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 – IA) 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.

Л е м м а 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.

О п р е д е л е н и е 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.

Л е м м а 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:

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

Л е м м а 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.

Л е м м а 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*

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

(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*

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

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

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

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

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

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

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

(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:

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

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:

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

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 $\{z_1 = 1, z_2, \ldots, z_{h-1}\}$ – 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

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

где матрица $G_b^-(z_i)$ для любого $i = 2, \ldots, h - 1$ 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

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

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

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

§ 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