стертая координата кодового слова кода Рида – Соломона может быть восстановлена при чтении всех остальных координат.

Недвоичные коды Рида – Маллера, предложенные в ряде параллельных работ в 1968–1970 гг., являются естественным обобщением кодов Рида – Соломона. Подобный код может быть задан как образ отображения вычисления значений многочленов от $m \geqslant 2$ переменных степени не выше $d-1$ во всех точках пространства $\mathbb{F}_q^m$. При $d < q$ недвоичные коды Рида – Маллера обладают свойством локального восстановления: произвольная стертая координата кодового слова, соответствующая вычислению в точке $\boldsymbol{x}_0 \in \mathbb{F}_q^m$, может быть восстановлена после прочтения координат кодового слова, соответствующих произвольной прямой в $\mathbb{F}_q^m$, проходящей через $\boldsymbol{x}_0$. Это свойство выполнено, поскольку ограничение кодового слова недвоичного кода Рида – Маллера на произвольную прямую является кодовым словом кода Рида – Соломона. Однако кодовая скорость недвоичных кодов Рида – Маллера при $d < q$ и $m \geqslant 2$ не превышает $1/2$.

Чтобы построить код более высокой скорости, сохранив при этом свойство локального восстановления, Го, Коппарти и Судан [4] предложили в 2013 г. так называемые многомерные коды Рида – Соломона (lifted Reed–Solomon codes), соответствующие определению 5 при $s = 1$. Другой естественный способ обобщить коды Рида – Соломона был также предложен Розенблюмом и Цфасманом [5] в 1997 году в контексте введенной ими же новой метрики (так называемой s-метрики, или метрики Розенблюма – Цфасмана). Таким образом, в [5] был построен код, соответствующий определению 5 при $m = 1$, и назван s-кодом Рида – Соломона. Отметим, что s-код Рида – Соломона, так же как и обычный код Рида – Соломона, не обладает желанным сочетанием высокой скорости и локального восстановления. Таким образом, в 2014 г. Коппарти, Шараф и Еханин [6] разработали недвоичные s-коды Рида – Маллера (multiplicity codes), которые можно задать как образ отображения вычисления значений многочленов от $m \geqslant 2$ переменных степени не выше $d-1$ и

всех их производных до $(s-1)$-го порядка во всех точках пространства $\mathbb{F}_q^m$, т.е.

$$\mathcal{M}_q^s(d,m) := \left\{ \mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})) :\ f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}],\ \deg(f(\boldsymbol{X})) < d \right\}.$$

При $d \leqslant sq$ имеет место вложение $\mathcal{M}_q^s(d,m) \subseteq \mathcal{C}_q^s(d,m)$, поскольку множество $V_q^s(m,d)$ содержит всевозможные многочлены степени, меньшей d, а также некоторые многочлены значительно большей степени (см. подробнее [7]). В той же работе [6] было также показано, что недвоичные s-коды Рида – Маллера наряду с многомерными кодами Рида – Соломона могут достигать высокой скорости (сколь угодно близкой к 1), сохраняя при этом хорошие свойства локального восстановления.

Наконец, отметим, что наиболее родственные по смыслу коды, но все же отличные (см. [7]) от определения 5, – многомерные s-коды Рида – Соломона (чаще всего называемые в англоязычной литературе lifted multiplicity codes) – были изначально определены Ву [8] в 2015 г. с целью построить наиболее широкий класс кодов с высокой скоростью и отличными способностями локального восстановления. Подобный m-мерный s-код Рида – Соломона может быть задан как образ отображения вычисления значений всевозможных $(m,d)_q^s$-хороших многочленов и их производных. Здесь под $(m,d)_q^s$-хорошим многочленом мы понимаем такой многочлен, который при ограничении на произвольную прямую в пространстве $\mathbb{F}_q^m$ является s-эквивалентным некоторому многочлену от одной переменной степени не выше $d-1$. В работах [7–9] приведен анализ скорости многомерных s-кодов Рида – Соломона и предложены некоторые алгоритмы локального восстановления.

Очевидно, что обобщение s-кода Рида – Соломона $\mathcal{C}_q^s(m,d)$ является подкодом соответствующего m-мерного s-кода Рида – Соломона. В данной статье нам необходимо непосредственно использовать структурное свойство кода $\mathcal{C}_q^s(m,d)$, а именно то, что всякое кодовое слово этого кода соответствует линейной комбинации $(m,d)_q^s$-хороших мономов. В следующем предложении отметим несколько важных свойств кода $\mathcal{C}_q^s(m,d)$, которые более формально разъясняют вышеописанную мотивацию. Это утверждение было доказано в [7,9] для полей характеристики 2. В общем случае доказательство работает без изменений.

Предложение 6. *Пусть $m \geqslant 2$ и $\mathcal{C} = \mathcal{C}_q^s(m,d)$. Тогда имеют место следующие свойства.*

1. *Мощность кода удовлетворяет соотношению*

$$\log_q |\mathcal{C}| = N_q^s(m,d).$$

Другими словами, образ $(m,d)_q^s$-хороших мономов при отображении $\mathrm{Ev}_{q,m}^s$ задает $\mathbb{F}_q$-базис кода $\mathcal{C}$, и кодовое слово, состоящее из символов $\mathbf{0}$, соответствует лишь тождественно нулевому многочлену;

2. *Минимальное расстояние в коде $\mathcal{C}$ не меньше*

$$1 + \left\lceil \frac{qs-d-s+1}{s} \right\rceil (q-s)q^{m-2};$$

3. *Пусть даны точка в пространстве $\boldsymbol{x}_0 \in \mathbb{F}_q^m$ и $m-1$ множество $A_j \subseteq \mathbb{F}_q$, $|A_j| = s$, $j \in [m-1]$. Определим множество*

$$S := \{\boldsymbol{x}_0 + \lambda \boldsymbol{a} :\ \lambda \in \mathbb{F}_q^*,\ \boldsymbol{a} = (a_1, \ldots, a_{m-1}, 1),\ a_j \in A_j,\ j \in [m-1]\}.$$

Пусть $d \leqslant qs - s$. Тогда для произвольного $\boldsymbol{x}_0 \in \mathbb{F}_q^m$ компонента $f^{(<s)}(\boldsymbol{x}_0) \in \in \mathbb{F}_q^{\binom{s+m-1}{m}}$ кодового слова $\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X}))$ может быть восстановлена с помощью вектора значений $\left(f^{(<s)}(\boldsymbol{y}_0)\right)\big|_{\boldsymbol{y}_0 \in S}$. Таким образом, можно найти $\left(\frac{q}{s}\right)^{m-1}$ вза-

имно непересекающихся восстанавливающих множеств для каждой компоненты $f^{(<s)}(\boldsymbol{x}_0)$ кодового слова кода $\mathcal{C}$.

Замечание 2. Как сказано ранее, интерес к кодам $\mathcal{C}_q^s(m,d)$ в последние годы во многом объясняется свойством 3 в предложении 6, а также тем фактом, что при $d \geqslant qs-q$, фиксированном m, и $q=p^c \to \infty$ скорость этих кодов можно оценить величиной

$$1 - O\left(s^{-1}\left(\frac{q}{qs-d}\right)^{\lambda_p}\right),$$

где константа $\lambda_p < 0$. Также отметим, что при $qs-q \leqslant d < qs$, фиксированном m и $q=p^c \to \infty$ скорость кодов $\mathcal{M}_q^s(d,m)$ (недвоичных s-кодов Рида – Маллера) равна $1-\Theta(s^{-1})$, что меньше вышеуказанной оценки скорости кодов $\mathcal{C}_q^s(m,d)$ (более подробно см. в [7]).

1.3. Списочное декодирование s-кодов Рида – Соломона. Обобщение списочного алгоритма декодирования Гурусвами – Судана на случай s-кодов Рида – Соломона было впервые предложено в работе [10]. Отметим, что в случае $m=1$ можно опустить ограничение на то, что s является степенью простого p в определениях 4, 5. Мы приведем чуть более слабую версию утверждения из [10], более удобную для использования.

Предложение 7. *Пусть даны целые положительные числа s и q, где q – степень простого числа p, а $s<q$. Выберем некоторое целое число $\varphi \geqslant 3$ и целое число $d \in [s, qs]$. Тогда существует алгоритм $\mathfrak{A}_q^s(d,\varphi)$, входом которого является произвольный вектор $\boldsymbol{r} \in (\mathbb{F}_q^s)^q$, а выходом – множество всевозможных кодовых слов s-кода Рида – Соломона $\mathcal{L} \subseteq \mathcal{C}_q^s(1,d)$, для которых расстояние Хэмминга $d_H(\boldsymbol{c},\boldsymbol{r})$ удовлетворяет неравенству*

$$d_H(\boldsymbol{c},\boldsymbol{r}) \leqslant q - (1+3/\varphi)\sqrt{q(d-1)/s} - 1, \quad \boldsymbol{c} \in \mathcal{L}.$$

Более того, время работы этого алгоритма равно $\mathrm{poly}(q,\varphi)$, *а размер списка* $|\mathcal{L}| = O(\varphi\sqrt{sq/d})$.

В дальнейшем были найдены [11,12] более эффективные списочные декодеры для s-кода Рида – Соломона, заданного над простым полем $\mathbb{F}_p$. Однако мы воспользуемся вышеуказанным утверждением, поскольку нам потребуется использовать биективное отображение между пространством $\mathbb{F}_q^m$ и полем $\mathbb{F}_{q^m}$, а поле $\mathbb{F}_{q^m}$ при $m \geqslant 2$ гарантированно не является простым. Также отметим, что при $s=1$ списочное декодирование соответствующих кодов $\mathcal{C}_q^1(m,d)$ (m-мерных кодов Рида – Соломона) было впервые предложено в работе [13]. Мы воспользуемся идеями из этой работы, а также структурой алгоритма списочного декодера кодов $\mathcal{M}_q^s(d,m)$ (недвоичных s-кодов Рида – Маллера) из работы [11].

1.4. Базис в поле $\mathbb{F}_{q^m}$ и параметризация пространства $\mathbb{F}_q^m$. Пусть элементы $\alpha_1,\ldots,\alpha_m \in \mathbb{F}_{q^m}$ образуют $\mathbb{F}_q$-*базис* поля $\mathbb{F}_{q^m}$, т.е. всякий элемент $\beta \in \mathbb{F}_{q^m}$ представим в виде $\beta = \sum\limits_{j=1}^{m} \lambda_j \alpha_j$ для некоторых $\lambda_j \in \mathbb{F}_q$, $j \in [m]$. Через $\boldsymbol{\alpha}$ обозначим вектор $(\alpha_1,\ldots,\alpha_m)$. В дальнейшем будем кратко говорить, что $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ является *базисом*.

Определение 6. Будем говорить, что набор из базисов $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_t \in \mathbb{F}_{q^m}^m$ находится в s-*общем положении*, если для произвольного ненулевого многочлена $r(\boldsymbol{X}) \in \mathbb{F}_{q^m}[\boldsymbol{X}]$ степени $\deg(r(\boldsymbol{X})) < s$ существует такое число $i \in [t]$, что $r(\boldsymbol{\alpha}_i) \neq 0$.

Следующее утверждение было доказано в [11, 14].

Предложение 8. *Пусть даны число q, являющееся степенью простого числа p, целое число $m \geqslant 2$, а также целое положительное число s, $s < q$. Если $t \geqslant s^m$, то существует набор из базисов $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t \in \mathbb{F}_{q^m}^m$, находящийся в s-общем положении. Более того, такой набор может быть найден за время* $\mathrm{poly}(q, m)$.

Пусть $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ является базисом. Определим биективное отображение $\gamma_{\boldsymbol{\alpha}} \colon \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ следующим образом:

$$\gamma_{\boldsymbol{\alpha}}(x) := \big(\mathrm{Tr}(\alpha_1 x), \ldots, \mathrm{Tr}(\alpha_m x)\big),$$

где функция $\mathrm{Tr} \colon \mathbb{F}_{q^m} \to \mathbb{F}_q$ является стандартным *следом* элементов расширенного поля $\mathbb{F}_{q^m}$ в $\mathbb{F}_q$, т.е. $\mathrm{Tr}(y) = \sum\limits_{i=0}^{m-1} y^{q^i}$. Кроме того, будем использовать запись $\mathrm{Tr}(T)$ для обозначения многочлена $\sum\limits_{i=0}^{m-1} T^{q^i}$. Следующее естественное утверждение было также доказано в [11, 14].

Предложение 9. *Пусть даны число q, являющееся степенью простого числа p, и целое число $m \geqslant 2$. Пусть также заданы многочлен $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ и базис $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$. Определим*

$$g(T) := f \circ \gamma_{\boldsymbol{\alpha}}(T) \in \mathbb{F}_{q^m}[T].$$

Тогда для произвольной точки $x_0 \in \mathbb{F}_{q^m}$ и любого $i \in [0, q-1]$ выполнено следующее соотношение:

$$g^{(i)}(x_0) = \sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = i}} f^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}}(x_0)) \prod_{j=1}^{m} \alpha_j^{e_j}.$$

§ 2. Основные результаты

Главным результатом данной статьи является следующее утверждение.

Теорема 1. *Пусть даны числа q и s, являющиеся степенями простого числа p, а также положительные числа $m \geqslant 2$ и d, для которых верно $d \leqslant sq - m - 2(s-1)$ и $m + s \leqslant q$. Определим целое число*

$$\widetilde{d} := q^{m-1}\left(s - 1 + \frac{q-1}{q}(m + d - 1)\right)$$

и зададим некоторый целочисленный параметр $\varphi \geqslant 3$. Тогда существует алгоритм $\mathfrak{A}_q^s(d, m, \varphi)$, входом которого является произвольный вектор $\boldsymbol{r} \in \left(\mathbb{F}_q^{\binom{s+m-1}{m}}\right)^{q^m}$, а выходом – множество $\mathcal{L} \subseteq \mathcal{C}_q^s(m, d)$ всевозможных кодовых слов кода $\mathcal{C}_q^s(m, d)$, для которых расстояние Хэмминга $d_H(\boldsymbol{c}, \boldsymbol{r})$ удовлетворяет неравенству

$$d_H(\boldsymbol{c}, \boldsymbol{r}) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1, \quad \boldsymbol{c} \in \mathcal{L}.$$

Более того, время работы этого алгоритма равно $\mathrm{poly}\left(q^m, \left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$, *а размер списка можно оценить величиной* $O\left(\left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$.

Замечание 3. Время работы данного алгоритма и размер списка равны $\mathrm{poly}(q^m)$ в случае $q = p^c \to \infty$, $s = O(1)$, $m = O(1)$. Отметим, что используя некоторые идеи из [14], можно привести списочный алгоритм декодирования со сложностью

и размером списка $\mathrm{poly}(q^m)$ без подобного ограничения на s и m. Однако радиус декодирования для подобного алгоритма будет уступать вышеуказанному.

Мы приведем алгоритм списочного декодирования в п. 2.1 и проанализируем его в п. 2.2. В процессе доказательства мы выведем утверждение, которое поможет (незначительно) улучшить оценку на минимальное расстояние кодов $\mathcal{C}_q^s(m,d)$, указанную ранее в предложении 6. Следующее утверждение будет доказано в п. 2.3.

Т е о р е м а 2. *Пусть даны числа q и s, являющиеся степенями простого числа p, а также положительные числа $m \geqslant 2$ и d, такие что*

$$d \leqslant sq - m - 2(s-1) \quad u \quad m + s \leqslant q.$$

Тогда минимальное расстояние кода $\mathcal{C}_q^s(m,d)$ находится в интервале $[\underline{d}, \overline{d}\,]$, где величины $\underline{d}$ и $\overline{d}$ заданы следующим образом:

$$\underline{d} := q^m - \left\lfloor \frac{s - 1 + \dfrac{q-1}{q}(m+d-1)}{s} q^{m-1} \right\rfloor, \quad \overline{d} := q^m - \left\lfloor \frac{d-1}{s} \right\rfloor q^{m-1}.$$

2.1. Алгоритм списочного декодирования. Опишем алгоритм списочного декодирования, которым воспользуемся для доказательства теоремы 1. Пусть входом алгоритма является $\boldsymbol{r} \in \left(\mathbb{F}_q^{\binom{s+m-1}{m}}\right)^{q^m}$. Пусть $\boldsymbol{y}_0 \in \mathbb{F}_q^m$ и $\boldsymbol{e} \in \mathbb{N}^m$, $\deg(\boldsymbol{e}) < s$. Для удобства обозначений будем писать $r^{(\boldsymbol{e})}(\boldsymbol{y}_0)$ при обращении к элементу (из $\mathbb{F}_q$) вектора $\boldsymbol{r}$, который естественно индексировать парой $(\boldsymbol{y}_0, \boldsymbol{e})$.

1. Пусть $t = s^m$. Найдем набор базисов $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t \in \mathbb{F}_{q^m}^m$, находящийся в s-общем положении.
2. Для всякого $\ell \in [t]$ определим функцию (вектор) $\boldsymbol{h}_\ell \colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}^s$ по правилу

$$(h_\ell(x_0))_i = \sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = i}} r^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}_\ell}(x_0)) \prod_{j=1}^{m} {\alpha_{\ell,j}}^{e_j}, \quad \forall x_0 \in \mathbb{F}_{q^m},\ i \in [0, s-1].$$

3. Для всякого $\ell \in [t]$ воспользуемся алгоритмом $\mathfrak{A}_q^s(\widetilde{d}+1, \varphi)$ из предложения 7 и восстановим множество $\mathcal{L}_\ell$ всевозможных кодовых слов $\boldsymbol{c} \in \mathcal{C}_{q^m}^s(1, \widetilde{d}+1)$, для которых выполнено

$$d_H(\boldsymbol{c}, \boldsymbol{h}_\ell) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

4. Для всякого набора $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_t) \in \mathcal{L}_1 \times \cdots \times \mathcal{L}_t$ найдем сначала соответствующий им набор $(\widetilde{g}_1(T), \ldots, \widetilde{g}_t(T)) \in (\mathbb{F}_{q^m}[T])^t$ многочленов степени не выше $\widetilde{d}$, а затем множество всевозможных "согласованных" многочленов $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m,d)$, таких что

$$\widetilde{f} \circ \gamma_{\alpha_\ell}(T) \equiv_s \widetilde{g}_\ell(T), \quad \forall \ell \in [t]. \tag{2}$$

5. Выходом алгоритма будет список всевозможных многочленов $\widetilde{f}(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$, найденных на четвертом шаге, для которых выполнено

$$d_H(\mathrm{Ev}_{q,m}^s(\widetilde{f}(\boldsymbol{X})), \boldsymbol{r}) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

2.2. Анализ алгоритма. Сначала кратко рассмотрим каждый из шагов алгоритма, а затем проанализируем важные аспекты некоторых шагов более подробно.

Первый шаг. В силу предложения 8 такой набор существует и может быть найдет за время $\mathrm{poly}(q, m)$.

Второй шаг. В силу предложения 9 способ задания функции (вектора) $\boldsymbol{h}_\ell$ соответствует заданию функции $h_\ell(T) = r \circ \gamma_{\boldsymbol{\alpha}_\ell}(T)$, если интерпретировать вектор $\boldsymbol{r}$ как функцию $r(\boldsymbol{X})$.

Третий шаг. Пусть $f(\boldsymbol{X}) \in V_q^s(m, d)$. Тогда в силу леммы 3, которую мы докажем чуть позже, многочлен $g_\ell(T) := f \circ \gamma_{\boldsymbol{\alpha}_\ell}(T)$ является s-эквивалентным многочлену степени не выше $\widetilde{d}$. Таким образом, если расстояние Хэмминга между $\boldsymbol{r}$ и $\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X}))$ невелико, то одно из кодовых слов в множестве $\mathcal{L}_\ell$ будет соответствовать многочлену $g_\ell(T)$ (см. более подробно лемму 1).

Четвертый шаг. Каждый многочлен $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m, d)$ можно задать с помощью $N_q^s(m, d)$ коэффициентов из $\mathbb{F}_q$, каждый из которых соответствует некоторому $(m, d)_q^s$-хорошему моному (см. обозначения после определения 4). Многочлен, стоящий в правой части уравнения (2), уже определен, а в левой части стоит неопределенный многочлен с $N_q^s(m, d)$ неизвестными, для которого можно взять остаток при делении на $T^{sq^m} + (-T)^s$ (см. предложение 3). Отметим, что в силу леммы 3 степень многочлена, полученного как остаток, не превосходит $\widetilde{d}$. Таким образом, нужно решить систему линейных уравнений с $N_q^s(m, d)$ неизвестными и $t(\widetilde{d}+1)$ ограничениями. В силу леммы 2, которую мы докажем чуть позже, существует не более одного многочлена $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m, d)$, удовлетворяющего системе уравнений (2) для данного набора $(\widetilde{g}_1(T), \ldots, \widetilde{g}_t(T))$. Таким образом, для поиска всевозможных $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m, d)$ нужно потратить время $\mathrm{poly}\big(q^m, t\widetilde{d}, N_q^s(m, d)\big) \prod\limits_{\ell=1}^{t} |\mathcal{L}_\ell|$.

Пятый шаг. Перед выходом из алгоритма нужно будет отсеять те многочлены $f(\boldsymbol{X}) \in V_q^s(m, d)$, для которых выполнено

$$d_H(\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})), \boldsymbol{r}) > q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

Мы докажем корректность всего алгоритма в лемме 1.

Используя предложение 7, оценим суммарную сложность и время работы алгоритма. Сложность первого шага равна $\mathrm{poly}(q, m)$, второго – $\mathrm{poly}(q^m)$, третьего – $\mathrm{poly}(q^m, \varphi)$, четвертого и пятого шагов – $\mathrm{poly}\left(q^m, \left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$. Итоговый размер списка оценивается величиной $O\left(\left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$.

Наконец, докажем несколько оставшихся утверждений.

Лемма 1. *Предположим, что для некоторого многочлена $f(\boldsymbol{X}) \in V_q^s(m, d)$ расстояние Хэмминга удовлетворяет неравенству*

$$d_H(\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})), \boldsymbol{r}) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

Тогда список многочленов на выходе предложенного списочного алгоритма будет содержать $f(\boldsymbol{X})$.

Доказательство. Для всякого $\ell \in [t]$ рассмотрим базис

$$\boldsymbol{\alpha}_\ell = (\alpha_{\ell,1}, \ldots, \alpha_{\ell,m}) \in \mathbb{F}_{q^m}^m$$

и многочлен

$$g_\ell(T) := f \circ \gamma_{\boldsymbol{\alpha}_\ell}(T).$$

Используя предложение 9, имеем

$$g_\ell^{(i)}(x_0) = \sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} f^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}_\ell}(x_0)) \prod_{j=1}^{m} \alpha_{\ell,j}^{e_j}, \quad \forall x_0 \in \mathbb{F}_{q^m},\ i \in [0, s-1].$$

Из условия утверждения существуют не менее $(1+3/\varphi)\sqrt{q^m\widetilde{d}/s}+1$ точек $\boldsymbol{y}_0 \in \mathbb{F}_q^m$, таких что $f^{(<s)}(\boldsymbol{y}_0) = r^{(<s)}(\boldsymbol{y}_0)$. Также отметим, что $\gamma_{\boldsymbol{\alpha}_\ell}$ является биекцией между $\mathbb{F}_{q^m}$ и $\mathbb{F}_q^m$. Тогда на втором шаге алгоритма найдется не менее $(1+3/\varphi)\sqrt{q^m\widetilde{d}/s}+1$ точек $x_0 \in \mathbb{F}_{q^m}$, для которых выполнено $g_\ell^{(i)}(x_0) = (h_\ell(x_0))_i$ для всех $i \in [0, s-1]$. Заметим, что степень $\deg(g_\ell(T)) \leqslant \widetilde{d}$ в силу леммы 3. Следовательно, множество $\mathcal{L}_\ell$, полученное на третьем шаге, будет содержать кодовое слово кода $\mathcal{C}_{q^m}^s(1, \widetilde{d}+1)$, соответствующее многочлену $g_\ell(T)$. Таким образом, на четвертом шаге будет рассмотрен набор, соответствующий $(g_1(T), \ldots, g_t(T))$, и многочлен $f(\boldsymbol{X}) \in V_q^s(m,d)$ будет найден при решении системы уравнений и включен в список на выходе алгоритма. ▲

Лемма 2. *Предположим, что существуют два многочлена* $\widetilde{f}_1(\boldsymbol{X}), \widetilde{f}_2(\boldsymbol{X}) \in V_q^s(m,d)$, *удовлетворяющие соотношению* (2). *Тогда* $\widetilde{f}_1(\boldsymbol{X}) = \widetilde{f}_2(\boldsymbol{X})$.

Доказательство. Определим $h(\boldsymbol{X}) := \widetilde{f}_1(\boldsymbol{X}) - \widetilde{f}_2(\boldsymbol{X})$. Рассмотрим некоторое число $\ell \in [t]$ и базис $\boldsymbol{\alpha}_\ell = (\alpha_{\ell,1}, \ldots, \alpha_{\ell,m}) \in \mathbb{F}_{q^m}^m$. Тогда выполнено соотношение

$$h \circ \gamma_{\boldsymbol{\alpha}_\ell}(T) \equiv_s 0.$$

В силу предложения 9 выполнено

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} h^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}_\ell}(x_0)) \prod_{j=1}^{m} \alpha_{\ell,j}^{e_j} = 0, \quad \forall x_0 \in \mathbb{F}_{q^m},\ i \in [0, s-1],$$

где $\boldsymbol{e} = (e_1, \ldots, e_m)$. Поскольку отображение $\gamma_{\boldsymbol{\alpha}_\ell}$ задает биекцию между $\mathbb{F}_{q^m}$ и $\mathbb{F}_q^m$, мы можем заключить, что для всякой точки $\boldsymbol{y}_0 \in \mathbb{F}_q^m$ верно

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} h^{(\boldsymbol{e})}(\boldsymbol{y}_0) \prod_{j=1}^{m} \alpha_{\ell,j}^{e_j} = 0.$$

Мы можем думать о вышеуказанном выражении как о вычислении в точке $\boldsymbol{\alpha}_\ell$ значения многочлена

$$v(\boldsymbol{X}) := \sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} h^{(\boldsymbol{e})}(\boldsymbol{y}_0)\boldsymbol{X}^{\boldsymbol{e}}.$$

Степень данного многочлена меньше s. Поскольку набор базисов был выбран в s-общем положении, в силу определения 6 можно заключить, что $v(\boldsymbol{X})$ тождественно равен нулю. Отсюда следует, что $h^{(\boldsymbol{e})}(\boldsymbol{y}_0) = 0$ для всех $\boldsymbol{y}_0 \in \mathbb{F}_q^m$ и $\boldsymbol{e} \in \mathbb{N}^m$, $\deg(\boldsymbol{e}) < s$. Поскольку $h(\boldsymbol{X}) \in V_q^s(m,d)$, из первого утверждения в предложении 6 следует, что $h(\boldsymbol{X}) = 0$. Таким образом, требуемое утверждение доказано. ▲

Лемма 3. *Пусть даны числа q и s, являющиеся степенями простого числа p, а также положительные числа $m \geqslant 2$ и d, такие что*

$$d \leqslant sq - m - 2(s-1) \quad и \quad m + s \leqslant q.$$

Пусть вектор $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ является базисом, и пусть $f(\boldsymbol{X}) \in V_q^s(m,d)$. Определим $g(T) := f \circ \gamma_{\boldsymbol{\alpha}}(T)$. Тогда существует единственный многочлен $r(T) \in \mathbb{F}_{q^m}[T]$, для которого верно $r(T) \equiv_s g(T)$ и $\deg(r(T)) \leqslant \widetilde{d}$, где

$$\widetilde{d} = q^{m-1}\left(s - 1 + \frac{q-1}{q}(m+d-1)\right).$$

Доказательство. Пусть $\lambda \in \mathbb{F}_q$, а $z(\boldsymbol{X}) \in V_q^s(d,m)$. В силу линейности

$$(f + \lambda z) \circ \gamma_{\boldsymbol{\alpha}}(T) = f \circ \gamma_{\boldsymbol{\alpha}}(T) + \lambda(z \circ \gamma_{\boldsymbol{\alpha}}(T))$$

достаточно рассматривать лишь многочлен $f(\boldsymbol{X})$, который является в точности $(m,d)_q^s$-хорошим мономом $\boldsymbol{X}^{\boldsymbol{v}}$, $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$. В дальнейшем будем использовать векторы $\boldsymbol{e}_j = (e_{j,0}, \ldots, e_{j,m-1})$, $j \in [m]$. Распишем получившийся многочлен $g(T)$ от одной переменной в таком случае:

$$g(T) = \prod_{j=1}^{m} \left(\mathrm{Tr}(\alpha_j T)\right)^{v_j} = \prod_{j=1}^{m} \left(\sum_{i=0}^{m-1} (\alpha_j T)^{q^i}\right)^{v_j} =$$

$$= \prod_{j=1}^{m} \left(\sum_{\substack{\boldsymbol{e}_j \in \mathbb{N}^m \\ \deg(\boldsymbol{e}_j) = v_j}} \binom{v_j}{e_{j,0}, \ldots, e_{j,m-1}} (\alpha_j T)^{\sum\limits_{i=0}^{m-1} e_{j,i} q^i} \right) =$$

$$= \sum_{\substack{\boldsymbol{e}_1 \in \mathbb{N}^m, \ldots, \boldsymbol{e}_m \in \mathbb{N}^m \\ \deg(\boldsymbol{e}_1) = v_1, \ldots, \deg(\boldsymbol{e}_m) = v_m}} T^{\sum\limits_{j=1}^{m} \sum\limits_{i=0}^{m-1} e_{j,i} q^i} \prod_{j=1}^{m} \binom{v_j}{e_{j,0}, \ldots, e_{j,m-1}} \alpha_j^{\sum\limits_{i=0}^{m-1} e_{j,i} q^i}.$$

Далее воспользуемся следствием 1, чтобы упростить данное выражение. Из этого утверждения следует, что если хотя бы для одного $i \in [0, m-1]$ не выполнено отношение порядка $e_{j,i} \leqslant_p v_j$, то соответствующий мультиномиальный коэффициент $\binom{v_j}{e_{j,0}, \ldots, e_{j,m-1}}$ равен нулю в поле характеристики p. В дальнейшем анализе будем рассматривать лишь слагаемые вышеуказанной суммы, для которых выполнено условие $\boldsymbol{e}_j \leqslant_p v_j$ для всех $j \in [m]$. В силу предложения 3 нас интересует многочлен $r(T)$ степени не выше $sq^m - 1$, для которого выполнено

$$r(T) \equiv g(T) \pmod{T^{sq^m} + (-T)^{q^m}}.$$

Для произвольного набора векторов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m \in \mathbb{N}^m$, для которых верно $\boldsymbol{e}_j \leqslant_p v_j$, $\deg(\boldsymbol{e}_j) = v_j$, $j \in [m]$, определим величину

$$\widetilde{e} := \sum_{j=1}^{m} \sum_{i=0}^{m-1} e_{j,i} q^i.$$

Таким образом, достаточно показать, что $\widetilde{e}$ удовлетворяет условию $\mathrm{Mod}_{q^m}^s(\widetilde{e}) \leqslant \widetilde{d}$.

Напомним, что моном $\boldsymbol{X}^{\boldsymbol{v}}$ является $(m,d)_q^s$-хорошим. Следовательно, из определения 4 имеем, что для произвольного $\boldsymbol{a} \in \mathbb{N}^m$, $a_j \leqslant_p v_j$, $j \in [m]$, выполнено неравенство $\mathrm{Mod}_q^s(\deg(\boldsymbol{a})) < d$. Возьмем в качестве $\boldsymbol{a} = (a_1, \ldots, a_m)$ вектор, j-я компонента

которого равна $a_j = e_{j,m-1}$. Тогда из определений хороших мономов и операции Mod_q^s получим, что

$$\sum_{j=1}^{m} e_{j,m-1} = \eta(qs - s) + \mu,$$

где целые числа удовлетворяют соотношениям $\eta \geqslant 0$ и $0 \leqslant \mu < d$. Более того, если $\eta > 0$, то $\mu \geqslant s$.

В дальнейшем мы получим верхнюю и нижнюю оценки на величину $\widetilde{e}$, что поможет доказать необходимое неравенство $\mathrm{Mod}_{q^m}^s(\widetilde{e}) \leqslant \widetilde{d}$. Начнем с верхней границы, при выводе которой воспользуемся соотношениями

$$v_j = \sum_{i=0}^{m-1} e_{j,i}, \quad j \in [m], \quad \text{и} \quad \sum_{j=1}^{m} v_j \leqslant q(s-1) + m(q-1)$$

(эквивалентно условию $\deg_q(\boldsymbol{v}) \leqslant s - 1$ в определении 4). Имеем

$$\widetilde{e} = \sum_{j=1}^{m}\sum_{i=0}^{m-1} e_{j,i}q^i \leqslant q^{m-1}\sum_{j=1}^{m} e_{j,m-1} + q^{m-2}\sum_{j=1}^{m}(v_j - e_{j,m-1}) \leqslant$$
$$\leqslant (q^{m-1} - q^{m-2})\sum_{j=1}^{m} e_{j,m-1} + q^{m-2}(q(s-1) + m(q-1)).$$

Напомним, что $\sum\limits_{j=1}^{m} e_{j,m-1} = \eta(qs - s) + \mu$. Продолжим вывод верхней оценки:

$$\widetilde{e} \leqslant (q^{m-1} - q^{m-2})(\eta(qs-s) + \mu) + q^{m-2}(qs - q + m(q-1)) =$$
$$= \eta(sq^m - s) + q^{m-1}(s - 1 + m + \mu - 2s\eta) + q^{m-2}(s\eta - \mu - m) + s\eta.$$

Теперь оценим $\widetilde{e}$ снизу:

$$\widetilde{e} = \sum_{j=1}^{m}\sum_{i=0}^{m-1} e_{j,i}q^i \geqslant \sum_{j=1}^{m} e_{j,m-1}q^{m-1} = q^{m-1}(\eta(qs-s) + \mu) \geqslant$$
$$\geqslant \eta(sq^m - s) + \eta s + (\mu - s\eta)q^{m-1}.$$

Заметим, что моном $\boldsymbol{X}^{\boldsymbol{a}}$ с $\boldsymbol{a} = (e_{1,m-1}, \ldots, e_{m,m-1})$ является также $(m,d)_q^s$-хорошим, поскольку $\boldsymbol{a} \leqslant_p \boldsymbol{v}$, и выполнено естественное свойство транзитивности для $(m,d)_q^s$-хороших мономов. Напоследок воспользуемся оценкой $\mu \geqslant s\eta$, которая следует из предложения 10, поскольку верно $d \leqslant sq - m - 2(s-1)$ по условию доказываемого утверждения. Таким образом, объединяя верхнюю и нижнюю границы для $\widetilde{e}$, получаем

$$\eta(sq^m - s) + \eta s \leqslant \widetilde{e} \leqslant \eta(sq^m - s) + d',$$

где

$$d' := q^{m-1}(s - 1 + m + \mu - 2s\eta) + q^{m-2}(s\eta - \mu - m) + s\eta.$$

Очевидно, что d' достигает максимального значения

$$\widetilde{d} = q^{m-1}\left(s - 1 + \frac{q-1}{q}(m + d - 1)\right)$$

при $\eta = 0$, $\mu = d - 1$. Если $\eta = 0$, то $\widetilde{e} \leqslant \widetilde{d}$ и $\mathrm{Mod}^s_{q^m}(\widetilde{e}) \leqslant \widetilde{d}$. Если $\eta > 0$, то $\widetilde{e} \geqslant \eta s$ и $\mathrm{Mod}^s_{q^m}(\widetilde{e}) = b$, где $b \in [\eta s, \widetilde{d}]$ и $b \equiv \widetilde{e} \pmod{sq^m - s}$. Эти рассуждения завершают доказательство. ▲

Предложение 10. *Пусть даны числа s и q, являющиеся степенями простого числа p, и положительное число $m \geqslant 2$, $m + s \leqslant q$. Предположим, что моном $\boldsymbol{X}^{\boldsymbol{v}}$ для некоторого вектора $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$ является $(m, sq - m - 2(s-1))^s_q$-хорошим. Тогда для целых чисел $\eta \geqslant 0$ и $0 \leqslant \mu < sq - m - 2(s-1)$ (причем $\mu \geqslant s$ при $\eta > 0$), удовлетворяющих соотношению*

$$\sum_{j=1}^{m} v_j = \eta s(q-1) + \mu,$$

выполнено неравенство $\eta s \leqslant \mu$.

Доказательство. Предположим противное, т.е. выполнено $\eta s > \mu$. Определим целые числа $h := \eta s$ и $k := p^\ell - h + \mu$, где $\ell \in \mathbb{N}$ – наименьшее число, при котором $p^\ell > h$. Заметим, что выполнено неравенство $q > h = \eta s$, так как

$$\deg(\boldsymbol{v}) = \eta s(q-1) + \mu \leqslant q(s-1) + m(q-1)$$

(из условия $\deg_q(\boldsymbol{v}) \leqslant s - 1$ в определении 4), и следовательно,

$$\eta s \leqslant m + \left\lfloor \frac{q}{q-1}(s-1) \right\rfloor = m + s - 1 < q. \tag{3}$$

Также отметим, что при таком выборе чисел имеет место следующее (частичное) p-ичное разложение:

$$\deg(\boldsymbol{v}) = \sum_{j=1}^{m} v_j = \eta s(q-1) + \mu = hq - h + \mu =$$
$$= (h-1)p^{\log_p q} + (p-1) \sum_{i=\ell}^{\log_p q - 1} p^i + k.$$

Тогда h, k, p и μ удовлетворяют условию предложения 12, так как $h = \eta s > \mu$ по предположению и $h < p^\ell$, $k = p^\ell - h + \mu$ по построению. Из этого утверждения следует, что существует число $\theta \in \mathbb{N}$, для которого верно $\theta \leqslant_p k$ и $\mu \leqslant \theta \leqslant h - 1$. Определим $e := \sum\limits_{j=1}^{m} v_j - \theta$. Поскольку $\theta \leqslant_p k$ и выполнено вышеуказанное (частичное) p-ичное разложение для суммы $\sum\limits_{j=1}^{m} v_j$, имеем $e \leqslant_p \sum\limits_{j=1}^{m} v_j$. Из предложения 11 следует, что существуют $e_1, \ldots, e_m \in \mathbb{N}$, такие что $\sum\limits_{j=1}^{m} e_j = e$ и $e_j \leqslant_p v_j$ для всех $j \in [m]$. Наконец, для получения противоречия посчитаем величину $\mathrm{Mod}^s_q(e)$. Поскольку

$$e = \sum_{j=1}^{m} v_j - \theta = \eta s(q-1) + \mu - \theta$$

и $\mu \leqslant \theta \leqslant s\eta - 1$, получаем, что

$$\mathrm{Mod}^s_q(e) \geqslant sq - s + (\mu - \theta) \geqslant sq - s - \eta s + 1.$$

Воспользуемся неравенством (3) и получим $\mathrm{Mod}^s_q(e) \geq sq - m - 2(s-1)$, что противоречит тому, что $\boldsymbol{X}^{\boldsymbol{v}}$ является $(sq - m - 2(s-1), m)^s_q$-хорошим. ▲

Следующие два технических утверждения необходимы для доказательства предложения 10.

Предложение 11. *Пусть даны числа* $v_1, \ldots, v_m, h \in \mathbb{N}$ *и простое число* p. *Предположим, что имеет место отношение порядка* $e \leqslant_p \sum\limits_{j=1}^{m} v_j$. *Тогда существуют* $e_1, \ldots, e_m \in \mathbb{N}$, *такие что* $\sum\limits_{j=1}^{m} e_j = e$ *и* $e_j \leqslant_p v_j$ *для всех* $j \in [m]$.

Доказательство. Рассмотрим многочлен $(1+T)^{\sum\limits_{j=1}^{m} v_j}$. Коэффициент при мономе T^e равен $\binom{\sum\limits_{j=1}^{m} v_j}{e}$. Из предложения 4 следует, что этот коэффициент удовлетворяет условию

$$\binom{\sum\limits_{j=1}^{m} v_j}{e} \not\equiv 0 \pmod{p},$$

так как справедливо отношение порядка $e \leqslant_p \sum\limits_{j=1}^{m} v_j$. С другой стороны, этот коэффициент при T^e равен

$$\sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = e}} \prod_{j=1}^{m} \binom{v_j}{e_j},$$

откуда получаем, что существуют хотя бы один выбор $e_1, \ldots, e_m \in \mathbb{N}$, такой что $\prod\limits_{j=1}^{m} \binom{v_j}{e_j} \not\equiv 0 \pmod{p}$. Если воспользоваться предложением 4 для e_j и v_j, то получим требуемое утверждение. ▲

Предложение 12. *Пусть даны числа* $h, k, \ell, \mu \in \mathbb{N}$ *и простое число* p. *Предположим, что выполнено* $k = p^\ell - h + \mu$ *и* $\mu < h < p^\ell$. *Тогда существует некоторое число* $\theta \in \mathbb{N}$, *для которого* $\theta \leqslant_p k$ *и* $\mu \leqslant \theta \leqslant h-1$.

Доказательство. Воспользуемся тождеством

$$\binom{p^\ell - 1}{\mu + p^\ell - k - 1} = \sum_{\theta=\mu}^{\min\{h-1,k\}} \binom{k}{\theta} \binom{p^\ell - k - 1}{\mu + p^\ell - k - 1 - \theta} =$$

$$= \sum_{\theta=\mu}^{\min\{h-1,k\}} \binom{k}{\theta} \binom{p^\ell - k - 1}{\theta - \mu}.$$

Действительно, левая часть равна числу способов выбрать $\mu + p^\ell - k - 1$ элементов из данного множества мощности $p^\ell - 1$. В средней части мы сначала выбираем среди первых k элементов некоторое подмножество из θ элементов, а затем из оставшихся $p^\ell - k - 1$ элементов некоторые $\mu + p^\ell - k - 1 - \theta$. Из предложения 4 следует, что левая часть по модулю p не равна нулю. Действительно, выполнено соотношение $a \leqslant_p p^\ell - 1$ для всякого $a \leqslant p^{\ell-1}$. Следовательно, существует хотя бы один выбор θ, при котором одно из слагаемых в правой части не равно нулю по модулю p. Используя снова предложение 4, получаем что для такого θ верно отношение порядка $\theta \leqslant_p k$. Более того, из ограничений суммы имеем $\mu \leqslant \theta \leqslant h-1$. ▲

2.3. Доказательство теоремы 2. Определим число $n_0 := \lfloor (d-1)/s \rfloor$ и произвольное подмножество $B \subseteq \mathbb{F}_q$ размера $|B| = n_0$. Для доказательства границы сверху на минимальное расстояние заметим, что ненулевой многочлен $f(X_1, \ldots, X_m) :=$

$:= \prod\limits_{\beta \in B} (X_1 - \beta)^s$ степени $\deg(f(\boldsymbol{X})) \leqslant d-1$ является $(m,d)_q^s$-хорошим. В силу предложения 2 и формулы для производной Хассе несложно видеть, что число позиций в кодовом слове $\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X}))$, не равных $\mathbf{0}$, равно $\overline{d} = (q-n_0)q^{m-1}$.

Теперь докажем оценку снизу на минимальное расстояние. Пусть даны два различных многочлена $f_1(\boldsymbol{X}), f_2(\boldsymbol{X}) \in V_q^s(m,d)$. Определим $\widehat{f}(\boldsymbol{X}) := f_1(\boldsymbol{X}) - f_2(\boldsymbol{X}) \neq 0$. Для базиса $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ определим $g(T) := \widehat{f} \circ \gamma_{\boldsymbol{\alpha}}(T)$. В силу леммы 3 можно заключить, что $g(T)$ является s-эквивалентным многочлену $r(T)$ степени не выше $\widetilde{d} = q^{m-1}\left(s - 1 + \dfrac{q-1}{q}(m+d-1)\right)$. Более того, используя формулу для подсчета производных из предложения 9, можно найти базис $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$, такой что соответствующий многочлен $r(T) \neq 0$. Действительно, для $x_0 \in \mathbb{F}_{q^m}$ и $i \in [0, s-1]$ верно соотношение

$$r^{(i)}(x_0) = \sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = i}} \widehat{f}^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}}(x_0)) \prod_{j=1}^{m} \alpha_j^{e_j}.$$

Так как многочлен $\widehat{f}(\boldsymbol{X}) \in V_q^s(m,d)$ ненулевой, а отображение $\gamma_{\boldsymbol{\alpha}}$ задает биекцию между $\mathbb{F}_{q^m}$ и $\mathbb{F}_q^m$, то найдутся $y_0 \in \mathbb{F}_{q^m}$ и $\boldsymbol{w} \in \mathbb{N}^m$, $\deg(\boldsymbol{w}) < s$, такие что $\widehat{f}^{(\boldsymbol{w})}(\gamma_{\boldsymbol{\alpha}}(y_0)) \neq 0$. Из предложения 8 следует, что существует базис $\boldsymbol{\alpha}$, для которого $r^{(\deg(\boldsymbol{w}))}(y_0) \neq 0$. Значит, для этого же $\boldsymbol{\alpha}$ верно $r(T) \neq 0$. Тогда число точек $x_0 \in \mathbb{F}_{q^m}$, для которых выполнено $r^{(i)}(x_0) = 0$ для всех $i \in [0, s-1]$, не превосходит величины $\left\lfloor \dfrac{\widetilde{d}}{s} \right\rfloor$. Следовательно, число точек $x_0 \in \mathbb{F}_{q^m}$, для которых $r^{(<s)}(x_0) \neq \mathbf{0}$, не меньше $\underline{d} = q^m - \left\lfloor \dfrac{\widetilde{d}}{s} \right\rfloor$. Снова воспользовавшись формулой для подсчета производной $r^{(i)}(x_0)$, заключаем, что число точек $\boldsymbol{z}_0 \in \mathbb{F}_q^m$, для которых $\widehat{f}^{(<s)}(\boldsymbol{z}_0) \neq \mathbf{0}$, не меньше $\underline{d}$.

§ 3. Доказательства вспомогательных утверждений

Доказательство предложения 3. Сначала докажем существование такого многочлена. Рассмотрим многочлен $g(T)$, полученный из $f(T)$ в качестве остатка при делении на $(T^q - T)^s$. Его степень очевидно меньше sq. Отметим, что

$$g(T) = f(T) + h(T)(T^q - T)^s$$

для некоторого $h(T) \in \mathbb{F}_q[T]$. Из свойств производных Хассе (предложения 1 и 2) следует, что вычисление $g^{(i)}(t_0)$ в точке $t_0 \in \mathbb{F}_q$ для всякого $i \in [0, s-1]$ эквивалентно вычислению $f^{(i)}(t_0)$, поскольку $t_0^q = t_0$ для всех $t_0 \in \mathbb{F}_q$.

Предположим, что существует другой многочлен $\widehat{g}(t)$ степени не выше $sq-1$, такой что $\widehat{g}(T) \equiv_s f(T)$. Тогда рассмотрим многочлен $r(T) := \widehat{g}(T) - g(T)$, степень которого не выше $sq-1$. Из определения производной Хассе (см. определение 1) для всякого $t_0 \in \mathbb{F}_q$ имеем

$$r(T) = r(t_0 + (T - t_0)) = \sum_{i \in \mathbb{N}} r^{(i)}(t_0)(T - t_0)^i.$$

С другой стороны, из линейности производной Хассе (предложение 1) следует, что

$$r^{(i)}(t_0) = \widehat{g}^{(i)}(t_0) - g^{(i)}(t_0) = 0 \quad \text{для } i \in [0, s-1].$$

Следовательно, $(T-t_0)^s \mid r(T)$ для всякого $t_0 \in \mathbb{F}_q$, откуда $(T^q-T)^s \mid r(X)$, поскольку

$$\prod_{t_0 \in \mathbb{F}_q} (T - t_0) = T^q - T.$$

Наконец, пусть число s равно степени числа p. Тогда

$$(T^q - T)^s = \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} T^{qj+(s-j)}.$$

В силу предложения 4 имеем, что $\binom{s}{j} \equiv 0 \pmod p$ для $j \in [1, s-1]$. Это означает, что $(T^q - T)^s = T^{qs} + (-T)^s$. ▲

Доказательство предложения 5. Пусть $\lambda \in \mathbb{F}_q$, а $z(\boldsymbol{X}) \in V_q^s(d, m)$. В силу линейности

$$(f + \lambda z) \circ \gamma(T) = f \circ \gamma(T) + \lambda(z \circ \gamma(T))$$

достаточно рассматривать лишь многочлен $f(\boldsymbol{X})$, который является в точности $(m, d)_q^s$-хорошим мономом $\boldsymbol{X}^{\boldsymbol{v}}$, $\boldsymbol{v} \in \mathbb{N}^m$. Распишем получившийся многочлен $g(T)$ от одной переменной в таком случае:

$$g(T) = \prod_{j=1}^{m} (a_j T + b_j)^{v_j} = \prod_{j=1}^{m} \sum_{e_j=0}^{v_j} \binom{v_j}{e_j} a_j^{e_j} b_j^{v_j - e_j} T^{e_j} =$$

$$= \sum_{e_1 \in [0, v_1], \ldots, e_m \in [0, v_m]} T^{\sum\limits_{j=1}^{m} e_j} \prod_{j=1}^{m} \binom{v_j}{e_j} \alpha_j^{e_j} b_j^{v_j - e_j}.$$

Далее воспользуемся предложением 4, из которого следует, что коэффициент при $T^{\sum\limits_{j=1}^{m} e_j}$ может быть отличен от нуля только в том случае, когда для вектора $\boldsymbol{e} = (e_1, \ldots, e_m)$ выполнено отношение порядка $\boldsymbol{e} \leqslant_p \boldsymbol{v}$. Поскольку моном $\boldsymbol{X}^{\boldsymbol{v}}$ является $(m, d)_q^s$-хорошим, то выполнено неравенство $\operatorname{Mod}_q^s(\deg(\boldsymbol{e})) < d$ для интересующих нас векторов $\boldsymbol{e}$. Наконец, воспользуемся наблюдением (1). Получаем, что многочлен $h(T)$, s-эквивалентный $g(T)$, имеет степень не выше $\operatorname{Mod}_q^s(\deg(\boldsymbol{e}))$, где $\boldsymbol{e} \leqslant_p \boldsymbol{v}$. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Hirschfeld J.W.P., Korchmáros G., Torres F.* Algebraic Curves over a Finite Field. Princeton: Princeton Univ. Press, 2008.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988.
3. *Lucas E.* Théorie des fonctions numériques simplement périodiques // Amer. J. Math. 1878. V. 1. № 4. P. 289–321. https://doi.org/10.2307/2369373
4. *Guo A., Kopparty S., Sudan M.* New Affine-Invariant Codes from Lifting // Proc. 4th Conf. on Innovations in Theoretical Computer Science (ITCS'13). Berkeley, CA, USA. Jan. 9–12, 2013. P. 529–540. https://doi.org/10.1145/2422436.2422494
5. *Розенблюм М.Ю., Цфасман М.А.* Коды для m-метрики // Пробл. передачи информ. 1997. Т. 33. № 1. С. 55–63. http://mi.mathnet.ru/ppi359
6. *Kopparty S., Saraf S., Yekhanin S.* High-Rate Codes with Sublinear-Time Decoding // J. ACM. 2014. V. 61. № 5. Art. 28. P. 1–20. https://doi.org/10.1145/2629416
7. *Holzbaur L., Polyanskaya R., Polyanskii N., Vorobyev I., Yaakobi E.* Lifted Reed–Solomon Codes and Lifted Multiplicity Codes // IEEE Trans. Inform. Theory. 2021. V. 67. № 12. P. 8051–8069. https://doi.org/10.1109/TIT.2021.3116520

8. *Wu L.* Revisiting the Multiplicity Codes: A New Class of High-Rate Locally Correctable Codes // Proc. 53rd Annu. Allerton Conf. on Communication, Control, and Computing. Monticello, IL, USA. Sept. 29 – Oct. 2, 2015. P. 509–513. https://doi.org/10.1109/ALLERTON.2015.7447047
9. *Li R., Wootters M.* Lifted Multiplicity Codes and the Disjoint Repair Group Property // IEEE Trans. Inform. Theory. 2021. V. 67. № 2. P. 716–725. https://doi.org/10.1109/TIT.2020.3034962
10. *Nielsen R.R.* List Decoding of Linear Block Codes. Ph.D. Thesis. Dept. Math., Tech. Univ. Denmark, Lyngby, Denmark, Sept. 2001. Available from https://orbit.dtu.dk/en/publications/list-decoding-of-linear-block-codes.
11. *Kopparty S.* List-Decoding Multiplicity Codes // Theory Comput. 2015. V. 11. Art. 5. P. 149–182. https://doi.org/10.4086/toc.2015.v011a005
12. *Guruswami V., Wang C.* Optimal Rate List Decoding via Derivative Codes // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (Proc. 14th Int. Workshop, APPROX'2011, and 15th Int. Workshop, RANDOM'2011. Princeton, NJ, USA. Aug. 17–19, 2011). Lect. Notes Comput. Sci. V. 6845. Berlin: Springer, 2011. P. 593–604. https://doi.org/10.1007/978-3-642-22935-0_50
13. *Guo A., Kopparty S.* List-Decoding Algorithms for Lifted Codes // IEEE Trans. Inform. Theory. 2016. V. 62. № 5. P. 2719–2725. https://doi.org/10.1109/TIT.2016.2538766
14. *Kopparty S.* Some Remarks on Multiplicity Codes // Discrete Geometry and Algebraic Combinatorics (AMS Special Session on Discrete Geometry and Algebraic Combinatorics. San Diego, CA, USA. Jan. 11, 2013). Providence, RI: Amer. Math. Soc., 2014. P. 155–176.

Полянский Никита Андреевич
Сколковский институт науки и технологий (Сколтех)
nikita.polyansky@gmail.com

Поступила в редакцию
05.03.2021
После доработки
17.11.2021
Принята к публикации
23.11.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391.1 : 519.725

© 2021 г. **Ф.И. Соловьева**

О ПЕРЕСЕЧЕНИИ КОДОВ ТИПА РИДА – МАЛЛЕРА[1]

Двоичный код с параметрами и основными свойствами классического кода Рида – Маллера $RM_{r,m}$ порядка r будем называть кодом типа Рида – Маллера порядка r и обозначать через $LRM_{r,m}$. Класс таких кодов содержит семейство кодов, полученных конструкцией Пулатова, а также классические линейные и $\mathbb{Z}_4$-линейные коды Рида – Маллера. Исследуется проблема пересечения кодов типа Рида – Маллера. Доказано, что для любого четного k в интервале $0 \leqslant k \leqslant 2^{2^{\sum_{i=0}^{r-1}\binom{m-1}{i}}}$ существуют коды $LRM_{r,m}$ порядка r длины 2^m, пересечение которых равно k. Доказано также, что существуют два кода типа Рида – Маллера порядка r длины 2^m, пересечение которых равно $2k_1k_2$, где $1 \leqslant k_s \leqslant |RM_{r-1,m-1}|$, $s \in \{1,2\}$, для любой допустимой длины, начиная с 16.

Ключевые слова: код Рида – Маллера, код типа Рида – Маллера, задача о пересечении кодов, коды Пулатова, компоненты кода Рида – Маллера, i-компонента, свитчинг, свитчинговая конструкция кодов.

DOI: 10.31857/S0555292321040057

§ 1. Введение

Векторное пространство размерности n над полем Галуа $GF(2)$, снабженное метрикой Хэмминга, будем обозначать через $\mathbb{F}^n$. Основные определения см. в [1].

Напомним определение и основные свойства классического двоичного линейного кода *Рида – Маллера порядка* r, который будем обозначать через $RM_{r,m}$, а его выколотый код – через $RM^*_{r,m}$. Код Рида – Маллера определяется для любых $1 \leqslant m$, $0 \leqslant r \leqslant m$, как совокупность всех векторов длины 2^m, отвечающих булевым функциям степени не более r от m переменных. Код $RM_{r,m}$ имеет следующие параметры: длина кода равна $n = 2^m$, мощность 2^k, где $k = \sum\limits_{i=0}^{r}\binom{m}{i}$, кодовое расстояние 2^{m-r}. Код $RM_{r,m}$ *антиподален*, т.е. для любого кодового слова x вектор $\bar{x} = x + \mathbf{1}^n$ также принадлежит коду, здесь и далее $\mathbf{1}^n$ – вектор длины n, состоящий из единичных координат, а знаком $+$ обозначено сложение по модулю 2. Код $RM_{r,m}$ является дуальным к коду $RM_{m-1-r,m}$, $0 \leqslant r \leqslant m$, и кроме того, $RM_{r-1,m} \subset RM_{r,m}$. Коды $RM_{m-2,m}$ и $RM_{1,m}$ являются расширенными кодами Хэмминга и Адамара соответственно. Код Рида – Маллера $RM_{r,m}$ порождается множеством своих кодовых слов минимального веса (см. [1, § 13.5]).

Двоичный антиподальный код с параметрами классического кода Рида – Маллера $RM_{r,m}$ порядка r назовем *кодом типа Рида – Маллера* порядка r и будем обозначать через $LRM_{r,m}$. Этот код не обязательно линеен. Класс данных кодов совпадает с обширным классом расширенных совершенных кодов при $r = m-2$. По определению все коды $RM_{r,m}$ являются кодами $LRM_{r,m}$. При $r \in \{0, m-1, m\}$ код $LRM_{r,m}$

[1] Работа выполнена в рамках государственного задания ИМ СО РАН (проект № 0314-2019-0016).

совпадает с кодом $RM_{r,m}$. Несколько конструкций кодов $LRM_{r,m}$ любых порядков, т.е. содержащих не только совершенные расширенные коды и коды Адамара, были предложены в работах [2–4]. Заметим, что, как и код $RM_{r,m}$ длины $n = 2^m$, код типа Рида – Маллера с теми же параметрами, полученный конструкцией Пулатова [3] из кодов Рида – Маллера длины $n = 2^{m-1}$ с нелинейной функцией λ (см. определение кода в § 2), образует ортогональный массив силы $2^r - 1$. Класс кодов типа Рида – Маллера содержит важный класс $\mathbb{Z}_4$-линейных кодов Рида – Маллера (см. их конструкции в работах [5, 6]). Групповые коды над кольцом $\mathbb{Z}_4$, являющиеся прообразами этих $\mathbb{Z}_4$-линейных кодов Рида – Маллера под действием отображения Грэя, имеют базисы минимального веса (см. [7]).

В настоящей работе исследуется следующий вопрос: каков размер пересечения двух кодов $LRM_{r,m}$? Аналогичная проблема ранее, в 1994 г., была выдвинута в [8] для совершенных кодов.

Исследованиям проблемы пересечения совершенных q-ичных кодов и двоичных кодов Адамара посвящено достаточно много статей (см. обзор [9] и библиографию в нем). Полное решение проблемы пересечения двоичных кодов Хэмминга найдено в работе [10]. В статье [11] решена проблема пересечения для всех q-ичных линейных кодов, $q \geqslant 2$, включая двоичные коды Рида – Маллера. Согласно [11] для некоторой подстановки π длины 2^m код Рида – Маллера $RM_{r,m}$ порядка r удовлетворяет условию $|RM_{r,m} \cap \pi(RM_{r,m})| \geqslant 2$, где минимальное значение 2 достижимо только при $r \leqslant [(m-1)/2]$. В [10] показано, что для каждого $m \geqslant 3$ существуют два нелинейных совершенных двоичных кода длины $2^m - 1$, пересекающихся по двум кодовым словам. В работе [12] доказано, что для любых чисел k_1 и k_2, таких что $1 \leqslant k_s \leqslant 2^{(n+1)/2-\log(n+1)}$, $s = 1, 2$, найдутся совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geqslant 4$, удовлетворяющие $|C_1 \cap C_2| = 2k_1k_2$. В [13] показано, что для любого четного числа k в интервале $0 \leqslant k \leqslant 2^{n+1-2\log(n+1)}$ существуют совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geqslant 4$, такие что $\eta(C_1, C_2) = k$. Следует отметить, что совокупности чисел пересечений, полученных в [12] и [13], не покрывают друг друга. В работе [14] исследовались пересечения кодов Адамара. В [15] полностью решена проблема пересечения аддитивных ($\mathbb{Z}_4$- и $\mathbb{Z}_2\mathbb{Z}_4$-линейных), расширенных и нерасширенных совершенных кодов. Аналогичный результат был получен для аддитивных ($\mathbb{Z}_4$- и $\mathbb{Z}_2\mathbb{Z}_4$-линейных) кодов Адамара (дуальных кодов к $\mathbb{Z}_4$- и $\mathbb{Z}_2\mathbb{Z}_4$-линейным совершенным кодам соответственно) в работе [16].

Очевидно, что мощность пересечения расширений кодов C_1 и C_2 посредством общей проверки на четность остается такой же, как и для исходных кодов, причем верно также и обратное.

В данной работе доказано (см. теорему 2), что для любого четного k в интервале $0 \leqslant k \leqslant 2^{2\sum_{i=0}^{r-1}\binom{m-1}{i}}$ существуют $LRM_{r,m}$ коды C и C' с длинами 2^m, пересечение которых равно k. Доказано также (см. теорему 3), что существуют два кода $LRM_{r,m}$ порядка r, имеющих длину по крайней мере 16 и пересекающихся по $2k_1k_2$ кодовым словам, где $1 \leqslant k_s \leqslant |RM_{r-1,m-1}|$, $s \in \{1, 2\}$. Отметим, что полученные результаты обобщают результаты работ [8, 11–13]. Кроме того, значение 2 также достижимо среди указанных множеств чисел пересечений кодов типа Рида – Маллера, и как и в случае совершенных кодов, совокупности чисел пересечений, представленных в этих теоремах, не покрывают друг друга. Для получения данных результатов потребовалось изучить свойства i-компонент кода Рида – Маллера и использовать свитчинговую конструкцию Пулатова [3] для построения кодов типа Рида – Маллера.

§ 2. Необходимые определения и понятия

В этом параграфе рассмотрим необходимые определения и понятия и напомним конструкцию Пулатова [3] для кодов типа Рида – Маллера.

Число η для кодов C_1 и C_2 назовем *числом пересечения* этих кодов. Обозначим выколотый код типа Рида – Маллера порядка r через $LRM^*_{r,m}$. Приведем конструкцию Пулатова. Пусть $LRM^*_{r,m-1}$ и $LRM^*_{r-1,m-1}$ – два выколотых кода типа Рида – Маллера порядков r и $r-1$ длины $2^{m-1}-1$, мощностей 2^{k_r} и $2^{k_{r-1}}$, с кодовыми расстояниями $2^{m-r-1}-1$ и $2^{m-r}-1$ соответственно, где $k_r = \sum\limits_{i=0}^{r} \binom{m-1}{i}$ и $k_{r-1} = \sum\limits_{i=0}^{r-1} \binom{m-1}{i}$. Пусть λ – произвольная функция, действующая на множестве кодовых слов кода $LRM^*_{r-1,m-1}$ со значениями в множестве $\{0,1\}$. Для любых r и $m \geqslant 2$, $0 < r < m$, код, полученный итеративной конструкцией Пулатова

$$\{(x+y, x, |x| + \lambda(y)) : \ x \in LRM^*_{r,m-1}, \ y \in LRM^*_{r-1,m-1}\}, \tag{1}$$

является выколотым кодом типа Рида – Маллера длины $n = 2^m - 1$ с числом кодовых слов 2^k, где $k = \sum\limits_{i=0}^{r} \binom{m}{i}$, и кодовым расстоянием, равным $2^{m-r}-1$.

Если $LRM^*_{r,m-1} = RM^*_{r,m-1}$, $LRM^*_{r-1,m-1} = RM^*_{r-1,m-1}$ и $\lambda \equiv 0$, то код, полученный конструкцией Пулатова, является выколотым линейным кодом Рида – Маллера $RM^*_{r,m}$ порядка r. Конструкция Пулатова (1) для выколотых кодов типа Рида – Маллера является обобщением известной свитчинговой конструкции Васильева для совершенных двоичных кодов [17], а для расширенного случая – известной конструкции Плоткина [1].

Пусть C – произвольный код длины n с кодовым расстоянием d, $d \geqslant 3$. Для $i \in \{1, \ldots, n\}$ через $G_i(C)$ обозначим граф с множеством кодовых слов кода C в качестве множества вершин и с множеством ребер $\{(x,y) : \ d(x,y) = d, \ x_i \neq y_i\}$. Компонента связности K графа $G_i(C)$ называется *i-компонентой* кода C. При этом говорят, что код $C' = (C \setminus K) \cup (K + e_i)$ получен из кода C методом *свитчинга i-компоненты K*. Здесь и далее e_i обозначает вектор веса один пространства $\mathbb{F}^n$, имеющий единицу только в i-й координатной позиции. Код C' имеет те же параметры, что и код C: длину, мощность и кодовое расстояние. Метод свитчинга i-компонент оказался весьма эффективным для построения и исследования свойств совершенных кодов и позволил решить ряд проблем, стоящих для совершенных q-ичных кодов, $q \geqslant 2$ (см. обзоры в работах [9, 18]).

Рассмотрим конструкцию Пулатова (1) в случае, когда $LRM^*_{r,m-1}$ и $LRM^*_{r-1,m-1}$ – выколотые линейные коды Рида – Маллера $RM^*_{r,m-1}$ и $RM^*_{r-1,m-1}$ соответственно, а λ – произвольная функция из множества кодовых слов кода $RM^*_{r-1,m-1}$ в множество $\{0,1\}$:

$$LRM^*_{r,m} = \{(x+y, x, |x| + \lambda(y)) : \ x \in RM^*_{r,m-1}, \ y \in RM^*_{r-1,m-1}\}. \tag{2}$$

Через $\mathbf{0}^n$ обозначим вектор длины n, состоящий из нулевых координат.

Согласно [3] множество

$$R_n = \{(x, x, |x|) : \ x \in RM^*_{r,m-1}\}$$

является n-компонентой кодов $LRM^*_{r,m}$ и $RM^*_{r,m}$, где $n = 2^m - 1$. Легко видеть, что код (2) может быть представлен в виде

$$LRM^*_{r,m} = \left(RM^*_{r,m} \Big\setminus \bigcup_{y \in RM^*_{r-1,m-1}, \, \lambda(y)=1} R^y_n \right) \cup \bigcup_{y \in RM^*_{r-1,m-1}, \, \lambda(y)=1} (R^y_n + e_n), \tag{3}$$

где $R^y_n = R_n + (y, \mathbf{0}^{2^{m-1}})$, $y \in RM^*_{r-1,m-1}$. Код (3) задан свитчинговой конструкцией, так как получен из кода $RM^*_{r,m}$ свитчингами n-компонент R^y_n и $R^y_n + e_n$ для каждого y, удовлетворяющего $\lambda(y) = 1$.

Теорема 1. *Для любых r и m, $2 \leqslant m$, $0 \leqslant r < m$, существуют два выколотых кода типа Рида – Маллера порядка r длины $2^m - 1$ (а также их расширения длины 2^m посредством общей проверки на четность), имеющих пересечение η, где*

$$\eta \in \left\{ |RM^*_{r,m-1}|, 2|RM^*_{r,m-1}|, \ldots, (|RM^*_{r-1,m-1}| - 1)|RM^*_{r,m-1}| \right\}.$$

Доказательство. Для получения требуемых чисел пересечений выколотых кодов типа Рида – Маллера рассмотрим следующие пары кодов длины $2^m - 1$: выколотый код Рида – Маллера порядка r и выколотые коды типа Рида – Маллера порядка r, определенные в (3). Пусть A – произвольное подмножество кодовых слов кода $RM^*_{r-1,m-1}$ и $\lambda(y) = 1$ в случае $y \in A$. Поскольку по определению R^y_n выполняется $|R^y_n| = |RM^*_{r,m-1}|$, то легко видеть, что коды

$$RM^*_{r,m} \quad \text{и} \quad \left(RM^*_{r,m} \setminus \bigcup_{y \in A} R^y_n \right) \cup \bigcup_{y \in A} (R^y_n + e_n)$$

пересекаются по

$$(|RM^*_{r-1,m-1}| - |A|)|RM^*_{r,m-1}|$$

кодовым словам. Выбирая подмножество A в коде $RM^*_{r-1,m-1}$ произвольным образом, т.е. варьируя число кодовых слов y в $RM^*_{r-1,m-1}$, удовлетворяющих $\lambda(y) = 1$, из конструкции (3) немедленно получаем, что следующие числа пересечений η являются достижимыми для выколотых кодов типа Рида – Маллера:

$$\eta \in \left\{ |RM^*_{r,m-1}|, 2|R^*_{r,m-1}|, \ldots, (|RM^*_{r-1,m-1}| - 1)|RM^*_{r,m-1}| \right\}.$$

Заметим, что $(|RM^*_{r-1,m-1}| - 1)|RM^*_{r,m-1}| = |RM^*_{r,m}| - |RM^*_{r,m-1}|$.

Такое же множество чисел пересечений получаем и для расширенных кодов $LRM_{r,m}$. ▲

Отметим, что аналогичный результат был получен для совершенных кодов в работе [8].

§ 3. Пересечение кодов типа Рида – Маллера

В данном параграфе будут получены два существенно более богатых класса чисел пересечений для кодов типа Рида – Маллера, чем те, которые дает прямой свитчинговый метод, описанный в теореме 1. Для достижения этой цели построим два кода типа Рида – Маллера специального вида, используя конструкцию Пулатова (1) для расширенного случая.

Прежде чем привести описание кодов, рассмотрим три вспомогательных леммы, одна из которых взята из работы [13]. Пусть π – циклическая подстановка длины $n/2$, здесь и всюду далее $n = 2^m$. Пусть φ обозначает отображение $x \mapsto x + \pi(x)$ из $\mathbb{F}^{n/2}$ в себя, и пусть $\mathbb{F}^{n/2} = \mathbb{F}^{n/2}_0 \cup \mathbb{F}^{n/2}_1$, где $\mathbb{F}^{n/2}_0$ и $\mathbb{F}^{n/2}_1$ – множества всех векторов четного и нечетного весов в $\mathbb{F}^{n/2}$ соответственно. Обозначим через $\ker(\varphi)$ ядро отображения φ, а через $\dim(\ker(\varphi))$ – его размерность. Для полноты изложения приведем с доказательством лемму из [13] о свойствах отображения φ, которые потребуются нам в дальнейшем.

Лемма 1. *Отображение φ линейно и обладает следующими свойствами*:

1. $\dim(\ker(\varphi)) = 1$;
2. $\varphi(\mathbb{F}^{n/2}) = \mathbb{F}^{n/2}_0$;
3. $\varphi(\mathbb{F}^{n/2}) = V \cup (z + V)$, *где* $V = \varphi(\mathbb{F}^{n/2}_0)$, $z = \varphi(u)$ *для некоторого* $u \in \mathbb{F}^{n/2}_1$ *и* $z + V = \varphi(\mathbb{F}^{n/2}_1)$.

Доказательство. 1. Очевидно, что φ – линейное отображение, и так как $x = \pi(x)$ только при $x \in \{\mathbf{0}^{n/2}, \mathbf{1}^{n/2}\}$, то размерность ядра этого отображения равна 1.

2. Поскольку $w(x) = w(\pi(x))$ для любого $x \in \mathbb{F}^{n/2}$, то справедливо $\varphi(\mathbb{F}^{n/2}) = \mathbb{F}_0^{n/2}$, и размерность $\varphi(\mathbb{F}^{n/2})$, очевидно, равна $\frac{n}{2} - \dim(\ker(\varphi)) = \frac{n}{2} - 1$.

Аналогично $\dim(\varphi(\mathbb{F}_0^{n/2})) = \dim(\varphi(\mathbb{F}^{n/2})) - \dim(\ker(\varphi)) = \frac{n}{2} - 2$.

3. Так как $V = \varphi(\mathbb{F}_0^{n/2})$ – подпространство пространства $\varphi(\mathbb{F}^{n/2})$, то $\varphi(\mathbb{F}^{n/2}) = V \cup (z+V)$, где $z+V$ – класс смежности подпространства V с лидером z. Поскольку $z + V \subset \varphi(\mathbb{F}^{n/2})$, то найдется вектор u в $\mathbb{F}_1^{n/2}$, такой что $z = \varphi(u)$. ▲

Лемма 2. *Для любого кодового слова y из кода $RM_{r-1,m}$, $0 \leqslant r \leqslant m-1$, $4 \leqslant m$, $n = 2^m$, существуют ровно два различных кодовых слова $u, \bar{u} \in RM_{r,m}$, удовлетворяющих $y = u + \pi(u)$ и $y = \bar{u} + \pi(\bar{u})$, где $\bar{u} = u + \mathbf{1}^n$.*

Доказательство. Заметим, что в силу леммы 1 размерность ядра отображения φ равна единице. Отсюда, если существует одно решение для y, т.е. найдется некоторый u, такой что $y = u + \pi(u)$, то решений ровно два, так как антиподальный к u вектор $\bar{u} = u + \mathbf{1}^n$ также удовлетворяет $y = \bar{u} + \pi(\bar{u})$. Поэтому достаточно ограничиться в лемме доказательством существования одного вектора u.

Доказательство проведем индукцией по $m \geqslant 3$. При $m = 3$ имеем вложение кодов Рида–Маллера $RM_{0,3} \subset RM_{1,3} \subset RM_{2,3}$. Непосредственной проверкой для любого кодового слова y кода $RM_{1,3}$, который является расширенным кодом Хэмминга длины 8, легко найти два кодовых слова u и $\bar{u}$ из $RM_{2,3}$, удовлетворяющих $y = u + \pi(u)$ и $y = \bar{u} + \pi(\bar{u})$. Для этого достаточно решить для любого $y = (y_1, \ldots, y_8) \in RM_{1,3}$ систему линейных уравнений $u_i + u_{(i+1) \bmod 8} = y_i$, $i = 1, 2, \ldots, 8$. Положим $u_1 = 0$. Легко проверить, что в этом случае система имеет единственное решение u, $u \in RM_{2,3}$, что дает представление $y = u + \pi(u)$. Второе решение также получаем однозначно, полагая $u_1 = 1$, т.е. имеем $y = \bar{u} + \pi(\bar{u})$. Для наглядности приведем для каждого вектора y^i, $y^i \in RM_{1,3}$, соответствующий вектор u^i, $u^i \in RM_{2,3}$, $i = 1, \ldots, 16$:

$$
\begin{aligned}
y^1 &= (0,0,0,0,0,0,0,0), & u^1 &= (0,0,0,0,0,0,0,0);\\
y^2 &= (1,1,1,1,0,0,0,0), & u^2 &= (0,1,0,1,1,1,1,1);\\
y^3 &= (1,1,0,0,1,1,0,0), & u^3 &= (0,1,1,1,0,1,1,1);\\
y^4 &= (1,0,1,0,1,0,1,0), & u^4 &= (0,0,1,1,0,0,1,1);\\
y^5 &= (1,1,0,0,0,0,1,1), & u^5 &= (0,1,1,1,1,1,0,1);\\
y^6 &= (1,0,1,0,0,1,0,1), & u^6 &= (0,0,1,1,1,0,0,1);\\
y^7 &= (1,0,0,1,1,0,0,1), & u^7 &= (0,0,0,1,0,0,0,1);\\
y^8 &= (1,0,0,1,0,1,1,0), & u^8 &= (0,0,0,1,1,0,1,1);\\
y^9 &= (1,1,1,1,1,1,1,1), & u^9 &= (0,1,0,1,0,1,0,1);\\
y^{10} &= (0,0,0,0,1,1,1,1), & u^{10} &= (0,0,0,0,1,0,1,0);\\
y^{11} &= (0,0,1,1,0,0,1,1), & u^{11} &= (0,0,1,0,0,0,1,0);\\
y^{12} &= (0,1,0,1,0,1,0,1), & u^{12} &= (0,1,1,0,0,1,1,0);\\
y^{13} &= (0,0,1,1,1,1,0,0), & u^{13} &= (0,0,1,0,1,0,0,0);\\
y^{14} &= (0,1,0,1,1,0,1,0), & u^{14} &= (0,1,1,0,1,1,0,0);\\
y^{15} &= (0,1,1,0,0,1,1,0), & u^{15} &= (0,1,0,0,0,1,0,0);\\
y^{16} &= (0,1,1,0,1,0,0,1), & u^{16} &= (0,1,0,0,1,1,1,0).
\end{aligned}
$$

Для кода $RM_{0,3}$ выполняется $\mathbf{1}^8 = u + \pi(u)$, где вектор $u = (0,1,0,1,0,1,0,1)$ принадлежит $RM_{1,3}$.

Пусть при $m-1$ лемма верна, т.е. для каждого кодового слова x произвольного кода Рида – Маллера длины 2^{m-1} порядка не более $m-2$ существует $u \in RM_{r,m-1}$, удовлетворяющий $x = u + \pi(u)$. Докажем справедливость леммы для m и любого $0 \leqslant r \leqslant m-1$.

Согласно конструкции Плоткина для линейных кодов Рида – Маллера имеем

$$RM_{r,m} = \{(x+y, x) :\ x \in RM_{r,m-1},\ y \in RM_{r-1,m-1}\}. \tag{4}$$

По предположению индукции для кодовых слов кодов $RM_{r,m-1}$ и $RM_{r-1,m-1}$ выполняется утверждение леммы.

Обозначим через Π подстановку на 2^m координатных позициях, являющуюся циклическим сдвигом на одну координатную позицию вправо.

Рассмотрим произвольный вектор $(x+y, x)$ кода $RM_{r,m}$. Возможны следующие случаи.

Случай 1. Пусть $x \neq \mathbf{0}^{n/2}$, $x \in RM_{r,m-1}$, $y = \mathbf{0}^{n/2}$, $y \in RM_{r-1,m-1}$, где $n = 2^m$. В этом случае согласно (4) имеем $(x,x) \in RM_{r,m}$ для любого x из $RM_{r,m-1}$. По предположению индукции для вектора x найдется вектор u, такой что $x = u + \pi(u)$. Отсюда

$$(x,x) = (u + \pi(u), u + \pi(u)) = (u,u) + (\pi(u), \pi(u)) = (u,u) + \Pi((u,u)). \tag{5}$$

Случай 2. Пусть $x = \mathbf{0}^{n/2}$, $x \in RM_{r,m-1}$, а $y \neq \mathbf{0}^{n/2}$, $y \in RM_{r-1,m-1}$. По предположению индукции для вектора y найдется вектор $u \in RM_{r,m-1}$, такой что $y = u + \pi(u)$.

Рассмотрим подслучай, когда последняя координата вектора u равна 0. Тогда первая координата вектора $\pi(u)$ равна 0. Следовательно,

$$\begin{aligned}(y, \mathbf{0}^{n/2}) &= (u + \pi(u), \mathbf{0}^{n/2}) = (u, \mathbf{0}^{n/2}) + (\pi(u), \mathbf{0}^{n/2}) = \\ &= (u, \mathbf{0}^{n/2}) + \Pi((u, \mathbf{0}^{n/2})),\end{aligned} \tag{6}$$

где $(u, \mathbf{0}^{n/2}) \in RM_{r,m}$.

Если последняя координата вектора u равна 1, то первая координата вектора $\pi(u)$ кода $\pi(RM_{r,m-1})$ равна 1. В этом случае воспользуемся антиподальностью кода $\pi(RM_{r,m-1})$, согласно которой вектор $\pi(u) + \mathbf{1}^{n/2}$ принадлежит коду $\pi(RM_{r,m-1})$, и следовательно, $(u, \mathbf{1}^{n/2}) \in RM_{r,m}$. Отсюда

$$\begin{aligned}(y, \mathbf{0}^{n/2}) &= (u + \pi(u), \mathbf{1}^{n/2} + \pi(\mathbf{1}^{n/2})) = (u, \mathbf{1}^{n/2}) + (\pi(u), \pi(\mathbf{1}^{n/2})) = \\ &= (u, \mathbf{1}^{n/2}) + \Pi((u, \mathbf{1}^{n/2})).\end{aligned} \tag{7}$$

Случай 3. Пусть $x \neq \mathbf{0}^{n/2}$, где $x \in RM_{r,m-1}$ и $y \neq \mathbf{0}^{n/2}$, $y \in RM_{r-1,m-1}$. По предположению индукции для кодовых слов x и y найдутся два вектора u и v, соответственно, удовлетворяющих $x = u + \pi(u)$ и $y = v + \pi(v)$. Отсюда

$$\begin{aligned}(x+y, x) &= (u + \pi(u) + v + \pi(v), u + \pi(u)) = \\ &= [(u,u) + (\pi(u), \pi(u))] + [(v, \mathbf{0}^{n/2}) + (\pi(v), \mathbf{0}^{n/2})].\end{aligned}$$

Таким образом здесь, как и в случае 1, для вектора (x,x) справедливо (5). Для вектора $(y, \mathbf{0}^{n/2})$ аналогично случаю 2 имеем (6) при $v_{n/2} = 0$, а при $v_{n/2} = 1$ справедливо (7). Отсюда при $v_{n/2} = 0$ вытекает требуемое, а именно:

$$(x+y, x) = (u + v, u) + \Pi((u+v, u)).$$

При $v_{n/2} = 1$ с учетом антиподальности кода Рида – Маллера $RM_{r,m-1}$ имеем

$$(x+y,x) = (u,u) + \Pi((u,u)) + (y, \mathbf{0}^{n/2}) =$$
$$= (u,u) + \Pi((u,u)) + (v, \mathbf{1}^{n/2}) + \Pi((v, \mathbf{1}^{n/2})) =$$
$$= (u+v, u+\mathbf{1}^{n/2}) + \Pi((u+v, u+\mathbf{1}^{n/2})). \quad \blacktriangle$$

Пусть $RM_{r-1,m-1} = P_0 \cup P_1$, где P_0 и P_1 – подкоды кода $RM_{r-1,m-1}$ с одинаковыми и различными первыми двумя координатными позициями соответственно. Пусть ν – транспозиция первых двух координатных позиций векторов из $\mathbb{F}^{n/2}$. Тогда

$$\nu(RM_{r-1,m-1}) = P_0 \cup \nu(P_1),$$

так как $\nu(P_0) = P_0$.

Рассмотрим вектор

$$z = (1,0,1,0,\ldots,1,0) \tag{8}$$

длины $n/2$ с чередующимися координатами, равными 1 и 0. Этот вектор принадлежит коду Адамара $RM_{1,m-1}$, заданному порождающей матрицей, столбцы которой представлены в лексикографическом порядке, и следовательно, принадлежит любому коду Рида – Маллера ненулевого порядка, содержащему этот код Адамара. В частности, $z \in RM_{r-1,m-1}$, и следовательно, вектор z может быть взят в качестве представителя класса смежности P_1 по подкоду P_0, т.е. $P_1 = z + P_0$. Значит, вектор

$$\nu(z) = (0,1,1,0,\ldots,1,0) \in \nu(P_1) \tag{9}$$

может быть взят в качестве представителя класса смежности $\nu(P_1)$ по подкоду P_0, т.е. $\nu(P_1) = \nu(z) + P_0$.

Лемма 3. *Пусть y и y' – произвольные кодовые слова кодов P_0 и $\nu(P_1)$ либо P_1 и $\nu(P_1)$ соответственно. Тогда существуют ровно два различных вектора u и $\bar{u} = u + \mathbf{1}^{n/2}$, удовлетворяющих $y + y' = u + \pi(u)$ и $y + y' = \bar{u} + \pi(\bar{u})$. Более того, оба вектора u и $\bar{u}$ имеют нечетный вес.*

Доказательство. Случай 1. Пусть $y \in P_0$ и $y' \in \nu(P_1)$. Поскольку $\mathbf{0}^{n/2} \in P_0$, достаточно рассмотреть доказательство для $\nu(z) = (0,1,1,0,\ldots,1,0)$ – представителя класса смежности $\nu(P_1)$, поскольку для P_0 справедлива лемма 2. Решая систему линейных уравнений $\nu(z_i) = u_i + u_{i+1}$, $i = 1,2,\ldots,n/2$, полагая $u_1 = 0$, однозначно находим $u = (u_1,\ldots,u_{n/2})$ и $\pi(u)$:

$$u = (0,1,0,0,1,1,\ldots,1,1,0,0), \quad \pi(u) = (0,0,1,0,0,1,1,\ldots,1,1,0),$$

где u и $\pi(u)$ – векторы нечетного веса. Аналогично ищем $\bar{u}$, полагая в этом случае $\bar{u}_1 = 1$:

$$\bar{u} = (1,0,1,1,0,0,\ldots,1,1), \quad \pi(\bar{u}) = (1,1,0,1,1,0,\ldots,0,1),$$

где u и $\pi(u)$ – векторы нечетного веса.

Случай 2. Рассмотрим $y \in P_1$ и $y' \in \nu(P_1)$. Векторы $y \in P_1$ и $y' \in \nu(P_1)$ представимы в виде $y = \widetilde{y} + z$ и $y' = y'' + \nu(z)$ соответственно, где z и $\nu(z)$ определены выше в (8) и (9). Здесь $\widetilde{y}, y'' \in P_0$. Тогда

$$y + y' = \widetilde{y} + y'' + \nu(z) + z,$$

где $\widetilde{y} + y'' \in P_0$. Отсюда с учетом случая 1 данной леммы имеем $\widetilde{y} + y'' + \nu(z) = u + \pi(u)$, где u – вектор нечетного веса. В силу того, что вектор $z \in P_1 \subset RM_{1,m-1}$, по лемме 2

справедливо $z = u' + \pi(u')$, где $u' \in RM_{2,m-1}$, в частности, u' имеет четный вес. Следовательно, для $y + y'$ верно требуемое. ▲

Определим коды $D_\lambda(RM_{r-1,m-1})$ и $D_{\lambda'}(\nu(RM_{r-1,m-1}))$ длины n, используя конструкцию Пулатова для расширенных кодов типа Рида – Маллера.

Первый код имеет вид

$$D_\lambda(RM_{r-1,m-1}) = D_0 \cup D_1,$$
$$D_0 = \bigcup_{y \in RM_{r-1,m-1},\ \lambda(y)=0} \{(x+y, x) :\ x \in RM_{r,m-1},\ y \in RM_{r-1,m-1}\},$$
$$D_1 = \bigcup_{y \in RM_{r-1,m-1},\ \lambda(y)=1} \{(x+y+e_i, x+e_i) :\ x \in RM_{r,m-1},\ y \in RM_{r-1,m-1}\},$$

где λ – произвольная функция, действующая из множества кодовых слов кода $RM_{r-1,m-1}$ в множество $\{0,1\}$, а i – произвольный элемент множества $\{1, 2, \ldots, n/2\}$.

Код $D_{\lambda'}(\nu(RM_{r-1,m-1})) = D'_0 \cup D'_1$ определим, используя подстановки π, ν и произвольную функцию λ', действующую из кода $\nu(RM_{r-1,m-1})$ в множество $\{0,1\}$:

$$D'_0 = \bigcup_{\substack{y \in \nu(RM_{r-1,m-1}),\\ \lambda'(y)=0}} \{(x+y, \pi(x)) :\ x \in RM_{r,m-1},\ y \in \nu(RM_{r-1,m-1})\},$$
$$D'_1 = \bigcup_{\substack{y \in \nu(RM_{r-1,m-1}),\\ \lambda'(y)=1}} \{(x+y+e_i, \pi(x+e_i)) :\ x \in RM_{r,m-1},\ y \in \nu(RM_{r-1,m-1})\},$$

здесь i – то же самое число, что и для кода $D_\lambda(RM_{r-1,m-1})$.

Используя отображение φ, свойства которого описаны в лемме 1, и подстановку ν, введем следующие обозначения:

$$N_0 = |RM_{r-1,m-1} \cap \varphi(RM_{r,m-1})|, \quad N_1 = |RM_{r-1,m-1} \cap \varphi(\mathbb{F}_1^{n/2})|,$$
$$M_0 = |\nu(RM_{r-1,m-1}) \cap \varphi(RM_{r,m-1})|, \quad M_1 = |\nu(RM_{r-1,m-1}) \cap \varphi(\mathbb{F}_1^{n/2})|.$$

Кроме того, далее нам потребуются связанные с сужениями функций λ и λ' на введенные подкоды кодов $RM_{r-1,m-1}$ и $\nu(RM_{r-1,m-1})$ следующие числа:

$$\mu_0 = \big|\{y \in RM_{r-1,m-1} \cap \varphi(RM_{r,m-1}) :\ \lambda(y) = 0\}\big|,$$
$$\mu_1 = \big|\{y \in RM_{r-1,m-1} \cap \varphi(\mathbb{F}_1^{n/2}) :\ \lambda(y) = 0\}\big|,$$
$$\gamma_0 = \big|\{y \in \nu(RM_{r-1,m-1}) \cap \varphi(RM_{r,m-1}) :\ \lambda'(y) = 0\}\big|,$$
$$\gamma_1 = \big|\{y \in \nu(RM_{r-1,m-1}) \cap \varphi(\mathbb{F}_1^{n/2}) :\ \lambda'(y) = 0\}\big|.$$

Лемма 4. *Число векторов, лежащих в пересечении кодов $D_\lambda(RM_{r-1,m-1})$ и $D_{\lambda'}(\nu(RM_{r-1,m-1}))$, равно*

$$2\big(\mu_0\gamma_0 + \mu_1\gamma_1 + (N_0 - \mu_0)(M_1 - \gamma_1) + (N_1 - \mu_1)(M_0 - \gamma_0)\big),$$

где $m \geqslant 4$.

Доказательство. Рассмотрим произвольные кодовые слова этих кодов. В силу определения обоих кодов для совпадения этих кодовых слов имеются только следующие две возможности. Если $(x+y, x) \in D_\lambda(RM_{r-1,m-1})$ и $(x'+y', \pi(x')) \in \in D_{\lambda'}(\nu(RM_{r-1,m-1}))$, где x, x' – векторы четного веса, то

$$(x+y, x) = (x'+y', \pi(x')). \tag{10}$$

Если $(x+y+e_i, x+e_i) \in D_\lambda(RM_{r-1,m-1})$ и $(x'+y'+e_i, \pi(x'+e_i)) \in D_{\lambda'}(\nu(RM_{r-1,m-1}))$, где векторы $x+e_i, x'+e_i$ имеют нечетный вес, то справедливо

$$(x+y+e_i, x+e_i) = (x'+y'+e_i, \pi(x'+e_i)), \tag{11}$$

где $x, x' \in RM_{r,m-1}$, $y \in RM_{r-1,m-1}$ и $y' \in \nu(RM_{r-1,m-1})$. В первом случае имеем $\lambda(y) = \lambda'(y') = 0$, во втором случае $\lambda(y) = \lambda'(y') = 1$.

Рассмотрим первый случай. В этой ситуации имеем $x = \pi(x')$, и значит,

$$y + y' = x + x' = x' + \pi(x') = \varphi(x').$$

Следовательно, равенство (10) эквивалентно системе линейных уравнений

$$\begin{cases} x = x' + y + y', \\ \varphi(x') = y + y'. \end{cases} \tag{12}$$

Возможны следующие подслучаи.

а) Пусть $y, y' \in P_0$ либо $y \in P_1$, а $y' \in P_0$, где множества P_0 и P_1 определены выше, $RM_{r-1,m-1} = P_0 \cup P_1$. Тогда в обоих ситуациях имеем $y + y' \in RM_{r-1,m-1}$, и по лемме 2 для вектора $y + y' \in P_0$ существуют два кодовых слова кода $RM_{r,m-1}$, удовлетворяющих второму уравнению в (12), т.е. $\varphi(x') = y + y'$. Следовательно, система уравнений (12) имеет ровно два различных решения относительно x, x' при фиксированном кодовом слове $y + y'$ из $RM_{r-1,m-1}$.

б) Пусть $y \in P_0$, $y' \in \nu(P_1)$ либо $y \in P_1$, а $y' \in \nu(P_1)$, где подстановка ν определена выше (является транспозицией первых двух координат кодовых слов кода $RM_{r-1,m-1}$), $\nu(RM_{r-1,m-1}) = P_0 \cup \nu(P_1)$. Тогда по лемме 3 для фиксированного вектора $y + y'$ найдутся ровно два решения u, таких что $\varphi(u) = y + y'$, причем оба вектора имеют нечетный вес. Но поскольку $y + y' = x + x'$, где $x + x' \in RM_{r,m-1}$, и в частности, этот вектор имеет четный вес, то система уравнений (12) не имеет решений относительно $x, x' \in RM_{r,m-1}$.

Во втором случае, т.е. при $\lambda(y) = \lambda'(y') = 1$, имеем $x + e_i = \pi(x' + e_i)$, следовательно,

$$y + y' = x + x' = x' + e_i + x + e_i = x' + e_i + \pi(x' + e_i) = \varphi(x' + e_i).$$

С учетом этого равенство (11) эквивалентно системе линейных уравнений

$$\begin{cases} x = x' + y + y', \\ \varphi(x' + e_i) = y + y'. \end{cases} \tag{13}$$

Аналогично рассуждениям, проведенным в первом случае, имеется два различных решения системы (13) относительно $x + e_i, x' + e_i$ в случае $y + y' \in \nu(P_1)$ и нет решений в противном случае. ▲

Лемма 5. *Для кодов $D_\lambda(RM_{r-1,m-1})$ и $D_{\lambda'}(\nu(RM_{r-1,m-1}))$, $m \geqslant 4$, справедливо*

$$N_0 = |RM_{r-1,m-1}|, \quad N_1 = 0, \quad M_0 = M_1 = \frac{1}{2}|RM_{r-1,m-1}|.$$

Доказательство. Из леммы 2 вытекает, что $RM_{r-1,m-1} \subset \varphi(RM_{r,m-1})$, значит, $N_0 = |RM_{r-1,m-1}|$, и как следствие, получаем $N_1 = 0$.

Докажем, что $M_0 = M_1 = \frac{1}{2}|RM_{r-1,m-1}|$. С этой целью рассмотрим векторы $u = (0,1,0,0,1,1,\ldots,1,1,0,0)$ и $\pi(u) = (0,0,1,0,0,1,1,\ldots,1,1,0)$, полученные в доказательстве леммы 3, а также их сумму $\varphi(u) = u + \pi(u) = (0,1,1,0,\ldots,1,0)$. Вектор $u + \pi(u)$ равен вектору $\nu(z)$ из леммы 3, т.е. представителю класса смежности $\nu(P_1)$, поскольку $\nu^{-1}(u + \pi(u)) = (1,0,1,0,\ldots,1,0) = z \in RM_{1,m-1} \subset RM_{r-1,m-1}$ для

любого $1 < r \leqslant m-1$. Так как вектор u имеет нечетный вес, то по лемме 3 выполняется $\nu(RM_{r-1,m-1}) \cap \varphi(\mathbb{F}_1^{n/2}) = \nu(P_1)$. Отсюда $M_1 = \frac{1}{2}|\nu(RM_{r-1,m-1})|$, и поскольку $|\nu(RM_{r-1,m-1})| = |RM_{r-1,m-1}|$, то $M_0 = M_1 = \frac{1}{2}|RM_{r-1,m-1}|$. ▲

Теорема 2. *Для любого четного k в интервале*

$$0 \leqslant k \leqslant 2^{2\sum\limits_{i=0}^{r-1}\binom{m-1}{i}}$$

существуют два кода типа Рида – Маллера порядка r длины 2^m, $m \geqslant 4$, пересечение которых равно k.

Доказательство. Для кодов типа Рида – Маллера $C = D_\lambda(RM_{r-1,m-1})$ и $C' = D_{\lambda'}(\nu(RM_{r-1,m-1}))$, имеющих порядок r и длину $n = 2^m$, из лемм 4 и 5 получаем следующую формулу для числа их пересечения η:

$$\eta(C, C') = 2\Big(\mu_0\gamma_0 + (|RM_{r-1,m-1}| - \mu_0)\Big(\frac{1}{2}|RM_{r-1,m-1}| - \gamma_1\Big)\Big).$$

Варьируя значения функций λ и λ' произвольным образом, т.е. выбирая числа μ_0, γ_i произвольным образом в пределах

$$0 \leqslant \mu_0 \leqslant |RM_{r-1,m-1}|, \quad 0 \leqslant \gamma_i \leqslant \frac{1}{2}|\nu(RM_{r-1,m-1}|, \quad i = 1, 2,$$

с учетом $|\nu(RM_{r-1,m-1})| = |RM_{r-1,m-1}|$ получаем требуемое. ▲

Полагая код C' равным $D_{\lambda'}(RM_{r-1,m-1})$ и оставляя код $C = D_\lambda(RM_{r-1,m-1})$ без изменения, согласно лемме 5 имеем

$$N_0 = M_0 = |RM_{r-1,m-1}|, \quad N_1 = M_1 = 0,$$

т.е. в этом случае выполняется $\mu_1 = \gamma_1 = 0$. Отсюда и из леммы 4 вытекает

Теорема 3. *Для любых чисел k_1 и k_2, удовлетворяющих условиям*

$$1 \leqslant k_s \leqslant 2^{\sum\limits_{i=0}^{r-1}\binom{m-1}{i}}, \quad s \in \{1, 2\},$$

существуют два кода типа Рида – Маллера порядка r длины 2^m, $m \geqslant 4$, пересечение которых равно $2k_1k_2$.

Нетрудно убедиться в том, что множества чисел пересечений кодов типа Рида – Маллера порядка r длины 2^m, полученных в теоремах 2 и 3, не покрывают друг друга.

Автор выражает свою признательность И.Ю. Могильных за плодотворные дискуссии и рецензенту за ряд полезных замечаний, позволивших улучшить изложение настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Liu C.L., Ong B.G., Ruth G.R.* A Construction Scheme for Linear and Non-linear Codes // Discrete Math. 1973. V. 4. № 2. P. 171–184. https://doi.org/10.1016/0012-365X(73)90080-0
3. *Пулатов А.К.* Нижняя оценка сложности схемной реализации для одного класса кодов // Дискретный анализ. Вып. 25. Новосибирск: Ин-т матем. СО АН СССР, 1974. С. 56–61.

4. *Соловьева Ф.И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. Новосибирск: Ин-т матем. СО АН СССР, 1981. С. 65–76.
5. *Соловьева Ф.И.* О $\mathbb{Z}_4$-линейных кодах с параметрами кодов Рида – Маллера // Пробл. передачи информ. 2007. Т. 43. № 1. С. 32–38. http://mi.mathnet.ru/ppi4
6. *Pujol J., Rifà J., Solov'eva F.I.* Construction of $\mathbb{Z}_4$-Linear Reed–Muller Codes // IEEE Trans. Inform. Theory. 2009. V. 55. № 1. P. 99–104. https://doi.org/10.1109/TIT.2008.2008143
7. *Solov'eva F.I.* Minimum Weight Bases for Quaternary Reed–Muller Codes // Сиб. электрон. матем. изв. 2021. V. 18. № 2. P. 1358–1366. https://doi.org/10.33048/semi.2021.18.103
8. *Etzion T., Vardy A.* Perfect Binary Codes: Constructions, Properties and Enumeration // IEEE Trans. Inform. Theory. 1994. V.40. № 3. P. 754–763. https://doi.org/10.1109/18.335887
9. *Соловьева Ф.И.* Обзор по совершенным кодам // Математические вопросы кибернетики. Вып. 18. М.: Физматлит, 2013. С. 5–34.
10. *Etzion T., Vardy A.* On Perfect Codes and Tilings: Problems and Solutions // SIAM J. Discrete Math. 1998. V. 11. № 2. P. 205–223. https://doi.org/10.1137/S0895480196309171
11. *Bar-Yahalom E., Etzion T.* Intersection of Isomorphic Linear Codes // J. Combin. Theory. Ser. A. 1997. V. 80. № 2. P. 247–256. https://doi.org/10.1006/jcta.1997.2805
12. *Avgustinovich S.V., Heden O., Solov'eva F.I.* On Intersections of Perfect Binary Codes // Bayreuth. Math. Schr. 2005. № 71. P. 1–6.
13. *Avgustinovich S.V., Heden O., Solov'eva F.I.* On Intersection Problem for Perfect Binary Codes // Des. Codes Cryptogr. 2006. V. 39. № 3. P. 317–322. https://doi.org/10.1007/s10623-005-4982-8
14. *Phelps K.T., Villanueva M.* Intersection of Hadamard Codes // IEEE Trans. Inform. Theory. 2007. V. 53. № 5. P. 1924–1928. https://doi.org/10.1109/TIT.2007.894687
15. *Rifá J., Solov'eva F.I., Villanueva M.* On the Intersection of $\mathbb{Z}_2\mathbb{Z}_4$-Additive Perfect Codes // IEEE Trans. Inform. Theory. 2008. V. 54. № 3. P. 1346–1356. https://doi.org/10.1109/TIT.2007.915917
16. *Rifá J., Solov'eva F.I., Villanueva M.* On the Intersection of $\mathbb{Z}_2\mathbb{Z}_4$-Additive Hadamard Codes // IEEE Trans. Inform. Theory. 2009. V. 55. № 4. P. 1766–1774. https://doi.org/10.1109/TIT.2009.2013037
17. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
18. *Solov'eva F.I.* Switchings and Perfect Codes // Numbers, Information and Complexity. Boston: Springer, 2000. P. 311–324. https://doi.org/10.1007/978-1-4757-6048-4_25

Соловьева Фаина Ивановна
Институт математики им. С.Л. Соболева
СО РАН, Новосибирск
sol@math.nsc.ru

Поступила в редакцию
25.06.2021
После доработки
10.11.2021
Принята к публикации
10.11.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 2021 Вып. 4

УДК 621.391 : 519.2

 Н.Г. Докучаев

К ОДНОЗНАЧНОСТИ ВОССТАНОВЛЕНИЯ ДАННЫХ ПРИ ОГРАНИЧЕНИЯХ НА МНОЖЕСТВО СПЕКТРАЛЬНЫХ ЗНАЧЕНИЙ

Изучаются возможности восстановления данных для конечных последовательностей при ограничениях на возможное множество спектральных значений. Соответствующие последовательности плотны в пространстве всех последовательностей. Показано, что множество однозначности для них может быть одноточечным.

Ключевые слова: восстановление данных, сжатие данных, Z-преобразование, дискретное преобразование Фурье, дискретизация множества спектральных значений.

DOI: 10.31857/S0555292321040069

§ 1. Введение

Статья изучает возможности восстановления данных для конечных последовательностей при ограничениях на значения спектра, возникающих при специальной дискретизации области возможного диапазона спектра. Обычно такого рода восстановимость ассоциируется с ограничениями на носитель спектра, такими как разреженность носителя спектра или наличие областей с нулевыми значениями спектра (см., например, работы [1–5] и ссылки в них).

Настоящая статья исследует задачи восстановления и сжатия данных данных в условиях ограничений только на множество спектральных значений. Показано, что существуют классы последовательностей, которые плотны в пространстве всех последовательностей и в то же время имеют однотонные множества однозначности (теорема 2). Эти классы определяются ограничениями, налагаемыми специальной дискретизацией возможного множества спектральных значений. Подразумеваемая процедура восстановления потребует решения уравнения диофантового типа. Хотя эффективное численное решение в больших измерениях неосуществимо, эта теорема может привести к некоторым новым выводам о вычислительных ограничениях для эффективности сжатия данных.

§ 2. Определения и постановка задачи

Для целого числа $N > 0$ обозначим через $\mathcal{X}$ множество отображений $x\colon D \to \mathbb{C}$, где $D \triangleq \{0, 1, \dots, N-1\}$. Это множество мы также будем ассоциировать с векторным пространством $\mathbb{C}^N$. Будем рассматривать $\mathcal{X}$ как линейное нормированное пространство со стандартной нормой из $\mathbb{C}^N$.

Рассмотрим следующее Z-преобразование $Y = Zy$ для $y \in \mathcal{X}$:

$$Y(z) = \sum_{k=0}^{N-1} z^{-k} y_k, \quad z \in \mathbb{C}.$$

Также будем рассматривать дискретное преобразование Фурье (ДПФ) – отображение $\mathcal{F}\colon \mathcal{X} \to \mathcal{X}$, такое что $Y = \mathcal{F}y$ задано условиями

$$Y_d = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i\omega_k d} y_k, \quad d = 0, 1, \ldots, N-1,$$

где $i = \sqrt{-1}$,

$$\omega_k = \frac{2\pi}{N} k.$$

Определение 1. Пусть заданы подмножество U в $\mathbb{C}$ и подмножество $\mathcal{Y}$ в $\mathcal{X}$.

1. Если любой $y \in \mathcal{Y}$ однозначно определяется значениями $Y|_U$, где $Y = Zy$, то будем говорить, что U является множеством однозначности для $\mathcal{Y}$ в частотной области относительно Z-преобразования;
2. Если любой элемент $y \in \mathcal{Y}$ однозначно определяется значениями $Y|_U$, где $Y = \mathcal{F}y$, то будем говорить, что U является множеством однозначности для $\mathcal{Y}$ в частотной области относительно дискретного преобразования Фурье.

Приведем несколько примеров множеств однозначности.

Пример 1. Следующие множества $U \subset \mathbb{C}$ являются множествами однозначности для $\mathcal{X}$ в частотной области относительно Z-преобразования:

1. Любое открытое множество $U \subset \mathbb{C}$;
2. Множество $U = \{e^{i\omega},\ \omega \in [0, 2\pi)\}$.

Будем обозначать через $|U|$ количество элементов в множестве U.

Пример 2. Пусть задано $S \in \{1, \ldots, N-1\}$. Пусть $\mathcal{X}_S$ – множество всех $y \in \mathcal{X}$, таких что $\sum\limits_{k \in D} \mathbb{I}_{\{y_k \neq 0\}} \leqslant S$.

1. Если N – простое число, то любое множество $U \subset D$, такое что $|U| = 2S$, является множеством однозначности для $\mathcal{Y}_S$ в частотной области относительно дискретного преобразования Фурье (см., например, [1, теорема 1.1]);
2. Пусть $U \subset D$ таково, что $|U| = 2S$ и существуют такие $u, v \in D$, что

$$U = \{u, u+v, u+2v, \ldots, u+(2S-1)v\}.$$

Тогда U является множеством однозначности для $\mathcal{Y}_S$ в частотной области относительно дискретного преобразования Фурье (см., например, [6]).

Ниже мы покажем, что существуют примеры одноэлементных множеств однозначности для некоторых классов процессов, допускающих конструктивное описание через ограничения на возможное множество спектральных значений.

§ 3. Случай частично наблюдаемого Z-преобразования

В этом параграфе мы рассмотрим случай, где для данного $x \in \mathcal{X}$ наблюдаются некоторые отсчеты Z-преобразования $X = \mathcal{Z}x$.

Обозначим через $\mathcal{X}_{\text{alg}}$ множество всех $x \in \mathcal{X}$, таких что члены соответствующих последовательностей $\operatorname{Re} x$ и $\operatorname{Im} x$ являются алгебраическими числами (см., например, [7, гл. 1]).

В частности, класс $\mathcal{X}_{\text{alg}}$ включает в себя все $x \in \mathcal{X}$, такие что их компоненты имеют рациональные вещественные и мнимые части. Очевидно, что множество $\mathcal{X}_{\text{alg}}$ всюду плотно в $\mathcal{X}$.

Теорема 1. *Пусть для некоторого $\widehat{z} \in \mathbb{C}$ его модуль и аргумент являются алгебраическими числами, т.е. $\widehat{z} = re^{i\omega}$, где $r > 0$ и $\omega \neq 0$ – вещественные алгебраические числа. Тогда одноточечное множество $U = \{\widehat{z}\}$ является множеством однозначности для $\mathcal{X}_{\text{alg}}$ в частотной области относительно Z-преобразования.*

Доказательство. Для доказательства достаточно показать, что если $\widetilde{y}, \overline{y} \in \in \mathcal{X}_{\text{alg}}$ и $\widehat{Y}(\widehat{z}) = \overline{Y}(\widehat{z})$ для $\widehat{Y} = \mathcal{Z}\widehat{y}$, $\overline{Y} = \mathcal{Z}\overline{y}$, то $\widetilde{y} = \overline{y}$. Следовательно, достаточно показать, что если $Y(\widehat{z}) = 0$ для $y = (y_0, \ldots, y_{N-1}) \in \mathcal{X}_{\text{alg}}$ и $Y = \mathcal{Z}y$, то y равен нулю. Покажем это.

Имеем

$$0 = Y(\widehat{z}) = \sum_{k=0}^{N-1} r^{-k} e^{-i\omega k} y_k. \tag{1}$$

Поскольку $y \in \mathcal{X}_{\text{alg}}$, компоненты вектора y являются алгебраическими числами. Кроме того, коэффициенты $r^{-k}y_k$ являются алгебраическими числами. Из теоремы Линдемана – Вейерштрасса (см. [7, гл. 1, теорема 1.4]) следует, что $r^{-k}y_k = 0$ для всех k, что и завершает доказательство. ▲

§ 4. Случай частично наблюдаемого ДПФ

В этом параграфе мы рассматриваем ситуацию, где для данного $x \in \mathcal{X}$ наблюдаются некоторые компоненты дискретного преобразования Фурье $X = \mathcal{F}x$.

Зафиксируем $d \in \{1, \ldots, N-1\}$ и зададим вектор $a = (a_0, a_1, \ldots, a_{N-1}) \in \mathbb{R}^N$, компоненты которого являются алгебраическими числами. Зададим вектор $\zeta(a, d) = = (\zeta_0(a, d), \ldots, \zeta_{N-1}(a, d)) \in \mathcal{X}$ таким образом, что

$$\zeta_k(a, d) = e^{i(a_k - \omega_k)d}.$$

Обозначим через $\widehat{\mathcal{Y}}_{a,d}$ набор всех $y = (y_0, y_1, \ldots, y_{N-1}) \in \mathcal{X}$, таких что $x = = (x_0, x_1, \ldots, x_{N-1}) \in \mathcal{X}_{\text{alg}}$, где $x_k = \zeta_k(a, d)y_k$, $k = 0, 1, \ldots, N-1$.

Теорема 2. *Для любого $d \in \{1, \ldots, N-1\}$ одноточечное множество $U = \{d\}$ является множеством однозначности для класса $\widehat{\mathcal{Y}}_{a,d}$ в частотной области относительно дискретного преобразования Фурье.*

Замечание 1. Поскольку a_k могут быть сколь угодно близкими к π, то и коэффициенты $\zeta_k(a, d)$ могут быть сколь угодно близкими к 1. Отсюда следует, что для любого $\varepsilon > 0$ существует a, такое что множество $\widehat{\mathcal{Y}}_{a,d}$ является ε-плотным в $\mathcal{X}$, и множество $\bigcup\limits_{a} \widehat{\mathcal{Y}}_{a,d}$ всюду плотно в $\mathcal{X}$.

Доказательство теоремы 2. Рассмотрим $y = (y_0, \ldots, y_{N-1}) \in \widehat{\mathcal{Y}}_{a,d}$, $Y = = (Y_0, \ldots, Y_{N-1}) = \mathcal{F}y$, а также $x = (x_0, \ldots, x_{N-1}) \in \mathcal{X}_{\text{alg}}$, такой что $x_k = \zeta_k(a, d)y_k$. Имеем

$$Y_d = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i\omega_k d} y_k = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-ia_k d} \zeta_k(a, d) y_k.$$

Следовательно,

$$Y_d = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-ia_k d} x_k. \tag{2}$$

Для доказательства теоремы достаточно показать, что для любого $y \in \widehat{\mathcal{Y}}_{a,d}$ существует единственный вектор $x = (x_0, \ldots, x_{N-1}) \in \mathcal{X}_{\text{alg}}$, удовлетворяющий (2). Для

этого достаточно показать, что если $\widehat{Y}_d = \widetilde{Y}_d$ для некоторых $\widehat{y}, \widetilde{y} \in \widehat{\mathcal{Y}}_{a,d}$, $\widehat{Y} = \mathcal{F}(\widehat{y})$ и $\widetilde{Y} = \mathcal{F}(\widetilde{y})$, то $\widehat{y} = \widetilde{y}$.

Теперь можно завершить доказательство. Достаточно показать, что если $Y_d = 0$ для $y \in \widehat{\mathcal{Y}}_{a,d}$ и $Y = \mathcal{F}y$, то уравнение (2) имеет только нулевое решение x в $\mathcal{X}_{\text{alg}}$. Покажем это.

Поскольку $y \in \widehat{\mathcal{Y}}_{a,d}$, из определений следует, что x_k – алгебраические числа для $k = 0, 1, \ldots, N-1$. Кроме того, a_k – также алгебраические числа. Снова применив теорему Линдемана – Вейерштрасса (см. [7, гл. 1, теорема 1.4]), получаем, что $x_k = 0$ для всех k, что и завершает доказательство. ▲

О возможности восстановления данных. Теорема 2 и ее доказательство формально ведут к следующей процедуре сжатия и декодирования данных: (i) последовательность $x \in \mathcal{X}$ можно аппроксимировать некоторым достаточно близким вектором $y \in \widehat{\mathcal{Y}}_{a,d}$; этот вектор y восстанавливается из решения $\{x_k\}$ уравнения (2).

Далее, существование решения $\{x_k\}$ уравнения (2) в нашем подходе заведомо предполагается, поскольку x_k являются параметрами исследуемого процесса y; это решение приводит к восстановлению y. Мы показали, что это решение единственно. Однако теорема 2 не приводит к эффективному численному алгоритму.

Если класс $\mathcal{X}_{\text{alg}}$ заменить конечным множеством, то решение могло бы быть получено полным перебором. Очевидно, что результат об однозначности остается верным, если класс $\mathcal{X}_{\text{alg}}$ заменить его конечным подмножеством.

Приведем пример таких подмножеств.

Будем использовать обозначение

$$\lfloor a \rfloor = \begin{cases} \{k \in \mathbb{Z} : \ a \in [k, k+1)\} & \text{для } a \in \mathbb{R},\ a \geqslant 0, \\ \{k \in \mathbb{Z} : \ a \in (k-1, k]\} & \text{для } a \in \mathbb{R},\ a < 0. \end{cases}$$

Для положительных целых чисел ν и μ зададим $\rho_{\nu,\mu}(a) = \nu^{-\mu} \lfloor \nu^{\mu} a \rfloor$ для $a \in \mathbb{R}$ и

$$\rho_{\nu,\mu}(z) = \rho_{\nu,\mu}(\operatorname{Re} z) + i\rho_{\nu,\mu}(\operatorname{Im} z) \quad \text{для } z \in \mathbb{C}.$$

Определим множество $\mathcal{X}^{\mu,\nu,M}$ как множество "округленных" последовательностей $x \in \mathcal{X}$, таких что $\max\limits_t |x(t)| \leqslant M$ и $x(t) = \rho_{\nu,\mu}(x(t))$. Это множество конечно, и уравнение (2) представляет собой вариант диофантова уравнения. Для определенного диапазона значений N, M, μ, ν решение может быть получено полным перебором. Постоянно растущие доступные вычислительные мощности позволяют увеличивать значения N, M, μ и ν.

Далее, перебор может быть сокращен при наличии дополнительных наблюдений, поскольку эти наблюдения порождают дополнительные уравнения, ограничивающие перебор.

Предположим, что в условиях и обозначениях доказательства теоремы 2 доступны дополнительные наблюдения Y_m для $m \in \widehat{D} \cup \{d\}$, где $\widehat{D}$ – подмножество множества D. Здесь $Y = \mathcal{F}y$, и вектор $y = (y_0, \ldots, y_{N-1}) \in \mathcal{X}$ таков, что $y_k = \zeta_k(a, d)x_k$ для $x \in X^{\mu,\nu,M}$. В этом случае уравнение (2) можно дополнить уравнениями

$$Y_m = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i\omega_k m} \frac{x_k}{\zeta_k(a,d)}, \quad m \in \widehat{D}.$$

Полученная расширенная система имеет единственное решение, поскольку уравнение (2) имеет единственное решение; тем не менее, включение дополнительных уравнений может помочь сократить поиск.

Другая возможность сократить поиск – рассматривать последовательности с дополнительными ограничениями, такими как как ограничение снизу на количество нулей для x или X, рассматривавшееся в [1, 2].

§ 5. Заключительные замечания

Обычно возможности восстановления и экстраполяции данных рассматриваются в связи с вырожденностью спектра, например, ограниченностью полосы частот, наличием пропусков в спектре и разреженностью спектра. Теоремы 1 и 2 предлагают изучить ограничения на возможные значения спектра. Эти теоремы устанавливают существование плотных множеств последовательностей, которые однозначно восстанавливаются по значениям спектра только в одной точке. Возможные значения спектра последовательности из этого класса определяются специальным типом дискретизации; ограниченность диапазона или наличие пропусков в спектре не требуются.

Теоремы 1 и 2 не дают эффективного численного алгоритма, поскольку решение уравнения (2) затруднительно. Для некоторых более узких классов лежащих в основе процессов уравнение (2) может быть решено с помощью перебора, как упоминалось выше. Эта задача выходит за рамки данной статьи; обзор некоторых связанных методов, а также некоторые ссылки можно найти, например, в [8].

СПИСОК ЛИТЕРАТУРЫ

1. *Candés E., Romberg J., Tao T.* Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information // IEEE Trans. Inform. Theory. 2006. V. 52. № 2. P. 489–509. https://doi.org/10.1109/TIT.2005.862083
2. *Candés E., 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
3. *Dokuchaev N.* On Recovery of Discrete Time Signals from Their Periodic Subsequences // Signal Process. 2019. V. 162. P. 180–188. https://doi.org/10.1016/j.sigpro.2019.04.008
4. *Dokuchaev N.* On Linear Weak Predictability with Single Point Spectrum Degeneracy // Appl. Comput. Harmon. Anal. 2021. V. 53. P. 116–131. https://doi.org/10.1016/j.acha.2021.01.005
5. *Olevskii A.M., Ulanovskii A.* Functions with Disconnected Spectrum: Sampling, Interpolation, Translates. Providence, RI: Amer. Math. Soc., 2016.
6. *Venkataramani R., Bresler Y.* Sub-Nyquist Sampling of Multiband Signals: Perfect Reconstruction and Bounds on Aliasing Error // Proc. 1998 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'98). May 12–15, 1998. Seattle, WA, USA. V. 3. P. 1633–1636. https://doi.org/10.1109/ICASSP.1998.681767
7. *Baker A.* Transcendental Number Theory. London/New York: Cambridge Univ. Press, 1975.
8. *Smart N.P.* The Algorithmic Resolution of Diophantine Equations. New York: Cambridge Univ. Press, 1998.

Докучаев Николай Геннадьевич
Институт ZJU-UIUC (Чжэцзянский университет / Иллинойский университет в Урбане-Шампейне), Чжэцзянский университет, Хайнин, провинция Чжэцзян, Китай
Dokuchaev@intl.zju.edu.cn

Поступила в редакцию
18.08.2021
После доработки
10.10.2021
Принята к публикации
08.11.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391 : 519.176

© 2021 г. **Н.А. Дубинин**

НОВЫЕ ОЦЕНКИ ТУРАНОВСКОГО ТИПА ДЛЯ ГРАФОВ ДЖОНСОНА

Получена новая оценка числа ребер в индуцированных подграфах графов Джонсона.

Ключевые слова: теорема Турана, дистанционные графы, графы Джонсона.

DOI: 10.31857/S0555292321040070

§ 1. Введение

В данной статье рассматривается граф $G(n, r, s)$, вершины которого – r-элементные подмножества множества $\{1, 2, \ldots, n\}$, а ребро между двумя вершинами проводится в том случае, если размер пересечения соответствующих подмножеств равен s. Другое определение графа $G(n, r, s)$ следующее: вершинами графа являются вершины единичного куба в n-мерном пространстве, имеющие в координатной записи ровно r единиц, а ребро между двумя вершинами проводится, когда расстояние между ними равно $\sqrt{2(r-s)}$. Понятно, что эти две формулировки эквивалентны.

Графы $G(n, r, s)$ называются графами Джонсона. Они играют огромную роль в задачах комбинаторной геометрии (см., например, [1–3], где описаны, среди прочего, контрпримеры к гипотезе Борсука, основанные на графах Джонсона; далее, см. [1, 4, 5], где обсуждается применение графов Джонсона к задачам о раскрасках метрических пространств; наконец, см. [6–8], где говорится о некоторых смежных задачах, решаемых с помощью графов Джонсона). Также они играют огромную роль в теории кодирования (см., например, [9, 10]), теории Рамсея (см., например, [11–13]) и др.

В настоящей статье изучаются экстремальные свойства графа $G(n, r, s)$. А именно, исследуется число ребер в произвольном подграфе этого графа. Напомним, что *независимое множество вершин* графа G – это такое подмножество его вершин, что никакие две вершины из этого подмножества не соединены ребром. *Числом независимости* $\alpha(G)$ называется наибольшая мощность независимого множества вершин графа.

Обозначим через $r(W)$ количество ребер графа $G = (V, E)$ на множестве $W \subseteq V$. Иными словами,

$$r(W) = |\{(x, y) \in E \mid x \in W,\ y \in W\}|.$$

Также положим

$$r(\ell) = \min_{|W|=\ell,\, W \subseteq V} r(W).$$

Возникает вопрос об изучении данной величины. Классическая теорема Турана 1941 года дает ответ на этот вопрос в общем случае.

Теорема 1. *Пусть G – произвольный граф, α – его число независимости, $\ell > \alpha$. Тогда*

$$r(\ell) \geqslant \frac{\ell^2}{2\alpha} - \frac{\ell}{2}.$$

В доказательстве этой теоремы не учитываются никакие специальные свойства графа G, и более того, эта теорема в общем случае неулучшаема. Однако разумно предположить, что для графов с некоторыми ограничениями оценку можно улучшить. Мы рассматриваем *дистанционные* графы – графы, вершинами которых являются точки в пространстве $\mathbb{R}^n$, а ребро между такими вершинами проводится тогда и только тогда, когда расстояние между ними равно некоторому фиксированному числу. Понятно, что определенный выше граф $G(n, r, s)$ является дистанционным.

Для произвольных дистанционных графов была доказана следующая теорема (см. [14, лемма 4]).

Теорема 2. *Пусть G_n – последовательность дистанционных графов, у которых $V(G_n) \subset \mathbb{R}^n$. Положим $\alpha_n = \alpha(G_n)$. Пусть W_n – подмножество множества $V(G_n)$. Тогда если $|W_n| = \ell(n)$ и $n\alpha_n = o(\ell(n))$, то при $n \to \infty$*

$$r(\ell(n)) \geqslant \frac{\ell(n)^2}{\alpha_n}(1 + o(1)).$$

Таким образом, мы видим, что на классе дистанционных графов, образующих последовательности с определенными асимптотическими свойствами, оценка Турана улучшается примерно в два раза. Можно предположить, что на еще более узком классе дистанционных графов $G(n, r, s)$ оценка допускает дальнейшее улучшение. И действительно, в работе [15] была доказана следующая теорема (см. также [16,17]).

Теорема 3. *Рассмотрим граф $G(n, 3, 1)$. Пусть функция $\ell\colon \mathbb{N} \to \mathbb{N}$ такова, что $n^2 = o(\ell)$ при $n \to \infty$. Тогда существует такая функция $h\colon \mathbb{N} \to \mathbb{N}$, что $h \sim \dfrac{3\ell^2}{2n}$ при $n \to \infty$ и $r(\ell(n)) \geqslant h(n)$ для любого достаточно большого $n \in \mathbb{N}$.*

Чтобы пояснить, как соотносятся между собой результаты теорем 2 и 3, заметим, что $\alpha(G(n, 3, 1)) \in \{n-2, n-1, n\}$ (см. [13]). Это значит, что на своем классе графов теорема 3 в полтора раза сильнее общей теоремы 2. Наш основной результат будет обобщением теоремы 3 на случай фиксированных r и s с условием, что $r = 2s + 1$ и что $r - s$ – степень простого числа. Очевидно, что параметры теоремы 3 удовлетворяют этим условиям. Заметим, что именно в этих ограничениях на r и s в работе [18] было показано, что $\alpha(G(n, r, s)) \sim n^s \dfrac{(2r - 2s - 1)!}{r!\,(r - s - 1)!}$. Эта запись означает, что существует такая функция $q(n) = (1 + o(1))$, что $\alpha(G(n, r, s)) = q(n)n^s \dfrac{(2r - 2s - 1)!}{r!\,(r - s - 1)!}$. Кроме того, поскольку функция $q(n)$ ограничена, существует такая константа C_0, что $\alpha(G(n, r, s)) \leqslant C_0 n^s$. Такого рода огрубления нам иногда понадобятся. Итак, справедлива

Теорема 4. *Пусть $r = 2s+1$, где $r-s$ – степень простого числа, и пусть $\ell(n)$ – любая функция с ограничением $n^{2s} = o(\ell(n))$. Положим $\alpha_n = \alpha(G(n, r, s))$. Тогда существует такая функция $h\colon \mathbb{N} \to \mathbb{N}$, что $h \sim \dfrac{3\ell(n)^2}{2\alpha_n}$ при $n \to \infty$ и $r(\ell(n)) \geqslant h(n)$.*

В работе [17] Пушняковым доказана следующая

Теорема 5. *Пусть даны числа r, s. Пусть $G_n = G(n, r, s)$. Пусть $\ell = \ell(n) \to \infty$. Тогда*

$$r(\ell) \leqslant (1 + o(1))\frac{\ell^2}{n^s}\frac{C_r^s r!}{2(r-s)!}.$$

Таким образом, отличие нашей новой нижней оценки от известной верхней границы имеет величину порядка константы при фиксированных r, s. Например, в случае, когда $r = 3$, $s = 1$, оценка из теоремы 5 имеет вид $\frac{9}{2}\frac{\ell^2}{n}$, т.е. отличается от воспроизведенной нами оценки Пушнякова всего в 3 раза. Ни для каких других значений r, s ранее нижние оценки, превосходящие результаты теорем 1 и 2, получены не были.

Отметим также, что условие теоремы 4, требующее, чтобы функция ℓ росла быстрее, чем n^{2s}, в случае $r = 3$, $s = 1$, который изучал Пушняков, не является сильно ограничительным. А именно, Пушняков доказал (см. [17]), что в противоположных условиях величина $r(\ell)$ асимптотически равна либо своей нижней границе из теоремы 1, либо своей нижней границе из теоремы 2. В нашем, существенно более общем случае остается достаточно большой диапазон значений функции ℓ, который пока не изучен. Разумеется, в этом диапазоне верны теоремы 1, 2 и 5. Дальнейшие уточнения – дело будущего.

В чем-то наше доказательство будет следовать идеям Пушнякова. Однако будет и значимое количество существенных отличий. Так, для доказательства теоремы 4 нам понадобится вспомогательная лемма, напоминающая утверждение из работы Пушнякова [17].

Лемма. *Пусть параметры r, s и функция ℓ удовлетворяют условиям теоремы 4. Пусть W – произвольное множество вершин графа $G(n, r, s)$, имеющее мощность $\ell(n)$. Пусть Γ – любое наибольшее по мощности независимое множество вершин в подграфе графа $G(n, r, s)$, порожденном вершинами из W. Пусть $w \in W \setminus \Gamma$. Обозначим через $n(\Gamma, w)$ число вершин в множестве Γ, смежных с w. Пусть U_1 и U_2 – множества таких вершин $w \in W \setminus \Gamma$, что $n(\Gamma, w) = 1$ или 2 соответственно. Тогда существует такая константа C_1, что $|U_1 \cup U_2| \leqslant C_1 n^{2s}$.*

Подчеркнем, что константа в лемме будет зависеть только от r и s, но не от ℓ, W и Γ.

В следующем параграфе мы сперва приведем доказательство леммы, а потом – в п. 2.2 – докажем теорему 4. В доказательствах во избежание путаницы нам удобно будет иногда различать обозначения для той или иной вершины u графа $G(n, r, s)$ и отвечающего ей r-элементного подмножества. Последнее мы будем обозначать через $\mathrm{supp}(u)$ и называть *носителем* вершины u.

Отметим, наконец, что близкие результаты для случая произвольных дистанционных графов на плоскости можно найти в работе [19].

§ 2. Доказательства

2.1. Доказательство леммы. Докажем сначала, что существует такая константа C_2, что $|U_1| \leqslant C_2 n^{s+1}$. Выберем вершину $u \in \Gamma$. Пусть

$$U_{1,u} = \{w : \ w \in W \setminus \Gamma, \ n(\Gamma, w) = 1 \text{ и } (w, u) \in E\}.$$

Тогда U_1 – объединение множеств $U_{1,u}$ по всем $u \in \Gamma$. Зафиксируем u и оценим мощность $U_{1,u}$. Пусть $v \in U_{1,u}$. Носители вершин u и v пересекаются по s элементам, и выбрать эти элементы можно C_r^s способами. Следующий, $(s+1)$-й, элемент носителя v выбираем $n - r$ способами. Для этих выбранных $s + 1$ элементов существует не более одного способа выбрать все остальные. Пусть это не так, тогда существует

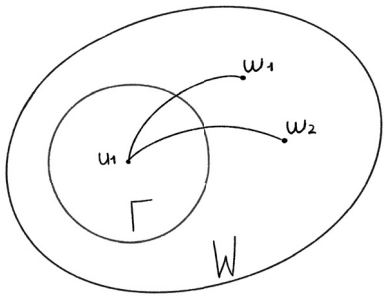

Рис. 1. Вершины с единственным ребром в Γ

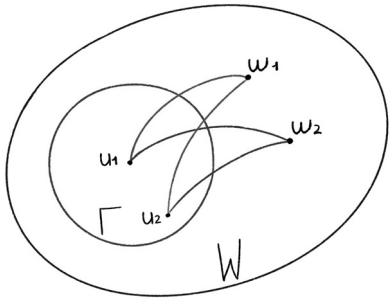

Рис. 2. Галочки

как минимум две вершины $v_1 = \{v^1, v^2, \ldots, v^{s+1}, a, \ldots\}$ и $v_2 = \{v^1, v^2, \ldots, v^{s+1}, b, \ldots\}$. Заметим, что между ними нет ребра, поскольку их носители пересеклись как минимум по $s+1$ элементам. Также заметим, что каждая из вершин имеет лишь одно ребро с множеством Γ, и это ребро ведет в выбранную вершину u (см. рис. 1). Тогда множество $(\Gamma \setminus \{u\}) \cup \{v_1, v_2\}$ не имеет ребер, т.е. является независимым, и имеет мощность больше, чем мощность множества Γ, что противоречит предположению максимальности Γ. Итак,

$$|U_1| \leqslant C_r^s |\Gamma| n \leqslant C_r^s \alpha_n n \sim n^{s+1} C_r^s \frac{(2r-2s-1)!}{r!\,(r-s-1)!}.$$

Теперь докажем, что существует такая константа C_3, что $|U_2| \leqslant C_3 n^{2s}$. Иными словами, надо оценить количество таких вершин $w \in W \setminus \Gamma$, что $n(\Gamma, w) = 2$. Пусть w имеет ребра с $u_1, u_2 \in \Gamma$. Носители вершин u_1, u_2 могут пересекаться по $0, 1, \ldots, s-1, s+1, \ldots, r-1 = 2s$ элементам. Поскольку вершина w имеет ребро с каждой из вершин u_1, u_2, носитель w и объединение носителей u_1, u_2 могут пересечься по $s, s+1, \ldots, r-1 = 2s$ элементам. Введем понятие *галочки*. Назовем *галочкой* три вершины, обладающие следующими свойствами: $u_1, u_2 \in \Gamma$ и $w \in W \setminus \Gamma$, $n(\Gamma, w) = 2$, причем $(u_1, w) \in E, (u_2, w) \in E$ (см. рис. 2). Вершину w будем называть *центром* галочки, остальные вершины галочки назовем ее *краями*.

Разделим доказательство на два случая. В первом случае носитель центра галочки пересекается с объединением носителей краев галочки больше чем по s элементам. Во втором случае носитель центра пересекается с объединением носителей краев по s элементам. Это возможно, если сами носители краев галочки имеют хотя бы $s+1$ общий элемент (а не s, ведь между u_1, u_2 нет ребра).

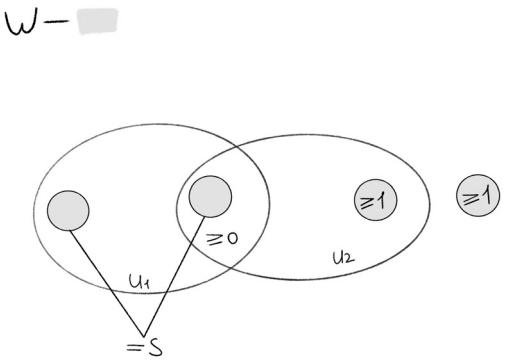

Рис. 3. Носители вершин в случае 1

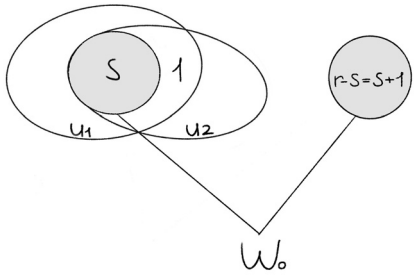

Рис. 4. Носители вершин в случае 2

Случай 1. Пусть $|(\operatorname{supp}(u_1) \cup \operatorname{supp}(u_2)) \cap \operatorname{supp}(w)| = k$, $k \geqslant s+1$. Выберем пару $u_1, u_2 \in \Gamma$ и посчитаем количество галочек с краями в этой паре и центрами в тех или иных w. Поскольку $|\operatorname{supp}(u_1) \cap \operatorname{supp}(w)| = s$, существует C_r^s способов выбрать s элементов носителя w, по которым он пересечется с носителем u_1. Среди не более чем r элементов, находящихся в разности носителя u_2 и носителя u_1, надо выбрать $k - s \geqslant 1$ элементов (см. рис. 3). Значит, $s+1$-й элемент выбирается не более чем r способами в носителе u_2. А способов выбрать остальные элементы не больше двух, причем неважно, где эти элементы выбирать – в носителе или во всем множестве из n чисел. Пусть это не так, тогда есть как минимум три вершины w_1, w_2, w_3, носители которых имеют хотя бы $s+1$ общий элемент, а следовательно, между ними нет ребер. Таким образом, поскольку из каждой вершины w_1, w_2, w_3 идет ровно два ребра в множество Γ, причем все ребра идут в вершины u_1, u_2, множество $(\Gamma \setminus \{u_1, u_2\}) \cup \{w_1, w_2, w_3\}$ является независимым и имеет мощность больше, чем мощность Γ, что противоречит максимальности Γ. Значит, для любых двух вершин u_1, u_2 существует не более $2rC_r^s$ галочек. Пару вершин можно выбрать не более чем $\alpha_n^2 \sim n^{2s}\Big(\dfrac{(2r-2s-1)!}{r!\,(r-s-1)!}\Big)^2$ способами, а стало быть, всего вершин w не более

$$\alpha_n^2 2rC_r^s < C_4 n^{2s}.$$

Случай 2. Здесь нас интересуют галочки, у которых $|(\operatorname{supp}(u_1) \cup \operatorname{supp}(u_2)) \cap$ $\cap \operatorname{supp}(w)| = s$. Выберем одну вершину $u_1 \in \Gamma$ и в ее носителе зафиксируем s элементов. Пусть существует хотя бы одна такая галочка, что носитель ее центра w_0

пересекается с носителями краев u_1, u_2 именно по этим s элементам (будем называть их *фиксированными*), а носители ее краев, соответственно, пересекаются по фиксированным s и еще хотя бы по какому-нибудь одному элементу (см. рис. 4). Теперь посчитаем, сколько еще может быть краев галочек с краем в вершине u_1 и этими же s элементами (мы хотим оценить именно число краев; оценивать число центров для данной пары краев мы будем позже). Поскольку все носители краев галочек имеют общие фиксированные элементы с носителем u_1 и этих элементов s штук, каждый из носителей краев должен иметь некоторый $(s+1)$-й общий элемент с носителем u_1, иначе в независимом множестве вершин Γ образуется ребро. Более того, все края галочек, кроме u_1 и второго края галочки с центром w_0, не имеют ребра с w_0, ведь центр галочки имеет ровно два ребра с множеством Γ. Однако все носители этих краев и носитель w_0 имеют в пересечении одни и те же фиксированные s элементов. Значит, каждый из этих носителей краев должен иметь хотя бы один дополнительный общий элемент с носителем w_0. Таким образом, искомое число краев не больше величины

$$(r-s)^2 C_n^{r-s-2} \leqslant C_5 n^{r-s-2} = C_5 n^{s-1}.$$

Теперь для каждой пары краев галочек посчитаем, сколько центров w может существовать. Первые s элементов носителя зафиксированы – по ним w пересекается с носителями u_1 и u_2. Следующий элемент выбираем не более чем n способами вне носителей u_1 и u_2. А для выбора всех остальных элементов есть не более двух способов. Доказательство аналогично доказательству в случае 1 – иначе у нас будет три вершины w_1, w_2, w_3 без ребер, и множество $(\Gamma \setminus \{u_1, u_2\}) \cup \{w_1, w_2, w_3\}$ будет иметь большую, чем Γ, мощность, оставаясь независимым. Значит, для вершины u_1 и каких-то s элементов из ее носителя галочек с центрами в некоторых w не больше чем $2n$, откуда получаем, что число галочек с данным u_1 и данными s фиксированными элементами не превосходит величины $2nC_5 n^{s-1} = C_6 n^s$. Способов выбрать вершину u_1 и s элементов в ней, соответственно,

$$\alpha_n C_r^s \leqslant n^s C_7,$$

и значит, в текущем случае количество вершин w не больше чем

$$(C_6 n^s)(C_7 n^s) = C_8 n^{2s}.$$

Итак, в каждом из случаев имеем оценку величиной вида Cn^{2s}. Складывая все константы, получаем заявленную в лемме величину C_1. ▲

2.2. Доказательство теоремы 4. Пусть W – некоторое подмножество в множестве вершин графа $G(n, r, s)$, имеющее мощность $\ell = \ell(n)$. Рассмотрим наибольшее по мощности независимое множество Γ_1 в подграфе графа $G(n, r, s)$, порожденном множеством вершин W. Пусть его мощность равна $\beta_1 \leqslant \alpha_n$. Пусть F_1 – подмножество таких вершин в множестве $W \setminus \Gamma_1$, что для любой вершины $w \in F_1$ выполнено $n(\Gamma_1, w) \leqslant 2$. Пусть $f_1 = |F_1|$. Из леммы следует, что $f_1 \leqslant C_1 n^{2s}$. Заметим, что любая вершина $u \in W \setminus (\Gamma_1 \cup F_1)$ имеет хотя бы три ребра с Γ_1. Тогда найдено хотя бы

$$3(\ell(n) - f_1 - \beta_1) + f_1 \geqslant 3(\ell(n) - \alpha_n) - 2C_1 n^{2s}$$

ребер. Выкинем из W независимое множество Γ_1, и в получившемся множестве $W \setminus \Gamma_1$ выберем новое наибольшее независимое множество Γ_2 мощности $\beta_2 \leqslant \alpha_n$. Пусть F_2 – такое подмножество множества $W \setminus (\Gamma_1 \cup \Gamma_2)$, что для любой вершины $w \in F_2$ выполнено $n(\Gamma_2, w) \leqslant 2$. Пусть $f_2 = |F_2|$. Из леммы имеем оценку $f_2 \leqslant C_1 n^{2s}$. Мы снова нашли хотя бы

$$3(\ell(n) - 2\alpha_n) - 2C_1 n^{2s}$$

ребер. Повторив эту операцию $\left[\dfrac{\ell(n)}{\alpha_n}\right]$ раз, получим оценку

$$r(\ell(n)) \geqslant \sum_{i=1}^{[\ell(n)/\alpha_n]} \bigl(3(\ell(n) - i\alpha_n) - 2C_1 n^{2s}\bigr) \sim$$
$$\sim 3\ell(n)\frac{\ell(n)}{\alpha_n} - \frac{3}{2}\alpha_n \frac{\ell(n)}{\alpha_n}\left(\frac{\ell(n)}{\alpha_n} + 1\right) - \frac{\ell(n)}{\alpha_n} 2C_1 n^{2s} \sim$$
$$\sim 3\frac{\ell^2(n)}{\alpha_n} - \frac{3}{2}\frac{\ell^2(n)}{\alpha_n} - 2C_1 n^{2s}\frac{\ell(n)}{\alpha_n} \sim \frac{3}{2}\frac{\ell^2(n)}{\alpha_n}$$

при $n \to \infty$, поскольку по предположению $n^{2s} = o(\ell(n))$. Теорема 4 доказана. ▲

Автор признателен Андрею Михайловичу Райгородскому за многогранную поддержку, без которой работа не состоялась бы. Также автор признателен и выражает благодарность художнице рисунков и схем студентке ВШЭ Марии Сметаниной.

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. *Boltyanski V.G., Martini H., Soltan P.S.* Excursions into Combinatorial Geometry. Berlin: Springer, 2012.
3. *Бердников А.В., Райгородский А.М.* Оценки чисел Борсука по дистанционным графам специального вида // Пробл. передачи информ. 2021. Т. 57. № 2. С. 44–50. https://doi.org/10.31857/S0555292321020030
4. *Pach J., Agarwal P.K.* Combinatorial Geometry. New York: Wiley, 2011.
5. *Soifer A.* The Mathematical Coloring Book: Mathematics of Coloring and the Colorful Life of Its Creators. New York: Springer, 2009.
6. *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
7. *Ипатов М.М., Кошелев М.М., Райгородский А.М.* Модулярность некоторых дистанционных графов // Докл. РАН. Матем., информ., процессы упр. 2020. Т. 490. № 1. С. 71–73. https://doi.org/10.31857/S2686954320010142
8. *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
9. *Bassalygo L., Cohen G., Zémor G.* Codes with Forbidden Distances // Discrete Math. 2000. V. 213. № 1–3. P. 3–11. https://doi.org/10.1016/S0012-365X(99)00161-2
10. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
11. *Graham R.L., Rothschild B.L., Spencer J.H.* Ramsey Theory. New York: Wiley, 1990.
12. *Kupavskii A., Sagdeev A.* All Finite Sets Are Ramsey in the Maximum Norm // Forum Math. Sigma. 2021. V. 9. Paper No. e55 (12 pp.). https://doi.org/10.1017/fms.2021.50
13. *Nagy Zs.* A Ramsey-szám egy konstruktiv becslése (A Constructive Estimation of the Ramsey Number) // Matem. Lapok. 1972. V. 23. № 3–4. P. 301–302.
14. *Райгородский А.М., Михайлов К.А.* О числах Рамсея для полных дистанционных графов с вершинами в $\{0,1\}^n$ // Матем. сб. 2009. Т. 200. № 12. С. 63–80. https://doi.org/10.4213/sm6373
15. *Пушняков Ф.А.* Новая оценка числа ребер в индуцированных подграфах специального дистанционного графа // Пробл. передачи информ. 2015. Т. 51. № 4. С. 71–77. http://mi.mathnet.ru/ppi2188

16. *Пушняков Ф.А.* О количествах ребер в порожденных подграфах некоторых дистанционных графов // Матем. заметки. 2019. Т. 105. № 4. С. 592–602. https://doi.org/10.4213/mzm11942
17. *Пушняков Ф.А., Райгородский А.М.* Оценка числа ребер в подграфах графа Джонсона // Докл. РАН. Матем., информ., процессы упр. 2021. Т. 499. № 1. С. 40–43. https://doi.org/10.31857/S2686954321040135
18. *Frankl P., Füredi Z.* Forbidding Just One Intersection // J. Combin. Theory Ser. A. 1985. V. 39. № 2. P. 160–176. https://doi.org/10.1016/0097-3165(85)90035-4
19. *Shabanov L.E., Raigorodskii A.M.* Turán Type Results for Distance Graphs // Discrete Comput. Geom. 2016. V. 56. № 3. P. 814–832. https://doi.org/10.1007/s00454-016-9817-z

Дубинин Никита Андреевич
Московский физико-технический институт
(национальный исследовательский университет)
nikita.dubinin2010@yandex.ua

Поступила в редакцию
10.05.2021
После доработки
04.09.2021
Принята к публикации
05.09.2021

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391 : 519.175.4

© 2021 г. **Н.М. Деревянко, М.М. Кошелев**

НОВЫЕ ОЦЕНКИ МОДУЛЯРНОСТИ ГРАФОВ $G(n, r, s)$ И $G_p(n, r, s)$[1]

Исследуется поведение модулярности графов $G(n, r, s)$ для случая $r = o(\sqrt{n})$ и $n \to \infty$, а также графов $G_p(n, r, s)$ при фиксированных r, s и $n \to \infty$. Для графов $G(n, r, s)$ при $r \geqslant cs^2$ получены существенные улучшения предыдущих верхних оценок. На семейство графов $G_p(n, r, s)$ при $p = p(n) = \omega\big(n^{-\frac{r-s-1}{2}}\big)$ и фиксированных r и s перенесены верхние и нижние оценки, полученные ранее для графов $G(n, r, s)$.

Ключевые слова: модулярность, графы Джонсона, кластеризация, случайные графы.

DOI: 10.31857/S0555292321040082

§ 1. Введение

Модулярность графа – величина, впервые возникшая в работе Ньюмана и Гирвана [1], которая впоследствии оказалась полезной для оценки качества кластеризационных алгоритмов (см. [2–5]). Такие алгоритмы играют важную роль в биологии, физике, социологии и программировании (см. [6]).

Благодаря широкому применению в программировании задача подсчета модулярности получила большое развитие в последние годы. Поскольку вычисление модулярности с помощью компьютера представляется сложной задачей (в [7] было доказано, что задача оценки модулярности является NP-полной), интересным представляется получение оценок для различных классов графов. В последние годы было получено множество оценок для различных классов графов, таких как звезды, гиперкубы, графы, удовлетворяющие степенному закону [8], графы, близкие к полным [9], деревья с небольшой максимальной степенью [10], а также большого числа моделей случайных графов. В частности, были получены результаты для различных вероятностных моделей веб-графов, таких как модели предпочтительного присоединения [11], а также графов $G(n, d)$ (случайные d-регулярные графы) [12] и классической модели Эрдёша – Реньи [13].

Говоря о модели Эрдёша – Реньи, нельзя не упомянуть широкий класс теорем, называемых теоремами о стабильности. В теоремах подобного типа доказывается, что результаты, полученные для определенного графа, можно перенести и на его случайные подграфы. Одним из ярких примеров теорем такого класса является теорема о стабильности числа независимости кнезеровского графа, доказанная в работе [14].

Данная статья посвящена исследованию стабильности модулярности для семейства графов $G(n, r, s)$, которые являются обобщением кнезеровских графов и графов

[1] Работа выполнена за счет гранта Президента Российской Федерации для государственной поддержки ведущих научных школ (номер гранта НШ-2540.2020.1), а также гранта Фонда развития теоретической физики и математики “БАЗИС”.

Джонсона. Эти графы нашли свое применение в задачах о кодах с одним запрещенным расстоянием (см. [15]), а также в различных задачах комбинаторной геометрии, таких как гипотезы Борсука и Нелсона – Эрдёша – Хадвигера (см. [16–18]).

Оценки модулярности, полученные ранее для $G(n, r, s)$, удалось перенести на случайные графы $G_p(n, r, s)$, т.е. подграфы $G(n, r, s)$, в которых каждое ребро выбрасывается из графа с вероятностью $1 - p$. Помимо этого, удалось получить новые оценки модулярности $G(n, r, s)$, которые также были распространены на случайные подграфы.

Прежде чем перейти к определению основных понятий, введем некоторые обозначения, которыми мы будем пользоваться:

- $e(V)$ – количество ребер, оба конца которых лежат в V;
- $e(U, V)$ – количество ребер, один конец которых лежит в U, а другой – в V;
- V_G – множество всех вершин графа;
- $\deg(v)$ – степень вершины v;
- $e(V, p)$ – случайная величина, равная количеству ребер, оба конца которых лежат в V, для случайного графа $G_p(n, r, s)$, определение которого будет дано ниже;
- $e(U, V, p)$ – случайная величина, равная количеству ребер, один конец которых лежит в U, а другой – в V, для случайного графа $G_p(n, r, s)$;
- $\deg(v, p)$ – случайная величина, равная степени вершины v, для случайного графа $G_p(n, r, s)$.

Настало время дать формальные определения основных объектов исследования.

Определение 1. *Модулярность графа* G – характеристика графа, которая показывает, насколько оптимально можно разбить граф на части, где вершины внутри одной части сильно связаны, а связь между различными частями мала. Модулярность графа G обозначается через $q^*(G)$ и выражается формулой

$$q^*(G) := \max_{\mathcal{A}} \left(\sum_{A \in \mathcal{A}} \frac{e(A)}{e(G)} - \sum_{A \in \mathcal{A}} \frac{\Big(\sum\limits_{v \in A} \deg(v) \Big)^2}{4e^2(G)} \right),$$

где максимум берется по всем разбиениям множества вершин графа

$$\mathcal{A} = \{A_1, A_2, \ldots, A_k\}.$$

Помимо этого, определяется понятие *модулярности разбиения*, а именно

$$q(\mathcal{A}) := \sum_{A \in \mathcal{A}} \frac{e(A)}{e(G)} - \sum_{A \in \mathcal{A}} \frac{\Big(\sum\limits_{v \in A} \deg(v) \Big)^2}{4e^2(G)}.$$

При этом первую сумму $\sum\limits_{A \in \mathcal{A}} \frac{e(A)}{e(G)}$ принято называть *реберным вкладом*, а вторую сумму $\sum\limits_{A \in \mathcal{A}} \frac{\Big(\sum\limits_{v \in A} \deg(v) \Big)^2}{4e^2(G)}$ – *степенным штрафом*.

Замечание 1. Если граф d-регулярный, то сумму степенного штрафа можно записать в более удобном виде:

$$\sum_{A \in \mathcal{A}} \frac{\Big(\sum\limits_{v \in A} \deg(v) \Big)^2}{4e^2(G)} = \sum_{A \in \mathcal{A}} \frac{|A|^2 d^2}{|V|^2 d^2} = \sum_{A \in \mathcal{A}} \frac{|A|^2}{|V|^2}.$$

Определение 2. Пусть $1 \leqslant r \leqslant n$, $0 \leqslant s \leqslant r$, $n, r, s \in \mathbb{N}$, $\Gamma := \{1, 2, \ldots, n\}$, тогда $G(n, r, s) := (V_G(n, r), E(n, r, s))$ является *регулярным графом*, в котором:

$V_G = V_G(n, r) := \binom{\Gamma}{r}$ – все r-элементные подмножества множества Γ;

$E(n, r, s) := \{(u, v) : u, v \in V_G(n, r),\ |u \cap v| = s\}$.

Множество Γ называется *множеством элементов*.

Замечание 2. Несложно заметить, что для числа вершин и числа ребер в графе $G(n, r, s)$ верно следующее:

$$|V_G| = \binom{n}{r}, \quad |E(n, r, s)| = \frac{1}{2}\binom{n}{r}\binom{r}{s}\binom{n-r}{r-s}.$$

При этом степень каждой вершины равна $\binom{r}{s}\binom{n-r}{r-s}$.

Семейство случайных графов $G_p(n, r, s)$ состоит из всех графов с множеством вершин $V_G(n, r)$ и ребрами из множества $E(n, r, s)$. Каждое ребро этого множества добавляется в граф независимо с вероятностью p. Таким образом, каждый граф с множеством вершин $V_G(n, r)$ и множеством ребер $E \subseteq E(n, r, s)$ может быть выбран с вероятностью $p^{|E|}(1-p)^{|E(n,r,s)|-|E|}$.

Ранее в работах [19–21] были получены следующие оценки на модулярность графов $G(n, r, s)$.

Теорема 1 (см. [19]). *Пусть* $r \geqslant 2$ *и* $1 \leqslant s \leqslant \left[\frac{r}{2}\right]$. *Тогда*

$$\limsup_{n\to\infty} q^*(G(n, r, s)) \leqslant 1 - \frac{\binom{[r/2]}{s}}{2\binom{r}{s}}.$$

Теорема 2 (см. [20]). *Справедливо равенство*

$$q^*(G(n, 2, 1)) = \frac{1}{3} + \frac{2w(w-1)(w-2)}{3n(n-1)(n-2)} - \frac{w^2(w-1)^2}{n^2(n-1)^2} - \frac{4n-2}{3n(n-1)} + \\ + \frac{w(w-1)(4w-2)}{3n^2(n-1)^2}$$

при всех $n \geqslant 5$, *где* $w = \left[\frac{n}{2}\right] + 1$. *Предел выражения в правой части при* $n \to \infty$ *равен* $\frac{17}{48}$.

Теорема 3 (см. [21]). *Пусть* $r > s \geqslant 1$. *Тогда*

$$\liminf_{n\to\infty} q^*(G(n, r, s)) \geqslant \frac{s}{2r-s}\left(1 + \left(\frac{r-s}{r}\right)^{\frac{2r}{s}}\right).$$

Отметим, что верхние и нижние оценки модулярности графов $G(n, r, s)$ на данный момент весьма далеки друг от друга. Так, при $r = 3$, $s = 1$ нижняя оценка равна $\frac{793}{3645} < 0{,}22$, в то время как верхняя оценка составляет всего лишь $1 - \frac{1}{6} > 0{,}83$. Более того, при больших r и s разница между оценками становится все более существенной. Так, например, уже при $s = 10$, $r = 20$ нижняя оценка равна $\frac{17}{48}$, в то время как верхняя оценка – всего лишь $1 - \frac{1}{2\binom{20}{10}} > 0{,}99999$.

Таким образом, единственный случай, когда верхние и нижние оценки модулярности $G(n,r,s)$ близки между собой, – это случай $r=2$, $s=1$, в котором благодаря теореме 2 известно точное значение модулярности. Отметим также, что для таких параметров оценка из теоремы 3 дает нижнюю оценку предела модулярности $\frac{17}{48}$, совпадающую с настоящим пределом модулярности в этом случае, в то время как теорема 1 дает лишь оценку $\frac{3}{4}$.

В § 2 будут получены новые верхние оценки модулярности графов $G(n,r,s)$. Затем § 3 будет посвящен переносу результатов § 2, а также теорем 1 и 3 на графы $G_p(n,r,s)$.

§ 2. Верхняя оценка модулярности графов $G(n,r,s)$

2.1. Формулировка основных результатов. Первая теорема, которую мы докажем, дает верхнюю оценку величины $e(U)$ для всех $U \subset V_G$, размер которых хотя бы в константу раз меньше $|V_G|$.

Теорема 4. *Пусть* $\alpha,\beta \in (0,1)$, $\alpha < \beta^2$, $s \geqslant 1$,

$$r \geqslant -\frac{1}{\ln\left(\frac{1-\beta}{1-\alpha/\beta}\right)}s^2 + 2s - 1.$$

Пусть также $U \subseteq V_G(n,r)$, $|U| < \alpha\binom{n}{r}$. *Тогда*

$$e(U) \leqslant \frac{1+\beta-\beta^2}{2(2-\beta)}\binom{r}{s}\binom{n-s}{r-s}|U|.$$

Также сформулируем следствия теоремы 4.

Следствие 1. *В условиях теоремы* 4 *при* $n \to \infty$, $r = o(\sqrt{n})$ *верно неравенство*

$$e(U,\overline{U}) \geqslant (1+o(1))\frac{(1-\beta)^2}{2-\beta}\binom{r}{s}\binom{n-s}{r-s}|U|.$$

Следствие 2. *В условиях теоремы* 4 *при* $n \to \infty$, $r = o(\sqrt{n})$ *верно неравенство*

$$\frac{e(U)}{e(G)} \leqslant (1+o(1))\frac{1+\beta-\beta^2}{2-\beta}\frac{|U|}{|V_G|}.$$

Доказательство следствия 2 мы опустим в силу его тривиальности.

Сформулируем, наконец, основной результат этого параграфа:

Теорема 5. *Пусть* $\varepsilon \in (0,1)$, $s = s(n) \geqslant 1$,

$$r = r(n) \geqslant -\frac{1}{\ln(1-\varepsilon)}s^2 + 2s - 1,$$

$r = o(\sqrt{n})$. *Тогда*

$$\limsup_{n\to\infty} q^*(G(n,r,s)) \leqslant f(\varepsilon),$$

где $f(\varepsilon) = \max\limits_{x\in[0,1]}\Big(\frac{1+x-x^2}{2-x} - \max\Big(\frac{x^2-\varepsilon x}{1-\varepsilon}, 0\Big)\Big)$.

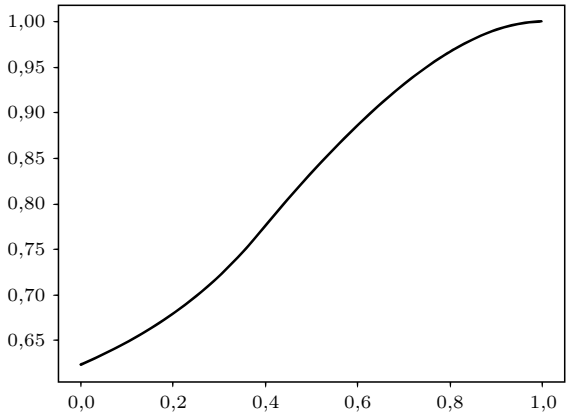

Рис. 1. График функции $f(\varepsilon)$

Таблица 1

ε	$r \geqslant$	$f(\varepsilon)$
0,01	$99{,}4992s^2 + 2s - 1$	0,6246
0,1	$9{,}4912s^2 + 2s - 1$	0,6469
0,2	$4{,}4814s^2 + 2s - 1$	0,6783
0,3	$2{,}8037s^2 + 2s - 1$	0,7195
0,4	$1{,}9576s^2 + 2s - 1$	0,7750
0,5	$1{,}4427s^2 + 2s - 1$	0,8333
0,6	$1{,}0914s^2 + 2s - 1$	0,8857
0,7	$0{,}8306s^2 + 2s - 1$	0,9308
0,8	$0{,}6213s^2 + 2s - 1$	0,9667
0,9	$0{,}4343s^2 + 2s - 1$	0,9909
0,99	$0{,}2171s^2 + 2s - 1$	0,9999

На рис. 1 приведен график, показывающий зависимость функции f от ε.

Приведем также таблицу приближенных значений $f(\varepsilon)$ и ограничений на r, порождаемых соответствующим ε (табл. 1).

Сравним новые результаты с имеющимися. Заметим, что верхняя оценка из теоремы 1 имеет вид

$$1 - \frac{\binom{[r/2]}{s}}{2\binom{r}{s}} \geqslant 1 - 2^{-s-1}.$$

В частности, из этого следует, что при любом $s \geqslant 1$ такая оценка не лучше, чем $\frac{3}{4}$. Тогда, взяв, например, $r \geqslant -\frac{1}{\ln 0,7}s^2 + 2s - 1$, можно увидеть, что при таких параметрах r и s новая оценка, примерно равная 0,7195, существенно лучше предыдущей. При возрастании s разрыв между оценками становится еще более драматическим. Например, при $s = 10$ и $r \geqslant 129$ (для таких r выполняется условие теоремы 5 с $\varepsilon = 0{,}6$) новая теорема дает оценку $f(0{,}6) \approx 0{,}8857$, в то время как теорема 2 не позволяет оценить модулярность даже числом 0,999.

К сожалению, зазор между верхними и нижними оценками модулярности все еще достаточно велик. Нетрудно видеть, что нижняя оценка модулярности зависит

лишь от отношения s и r, в то время как в теореме 5 требуется условие

$$r \geqslant Cs^2 + 2s - 1.$$

Таким образом, если мы зафиксируем C, то с ростом r и s нижняя оценка будет стремиться к 0, в то время как верхняя будет оставаться на одном и том же уровне.

2.2. Вспомогательные леммы и определения.

Лемма 1. *Пусть* $\alpha \in (0,1)$, $r \geqslant -\dfrac{1}{\ln\alpha}s^2 + 2s - 1$, $s \geqslant 1$. *Тогда*

$$\binom{r-s}{s} \geqslant \alpha\binom{r}{s}.$$

Доказательство. Перепишем требуемое неравенство в виде

$$\alpha r!\,(r-2s)! \leqslant ((r-s)!)^2 \iff \prod_{k=0}^{s-1}\frac{r-k}{r-s-k} \leqslant \frac{1}{\alpha}.$$

Оценим сверху левую часть требуемого неравенства:

$$\prod_{k=0}^{s-1}\frac{r-k}{r-s-k} = \prod_{k=0}^{s-1}\left(1+\frac{s}{r-s-k}\right) \leqslant \left(1+\frac{s}{r-2s+1}\right)^s =$$

$$= \left(1+\frac{s}{r-2s+1}\right)^{\frac{r-2s+1}{s}\frac{s^2}{r-2s+1}} \leqslant e^{\frac{s^2}{r-2s+1}}.$$

Осталось понять, при каких условиях $e^{\frac{s^2}{r-2s+1}} \leqslant \dfrac{1}{\alpha}$. Это эквивалентно тому, что

$$\frac{s^2}{r-2s+1} \leqslant \ln\frac{1}{\alpha},$$

или

$$r \geqslant -\frac{1}{\ln\alpha}s^2 + 2s - 1. \quad \blacktriangle$$

Определение 3. Пусть V – некоторое множество вершин графа $G(n,r,s)$, а S – некоторое множество s-элементных подмножеств множества $\{1,2,\ldots,n\}$.

Вкладом вершин V в множество S назовем следующую величину:

$$W(V,S) := \sum_{v\in V}|\{S_j \in S:\ S_j \subset v\}| = \sum_{S_j\in S}|\{v \in V:\ S_j \subset v\}|.$$

Далее для удобства будем использовать следующие обозначения:

- $S_{\text{all}} := \{S_1, S_2, \ldots, S_{\binom{n}{s}}\}$, $|S_{\text{all}}| = \binom{n}{s}$, – всевозможные s-элементные множества;
- $\overline{S} := S_{\text{all}} \setminus S$ для $S \subseteq S_{\text{all}}$;
- $V_{S_i} := \{v \in V_G:\ S_i \subset v\}$, $S_i \in S_{\text{all}}$;
- $W_{S_i}(V) := W(V,\{S_i\}) = |\{v \in V:\ S_i \subset v\}|$.

Лемма 2. *Пусть* $\alpha, \beta \in (0,1)$, $\alpha < \beta$, $s \geqslant 1$,

$$r \geqslant -\frac{1}{\ln\left(\frac{1-\beta}{1-\alpha}\right)}s^2 + 2s - 1.$$

Пусть также $U \subseteq V_G$, $S \subseteq S_{\text{all}}$, $|S| < \alpha\binom{n}{s}$. *Тогда для любого* $S_i \in S$, *такого что*

$$W_{S_i}(U) = \beta\binom{n-s}{r-s} + d, \quad d \geqslant 0,$$

верно неравенство

$$W(V_{S_i} \cap U, \overline{S}) \geqslant d\binom{r}{s}.$$

Доказательство. Определим $V_{\text{left}} := V_{S_i} \setminus (V_{S_i} \cap U)$. Имеем

$$|V_{\text{left}}| = (1-\beta)\binom{n-s}{r-s} - d.$$

Оценим $W(V_{S_i}, \overline{S})$:

$$W(V_{S_i}, \overline{S}) = \sum_{S_j \in \overline{S}} W_{S_j}(V_{S_i}) \geqslant \sum_{S_j \in \overline{S}} \binom{n-2s}{r-2s} = |\overline{S}|\binom{n-2s}{r-2s} >$$
$$> (1-\alpha)\binom{n}{s}\binom{n-2s}{r-2s} > (1-\alpha)\binom{n-s}{s}\binom{n-2s}{r-2s} = (1-\alpha)\binom{r-s}{s}\binom{n-s}{r-s}.$$

Применяя лемму 1, получаем, что

$$W(V_{S_i}, \overline{S}) > (1-\alpha)\binom{r-s}{s}\binom{n-s}{r-s} \geqslant (1-\beta)\binom{r}{s}\binom{n-s}{r-s}.$$

С другой стороны, имеем

$$W(V_{S_i}, \overline{S}) = W(V_{S_i} \cap U, \overline{S}) + W(V_{\text{left}}, \overline{S}) \leqslant W(V_{S_i} \cap U, \overline{S}) +$$
$$+ (1-\beta)\binom{n-s}{r-s}\binom{r}{s} - d\binom{r}{s} = \left(W(V_{S_i} \cap U, \overline{S}) - d\binom{r}{s}\right) + (1-\beta)\binom{r}{s}\binom{n-s}{r-s},$$

откуда тривиально следует требуемое неравенство. ▲

2.3. Доказательство основных результатов.

Доказательство теоремы 4. Определим $e_{S_i}(U)$ – множество ребер с концами в множестве U, оба конца которых содержат s-элементное множество S_i.

Мы знаем, что $e(U) = \sum\limits_{i=1}^{\binom{n}{s}} e_{S_i}(U)$. Очевидно, что $e_{S_i}(U) \leqslant \dfrac{W^2_{S_i}(U)}{2}$. Отсюда имеем оценку $e(U) \leqslant \sum\limits_{i=1}^{\binom{n}{s}} \dfrac{W^2_{S_i}(U)}{2}$.

Будем считать, что $W_{S_1}(U) \geqslant W_{S_2}(U) \geqslant \ldots$ Пусть m таково, что

$$W_{S_m}(U) \geqslant \beta\binom{n-s}{r-s}, \quad W_{S_{m+1}}(U) < \beta\binom{n-s}{r-s},$$

или $m = \binom{n}{s}$, если первое неравенство верно для всех S_i. Множество $\{S_1, \ldots, S_m\}$ будем обозначать через $S_{\max}$. Оценим m. Очевидно, что $\sum\limits_{i=1}^{\binom{n}{s}} W_{S_i}(U) = \binom{r}{s}|U|$, откуда

имеем оценку

$$m\beta\binom{n-s}{r-s} \leqslant \binom{r}{s}|U| \iff m \leqslant \frac{\binom{r}{s}|U|}{\beta\binom{n-s}{r-s}} < \frac{\binom{r}{s}\alpha\binom{n}{r}}{\beta\binom{n-s}{r-s}} = \frac{\alpha}{\beta}\binom{n}{s}.$$

Представим $W_{S_i}(U)$, $i \leqslant m$, в виде

$$W_{S_i}(U) = \beta\binom{n-s}{r-s} + d_i, \quad d_i \geqslant 0.$$

Оценим $W(U, \overline{S_{\max}})$. Применяя лемму 2 с $S = S_{\max}$, $\alpha = \alpha/\beta$, $\beta = \beta$ (и суммируя результат по всем $S_i \in S_{\max}$), получаем неравенство

$$\sum_{S_i \in S_{\max}} W(V_{S_i} \cap U, \overline{S_{\max}}) \geqslant \sum_{S_i \in S_{\max}} d_i\binom{r}{s}.$$

Заметим, что в левой части неравенства каждое вхождение множества из $\overline{S_{\max}}$ в вершину из U посчитано не более $\binom{r}{s}$ раз. Отсюда получаем

$$W(U, \overline{S_{\max}}) \geqslant \frac{1}{\binom{r}{s}} \sum_{S_i \in S_{\max}} d_i\binom{r}{s} = \sum_{S_i \in S_{\max}} d_i.$$

Теперь можно получить оценку на $\sum\limits_{S_i \in S_{\max}} d_i$. Действительно,

$$\binom{r}{s}|U| = W(U, S_{\text{all}}) = \sum_{S_i \in S_{\max}} W_{S_i}(U) + W(U, \overline{S_{\max}}) \geqslant$$

$$\geqslant \sum_{S_i \in S_{\max}} \left(\beta\binom{n-s}{r-s} + d_i\right) + \sum_{S_i \in S_{\max}} d_i,$$

откуда имеем

$$\sum_{S_i \in S_{\max}} d_i \leqslant \frac{1}{2}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right).$$

Получим еще одну оценку на $\sum\limits_{S_i \in S_{\max}} d_i$. Она тривиальна, ибо $d_i \leqslant (1-\beta)\binom{n-s}{r-s}$. Отсюда имеем оценку

$$\sum_{S_i \in S_{\max}} d_i \leqslant (1-\beta)\binom{n-s}{r-s}m.$$

Нетрудно видеть, что при таких ограничениях на $\sum\limits_{S_i \in S_{\max}} d_i$ верна следующая оценка на $\sum\limits_{i=1}^{\binom{n}{s}} \frac{W_{S_i}^2(U)}{2}$ (она вытекает из того, что максимум такой суммы, очевидно, достигается на последовательности W_{S_i}, равной $\binom{n-s}{r-s}, \ldots, \binom{n-s}{r-s}, \beta\binom{n-s}{r-s}, \ldots, \beta\binom{n-s}{r-s}, 0, 0, \ldots, 0$):

$$\sum_{i=1}^{\binom{n}{s}} \frac{W_{S_i}^2(U)}{2} \leqslant \frac{\min\left((1-\beta)\binom{n-s}{r-s}m, \frac{1}{2}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right)\right)}{(1-\beta)\binom{n-s}{r-s}} \frac{\binom{n-s}{r-s}^2}{2} +$$

$$\binom{r}{s}|U| - \frac{\min\left((1-\beta)\binom{n-s}{r-s}m, \frac{1}{2}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right)\right)}{(1-\beta)\binom{n-s}{r-s}}\binom{n-s}{r-s} + \frac{}{\beta\binom{n-s}{r-s}} \times$$

$$\times \frac{\beta^2\binom{n-s}{r-s}^2}{2}.$$

Прокомментируем эту оценку. Первое слагаемое в ней соответствует членам вида $\binom{n-s}{r-s}$ в оптимальной последовательности, в то время как второе слагаемое соответствует членам вида $\beta\binom{n-s}{r-s}$.

Упростив выражение в правой части, получаем

$$\sum_{i=1}^{\binom{n}{s}} \frac{W_{S_i}^2(U)}{2} \leqslant \min\left(\binom{n-s}{r-s}m, \frac{1}{2(1-\beta)}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right)\right)\frac{\binom{n-s}{r-s}}{2} +$$

$$+ \left(\binom{r}{s}|U| - \min\left(\binom{n-s}{r-s}m, \frac{1}{2(1-\beta)}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right)\right)\right)\frac{\beta\binom{n-s}{r-s}}{2} =$$

$$= \frac{\beta}{2}\binom{r}{s}\binom{n-s}{r-s}|U| + \min\left(\binom{n-s}{r-s}m, \frac{1}{2(1-\beta)}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right)\right) \times$$

$$\times \frac{\binom{n-s}{r-s}(1-\beta)}{2} = \frac{\beta}{2}\binom{r}{s}\binom{n-s}{r-s}|U| +$$

$$+ \min\left((1-\beta)\binom{n-s}{r-s}m, \frac{1}{2}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m\right)\right)\frac{\binom{n-s}{r-s}}{2}.$$

Осталось оценить этот минимум. Так как одна из величин монотонно возрастает по m, а другая монотонно убывает по m, то максимум минимума достигается в точке равенства этих величин. Получаем уравнение на m_{opt}:

$$(1-\beta)\binom{n-s}{r-s}m_{\text{opt}} = \frac{1}{2}\left(\binom{r}{s}|U| - \beta\binom{n-s}{r-s}m_{\text{opt}}\right) \iff$$

$$\iff (1-\frac{\beta}{2})\binom{n-s}{r-s}m_{\text{opt}} = \frac{1}{2}\binom{r}{s}|U| \iff m_{\text{opt}} = \frac{1}{2\left(1-\frac{\beta}{2}\right)}\frac{\binom{r}{s}|U|}{\binom{n-s}{r-s}}.$$

Подставляя m_{opt} в оценку для $\sum\limits_{i=1}^{\binom{n}{s}} \frac{W_{S_i}^2(U)}{2}$, получаем

$$\sum_{i=1}^{\binom{n}{s}} \frac{W_{S_i}^2(U)}{2} \leqslant \frac{\beta}{2}\binom{r}{s}\binom{n-s}{r-s}|U| + \frac{1-\beta}{2(2-\beta)}\binom{r}{s}\binom{n-s}{r-s}|U| =$$

$$= \frac{1+\beta-\beta^2}{2(2-\beta)}\binom{r}{s}\binom{n-s}{r-s}|U|. \quad \blacktriangle$$

Доказательство следствия 1. Заметим, что при $r = o(\sqrt{n})$ выполняется соотношение $\binom{n-r}{r-s} = (1+o(1))\binom{n-s}{r-s}$. Действительно,

$$1 > \frac{\binom{n-r}{r-s}}{\binom{n-s}{r-s}} = \frac{(n-r)!^2}{(n-s)!(n-2r+s)!} = \frac{(n-r)\dots(n-2r+s+1)}{(n-s)\dots(n-r+1)} \geqslant$$
$$\geqslant \left(\frac{n-2r+s+1}{n-r+1}\right)^{r-s} = \left(1 - \frac{r-s}{n-r+1}\right)^{r-s}.$$

Обозначая $\dfrac{r-s}{n-r+1} = t$, получаем

$$1 > \frac{\binom{n-r}{r-s}}{\binom{n-s}{r-s}} \geqslant (1-t)^{\frac{(r-s)^2}{t(n-r+1)}}.$$

При достаточно больших n имеем $(1-t)^{1/t} > 1/3$, т.е.

$$1 > \frac{\binom{n-r}{r-s}}{\binom{n-s}{r-s}} \geqslant \left(\frac{1}{3}\right)^{\frac{(r-s)^2}{n-r+1}}.$$

Осталось заметить, что при $n \gg r^2$ выполняется соотношение $(1/3)^{\frac{(r-s)^2}{n-r+1}} = 1 + o(1)$.

Следствие теперь тривиально вытекает из равенства

$$2e(U) + e(U, \overline{U}) = \sum_{v \in U} \deg(v) = \binom{r}{s}\binom{n-r}{r-s}|U| = (1+o(1))\binom{r}{s}\binom{n-s}{r-s}|U|.$$

и теоремы 4. ▲

Доказательство теоремы 5. Введем функцию $\alpha(x) = x\dfrac{x-\varepsilon}{1-\varepsilon}$. Проверим, что в условиях теоремы $\alpha(x) < x^2$ всюду на $(0,1)$. Действительно,

$$x\frac{x-\varepsilon}{1-\varepsilon} = \frac{x^2}{1-\varepsilon} - \frac{\varepsilon x}{1-\varepsilon} = x^2 - \frac{\varepsilon(x-x^2)}{1-\varepsilon}.$$

Так как второе слагаемое положительно, то оценка очевидна. Заметим также, что

$$\frac{1-x}{1-\dfrac{\alpha(x)}{x}} = \frac{1-x}{1-\dfrac{x-\varepsilon}{1-\varepsilon}} = 1-\varepsilon.$$

Зафиксируем $k \in \mathbb{N}$ и введем обозначения: $\beta_i = \dfrac{i}{k}$, $i \in \{0, \dots, k\}$, $\alpha_i = \alpha(\beta_i)$. Рассмотрим оптимальное разбиение $\mathcal{A} = \{A_1, \dots, A_\ell\}$, $\ell > 1$, множества вершин графа $G(n,r,s)$ на части. Представим наше разбиение в виде объединения множеств C_i, $i \in \{1, \dots, k\}$, таких что $A_j \in C_i \Leftrightarrow \dfrac{|A_j|}{|V_G|} \in [\alpha_{i-1}, \alpha_i)$. Стоит отметить, что некоторые интервалы могут быть некорректными, т.е. такими, что $\alpha_{i-1} > \alpha_i$. В таком случае мы полагаем этот интервал равным пустому множеству. Нетрудно видеть, что любое число из полуинтервала $[0,1)$ попадет ровно в один отрезок. Тогда модулярность

можно переписать в следующем виде:

$$q(\mathcal{A}) = \sum_{A\in\mathcal{A}} \left(\frac{e(A)}{e(G)} - \frac{|A|^2}{|V_G|^2}\right) = \sum_{i=1}^{k} \sum_{A\in C_i} \left(\frac{e(A)}{e(G)} - \frac{|A|^2}{|V_G|^2}\right).$$

Пусть m – минимальное число, для которого $\alpha_m > 0$. Тогда $C_1, \ldots, C_{m-1}$ будут пустыми, поэтому нижний индекс суммирования положим равным m. Предположим теперь, что C_k не пусто. В этом случае имеем

$$q(\mathcal{A}) \leqslant 1 - \sum_{A\in\mathcal{A}} \frac{|A|^2}{|V_G|^2} \leqslant 1 - \alpha^2\left(1 - \frac{1}{k}\right).$$

Поскольку $\alpha(1-1/k) \to 1$ при $k \to \infty$, при достаточно больших k необходимая оценка тривиальна. Таким образом, можно считать, что C_k пусто, а суммирование ведется до $k-1$. Получим

$$q(\mathcal{A}) = \sum_{i=m}^{k-1} \sum_{A\in C_i} \left(\frac{e(A)}{e(G)} - \frac{|A|^2}{|V_G|^2}\right).$$

Теперь для каждого элемента A из $C_i, i < k$, воспользуемся следствием 2 с $\alpha = \alpha_i$, $\beta = \beta_i$. Также воспользуемся тем, что для любого A из C_i верно неравенство $\frac{|A|}{|G|} \geqslant \max(\alpha_{i-1}, 0)$. Оценка получится такой:

$$q(\mathcal{A}) \leqslant \sum_{i=m}^{k-1} \sum_{A\in C_i} \left((1+o(1))\frac{1+\beta_i-\beta_i^2}{2-\beta_i}\frac{|A|}{|V_G|} - \max(\alpha_{i-1},0)\frac{|A|}{|V_G|}\right),$$

или, что тоже самое,

$$q(\mathcal{A}) \leqslant \sum_{i=m}^{k-1} \left((1+o(1))\frac{1+\beta_i-\beta_i^2}{2-\beta_i} - \max(\alpha_{i-1},0)\right) \frac{\sum\limits_{A\in C_i}|A|}{|V_G|}.$$

Отсюда

$$\begin{aligned} q(\mathcal{A}) &\leqslant \max_{i\in m,\ldots,k-1} \left((1+o(1))\frac{1+\beta_i-\beta_i^2}{2-\beta_i} - \max(\alpha_{i-1},0)\right) \sum_{i=m}^{k-1} \frac{\sum\limits_{A\in C_i}|A|}{|V_G|} = \\ &= \max_{i\in\{m,\ldots,k-1\}} \left(\frac{1+\beta_i-\beta_i^2}{2-\beta_i} - \max(\alpha_{i-1},0)\right) + o(1) \leqslant \\ &\leqslant \max_{i\in\{1,\ldots,k\}} \left(\frac{1+\beta_i-\beta_i^2}{2-\beta_i} - \max(\alpha_{i-1},0)\right) + o(1). \end{aligned}$$

Осталось оценить этот максимум. Действительно,

$$\begin{aligned} &\max_{i\in\{1,\ldots,k\}} \left(\frac{1+\beta_i-\beta_i^2}{2-\beta_i} - \max(\alpha_{i-1},0)\right) = \\ &= \max_{i\in\{1,\ldots,k\}} \left(\frac{1+\frac{i}{k}-\left(\frac{i}{k}\right)^2}{2-\frac{i}{k}} - \max\left(\left(\frac{i}{k}-\frac{1}{k}\right)\frac{\frac{i}{k}-\frac{1}{k}-\varepsilon}{1-\varepsilon}, 0\right)\right) = \\ &= \max_{i\in\{1,\ldots,k\}} \left(\frac{1+\frac{i}{k}-\left(\frac{i}{k}\right)^2}{2-\frac{i}{k}} - \max\left(\frac{i}{k}\frac{\frac{i}{k}-\varepsilon}{1-\varepsilon} - \frac{i}{k}\frac{\frac{1}{k}}{1-\varepsilon} - \frac{1}{k}\frac{\frac{i}{k}-\frac{1}{k}-\varepsilon}{1-\varepsilon}, 0\right)\right) \leqslant \end{aligned}$$

$$\leqslant \max_{i\in\{1,\dots,k\}} \left(\frac{1+\frac{i}{k}-\left(\frac{i}{k}\right)^2}{2-\frac{i}{k}} - \max\left(\frac{i}{k}\frac{\frac{i}{k}-\varepsilon}{1-\varepsilon}, 0\right) + \frac{1}{k}\frac{1}{1-\varepsilon} + \frac{1}{k}\right) =$$

$$= \max_{i\in\{1,\dots,k\}} \left(\frac{1+\frac{i}{k}-\left(\frac{i}{k}\right)^2}{2-\frac{i}{k}} - \max\left(\frac{i}{k}\frac{\frac{i}{k}-\varepsilon}{1-\varepsilon}, 0\right)\right) + \frac{1}{k}\left(\frac{1}{1-\varepsilon}+1\right) \leqslant$$

$$\leqslant \max_{x\in[0,1]} \left(\frac{1+x-x^2}{2-x} - \max\left(\frac{x^2-\varepsilon x}{1-\varepsilon}, 0\right)\right) + \frac{1}{k}\left(\frac{1}{1-\varepsilon}+1\right).$$

Устремляя k к бесконечности, получаем утверждение теоремы. ▲

§ 3. Оценки модулярности графов $G_p(n, r, s)$

3.1. Формулировка основных результатов. Введем формальное определение случайных графов $G_p(n, r, s)$. Множество вершин такого графа совпадает с множеством вершин графа $G(n, r, s)$, а множество ребер есть случайное подмножество $E_p(n, r, s)$ множества ребер графа $G(n, r, s)$, удовлетворяющее следующим свойствам:

1. Для любого e из $E(n, r, s)$ верно $\mathbf{P}(e \in E_p(n, r, s)) = p$;
2. Все индикаторы $\mathbb{1}\{e \in E_p(n, r, s)\}$ независимы в совокупности.

В данном параграфе будем считать, что графы $G_p(n, r, s)$ при всех n определены на одном вероятностном пространстве. Таким образом, элементарным исходом в таком вероятностном пространстве будет последовательность $\{H_i\}_{i=r}^{\infty}$, $H_i \sim G_p(i, r, s)$, причем все H_i независимы в совокупности.

На случай графов $G_p(n, r, s)$ удалось перенести теоремы 5 и 1.

Теорема 6. *Пусть r, s – фиксированные целые числа, для которых выполняется равенство*

$$r \geqslant -\frac{1}{\ln(1-\varepsilon)}s^2 + 2s - 1, \quad \text{где} \quad \varepsilon \in (0, 1).$$

Пусть также $p = p(n) = \omega\left(n^{-\frac{r-s-1}{2}}\right)$. Тогда почти наверное

$$\limsup_{n\to\infty} q^*(G_p(n, r, s)) \leqslant f(\varepsilon),$$

где $f(\varepsilon) = \max\limits_{x\in[0,1]} \left(\dfrac{1+x-x^2}{2-x} - \max\left(\dfrac{x^2-\varepsilon x}{1-\varepsilon}, 0\right)\right)$.

Теорема 7. *Пусть s и $r \geqslant 2s$ – фиксированные целые числа, $p = p(n) = \omega\left(n^{-\frac{r-s-1}{2}}\right)$. Тогда почти наверное*

$$\limsup_{n\to\infty} q^*(G_p(n, r, s)) \leqslant 1 - \frac{\binom{[r/2]}{s}}{2\binom{r}{s}}.$$

Также удалось перенести теорему 3, в которой, однако, пришлось ввести дополнительное ограничение на r.

Теорема 8. *Пусть $s \geqslant 1$ и $r \geqslant 2s$ – фиксированные целые числа, $p = p(n) = \omega\left(n^{-\frac{r-s-1}{2}}\right)$. Тогда почти наверное*

$$\liminf_{n\to\infty} q^*(G_p(n, r, s)) \geqslant \frac{s}{2r-s}\left(1 + \left(\frac{r-s}{r}\right)^{\frac{2r}{s}}\right).$$

3.2. Вспомогательные леммы. Для доказательства теорем 6–8 будем использовать следующее классическое неравенство, доказанное в [22].

Лемма 3 (неравенство Хёфдинга). *Пусть $X_1, \ldots, X_n$ – независимые случайные величины, причем при всех i существует пара чисел a_i, b_i, для которой $\mathbf{P}(X_i \in [a_i, b_i]) = 1$. Тогда для случайной величины $S_n = X_1 + \ldots + X_n$ выполняется следующее неравенство*:

$$\mathbf{P}(|S_n - \mathbf{E}S_n| \geqslant \varepsilon n) < 2\exp\left(-\frac{2\varepsilon^2 n^2}{\sum\limits_{i=1}^{n}(b_i - a_i)^2}\right).$$

Помимо этого, нам понадобится следующее тривиальное утверждение.

Предложение 1. *Пусть Q_n – последовательность событий, такая что $\mathbf{P}(\overline{Q_n}) \leqslant e^{-Cn}$ для некоторого $C > 0$. Тогда почти наверное найдется такое N, что все события Q_n, $n > N$, реализовались.*

Доказательство. Из условия теоремы следует, что

$$\sum_{i=1}^{\infty} \mathbf{P}\left(\overline{Q_n}\right) < +\infty.$$

Тогда по лемме Бореля – Кантелли почти наверное реализуется лишь конечное число событий $\overline{Q_n}$, откуда утверждение очевидно. ▲

Докажем с помощью этого оценку на число ребер в графах $G_p(n, r, s)$. Далее для краткости будем обозначать $G_n = G(n, r, s)$.

Лемма 4. *Пусть $p = p(n) = f(n)n^{-\frac{r-s-1}{2}}$, где $f(n) \to \infty$. Тогда почти наверное выполняется свойство*

$$\exists N : \forall n > N : |e(G_n, p) - pe(G_n)| < \frac{p\log f(n)}{f(n)} e(G_n).$$

Доказательство. Зафиксируем сначала достаточно большое $n \in \mathbb{N}$. По лемме 3 для $\varepsilon = \dfrac{p\log f(n)}{f(n)}$, $a_i = 0$, $b_i = 1$ имеем

$$\mathbf{P}(|e(G_n, p) - pe(G_n)| \geqslant \varepsilon e(G_n)) \leqslant 2e^{-2\varepsilon^2 e(G_n)} \leqslant e^{-Cn}.$$

Отметим, что имеет место гораздо более сильная оценка на вероятность

$$\mathbf{P}(|e(G_n, p) - pe(G_n)| \geqslant \varepsilon e(G_n)) \leqslant 2e^{-2\varepsilon^2 e(G_n)} \leqslant e^{-Cn^{r+1}\log^2 f(n)},$$

однако для доказательства требуемого утверждения достаточно оценки e^{-Cn}. Таким образом, при достаточно большом n имеем оценку

$$\mathbf{P}\left(|e(G_n, p) - pe(G_n)| \geqslant \frac{p\log f(n)}{f(n)} e(G_n)\right) \leqslant e^{-Cn}.$$

Для завершения доказательства осталось применить предложение 1. ▲

Отметим, что в дальнейшем мы будем использовать обозначения C_i (или C без индекса) для положительных констант.

Для доказательства теоремы 6 нам понадобятся следующие леммы.

Лемма 5. *Пусть r, s удовлетворяют неравенству*

$$r \geqslant -\frac{1}{\ln\left(\frac{1-\beta}{1-\frac{\alpha}{\beta}}\right)} s^2 + 2s - 1$$

при некоторых $\alpha, \beta \in (0,1)$, $\alpha < \beta^2$. Пусть также $p = p(n) = f(n) n^{-\frac{r-s-1}{2}}$, где $f(n) \to \infty$, $c > 0$. Тогда почти наверное выполняется свойство

$$\exists N : \forall n > N,\ \forall V \subset V_G,\ \binom{[cn]}{r-1} \leqslant |V| \leqslant \alpha \binom{n}{r} :$$

1. $\left|e(V, \overline{V}, p) - pe(V, \overline{V})\right| < \dfrac{p \log f(n)}{f(n)} e(V, \overline{V})$;
2. $\left|\sum\limits_{v \in V} \deg(v, p) - p \sum\limits_{v \in V} \deg(v)\right| < \dfrac{p \log f(n)}{f(n)} d_n |V|$,

где $d_n = \binom{r}{s}\binom{n-r}{r-s}$ – степень вершин $G(n, r, s)$.

Доказательство. Зафиксируем сначала достаточно большое $n \in \mathbb{N}$. Воспользуемся леммой 3 для $\varepsilon = \dfrac{p \log f(n)}{f(n)}$, $a_i = 0$, $b_i = 1$, а также следствием 1:

$$\mathbf{P}\left(|e(V, \overline{V}, p) - pe(V, \overline{V})| \geqslant \frac{p \log f(n)}{f(n)} e(V, \overline{V})\right) \leqslant 2e^{-2\varepsilon^2 e(V, \overline{V})} \leqslant$$
$$\leqslant 2 \exp\left(-C_0 n^{-r+s+1} \log^2 f(n) n^{r-s} n^{r-1}\right) \leqslant 2 \exp\left(-C_0 n^r \log^2 f(n)\right).$$

Теперь получим аналогичную оценку для утверждения 2. Заметим, что

$$\sum_{v \in V} \deg(v, p) \sim \mathrm{Bin}(e(V, \overline{V}), p) + 2\,\mathrm{Bin}(e(V), p),$$

где биномиальные слагаемые в правой части независимы. Тогда можно оценить эту сумму с помощью неравенства Хёфдинга для суммы $e(V, \overline{V}) + e(V)$ независимых слагаемых, где первые $e(V, \overline{V})$ слагаемых распределены как $\mathrm{Bern}(p)$, а остальные – как $2\,\mathrm{Bern}(p)$, $a_i = 0$, $b_i = 2$. Тогда получаем, что

$$\mathbf{P}\left(\left|\sum_{v \in V} \deg(v, p) - p \sum_{v \in V} \deg(v)\right| \geqslant \varepsilon d_n |V|\right) =$$
$$= \mathbf{P}\left(\left|\sum_{v \in V} \deg(v, p) - p \sum_{v \in V} \deg(v)\right| \geqslant \varepsilon (e(V, \overline{V}) + e(V))\right) \leqslant$$
$$\leqslant 2e^{-\frac{1}{2}\varepsilon^2 (e(V, \overline{V}) + e(V))} \leqslant 2e^{-\frac{1}{4}\varepsilon^2 d_n |V|}.$$

Подставляя $\varepsilon = \dfrac{p \log f(n)}{f(n)}$, получаем оценку

$$\mathbf{P}\left(\left|\sum_{v \in V} \deg(v, p) - p \sum_{v \in V} \deg(v)\right| \geqslant \varepsilon d_n |V|\right) \leqslant 2 \exp\left(-C_1 n^r \log^2 f(n)\right).$$

Оценим вероятность того, что хотя бы для одного из V, удовлетворяющему условию леммы, нарушилось какое-либо из неравенств. Для этого обозначим индикатор

события, соответствующего нарушению хотя бы одного из неравенств для некоторого множества V, через $\mathbb{1}_V$. Из предыдущих оценок очевидно, что

$$\mathbf{P}(\mathbb{1}_V = 1) \leqslant 4e^{-C_2 n^r \log^2 f(n)}.$$

Имеем

$$\mathbf{P}\left(\exists V : \binom{[cn]}{r-1} \leqslant |V| \leqslant \alpha\binom{n}{r},\ \mathbb{1}_V = 1\right)$$
$$\leqslant \sum_{\binom{cn}{r-1} \leqslant |V| \leqslant \alpha\binom{n}{r}} \binom{\binom{n}{r}}{|V|} 4e^{-C_2 n^r \log^2 f(n)} \leqslant \binom{n}{r}\binom{\binom{n}{r}}{\frac{1}{2}\binom{n}{r}} 4e^{-C_2 n^r \log^2 f(n)}.$$

Воспользуемся неравенством $\binom{2a}{a} < 2^{2a}$ для дальнейшей оценки вероятности:

$$\binom{n}{r}\binom{\binom{n}{r}}{\frac{1}{2}\binom{n}{r}} 4e^{-C_2 n^r \log^2 f(n)} < 2^n 2^{\binom{n}{r}} 4e^{-C_2 n^r \log^2 f(n)} \leqslant$$
$$\leqslant \exp\left(n\ln 2 + \binom{n}{r}\ln 2 + 2\ln 2 - C_2 n^r \log^2 f(n)\right) \leqslant e^{-C_3 n^r \log^2 f(n)} \leqslant e^{-Cn}.$$

Для завершения доказательства осталось применить предложение 1. ▲

Лемма 6. *Пусть r, s удовлетворяют неравенству*

$$r \geqslant -\frac{1}{\ln\left(\frac{1-\beta}{1-\alpha/\beta}\right)} s^2 + 2s - 1$$

при некоторых $\alpha, \beta \in (0,1)$, $\alpha < \beta^2$. Пусть также $p = p(n) = f(n) n^{-\frac{r-s-1}{2}}$, где $f(n) \to \infty$, $c > 0$. Тогда почти наверное выполняется свойство

$$\exists N : \forall n > N,\ \forall V \subset V_G,\ \binom{[cn]}{r-1} \leqslant |V| \leqslant \alpha\binom{n}{r} :$$

1. $\dfrac{e(V, \overline{V}, p)}{e(G_n, p)} = (1 + o(1)) \dfrac{e(V, \overline{V})}{e(G_n)}$;
2. $\dfrac{\left(\sum\limits_{v \in V} \deg(v, p)\right)^2}{4e^2(G_n, p)} = (1 + o(1)) \dfrac{|V|^2}{|V_G|^2}$.

Доказательство. Докажем сначала утверждение 1. Воспользовавшись леммами 5 и 4, оценим $\dfrac{e(V, \overline{V}, p)}{e(G_n, p)}$ сверху и снизу:

$$\frac{e(V, \overline{V})\left(p - \frac{p\log f(n)}{f(n)}\right)}{e(G_n)\left(p + \frac{p\log f(n)}{f(n)}\right)} \leqslant \frac{e(V, \overline{V}, p)}{e(G_n, p)} \leqslant \frac{e(V, \overline{V})\left(p + \frac{p\log f(n)}{f(n)}\right)}{e(G_n)\left(p - \frac{p\log f(n)}{f(n)}\right)},$$

откуда

$$\frac{e(V, \overline{V}, p)}{e(G_n, p)} = (1 + o(1)) \frac{e(V, \overline{V})}{e(G_n)}.$$

Аналогично для утверждения 2 выполняется цепочка неравенств

$$\frac{\Big(\sum\limits_{v\in V}\deg(v)\Big)^2\Big(p-\frac{p\log f(n)}{f(n)}\Big)^2}{4e^2(G_n)\Big(p+\frac{p\log f(n)}{f(n)}\Big)^2}\leqslant\frac{\Big(\sum\limits_{v\in V}\deg(v,p)\Big)^2}{4e^2(G_n,p)}\leqslant$$
$$\leqslant\frac{\Big(\sum\limits_{v\in V}\deg(v)\Big)^2\Big(p+\frac{p\log f(n)}{f(n)}\Big)^2}{4e^2(G_n)\Big(p-\frac{p\log f(n)}{f(n)}\Big)^2},$$

откуда

$$\frac{\Big(\sum\limits_{v\in V}\deg(v,p)\Big)^2}{4e^2(G_n,p)}=(1+o(1))\frac{\Big(\sum\limits_{v\in V}\deg(v)\Big)^2}{4e^2(G_n)}.\quad\blacktriangle$$

Для доказательства теоремы 7 нам понадобятся аналогичные леммы. Однако прежде чем формулировать и доказывать эти леммы, сформулируем аналог следствия 1, доказанный в работе [19].

Лемма 7. *Пусть* $k\geqslant 2$, $k\in\mathbb{N}$, $s\leqslant\left\lceil\frac{r}{2}\right\rceil$, $r,s\in\mathbb{N}$, $\varepsilon\in(0,1)$. *Тогда существует* $N:=N(\varepsilon,k)$, *такое что для любого* $n>N$ *и любого множества вершин* $V\in$ $\in V_G(n,r)$, *такого что*

$$|V|\in\left[\frac{1}{k}\binom{n}{r},\frac{k-1}{k}\binom{n}{r}\right],$$

верно неравенство

$$e(V,\overline{V})\geqslant\frac{\binom{[r/2]}{s}\binom{n-2r}{r-s}|V||\overline{V}|(1-\varepsilon)}{2\binom{n}{r}}.$$

Здесь $\overline{V}$ *– дополнение* V *до вершин графа* $G(n,r,s)$.

Теперь мы готовы сформулировать необходимые леммы.

Лемма 8. *Пусть* $r\geqslant 2s$, $p=p(n)=f(n)n^{-\frac{r-s-1}{2}}$, *где* $f(n)\to\infty$, $k\in\mathbb{N}$. *Тогда почти наверное выполняется свойство*

$$\exists N:\ \forall n>N,\ \forall V\subset V_G,\ \frac{1}{k}\binom{n}{r}\leqslant|V|\leqslant\frac{k-1}{k}\binom{n}{r}:$$

1. $\big|e(V,\overline{V},p)-pe(V,\overline{V})\big|<\dfrac{p\log f(n)}{f(n)}e(V,\overline{V})$;
2. $\left|\sum\limits_{v\in V}\deg(v,p)-pd_n|V|\right|<\dfrac{p\log f(n)}{f(n)}d_n|V|$.

Доказательство. Зафиксируем сначала достаточно большое $n\in\mathbb{N}$. Воспользуемся леммой 3 для $\varepsilon=\dfrac{p\log f(n)}{f(n)}$, $a_i=0$, $b_i=1$, а также леммой 7:

$$\mathbf{P}\left(|e(V,\overline{V},p)-pe(V,\overline{V})|\geqslant\frac{p\log f(n)}{f(n)}e(V,\overline{V})\right)\leqslant 2e^{-2\varepsilon^2e(V,\overline{V})}\leqslant$$

$$\leqslant 2\exp\left(-C_0 n^{-r+s+1}\log^2 f(n) n^{r-s} n^r\right) \leqslant 2\exp\left(-C_0 n^{r+1}\log^2 f(n)\right).$$

Теперь получим аналогичную оценку для утверждения 2. Заметим, что

$$\sum_{v\in V}\deg(v,p) \sim \mathrm{Bin}(e(V,\overline{V}),p) + 2\,\mathrm{Bin}(e(V),p),$$

где биномиальные слагаемые в правой части независимы. Тогда мы можем оценить эту сумму с помощью неравенства Хёфдинга для суммы $e(V,\overline{V})+e(V)$ независимых слагаемых, где первые $e(V,\overline{V})$ слагаемых распределены как $\mathrm{Bern}(p)$, а остальные – как $2\,\mathrm{Bern}(p)$, $a_i = 0$, $b_i = 2$. Тогда получаем, что

$$\begin{aligned}
&\mathbf{P}\left(\left|\sum_{v\in V}\deg(v,p) - p\sum_{v\in V}\deg(v)\right| \geqslant \varepsilon d_n |V|\right) = \\
&= \mathbf{P}\left(\left|\sum_{v\in V}\deg(v,p) - p\sum_{v\in V}\deg(v)\right| \geqslant \varepsilon(e(V,\overline{V})+e(V))\right) \leqslant \\
&\leqslant 2e^{-\frac{1}{2}\varepsilon^2(e(V,\overline{V})+e(V))} \leqslant 2e^{-\frac{1}{4}\varepsilon^2 d_n|V|}.
\end{aligned}$$

Подставляя $\varepsilon = \dfrac{p\log f(n)}{f(n)}$, получаем оценку

$$\mathbf{P}\left(\left|\sum_{v\in V}\deg(v,p) - p\sum_{v\in V}\deg(v)\right| \geqslant \varepsilon d_n |V|\right) \leqslant 2\exp\left(-C_1 n^r \log^2 f(n)\right).$$

Оценим вероятность того, что хотя бы для одного из V, удовлетворяющих условию леммы, нарушилось какое-либо из неравенств. Для этого обозначим индикатор события, соответствующего нарушению хотя бы одного из неравенств для некоторого множества V, через $\mathbb{1}_V$. Из предыдущих оценок очевидно, что

$$\mathbf{P}(\mathbb{1}_V = 1) \leqslant 4e^{-C_2 n^r \log^2 f(n)}.$$

Имеем

$$\begin{aligned}
&\mathbf{P}\left(\exists V:\ \binom{[cn]}{r-1} \leqslant |V| \leqslant \alpha\binom{n}{r},\ \mathbb{1}_V = 1\right) \\
&\leqslant \sum_{\frac{1}{k}\binom{n}{r}\leqslant|V|\leqslant\frac{k-1}{k}\binom{n}{r}} \binom{\binom{n}{r}}{|V|} 4e^{-C_2 n^r\log^2 f(n)} \leqslant \binom{n}{r}\binom{\binom{n}{r}}{\frac{1}{2}\binom{n}{r}} 4e^{-C_2 n^r\log^2 f(n)}.
\end{aligned}$$

Воспользуемся неравенством $\binom{2a}{a} < 2^{2a}$ для дальнейшей оценки вероятности:

$$\begin{aligned}
&\binom{n}{r}\binom{\binom{n}{r}}{\frac{1}{2}\binom{n}{r}} 4e^{-C_2 n^r\log^2 f(n)} < 2^n 2^{\binom{n}{r}} 4e^{-C_2 n^r\log^2 f(n)} \leqslant \\
&\leqslant \exp\left(n\ln 2 + \binom{n}{r}\ln 2 + 2\ln 2 - C_2 n^r \log^2 f(n)\right) \leqslant e^{-C_3 n^r\log^2 f(n)} \leqslant e^{-Cn}.
\end{aligned}$$

Для завершения доказательства осталось применить предложение 1. ▲

Лемма 9. *Пусть $r \geqslant 2s$, $p = p(n) = f(n)n^{-\frac{r-s-1}{2}}$, где $f(n)\to\infty$, $k\in\mathbb{N}$. Тогда почти наверное выполняется свойство*

$$\exists N:\ \forall n > N,\ \forall V\subset V_G,\ \frac{1}{k}\binom{n}{r} \leqslant |V| \leqslant \frac{k-1}{k}\binom{n}{r}:$$

1. $\dfrac{e(V,\overline{V},p)}{e(G_n,p)} = (1+o(1))\dfrac{e(V,\overline{V})}{e(G_n)}$;

2. $\dfrac{\Big(\sum\limits_{v\in V}\deg(v,p)\Big)^2}{4e^2(G_n,p)} = (1+o(1))\dfrac{|V|^2}{|V_G|^2}$.

Доказательство дословно совпадает с доказательством леммы 6. ▲

Также нам понадобится определить построение из $\mathcal{A}$ множеств $\mathcal{A}'$ и $\mathcal{A}_{\text{big}}$, которое использовалось в работе [19].

Конструкция 1. Пусть $k \geqslant 2$, $k \in \mathbb{N}$. Определим алгоритм построения множеств $\mathcal{A}'$ и $\mathcal{A}_{\text{big}}$ по разбиению $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$. Нам потребуется вспомогательное множество A_{merged}, исходно оно пусто.

Проходим по всем $i \in \{1, 2, \ldots, m\}$:

- Если $|A_i| > \dfrac{1}{k}\binom{n}{r}$, то добавляем A_i в A';
- Если $|A_i| \leqslant \dfrac{1}{k}\binom{n}{r}$:
  - Если $|A_i| + |A_{\text{merged}}| < \dfrac{1}{k}\binom{n}{r}$, то $A_{\text{merged}} := A_{\text{merged}} \cup A_i$;
  - Если $|A_i|+|A_{\text{merged}}| \geqslant \dfrac{1}{k}\binom{n}{r}$, то текущее A_{merged} добавляется в $\mathcal{A}'$ и $A_{\text{merged}} := A_i$.

После итерирования по всем $A_i \in \mathcal{A}$, смотрим на множество A_{merged}:

- Если $|A_{\text{merged}}| > \dfrac{1}{k}\binom{n}{r}$, то A_{merged} добавляется в $\mathcal{A}'$;
- Если $|A_{\text{merged}}| \leqslant \dfrac{1}{k}\binom{n}{r}$, то A_{merged} игнорируется.

Множество $\mathcal{A}_{\text{big}}$ легко определить по $\mathcal{A}'$:

$$\mathcal{A}_{\text{big}} := \left\{A :\ A \in \mathcal{A}',\ |A| > \frac{2}{k}\binom{n}{r}\right\}.$$

Приведем часть доказательства теоремы 1 из работы [19] в виде леммы.

Лемма 10. *Пусть r, s таковы, что $r \geqslant \left\lfloor \dfrac{s}{2} \right\rfloor$. Пусть также $k \geqslant 2$, $k \in \mathbb{N}$, и $\varepsilon > 0$. Возьмем разбиение $\mathcal{A}$ и построим по нему множества $\mathcal{A}'$ и $\mathcal{A}_{\text{big}}$ с помощью конструкции* 1. *Тогда*

$$\frac{1}{2}\sum_{A\in\mathcal{A}'}\frac{e(V_A,\overline{V_A})}{e(G)} + \sum_{A\in\mathcal{A}_{\text{big}}}\left(\frac{|V_A|}{\binom{n}{r}}\right)^2 \geqslant \frac{\binom{\lceil r/2\rceil}{s}}{2\binom{r}{s}}(1-\varepsilon)\left(1-\frac{1}{k}\right) - \frac{1}{k}.$$

Наконец, для доказательства теоремы 8 нам понадобится описать разбиение, оценка модулярности которого и послужила основой доказательства теоремы 3.

Конструкция 2. Рассмотрим следующее разбиение графа $G(n, r, s)$:

$$A_i := \{v \in G(n,r,s) :\ i \in v,\ \forall j > i :\ j \notin v\}$$

для всех i из $\{r, r+1, \ldots, n\}$. Нетрудно видеть, что $|A_i| = \binom{i-1}{r-1}$, а

$$e(A_i) = \frac{1}{2}\binom{i-1}{r-1}\binom{r-1}{s-1}\binom{i-r}{r-s}.$$

Тогда желаемая конструкция имеет вид

$$\mathcal{A} = \left\{ A_n, \dots, A_{[cn]+1}, \bigcup_{i=r}^{[cn]} A_i \right\}, \quad c = \left(\frac{r-s}{r}\right)^{\frac{1}{s}}.$$

Помимо этого, в доказательстве теоремы 8 будет использована лемма 6.

3.3. Доказательство теорем 6 и 7.

Доказательство теоремы 6. В доказательстве мы можем рассматривать только достаточно большие n, поэтому без ограничения общности считаем, что

$$2\binom{n}{r-1} > \alpha\binom{n}{r}.$$

Рассмотрим функцию

$$\alpha(x) = x\frac{x-\varepsilon}{1-\varepsilon} < x^2.$$

В силу непрерывности этой функции, существует такое β, что $\alpha(\beta) \in (0,1)$, где $1-\alpha^2(\beta) < f(\varepsilon)$.

Отметим, что при данных α, β выполняется соотношение

$$r \geqslant -\frac{1}{\ln(1-\varepsilon)}s^2 + 2s - 1 = -\frac{1}{\ln\left(\frac{1-\beta}{1-\alpha/\beta}\right)}s^2 + 2s - 1,$$

поэтому мы можем использовать лемму 6 с данными α и β.

В силу монотонности степенного штрафа по множеству мы знаем, что для почти всех последовательностей $G_n^p \in G_p(n,r,s)$ разбиения, содержащие множества размера хотя бы $\alpha\binom{n}{r} - 2\binom{n}{r-1}$, обладают модулярностью

$$q^*(G_n^p) < 1 - \frac{\alpha^2\binom{n}{r}^2}{\binom{n}{r}^2}(1+o(1)) = 1 - \alpha^2(1+o(1)),$$

не превосходящей требуемой оценки.

Таким образом, без ограничения общности можно считать, что оптимальное разбиение всех графов $G \in G_p(n,r,s)$ содержит только множества с размером меньше чем $\alpha\binom{n}{r} - 2\binom{n}{r-1}$.

Рассмотрим оптимальное разбиение $\mathcal{A}$ графа $G_n^p \in G_p(n,r,s)$. Опишем процесс преобразования $\mathcal{A}$ в новое разбиение $\mathcal{A}'$:

- Пока есть хотя бы две части разбиения $\mathcal{A}$ размера меньше $\binom{n}{r-1}$, склеиваем их;
- Если в какой-то момент у нас осталась только одна часть разбиения, имеющая размер меньше $\binom{n}{r-1}$, то приклеиваем ее к какой-то из оставшихся частей.

Отметим, что после выполнения алгоритма для каждого из полученных множеств будет выполняться условие

$$\binom{n}{r-1} \leqslant |U| \leqslant \alpha\binom{n}{r}.$$

Оценим, на какую величину могла уменьшиться модулярность при таком процессе. Заметим, что реберный вклад нестрого возрастал, поэтому достаточно оценить изменение размера степенного штрафа.

Сначала разберем случай, когда процесс закончился после склеивания двух маленьких частей. Рассмотрим все множества $\mathcal{A}_{\text{new}} := \{A \in \mathcal{A}' : A \notin \mathcal{A}\}$, которые появились в ходе нашего процесса. Очевидно, размер любого множества из $\mathcal{A}_{\text{new}}$ не больше чем $2\binom{n}{r-1}$, что дает возможность применить для них лемму 6. Тогда степенной штраф асимптотически почти наверное увеличился не более чем на

$$\sum_{A\in\mathcal{A}_{\text{new}}} \frac{\Big(\sum\limits_{v\in A}\deg(v,p)\Big)^2}{4e^2(G,p)} = (1+o(1))\sum_{A\in\mathcal{A}_{\text{new}}}\frac{|A|^2}{|V_G|^2} \leqslant (1+o(1))\frac{2\binom{n}{r-1}}{\binom{n}{r}} = O(n^{-1}).$$

Теперь посмотрим на изменение степенного штрафа, когда процесс закончился доклеиванием одного маленького множества (обозначим его через B) к какому-то из оставшихся множеств C. В данном случае для всех $A \in \mathcal{A}_{\text{new}} \setminus \{B\cup C\}$ выполнено $|A| \leqslant 2\binom{n}{r-1}$, а значит, и нужная оценка. Осталось провести оценку для $B \cup C$:

$$\frac{\Big(\sum\limits_{v\in B\cup C}\deg(v,p)\Big)^2}{4e^2(G,p)} - \frac{\Big(\sum\limits_{v\in B}\deg(v,p)\Big)^2}{4e^2(G,p)} - \frac{\Big(\sum\limits_{v\in C}\deg(v,p)\Big)^2}{4e^2(G,p)} \leqslant$$
$$\leqslant \frac{\Big(\sum\limits_{v\in B\cup C}\deg(v,p)\Big)^2}{4e^2(G,p)} - \frac{\Big(\sum\limits_{v\in C}\deg(v,p)\Big)^2}{4e^2(G,p)} = (1+o(1))\left(\frac{(|B|+|C|)^2}{|V_G|^2} - \frac{|C|^2}{|V_G|^2}\right) =$$
$$= (1+o(1))\frac{|B|(|B|+2|C|)}{|V_G|^2} \leqslant 2(1+o(1))\frac{|B|}{|V_G|} = O(n^{-1}).$$

Итак, удалось доказать, что для почти всех последовательностей $G_n^p \in G_p(n,r,s)$ существуют разбиения $\mathcal{A}'_n$ графов G_n^p, удовлетворяющее условию

$$q^*(G_n^p) - q(\mathcal{A}'_n) = O(n^{-1}), \quad \forall U \in \mathcal{A}'_n : \binom{n}{r-1} \leqslant |U| \leqslant \alpha\binom{n}{r}.$$

Для таких разбиений в силу леммы 6 имеем

$$q(\mathcal{A}'_n) = 1 - \frac{1}{2}\sum_{A\in\mathcal{A}'_n}\frac{e(A,\overline{A},p)}{e(G,p)} - \sum_{A\in\mathcal{A}'_n}\frac{\Big(\sum\limits_{v\in A}\deg(v)\Big)^2}{4e^2(G,p)} =$$
$$= (1+o(1))\left(1 - \frac{1}{2}\sum_{A\in\mathcal{A}'_n}\frac{e(A,\overline{A})}{e(G)} - \sum_{A\in\mathcal{A}'_n}\frac{|A|^2}{|V_G|^2}\right) =$$
$$= (1+o(1))\left(\sum_{A\in\mathcal{A}'_n}\frac{e(A)}{e(G)} - \sum_{A\in\mathcal{A}'_n}\frac{|A|^2}{|V_G|^2}\right),$$

после чего доказательство дословно повторяет рассуждения теоремы 5. ▲

Доказательство теоремы 7. Пойдем по пути доказательства теоремы 1 с небольшими изменениями:

$$q(\mathcal{A}) = \sum_{A\in\mathcal{A}} \frac{e(A,p)}{e(G,p)} - \sum_{A\in\mathcal{A}} \frac{\Big(\sum\limits_{v\in V_A} \deg(v,p)\Big)^2}{4e^2(G,p)} =$$

$$= 1 - \frac{1}{2}\sum_{A\in\mathcal{A}} \frac{e(V_A,\overline{V_A},p)}{e(G,p)} - \sum_{A\in\mathcal{A}} \frac{\Big(\sum\limits_{v\in V_A} \deg(v,p)\Big)^2}{4e^2(G,p)}.$$

Строим по разбиению $\mathcal{A}$ множества $\mathcal{A}'$ и $\mathcal{A}_{\text{big}}$ по алгоритму из конструкции 1. Для них выполнены следующие условия:

$$\forall A\in\mathcal{A}':\ |A| > \frac{1}{k}\binom{n}{r}, \quad \forall A\in\mathcal{A}_{\text{big}}:\ |A| \geqslant \frac{2}{k}\binom{n}{r}.$$

Для случайного графа по-прежнему верно, что

$$q(\mathcal{A}) \leqslant 1 - \frac{1}{2}\sum_{A\in\mathcal{A}'} \frac{e(V_A,\overline{V_A},p)}{e(G,p)} - \sum_{A\in\mathcal{A}_{\text{big}}} \frac{\Big(\sum\limits_{v\in V_A} \deg(v,p)\Big)^2}{4e^2(G,p)}.$$

Воспользуемся леммой 6 и получим

$$q(\mathcal{A}) \leqslant 1 - \frac{1}{2}(1+o(1))\sum_{A\in\mathcal{A}'} \frac{e(V_A,\overline{V_A})}{e(G)} - (1+o(1))\sum_{A\in\mathcal{A}_{\text{big}}} \frac{\Big(\sum\limits_{v\in V_A} \deg(v)\Big)^2}{4e^2(G)} =$$

$$= 1 - (1+o(1))\left(\frac{1}{2}\sum_{A\in\mathcal{A}'} \frac{e(V_A,\overline{V_A})}{e(G)} + \sum_{A\in\mathcal{A}_{\text{big}}} \left(\frac{|V_A|}{\binom{n}{r}}\right)^2\right).$$

Дальше по лемме 10 воспользуемся оценкой на суммы в скобках:

$$q(\mathcal{A}) \leqslant 1 - (1+o(1))\left(\frac{\binom{\lceil r/2\rceil}{s}}{2\binom{r}{s}}(1-\varepsilon)\Big(1-\frac{1}{k}\Big) - \frac{1}{k}\right).$$

Устремляя n и k к бесконечности и пользуясь тем, что $\varepsilon > 0$, получаем

$$q(\mathcal{A}) \leqslant 1 - \frac{\binom{\lceil r/2\rceil}{s}}{2\binom{r}{s}}. \quad \blacktriangle$$

3.4. Доказательство теоремы 8. Рассмотрим разбиение $\mathcal{A}$ из конструкции 2. Нетрудно видеть, что при $[cn] \geqslant r$ каждый элемент этого разбиения имеет размер не меньше чем $\binom{[cn]}{r-1}$ и не больше чем $\binom{[cn]}{r} \leqslant c^r\binom{n}{r}$. Выберем $\varepsilon\in(0,1)$ таким, что $\ln(1-\varepsilon) < -s^2$, тогда

$$\frac{-1}{\ln(1-\varepsilon)} < \frac{1}{s^2}.$$

Теперь обратим внимание на функцию $\alpha(x) = x\dfrac{x-\varepsilon}{1-\varepsilon}$. Как было доказано ранее, $\alpha(x) < x^2, x \in (0,1)$. Заметим, что $\alpha(x)$ непрерывна на $\mathbb{R}$, а $\alpha(1) = 1$, поэтому существует $\beta \in (0,1)$, для которого $\alpha(\beta) = c^r$.

Убедимся, что r, s удовлетворяют условиям теоремы 4 с выбранными α и β. Действительно, так как $\ln\Big(\dfrac{1-\beta}{1-\alpha/\beta}\Big) = \ln(1-\varepsilon)$, имеем

$$r \geqslant 2s = 2s + \frac{s^2}{s^2} - 1 > -\frac{s^2}{\ln(1-\varepsilon)} + 2s - 1 = -\frac{s^2}{\ln\Big(\dfrac{1-\beta}{1-\alpha/\beta}\Big)} + 2s - 1.$$

Применяя лемму 6, получаем, что модулярность разбиения $\mathcal{A}$ как разбиения $G_p(n,r,s)$ почти наверное равна $(1+o(1))q(\mathcal{A})$, где $q(\mathcal{A})$ – модулярность разбиения $\mathcal{A}$ как разбиения $G(n,r,s)$. Наконец, применяя теорему 3, получаем требуемое утверждение. ▲

Авторы выражают благодарность проф. А.М. Райгородскому за постановку задачи и обсуждение полученных результатов.

СПИСОК ЛИТЕРАТУРЫ

1. *Newman M.E.J., Girvan M.* Finding and Evaluating Community Structure in Networks // Phys. Rev. E. 2004. V. 69. № 2. P. 026113 (15 pp.). https://doi.org/10.1103/PhysRevE.69.026113
2. *Lancichinetti A., Fortunato S.* Limits of Modularity Maximization in Community Detection // Phys. Rev. E. 2011. V. 84. № 6. P. 066122 (8 pp.). https://doi.org/10.1103/PhysRevE.84.066122
3. *Miasnikof P., Prokhorenkova L., Shestopaloff A.Y., Raigorodskii A.* A Statistical Test of Heterogeneous Subgraph Densities to Assess Clusterability // Learning and Intelligent Optimization (13th Int. Conf. LION'13. Chania, Crete, Greece. May 27–31, 2019. Revised Selected Papers). Lect. Notes Comput. Sci. V. 11968. Cham: Springer, 2000. P. 17–29. https://doi.org/10.1007/978-3-030-38629-0_2
4. *Newman M.E.J.* Fast Algorithm for Detecting Community Structure in Networks // Phys. Rev. E. 2004. V. 69. № 6. P. 066133 (5 pp.). https://doi.org/10.1103/PhysRevE.69.066133
5. *Ostroumova Prokhorenkova L.* General Results on Preferential Attachment and Clustering Coefficient // Optim. Lett. 2017. V. 11. № 2. P. 279–298. https://doi.org/10.1007/s11590-016-1030-8
6. *Porter M.A., Onnela J.-P., Mucha P.J.* Communities in Networks // Notices Amer. Math. Soc. 2009. V. 56. № 9. P. 1082–1097. Available at https://www.ams.org/notices/200909/rtx090901082p.pdf.
7. *Brandes U., Delling D., Gaertler M., Görke R., Hoefer M., Nikoloski Z., Wagner D.* On Finding Graph Clusterings with Maximum Modularity // Graph-Theoretic Concepts in Computer Science (33rd Int. Workshop WG'2007. Dornburg, Germany. June 21–23, 2007. Revised Papers). Lect. Notes Comput. Sci. V. 4769. Berlin: Springer, 2007. P. 121–132. https://doi.org/10.1007/978-3-540-74839-7_12
8. *De Montgolfier F., Soto M., Viennot L.* Asymptotic Modularity of Some Graph Classes // Algorithms and Computation (Proc. 22nd Int. Sympos. ISAAC'2011. Yokahama, Japan. Dec. 5–8, 2011). Lect. Notes Comput. Sci. V. 7074. Berlin: Springer, 2011. P. 435–444. https://doi.org/10.1007/978-3-642-25591-5_45
9. *Trajanovski S., Wang H., Van Mieghem P.* Maximum Modular Graphs // Eur. Phys. J. B. 2012. V. 85. № 7. Art. 244 (14 pp.) https://doi.org/10.1140/epjb/e2012-20898-3
10. *McDiarmid C., Skerman F.* Modularity of Regular and Treelike Graphs // J. Complex Netw. 2018. V. 6. № 4. P. 596–619. https://doi.org/10.1093/comnet/cnx046

11. *Ostroumova Prokhorenkova L., Prałat P., Raigorodskii A.* Modularity in Several Random Graph Models // Electron. Notes Discrete Math. 2017. V. 61. P. 947–953. https://doi.org/10.1016/j.endm.2017.07.058
12. *Bollobás B.* The Isoperimetric Number of Random Regular Graphs // European J. Combin. 1988. V. 9. № 3. P. 241–244. https://doi.org/10.1016/S0195-6698(88)80014-3
13. *McDiarmid C., Skerman F.* Modularity of Erdős–Rényi Random Graphs // Random Structures Algorithms. 2020. V. 57. № 1. P. 211–243. https://doi.org/10.1002/rsa.20910
14. *Bollobás B., Narayanan B.P., Raigorodskii A.M.* On the Stability of the Erdős–Ko–Rado Theorem // J. Combin. Theory Ser. A. 2016. V. 137. P. 64–78. https://doi.org/10.1016/j.jcta.2015.08.002
15. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
16. *Frankl P., Wilson R.M.* Intersection Theorems with Geometric Consequences // Combinatorica. 1981. V. 1. № 4. P. 357–368. https://doi.org/10.1007/BF02579457
17. *Kahn J., Kalai G.* A Counterexample to Borsuk's Conjecture // Bull. Amer. Math. Soc. (N.S.). 1993. V. 29. № 1. P. 60–62. https://doi.org/10.1090/S0273-0979-1993-00398-7
18. *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
19. *Ipatov M.M., Koshelev M.M., Raigorodskii A.M.* Modularity of Some Distance Graphs // European J. Combin. (submitted).
20. *Ipatov M.M.* Exact Modularity of Line Graphs of Complete Graphs // Moscow J. Comb. Number Theory. 2021. V. 10. № 1. P. 61–75. https://doi.org/10.2140/moscow.2021.10.61
21. *Koshelev M.M.* New Lower Bound on the Modularity of Johnson Graphs // Moscow J. Comb. Number Theory. 2021. V. 10. № 1. P. 77–82. https://doi.org/10.2140/moscow.2021.10.77
22. *Hoeffding W.* Probability Inequalities for Sums of Bounded Random Variables // J. Amer. Statist. Assoc. 1963. V. 58. № 301. P. 13–30. https://doi.org/10.2307/2282952

Деревянко Никита Михайлович
Московский физико-технический институт
(национальный исследовательский университет)
nikitaderevyanko@gmail.com
Кошелев Михаил Михайлович
Московский государственный университет
им. М.В. Ломоносова
mkoshelev99@gmail.com

Поступила в редакцию
22.06.2021
После доработки
27.11.2021
Принята к публикации
27.11.2021

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»