ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.725

© 2022 г. **П. Бойваленков[1], К. Делчев[2], В.А. Зиновьев[3], Д.В. Зиновьев[3]**

О КОДАХ С РАССТОЯНИЯМИ d И n

Перечислены все q-ичные аддитивные (и в частности, линейные) блоковые коды длины n и мощности $N \geqslant q^2$, имеющие ровно два расстояния: d и n. Для произвольных кодов длины n с расстояниями d и n получены верхние оценки на мощность с помощью линейного программирования и через связь с множествами точек на евклидовой сфере с двумя расстояниями.

Ключевые слова: код с двумя расстояниями, двухвесовой код, линейный двухвесовой код, разностная матрица, максимальная дуга, латинский квадрат, ортогональная таблица, оценка на коды, граница линейного программирования, сферический код.

DOI: 10.31857/S0555292322040064, **EDN:** NAWXWG

§ 1. Введение

В статье рассматриваются q-ичные блоковые коды длины n, имеющие ровно два расстояния – d и n. Коды с двумя расстояниями – это классический объект исследования в алгебраической теории кодирования в течение более 55 лет. Исчерпывающий обзор таких кодов можно найти в работе [1]. Построение новых семейств таких кодов, так же как и описание некоторых существующих классов таких кодов, остаются важнейшими открытыми проблемами алгебраической теории кодирования (см., например, работу [2] и библиографию в ней). Несмотря на многие известные бесконечные классы двухвесовых кодов, полная классификация таких линейных кодов весьма далека от завершения. Даже в случае кодов с расстояниями d и n до этой статьи мы не могли сказать, что все такие коды известны.

В двух предыдущих работах [3, 4] мы описали такие коды для специального случая, когда два расстояния – это d и $d+1$, и показали, что все такие коды получаются из эквидистантных кодов двумя способами: либо добавлением одной произвольной позиции (так чтобы сохранить линейность кода) ко всем словам, либо выбрасыванием одной произвольной позиции из всех кодовых слов. Затем в работах [5, 6] мы рассмотрели произвольные линейные и нелинейные коды с двумя весами d и $d+\delta$ и усилили известные результаты Дельсарта [7, 8], касающиеся необходимых условий существования таких проективных кодов. Следует также упомянуть работу [9], где с помощью описания всех дуг в проективной геометрии $PG(r, q)$ с кратностями

[1] Работа выполнена при частичной поддержке Национального научного фонда Болгарии (NSF) (проект КР-06-Russia/33-2020).

[2] Работа выполнена при частичной поддержке Национального научного фонда Болгарии (NSF) (проект КР-06-N32/2-2019).

[3] Исследования 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).

пересекающих их гиперплоскостей w, $w+1$ и $w+2$ были классифицированы все q-ичные линейные коды с расстояниями d, $d+1$ и $d+2$.

Главная цель данной статьи – это перечисление аддитивных и неаддитивных (включая дистанционно инвариантные) блоковых кодов длины n, имеющих ровно два расстояния для очень специального случая, когда эти расстояния равны d и n. Интересно, что линейные коды такого вида имеют порождающие матрицы, связанные с порождающими матрицами эквидистантных линейных кодов (они получаются из последних добавлением нулевого столбца и строки из всех единиц). Этот эффект был замечен в [10] в терминах полностью регулярных кодов с радиусом покрытия $\rho = 2$. Мы приводим необходимые и достаточные условия для существования таких кодов и даем их простое описание. Мы также приводим некоторые новые верхние оценки на мощность таких произвольных кодов ровно с двумя расстояниями d и n. Одна из таких оценок это граница линейного программирования, а другая оценка связана со сферическими кодами, имеющими между кодовыми точками ровно два расстояния в евклидовой метрике.

§ 2. Предварительные результаты

Пусть $q \geqslant 2$ – целое положительное число, и пусть всюду далее $Q = \{0, 1, \ldots, q-1\}$ – абелева группа, представленная в аддитивной форме, с нейтральным элементом 0. Любое подмножество $C \subseteq Q^n$ представляет собой код длины n, мощности $N = |C|$ с минимальным расстоянием d (т.е. $d = \min\{d(x,y) : x, y \in C,\ x \neq y\}$), где

$$d(x,y) = |\{i\} : x_i \neq y_i,\ i = 1, \ldots, n\}| \quad \text{для } x = (x_1, \ldots, x_n) \text{ и } y = (y_1, \ldots, y_n),$$

который обозначается через $(n, N, d)_q$. Если q – степень простого числа, то Q – это множество элементов поля Галуа $\mathbb{F}_q$, которые мы также будем обозначать через $0, 1, \ldots, q-1$, но операции над этими элементами будут осуществляться в поле $\mathbb{F}_q$. Если $(n, N, d)_q$-код C представляет собой k-мерное подпространство линейного пространства Q^n, то мы используем для такого кода стандартное обозначение $[n, k, d]_q$, где $N = q^k$. Для двоичного случая, т.е. когда $q = 2$, символ q опускается и используются обозначения (n, N, d) и $[n, k, d]$ соответственно. В настоящей статье под понятием *аддитивный* мы имеем ввиду абелеву подгруппу в абелевой группе Q^n с аддитивной покоординатной операцией в Q (так что, конечно, эти коды включают в себя и линейные коды).

Пусть $(n, N, \{d, n\})_q$ обозначает $(n, N, d)_q$-код $C \subset Q^n$, обладающий следующим свойством: для любых двух различных кодовых слов x и y кода C расстояние Хэмминга $d(x, y)$ между этими словами равно либо d, либо n. Если не оговорено противное, то мы всегда полагаем, что в таком коде оба расстояния d и n реализуются.

Нас будут интересовать вопросы существования, построения и перечисления таких $(n, N, \{d, n\})_q$-кодов, а также верхние оценки максимально возможной мощности произвольных кодов такого вида.

Мы не рассматриваем тривиальные случаи таких кодов, как, например, повторение двух (или более) $(n_1, N, \{d_1, n_1\})_q$- и $(n_2, N, \{d_2, n_2\})_q$-кодов с одинаковыми или разными параметрами, эквидистантные коды, коды с тривиальными (т.е. постоянными) координатными позициями и так далее.

Определение 1. Пусть G – абелева группа порядка q, представленная в аддитивном виде. Квадратная матрица D порядка $q\mu$ с элементами из G называется *разностной матрицей* и обозначается через $D = D(q, \mu)$, если покоординатная разность любых двух ее различных строк содержит каждый элемент G ровно μ раз.

Ясно, что матрица D инвариантна относительно сложения любой ее строки или столбца с постоянным вектором $(a, a, \ldots, a)$, где $a \in G$. Осуществляя такие операции, мы всегда можем привести разностную матрицу D к *нормализованной* разностной

матрице, которая имеет нулевую первую строку и нулевой первый столбец. В дальнейшем, если не оговорено противное, без ограничения общности мы всегда будем полагать, что разностная матрица представлена в нормализованной форме.

Из [11] (см. также [12]) известен следующий результат.

Лемма 1. *Для любого простого числа p и любых натуральных чисел ℓ и h существует разностная матрица $D(p^\ell, p^h)$.*

Опишем кратко построение всех таких разностных матриц $D(p^\ell, p^h)$ из работы [12]. Для любого целого $m \geqslant 1$ зафиксируем взаимно-однозначное соответствие между элементами поля $\mathbb{F}_{p^m}$ и элементами векторного пространства $\mathbb{F}_p^m$. Для любых натуральных чисел ℓ и h положим $u = \ell + h$. Для поля Галуа $\mathbb{F}_{p^u}$ с элементами $\{f_0 = 0,\ f_1 = 1,\ f_2,\ \ldots,\ f_{p^u-1}\}$ обозначим через $F = [f_{i,j}]$ матрицу размера $p^u \times p^u$, строки и столбцы которой индексированы элементами поля $\mathbb{F}_{p^u}$, где $f_{i,j} = f_i f_j$, т.е. F – таблица умножения элементов $\mathbb{F}_{p^u}$. Определим оператор $\Phi = \Phi_{u\to\ell}$, отображающий элементы $x = (x_1, \ldots, x_u)$ поля $\mathbb{F}_p^u$ в элементы $x^{(\ell)} = (x_1, \ldots, x_\ell)$ поля $\mathbb{F}_p^\ell$ путем удаления правых $u - \ell$ координатных позиций векторов из $\mathbb{F}_p^u$:

$$\Phi_{u\to\ell}(x_1, \ldots, x_\ell, \ldots, x_u) = (x_1, \ldots, x_\ell).$$

Обозначим через $F^{[\ell]}$ матрицу, полученную из матрицы F действием оператора Φ на все элементы матрицы F:

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

Получаем теперь (см. [11], а также [12]), что имеет место следующая

Лемма 2. *Для любого простого числа p и любых натуральных чисел ℓ и h матрица $F^{[\ell]}$ представляет собой аддитивную разностную матрицу $D = D(p^\ell, p^h)$. Если ℓ делит h, т.е. $N = p^{h+\ell} = p^{\ell(h/\ell+1)}$, то $F^{[\ell]}$ является векторным пространством, откуда вытекает, что разностная матрица D линейна.*

Опишем построение $(n, N, \{d, n\})_q$-кода на основе разностной матрицы $D(q, \mu)$ над G. В рассматриваемом случае $G = \mathbb{F}_q$. Предположим, что первая строка D состоит из нулей. Обозначим через $D^{(g)}$ матрицу, полученную из D прибавлением элемента $g \in G$ ко всем элементам D, т.е. если $D = [d_{i,j}]$, то $D^{(g)} = [d_{i,j} + g]$ для всех i и j (напомним, что сложение осуществляется в G). По определению D матрица $D^{(g)}$ является разностной матрицей $D(q, \mu)$. Из определения следует также, что для любых двух строк $\boldsymbol{r}$ из D и $\boldsymbol{r}^{(g)}$ из $D^{(g)}$ выполняется следующее свойство [12]:

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

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

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

если знаменатель положителен. Чтобы убедится в этом, следует вначале представить D в нормализованной форме, при которой первый столбец состоит из нулей, а затем выкинуть этот тривиальный столбец. Из (1) вытекает следующий результат.

Лемма 3 [12]. *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*

$$n = q\mu, \quad N = q^2\mu, \quad d = \mu(q-1). \tag{3}$$

Назовем код C, основанный на разностной матрице D (как описано выше), *разностным матричным кодом*, или кратко *РМ-кодом*. Любой $(n, N, \{d, n\})_q$-код, параметры которого удовлетворяют (3), будем называть *псевдоразностным матричным кодом*, или кратко *ПРМ-кодом*. Ниже мы убедимся, что аддитивные ПРМ-коды представляют собой РМ-коды. Все эти коды оптимальны относительно q-ичного аналога верхней границы Грея – Рэнкина [13], которого они достигают с точным равенством. Любой q-ичный $(n, N, \{d, n\})_q$-код, который можно разбить на тривиальные $(n, q, n)_q$-подкоды (называемые *симплексами*), удовлетворяет этой границе [13]

$$\frac{N}{q} \leqslant \frac{q(qd - (q-2)n)(n-d)}{n - ((q-1)n - qd)^2} \tag{4}$$

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

Напомним также границу линейного программирования на мощность N кода C, в котором максимальное расстояние между кодовыми словами ограничено, скажем, величиной D (см. работы [14] для первого случая границы $D = n$ и [15] для общего случая). Для $D = n$ эта оценка выглядит следующим образом:

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

если знаменатель положителен. Заметим, что $(n, N, \{d, n\})_q$-ПРМ-код достигает этой границы с точным равенством.

Как мы уже упоминали, мы рассматриваем не только аддитивные коды, но также и те, которые не являются аддитивными. В частности, рассматриваются *дистанционно инвариантные* коды, т.е. такие, весовой спектр которых не зависит от выбора нулевого слова.

Напомним, что q-ичная $(N \times n)$-матрица M называется *ортогональной таблицей* силы t индекса $\lambda = N/q^t$ с n ограничениями и обозначается через $\mathrm{OA}(N, n, q, t)$, если каждая $(N \times t)$-подматрица содержит в качестве строк каждый q-ичный вектор длины t ровно λ раз [16].

Будем говорить, что $(n+1, N, d^*)_q$-код C^*, где $d^* \in \{d, d+1\}$, получен расширением $(n, N, d)_q$-кода C, если ко всем кодовым словам кода C добавлена координатная позиция общей проверки на четность, т.е.

$$C^* = \{(c_1, \ldots, c_n, c_{n+1}) : (c_1, \ldots, c_n) \in C\}, \quad \text{где} \quad c_{n+1} = \sum_{i=1}^{n+1} c_i.$$

Следующий результат хорошо известен; его можно найти, например, в [17]. Для заданного q и натурального m введем величину $n_m = (q^m - 1)/(q-1)$.

Лемма 4. *Пусть $\mathcal{H}_m$ – $[n_m, k, 3]_q$-код Хэмминга. Тогда расширенный код $\mathcal{H}_m^*$ имеет минимальное расстояние 4, если и только если*

(i) $q = 2$ *и* $m \geqslant 2$, *или*

(ii) $q = 2^r \geqslant 4$ *и* $m = 2$, *т.е.* $n_m + 1 = q + 2$ *и* $k = q - 1$.

Для произвольного $(n, N, d)_q$-кода C определим его *радиус покрытия* $\rho = \rho_C$ как наименьшее целое число, такое что все шары радиуса ρ, проведенные вокруг всех кодовых слов C (с центрами в этих словах), покрывают все пространство Q^n.

§ 3. Необходимые условия

Естественный вопрос о существовании q-ичного двухвесового $(n, N, \{d, d+\delta\})_q$-кода – это при каких условиях существует такой код? Здесь мы отвечаем на этот

вопрос для случая, когда $d+\delta=n$ и код удовлетворяет некоторым условиям регулярности. Нам потребуются некоторые известные факты о проективных двухвесовых кодах (см. работы [1, 7, 8] и библиографию в них). Пусть $\mathrm{PG}(n,q)$ обозначает n-мерное проективное пространство над полем $\mathbb{F}_q$. Тогда *m-дуга* точек в $\mathrm{PG}(n,q)$, где $m \geqslant n+1$ и $n \geqslant 2$, – это множество M, содержащее m точек, такое что никакие $n+1$ точек множества M не лежат в гиперплоскости пространства $\mathrm{PG}(n,q)$. Дуга, содержащая $(q+1)$ точек $\mathrm{PG}(2,q)$, называется *овалом*, а дуга из $(q+2)$ точек пространства $\mathrm{PG}(2,q)$ для четного q называется *полным овалом*, или *гиперовалом* (см., например, [18–20]).

Линейный код C называется *проективным*, если дуальный к нему код $C^\perp$ имеет минимальное расстояние $d^\perp \geqslant 3$ (т.е. любая порождающая матрица C не содержит двух столбцов, являющихся скалярными кратными друг друга). Для проективных $[n,k,d]_q$-кодов C можно ввести понятие *дополнительного* к нему кода C_c (см., например, [1, 7]). Пусть $[C]$ обозначает матрицу, образованную всеми кодовыми словами кода C (т.е. строками $[C]$ являются кодовые слова C). Код C_c называется дополнительным к коду C, если матрица $\big[[C]\,|\,[C_c]\big]$ является линейным эквидистантным кодом и C_c имеет минимально возможную длину, обеспечивающую это свойство. Для данного $[n,k,d]_q$-кода C с проверочной матрицей H дополнительный к нему $[n_{n-k}-n,k,d_c]$-код C_c имеет проверочную матрицу H_c, полученную из матрицы H_{n-k} удалением всех столбцов матрицы H и столбцов, кратных столбцам H. Напомним важное свойство дополнительного кода: *любому кодовому слову веса w в $[n,k,d]_q$-коде C соответствует кодовое слово веса $w_c=q^{k-1}-w$ в дополнительном к нему коде C_c.* Следствием этого простого факта является

Лемма 5 [7]. *Линейный $[n,k,d]_q$-код C с радиусом покрытия $\rho=2$, не дуальный РМ-коду, существует одновременно с дуальным к нему проективным кодом C_c с тем же самым радиусом покрытия $\rho_c=2$.*

Обобщение этих хорошо известных фактов на произвольные линейные двухвесовые $[n,k,\{d,d+\delta\}]_q$-коды было получено в [5, 6]. Здесь мы приводим вариант этого результата на случай $[n,k,\{d,n\}]_q$-кодов. Для любого кода C с проверочной матрицей H обозначим через s максимальное число появлений любого столбца H с учетом кратных к нему столбцов, т.е. полученных из него умножением на ненулевой элемент поля $\mathbb{F}_q$.

Лемма 6 [5, 6]. *Пусть C – q-ичный линейный нетривиальный двухвесовой $[n,k,\{d,n\}]_q$-код, не дуальный s раз повторенному РМ-коду, и пусть μ_1 и μ_2 обозначают число кодовых слов веса d и n соответственно. Тогда существует дополнительный к нему линейный двухвесовой $[n_c,k,\{d_c,d_c+\delta\}]_q$-код C_c, такой что*

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

причем C_c содержит μ_1 кодовых слов веса $d_c+\delta$ и μ_2 кодовых слов веса d_c, и C_c имеет минимально возможную длину n_c, такую что 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 является максимальным числом столбцов в порождающей матрице C, которые являются скалярными кратными одного столбца. Для проективных двухвесовых $[n,k,\{d,n\}]_q$-кодов (т.е. для случая $s=1$) известны следующие результаты.

Лемма 7 [8]. *Пусть C – проективный двухвесовой $[n,k,\{w,n\}]_q$-код над $\mathbb{F}_q$, где $q=p^m$ и p простое. Тогда существуют два целых числа $u\geqslant 0$ и $h\geqslant 1$, такие что*

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

Напомним для проективного случая следующий результат (который прямо вытекает из тождеств Мак-Вильямс, если принять во внимание, что дуальный код $C^\perp$ имеет минимальное расстояние $d^\perp \geqslant 3$) (см. [8]).

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

$$\begin{cases} w\mu_1 + n\mu_2 = n(q-1)q^{k-1}, \\ w^2\mu_1 + n^2\mu_2 = n(q-1)(n(q-1)+1)q^{k-2}. \end{cases} \tag{6}$$

В [5, 6] (см. также [4] для специального случая $n - d = 1$) нами были получены условия целочисленности, аналогичные условиям, полученным Дельсартом в [8] (см. также [1]), для проективных двухвесовых кодов на основе простых комбинаторных аргументов, не связанных с собственными значениями сильно регулярных графов. Для случая произвольных двухвесовых $(n, N, \{d, n\})_q$-кодов с расстояниями d и n эти условия сводятся к следующему. Как и в работах [8] и [1], мы рассматриваем здесь только двухвесовые $(n, N, \{d, n\})_q$-коды мощности $N \geqslant q^2$. Имеются тривиальные и нетривиальные примеры таких кодов с $N \leqslant q^2$, которые мы упомянем ниже. Мы считаем такие коды неинтересными, так как их мощность не всегда оптимальна, т.е. не достигает верхних границ. Напомним, что под тривиальными кодами мы понимаем также такие двухвесовые коды, которые можно представить в виде прямой суммы (или повторения) двух или более $(n_i, N, \{d_i, n_i\})_q$-кодов.

Теорема 1. *Пусть Q – алфавит любого размера q, и пусть C – произвольный нетривиальный q-ичный двухвесовой $(n, N, \{d, n\})_q$-код, где $N \geqslant q^2$. Тогда*

(i) *Мощность N кода C лежит в следующих пределах*:

$$(q-1)n + 1 \leqslant N \leqslant \frac{q^2 d}{qd - (q-1)(n-1)} \tag{7}$$

при условии, что $qd - (q-1)(n-1) > 0$;

(ii) *Правое неравенство в (7) становится равенством, если и только если матрица $[C]$, образованная всеми кодовыми словами кода C, является ортогональной таблицей силы $t \geqslant 2$;*

(iii) *Если правое неравенство в (7) является равенством, то длина n и расстояние d кода C имеют следующий вид*:

$$n = \frac{N(q(d+1)-1) - q^2 d}{N(q-1)} \tag{8}$$

и

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

(iv) *Левое неравенство в (7) становится равенством, если и только если C – эквидистантный $(n, N, d)_q$-код;*

(v) *Если правое неравенство в (7) является равенством, то число N делит $q^2 d$, а число $q - 1$ делит $(N - 1)d$.*

Доказательство. (i) Для случая, когда C – произвольный q-ичный двухвесовой $(n, N, \{d, n\})_q$-код, это утверждение следует непосредственно из границы линейного программирования для этих кодов, которую мы приводим в п. 5.1. Для случая, когда C – ортогональная таблица силы $t \geqslant 2$, этот результат получается из аргументов, аналогичных тем, которые мы использовали в [6]. Здесь мы приведем простое доказательство для общего случая, когда C – произвольный дистанционно

инвариантный $(n, N, \{d, n\})_q$-код мощности $N \geqslant q^2$; приводимые здесь аргументы понадобятся нам в дальнейшем.

Предположим, что C содержит нулевое кодовое слово и μ кодовых слов веса d. Пусть код C^* состоит только из кодовых слов веса d, и пусть $[C^*]$ – матрица размера $\mu \times n$, строками которой являются слова кода C^*.

Сначала подсчитаем полное число нулей (которое мы обозначим Σ_0) в матрице $[C^*]$ двумя разными (очевидными) способами. Действительно, по определению

$$\Sigma_0 = \mu(n-d) = (N/q-1)n.$$

Далее, так как C дистанционно инвариантен, и следовательно, каждый столбец содержит одно и то же число нулей, а именно $N/q = \mu(n-d)/n + 1$, то получаем, что

$$\mu = \frac{n(N-q)}{q(n-d)}. \tag{10}$$

Затем найдем полное число $\Sigma_{(0,0)}$ пар координатных позиций, содержащих нулевые элементы $(0,0)$, которые встречаются во всех $n(n-1)/2$ позициях всех строк матрицы $[C^*]$. Обозначим через $s(i,j)$ число таких нулевых пар $(0,0)$, встречающихся в столбцах с номерами i и j матрицы $[C^*]$. Получаем очевидным образом

$$\left(\frac{N}{q^2} - 1\right) n(n-1) \leqslant \Sigma_{(0,0)} = \sum_{1 \leqslant i < j = n} s(i,j) = \mu(n-d)(n-d-1). \tag{11}$$

Подставляя выражение для μ из (10) в формулу (11), получаем следующее неравенство:

$$N\,(qd - (q-1)(n-1)) \leqslant q^2 d. \tag{12}$$

Отсюда получаем правое неравенство в (7), так как выполняется условие

$$qd - (q-1)(n-1) > 0.$$

Рассмотрим теперь левое неравенство в (7). Правое неравенство в (7) (которое имеет место для произвольного двухвесового $(n, N, \{d, n\})_q$-кода) влечет следующую верхнюю оценку на величину d:

$$d \leqslant (n-1)\frac{N(q-1)}{q(N-q)}.$$

Но величина d для $(n, N, \{d, n\})_q$-кода не может быть больше величины (обозначим ее через $d^{(p)}$), гарантируемой верхней границей Плоткина (2), которая точна для эквидистантного кода (действительно, средняя оценка по всем расстояниям всегда больше минимального расстояния кода с несколькими расстояниями). Поэтому из неравенства

$$d \leqslant (n-1)\frac{N(q-1)}{q(N-q)} \leqslant d^{(p)} = n\frac{(q-1)N}{q(N-1)}$$

получаем, что

$$(n-1)(N-1) \leqslant n(N-q),$$

откуда вытекает левое неравенство для N в формуле (7).

(ii) Правое неравенство в (7) становится равенством, если и только если выражение (11) является равенством. Это имеет место, когда код C удовлетворяет

следующему условию: *величина* $s_0(i,j) = s(i,j)$ *постоянна для любых выбранных позиций кода с номерами* i *и* j. Мы утверждаем, что это возможно только тогда, когда матрица $[C]$ является ортогональной таблицей силы $t \geqslant 2$. Предположим противное – пусть для некоторого элемента $a \in Q$ величина $s_a(i,j)$ не одна и та же для всех i и j. Тогда определим новый код $C^{(a)}$, полученный из C перестановкой элементов алфавита 0 и a во всех кодовых словах C. Производя для него такие же вычисления, мы придем к противоречию. Так как величина $s_a(i,j)$ не постоянна в выражении (7), мы получим строгое неравенство, противоречащее условию утверждения. Итак, заключаем, что матрица $[C]$ должна быть ортогональной таблицей. Но если $[C]$ – ортогональная таблица, то тогда $s_0(i,j) = s(i,j)$ является постоянной величиной для всех i j, выражение (11) представляет собой равенство, и следовательно, правое неравенство в (7) является равенством.

(iii) Если правая часть (7) является равенством, то это означает, что неравенство (11) также является равенством, что можно переписать в следующем виде:

$$(N - q^2)n(n-1) = qn(N-q)(n-d-1). \tag{13}$$

Поэтому можно выписать выражение для n как функции от q, d и N, получая таким образом (8), и выражение для d как функции от q, n и N, получая (9).

(iv) Условие $N = (q-1)n+1$ относится к случаю эквидистантных кодов, подробно рассмотренному в [21] (в этом случае матрица $[C]$ также является ортогональной таблицей силы $t = 2$).

(v) Так как n – натуральное число, мы заключаем из (13), что число d должно быть кратным N/q^2. Из этого же равенства, учитывая, что

$$N(q(d+1)-1) - q^2 d = (q-1)\left(N(d+1) - d(q+1)\right) + d(N-1),$$

мы заключаем, что $d(N-1)$ кратно $q-1$. ▲

Следующий результат показывает, что существование аддитивного двухвесового $(n, N, \{d, n\})_q$-кода C над алфавитом Q, представляющим собой абелеву группу, накладывает очень сильное условие на эту группу. Порядок группы q, а также структура группы Q совсем не произвольны. Напомним, что для заданной аддитивно абелевой группы Q порядком элемента x, обозначаемым через $\mathrm{ord}(x)$, называется минимальное число t, такое что $tx = \underbrace{x + x + \ldots + x}_{t \text{ раз}} = 0$.

Имеет место следующая

Теорема 2. *Пусть* Q *– абелева группа порядка* q*, и пусть* C *– аддитивный нетривиальный* q*-ичный двухвесовой* $(n, N, \{d, n\})_q$*-код* C *над алфавитом* Q*, содержащий нулевое кодовое слово. Тогда*

(i) *Все элементы* Q *имеют один и тот же порядок, т.е.* $\mathrm{ord}(x) = \mathrm{ord}(y)$*, для любой пары ненулевых элементов* $x, y \in Q^*$;

(ii) *Группа* Q *является прямой суммой* m *циклических групп* $\mathbb{Z}_p$*, так что*

$$Q = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p;$$

(iii) *Число* q *имеет вид* $q = p^m$*, где* p *– простое число, а* m *– натуральное*;

(iv) *Код* C *содержит не менее чем* $q-1$ *слов веса* n.

Доказательство. Очевидно, что любая перестановка π элементов Q, такая что $\pi(0) = 0$, примененная к любой позиции кода C, сохраняет свойство кода оставаться двухвесовым $(n, N, \{d, n\})_q$-кодом с нулевым кодовым словом. Обозначим через π перестановку, которая не меняет свойство кода C быть аддитивным, так что

$$x - y = \pi(x) - \pi(y) = \pi(x - y).$$

(i) Для заданной пары элементов алфавита $x, y \in Q^* = Q \setminus \{0\}$ и кодового слова $c = (x_1, x_2, \ldots, x_n) \in C$ веса n выберем некоторые перестановки $\pi_1, \ldots, \pi_n$ элементов Q с условием $\pi_i(0) = 0$ и такие, что при их применении ко всем координатным позициям кодового слова c мы получим слово $c' = (x, y, \ldots, y)$ аддитивного кода (действительно, применение таких перестановок π_i ко всем координатам не меняет свойство кода быть аддитивным). Предположим, что $t = \mathrm{ord}(x) \neq \mathrm{ord}(y)$. Тогда t-кратная сумма c' с самим собой $c'+\ldots+c'$ будет равна кодовому слову $(0, ty, \ldots, ty)$, вес которого равен $n-1$, так как по предположению $ty \neq 0$. Тем самым, приходим к противоречию, и поэтому все ненулевые элементы алфавита имеют один и тот же порядок.

(ii) Этот факт прямо следует из (i). Действительно, хорошо известно, что любая абелева группа представляет собой прямую сумму (прямое произведение) циклических групп. С другой стороны, любая циклическая группа $\mathbb{Z}_{p_1 p_2}$ имеет элементы порядка p_1, p_2 и $p_1 p_2$, что противоречит (i) и доказывает утверждение.

(iii) Из (ii) следует, что все p_i равны, откуда получаем утверждение.

(iv) Так как код аддитивен, мы заключаем, что $N \geqslant qn$. Зафиксируем координатную позицию, скажем, первую. Разобьем все кодовые слова на смежные классы согласно элементам, стоящим на первой позиции. Каждый смежный класс является эквидистантным кодом, мощность которого не менее n [21] (откуда следует вышеприведенное неравенство). Так как код является группой, то ясно, что мы можем сдвинуть смежный класс с нулем на первой позиции в любой другой смежный класс. Отсюда следует также, что каждый элемент алфавита встречается в столбце одно и то же число раз.

Пусть μ_1 обозначает число слов кода C веса d, а μ_2 – число слов веса n. Рассмотрим сначала случай $N = qn$. Положим $\mu = n - d$. Тогда можно подсчитать общее число ненулевых позиций в коде C. Имеем следующие два выражения:

$$\begin{cases} \mu_1 + \mu_2 = N - 1, \\ d\mu_1 + n\mu_2 = nN\Big(1 - \dfrac{1}{q}\Big). \end{cases} \tag{14}$$

Выражение для μ_1 из первого уравнения подставим во второе, и учитывая, что $N = nq$, приведем его к виду

$$d(N - 1 - \mu_2) + n\mu_2 = nN\left(1 - \frac{1}{q}\right) = n^2(q-1).$$

Учитывая, что $\mu = n - d$, получаем

$$d(qn - 1 - \mu_2) + n\mu_2 = d(qn-1) + (n-d)\mu_2 = (n-\mu)(qn-1) + \mu\mu_2 = n^2(q-1).$$

Таким образом, приходим к уравнению

$$\mu\mu_2 = n(q\mu - n) + n - \mu. \tag{15}$$

Так как обе его части – положительные целые числа, заключаем, что $q\mu - n \geqslant 0$. Поэтому можно положить

$$q\mu = n + \lambda,$$

где $\lambda \geqslant 0$ – целое число. Уравнение (15) можно переписать в следующем виде (где μ перенесено в левую сторону):

$$\begin{cases} q\mu = n + \lambda, \\ \mu(\mu_2 + 1) = (\lambda + 1)n. \end{cases} \tag{16}$$

Так как $(\lambda+1)n \geqslant n+\lambda$, то отсюда вытекает, что

$$\mu(\mu_2+1) \geqslant q\mu,$$

или, эквивалентным образом, $\mu_2+1 \geqslant q$. Следовательно, мы получаем, что $\mu_2 \geqslant q-1$. Для случая $N > qn$ доказательство не изменяется. ▲

В следующем утверждении мы сформулируем вариант теоремы 2 из [6] для случая нетривиальных $[n,k,\{d,n\}]_q$-кодов, и поэтому это утверждение не нуждается в доказательстве. Здесь мы предположим, что $q=p^m$, где $m \geqslant 1$ и p – простое. Для заданного $q=p^m$ и произвольного натурального числа a обозначим через $\gamma_a \geqslant 0$ максимальное целое число, такое что p^{γ_a} делит a, т.е. $a=p^{\gamma_a}h$, где h и p взаимно просты. Пусть числа γ_d, γ_δ и γ_c определены аналогичным образом для d, δ и d_c соответственно. Напомним, что через (a,b) обозначается наибольший общий делитель целых чисел a и b.

Теорема 3. *Пусть $q=p^m$, где $m \geqslant 1$ и p – простое число. Пусть C – q-ичный линейный (двухвесовой) $[n,k,\{d,n\}]_q$-код размерности $k \geqslant 2$, и пусть C_c – дополнительный к нему двухвесовой $[n_c,k,\{d_c,d_c+\delta\}]_q$-код C_c, 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 и, следовательно, C_c – проективные коды, то справедливы следующие два равенства*:

$$(q,d)=(q,\delta) \quad и \quad (q,d_c)=(q,\delta); \tag{17}$$

(ii) *Если $s=1$ и $k=3$, то оба равенства в (17) имеют место, если справедливо одно из следующих 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 выполняется по крайней мере одно из следующих двух равенств*:

$$\gamma_d=\gamma_\delta \quad или \quad \gamma_c=\gamma_\delta; \tag{18}$$

(iv) *Если $s \geqslant 1$ и $k \geqslant 3$, то выполняется по крайней мере одно из двух равенств в (18) (соответственно, в (17)).*

§ 4. Известные $(n, N, \{d, n\})_q$-коды

Здесь мы перечислим все известные нетривиальные аддитивные $(n,N,\{d,n\})_q$-коды. Большинство этих двухвесовых кодов можно найти в подробном обзоре таких кодов в [1].

Мы начнем с формулировки утверждения, которое является перефразировкой соответствующего результата из [10], где были приведены все известные полностью регулярные линейные коды с радиусом покрытия 2, для которых дуальные коды антиподальны (т.е. содержат слова веса n). В работе [10] эта теорема была приведена и доказана для случая линейных кодов. Здесь мы сформулируем аналогичный результат для произвольных аддитивных кодов.

Теорема 4. *Пусть C – нетривиальный аддитивный $(n,N,\{d,n\})_q$-код мощности $N \geqslant q^2$ над Q. Код C можно привести эквивалентными преобразованиями к коду C^* так, чтобы имели место следующие условия*:

(i) *Для каждого ненулевого кодового слова $\boldsymbol{v} \in C^*$ веса d каждый элемент $a \in Q$, который встречается в координатной позиции этого слова $\boldsymbol{v}$, встречается в этом слове ровно $n-d$ раз*;

(ii) *Каждое ненулевое кодовое слово* $\boldsymbol{v} \in C^*$ *веса* n *либо удовлетворяет свойству* (i), *либо имеет вид* $\boldsymbol{v} = (a, a, \ldots, a)$, *где* $a \in Q$;

(iii) *Длина* n *кода* C^* (*а значит, и кода* C) *кратна* $n - d$.

Напомним, что в § 2, следуя [13], мы назвали тривиальный $(n, q, n)_q$-код *симплексом*. Напомним также, что q-ичный дистанционно инвариантный код длины n является *симплексным кодом*, если он содержит в качестве подкода симплекс, т.е. $(n, q, n)_q$-код. Ясно, что аддитивный $(n, N, \{d, n\})_q$-код, содержащий симплекс, представляет собой дистанционно инвариантный симплексный код. Следующий результат можно найти в [13].

Предложение 1. *Пусть* q*-ичный код* C *длины* n *с минимальным расстоянием* $d = \dfrac{(q-1)n}{q}$ *имеет мощность* $N = qn$. *Тогда этот код* C *можно представить в виде объединения непересекающихся симплексов.*

Возникает естественный вопрос: *при каких условиях симплексный код, указанный в предложении* 1, *является ПРМ- или РМ-кодом*? Следующее утверждение дает частичный ответ на этот вопрос.

Теорема 5. *Пусть* C – *дистанционно инвариантный симплексный код с параметрами* $(n, N, \{d, n\})_q$. *Тогда*

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

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

где C_i *для каждого* i *является симплексом, а мощность* N *кратна* q;

(ii) *Для любого кодового слова* $\boldsymbol{c} \in C$, *отличного от слов вида* $(a, a, \ldots, a)$, $a \in Q$, *каждый символ* $\alpha \in Q$, *который встречается на координатной позиции слова* $\boldsymbol{c}$, *встречается на этой позиции ровно* μ *раз, где* $\mu = n - d$, a n *кратно числу* μ;

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

$$d \leqslant n\frac{q-1}{q}; \tag{19}$$

(iv) *Если* (19) *обращается в равенство и* $N = qn$, *то код* C *представляет собой ПРМ-код с параметрами*

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

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

Доказательство. (i) Так как C содержит в качестве подкода симплекс, содержащий нулевое кодовое слово $\mathbf{0}$, то можно выбрать $q-1$ кодовых слов веса n вида $\boldsymbol{a} = (a, a, \ldots, a)$, где $a \in \{1, \ldots, q-1\}$, которые имеются в C. В противном случае можно получить такие слова из кодовых слов веса n с помощью перестановок элементов алфавита. Так как C дистанционно инвариантен, это справедливо для любого выбора нулевого кодового слова. Для любого такого выбора мы получаем в качестве подкода некоторый симплекс, содержащий $q-1$ кодовых слов веса n. Таким способом мы получаем разбиение кода C на подкоды, каждый из которых представляет собой симплекс. Ясно, что каждое кодовое слово кода C будет принадлежать некоторому симплексу. Осталось показать, что никакие два разных симплекса не могут иметь одно и то же кодовое слово. В самом деле, один из таких симплексов мы можем сдвинуть в симплекс, содержащий кодовые слова вида $\boldsymbol{a} = (a, a, \ldots, a)$. Ни одно из его слов не может принадлежать другому симплексу, так как все кодовые слова из других симплексов находятся на расстоянии d от этого симплекса.

Мы заключаем, что C можно разбить на непересекающиеся подкоды мощности q, и следовательно, мощность N должна быть кратна q.

(ii) Обозначим через C_0 симплекс, который содержит нулевое кодовое слово и остальные $q-1$ кодовых слов вида $\boldsymbol{a} = (a, a, \ldots, a)$. Рассмотрим любое кодовое слово $\boldsymbol{c}$, не принадлежащее симплексу C_0. Ясно, что каждый элемент a, встречающийся на координатной позиции слова $\boldsymbol{c}$, должен встречаться (для того чтобы расстояние было в точности d от q слов симплекса C_0) ровно $n-d$ раз. Отсюда следует, во-первых, что каждый элемент, который встречается на позициях $\boldsymbol{c}$, должен встречаться ровно $\mu = n-d$ раз, а во-вторых, что число n должно быть кратным $n-d$.

(iii) Так как на позициях любого кодового слова $\boldsymbol{c}$, не принадлежащего C_0, имеются q различных элементов, то должно выполняться следующее очевидное неравенство: $n \leqslant q(n-d)$. Отсюда вытекает неравенство (19).

(iv) Равенство в (19) означает, что n можно представить в виде $n = q\mu$, где $\mu = n-d$, и следовательно, $d = \mu(q-1)$. Для этих значений n и d мы заключаем из оценки (4), что $N \leqslant q^2\mu$. Если $N = qn$, то $N = q^2\mu$, и согласно [13] код C представляет собой ПРМ-код, что дает (iv).

(v) Из (iv) мы получили, что C является ПРМ-кодом. Покажем теперь, что аддитивный ПРМ-код является РМ-кодом. Так как C аддитивен, то сумма любых двух строк, скажем, $\boldsymbol{r}_1$ и $\boldsymbol{r}_2$, принадлежит C и содержит на координатных позициях каждый элемент алфавита μ раз (теорема 4). Из кода C строим матрицу D размера $q\mu \times q\mu$, содержащую все кодовые слова с нулем на первой позиции, где $\mu = n-d$. Ясно, что это справедливо, так как C – аддитивный код.

Итак каждая строка D содержит любой элемент Q ровно μ раз (теорема 4), и для любых двух строк $\boldsymbol{c}_1$ и $\boldsymbol{c}_2$ кода D покомпонентная разность этих строк $\boldsymbol{c}_1 - \boldsymbol{c}_2$ также принадлежит (по определению слова D имеют 0 в первой позиции) коду D. Любое кодовое слово $\boldsymbol{c} \in C$ с первой ненулевой позицией $a \in Q$ получено из D сложением с вектором $(a, a, \ldots, a)$, который принадлежит C, так как C – симплексный код по условию. Мы заключаем, что D – разностная матрица $D(q, n-d)$, а C – $(n, qn, \{d, n\})_q$-РМ-код. ▲

Замечание 1. Условия $n = q(n-d)$ и $N = qn$ в (iv) и (v) опустить нельзя, как показывает следующий пример. Рассмотрим матрицу $[C] = [D^{(0)} \mid \ldots \mid D^{(q-1)}]^t$, образованную сдвигами $D^{(i)}$ разностной матрицы $D = D(q, \mu)$, где C – $(n, N, \{d, n\})_q$-РМ-код. Если мы удалим одну или несколько таких матриц $D^{(i)}$ из матрицы $[C]$, то получим дистанционно инвариантный симплексный код некоторой мощности $N^* < qn$, т.е. нелинейный двухвесовой $(n, N^*, \{d, n\})_q$-код, удовлетворяющий условию теоремы. Аналогично нельзя опустить условие $N = qn$ в (iv) и (v). Например, линейный код Боуза – Буша имеет длину (см. ниже) $n < q(n-d)$. Аналогично, аддитивный $(n, N, \{d, n\})_q$-код не обязательно должен иметь мощность q^k. Так, например, разностная матрица $D(4, 2)$ индуцирует оптимальный аддитивный $(8, 32, \{6, 8\})_4$-код мощности $N \neq 4^k$.

Замечание 2. Случай кодов мощности $N = q^2$ также очень специален. Хорошо известный результат гарантирует, что $r-2$ взаимно ортогональных латинских квадратов порядка q индуцирует $(r, q^2, \{r-1, r\})_q$-код. Для случая, когда q – степень простого числа, существуют $q-1$ взаимно ортогональных латинских квадратов, индуцирующих линейный эквидистантный $[q+1, 2, q]_q$-код (обратное утверждение также имеет место для любой длины $r \geqslant 2$ и также хорошо известно). Используя эти коды с соответствующими значениями r_i, можно построить с помощью прямой суммы (используя разбиения на симплексы) $(n, q^2, \{d, n\})_q$-код для любых натуральных $d = n-s$ и $n = r_1 + \ldots + r_s$, рассматривая прямую сумму s исходных $(r_i, q^2, \{r_i - 1, r_i\})_q$-кодов латинских квадратов. Поэтому мы исключили (как и в [1,8]) все эти тривиальные коды, за исключением $(r, q^2, \{r-1, r\})_q$-кодов длины $r \leqslant q$, которые индуцируются $r-2$ взаимно ортогональными латинскими квадратами по-

рядка q. Кроме того, имеются еще, конечно, $[q+2, 2, \{q+1, q+2\}]_q$-коды, полученные из эквидистантных $[q+1, 2, q]_q$-кодов добавлением одной позиции (см [4]).

Теперь мы можем привести все известные семейства нетривиальных аддитивных $(n, N, \{d, n\})_q$-кодов, которые были приведены в обзоре [1] (а также были указаны в [10] для линейного случая). Если исключить коды, образованные латинскими квадратами, то все известные $(n, N, \{d, n\})_q$-коды делятся на два больших класса кодов: разностно-матричные $(n = q\mu, N = qn, \{(q-1)\mu, q\mu\})_q$-коды, длина n которых кратна q, и $[n, k, \{d, n\}]_q$-коды Деннистона длины n, такой что $n-1$ кратно $(q^{k-1}-1)/(q-1)$.

Разностно-матричные коды (РМ-коды). Это $(q\mu, q^2\mu, \{(q-1)\mu, q\mu\})_q$-коды [12], индуцированные разностными матрицами. Лемма 1 описывает построение таких кодов для значений $q = p^h$ и $\mu = p^\ell$, где p – простое, а h и ℓ – произвольные натуральные числа.

Следует заметить, что эти коды включают в себя (двоичные) $(4m, 8m, \{2m, 4m\})$-*коды Адамара.* Действительно, двоичная (т.е. состоящая из элементов 0 и 1) матрица Адамара является разностной матрицей $D(2, 2m)$.

Коды Деннистона. Это $[n = 1+(q+1)(h-1), 3, \{q(h-1), n\}]_q$-коды, где $1 < h < q$ и h делит q, для $q = 2^r \geqslant 4$ (см. семейство TF2 в [1]). В теореме 1 этот случай соответствует расстоянию $d = n - h + 1 = (n-1)q/(q+1)$, из которого следует, что $N = q^3$. Для случая $h = 2$ мы получаем $[n = q+2, 3, \{q, n\}]_q$-коды Боуза – Буша (см. семейство TF1 в [1]), построенные в 1952 г. [11], которые индуцируются гиперовалами в $PG(3, q)$. Значению $h = q/2$ соответствуют $[n = q(q-1)/2, 3, \{q(q-2)/2, n\}]_q$-коды Дельсарта [7] (см. семейство $\mathrm{TF1}^d$ в [1]), построенные независимо в 1971 г., которые проективно дуальны кодам Боуза – Буша [1].

Коды Деннистона образованы максимальными дугами в проективных плоскостях [18] (см. также [19, 20]). Коротко объясним, как построить такие коды для произвольного $q = 2^m \geqslant 4$ и натурального $h \geqslant 2$, делящего q, т.е. $h = 2^u \leqslant q/2$. Для заданного $\mathbb{F}_q$ пусть H обозначает подгруппу порядка h аддитивной группы поля $\mathbb{F}_q$. Пусть $\varphi(x, y) = ax^2 + bxy + cy^2$ – неприводимая квадратичная форма над $\mathbb{F}_q$. Тогда $[n, 3, \{d, n\}]_q$-код Деннистона порождается следующей $(3 \times n)$-матрицей:

$$G_d = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{bmatrix}, \tag{20}$$

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

Приведем также порождающие матрицы для кодов Боуза – Буша, а также кодов Дельсарта, так как они приводятся в явном виде. Пусть матрица G имеет вид

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 0 & x_0 & x_1 & \dots & x_i & \dots & x_{q-2} \\ 0 & 0 & 1 & y_0 & y_1 & \dots & y_i & \dots & y_{q-2} \end{bmatrix}, \tag{21}$$

где x_i и y_i пробегают все ненулевые элементы поля $\mathbb{F}_q$. Тогда, если $y_i = x_i^2$, то матрица G порождает код Боуза – Буша. Если же x_i и y_i пробегают все упорядоченные пары ненулевых элементов (x_i, y_i) (число таких различных пар равно, очевидно, $(q-1) \times q/2$, т.е. длине кодов Дельсарта), такие что $\mathrm{Tr}(x_i y_i) = 1$, где $\mathrm{Tr}(x)$ – функция следа из $\mathbb{F}_q$ в поле $\mathbb{F}_2$, т.е.

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

то матрица G порождает код Дельсарта.

Теорема 6. *Пусть C – аддитивный нетривиальный $(n, N, \{d, n\})_q$-код, где $q = p^m$, p – произвольное простое число и $m = 1, 2, \ldots$ Предположим, что $N \geqslant q^2$ и $n > 2$. Тогда параметры этого кода совпадают с параметрами кода, принадлежащего одному из семейств указанных выше кодов.*

Доказательство. Так как C – нетривиальный аддитивный код, то он имеет мощность $N = q^2\mu \geqslant q^2$.

Начнем со случая $N = q^2$. Для любого натурального q существование r попарно ортогональных латинских квадратов влечет существование $(r+2, q^2, \{r+1, r+2\})_q$-МДР-кода (см. также замечание 2). Эти коды включают в себя самые короткие нетривиальные $(q, q^2, \{q-1, q\})_q$-РМ-коды, которые существуют для любой степени простого числа q и совпадают с кодами по латинским квадратам. Еще раз подчеркнем, что существует большое количество тривиальных аддитивных двухвесовых $(n, q^2, \{d, n\})_q$-кодов, указанных в замечаниях выше, которые мы не рассматриваем. Напомним также, что так как C аддитивен, то все ПРМ-коды согласно теореме 5 являются РМ-кодами.

Теперь докажем, что для случая $N = q^2\mu$, где $2 \leqslant \mu < q$, нетривиальный аддитивный $(n, N, \{d, n\})_q$-код C есть не что иное, как $(q\mu, q^2\mu, \{(q-1)\mu, n\})_q$-код ПРМ или РМ. Следующий аргумент использовался в [13] (см. также [21]), где были введены q новых кодов C_j, $j = \{0, 1, \ldots, q-1\}$, полученных из C выбором всех кодовых слов кода C, имеющих элемент j на первой позиции, и затем удалением этой первой позиции. Легко видеть [13], что каждый код C_j имеет только одно расстояние, а именно d. Следовательно, C_j – эквидистантный $(n_0, N_0, d_0)_q = (n-1, q\mu, d)_q$-код мощности $N_0 = q\mu$. Более того, параметры этого кода достигают верхней границы Плоткина (2) с точным целочисленным равенством, и следовательно, каждый символ i алфавита $\{0, 1, \ldots, q-1\}$ встречается одно и то же число раз (а именно μ) в каждой позиции всех кодовых слов кода C_j (см. [21]). Теперь применим теорему 4, которая утверждает, что каждое кодовое слово $\boldsymbol{c}$ кода C_j содержит все элементы $i \neq j$ алфавита как координатные элементы ровно μ раз, а элемент j – ровно $\mu - 1$ раз.

Так как C – аддитивный код, то его подкод C_0 также является аддитивным кодом, удовлетворяющим следующему свойству: каждое ненулевое слово кода C_0 содержит каждый ненулевой элемент алфавита ровно μ раз. Мы заключаем, следовательно, что по теореме 5 код C_0 станет разностной матрицей, если мы добавим ко всем словам кода C_0 нулевые позиции. Из свойства аддитивности вытекает, что любой подкод C_j представляет собой сдвиг кода C_0. Таким образом, C является РМ-кодом.

Рассмотрим теперь случай $N = q^3$. Сначала покажем, что в кодах Деннистона число h должно делить q. Из теоремы 5 заключаем, что n кратно $n-d$. Следовательно, n можно представить в виде $n = (n-d)\ell$ для некоторого натурального числа ℓ. Поэтому $d = n(\ell-1)/\ell$, и мы получаем из (19), что

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

откуда следует, что $\ell \leqslant q$. Но случай $\ell = q$ дает РМ-код. Мы заключаем, следовательно, что $\ell < q$. Предположим теперь, что

$$n = 1 + (q+1)(h-1) \quad \text{и} \quad d = q(h-1)$$

для некоторого натурального числа $h \geqslant 2$. Это означает, что

$$n = q(h-1) + h = d + h.$$

Таким образом, объединяя равенства

$$n = 1 + (q+1)(h-1) \quad \text{и} \quad d = q(h-1) = n\frac{\ell-1}{\ell},$$

получаем

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

откуда вытекает, что $h(\ell-1) = q(h-1)$. Так как $h \geqslant 2$, и следовательно, h и $h-1$ взаимно просты, мы заключаем, что h делит q, откуда следует, что получается код с параметрами кода Деннистона.

Случай $N > q^3$ исключается из аналогичных аргументов. Сначала рассматривается случай $N = q^3\mu$, где $2 \leqslant \mu < q$. Напомним, что $q = p^m$. Мы утверждаем, что в этом случае могут получиться только РМ-коды. Действительно, для всех значений $\mu = p^r$, где $0 < r < m$, существует $(q^2\mu, q^3\mu, \{q(q-1)\mu, n\})_q$-РМ-код. В § 2 мы описали построение всех таких кодов (см. текст после леммы 1), которое можно найти в [12]. Убедимся, почему это единственно возможные случаи. Деля обе стороны выражения (8) на $q^3\mu$, мы получим, что $d = n(q-1)/q$, поэтому это должна быть разностная матрица. Следовательно, для случая, когда $d \neq n(q-1)/q$, который (для случая $q^3\mu$) эквивалентен условию $d = q(q-1)\mu$, мы не получим целочисленное равенство в (8). Так как повторение s копий РМ-кода не меняет равенства $d = n(q-1)/q$, заключаем, что вышеуказанный нетривиальный РМ-код является единственным нетривиальным кодом для этих значений N.

Рассмотрим теперь случай $N = q^4$, который дает линейные разностно-матричные коды [12]. В самом деле, имея такой $[n, 4, \{d, n\}]_q$-код C, можно построить (как мы делали это раньше, например, в теореме 5) код C_0, представляющий собой линейный эквидистантный $[n-1, 3, d]_q$-код длины $n-1 = (q^4-1)/(q-1)$ с расстоянием $d = q^3$, дуальным к которому является q-ичный совершенный код Хэмминга.

Покажем теперь, что для случая $N = q^4$ не существует кодов типа Деннистона. По теореме 4 длина кода типа Деннистона должна иметь вид $n = s(q^3-1)/(q-1)+1$. Так как n кратно $n-d$ (см. снова теорему 4), то это выражение принимает вид $n = d\ell/(\ell-1)$ для некоторого натурального $\ell \leqslant q$. Учитывая, что $d = sq^2$, получаем

$$n = s\frac{q^3-1}{q-1} + 1 = d\frac{\ell}{\ell-1} = sq^2\frac{\ell}{\ell-1}. \tag{22}$$

Теперь следует рассмотреть отдельно случаи $(s, q-1) = 1$ и $(s, q-1) \geqslant 2$.

Пусть вначале $(s, q-1) = 1$. Тогда мы видим, что выражение для n в левой части (22) не делится на s и на q, а в правой части оно делится на оба эти числа. Мы заключаем, следовательно, что коды такого типа не существуют.

Рассмотрим теперь случай $(s, q-1) \geqslant 2$. Для случая $s = q-1$ получаем, что $n = q^3$, и так как $N = q^4$, т.е. $N = qn$, то заключаем, что C является РМ-кодом.

Предположим теперь, что $s = u(q-1)$, где $u \geqslant 2$. Используя это s в (22), приходим к равенству

$$u(q-1)\frac{q^3-1}{q-1} + 1 = u(q-1)q^2\frac{\ell}{\ell-1},$$

которое после упрощения и умножения обеих сторон на $(\ell-1)$ принимает следующий вид:

$$(\ell-1)(u(q^3-1)+1) = \ell u(q^3-q^2).$$

Упрощая, приходим к неравенству

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

что невозможно, так как $2 \leqslant \ell \leqslant q$ и $u \geqslant 2$, что завершает рассмотрение случая $N = q^4$.

Случай $q^4 < N < q^5$ рассматривается аналогично. Здесь мы имеем только аддитивные РМ-коды для значений $n = q^4\mu$, где μ пробегает все степени p и $q = p^m$.

Случай $N = q^k$ для $k \geqslant 5$ можно рассмотреть аналогичным образом, и мы его опускаем, чтобы не повторять одни и те же рассуждения.

Теперь следует сделать несколько замечаний для случая, когда q – степень простого нечетного числа. Буш в 1952 г. доказал в [22] несуществование $[q+2, 3, q]_q$-кодов для нечетного q, что влечет несуществование $[q(q-1)/2, 3, \{q(q-2)/2, q(q-1)/2\}]_q$-кодов Дельсарта, так как они проективно дуальны друг другу (см. семейства TF1 и $\mathrm{TF1}^d$ в [1]). Затем в 1997 г. в [23] было доказано несуществование максимальных дуг (на которых основаны коды Деннистона) в дезарговых плоскостях $PG(2, q)$ нечетного порядка, что автоматически влечет несуществование всех кодов Деннистона для нечетных q. ▲

§ 5. Верхние границы

Здесь мы рассмотрим верхние границы для величины

$$A_q(n; \{d, n\}) = \max\{N : \exists\, (n, N, \{d, n\})\text{-код}\},$$

т.е. границы на максимально возможную мощность кода в Q_q^n с двумя расстояниями d и n.

5.1. Границы линейного программирования. Мы провели всестороннее исследование границы линейного программирования (ЛП) Дельсарта на $A_q(n; \{d, n\})$, используя эту границу в следующем виде. Определим многочлены Кравчука

$$Q_i^{(n,q)}(t) = \frac{1}{r_i} K_i^{(n,q)}(z), \quad z = \frac{n(1-t)}{2}, \quad r_i = (q-1)^i \binom{n}{i},$$

где

$$K_i^{(n,q)}(z) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{z}{j} \binom{n-z}{i-j}$$

представляют собой (обычные) многочлены Кравчука. Для вещественного многочлена $f(t)$ степени не выше n рассмотрим его разложение

$$f(t) = \sum_{i=0}^{n} f_i Q_i^{(n,q)}(t) \tag{23}$$

по многочленам Кравчука.

Теорема 7. *Пусть $n \geqslant q \geqslant 2$, и пусть $f(t) \in \mathbb{R}[t]$ – многочлен степени не выше n, такой что*:

(A1) $f(-1) \leqslant 0$ *и* $f(1 - 2d/n) \leqslant 0$;

(A2) *Коэффициенты в разложении* (23) *удовлетворяют условиям* $f_0 > 0$ *и* $f_i \geqslant 0$ *для каждого* $i \geqslant 1$.

Тогда $A_q(n;\{d,n\}) \leqslant f(1)/f_0$. *Если* $(n, N, \{d,n\})_q$*-код* C *достигает этой границы для некоторого* $f(t)$, *то* $f(1-2d/n) = f(-1) = 0$ *и* $f_i M_i(C) = 0$ *для каждого* $i \geqslant 1$, *где*

$$M_i(C) = \sum_{x,y\in C} Q_i^{(n,q)}(1-2d(x,y)/n). \tag{24}$$

Граница линейного программирования из нашей работы [6] (формула (40)), которая была выведена для $\delta = n-d$, дает для нашего случая оценку (5) (которая в точности представляет собой верхнюю границу в (7)). Это дает нам простое доказательство необходимого условия в утверждении (ii) теоремы 4.

Второе доказательство утверждения (ii) теоремы 1. Верхняя граница в (5) получена с помощью теоремы 1 с использованием многочлена $f(t) = (t-1+2d/n)(t+1)$ второй степени. Если эта оценка достигается $(n, N, \{d,n\})_q$-кодом C, то из условий теоремы 7 следует, что $M_1(C) = M_2(C) = 0$, так как $f_1 > 0$ и $f_2 > 0$. Это означает, что код C является ортогональной таблицей силы 2. Мы заключаем очевидным образом, что мощность N кода C, т.е. величина

$$N = \frac{dq^2}{qd-(q-1)(n-1)},$$

делится на q^2 и что d делится на $qd-(q-1)(n-1)$. ▲

Численные результаты дают несколько общих ЛП-границ для специальных случаев семейств параметров q, n, d. Одну из них (другие оценки кажутся слабее) мы приведем здесь. Эта оценка представляет собой специальной случай границы, недавно полученной в работе [24], для диапазона чуть вне диапазона границы Плоткина.

Т е о р е м а 8. *Для каждого натурального числа* $m \geqslant 2$ *имеет место неравенство*

$$A_2(4m+1, \{2m, 4m+1\}) \leqslant 4m+2. \tag{25}$$

Д о к а з а т е л ь с т в о. Используем теорему 7 для длины $n = 4m+1$ и расстояния $d = 2m$ с многочленом

$$f(t) = 1 + 2mQ_2^{(4m+1,2)}(t) + (2m+1)Q_{4m-1}^{(4m+1,2)}(t). \tag{26}$$

Условие (A2) очевидным образом выполняется. Докажем, что условие (A1) выполняется с равенствами.

Из условия $Q_i^{(n,2)}(-1) = (-1)$ получаем $f(-1) = 0$. Так как $1-2d/n = 1/(4m+1)$, рассмотрим выражение

$$f\left(\frac{1}{4m+1}\right) = 1 + \frac{2m}{\binom{4m+1}{2}} \sum_{j=0}^{2} (-1)^j \binom{2m}{j}\binom{2m+1}{2-j} +$$
$$+ \frac{2m+1}{\binom{4m+1}{4m-1}} \sum_{j=0}^{4m-1} (-1)^j \binom{2m}{j}\binom{2m+1}{4m-1-j}.$$

Первую сумму можно подсчитать непосредственно, и она равна $-2m/(4m+1)$. Для подсчета второй суммы заметим, что единственные значения j, для которых оба биномиальных коэффициента ненулевые, – это $2m-2 \leqslant j \leqslant 2m$. Отсюда приходим к равенству $f(1/(4m+1)) = 0$.

Таблица 1

Оптимальные многочлены с одним ненулевым коэффициентом, $q = 3$

n	d	f_3	$\mathrm{sb}_3(n,d)$	n	d	f_3	$\mathrm{sb}_3(n,d)$
4	1	8	9	4	2	8	9
5	2	8	9	9	4	28	29
10	5	32	33	12	6	44	45
16	8	80	81	20	10	152	153
22	11	224	225				

Вычисление соответствующих моментов $M_i(C)$, заданных выражением (24), дает равенство $M_2(C) = M_{4m-1}(C) = 0$ (так как $f_2 > 0$ и $f_{2m+1} > 0$) для любого $(4m+1, 4m+2, \{2m, 4m+1\})$-кода, достигающего этой оценки. ▲

5.2. Численные вычисления верхних оценок линейного программирования. Здесь мы представим ЛП-границы для величины $A_q(n, \{d, n\})$, полученные прямым вычислением ЛП-границы с помощью симплекс-метода с использованием программного пакета Maple 19. Используемый алгоритм был применен нами для каждого $q \leqslant 5$ и $n \leqslant 50$. Имеется много случаев, для которых наилучшие оценки получались с помощью многочленов степени 1 и 2, приводящих к уже существующим оценкам. Поэтому мы исключили все такие случаи, предпочитая исследовать границы, полученные с помощью многочленов степени 3 или выше. Более того, мы исключили границы на все тривиальные коды мощности 4 или менее, границу, заданную выражением (5), а также все границы, значения которых не являются натуральными числами. Наконец, мы исключили также случаи, для которых граница, полученная с помощью сферических кодов (см. п. 5.3 ниже), лучше, или которые соответствуют случаю, включенному в теорему 8.

Нашу ЛП-границу мы нормализовали, положив $f_0 = 1$, и поэтому оценка, задаваемая допустимым многочленом f, выглядит следующим образом:

$$A_q(n, \{d, n\}) \leqslant 1 + f_1 + f_2 + \ldots + f_n,$$

в точности как и в классической формулировке Дельсарта границы линейного программирования. Во всех интересных случаях только один или два коэффициента f_i не равны нулю. Отметим, что благодаря специфике ЛП-границы мы не ожидаем большого числа ненулевых коэффициентов, и на самом деле, мы не увидели ни одного случая с тремя или более ненулевыми коэффициентами.

Обозначим через $\mathrm{sb}_q(n, d)$ наилучший численный результат, полученный указанным выше путем, для величины $A_q(n, \{d, n\})$. Так как все случаи для $q = 2$ уже покрыты указанными выше исключениями и результатами из работы [24], мы начнем наш обзор результатов по интересующей нас ЛП-границе с $q = 3$.

Результаты для $q = 3$. Как и для двоичного случая, для случая $q = 3$ среди множеств числовых параметров, содержащих только один ненулевой коэффициент (не считая, конечно, $f_0 = 1$) в разложении по многочленам Кравчука оптимального многочлена, мы наблюдали только коэффициент f_3. Это означает, что ЛП-многочлен имеет вид $f(t) = 1 + f_3 Q_3^{(n,3)}(t)$. Все эти многочлены, кроме одного, имеют d, близкое к $n/2$. Все эти результаты систематизированы в табл. 1.

Остальные случаи, где мы имели два ненулевых коэффициента, кроме обязательного значения $f_0 = 1$, приведены в табл. 2.

Наконец, мы приводим два случая многочленов

$$f(t) = 1 + f_5 Q_5^{(n,3)}(t)$$

Таблица 2

Оптимальные многочлены с двумя ненулевыми коэффициентами, $q = 3$

n	d	Ненулевые коэффициенты	$\mathrm{sb}_3(n,d)$	n	d	Ненулевые коэффициенты	$\mathrm{sb}_3(n,d)$
7	4	$f_2 = 6,\ f_3 = 20$	27	10	6	$f_2 = 12,\ f_3 = 20$	45
24	12	$f_3 = 113,\ f_4 = 210$	324	28	14	$f_3 = 208,\ f_4 = 400$	609
30	15	$f_3 = 320,\ f_4 = 624$	945	7	2	$f_3 = 4,\ f_5 = 16$	21

Таблица 3

Оптимальные многочлены для $q = 4$

n	d	Ненулевые коэффициенты	$\mathrm{sb}_4(n,d)$	n	d	Ненулевые коэффициенты	$\mathrm{sb}_4(n,d)$
5	2	$f_1 = 3/4,\ f_3 = 81/4$	22	5	3	$f_3 = 27$	28
6	3	$f_1 = 1/2,\ f_3 = 45/2$	24	9	6	$f_2 = 12,\ f_3 = 63$	76
10	5	$f_3 = 81$	82	18	12	$f_2 = 33,\ f_3 = 126$	160
24	16	$f_2 = 57,\ f_3 = 198$	256	42	28	$f_3 = 615$	616

для $(n,d) = (46,23)$ и $(48,24)$, что дает

$$\mathrm{sb}_3(46,23) = 2753 \quad \text{и} \quad \mathrm{sb}_3(48,24) = 3009$$

соответственно.

Результаты для $q = 4$. Для $q = 4$ мы нашли оптимальные многочлены почти полностью третьей степени, всего восемь таких случаев, как показано в табл. 3.

Единственный случай, отличный от приведенных в табл. 3, был многочлен пятой степени

$$f(t) = 1 + 75Q_4^{(18,4)}(t) + 468Q_5^{(18,4)}(t),$$

который дает

$$\mathrm{sb}_4(18,9) = 544.$$

Результаты для $q = 5$. Найденные нами для случая $q = 5$ оптимальные многочлены приведены в табл. 4.

5.3. Верхние границы с помощью сферических кодов. Взаимосвязь между кодами с двумя расстояниями в множестве Q_q^n и сферическими кодами с двумя расстояниями на евклидовой сфере $\mathbb{S}^{n-1}$ (описанной, например, в [6, раздел 4.3]) влечет, что каждый $(n, N, \{d,n\})_q$-код $C \subset Q_q^n$ соответствует сферическому коду с двумя расстояниями $W \subset \mathbb{S}^{(q-1)n-1}$. Квадраты расстояний между точками W равны $2dq/(q-1)n$ и $2q/(q-1)$. Используя классический результат работы [25], а также результаты из [6], мы заключаем, что либо

$$d = \frac{(k-1)n}{k} \tag{27}$$

для некоторого натурального $k \in \left[2, (\sqrt{2(q-1)n}+1)/2\right]$ (и число n очевидным образом делится на k), либо мощность N ограничена сверху неравенством $N \leqslant 2(q-1)n+1$.

Для произвольного $q \geqslant 3$ выражение (27) при $k > q$ влечет, что $d > (q-1)n/q$, т.е. величина d находится в диапазоне границы Плоткина. Используя оценку Плоткина, получаем, что ее можно записать в виде $N \leqslant (k-1)q/(k-q)$. Эти наблюдения можно суммировать следующим образом.

Таблица 4

Оптимальные многочлены для $q = 5$

n	d	Ненулевые коэффициенты	$\mathrm{sb}_5(n,d)$	n	d	Ненулевые коэффициенты	$\mathrm{sb}_5(n,d)$
6	3	$f_1 = 4/3,\ f_3 = 128/3$	45	6	4	$f_3 = 64$	65
7	4	$f_1 = 1,\ f_3 = 48$	50	16	12	$f_2 = 40,\ f_3 = 224$	265
21	14	$f_3 = 304$	305	27	18	$f_3 = 624,$	625
32	24	$f_2 = 92,\ f_3 = 432$	525	33	22	$f_3 = 1984$	1985
44	33	$f_2 = 152,\ f_3 = 672$	825	36	24	$f_3 = 32,\ f_4 = 2272$	2405
42	28	$f_3 = 1696,\ f_4 = 6528$	8225				

Теорема 9. *Если C – $(n, N, \{d, n\})_q$-код, то либо*

$$N \leqslant 2(q-1)n + 1,$$

либо

$$d = (k-1)n/k,$$

где $k \in \left[2, (\sqrt{2(q-1)n} + 1)/2\right]$ – натуральное число, и более того, имеет место неравенство

$$N \leqslant \frac{(k-1)q}{k-q}$$

для $q \geqslant 3$ и $q < k \leqslant (\sqrt{2(q-1)n} + 1)/2$.

Дальнейший набор оценок (для применения их к различным режимам для d и n) можно извлечь из результатов по сферическим множествам с двумя расстояниями, которые были рассмотрены и использованы в [26]. Отметим, что работа [26] имеет дело только с двоичными кодами, но при этом лемму 3.3 и теорему 3.5 из этой работы можно также применять и для $q \geqslant 3$. Хотя мы интересуемся здесь случаем, когда расстояния равны d и n, другие случаи также следуют из этих результатов. В дальнейшем предположим, что $q \geqslant 3$.

В этом месте будет удобно переключится на скалярные произведения для точек сферического кодов. Легко видеть, что скалярные произведения α и β, $-1 < \alpha < \beta < 1$, для точек из множества W равны

$$\alpha = -\frac{1}{q-1}, \quad \beta = \frac{n(q-1) - dq}{n(q-1)}.$$

Теперь из [26, лемма 3.3] вытекает, что если $d > n(q-2)/q$ (это эквивалентно условию $\alpha + \beta < 0$), то

$$A_q(n, \{d, n\}) \leqslant \binom{n(q-1)}{2}$$

за исключением (возможно) случаев $n(q-1) = \gamma^2 - 2$ и $n(q-1) = \gamma^2 - 3$, где $\gamma := (n-d)q/n(q-1)$ – целое нечетное число. Аналогично [26, теорема 3.5] (первоначально полученная в [27]) дает оценку

$$A_q(n, \{d, n\}) \leqslant \frac{n(q-1) + 2}{1 - (n(q-1) - 1)(q-1)^2/dq},$$

которая справедлива для $dq > (n(q-1) - 1)(q-1)^2$.

СПИСОК ЛИТЕРАТУРЫ

1. *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
2. *Shi M., Guan Y., Solé P.* Two New Families of Two-Weight Codes // IEEE Trans. Inform. Theory. 2017. V. 63. № 10. P. 6240–6246. https://doi.org/10.1109/TIT.2017.2742499
3. *Boyvalenkov P., Delchev K., Zinoviev D.V., Zinoviev V.A.* Codes with Two Distances: d and $d+1$ // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XVI). Svetlogorsk, Kaliningrad region, Russia. Sept. 2–8, 2018. P. 40–45. Available at https://www.dropbox.com/s/h7u89lh8vyirww9.
4. *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
5. *Boyvalenkov P., Delchev K., Zinoviev D.V., Zinoviev V.A.* Two-Weight (Linear and Non-linear) Codes // Proc. 17th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2020). On-line, Bulgaria. Oct. 11–17, 2020. P. 11–17. https://doi.org/10.1109/ACCT51235.2020.9383353
6. *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
7. *Delsarte P.* Two-Weight Linear Codes and Strongly Regular Graphs // MBLE Research Lab. Report R160. Brussels, Belgium, 1971.
8. *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
9. *Landjev I., Rousseva A., Storme L.* On Linear Codes of Almost Constant Weight and the Related Arcs // C. R. Acad. Bulgare Sci. 2019. V. 72. № 12. P. 1626–1633. https://doi.org/10.7546/CRABS.2019.12.04
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. *Bose R.C., Bush K.A.* Orthogonal Arrays of Strength Two and Three // Ann. Math. Statist. 1952. V. 23. № 4. P. 508–524. https://doi.org/10.1214/aoms/1177729331
12. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87. http://mi.mathnet.ru/ppi1804
13. *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. http://mi.mathnet.ru/ppi51
14. *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
15. *Boyvalenkov P.G., Dragnev P.D., Hardin D.P., Saff E.B., Stoyanova M.M.* Universal Bounds for Size and Energy of Codes of Given Minimum and Maximum Distances // IEEE Trans. Inform. Theory. 2021. V. 67. № 6. P. 3569–3584. https://doi.org/10.1109/TIT.2021.3056319
16. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge, UK: Cambridge Univ. Press, 1986.
17. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
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.* Construction of Maximal Arcs and Partial Geometry // Geom. Dedicata. 1974. V. 3. № 1. P. 61–64. https://doi.org/10.1007/BF00181361
20. *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
21. *Семаков Н.В., Зиновьев В.А.* Эквидистантные q-ичные коды с максимальным расстоянием и разрешимые уравновешенные неполные блок-схемы // Пробл. передачи информ. 1968. Т. 4. № 2. С. 3–10. http://mi.mathnet.ru/ppi1845
22. *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
23. *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
24. *Landjev I., Rousseva A., Vorobev K.* Constructions of Binary Codes with Two Distances. Preprint, 2022.
25. *Larman D.G., Rogers C.A., Seidel J.J.* On Two-Distance Sets in Euclidean Space // Bull. London Math. Soc. 1977. V. 9. № 3. P. 261–267. https://doi.org/10.1112/blms/9.3.261
26. *Barg A., Glazyrin A., Kao W.-J., Lai C.-Y., Tseng P.-C., Yu W.-H.* On the Size of Maximal Binary Codes with 2, 3, and 4 Distances, https://arXiv.org/abs/2210.07496 [math.CO], 2022.
27. *Glazyrin A., Yu W.-H.* Upper Bounds for s-Distance Sets and Equiangular Lines // Adv. Math. 2018. V. 330. P. 810–833. https://doi.org/10.1016/j.aim.2018.03.024

Бойваленков Петър
Делчев Константин
Институт математики и информатики
Болгарской академии наук, София, Болгария
peter@math.bas.bg
kdelchev@math.bas.bg
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
14.11.2022
После доработки
25.11.2022
Принята к публикации
28.11.2022