ISSN 0555-2923

РОССИЙСКАЯ АКАДЕМИЯ НАУК

Проблемы передачи информации

том 59 вып. 3

2023

РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

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

Том 59, 2023 **Вып. 3**

М о с к в а

С О Д Е Р Ж А Н И Е

Теория кодирования

CONTENTS

Coding Theory

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 3**

УДК 621.391 : 519.725.3

© 2023 г. **И. Станоевич, В. Шенк**

СВЕРТОЧНЫЕ КОДЫ С ОПТИМАЛЬНЫМ ДВУСТОРОННИМ ПРОФИЛЕМ РАССТОЯНИЙ[1]

Двусторонний профиль расстояний (ДПР) сверточного кода определяется как минимум из профилей расстояний этого кода и соответствующего ему "инверсного" кода. Представлены таблицы кодов с оптимальным ДПР (ОДПР-кодов), минимизирующих среднюю сложность алгоритмов двустороннего последовательного декодирования. Компьютерный поиск можно ускорить благодаря тому, что коды с оптимальным профилем расстояния (ОПР) большей памяти имеют в качестве своих префиксов ОПР-коды меньшей памяти, а также тому, что ОДПР-коды можно получать путем конкатенации ОПР- и инверсных ОПР-кодов с меньшей памятью. С помощью моделирования проводится сравнение производительности ОДПР-кодов и других кодов.

Ключевые слова: сверточные коды, профиль расстояний, двустороннее декодирование.

DOI: 10.31857/S0555292323030014, **EDN:** FQBJWI

§ 1. Введение

Пусть

$$G(D) = \begin{bmatrix} g_{11}(D) & \dots & g_{1n}(D) \\ \dots\dots\dots\dots\dots & & \\ g_{k1}(D) & \dots & g_{kn}(D) \end{bmatrix} \tag{1}$$

– порождающая матрица сверточного кодера со скоростью $R = k/n$, где $g_{ij}(D) \in \in \mathbb{F}_2[D]$ – двоичные порождающие многочлены, и пусть $m = \max\limits_{i,j} \deg(g_{ij}(D))$ – его память.

Тогда ℓ-м значением функции столбцового расстояния (ФСР) кода [1] называется

$$d_\ell = \min_{\boldsymbol{u}:\, \boldsymbol{u}_0 \neq \boldsymbol{0}} w_{\mathrm{H}}(\boldsymbol{v}_{[0,\ell]}), \tag{2}$$

где $w_{\mathrm{H}}(\cdot)$ – вес Хэмминга последовательности, двоичные векторы $\boldsymbol{u} = (\boldsymbol{u}_0, \boldsymbol{u}_1, \dots)$ и $\boldsymbol{v} = (\boldsymbol{v}_0, \boldsymbol{v}_1, \dots)$ представляют собой k-мерную информационную последовательность и n-мерное кодовое слово соответственно, и для последовательности $\boldsymbol{x}$ мы обозначаем $x_{[a,b]} = (x_a, x_{a+1}, \dots, x_b)$. Если для двух ФСР $\boldsymbol{d} = (d_0, d_1, \dots)$ и $\boldsymbol{d}' = (d'_0, d'_1, \dots)$ выполнены условия $d_0 = d'_0$, $\dots$, $d_{\ell-1} = d'_{\ell-1}$, $d_\ell > d'_\ell$ для некоторого ℓ, то будем говорить, что $\boldsymbol{d}$ лучше, чем $\boldsymbol{d}'$, или $\boldsymbol{d} > \boldsymbol{d}'$. Кодом с оптимальной ФСР $\boldsymbol{d}^*$ для заданных параметров k, n и m будем называть такой код, для которого не существует другого кода с теми же параметрами, чья ФСР $\boldsymbol{d}$ лучше, чем $\boldsymbol{d}^*$. Профилем расстояний (ПР)

[1] Работа выполнена при поддержке Министерства образования, науки и технологического развития Республики Сербия в рамках проекта № 451-03-68/2020-14/200156: "Инновационные научные и творческие исследования в области деятельности факультета технических наук".

кода [1] называется его усеченная ФСР $d_{[0,m]}$, где сравнение и оптимальность определяются таким же образом. Чтобы иметь бóльшую гибкость при выборе оптимизируемых свойств кода, определим также укороченный профиль расстояний $\text{ПР}^{(s)}$ для $s < m$ как $d_{[0,m-s]}$, и для удобства обозначений будем обозначать ФСР через $\text{ПР}^{(-\infty)}$.

В наиболее часто используемых алгоритмах последовательного декодирования, таких как стек-алгоритм [2, 3] и алгоритм Фано [4], применение ОПР-кодов минимизирует среднее число расширений узлов кодового дерева. Влияние ФСР и ПР на сложность декодирования было изучено для двоичного симметричного канала [5] и канала с аддитивным белым гауссовским шумом (АБГШ-канала) [6]. В обоих случаях желательно, чтобы значения d_ℓ росли как можно быстрее в начале ФСР, откуда и вытекает определение ее оптимальности, причем начальные значения оказывают более существенное влияние. ОПР-коды и коды, оптимизированные по другим критериям, широко исследовались, например, в [7–15].

Хотя сложность стандартных алгоритмов однонаправленного декодирования минимизируется при использовании ОПР-кодов, это не относится к алгоритмам двустороннего декодирования, например, [16–19]. Количество посещенных узлов в прямом кодовом дереве зависит от ПР исходного кода (прямой ПР), а в обратном кодовом дереве – от ПР "инверсного" кода (обратный ПР).

В большинстве случаев, когда алгоритм последовательного декодирования не способен выдать правильную последовательность, это связано со слишком большим количеством посещенных узлов в его кодовом дереве (деревьях), что приводит к переполнению памяти или чрезмерно большому времени декодирования. В § 2 описывается процедура эффективного поиска кодов, удобных для декодирования алгоритмами двустороннего последовательного декодирования. Коды с оптимизированным прямым и обратным ПР стремятся минимизировать количество узлов в обоих кодовых деревьях декодера. В § 3 представлены коды, найденные с помощью этой процедуры для некоторых из выбранных наборов параметров. В § 4 производительность этих кодов сравнивается с другими оптимизированными кодами, используемыми при декодировании по методу максимального правдоподобия (Витерби), а также при одностороннем и двустороннем стековом декодировании. Улучшения в терминах вероятности ошибки на блок (FER) и общей сложности декодирования вычисляются с помощью имитационного моделирования.

§ 2. Двусторонний профиль расстояний

Пусть $\bar{G}(D) = D^m G(D^{-1})$ – порождающая матрица инверсного кода для кода, порожденного матрицей $G(D)$, с элементами $\bar{g}_{ij}(D)$. Пусть $\boldsymbol{\bar{d}} = (\bar{d}_0, \bar{d}_1, \ldots)$ – ФСР инверсного кода. Чтобы учитывать оба направления декодирования, определим двустороннюю ФСР (ДФСР) $\widehat{\boldsymbol{d}}$ как последовательность значений $\widehat{d}_\ell = \min(d_\ell, \bar{d}_\ell)$ и двусторонний $\text{ПР}^{(s)}$ ($\text{ДПР}^{(s)}$) как $\widehat{d}_{[0,m-s]}$, а также соответствующие оптимальные ДФСР- и $\text{ДПР}^{(s)}$-коды (ОДФСР- и $\text{ОДПР}^{(s)}$-коды).

Через $g_{ij}^{(\ell)}$ обозначим ℓ-й коэффициент порождающего многочлена $g_{ij}(D)$, и положим

$$G^{(\ell)} = \begin{bmatrix} g_{11}^{(\ell)} & \cdots & g_{1n}^{(\ell)} \\ \cdots\cdots\cdots\cdots \\ g_{k1}^{(\ell)} & \cdots & g_{kn}^{(\ell)} \end{bmatrix} \tag{3}$$

и

$$G^{[a,b]}(D) = \sum_{\ell=a}^{b} G^{(\ell)} D^\ell, \tag{4}$$

$$\bar{G}^{[a,b]}(D) = \sum_{\ell=a}^{b} G^{(m-\ell)} D^{\ell}, \tag{5}$$

так что $G(D) = G^{[0,m]}(D)$ и $\bar{G}(D) = \bar{G}^{[0,m]}(D)$. Кроме того, для

$$G(D) = G^{[0,p]}(D) + G^{[p+1,m]}(D)$$

будем говорить, что $G^{[0,p]}(D)$ является префиксом $G(D)$ и что $G(D)$ получена конкатенацией $G^{[0,p]}(D)$ и $G^{[p+1,m]}(D)$. Нетрудно видеть, что если код, задаваемый матрицей $G(D)$, является ОПР-кодом, то код, задаваемый матрицей $G^{[0,p]}(D)$, также должен быть ОПР-кодом.

Если память кода m нечетна, то можно рассмотреть аналогичное разложение порождающей матрицы в виде

$$G(D) = G^{\mathrm{F}}(D) + D^m G^{\mathrm{B}}(D^{-1}), \tag{6}$$

где

$$G^{\mathrm{F}}(D) = G^{[0,(m-1)/2]}(D), \tag{7}$$

$$G^{\mathrm{B}}(D) = \bar{G}^{[0,(m-1)/2]}(D). \tag{8}$$

В этом случае мы называем $G^{\mathrm{F}}(D)$ прямой половиной матрицы $G(D)$, а $G^{\mathrm{B}}(D)$ – обратной половиной, и порождающую матрицу инверсного кода можно выразить как

$$\bar{G}(D) = G^{\mathrm{B}}(D) + D^m G^{\mathrm{F}}(D^{-1}).$$

Из определений соответствующих ФСР видно, что $d_{[0,(m-1)/2]}$ зависит только от $G^{\mathrm{F}}(D)$, а $\bar{d}_{[0,(m-1)/2]}$ – только от $G^{\mathrm{B}}(D)$. Так как мы можем выбирать $G^{\mathrm{F}}(D)$ и $G^{\mathrm{B}}(D)$ независимо, то первую половину ДПР $\widehat{d}_{[0,(m-1)/2]}$ можно сделать равной первой половине ОПР $d^*_{[0,(m-1)/2]}$ тогда и только тогда, когда обе матрицы $G^{\mathrm{F}}(D)$ и $G^{\mathrm{B}}(D)$ задают ОПР-коды с памятью $(m-1)/2$.

Если память кода m четна, то можно разложить порождающую матрицу как

$$G(D) = G^{\mathrm{F}}(D) + G^{(m/2)} D^{m/2} + D^m G^{\mathrm{B}}(D^{-1}), \tag{9}$$

где на этот раз

$$G^{\mathrm{F}}(D) = G^{[0,m/2-1]}(D), \tag{10}$$

$$G^{\mathrm{B}}(D) = \bar{G}^{[0,m/2-1]}(D). \tag{11}$$

В этом случае можно оптимизировать $\widehat{d}_{[0,m/2-1]}$ аналогичным образом.

Для описания процедуры нахождения ОДФСР- и ОДПР$^{(s)}$-кодов нам понадобится несколько определений. В поле $\mathbb{F}_2$ положим $0 < 1$. Двоичные многочлены сравниваются лексикографически, т.е. для $g(D), h(D) \in \mathbb{F}_2[D]$ полагаем $g(D) < h(D)$, если $g^{(0)} = h^{(0)}, \ldots, g^{(\ell-1)} = h^{(\ell-1)}, g^{(\ell)} < h^{(\ell)}$ для некоторого ℓ. Векторы из двоичных многочленов сравниваются лексикографически, т.е. для $\boldsymbol{x}, \boldsymbol{y} \in (\mathbb{F}_2[D])^r$ полагаем $\boldsymbol{x} < \boldsymbol{y}$, если $x_1 = y_1, \ldots, x_{\ell-1} = y_{\ell-1}, x_\ell < y_\ell$ для некоторого ℓ. Если $\boldsymbol{g}_{i*}$ ($\boldsymbol{g}_{*j}$) – i-я строка (j-й столбец) $(k \times n)$-матрицы $G(D)$, то будем говорить, что матрица имеет упорядоченные строки (столбцы), если $\boldsymbol{g}_{1*} \leqslant \ldots \leqslant \boldsymbol{g}_{k*}$ ($\boldsymbol{g}_{*1} \leqslant \ldots \leqslant \boldsymbol{g}_{*n}$). Через Π_ℓ обозначим множество всех перестановок элементов $\{1, \ldots, \ell\}$.

Для заданных k и n обозначим через $\mathcal{U}_m$ множество ОПР-кодов с памятью m, а через $\mathcal{B}_m$ – множество ОДФСР-кодов (ОДПР$^{(s)}$-кодов) с памятью m. ОДФСР-коды (ОДПР$^{(s)}$-коды) можно находить с помощью следующей двухэтапной процедуры:

I. Найти все ОПР-коды для требуемых значений m.

1. Положить $\mathcal{U}_{-1} = \{\mathbf{0}_{k\times n}\}$.
   Положить $m = 0$.
2. Для всех префиксов $G'(D) \in \mathcal{U}_{m-1}$:
   Для всех двоичных $(k \times n)$-матриц $G^{(m)}$:
   Рассмотреть $G(D) = G'(D) + G^{(m)}D^m$.
   Если $G(D)$ имеет упорядоченные строки и столбцы, вычислить ее ПР.
   Оставить в $\mathcal{U}_m$ только те матрицы, которые имеют наилучшие ПР среди всех вычисленных.
3. Если требуется больше множеств, положить $m = m + 1$ и перейти к шагу 2.

II. Найти все ОДФСР-коды (ОДПР$^{(s)}$-коды) для всех требуемых значений m.

1. Положить $m = \max(1, 2s - 1)$.
2. Положить $\mathcal{B}_m = \{\}$.
   Положить $p = \lfloor (m-1)/2 \rfloor$.
3. Для всех $G^{\mathrm{F}}(D) \in \mathcal{U}_p$ и для всех $G^{\mathrm{B}}(D) \in \mathcal{U}_p$:
   [Только для четных m]
   [Для всех двоичных $(k \times n)$-матриц $G^{(m/2)}$:]
   Для всех $\pi \in \Pi_k$ и всех $\rho \in \Pi_n$:
   Рассмотреть

$$G(D) = G^{\mathrm{F}}(D) + [G^{(m/2)}D^{m/2}] + D^m \underline{G}^{\mathrm{B}}(D^{-1}),$$

   где $\underline{g}^{\mathrm{B}}_{i,j}(D) = g^{\mathrm{B}}_{\pi(i),\rho(j)}(D)$.
   Если $G(D)$ не задает катастрофический кодер [1], вычислить его ДФСР (ДПР$^{(s)}$).
   Оставить в $\mathcal{B}_m$ только те матрицы, которые имеют наилучшие ДФСР (ДПР$^{(s)}$) среди всех вычисленных.
4. Для всех пар матриц $G'(D), G''(D) \in \mathcal{B}_m$, $G'(D) \neq G''(D)$:
   Для всех $\pi \in \Pi_k$ и всех $\rho \in \Pi_n$:
   Если $G'(D)$ и $G''(D)$ тривиально эквивалентны, т.е. $g'_{i,j}(D) = g''_{\pi(i),\rho(j)}(D)$ для всех i, j или $g'_{i,j}(D) = \bar{g}''_{\pi(i),\rho(j)}(D)$ для всех i, j, удалить из $\mathcal{B}_m$ лексикографически бóльшую из матриц $G'(D)$ и $G''(D)$.
5. Если требуется больше множеств, положить $m = m + 1$ и перейти к шагу 2.

На первом этапе этой процедуры мы проверяем, имеет ли порождающая матрица упорядоченные строки и столбцы, чтобы избежать повторных вычислений тождественных ПР эквивалентных кодеров, различающихся только порядком входов или выходов.

На втором этапе процедуры циклы по перестановкам строк и столбцов матриц $G^{\mathrm{B}}(D)$ необходимы, поскольку хотя $d_{[0,p]} = \bar{d}_{[0,p]} = \widehat{d}_{[0,p]} = d^*_{[0,p]}$ для всех таких кодов, вторая часть их ДФСР $\widehat{d}_{[p+1,\infty]}$ (их ДПР$^{(s)}$ $\widehat{d}_{[p+1,m-s]}$) изменяется, и ее следует оптимизировать.

В большинстве случаев второй этап можно ускорить, пропуская цикл по двоичным матрицам $G^{(m/2)}$ (выделенный квадратными скобками и выполняемый только для четных m). Идея состоит в том, чтобы взять $G^{\mathrm{F}}(D) = G^{[0,m/2]}(D)$ и выбирать в качестве этих матриц все элементы $\mathcal{U}_{m/2}$ вместо $\mathcal{U}_{m/2-1}$ и вычислять ДФСР (ДПР$^{(s)}$) всех конкатенаций. Отсюда следует, что $d_{m/2} = d^*_{m/2}$, но не обязательно $\bar{d}_{m/2} = d^*_{m/2}$. Однако если это последнее условие выполнено, что можно проверить после того как множество $\mathcal{B}_m$ полностью построено, то такое сокращение перебора не будет влиять на оптимальность $\widehat{d}_{[0,m/2]}$.

При поиске ОДПР$^{(s)}$-кодов с $s \geqslant 2$ мы ограничиваемся случаем $m \geqslant 2s-1$, чтобы упростить процедуру. Когда $m < 2s-1$, конкатенация $G^{\mathrm{F}}(D), G^{\mathrm{B}}(D) \in \mathcal{U}_{(m-1)/2}$ для нечетных m или $G^{\mathrm{F}}(D) \in \mathcal{U}_{m/2}$ и $G^{\mathrm{B}}(D) \in \mathcal{U}_{m/2-1}$ для четных m может быть неоправданной, поскольку требуется лишь оптимальность $\widehat{d}_{[0,m-s]}$, а поиск должен включать в себя цикл по всем "промежуточным" матрицам $G^{[m+1-s,s-1]}(D)$.

Для некоторых значений k и n следует рассматривать специальный случай $m = 1$ отдельно, выполняя при этом полный перебор по всем кодам, так как конкатенация $G^{\mathrm{F}}(D), G^{\mathrm{B}}(D) \in \mathcal{U}_0$ может давать только порождающие матрицы катастрофических кодов.

§ 3. Результаты поиска кодов

В общем случае, для заданных k, n и m ОДФСР- и ОДПР$^{(s)}$-коды не единственны. Для оптимизации их вероятности ошибки мы проводили дополнительный отбор по спектрам информационных расстояний $\boldsymbol{c} = (c_1, c_2, \ldots)$. Пусть событие ошибки означает путь в кодовой решетке, который начинается в нулевом состоянии, выходит из него в самом начале и возвращается в нулевое состояние только при своей терминации. Тогда c_d – это сумма весов Хэмминга информационных последовательностей всех событий ошибок, кодовые слова которых имеют вес Хэмминга d. Как и ранее, мы полагаем $\boldsymbol{c} < \boldsymbol{c}'$, если $c_1 = c'_1, \ldots, c_{\ell-1} = c'_{\ell-1}, c_\ell < c'_\ell$ для некоторого ℓ, и ищем наименьший $\boldsymbol{c}$ [14].

В табл. 1–6 приведены порождающие матрицы ОДФСР- и ОДПР$^{(s)}$-кодов для скоростей 1/2, 1/3, 1/4, 2/3, 2/4 и 3/4 в восьмеричной записи (с использованием правила, принятого в [7], т.е. с выравниваем влево), а также свободные расстояния этих кодов. Из-за недостатка места здесь приведены не все найденные нами коды; более полные результаты см. в [20].

В таблицах ОДПР$^{(s)}$-кодов перечислены только улучшенные коды. Здесь под "улучшенными" мы понимаем коды с лучшими спектрами информационных расстояний, чем у ОДПР$^{(s-1)}$-кодов (или ОДФСР-кодов при $s = 0$) с теми же k, n и m. Для $R = 3/4$ и $m = 3$ улучшенных ОДПР$^{(2)}$-кодов нет.

Все эти коды имеют оптимизированные спектры информационных расстояний. Все матрицы единственны с точностью до инверсии и перестановок их строк или столбцов, за исключением случаев

- $R = 2/4$, ОДФСР, $m = 6$,
- $R = 2/4$, ОДПР$^{(0)}$, $m = 4$,
- $R = 2/4$, ОДПР$^{(2)}$, $m = 6$,

где коды имеют одинаковые спектры информационных расстояний, но их порождающие матрицы отличаются нетривиальным образом.

Таблица 1

ОДФСР/ОДПР-коды, $R = 1/2$

m	$G(D)$	d_∞
ОДФСР-коды		
1	[2 6]	3
2	[5 7]	5
3	[54 64]	6
4	[46 62]	6
5	[57 75]	8
6	[564 774]	8

7	[452 756]	10
8	[477 635]	10
9	[5414 6064]	10
10	[4522 6006]	9
11	[4417 6171]	12
12	[54464 60014]	11
13	[57276 76572]	12
14	[40375 71637]	12
15	[406564 710774]	16
16	[445222 611106]	14
17	[563477 771635]	16
18	[5632374 7713164]	18
19	[5574376 7513272]	20
20	[5736137 7643675]	18
21	[51265734 66263624]	21
22	[46701662 62153046]	21
23	[42544077 72625251]	22
24	[543567064 742331074]	23
25	[407402732 675600306]	21
26	[473063215 632451617]	24
27	[4624275754 6261156024]	26
28	[5665532672 6364242746]	22
29	[4644230357 7560621131]	24
30	[50160016024 67671635754]	26
31	[50107314766 67631561012]	26
Улучшенные ОДПР$^{(0)}$-коды		
6	[534 724]	8
9	[4674 7544]	12
11	[4173 6605]	13
12	[52274 71664]	15
15	[440564 616714]	17
16	[445362 611036]	17
17	[401177 670535]	18
18	[4440574 6107364]	20
19	[4560552 6062726]	20
20	[4775443 6344455]	20
21	[50265354 67453424]	21
22	[46176562 62453546]	23
23	[41732353 70767461]	24
24	[415755274 704555144]	24
25	[416262512 706141156]	25
26	[512043315 731676517]	27
27	[4147233534 7053240024]	27
28	[4075047376 6757475322]	28
29	[4317713123 6562116075]	29
30	[46747737324 62131433034]	28
31	[46026512472 75150113146]	30
Улучшенные ОДПР$^{(1)}$-коды		
10	[4046 6772]	12
16	[406072 674546]	18
23	[50635563 72252135]	24

27	[4165155544 7064264114]	28
30	[51477667274 73460644664]	30
Улучшенные ОДПР$^{(2)}$-коды, $m \geqslant 3$		
4	[46 72]	7
6	[434 724]	9
8	[435 657]	12
11	[4363 7335]	14
13	[42756 64712]	16
17	[434323 731231]	19
20	[4147563 6624135]	22
24	[417136244 707535014]	25
28	[4151623456 7041374442]	28
31	[55701344176 75157532472]	31
Улучшенные ОДПР$^{(3)}$-коды, $m \geqslant 5$		
5	[53 75]	8
7	[452 766]	10
9	[4554 7524]	12
12	[46554 75624]	15
14	[52635 71077]	17
18	[4066164 7105374]	20
21	[44632424 76170134]	23
25	[415744152 704555326]	26
29	[4027363533 7175037345]	30
Улучшенные ОДПР$^{(4)}$-коды, $m \geqslant 7$		
10	[4752 6166]	14
13	[43372 65446]	16
15	[412764 667114]	18
19	[5327632 7026236]	22
22	[42431526 72713352]	24
26	[506477557 722102055]	27
30	[52762256724 64643055434]	30
Улучшенные ОДПР$^{(5)}$-коды, $m \geqslant 9$		
11	[4325 6747]	15
14	[42437 72711]	17
16	[551576 755072]	19
20	[4271771 6465163]	22
23	[40560411 67665743]	24
27	[4020517504 7170726534]	28
31	[42523570626 64546507642]	32

Таблица 2

ОДФСР/ОДПР-коды, $R = 1/3$

m	$G(D)$	d_∞
ОДФСР-коды		
1	[2 4 6]	4
2	[5 7 7]	8
3	[44 54 74]	9
4	[52 66 76]	12

5	[45 51 77]	12
6	[434 564 704]	13
7	[446 616 722]	14
8	[533 575 665]	15
9	[4674 6754 7544]	18
10	[5772 6056 7206]	18
11	[4135 5057 7263]	21
12	[51624 66234 71154]	22
13	[53256 65126 72552]	20
14	[40701 53765 67273]	22
15	[520454 644124 733334]	26
16	[403402 517712 730156]	24
17	[421765 531607 706321]	29
18	[4304304 5060254 6501424]	23
19	[4763236 6146306 7454762]	26
20	[5704623 6231075 7432617]	31
21	[46324714 54425344 62027664]	32
22	[40666602 53634752 67377566]	34
23	[51275623 66500617 71746075]	37
24	[551571614 616366264 770370374]	34
25	[527061652 641577756 737773026]	36
26	[533361127 650525053 724436665]	38
27	[4017417334 5150442624 7336076004]	38
28	[4333324526 5054103212 6522555542]	41
29	[4446061757 5406076103 7460043031]	38
30	[44137047714 63744372044 76211621174]	41
31	[40043101266 65362363716 71200036512]	45
Улучшенные ОДПР$^{(0)}$-коды		
3	[54 64 74]	10
5	[43 57 71]	12
6	[474 514 764]	14
7	[466 536 662]	16
8	[575 623 727]	18
13	[40246 53322 67576]	22
25	[513467436 664525446 716556172]	41
28	[4430505436 5463114632 7432121422]	41
29	[4156353665 5272053621 6646554507]	44
Улучшенные ОДПР$^{(1)}$-коды		
1	[2 6 6]	5
5	[57 63 75]	12
9	[4464 5154 6374]	18
10	[4662 5646 6272]	20
27	[5040413754 6772040424 7075467434]	40
Улучшенные ОДПР$^{(2)}$-коды, $m \geqslant 3$		
5	[45 53 67]	12
6	[514 564 674]	15
7	[456 646 772]	16
10	[4732 5562 6346]	21
15	[431724 507134 651654]	28
16	[472562 571076 761172]	28
21	[43617114 50176144 65531464]	34

24	[522211124 730404334]	35
28	[4331523516 5216527052 7134531542]	44
Улучшенные ОДПР$^{(3)}$-коды, $m \geqslant 5$		
5	[47 53 75]	13
6	[474 534 664]	15
7	[452 662 756]	16
9	[4754 5324 6744]	20
12	[42664 53714 70344]	23
17	[422543 662711 725135]	29
18	[5373724 6575134 7227654]	26
20	[4602545 5611033 7747647]	33
26	[410707237 506133675 724647071]	41
Улучшенные ОДПР$^{(4)}$-коды, $m \geqslant 7$		
9	[4714 5334 7724]	20
10	[4456 6546 7672]	22
11	[4551 5157 7353]	22
13	[42162 51572 64476]	24
14	[45755 55163 75271]	27
16	[431516 675542 731052]	28
19	[4340472 5270746 7165336]	32
21	[40555364 65473174 71462344]	35
22	[42105642 66074416 72756752]	36
24	[455116344 574065364 603503174]	39
26	[432166577 504132623 653567051]	42
29	[5341100365 6555670627 7205114353]	44
31	[41775322742 64230711252 70124437316]	48
Улучшенные ОДПР$^{(5)}$-коды, $m \geqslant 9$		
9	[4764 5134 6674]	20
10	[4652 5662 7716]	22
11	[4671 6625 7537]	24
12	[47274 51454 63364]	24
15	[451464 556414 756174]	28
17	[426163 664435 722757]	32
18	[5361654 6561724 7237134]	31
20	[4610365 5460353 6233627]	34
22	[41070752 52326416 66353642]	37
23	[46652143 56623517 77044371]	38
29	[4252213203 6666141151 7206766575]	45
30	[41056336124 50665003304 72432267234]	46

Таблица 3

ОДФСР/ОДПР-коды, $R = 1/4$

m	$G(D)$	d_∞
ОДФСР-коды		
1	[2 4 6 6]	6
2	[5 5 7 7]	10
3	[44 54 64 74]	12
4	[46 56 62 72]	14
5	[45 51 67 73]	16

6	[434 564 614 704]	17
7	[406 536 602 752]	18
8	[471 525 603 727]	21
9	[4314 5704 6174 7024]	22
10	[4102 5756 6106 7372]	24
11	[4633 5647 6631 7135]	30
12	[41204 52524 62074 74114]	25
13	[47516 57666 66772 71362]	32
14	[41057 52225 60503 75041]	27
15	[435314 503024 632704 760174]	34
16	[467516 545232 661066 713662]	38
17	[442753 564627 657211 723135]	40
18	[4665544 5440464 6604154 7121234]	38
19	[4733366 5746156 6755562 7306372]	38
20	[4502051 5535655 6465507 7055313]	45
21	[41256354 52575164 62006044 74145334]	44
22	[40153002 51135112 63027276 76564146]	46
23	[47015547 57277275 66036033 71554071]	44
24	[433163304 525446524 616735614 746161474]	48
25	[422044512 512220442 605716076 760717206]	48
26	[404671717 510050045 621451423 747473101]	50
27	[4666466064 5415455544 6454006454 7011462034]	50
Улучшенные ОДПР$^{(0)}$-коды		
7	[446 516 622 712]	18
8	[451 525 623 727]	21
10	[4422 5766 6772 7356]	26
11	[4427 5633 6551 7375]	30
21	[44736564 56573444 67431734 73630754]	46
Улучшенные ОДПР$^{(1)}$-коды		
1	[2 6 6 6]	7
6	[444 564 654 734]	19
7	[466 562 636 752]	22
8	[471 525 677 773]	22
10	[4116 5262 6266 7572]	27
18	[4576664 5557644 6425054 7004034]	40
20	[4076427 5363235 6155333 7422331]	46
21	[40236644 53771134 63422764 75637154]	46
Улучшенные ОДПР$^{(2)}$-коды, $m \geqslant 3$		
8	[455 571 647 733]	24
9	[4744 5564 6374 7514]	24
10	[4546 5532 6162 7736]	28
11	[4563 5537 6531 7235]	31
15	[443644 560034 672664 731054]	35
21	[43553134 50374764 63210644 76045154]	49
Улучшенные ОДПР$^{(3)}$-коды, $m \geqslant 5$		
6	[454 534 664 744]	19
8	[457 565 633 771]	24
9	[4554 5534 6164 7644]	26
10	[4532 5656 6326 7722]	28
15	[435424 506704 615374 772614]	36

Улучшенные ОДПР$^{(4)}$-коды, $m \geqslant 7$		
8	[455 523 671 757]	24
9	[4624 5344 6654 7574]	27
10	[4272 5176 6662 7246]	28
11	[4555 5247 6371 7273]	31
12	[45264 57634 64554 72344]	33
19	[4153362 5234356 6243572 7444166]	44
20	[4533731 5502433 6441647 7074515]	46
22	[47153556 57650766 67612772 73353162]	50
Улучшенные ОДПР$^{(5)}$-коды, $m \geqslant 9$		
10	[4566 5162 6552 7636]	29
11	[4527 5433 6471 7375]	31
12	[45534 50564 63754 71544]	33
13	[43372 52722 65546 71176]	36
14	[44207 56151 67355 73013]	33
15	[423354 532544 614564 774434]	38
21	[42647164 51270354 62464044 77553334]	50
23	[45704327 55073553 65567055 72610751]	48
27	[4126442534 5254267444 6202134254 7416644164]	55

Таблица 4

ОДФСР/ОДПР-коды, $R = 2/3$

m	$G(D)$	d_∞
ОДФСР-коды		
1	$\begin{bmatrix} 0 & 2 & 6 \\ 6 & 6 & 4 \end{bmatrix}$	3
2	$\begin{bmatrix} 2 & 5 & 7 \\ 7 & 2 & 7 \end{bmatrix}$	5
3	$\begin{bmatrix} 04 & 60 & 74 \\ 40 & 34 & 54 \end{bmatrix}$	6
4	$\begin{bmatrix} 00 & 46 & 62 \\ 42 & 34 & 56 \end{bmatrix}$	6
5	$\begin{bmatrix} 05 & 40 & 73 \\ 67 & 01 & 50 \end{bmatrix}$	8
6	$\begin{bmatrix} 024 & 664 & 770 \\ 420 & 104 & 604 \end{bmatrix}$	7
7	$\begin{bmatrix} 130 & 462 & 642 \\ 462 & 150 & 426 \end{bmatrix}$	10
8	$\begin{bmatrix} 020 & 673 & 757 \\ 505 & 174 & 623 \end{bmatrix}$	10
9	$\begin{bmatrix} 0324 & 6670 & 7614 \\ 7674 & 0444 & 5320 \end{bmatrix}$	13
Улучшенные ОДПР$^{(0)}$-коды		
2	$\begin{bmatrix} 1 & 5 & 6 \\ 5 & 2 & 7 \end{bmatrix}$	5

3	$\begin{bmatrix} 04 & 54 & 60 \\ 50 & 14 & 54 \end{bmatrix}$	6
4	$\begin{bmatrix} 10 & 52 & 66 \\ 42 & 34 & 76 \end{bmatrix}$	8
5	$\begin{bmatrix} 25 & 55 & 76 \\ 63 & 16 & 45 \end{bmatrix}$	10
6	$\begin{bmatrix} 100 & 524 & 744 \\ 514 & 350 & 554 \end{bmatrix}$	10
7	$\begin{bmatrix} 126 & 444 & 662 \\ 742 & 126 & 700 \end{bmatrix}$	12
8	$\begin{bmatrix} 037 & 473 & 532 \\ 676 & 317 & 633 \end{bmatrix}$	13
9	$\begin{bmatrix} 0070 & 5664 & 7244 \\ 4624 & 3344 & 7700 \end{bmatrix}$	14
Улучшенные ОДПР$^{(1)}$-коды		
4	$\begin{bmatrix} 14 & 56 & 62 \\ 46 & 34 & 76 \end{bmatrix}$	8
7	$\begin{bmatrix} 156 & 464 & 716 \\ 560 & 352 & 602 \end{bmatrix}$	12
Улучшенные ОДПР$^{(2)}$-коды, $m \geqslant 3$		
3	$\begin{bmatrix} 30 & 54 & 54 \\ 54 & 30 & 74 \end{bmatrix}$	7
8	$\begin{bmatrix} 053 & 406 & 755 \\ 421 & 361 & 712 \end{bmatrix}$	13

Таблица 5

ОДФСР/ОДПР-коды, $R = 2/4$

m	$G(D)$	d_∞
ОДФСР-коды		
1	$\begin{bmatrix} 0 & 2 & 6 & 6 \\ 6 & 6 & 0 & 4 \end{bmatrix}$	5
2	$\begin{bmatrix} 1 & 3 & 4 & 6 \\ 4 & 6 & 3 & 1 \end{bmatrix}$	6
3	$\begin{bmatrix} 14 & 34 & 54 & 74 \\ 70 & 60 & 74 & 64 \end{bmatrix}$	8
4	$\begin{bmatrix} 00 & 24 & 46 & 72 \\ 76 & 52 & 04 & 30 \end{bmatrix}$	9
5	$\begin{bmatrix} 04 & 35 & 52 & 77 \\ 73 & 67 & 67 & 73 \end{bmatrix}$	12
6	$\begin{bmatrix} 064 & 210 & 540 & 654 \\ 540 & 654 & 064 & 210 \end{bmatrix}, \begin{bmatrix} 064 & 250 & 540 & 614 \\ 540 & 614 & 064 & 250 \end{bmatrix}$	13
7	$\begin{bmatrix} 024 & 226 & 540 & 632 \\ 546 & 644 & 032 & 240 \end{bmatrix}$	14
Улучшенные ОДПР$^{(0)}$-коды		
3	$\begin{bmatrix} 04 & 30 & 54 & 60 \\ 74 & 44 & 34 & 04 \end{bmatrix}$	8

4	$\begin{bmatrix}06 & 34 & 52 & 70\\70 & 52 & 34 & 06\end{bmatrix}, \begin{bmatrix}10 & 22 & 54 & 76\\76 & 54 & 22 & 10\end{bmatrix}$	11
5	$\begin{bmatrix}05 & 34 & 47 & 62\\65 & 47 & 25 & 17\end{bmatrix}$	12
6	$\begin{bmatrix}014 & 354 & 544 & 704\\770 & 640 & 664 & 734\end{bmatrix}$	15
7	$\begin{bmatrix}052 & 276 & 444 & 730\\674 & 460 & 062 & 326\end{bmatrix}$	17
Улучшенные ОДПР$^{(1)}$-коды		
5	$\begin{bmatrix}04 & 36 & 55 & 73\\71 & 73 & 42 & 44\end{bmatrix}$	13
7	$\begin{bmatrix}130 & 252 & 466 & 654\\662 & 446 & 226 & 162\end{bmatrix}$	17
Улучшенные ОДПР$^{(2)}$-коды, $m \geqslant 3$		
5	$\begin{bmatrix}12 & 34 & 47 & 75\\63 & 55 & 34 & 16\end{bmatrix}$	14
6	$\begin{bmatrix}044 & 360 & 534 & 730\\730 & 534 & 360 & 044\end{bmatrix}, \begin{bmatrix}130 & 214 & 560 & 764\\764 & 560 & 214 & 130\end{bmatrix}$	16

Таблица 6

ОДФСР-коды, $R = 3/4$

m	$G(D)$	d_∞
ОДФСР-коды		
1	$\begin{bmatrix}0 & 0 & 2 & 6\\2 & 6 & 4 & 4\\6 & 4 & 0 & 2\end{bmatrix}$	3
2	$\begin{bmatrix}0 & 2 & 5 & 5\\0 & 5 & 2 & 7\\7 & 2 & 0 & 7\end{bmatrix}$	5
3	$\begin{bmatrix}04 & 34 & 40 & 70\\34 & 44 & 34 & 64\\70 & 54 & 70 & 44\end{bmatrix}$	6
Улучшенные ОДПР$^{(0)}$-коды		
1	$\begin{bmatrix}0 & 2 & 4 & 6\\2 & 4 & 2 & 6\\6 & 4 & 4 & 4\end{bmatrix}$	4
2	$\begin{bmatrix}2 & 2 & 5 & 7\\2 & 7 & 2 & 5\\7 & 0 & 5 & 0\end{bmatrix}$	5
3	$\begin{bmatrix}10 & 14 & 44 & 70\\10 & 70 & 14 & 44\\44 & 10 & 34 & 60\end{bmatrix}$	8
Улучшенные ОДПР$^{(1)}$-коды		
2	$\begin{bmatrix}1 & 3 & 4 & 6\\3 & 4 & 2 & 7\\6 & 5 & 1 & 2\end{bmatrix}$	6

В табл. 7–12 приведены сводные результаты о свободных расстояниях $d_\infty^{(s)}$ для ОДПР$^{(s)}$-кодов (как и ранее, только для улучшенных кодов). Для каждого множества параметров k, n и m вычислена соответствующая верхняя граница Грайсмера d_∞^{G} на свободное расстояние как наибольшее d_∞, удовлетворяющее неравенству [1]

$$\sum_{\ell=0}^{ki-1} \left\lceil \frac{d_\infty}{2^\ell} \right\rceil \leqslant (m+i)n \tag{12}$$

для всех $i = 1, 2, \ldots$ Видно, что некоторые из перечисленных кодов, в основном при малых значениях m, также оптимальны по свободному расстоянию.

Аналогичная процедура поиска кодов, подходящих для двустороннего декодирования, представлена в [17] для $R = 1/2$. Чтобы уменьшить объем поиска, авторы ограничиваются так называемыми симметричными кодами, обладающими тем свойством, что $g_1(D) = \bar{g}_{\pi(1)}(D)$ и $g_2(D) = \bar{g}_{\pi(2)}(D)$, где $G(D) = [g_1(D) \quad g_2(D)]$ и $\pi \in \Pi_2$, и тем самым, такими что $\boldsymbol{d} = \bar{\boldsymbol{d}}$. Сначала выполняется поиск симметричных кодов с $d_{[0,m]} = d^*_{[0,m]}$, и из них выбирается код, имеющий наилучший спектр расстояний. Если таких кодов нет, поиск выполняется снова, но на этот раз с ослабленным условием $d_{[0,m-4]} = d^*_{[0,m-4]}$. Из-за налагаемого условия симметрии при некоторых значениях m коды, приведенные в [17], имеют несколько меньшие свободные расстояния, чем наши.

Таблица 7

Свободное расстояние $d_\infty^{(s)}$, $R = 1/2$

m	s							d_∞^{G}
	$-\infty$	0	1	2	3	4	5	
1	3			–	–	–	–	4
2	5			–	–	–	–	5
3	6				–	–	–	6
4	6			7	–	–	–	8
5	8				8	–	–	8
6	8	8		9		–	–	10
7	10				10		–	11
8	10			12			–	12
9	10	12			12			13
10	9		12			14		14
11	12	13		14			15	16
12	11	15			15			16
13	12			16		16		17
14	12				17		17	18
15	16	17				18		20
16	14	17	18				19	20
17	16	18		19				22
18	18	20			20			23
19	20	20				22		24
20	18	20		22			22	24
21	21	21			23			26
22	21	23				24		27
23	22	24	24				24	28
24	23	24		25				29
25	21	25			26			30
26	24	27				27		32

27	26	27	28				28	32
28	22	28		28				32
29	24	29			30			34
30	26	28	30			30		35
31	26	30		31			32	36

Таблица 8

Свободное расстояние $d_\infty^{(s)}$, $R = 1/3$

m	s							d_∞^{G}
	$-\infty$	0	1	2	3	4	5	
1	4		5	–	–	–	–	6
2	8			–	–	–	–	8
3	9	10			–	–	–	10
4	12				–	–	–	12
5	12	12	12	12	13	–	–	13
6	13	14		15	15	–	–	15
7	14	16		16	16		–	16
8	15	18					–	18
9	18		18		20	20	20	20
10	18		20	21		22	22	22
11	21					22	24	24
12	22				23		24	24
13	20	22				24		26
14	22					27		28
15	26			28			28	30
16	24			28		28		32
17	29				29		32	32
18	23				26		31	34
19	26					32		36
20	31				33		34	38
21	32			34		35		40
22	34					36	37	40
23	37						38	42
24	34			35		39		44
25	36	41						46
26	38				41	42		48
27	38		40					48
28	41	41		44				50
29	38	44				44	45	52
30	41						46	53
31	45					48		55

Таблица 9

Свободное расстояние $d_\infty^{(s)}$, $R = 1/4$

m	s							d_∞^{G}
	$-\infty$	0	1	2	3	4	5	
1	6		7	–	–	–	–	8
2	10			–	–	–	–	10
3	12				–	–	–	13

4	14				–	–	–	16
5	16					–	–	18
6	17		19		19	–	–	20
7	18	18	22				–	22
8	21	21	22	24	24	24	–	24
9	22			24	26	27		27
10	24	26	27	28	28	28	29	29
11	30	30		31		31	31	32
12	25					33	33	33
13	32						36	36
14	27						33	38
15	34			35	36		38	40
16	38							42
17	40							44
18	38		40					46
19	38					44		48
20	45		46			46		50
21	44	46	46	49			50	52
22	46					50		55
23	44						48	56
24	48							59
25	48							61
26	50							64
27	50						55	64

Таблица 10

Свободное расстояние $d_\infty^{(s)}$, $R = 2/3$

m	s				d_∞^{G}
	$-\infty$	0	1	2	
1	3			–	4
2	5	5		–	6
3	6	6		7	8
4	6	8	8		8
5	8	10			10
6	7	10			12
7	10	12	12		14
8	10	13		13	16
9	13	14			16

§ 4. Характеристики кодов

Для сравнения ОДПР$^{(s)}$-кодов с другими кодами, используемыми на практике, мы провели моделирование их вероятности ошибки на блок (FER) и сложности декодирования. В моделировании мы использовали следующие алгоритмы декодирования:

- Алгоритм Витерби (VA),
- Стек-алгоритм (SA) [2, 3],
- Двусторонний стек-алгоритм (BSA) [17].

Таблица 11

Свободное расстояние $d_\infty^{(s)}$, $R = 2/4$

m	s				d_∞^{G}
	$-\infty$	0	1	2	
1	5			–	5
2	6			–	8
3	8	8			10
4	9	11			12
5	12	12	13	14	14
6	13	15		16	16
7	14	17	17		18

Таблица 12

Свободное расстояние $d_\infty^{(s)}$, $R = 3/4$

m	s				d_∞^{G}
	$-\infty$	0	1	2	
1	3	4		–	4
2	5	5	6	–	6
3	6	8			8

Таблица 13

Коды, использованные при моделировании

R	m	Код	$G(D)$; Описание	d_∞
1/3	6	$C_{1/3,6}^{\mathrm{OCпР}}$	$\left[554 \quad 724 \quad 744\right]$; ОСпР, обозначенный через $\left[133 \quad 165 \quad 171\right]$ в [14]	15
	12	$C_{1/3,12}^{\mathrm{OCпР}}$	$\left[55304 \quad 64734 \quad 76244\right]$; ОСпР, обозначенный через $\left[13261 \quad 15167 \quad 17451\right]$ в [14]	24
	19	$C_{1/3,19}^{\mathrm{ОПР}}$	$\left[5531236 \quad 6151572 \quad 7731724\right]$; ОПР [1]	35
	19	$C_{1/3,19}^{\mathrm{ОДПР}}$	$\left[4340472 \quad 5270746 \quad 7165336\right]$; ОДПР$^{(4)}$	32
	31	$C_{1/3,31}^{\mathrm{ОДПР}}$	$\left[41775322742 \quad 64230711252 \quad 70124437316\right]$; ОДПР$^{(4)}$	48
1/4	6	$C_{1/4,6}^{\mathrm{OCпР}}$	$\left[474 \quad 534 \quad 664 \quad 744\right]$; ОСпР, обозначенный через $\left[117 \quad 127 \quad 155 \quad 171\right]$ в [14]	20
	12	$C_{1/4,12}^{\mathrm{OCвР}}$	$\left[46254 \quad 56374 \quad 65044 \quad 75564\right]$; ОСД, обозначенный через $\left[11453 \quad 13477 \quad 15211 \quad 17335\right]$ в [13]	33
	21	$C_{1/4,21}^{\mathrm{ОПР}}$	$\left[45724414 \quad 55057474 \quad 65556514 \quad 72624710\right]$; ОПР [1]	50
	21	$C_{1/4,21}^{\mathrm{ОДПР}}$	$\left[43553134 \quad 50374764 \quad 63210644 \quad 76045154\right]$; ОДПР$^{(2)}$	49
	27	$C_{1/4,27}^{\mathrm{ОДПР}}$	$\left[4126442534 \quad 5254267444 \quad 6202134254 \quad 7416644164\right]$; ОДПР$^{(5)}$	55

Коды, использовавшиеся при моделировании, перечислены в табл. 13, где через ОСвР обозначено оптимальное свободное расстояние, а через ОСпР – оптимальный спектр расстояний кодов.

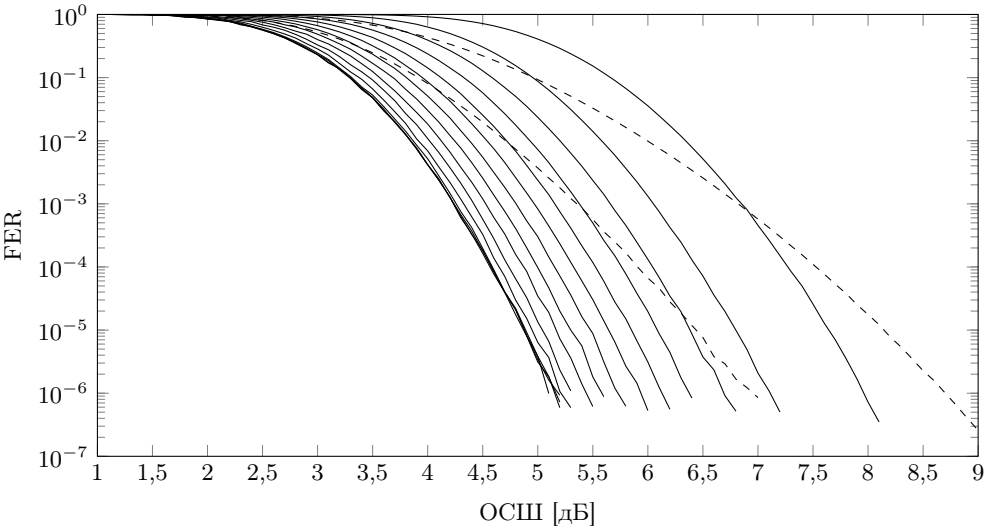

Рис. 1. FER, $R = 1/3$:
- - - VA($C^{\text{ОСпР}}_{1/3,6}$), VA($C^{\text{ОСпР}}_{1/3,12}$), —— BSA($C^{\text{ОДПР}}_{1/3,31}, \{2^{10}, 2^{11}, \ldots, 2^{24}\}$)

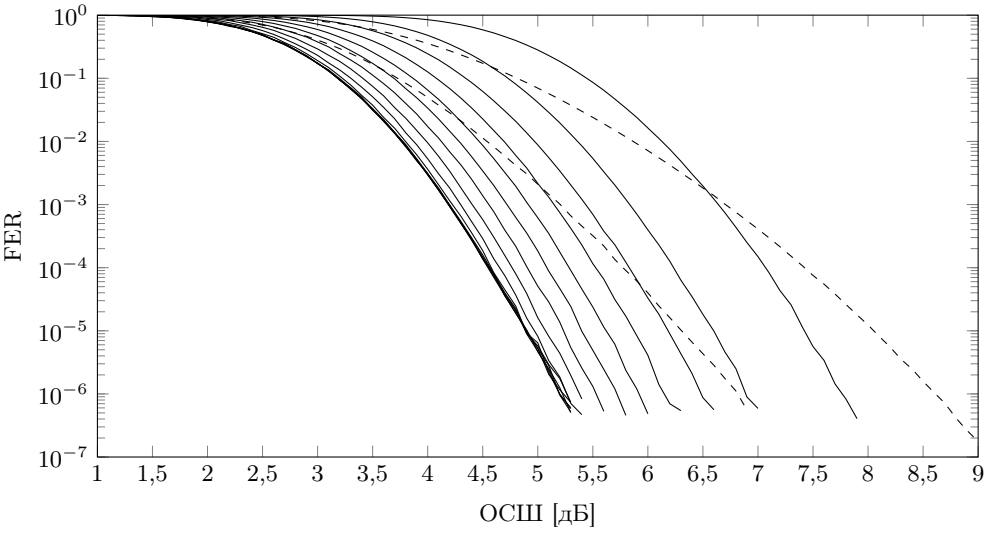

Рис. 2. FER, $R = 1/4$:
- - - VA($C^{\text{ОСпР}}_{1/4,6}$), VA($C^{\text{ОСвР}}_{1/4,12}$), —— BSA($C^{\text{ОДПР}}_{1/4,27}, \{2^{10}, 2^{11}, \ldots, 2^{24}\}$)

Во всех экспериментах длина информационной последовательности составляла $K = 224$ двоичных символов, а длина кодовых слов с нулевым усечением – $(K/k+m)n$ двоичных символов, в зависимости от используемого кода. Использовался АБГШ-канал с двоичным входом и симметричным биполярным отображением, а отношение сигнал/шум (ОСШ) определяется как $10 \log_{10}(E_{\text{b}}/N_0)$, где E_{b} – энергия на один информационный символ, а N_0 – односторонняя спектральная плотность мощности шума.

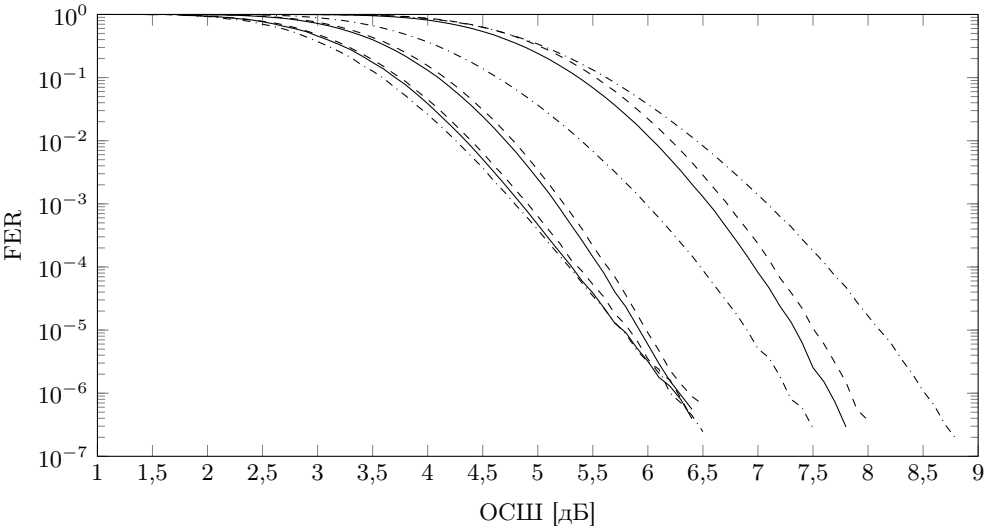

Рис. 3. FER, $R = 1/3$:
-·-·- SA($C^{\text{ОПР}}_{1/3,19}, \{2^{10}, 2^{13}, 2^{24}\}$), - - - BSA($C^{\text{ОПР}}_{1/3,19}, \{2^{10}, 2^{13}, 2^{24}\}$),
—— BSA($C^{\text{ОДПР}}_{1/3,19}, \{2^{10}, 2^{13}, 2^{24}\}$)

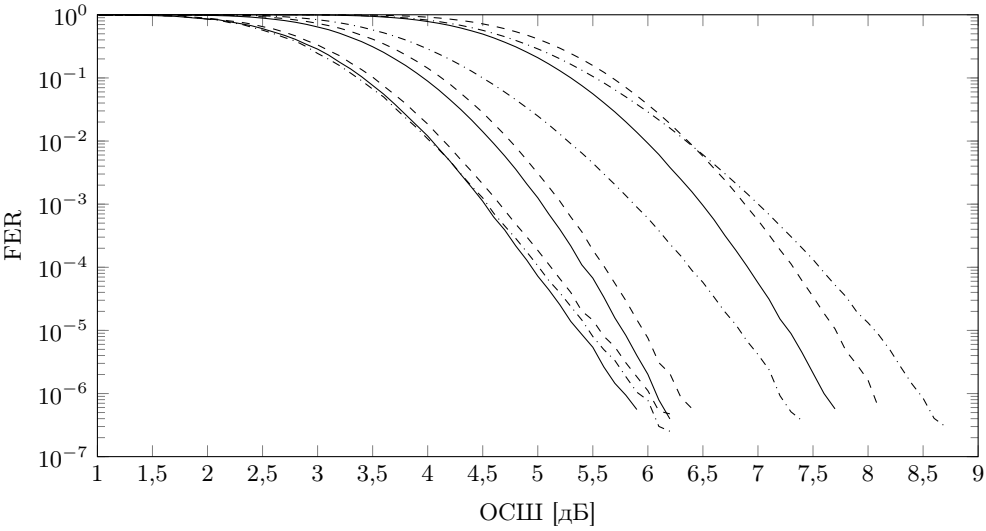

Рис. 4. FER, $R = 1/4$:
-·-·- SA($C^{\text{ОПР}}_{1/4,21}, \{2^{10}, 2^{13}, 2^{24}\}$), - - - BSA($C^{\text{ОПР}}_{1/4,21}, \{2^{10}, 2^{13}, 2^{24}\}$),
—— BSA($C^{\text{ОДПР}}_{1/4,21}, \{2^{10}, 2^{13}, 2^{24}\}$)

В описании всех результатов моделирования через $A(C)$ мы обозначаем применение алгоритма A к декодированию последовательностей кода C, и аналогично $A(C, M)$ в случае, когда в кодовое дерево (деревья) вставляется не более M узлов. В этом последнем случае M также может быть множеством значений, если их воздействие анализируется совместно.

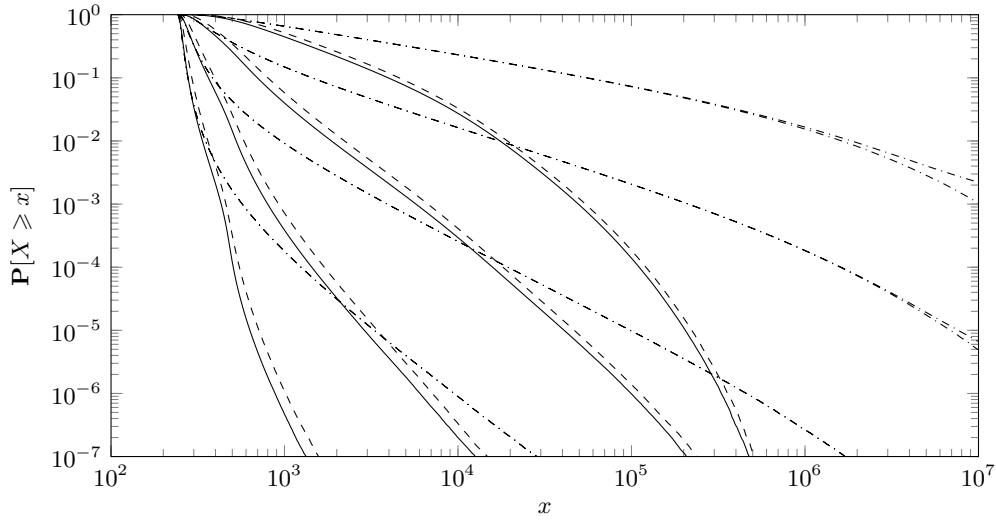

Рис. 5. Сложность декодирования, $R = 1/3$, сверху вниз ОСШ [дБ] $= 4, 5, 6, 7$:
-·-·- SA($C^{\text{ОПР}}_{1/3,19}$) (границы), - - - BSA($C^{\text{ОПР}}_{1/3,19}$), —— BSA($C^{\text{ОДПР}}_{1/3,19}$)

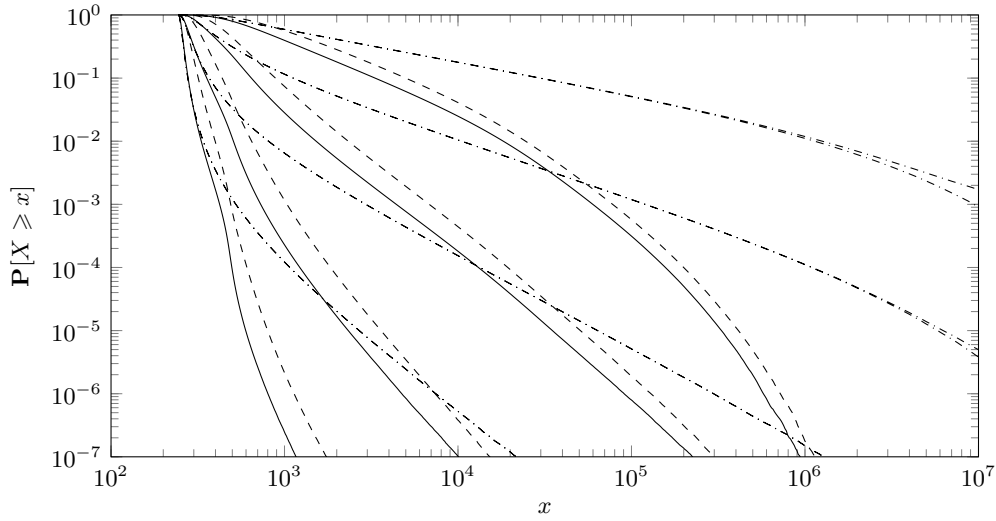

Рис. 6. Сложность декодирования, $R = 1/4$, сверху вниз ОСШ [дБ] $= 4, 5, 6, 7$:
-·-·- SA($C^{\text{ОПР}}_{1/4,21}$) (границы), - - - BSA($C^{\text{ОПР}}_{1/4,21}$), —— BSA($C^{\text{ОДПР}}_{1/4,21}$)

4.1. Сравнение с декодированием по Витерби. На рис. 1, 2 показаны результаты сравнения полученных при моделировании вероятностей ошибки на блок (FER) для BSA-декодирования выбранных ОДПР-кодов и декодирования по Витерби (по максимальному правдоподобию) ОСвР- и ОСпР-кодов с меньшей памятью для скоростей 1/3 и 1/4. ОДПР-коды, которые использовались для этого сравнения, – это коды с наибольшей памятью среди найденных.

Результаты BSA-декодирования приведены для различного максимально допустимого количества узлов, вставляемых в кодовые деревья (максимального общего

Таблица 14

Среднее число промежуточных узлов, $R = 1/3$

ОСШ [дБ]	SA($C^{\text{ОПР}}_{1/3,19}$), н.г.	BSA($C^{\text{ОПР}}_{1/3,19}$)	BSA($C^{\text{ОДПР}}_{1/3,19}$)
4	81000	2221,87	1950,36
5	2053,29	538,329	480,53
6	328,403	319,052	300,176
7	260,336	268,519	260,128

Таблица 15

Среднее число промежуточных узлов, $R = 1/4$

ОСШ [дБ]	SA($C^{\text{ОПР}}_{1/4,21}$), н.г.	BSA($C^{\text{ОПР}}_{1/4,21}$)	BSA($C^{\text{ОДПР}}_{1/4,21}$)
4	61758,3	2582,11	1831,05
5	1460,96	590,712	452,307
6	316,926	347,656	298,378
7	261,146	284,164	261,333

размера дерева), и кривые FER от верхней к нижней соответствуют его возрастающим значениям. Ошибками считаются как ситуация, когда декодер достигает максимального общего размера дерева без результата (отказ от декодирования), так и ситуация, когда он выдает неправильную декодированную последовательность. Мы видим, что для обеих скоростей кода в некоторый момент эта зависимость стабилизируется, когда FER начинает определяться только свойствами кода (свободным расстоянием и спектром расстояний).

Поскольку элементарные операции, выполняемые при BSA-декодировании и декодировании по Витерби, различны, не существует однозначного способа сравнения вычислительной эффективности этих двух алгоритмов, тем более что различные оптимизации обоих алгоритмов могут существенно повлиять на их суммарную сложность по времени и памяти. Однако точки пересечения кривых FER и соответствующие максимальные размеры деревьев BSA-алгоритма могут служить грубой оценкой того, насколько BSA-декодирование выгоднее декодирования по Витерби для конкретного приложения, т.е. когда известны ожидаемое ОСШ в канале и ограничения на аппаратные и/или программные возможности декодера.

4.2. Сравнение для последовательного декодирования. На рис. 3, 4 показаны полученные при моделировании значения FER для следующих случаев:

- SA-декодирование ОПР-кодов,
- BSA-декодирование ОПР-кодов,
- BSA-декодирование ОДПР-кодов.

Используются те же скорости, что и в предыдущем сравнении. Во всех экспериментах коды в сравниваемых системах имеют одинаковую память. Снова в качестве изменяемого параметра берется максимальный общий размер дерева M, а ошибками считаются как отказы от декодирования, так и неверные результаты.

При $R = 1/3$ результаты для ОДПР-кодов при различных значениях M оказываются на $\approx 0{,}05 - 0{,}2$ дБ лучше, чем для ОПР-кодов, в то время как при $R = 1/4$ отличие составляет $\approx 0{,}2 - 0{,}4$ дБ. Интересно отметить, что в большинстве случаев SA-декодирование ОПР-кодов уступает BSA-декодированию ОПР- или ОДПР-кодов, кроме случаев ($R = 1/3$, $M = 2^{24}$) и ($R = 1/4$, $M = 2^{24}$), когда они очень близки.

На рис. 5, 6 показаны распределения величины X – числа промежуточных узлов кодового дерева (деревьев) в случае, когда декодирование выдает правильную последовательность. Когда число промежуточных узлов становится слишком боль-

шим и декодирование конкретной полученной последовательности прерывается из-за практических ограничений, мы не можем определить, является ли декодированная последовательность правильной. Поэтому в некоторых результатах для SA-декодирования приведены лишь границы на распределение X. Как для $R = 1/3$, так и для $R = 1/4$ видно улучшение при использовании ОДПР-кодов. Видно также, что в большинстве случаев BSA-декодирование имеет меньшую среднюю сложность, чем SA-декодирование. Сводные данные о среднем числе промежуточных узлов приведены в табл. 14, 15, где для SA-декодирования указаны нижние границы (н.г.).

СПИСОК ЛИТЕРАТУРЫ

1. *Johannesson R., Zigangirov K.Sh.* Fundamentals of Convolutional Coding. Piscataway, NJ: IEEE Press; Hoboken, NJ: Wiley, 2015.
2. *Зигангиров К.Ш.* Некоторые последовательные процедуры декодирования // Пробл. передачи информ. 1966. Т. 2. № 4. С. 13–25. https://www.mathnet.ru/ppi1966
3. *Jelinek F.* Fast Sequential Decoding Algorithm Using a Stack // IBM J. Res. Develop. 1969. V. 13. № 6. P. 675–685. https://doi.org/10.1147/rd.136.0675
4. *Fano R.M.* A Heuristic Discussion of Probabilistic Decoding // IEEE Trans. Inform. Theory. 1963. V. 9. № 2. P. 64–74. https://doi.org/10.1109/TIT.1963.1057827
5. *Chevillat P., Costello D.* An Analysis of Sequential Decoding for Specific Time-Invariant Convolutional Codes // IEEE Trans. Inform. Theory. 1978. V. 24. № 4. P. 443–451. https://doi.org/10.1109/TIT.1978.1055916
6. *Narayanaswamy B., Negi R., Khosla P.* An Analysis of the Computational Complexity of Sequential Decoding of Specific Tree Codes over Gaussian Channels // Proc. 2008 IEEE Int. Symp. on Information Theory (ISIT'2008). Toronto, ON, Canada. July 6–11, 2008. P. 2508–2512. https://doi.org/10.1109/ISIT.2008.4595443
7. *Johannesson R.* Robustly Optimal Rate One-Half Binary Convolutional Codes // IEEE Trans. Inform. Theory. 1975. V. 21. № 4. P. 464–468. https://doi.org/10.1109/TIT.1975.1055397
8. *Johannesson R.* Some Long Rate One-Half Binary Convolutional Codes with an Optimum Distance Profile // IEEE Trans. Inform. Theory. 1976. V. 22. № 5. P. 629–631. https://doi.org/10.1109/TIT.1976.1055599
9. *Johannesson R.* Some Rate 1/3 and 1/4 Binary Convolutional Codes with an Optimum Distance Profile // IEEE Trans. Inform. Theory. 1977. V. 23. № 2. P. 281–283. https://doi.org/10.1109/TIT.1977.1055687
10. *Hagenauer J.* High Rate Convolutional Codes with Good Distance Profiles // IEEE Trans. Inform. Theory. 1977. V. 23. № 5. P. 615–618. https://doi.org/10.1109/TIT.1977.1055777
11. *Johannesson R., Paaske E.* Further Results on Binary Convolutional Codes with an Optimum Distance Profile // IEEE Trans. Inform. Theory. 1978. V. 24. № 2. P. 264–268. https://doi.org/10.1109/TIT.1978.1055850
12. *Johannesson R., Ståhl P.* New Rate 1/2, 1/3, and 1/4 Binary Convolutional Encoders with an Optimum Distance Profile // IEEE Trans. Inform. Theory. 1999. V. 45. № 5. P. 1653–1658. https://doi.org/10.1109/18.771238
13. *Sone N., Mohri M., Morii M., Sasano H.* Optimal Free Distance Convolutional Codes for Rates 1/2, 1/3, and 1/4 // Electron. Lett. 1999. V. 35. № 15. P. 1240–1241. https://doi.org/10.1049/el:19990871
14. *Frenger P., Orten P., Ottosson T.* Convolutional Codes with Optimum Distance Spectrum // IEEE Commun. Lett. 1999. V. 3. № 11. P. 317–319. https://doi.org/10.1109/4234.803468
15. *Hug F.* Codes on Graphs and More: Ph.D. Thesis. Dept. of Electrical and Information Technology, Lund Univ., Lund, Sweden, 2012.
16. *Šenk V., Radivojac P.* The Bidirectional Stack Algorithm // Proc. 1997 IEEE Int. Symp. on Information Theory (ISIT'97). Ulm, Germany. June 29 – July 4, 1997. P. 500. https://doi.org/10.1109/ISIT.1997.613437

17. *Kallel S., Li K.* Bidirectional Sequential Decoding // IEEE Trans. Inform. Theory. 1997. V. 43. № 4. P. 1319–1326. https://doi.org/10.1109/18.605602
18. *Bocharova I.E., Handlery M., Johannesson R., Kudryashov B.D.* BEAST Decoding of Block Codes Obtained via Convolutional Codes // IEEE Trans. Inform. Theory. 2005. V. 51. № 5. P. 1880–1891. https://doi.org/10.1109/TIT.2005.846448
19. *Xu R., Kocak T., Woodward G., Morris K., Dolwin C.* High Throughput Parallel Fano Decoding // IEEE Trans. Commun. 2011. V. 59. № 9. P. 2394–2405. https://doi.org/10.1109/TCOMM.2011.062011.100236
20. *Stanojević I., Šenk V.* Convolutional Codes with Optimum Bidirectional Distance Profile, https://arXiv:2210.15787v4 [cs.IT], 2022.

Станоевич Иван (Stanojević, Ivan)
Шенк Войин (Šenk, Vojin)
Факультет технических наук,
Университет г. Нови-Сад, Сербия
cet_ivan@uns.ac.rs
vojin_senk@uns.ac.rs

Поступила в редакцию
11.11.2022
После доработки
05.12.2023
Принята к публикации
06.12.2023

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 3**

УДК 621.391 : 519.725

© 2023 г. **Ж. Боржес, В.А. Зиновьев[1], Д.В. Зиновьев[1]**

О ПЕРЕЧИСЛЕНИИ ПОЛНОСТЬЮ РЕГУЛЯРНЫХ КОДОВ С РАДИУСОМ ПОКРЫТИЯ ДВА И ДУАЛЬНЫМИ АНТИПОДАЛЬНЫМИ КОДАМИ[2]

Классифицированы все линейные полностью регулярные коды с радиусом покрытия $\rho = 2$, дуальные коды которых являются антиподальными. Для этого вначале приводится ряд свойств для таких дуальных кодов, являющихся кодами с двумя расстояниями d и n.

Ключевые слова: линейный полностью регулярный код, код с радиусом покрытия 2, код с дуальным антиподальным, двухвесовой код, разностная матрица, латинский квадрат, проективный овал, эквидистантный код, матрица Адамара, код Хэмминга, максимальная дуга.

DOI: 10.31857/S0555292323030026, **EDN:** OKKXRQ

§ 1. Введение

Пусть $\mathbb{F}_q$ – конечное поле порядка q, где q – степень простого числа. Произвольное подмножество $C \subseteq \mathbb{F}_q^n$ называется q-ичным кодом и обозначается через $(n, N, d)_q$, где n – *длина* кода, N – число его кодовых слов (или *мощность*), а d – его *минимальное расстояние* (Хэмминга). Код C длины n с минимальным расстоянием d, являющийся линейным пространством размерности k над $\mathbb{F}_q$ (т.е. имеющий мощность q^k), обозначается через $[n, k, d]_q$.

Назовем *радиусом упаковки* кода C величину $e = \lfloor (d-1)/2 \rfloor$. Для произвольного вектора $\boldsymbol{v} \in \mathbb{F}_q^n$ определим его *расстояние до кода* C как

$$d(\boldsymbol{v}, C) = \min_{\boldsymbol{x} \in C} \{d(\boldsymbol{v}, \boldsymbol{x})\},$$

где $d(\boldsymbol{v}, \boldsymbol{x})$ обозначает расстояние между векторами $\boldsymbol{v}$ и $\boldsymbol{x}$. Определим *радиус покрытия* кода C как

$$\rho = \max_{\boldsymbol{v} \in \mathbb{F}_q^n} \{d(\boldsymbol{v}, C)\}.$$

Заметим, что $e \leqslant \rho$.

В данной статье мы будем рассматривать исключительно *нетривиальные* линейные коды $[n, k, d]_q$, в частности, размерности $2 \leqslant k \leqslant n-2$ с минимальным расстоянием $3 \leqslant d \leqslant n-1$.

[1] Исследования второго и третьего авторов были выполнены в ИППИ им. А.А. Харкевича РАН в рамках проводимых фундаментальных исследований по теме “Математические теории корректирующих кодов”, а также поддержаны грантом Национального научного фонда Болгарии (номер проекта 20-51-18002).

[2] Работа выполнена при частичной поддержке Министерства науки Испании, номера грантов PID2022-137924NB-I00 (AEI/FEDER UE) и RED2022-134306-T, а также программы AGAUR правительства Каталонии, номер гранта 2021-SGR-00643.

Для заданного кода C длины n и радиуса покрытия ρ определим множества

$$C(i) = \{\boldsymbol{x} \in \mathbb{F}_q^n : d(\boldsymbol{x}, C) = i\}, \quad i = 0, 1, \ldots, \rho.$$

Два вектора $\boldsymbol{x}$ и $\boldsymbol{y}$ назовем *соседями*, если $d(\boldsymbol{x}, \boldsymbol{y}) = 1$.

Определение 1 [1]. Назовем код C длины n с радиусом покрытия ρ *полностью регулярным* (сокращенно – ПР-кодом), если для произвольного $\ell \geqslant 0$ все векторы $x \in C(\ell)$ имеют одинаковое число c_ℓ соседей из $C(\ell - 1)$ и одинаковое число b_ℓ соседей из $C(\ell + 1)$. Пусть

$$a_\ell = (q-1)n - b_\ell - c_\ell,$$

и положим $c_0 = b_\rho = 0$. Числа a_i, b_i и c_i $(0 \leqslant i \leqslant \rho)$ будем называть *числами пересечения*, а последовательность $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$ назовем *вектором пересечений* (сокращенно – ИА) кода C.

Следующий класс равномерно упакованных в широком смысле кодов является более общим (в частности, содержит все ПР-коды).

Определение 2 [2]. Пусть C – код длины n с радиусом покрытия ρ. Будем называть код C *равномерно упакованным в широком смысле*, т.е. в смысле [2], если существуют рациональные числа $\beta_0, \ldots, \beta_\rho$, такие что для произвольного $\boldsymbol{v} \in \mathbb{F}^n$ имеет место следующее равенство:

$$\sum_{k=0}^{\rho} \beta_k \alpha_k(\boldsymbol{v}) = 1, \tag{1}$$

где $\alpha_k(\boldsymbol{v})$ – число кодовых слов на расстоянии k от $\boldsymbol{v}$.

Заметим, что случай $\rho = e+1$ и $\beta_{\rho-1} = \beta_\rho$ соответствует *равномерно упакованным в узком смысле* кодам [3], случай $\rho = e + 1$ и $\beta_{\rho-1} \neq \beta_\rho$ – *равномерно упакованным* кодам [4], а случай $\rho = e$ и $\beta_i = 1$ для всех $i = 0, 1, \ldots, e$ – *совершенным* кодам.

ПР-коды представляют собой классический объект изучения алгебраической теории кодирования, тесно связанный с теорией графов, комбинаторными конфигурациями и алгебраической комбинаторикой. Существование, построение и перечисление таких кодов – сложные нерешенные задачи (см., например, работы [1, 5–8] и библиографию в них).

Все ПР-коды с радиусом покрытия $\rho = 1$ хорошо известны [9, 10]. Следующий случай, т.е. ПР-коды с $\rho = 2$, представляется авторам исключительно сложным (имеется в виду ситуация с перечислением двухвесовых кодов). В настоящей статье описывается специальный класс таких кодов, а именно такие линейные полностью регулярные коды, дуальные коды которых антиподальны, т.е. являются $[n, k, d]_q$-кодами со следующим свойством: *для любых двух кодовых слов* $\boldsymbol{x}$ *и* $\boldsymbol{y}$ *расстояние* $d(\boldsymbol{x}, \boldsymbol{y})$ *равно одному из двух значений* d *или* n. В общем случае $(n, N, \{d_1, d_2\})_q$-код C – это код длины n с N элементами и расстоянием между произвольными двумя кодовыми словами $\boldsymbol{x}$ и $\boldsymbol{y}$, удовлетворяющим условию $d(\boldsymbol{x}, \boldsymbol{y}) \in \{d_1, d_2\}$. Поскольку мы рассматриваем только дистанционно-инвариантные коды, все слова такого кода имеют вес d_1 или d_2. Назовем такой код *двухвесовым* кодом. Если C – линейный код, будем обозначать его через $[n, k, \{d_1, d_2\}]_q$, где k – размерность кода C.

Наша классификация основана на описании аддитивных $(n, N, \{d, n\})_q$-кодов (т.е. таких, которые являются аддитивными подгруппами $\mathbb{F}_q^n$), данном в [11].

Статья организована следующим образом. В § 2 приводятся некоторые свойства и определения. В § 3 изучаются некоторые комбинаторные свойства двухвесовых кодов и выводятся необходимые условия существования таких кодов. В § 4 перечисляются известные семейства линейных полностью регулярных кодов с радиусом

покрытия 2 с дуальными антиподальными кодами. Наконец, в § 5 приводится основная теорема данной статьи, показывающая, что перечисленные в § 4 коды исчерпывают все линейные ПР-коды с радиусом покрытия 2 с дуальными антиподальными кодами.

§ 2. Предварительные сведения

В данном параграфе мы напомним некоторые результаты, которые понадобятся нам в дальнейшем.

Для $[n,k,d]$-кода C обозначим через $(\eta_0^\perp,\dots,\eta_n^\perp)$ весовой спектр его дуального $[n,n-k,d^\perp]$-кода $C^\perp$. Предположим, что $(\eta_0^\perp,\dots,\eta_n^\perp)$ имеет $s=s(C)$ ненулевых компонент $\eta_i^\perp$ для $1\leqslant i\leqslant n$. Следуя Дельсарту [12], назовем s *внешним расстоянием* кода C.

Лемма 1. *Пусть C – код с радиусом покрытия ρ и внешним расстоянием s. Тогда*:

(i) $\rho\leqslant s$ [12];
(ii) $\rho=s$, *если и только если C равномерно упакован в широком смысле* [13];
(iii) *Если C полностью регулярен, то он равномерно упакован в широком смысле* [6].

Из этой леммы следует, что если C – полностью регулярный $[n,k,d]_q$-код с радиусом покрытия $\rho=2$, то его дуальный код $C^\perp$ является (двухвесовым) $[n,n-k,\{d_1,d_2\}]_q$-кодом. Более того, если $C^\perp$ антиподален, то он является $[n,n-k,\{d^\perp,n\}]_q$-кодом (где $d^\perp$ – минимальное расстояние кода $C^\perp$). Именно этот класс полностью регулярных кодов изучается в настоящей статье.

Определение 3. Пусть G – абелева группа порядка q с операцией сложения. Квадратная матрица D порядка $q\mu$ с элементами из G называется *разностной матрицей* и обозначается через $D(q,\mu)$, если покомпонентная разность произвольных двух различных строк D содержит каждый элемент из G ровно μ раз.

Ясно, что матрица D сохраняет свое свойство при прибавлении строки вида $(a,a,\dots,a)$, где $a\in G$, к каждой строке D или к каждому столбцу. Применяя последовательно обе эти операции, получим *нормализованную* разностную матрицу, у которой первая строка и первый столбец состоят из нулей.

Из [14] получаем следующий результат.

Лемма 2. *Для любого q, являющегося степенью простого числа, и любых натуральных чисел ℓ и h существует разностная матрица $D(q^\ell,q^h)$.*

Напомним кратко конструкцию всех таких разностных матриц $D(q^\ell,q^h)$, см. [14]. Для произвольных натуральных чисел ℓ и h положим $u=\ell+h$. Для поля Галуа $\mathbb{F}_{q^u}$ с элементами $\{f_0=0,f_1=1,f_2,\dots,f_{q^u-1}\}$ обозначим через $F=[f_{i,j}]$ матрицу размера $q^u\times q^u$, строки и столбцы которой пронумерованы элементами поля $\mathbb{F}_{q^u}$, где $f_{i,j}=f_if_j$, т.е. F представляет собой таблицу умножения для элементов поля $\mathbb{F}_{q^u}$. Для произвольного натурального числа m будем представлять элементы из $\mathbb{F}_{q^m}$ векторами линейного пространства $\mathbb{F}_q^m$, и наоборот. Определим оператор $\Phi=\Phi_{u\to\ell}$, отображающий элемент $x=(x_1,\dots,x_u)$ пространства $\mathbb{F}_q^u$ в элемент $x^{(\ell)}=(x_1,\dots,x_\ell)$ пространства $\mathbb{F}_q^\ell$, стирая последние справа $u-\ell$ координат векторов из $\mathbb{F}_q^u$:

$$\Phi(x_1,\dots,x_\ell,\dots,x_u)=(x_1,\dots,x_\ell).$$

Обозначим через $F^{[\ell]}$ матрицу, полученную из F под действием оператора Φ, примененного к каждому элементу матрицы F:

$$F^{[\ell]}=\left[f_{i,j}^{[\ell]}\right],\quad f_{i,j}^{[\ell]}=\Phi_{u\to\ell}(f_{i,j}).$$

Лемма 3. *Для произвольного q, являющегося степенью простого числа, и произвольных натуральных чисел ℓ и h матрица $F^{[\ell]}$ является аддитивной разностной матрицей $D(q^\ell, q^h)$. Если ℓ делит h, т.е. $N = q^{h/\ell+1}$, то множество строк матрицы D образует линейное пространство.*

Рассмотрим теперь построение $(n, N, \{d, n\})_q$-кодов из разностных матриц. Без ограничения общности будем писать $G = \{0, 1, \ldots, q-1\}$, хотя операции над этими элементами выполняются как операции в группе G. Предположим, что первая строка матрицы $D = D(q, \mu)$ нулевая. Обозначим через $D^{(g)}$ матрицу, полученную из D прибавлением $g \in G$ к каждому элементу D, а именно если $D = [d_{i,j}]$, то $D^{(g)} = [d_{i,j} + g]$ для всех i и j (сумма берется в G). По определению матрицы D матрица $D^{(g)}$ является разностной матрицей $D(q, \mu)$. Кроме того, для любых двух строк $\boldsymbol{r}$ из D и $\boldsymbol{r}^{(g)}$ из $D^{(g)}$ выполняется следующее условие [14]:

$$d(\boldsymbol{r}, \boldsymbol{r}^{(g)}) = \begin{cases} q\mu, & \text{если } \boldsymbol{r}^{(g)} = \boldsymbol{r} + (g, g, \ldots, g), \\ (q-1)\mu, & \text{если } \boldsymbol{r}^{(g)} \neq \boldsymbol{r} + (g, g, \ldots, g). \end{cases} \tag{2}$$

Ясно, что матрица $D(q, \mu)$ порождает эквидистантный $(q\mu - 1, q\mu, \mu(q-1))_q$-код, являющийся оптимальным относительно верхней границы Плоткина

$$N \leqslant \frac{qd}{qd - (q-1)n}, \tag{3}$$

которая справедлива при условии, что знаменатель положителен. Чтобы показать это, достаточно привести матрицу D к виду с нулевым первым столбцом, а затем его стереть.

Пусть A^t обозначает транспонирование матрицы A. Из условия (2) получаем следующее утверждение.

Лемма 4 [14]. *Строки $(N \times n)$-матрицы $\left[D^{(0)} \mid \ldots \mid D^{(q-1)}\right]^t$ образуют двухвесовой $(n, N, \{d, n\})_q$-код с параметрами*

$$n = q\mu, \quad N = q^2\mu, \quad d = \mu(q-1). \tag{4}$$

Код C, построенный из разностной матрицы D, назовем *разностно-матричным кодом*, или сокращенно *DM-кодом*. Произвольный $(n, N, \{d, n\})_q$-код с параметрами, удовлетворяющими (4), назовем *псевдоразностно-матричным кодом*, или сокращенно *PDM-кодом*. Далее в статье мы покажем, что аддитивный PDM-код является DM-кодом. Такие коды являются оптимальными относительно q-ичного аналога границы Грэя–Рэнкина [15]. Произвольный q-ичный $(n, N, \{d, n\})_q$-код, который можно разбить на тривиальные $(n, q, n)_q$-подкоды (которые понадобятся нам позже), удовлетворяет неравенству

$$\frac{N}{q} \leqslant \frac{q(qd - (q-2)n)(n-d)}{n - ((q-1)n - qd)^2} \tag{5}$$

при условии, что $n - ((q-1)n - qd)^2 > 0$.

Напомним также оценку на мощность N кода C при условии ограничения сверху на максимальное расстояние (обозначим его через D) между различными кодовыми словами (см. [16]). Для случая $D = n$ эта оценка принимает следующий вид:

$$N \leqslant \frac{q^2 d}{dq - (q-1)(n-1)} \tag{6}$$

при условии, что знаменатель положителен.

Напомним, что q-ичная матрица M размера $N \times n$ называется ортогональной таблицей силы t, индекса $\lambda = N/q^t$ и длины n (и обозначается через $OA(N, n, q, t)$), если каждая ее $(N \times t)$-подматрица содержит среди своих строк каждый q-ичный вектор длины t ровно λ раз (см. [17]).

§ 3. Необходимые условия

Как мы уже упоминали, код $C^\perp$, дуальный к линейному $[n, k, d]_q$-ПР-коду C с радиусом покрытия $\rho = 2$, является линейным $[n, k^\perp = n-k, d^\perp]_q$-кодом со следующим свойством: для произвольного кодового слова $\boldsymbol{c} \in C^\perp$ его вес (Хэмминга) имеет два возможных значения $\mathrm{wt}(\boldsymbol{c}) \in \{w_1, w_2\}$, где $w_1 = d^\perp$. Известно [6], что если код C полностью регулярен, то его внешнее расстояние s (число ненулевых весов кода $C^\perp$) равно радиусу покрытия кода C (см. лемму 1).

В данной статье мы рассматриваем случай $w_2 = n$, т.е. код $C^\perp$ антиподален. Таким образом, для того чтобы классифицировать линейные ПР-коды с $\rho = 2$, дуальные коды которых антиподальны, необходимо перечислить все коды с двумя весами d и n, т.е. все $[n, k, \{d, n\}]_q$-коды. Такая классификация дана в работе [11]. Естественный вопрос о существовании q-ичного двухвесового $(n, N, \{d, n\})_q$-кода – это при каких условиях такой код существует. В работе [11] получен ответ на этот вопрос, и в настоящей статье мы ограничиваемся рассмотрением таких линейных кодов.

Через $\mathrm{PG}(n, q)$ обозначим n-мерное проективное пространство над полем $\mathbb{F}_q$. Под *m-дугой* будем подразумевать множество M, состоящее из m точек пространства $\mathrm{PG}(n, q)$, $m \geqslant n + 1$ и $n \geqslant 2$, таких что никакие $n + 1$ точки из M не принадлежат гиперплоскости в $\mathrm{PG}(n, q)$. При этом $(q + 1)$-дуга пространства $\mathrm{PG}(2, q)$ называется *овалом*, а $(q + 2)$-дуга пространства $\mathrm{PG}(2, q)$, где q четное, называется *полным овалом*, или *гиперовалом* (см., например, [18, 19]).

Линейный код C назовем *проективным*, если его дуальный код $C^\perp$ имеет минимальное расстояние $d^\perp \geqslant 3$ (когда любая порождающая матрица кода C не содержит двух пропорциональных столбцов, т.е. отличающихся друг от друга на скалярный множитель).

Пусть C – проективный $[n, k, d]_q$-код с ненулевыми весами $w_1, w_2, \ldots, w_s$ и порождающей матрицей G. Следуя [20], для $\alpha \neq 0$ и β, таких что для всех i сумма $\alpha w_i + \beta$ – неотрицательное целое число, определим дуальное преобразование, скажем, C^* кода C следующим образом. Рассмотрим все ненулевые векторы $v \in \mathbb{F}_q^k$, которым соответствуют различные точки в $\mathrm{PG}(k - 1, q)$. Построим матрицу G^* таким образом, что в качестве столбцов она содержит все векторы v, взятые $\alpha(vG) + \beta$ раз. Такая матрица G^* является порождающей матрицей двухвесового кода $C^*_{\alpha,\beta}$, который мы назовем *проективно дуальным* кодом для C. Следовательно, любой двухвесовой код всегда имеет проективно дуальный код.

Напомним результаты работы [21]. Положим $n_m = (q^m - 1)/(q - 1)$. Для заданного $[n, k, d]_q$-кода C с проверочной матрицей H определим *дополнительный* $[n_{n-k} - n, k, d_c]$-код C_c с проверочной матрицей H_c, полученной из проверочной матрицы H_{n-k} кода Хэмминга длины n_{n-k} стиранием всех столбцов матрицы H и скалярно кратных им. Напомним важное свойство дополнительных кодов: *произвольному кодовому слову веса w из $[n, k, d]_q$-кода C соответствует слово веса $w_c = q^{n-k-1} - w$ дополнительного кода C_c*. Из этого факта вытекает следующее утверждение.

Лемма 5 [21]. *Линейный $[n, k, d]_q$-код C с радиусом покрытия $\rho = 2$, не являющийся дуальным разностно-матричного кода, существует одновременно со своим дополнительным проективным кодом C_c с таким же радиусом покрытия $\rho_c = 2$.*

Этот хорошо известный результат был обобщен в работе [22] на произвольные двухвесовые $[n, k, \{d, d+\delta\}]_q$-коды. Приведем вариант такого утверждения для случая $[n, k, \{d, n\}]_q$-кодов. Отметим, что оно определенным образом связано с понятиями *антикодов* [23] и *миниподпространств* (minihypers) (см. [24]).

Лемма 6 [22]. *Пусть C – линейный q-ичный нетривиальный двухвесовой $[n, k, \{d, n\}]_q$-код, не являющийся дуальным к s-кратному повторению разностно-матричного кода, и пусть μ_1 и μ_2 – число кодовых слов веса, соответственно, d и n. Тогда существует линейный дополнительный двухвесовой $[n_c, k, \{d_c, d_c+\delta\}]_q$-код C_c, где*

$$n + n_c = s\frac{q^k - 1}{q - 1}, \quad d + d_c + \delta = sq^{k-1}, \quad n = d + \delta, \quad s = 1, 2, \ldots,$$

такой что C_c содержит μ_1 кодовых слов веса $d_c + \delta$, μ_2 слов веса d_c и имеет минимально возможную длину n_c, при которой матрица $\big[[C] \,|\, [C_c]\big]$ представляет собой эквидистантный $[s(q^k - 1)/(q - 1), k, sq^{k-1}]_q$-код.

Заметим, что целое число s в лемме 6 равно максимальному размеру набора столбцов порождающей матрицы кода C, скалярно кратных одному столбцу. Для проективных двухвесовых $[n, k, \{w, n\}]_q$-кодов (т.е. для случая $s = 1$) имеет место следующий результат.

Лемма 7 [25]. *Пусть C – проективный двухвесовой $[n, k, \{w, n\}]_q$-код над $\mathbb{F}_q$, где $q = p^m$, p – простое. Тогда существуют два целых числа $u \geqslant 0$ и $h \geqslant 1$, такие что*

$$w = hp^u, \quad n = (h + 1)p^u.$$

Для проективного случая мы напомним следующий результат, напрямую вытекающий из соотношений Мак-Вильямс, принимая во внимание, что минимальное расстояние $d^\perp$ дуального кода $C^\perp$ ограничено снизу: $d^\perp \geqslant 3$ (см. [25]).

Лемма 8. *Пусть C – проективный двухвесовой $[n, k, \{w, n\}]_q$-код над $\mathbb{F}_q$, где $q = p^m$, p – простое. Обозначим через μ_1 число кодовых слов кода C веса w, а через μ_2 – число кодовых слов веса n. Тогда*

$$\begin{cases} w\mu_1 + n\mu_2 = n(q-1)q^{k-1}, \\ w^2\mu_1 + n^2\mu_2 = n(q-1)(n(q-1)+1)q^{k-2}. \end{cases} \tag{7}$$

В работе [22] (см. также [26] для случая $n - d = 1$) были получены условия целочисленности, аналогичные условиям, найденным Дельсартом для проективных двухвесовых кодов в [25] (см. также [27]). Эти соотношения получаются простыми комбинаторными рассуждениями без привлечения понятия собственных значений сильно регулярных графов. Для случая произвольного двухвесового $(n, N, \{d, n\})_q$-кода с расстояниями d и n такие условия были выведены в работе [11].

Теорема 1. *Пусть C – нетривиальный q-ичный двухвесовой $(n, k, \{d, n\})_q$-код. Тогда*:

(i) *Код C имеет мощность $N = q^k$, при этом*

$$\max\{(q-1)n + 1, q^2\} \leqslant N \leqslant \frac{q^2 d}{qd - (q-1)(n-1)}; \tag{8}$$

(ii) *Правое неравенство в (8) превращается в равенство тогда и только тогда, когда матрица $[C]$ кодовых слов кода C является ортогональной таблицей силы $t \geqslant 2$;*

(iii) *В случае, когда правое неравенство в* (8) *превращается в равенство, длина* n *и расстояние* d *кода* C *имеют следующий вид*:

$$n = \frac{N(q(d+1)-1) - q^2 d}{N(q-1)} \tag{9}$$

и

$$d = (n-1)\frac{(q-1)N}{q(N-q)}; \tag{10}$$

(iv) *Левое неравенство в* (8) *превращается в равенство тогда и только тогда, когда либо код* C *с параметрами* $(n, q^2, \{n-1, n\})_q$ *получен из* $n-2$ *взаимно ортогональных латинских квадратов порядка* q*, где* $n \leqslant q$*, либо* C *является эквидистантным* $(n, N, d)_q$*-кодом (это случай, который мы не рассматриваем)*;

(v) *Если* C *– нетривиальный двухвесовой* $(n, q^2, \{d, n\})_q$*-код, то число* N *делит* $q^2 d$*, а число* $q-1$ *делит* $(N-1)d$.

Следующее утверждение является вариантом теоремы 2 из [22] для случая нетривиального $[n, k, \{d, n\}]_q$-кода (и поэтому не требует доказательства). Предположим, что $q = p^m$, где $m \geqslant 1$, p – простое. Для произвольного натурального числа a обозначим через $\gamma_a \geqslant 0$ максимальное число, такое что p^{γ_a} делит a, т.е. $a = p^{\gamma_a} h$, где h и p взаимно просты. Определим γ_d, γ_δ и γ_c аналогичным образом для чисел, соответственно, d, δ и d_c. Напомним, что (a, b) обозначает наибольший общий делитель (НОД) двух целых чисел a и b.

Теорема 2. *Пусть* $q = p^m$*, где* $m \geqslant 1$*,* p *– простое. Пусть* C *– линейный* q*-ичный (двухвесовой)* $[n, k, \{d, n\}]_q$*-код размерности* $k \geqslant 2$*, и обозначим через* C_c *его двухвесовой дополнительный* $[n_c, k, \{d_c, d_c + \delta\}]_q$*-код, где*

$$d + \delta = n \quad и \quad d + d_c + \delta = sq^{k-1}, \quad s \geqslant 1.$$

(i) *Если* $s = 1$ *и* $k \geqslant 4$*, т.е.* C*, а значит, и* C_c *– проективные коды, то выполнены следующие два равенства*:

$$(q, d) = (q, \delta) \quad и \quad (q, d_c) = (q, \delta); \tag{11}$$

(ii) *Если* $s = 1$ *и* $k = 3$*, то оба равенства в* (11) *выполняются, если выполнено хотя бы одно из двух условий*:

$$(d, q)^2 \leqslant q(n(n-1), q) \quad или \quad (d + \delta, q)^2 > q(n_c(n_c - 1), q);$$

(iii) *Если* $s = 1$ *и* $k \geqslant 2$*, то тогда выполняется хотя бы одно из двух условий*:

$$\gamma_d = \gamma_\delta \quad или \quad \gamma_c = \gamma_\delta; \tag{12}$$

(iv) *Если* $s \geqslant 1$ *и* $k \geqslant 3$*, то выполняется хотя бы одно из двух равенств в* (11) (*соответственно, в* (12)).

§ 4. Известные полностью регулярные коды с радиусом покрытия $\rho = 2$

Перечислим теперь все нетривиальные линейные $[n, k, \{d, n\}]_q$-коды. Это даст классификацию линейных ПР-кодов с $\rho = 2$, у которых дуальные коды антиподальны. Большая часть этих двухвесовых кодов содержится в обзоре двухвесовых кодов Кальдербэнка и Кантора [27], и все они приведены в [10].

Начнем с одного утверждения, являющегося переформулировкой результата из работы [10].

Теорема 3. *Пусть задан нетривиальный линейный $[n,k,d]_q$-код C. Пусть G – его порождающая матрица. Тогда C является $[n,k,\{d,n\}]_q$-кодом, если и только если матрица G с точностью до эквивалентности имеет вид*

$$G = \begin{bmatrix} 1 & \dots & 1 \\ & G^* & \end{bmatrix},$$

где матрица G^* порождает эквидистантный код C^* со следующим свойством: для произвольного ненулевого кодового слова $\boldsymbol{v} \in C^*$ каждый символ $\alpha \in \mathbb{F}_q$, встречающийся на координатной позиции слова $\boldsymbol{v}$, встречается там ровно $n-d$ раз, где d – минимальное расстояние кода C^*.

Следуя работе [15], будем называть тривиальный $(n,q,n)_q$-код *симплексом*. Будем говорить, что q-ичный дистанционно-инвариантный код длины n является *симплексным кодом*, если он содержит симплекс в качестве подкода. Ясно, что аддитивный $(n,N,\{d,n\})_q$-код является дистанционно-инвариантным симплексным кодом. Следующий результат можно найти в работе [15].

Предложение. *Пусть мощность q-ичного кода C длины n с расстоянием $d = \dfrac{(q-1)n}{q}$ равна qn. Тогда код C можно представить в виде объединения попарно непересекающихся симплексных кодов.*

Возникает естественный вопрос: *при каких условиях симплексный код из этого предложения является либо PDM-, либо DM-кодом*? Частичный ответ дает следующая

Теорема 4 [9]. *Пусть C является дистанционно-инвариантным симплексным $(n,N,\{d,n\})_q$-кодом. Тогда*:

(i) *Код C можно разбить на попарно непересекающиеся подкоды*:

$$C = \bigcup_{i=1}^{N/q} C_i,$$

где для каждого i подкод C_i – это симплекс, и при этом N кратно q;

(ii) *Для произвольного кодового слова $\boldsymbol{c} \in C$, отличного от $(a,a,\dots,a)$, $a \in \mathbb{F}_q$, каждый символ $\alpha \in \mathbb{F}_q$, встречающийся среди координат слова $\boldsymbol{c}$, встречается в этом кодовом слове ровно μ раз, где $\mu = n-d$, а n кратно числу μ;*

(iii) *Расстояние d кода C удовлетворяет следующему неравенству*:

$$d \leqslant n\frac{q-1}{q}; \tag{13}$$

(iv) *Если (13) является строгим неравенством, а $N = qn$, то код C является псевдоразностно-матричным кодом с параметрами*

$$n = \mu q, \quad N = \mu q^2, \quad d = \mu(q-1), \quad \mu = n-d;$$

(v) *Если в пункте* (iv) *код C аддитивен, то он является разностно-матричным кодом.*

Замечание 1. Покажем, что условия $n = q(n-d)$ в $N = qn$ для пунктов (iv) и (v) являются необходимыми. Рассмотрим матрицу $[C] = \left[D^{(0)} \mid \dots \mid D^{(q-1)}\right]^t$, образованную сдвигами $D^{(i)}$ разностной матрицы $D = D(q,\mu)$, где C – $(n,N,\{d,n\})_q$-DM-код. Если удалить одну (или более) таких матриц $D^{(i)}$ из матрицы кодовых слов $[C]$, то мы получим дистанционно-инвариантный симплексный код мощности $N^* < qn$, т.е. нелинейный двухвесовой $(n,N^*,\{d,n\})_q$-код, удовлетворяющий условиям теоремы.

Аналогично необходимым является условие $N = qn$ в пунктах (iv) и (v). Например, линейные коды Буша (см. далее) имеют длину $n < q(n-d)$. Аналогичным образом, аддитивный $(n, N, \{d, n\})_q$-код не обязательно имеет мощность q^k. Например, разностная матрица $D(4, 2)$ индуцирует оптимальный аддитивный $(8, 32, \{6, 8\})_4$-код мощности $N \neq 4^k$.

Замечание 2. Случай кодов с $N = q^2$ является особым. Как известно, $r-2$ попарно ортогональных латинских квадратов порядка q индуцируют $(r, q^2, \{r-1, r\})_q$-код. Для случая, когда q является степенью простого числа, существует $q-1$ попарно ортогональных латинских квадратов, порождающих линейный эквидистантный $[q+1, 2, q]_q$-код (обратное хорошо известное утверждение также справедливо для произвольной длины $r \leqslant q+1$). Используя эти коды с соответствующими длинами r, очевидным образом можно построить (пользуясь разбиением на симплексные коды) $(n, 2, \{d, n\})_q$-коды для произвольных натуральных d и n с единственным условием, что $d \geqslant n/2$, которое гарантируется границей Плоткина (3). Эти тривиальные коды мы не рассматриваем.

Приведем теперь все известные семейства линейных нетривиальных $[n, k, d]_q$-ПР-кодов, перечисленные в работе [10]:

(ПР.1) *Расширенные двоичные совершенные коды Хэмминга.* Это коды с параметрами $[n = 2^m, k = n-m-1, 4]$, наиболее известные двоичные разностно-матричные коды, дуальные к линейным $[2^m, m+1, 2^{m-1}]$-кодам Адамара. Проверочная матрица H_m для таких кодов имеет размер $(m+1) \times 2^m$, где m строчек матрицы H_m образованы всеми 2^m различными двоичными векторами длины m в качестве столбцов, а $(m+1)$-й строкой является вектор из всех единиц $\mathbf{1} = (1, 1, 1, \ldots, 1)$. Для этого случая дуальным к коду Адамара является расширенный двоичный совершенный код Хэмминга. Вектор пересечений для этих кодов имеет вид $\mathrm{IA} = (n, n-1; 1, n)$.

(ПР.2) *Дуальный к разностно-матричному коду.* Таковыми являются коды с параметрами $[n = q^m, n-m-1, 3]_q$, имеющие радиус покрытия 2, дуальные к разностно-матричным кодам, индуцированными разностными матрицами. Широкий класс таких матриц и соответствующих аддитивных и линейных DM-кодов с параметрами (4) даны в [14] (см. лемму 2), для значений

$$q = p^{mh}, \quad \mu = p^{m\ell}, \quad p \text{ – простое}, \quad m = 1, 2, 3, \ldots,$$

для любых натуральных чисел h и ℓ. Лемма 2 приводит пример простой конструкции всех таких кодов, а теорема 4 дает их описание. Вектор пересечений для этих кодов имеет вид

$$\mathrm{IA} = (n(q-1), n-1; 1, n(q-1)).$$

(ПР.3) *Дуальные к кодам латинских квадратов*, являющиеся также МДР-кодами. Это известные $[n, n-2, 3]_q$-коды, индуцированные $n-2$ взаимно ортогональными латинскими квадратами порядка q. В теореме 1 такие $[n, 2, \{n-1, n\}]_q$-коды, образованные латинскими квадратами, имеют длину n и кодовое расстояние $d = n-1$, откуда следует мощность $N = q^2$. Поскольку q – степень простого числа, линейный $[n, 2, \{n-1, n\}]_q$-код по латинским квадратам C_l имеет произвольную длину n в диапазоне $2 \leqslant n \leqslant q$ и порождается матрицей

$$G_l = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & a_2 & a_3 & \ldots & a_{n-1} \end{bmatrix},$$

где $a_0 = 0$, $a_1 = 1$, а $a_2, \ldots, a_{n-1}$ – различные элементы поля $\mathbb{F}_q$. Вектор пересечений для этих кодов имеет вид

$$\mathrm{IA} = (n(q-1), (q-n+1)(n-1); 1, n(n-1)).$$

(ПР.4) *Дуальный код к кодам Буша*, или расширенный код Хэмминга длины $q+1$ (в [11] эти коды назывались кодами Боуза – Буша, но на самом деле эти коды должны именоваться кодами Буша). Это семейство $[q+2, q-1, 4]_q$-кодов, дуальные коды которых были построены Бушем [28] в 1952 году (в терминах ортогональных таблиц индекса 1) и которые существуют для произвольного $q = 2^m \geqslant 4$ (семейство TF1 в [27]). В теореме 1 коды Буша соответствуют случаю расстояния $d = n-2$, откуда следует мощность $N = q^3$. Они являются классическим объектом проективной геометрии, поскольку такие коды индуцированны гиперовалами в пространстве $\mathrm{PG}(3, q)$. Дуальные $[q+2, q-1, 4]_q$-коды представляют собой расширенные q-ичные (совершенные) коды Хэмминга длины $q+1$. Приведем порождающую матрицу G_b для $[q+2, 3, \{q, q+2\}]_q$-кодов Буша, отличающуюся от матриц, приведенных Бушем [28] и Дельсартом [21], так как нам удобней следовать структуре порождающих матриц, приведенной в теореме 3:

$$G_b = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 0 & 1 & x_1 & \dots & x_i & \dots & x_{q-2} \\ 0 & 0 & 1 & 1 & y_1 & \dots & y_i & \dots & y_{q-2} \end{bmatrix}, \tag{14}$$

где

$$x_i = \frac{\alpha^i}{1+\alpha^i+\alpha^{2i}}, \quad y_i = \frac{\alpha^{2i}}{1+\alpha^i+\alpha^{2i}},$$

а α – примитивный элемент поля $\mathbb{F}_q$. Вектор пересечений для этих кодов имеет вид

$$\mathrm{IA} = ((q+2)(q-1), q^2-1; 1, q+2).$$

(ПР.5) *Коды, дуальные к коду Дельсарта*, с параметрами

$$[n = q(q-1)/2, k = n-3, 4]_q.$$

Для случая $q = 2^s \geqslant 4$ Дельсарт в [25] построил q-ичные коды с параметрами

$$[q(q-1)/2, 3, \{q(q-2)/2, q(q-1)/2\}]_q.$$

Эти коды являются проективно дуальными к кодам (ПР.4) (см. семейство $\mathrm{TF1}^d$ в [27]). В теореме 2 этот случай соответствует расстоянию $d = n(q-2)/(q-1)$, откуда следует мощность $N = q^3$. Дуальные коды – это расширенные q-ичные ПР-коды с порождающей матрицей G_d, состоящей из столбцов $\left[1, \alpha^i, \alpha^{2i}\right]^t$, таких что $\mathrm{Tr}(\alpha^{3i}) = 1$, где $\mathrm{Tr}(x)$ – функция следа из $\mathbb{F}_q$ в $\mathbb{F}_2$:

$$\mathrm{Tr}(x) = x + x^2 + x^4 + \ldots + x^{q/2}.$$

Вектор пересечений для этих кодов имеет вид

$$\mathrm{IA} = ((q-1)n, (q-2)(q+1)(q+2)/4; 1, q(q-1)(q-2)/4).$$

(ПР.6) *Дуальные к кодам Деннистона.* Это семейство кодов с параметрами

$$[n = 1+(q+1)(h-1), k = (q+1)(h-1)-2, d = 4]_q,$$

дуальных к $[n = 1+(q+1)(h-1), 3, \{q(h-1), n\}]_q$-кодам Деннистона, где $1 < h < q$, h делит q, $q = 2^r \geqslant 4$ (семейство TF2 в [27]). В теореме 1 этот случай соответствует расстоянию $d = (n-1)q/(q+1) = n-h+1$, откуда следует мощность $N = q^3$. Дуальные коды – это расширенные q-ичные коды с $d = 4$. При $h = 2$ получаем коды Буша (ПР.4). Коды (ПР.6) образованы максимальными дугами проективной плоскости [18]. Эта конструкция соответствует теореме 3. Кратко поясним,

следуя Деннистону, построение таких кодов для произвольного $q = 2^m \geqslant 4$ и натурального $h \geqslant 2$, делящего q, т.е $h = 2^u \leqslant q/2$. Для заданного поля $\mathbb{F}_q$ пусть H – подгруппа порядка h аддитивной группы поля $\mathbb{F}_q$. Пусть $\varphi(x, y)$ – неприводимая квадратичная форма над $\mathbb{F}_q$, например, вида $\varphi(x, y) = ax^2 + bxy + cy^2$. Тогда $[n, 3, \{d, n\}]_q$-код Деннистона [18] (см. также [19]) порождается следующей $(3 \times n)$-матрицей:

$$G_{dn} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{bmatrix}, \tag{15}$$

где $n = (q+1)((h-1)+1)$, $d = n-h$, а (x_i, y_i) – все упорядоченные пары элементов поля $\mathbb{F}_q$, такие что $\varphi(x_i, y_i) \in H$.

Приведем теперь новую явную конструкцию матриц G_{dn}, порождающих коды Деннистона. Пусть $\{z_1 = 1, z_2, \dots, z_{h-1}\}$ – ненулевые элементы подполя $\mathbb{F}_h$ поля $\mathbb{F}_q$. Пусть G_b^- – матрица размера $3 \times (q+1)$, полученная из G_b удалением первого столбца. Тогда матрица G_{dn} имеет вид

$$G_{dn} = \left[G_b \,|\, G_b^-(z_2) \,|\, \dots \,|\, G_b^-(z_{h-1})\right],$$

где матрица $G_b^-(z_i)$ для любого $i = 2, \dots, h-1$ получается из G_b^- умножением второй и третьей строки на элемент z_i.

Если множества всех элементов $\{x_i\}$ и $\{y_i\}$ не удовлетворяют теореме 3, то нетрудно построить такую порождающую матрицу из матрицы G_b кода Буша. Для этого случая матрицу G_{dn} можно представить в виде

$$G_{dn} = \left[G \,|\, G^*(u_1, s_1) \,|\, \dots \,|\, G^*(u_{h-2}, s_{h-2})\right].$$

Здесь G^* получается из G_b стиранием первого столбца, а затем $G^*(u_i, s_i)$ получается из G^* умножением второй строки матрицы G^* на α^{u_i} и третьей строки G^* на α^{s_i}. Существование таких натуральных чисел u_i и s_i следует из существования таких кодов [18, 27].

Вектор пересечений для этих кодов имеет вид

$$\text{IA} = ((q-1)n, (q+1)(h-1)(q-h+1); 1, (h-1)n).$$

§ 5. Основной результат

Теперь сформулируем и докажем основной результат данной статьи.

Теорема 5. *Пусть C – нетривиальный линейный полностью регулярный $[n, k, d]_q$-код с радиусом покрытия $\rho = 2$, дуальный код которого $C^\perp$ является антиподальным, т.е. $[n, n-k, \{d^\perp, n\}]_q$-кодом. Тогда код C имеет параметры, совпадающие с параметрами одного из кодов из рассмотренных семейств* (ПР.1)–(ПР.6).

Доказательство. В работе [11] были классифицированы все аддитивные $(n, N, \{d, n\})_q$-коды, и в линейном случае они соответствуют дуальным кодам семейств (ПР.1)–(ПР.6). Для независимости нашего изложения мы повторим основные моменты доказательства из [11] для линейного случая.

Поскольку C – нетривиальный линейный код, его мощность равна $N = q^k$, где $2 \leqslant k \leqslant n-2$.

Начнем со случая $k = 2$. Для любого числа q, являющегося степенью простого числа $q = p^s$, из существования r попарно ортогональных латинских квадратов следует существование $[r+2, 2, r+1]_q$-МДР-кода, дуальный код которого является $[r+2, r, 3]_q$-ПР-кодом из семейства (ПР.3) (см. замечание 2). Эти коды включают в себя разностно-матричные $[q, 2, q-1]_q$-коды наименьшей возможной длины

из семейства (ПР.2), которые существуют для произвольной степени простого q и совпадают с кодами по латинским квадратам.

Рассмотрим теперь случай $N = q^3$. Покажем сначала, что в кодах Деннистона число h должно делить q. Из теоремы 4 вытекает, что n – кратное числа $n - d$, а значит, n можно представить в виде $n = (n - d)\ell$ для некоторого натурального числа ℓ. Следовательно, $d = n(\ell - 1)/\ell$, и из (13) получаем

$$d = n\frac{\ell - 1}{\ell} \leqslant n\frac{q - 1}{q},$$

откуда следует, что $\ell \leqslant q$. Однако случай $\ell = q$ приводит к разностно-матричному коду, и следовательно, $\ell < q$. Теперь предположим, что $n = 1 + (q + 1)(h - 1)$ и $d = q(h - 1)$ для некоторого натурального числа $h \geqslant 2$. Из этого следует, что $n = q(h-1)+h = d+h$. Таким образом, объединяя два равенства $n = 1+(q+1)(h-1)$ и $d = q(h - 1) = n(\ell - 1)/\ell$, получаем, что

$$q(h - 1) = (q(h - 1) + h)\frac{\ell - 1}{\ell},$$

откуда следует, что $h(\ell - 1) = q(h - 1)$. Поскольку $h \geqslant 2$, и следовательно, h и $h - 1$ взаимно просты, то h делит q, а значит, мы получаем коды Деннистона или, для случая $h = 2$, коды Буша.

Случай $N = q^4$ также дает линейные коды из семейства (ПР.4) [14]. Действительно, из $[n, 4, \{d, n\}]_q$-кода C можно получить код C_0, являющийся линейным эквидистантным $[n-1, 3, d]_q$-кодом длины $n-1 = (q^4-1)/(q-1)$ с расстоянием $d = q^3$, дуальным кодом которого является совершенный q-ичный код Хэмминга.

Покажем теперь, что для случая $N = q^4$ не существует кодов типа Буша, Деннистона или Дельсарта. По теореме 3 длина кода Буша или Деннистона должна быть равной $n = s(q^3 - 1)/(q - 1) + 1$. Поскольку n кратно $n - d$ (см. теорему 3), то длина кода имеет вид $n = d\ell/(\ell - 1)$ для некоторого натурального $\ell \leqslant q$. Получаем (принимая во внимание, что $cd = sq^2$)

$$n = s\frac{q^3 - 1}{q - 1} + 1 = d\frac{\ell}{\ell - 1} = sq^2\frac{\ell}{\ell - 1}. \tag{16}$$

Далее необходимо рассмотреть случаи $(s, q - 1) = 1$ и $(s, q - 1) \geqslant 2$ по отдельности.

Пусть для начала $(s, q - 1) = 1$. Тогда видно, что целое число n, стоящее в левой части равенства, не делится ни на s, ни на q, однако целое число в правой части делится на s и q. Полученное противоречие показывает, что таких кодов не существует.

Теперь предположим, что $(s, q-1) \geqslant 2$. Для случая $s = q-1$ получаем, что $n = q^3$, и поскольку $N = q^4$, т.е. $N = qn$, то отсюда следует, что C – разностно-матричный код (ПР.2).

Пусть теперь $s = u(q - 1)$, где $u \geqslant 2$. Подставляя это значение s в (16), получаем

$$0 \leqslant uq^2(q - \ell) = -u\ell + (u + \ell) - 1 \leqslant -1,$$

что не может иметь места, поскольку $2 \leqslant \ell \leqslant q$ и $u \geqslant 2$, что и завершает разбор случая $N = q^4$.

Случай $N = q^k$ для $k \geqslant 5$ рассматривается аналогичным образом, и мы его опускаем.

Осталось рассмотреть случай, когда q – степень нечетного числа.

Для всех кодов семейств (ПР.1)–(ПР.3) приведенные доказательства справедливы как для четного, так и для нечетного случая степени простого q.

В 1952 г. Буш [28] доказал несуществование $(q+2, 3, q)_q$-кодов для нечетных q, т.е. кодов семейства (ПР.4), откуда следует несуществование $[q(q-1)/2, 3, \{q(q-2)/2, q(q-1)/2\}]_q$-кодов Дельсарта семейства (ПР.5) для случая нечетного q (поскольку они проективно дуальны к кодам Буша [27]). Затем в 1997 г. в работе [29] было доказано несуществование максимальных дуг в плоскостях Дезарга нечетного порядка, откуда следует несуществование кодов Деннистона семейства (ПР.6) для нечетных q. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Neumaier A.* Distance Matrices, Dimension, and Conference Graphs // Nederl. Akad. Wetensch. Indag. Math. 1981. V. 43. № 4. P. 385–391. https://doi.org/10.1016/1385-7258(81)90059-7
2. *Бассалыго Л.А., Зайцев Г.В., Зиновьев В.А.* О равномерно упакованных кодах // Пробл. передачи информ. 1974. Т. 10. № 1. С. 9–14. https://www.mathnet.ru/ppi1014
3. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. № 1. С. 38–50. https://www.mathnet.ru/ppi1621
4. *Goethals J.-M., van Tilborg H.C.A.* Uniformly Packed Codes // Philips Res. Rep. 1975. V. 30. P. 9–36.
5. *Боржес Ж., Рифа Ж., Зиновьев В.А.* О полностью регулярных кодах // Пробл. передачи информ. 2019. Т. 55. № 1. С. 3–50. https://doi.org/10.1134/S0134347519010017
6. *Brouwer A.E., Cohen A.M., Neumaier A.* Distance-Regular Graphs. Berlin: Springer, 1989.
7. *van Dam E.R., Koolen J.H., Tanaka H.* Distance-Regular Graphs // Electron. J. Combin. 2016. Dynamic Surveys, DS22 (156 pp.). https://doi.org/10.37236/4925
8. *Koolen J., Krotov D., Martin B.* Completely Regular Codes (electronic pages). https://sites.google.com/site/completelyregularcodes
9. *Bonisoli A.*, Every Equidistant Linear Code Is a Sequence of Dual Hamming Codes // Ars Combin. 1984. V. 18. P. 181–186.
10. *Borges J., Rifà J., Zinoviev V.A.* On q-ary Linear Completely Regular Codes with $\rho = 2$ and Antipodal Dual // Adv. Math. Commun. 2010. V. 4. № 4. P. 567–578. https://doi.org/10.3934/amc.2010.4.567
11. *Бойваленков П., Делчев К., Зиновьев Д.В., Зиновьев В.А.* О кодах с расстояниями d и n // Пробл. передачи информ. 2022. Т. 58. № 4. С. 62–83. https://doi.org/10.31857/S0555292322040064
12. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10 (97 pp.).
13. *Бассалыго Л.А., Зиновьев В.А.* Замечание о равномерно упакованных кодах // Пробл. передачи информ. 1977. Т. 13. № 3. С. 22–25. https://www.mathnet.ru/ppi1091
14. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87. https://www.mathnet.ru/ppi1804
15. *Бассалыго Л.А., Додунеков С.М., Зиновьев В.А., Хеллесет Т.* Граница Грея – Рэнкина для недвоичных кодов // Пробл. передачи информ. 2006. Т. 42. № 3. С. 37–44. https://www.mathnet.ru/rus/ppi51
16. *Helleseth T., Kløve T., Levenshtein V.I.* A Bound for Codes with Given Minimum and Maximum Distances // Proc. 2006 IEEE Int. Symp. on Information Theory (ISIT'2006). Seattle, WA, USA. July 9–14, 2006. P. 292–296. https://doi.org/10.1109/ISIT.2006.261600
17. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge, UK: Cambridge Univ. Press, 1986.
18. *Denniston R.H.F.* Some Maximal Arcs in Finite Projective Planes // J. Combin. Theory. 1969. V. 6. № 3. P. 317–319. https://doi.org/10.1016/S0021-9800(69)80095-5
19. *Thas J.A.* Projective Geometry over a Finite Field // Handbook of Incidence Geometry: Buildings and Foundations. Amsterdam: Elsevier, 1995. Ch. 7. P. 295–347. https://doi.org/10.1016/B978-044488355-1/50009-8

20. *Bouyukliev I.G.* Classification of Griesmer Codes and Dual Transform // Discrete Math. 2009. V. 309. № 12. P. 4049–4068. https://doi.org/10.1016/j.disc.2008.12.002
21. *Delsarte P.* Two-Weight Linear Codes and Strongly Regular Graphs // MBLE Research Lab. Report R160. Brussels, Belgium, 1971.
22. *Boyvalenkov P., Delchev K., Zinoviev D.V., Zinoviev V.A.* On Two-Weight Codes // Discrete Math. 2021. V. 344. № 5. Paper No. 112318 (15 pp.). https://doi.org/10.1016/j.disc.2021.112318
23. *Farrell P.G.* Linear Binary Anticodes // Electron. Lett. 1970. V. 6. № 13. P. 419–421. https://doi.org/10.1049/el:19700293
24. *Hamada N., Helleseth T.* Codes and Minihypers // Proc. 3rd EuroWorkshop on Optimal Codes and Related Topics (OC'2001). Sunny Beach, Bulgaria. June 10–16, 2001. P. 79–84.
25. *Delsarte P.* Weights of Linear Codes and Strongly Regular Normed Spaces // Discrete Math. 1972. V. 3. № 1–3. P. 47–64. https://doi.org/10.1016/0012-365X(72)90024-6
26. *Бойваленков П., Делчев К., Зиновьев Д.В., Зиновьев В.А.* О q-ичных кодах с двумя расстояниями d и $d+1$ // Пробл. передачи информ. 2020. Т. 56. № 1. С. 38–50. https://doi.org/10.31857/S0555292320010040
27. *Calderbank R., Kantor W.M.* The Geometry of Two-Weight Codes // Bull. London Math. Soc. 1986. V. 18. № 2. P. 97–122. https://doi.org/10.1112/blms/18.2.97
28. *Bush K.A.* Orthogonal Arrays of Index Unity // Ann. Math. Statist. 1952. V. 23. № 3. P. 426–434. https://doi.org/10.1214/aoms/1177729387
29. *Ball S., Blokhuis A., Mazzocca F.* Maximal Arcs in Desarguesian Planes of Odd Order Do Not Exist // Combinatorica. 1997. V. 17. № 1. P. 31–41. https://doi.org/10.1007/BF01196129

Боржес Жуаким (Borges, Joaquim)
Факультет информационно-коммуникационных технологий,
Независимый университет Барселоны, Испания
joaquim.borges@uab.cat
Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
14.06.2023
После доработки
27.11.2023
Принята к публикации
27.11.2023

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*

Москва
ФГБУ Издательство «Наука»