ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 1**

УДК 621.391.15

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

О q-ИЧНЫХ КОДАХ С ДВУМЯ РАССТОЯНИЯМИ d И $d+1$

Рассматриваются q-ичные блоковые коды с ровно двумя расстояниями: d и $d+1$. Приведено несколько конструкций таких кодов. В линейном случае показано, что все такие коды получаются простой модификацией линейных эквидистантных кодов. Получены верхние границы на максимальную мощность таких кодов. Приведены таблицы нижних и верхних границ для малых значений q и n.

Ключевые слова: коды с двумя расстояниями, эквидистантные коды, границы для кодов.

DOI: 10.31857/S0555292320010040

§ 1. Введение

Положим $Q = \{0, 1, \ldots, q-1\}$. Любое подмножество $C \subseteq Q^n$ называется кодом и обозначается через $(n, N, d)_q$ – код длины n и мощности $N = |C|$ с минимальным расстоянием (Хэмминга) d. Для линейных кодов используется обозначение $[n, k, d]_q$ (т.е. $N = q^k$). Эквидистантным называется $(n, N, d)_q$-код C, у которого для любых двух различных кодовых слов x и y имеет место равенство $d(x, y) = d$, где $d(x, y)$ – расстояние (Хэмминга) между x и y. Код C называется равновесным и обозначается через $(n, N, w, d)_q$, если каждое кодовое слово c имеет вес $\mathrm{wt}(c) = w$.

Мы рассматриваем коды, имеющие только два расстояния: d и $d+1$. Одна из наших целей – посмотреть, насколько можно увеличить мощность эквидистантных кодов, допуская еще одно значение для ближайшего расстояния между кодовыми словами. Как будет показано, при допущении еще одного расстояния многообразие кодов значительно увеличивается по сравнению с эквидистантными кодами. Такие коды могут представлять интерес как коды с почти постоянной энергией при амплитудно-фазовой модуляции (поскольку они почти эквидистантны). Мы также увидим, что такие коды часто бывают связаны с эквидистантными. В частности, мы покажем, что все линейные коды такого типа можно получить из линейных эквидистантных кодов. В то же время, нам не известны никакие исследования по кодам с двумя последовательными расстояниями.

Через $(n, N, \{d, d+1\})_q$ будем обозначать $(n, N, d)_q$-код $C \subset Q^n$ со следующим свойством: для любых двух различных кодовых слов x и y из C имеет место соотношение $d(x, y) \in \{d, d+1\}$. Нас будут интересовать конструкции, классификация и

[1] Работа выполнена при частичной финансовой поддержке Национальной научной программы “Информация и технологии связи для единого цифрового рынка в науке, образовании и безопасности” (ICTinSES) Министерства образования и науки Болгарии. Часть исследования была выполнена во время визита первого автора в отделение математических наук Университета Пердью в Форт-Уэйне.

[2] Работа выполнена при финансовой поддержке Национальной программы “Молодые ученые и постдокторанты” Министерства образования и науки Болгарии.

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

границы на максимально возможный размер $(n, N, \{d, d+1\})_q$-кодов. Мы покажем, что линейные q-ичные коды с двумя расстояниями d и $d+1$ полностью известны и могут быть получены простой модификацией линейных эквидистантных кодов. Предварительные результаты этой статьи (а именно, двоичный случай и гипотеза для $q \geqslant 3$) были приведены в [1]. Одновременно с нами этот же результат для линейных q-ичных кодов мощности $N \geqslant q^3$ был доказан в [2] другим методом.

§ 2. Предварительные сведения

Напомним следующую классическую границу Джонсона на размер $N_q(n, d, w)$ q-ичного равновесного $(n, N, w, d)_q$-кода [3]:

$$N_q(n, d, w) \leqslant \frac{(q-1)dn}{qw^2 - (q-1)(2w-d)n}, \tag{1}$$

если $qw^2 > (q-1)(2w-d)n$.

Определение 1. *Уравновешенной неполной блок-схемой* $B(v, k, \lambda)$ называется структура инцидентности (X, B), где $X = \{x_1, \dots, x_v\}$ – множество элементов, а $B = \{B_1, \dots, B_b\}$ – набор k-элементных множеств B_i (называемых *блоками*), таких что любые два различных элемента множества X содержатся ровно в $\lambda \geqslant 0$ блоках из B (здесь $1 \leqslant k \leqslant v-1$).

Двумя другими параметрами блок-схемы $B(v, k, \lambda)$ являются $b = |B|$ (количество блоков) и r (число блоков, содержащих один фиксированный элемент):

$$r = \lambda \frac{v-1}{k-1}, \quad b = \lambda \frac{v(v-1)}{k(k-1)}, \quad \text{если} \quad \lambda > 0$$

($\lambda = 0$ соответствует случаю $k = 1$ и, тем самым, $b = rv$).

Всякая блок-схема $B(v, k, \lambda)$ полностью описывается своей *матрицей инцидентности* $A = [a_{i,j}]$, где $a_{i,j} = 1$, если $a_i \in B_j$, и $a_{i,j} = 0$ в противном случае. Таким образом, A – двоичная $(v \times b)$-матрица со столбцами веса k, такая что любые две различные строки содержат ровно λ общих ненулевых позиций.

Схема $B(v, k, \lambda)$ называется *разрешимой* (и обозначается через $RB(v, k, \lambda)$), если ее матрица инцидентности A имеет вид

$$A = [A_1 \mid \dots \mid A_r], \tag{2}$$

где для любого $i \in \{1, \dots, r\}$ каждая строка матрицы A_i имеет вес 1. Блок-схема $B(v, k, \lambda)$ называется *m-квазиразрешимой* (схемой $NRB_m(v, k, \lambda)$) [4], если ее матрица инцидентности A представляется в виде

$$A = [A_1 \mid \dots \mid A_n], \quad n = \frac{bk}{v-m}, \tag{3}$$

таком что выполнены следующие свойства:

(1) Каждая подматрица A_j размера $v \times \dfrac{v-m}{k}$ состоит из строк веса 1, за исключением m нулевых строк, номера которых принадлежат множеству V_j, $|V_j| = m$, $V_j \subset \{1, 2, \dots, v\}$;

(2) Множества $V_1, \dots, V_n$ (как набор из n блоков размера m) индуцируют блок-схему $B(v, m, \xi)$ (называемую *сопутствующей*) для некоторого ξ.

Нам потребуются следующие результаты работ [4, 5].

Теорема 1. *Всякая m-квазиразрешимая блок-схема $NRB_m(v, k, \lambda)$ индуцирует q-ичный эквидистантный равновесный $(n, N, w, d)_q$-код C с параметрами $q =$*

$= (v-m+k)/k$, $N = v$,

$$n = \frac{\lambda v(v-1)}{(k-1)(v-m)}, \quad w = \frac{\lambda(v-1)}{k-1}, \quad d = \frac{\lambda(v+m-k)}{k-1},$$

лежащий на границе Джонсона (1), *с дополнительным свойством, что n его блоков размера $m = (n-w)N/n$, образованных номерами нулевых позиций, задают блок-схему $B(v, m, \xi)$.*

Напомним следующий широкий класс q-ичных эквидистантных кодов, построенных в [6].

Теорема 2. *Пусть p – простое, а s, ℓ и h – положительные целые числа. Тогда существует эквидистантный $(n, N, d)_q$-код с параметрами*

$$q = p^{sh}, \quad n = \frac{p^{s(h+\ell)}-1}{p^s-1}, \quad N = p^{s(h+\ell)}, \quad d = p^{s\ell}\frac{p^{sh}-1}{p^s-1}.$$

Определение 2 [7]. Пусть G – абелева группа порядка q в аддитивной записи. Квадратная матрица D с элементами из G порядка $q\mu$ называется разностной матрицей и обозначается через $D(q, \mu)$, если покомпонентные разности любых двух различных строк матрицы D содержат любой элемент группы G ровно μ раз.

Очевидно, матрица $D(q, \mu)$ индуцирует эквидистантный $(q\mu - 1, q\mu, \mu(q-1))_q$-код [6].

§ 3. Конструкции

3.1. Комбинаторные конструкции. Обозначим через $W_q(n)$ шар радиуса 1 с центром в нулевом векторе, т.е. $W_q(n) = \{x \in Q^n : \operatorname{wt}(x) \leqslant 1\}$.

Конструкция 1a. Шар $W_q(n)$ является $(n, (q-1)n+1, \{1, 2\})_q$-кодом.

Конструкция 1b. Добавляя к конструкции 1a проверку на четность (по модулю 2), получаем $(n+1, (q-1)n+1, \{2, 3\})_q$-код, который будем обозначать через $W_q^*(n+1)$. Для любого кодового слова $(0 \ldots 0\, a\, 0 \ldots 0)$ из $W_q(n)$ мы образуем кодовое слово $(0 \ldots 0\, a\, 0 \ldots 0 \,|\, a)$ из $W_q^*(n+1)$.

Конструкция 2. Эквидистантный $(n, N, d)_q$-код C дает два $(n', N, \{d', d'+1\})_q$-кода, а именно $(n-1, N, \{d-1, d\})_q$-код C_1, получаемый удалением (любой) позиции из C, и $(n+1, N, \{d, d+1\})_q$-код C_2, получаемый добавлением одной позиции к C.

Объединяя конструкции 1a, 1b с конструкцией 2, получаем следующие две конструкции.

Конструкция 3a. Эквидистантный $(n_1, N_1, d)_{q_1}$-код и $W_{q_2}(n_2) = (n_2, N_2, \{1, 2\})$ дают $(n, N, \{d+1, d+2\})_q$-код с параметрами

$$q = \max\{q_1, q_2\}, \quad n = n_1 + n_2, \quad N = \min\{N_1, N_2\}.$$

Конструкция 3b. Эквидистантный $(n_1, N_1, d)_{q_1}$-код и $W_{q_2}^*(n_2) = (n_2, N_2, \{2, 3\})$ дают $(n, N, \{d+2, d+3\})_q$-код с параметрами

$$q = \max\{q_1, q_2\}, \quad n = n_1 + n_2, \quad N = \min\{N_1, N_2\}.$$

Конструкция 4. Если существует r взаимно ортогональных латинских квадратов порядка q, то существует семейство $(s+2, q^2, \{s+1, s+2\})_q$-кодов C_s, где $s = 0, 1, \ldots, r$. Для степени простого q код C_s линеен.

Объединяя конструкции 2 и 4, получаем следующее:

Конструкция 5. Для любой степени простого числа q существует семейство (линейных) $[n, 2, \{d, d+1\}]_q$-кодов с параметрами

$$n = s(q+1) + r, \quad d = sq + r - 1, \quad s \geqslant 1, \quad r = 1, \ldots, q+1.$$

Конструкция 6. Если существует разностная матрица $D(q, \mu)$, то существуют $(n, N, \{d, d+1\})_q$-коды с параметрами

$$\begin{aligned} &n = q\mu - 2, \qquad && N = q\mu, \qquad && d = (q-1)\mu - 1, \\ &n = q\mu, && N = q\mu, && d = (q-1)\mu. \end{aligned}$$

Хорошо известный эквидистантный $[4, 2, 3]_3$-код C_1 и $[2, 2, \{1, 2\}]_3$-код C_2 (конструкция 4) по конструкции 3 дают $[6, 2, \{4, 5\}]_3$-код C, этот код не очень хорош, но линеен. Используя $[3, 2, \{2, 3\}]_3$-код C_3 (конструкция 4) и применяя конструкцию 3, получаем $[7, 2, \{5, 6\}]_3$-код, хуже оптимального по мощности на 1.

Из эквидистантного $(13, 27, 9)_3$-кода (теорема 2) с помощью конструкции 2 получаем $(14, 27, \{9, 10\})_3$-код, что лучше, чем случайный $(14, 18, \{9, 10\})_3$-код, а также $(12, 27, \{8, 9\})_3$-код, лежащий на верхней границе (наилучший найденный случайный код имеет мощность 18).

Разностная матрица $D(4, 3)$ (см. [8]) без тривиального столбца является оптимальным эквидистантным $(11, 12, 8)_3$-кодом. Разностная матрица $D(3, 4)$ (см. [8]) без тривиального столбца является оптимальным эквидистантным $(11, 12, 9)_4$-кодом.

Хорошо известный эквидистантный $(5, 16, 4)_4$-код C_1 и $(5, 16, \{1, 2\})_4$-код C_2 (конструкция 1) по конструкции 3 дают $(10, 16, \{5, 6\})_4$-код (не являющийся хорошим – имеется случайный $(10, 20, \{5, 6\})_4$-код). Двукратное повторение $(5, 16, 4)_4$-кода C_1 дает оптимальный $(10, 16, 8)_4$-код.

Из эквидистантного $(6, 9, 5)_4$-кода [4] с помощью двукратного повторения получаем $(12, 9, \{10, 11\})_4$-код (лучше, чем случайный). Из эквидистантного $(21, 64, 16)_4$-кода [6] получаем $(22, 64, \{16, 17\})_4$- и $(20, 64, \{15, 16\})_4$-коды с помощью конструкции 2. Из эквидистантного $(9, 10, 8)_5$-кода [5] с помощью конструкции 2 получаем $(8, 10, \{7, 8\})_5$- и $(10, 10, \{8, 9\})_5$-коды. С помощью конструкции 5 получаем следующее семейство $(n, N, \{d, d+1\})_5$-кодов:

$$n = 9 + s, \quad N = 10, \quad d = 8 + s - 1, \quad s = 0, 1, \ldots, 6.$$

В частности, при $s = 0$ получаем оптимальный $(9, 10, 8)_5$-код, а при $s \geqslant 2$ все получающиеся коды являются новыми. С помощью конструкции 1 из этого эквидистантного $(9, 10, 8)_5$-кода получаем $(11, 9, \{9, 10\})_5$-код.

Из эквидистантного $(6, 25, 5)_5$-кода получаем семейство $(6+s, 25, \{5+s-1, 5+s\})_5$-кодов, где $s = 0, 1, \ldots, 6$, что для $s \geqslant 1$ дает лучшие (или новые) коды.

Хорошо известная разрешимая блок-схема $(15, 35, 7, 3, 1)$ эквивалентна оптимальному эквидистантному $(7, 15, 6)_5$-коду [6]. Теперь, применяя конструкцию 5, получаем из него коды со следующими параметрами: $n = 7 + s$, $N = 15$, $d = 6 + s - 1$, $s = 1, \ldots, 6$.

Из аффинной блок-схемы $(16, 4, 1)$ (см. [5]) получаем эквидистантный равновесный $(16, 16, 15, 14)_6$-код, из которого в свою очередь получаем $(16, 17, \{14, 15\})_6$-код (добавлением нулевого кодового слова).

3.2. Случайные коды. Мы использовали компьютерную программу для генерации случайных кодов по простому эвристическому алгоритму. В качестве начального множества выбирается один нулевой вектор в простейшей версии или наилучшей из найденных кодов на единицу меньшей длины в более сложной. Далее пространство поиска состоит из векторов веса d и $d+1$. Оно выделяется из начальной базы данных всех q^n векторов длины n, генерируемой (один раз) стандартным лексикографическим образом. Программа добавляет случайно выбираемые подходящие векторы до тех пор, пока получаемый код является хорошим (т.е. пока в нем есть только расстояния d и $d+1$). Можно совершать много итераций, однако обычно наилучшие коды (получаемые таким образом) находятся довольно быстро. Мощности таких случайных кодов приведены в § 6 вместе с мощностями кодов, полученных из конструкций текущего параграфа.

Результаты показывают, что такой подход хорош, когда $d = 1, 2$ и когда d близко к $n-1$, но не позволяет находить хорошие коды с богатой структурой. Вероятно, он также не хорош для средних значений d.

§ 4. Линейные $(n, N, \{d, d+1\})_q$-коды

Здесь мы опишем результаты о классификации для случая линейных кодов с расстояниями d и $d+1$. В частности, мы покажем, что линейные коды с двумя расстояниями d и $d+1$ полностью известны. Нижеследующая теорема была доказана в двоичном случае в [1], где также была выдвинута гипотеза для q-ичного случая. Мы дадим здесь простое доказательство этой гипотезы для случая $q \geqslant 2$ и $k \geqslant 2$, опирающееся только на соображения из теории кодирования. Соответствующий результат для $k \geqslant 3$ был одновременно доказан в [2] на основе геометрических рассуждений.

Пусть C – q-ичный (линейный) эквидистантный $[n, 3, q^2]_q$-код длины $n = q^2+q+1$ с расстоянием q^2 и мощностью q^3.

Лемма. *Пусть C – вышеуказанный код, представленный в виде $(n \times q^3)$-матрицы над $\mathbb{F}_q$ (обозначим ее через $[C]$). Тогда $[C]$ нельзя представить в виде конкатенации двух матриц, т.е. $[C] = [C_1 \,|\, C_2]$, где $[C_1]$ – матрица размера $(x \times q^3)$ (здесь $x < (n-1)/2$), задающая линейный $[x, q^3, \{d, d+1\}]_q$-код C_1.*

Доказательство. Если $\boldsymbol{x} \in C$, то, очевидно, $\alpha\boldsymbol{x} \in C$ для всех $\alpha \in \mathbb{F}_q^*$. Тем самым, $q^3 - 1$ ненулевых кодовых слов кода C разбиваются на $q^2 + q + 1$ классов. Таким образом, мы получили код на классах таких элементов. Он задается $(n \times n)$-матрицей P.

Предположим, что матрица P является конкатенацией двух матриц P_1 и P_2, т.е. $P = [P_1 \,|\, P_2]$, где P_1 – матрица размера $x \times (q^2 + q + 1)$, соответствующая классам эквивалентности линейного $[x, q^3, \{d, d+1\}]$-кода C_1. Тогда каждое слово кода C_1 имеет $x - d$ или $x - d - 1$ позиций, содержащих нули. Для упрощения дальнейших вычислений положим $\ell = x - (d+1)$ (поскольку вместо веса слова мы будем рассматривать число его нулевых позиций).

Так как P соответствует эквидистантному коду с кодовым расстоянием q^2, то, очевидно, P_2 соответствует (линейному) $[n - x, 3, q^2 - d - 1]_q$-коду C_2 с двумя расстояниями $q^2 - d - 1$ и $q^2 - d$. Поэтому без ограничения общности можно считать, что $x \leqslant n/2$. Поскольку $n = q^2 + q + 1$, будем предполагать, что $x \leqslant q(q+1)/2$ и $\ell \leqslant (q+1)/2$ (действительно, каждая ненулевая строка (так же как и каждый столбец) матрицы P содержит $q+1$ нулей).

Так как любой столбец P содержит $q+1$ нулей, в матрице P имеется $n(q+1)$ нулевых элементов. Пусть матрица P_1 содержит ровно η слов веса $d+1$ (т.е. с ℓ нулями) и остальные $n - \eta$ слов веса d (т.е. с $\ell + 1$ нулями). Таким образом, имеем

$$\ell\eta + (\ell+1)(n-\eta) = (q+1)x.$$

Выражая отсюда η, получаем

$$\eta = (\ell+1)n - (q+1)x. \tag{4}$$

Поскольку C_1 – линейный код размерности 3, для любой пары координатных позиций существует ровно одна строка матрицы P_1 с нулями в этих позициях. Всего имеется x координатных позиций и $x(x-1)/2$ пар позиций. С другой стороны, имеется η строк с ℓ нулями (каждая строка дает $\ell(\ell-1)/2$ пар координат) и $n-\eta$ строк с $\ell+1$ нулями (каждая строка дает $\ell(\ell+1)/2$ пар координат). Итак, получаем равенство

$$\frac{x(x-1)}{2} = \frac{\ell(\ell-1)}{2}\eta + \frac{\ell(\ell+1)}{2}(n-\eta). \tag{5}$$

Наша цель – показать, что равенство (5) не может выполняться при любом x из интервала $[2, q(q+1)/2]$. С учетом (4) выражение (5) принимает вид

$$\begin{aligned} &x(x-1) = \ell(\ell-1)\eta + \ell(\ell+1)n - \ell(\ell+1)\eta = \ell(\ell+1)n - 2\ell\eta = \\ &= \ell(\ell+1)n - 2\ell[(\ell+1)n - (q+1)x] = 2\ell(q+1)x - \ell(\ell+1)n. \end{aligned}$$

Таким образом, приходим к следующему квадратному уравнению на x:

$$x^2 - (2\ell(q+1)+1)x + \ell(\ell+1)n = 0. \tag{6}$$

Покажем, что его дискриминант отрицателен. Итак, следует проверить, что

$$(2\ell(q+1)+1)^2 < 4\ell(\ell+1)n.$$

С учетом того, что $n = q^2+q+1$, это равносильно

$$\begin{aligned} &4\ell^2(q^2+2q+1) + 4\ell(q+1) + 1 < 4\ell(\ell+1)(q^2+q+1) = \\ &= 4\ell^2(q^2+q+1) + 4\ell(q^2+q+1). \end{aligned}$$

После упрощения получаем

$$4\ell^2 q + 1 < 4\ell q^2.$$

Так как $\ell \leqslant (q+1)/2$, последнее неравенство очевидно выполнено при $\ell \geqslant 1$. Таким образом, мы получили, что подматрицы P_1 не существует, и следовательно, линейный $[q^2+q+1, 3, q^2]_q$-код C не может быть представлен в виде конкатенации двух линейных кодов C_1 и C_2 типа $(n, N, \{d, d+1\})_q$. ▲

Т е о р е м а 3. *Пусть C – q-ичный линейный $[n,k,d]_q$-код с двумя расстояниями d и $d+1$, где $k \geqslant 2$. Тогда C может быть получен конструкцией 2 предыдущего параграфа, т.е. удалением или добавлением произвольного столбца в проверочной матрице линейного q-ичного эквидистантного кода, за исключением случая $k=2$ и $q \geqslant 3$, когда C может быть получен конструкцией 2 или конструкцией 5.*

Д о к а з а т е л ь с т в о. Вначале рассмотрим случай $k=2$. В этом случае может иметься $[n,2,d]_q$-код C с двумя расстояниями d и $d+1$, получаемый также конструкцией 5. Пусть C_1 – эквидистантный $[n_1,2,d_1]_q$-код с параметрами $n_1 = s(q+1)$, $d_1 = sq$, а C_2 – $[n_2,2,d_2]_q$-код с параметрами $n_2 = r$, $d_2 = r-1$. Порождающая матрица G кода C имеет вид $G = [G_1 \mid G_2]$, где G_1 и G_2 – порождающие матрицы кодов C_1 и C_2, имеющие (с точностью до эквивалентности) следующий вид: $G_1 = [G_0 \mid \ldots \mid G_0]$ является s-кратным повторением матрицы

$$G_0 = \begin{bmatrix} a_0 & a_1 & a_1 & a_1 & \ldots & a_1 \\ a_1 & a_0 & a_1 & a_2 & \ldots & a_{q-1} \end{bmatrix},$$

где используются обозначения $\mathbb{F}_q = \{a_0 = 0, a_1 = 1, a_2, \ldots, a_{q-1}\}$, а матрица G_2 имеет вид

$$G_2 = \begin{bmatrix} a_0 & a_1 & a_1 & a_1 & \ldots & a_1 \\ a_1 & a_0 & a_1 & a_2 & \ldots & a_{r-2} \end{bmatrix}.$$

Все эти факты широко известны и не нуждаются в доказательствах. Единственное, что требуется отметить, это тот факт, что все элементы второй строки матрицы G_2, начиная со второй позиции, должны быть различными, и это условие необходимо и достаточно для того, чтобы G_2 была порождающей матрицей кода C_2.

Теперь мы утверждаем, что любой $[n,2,d]_q$-код с двумя расстояниями должен иметь такой вид. Это очевидно для случая $n \leqslant q$. Для бóльших n предположим, что код C_1 длины $q+1$ не является эквидистантным $[q+1,2,q]_q$-кодом, т.е. имеет минимальное расстояние $d = q-1$. Поскольку его среднее расстояние известно (и равно q), отсюда заключаем, что этот код имеет три расстояния, а именно $q-1$, q и $q+1$. Обозначая через α_w число кодовых слов веса w и учитывая, что $\alpha_{q-1} = \alpha_{q+1}$, получаем

$$\alpha_{q-1} = \alpha_{q+1} = q-1, \quad \alpha_q = (q-1)^2. \tag{7}$$

Как мы знаем, $[r,2,r-1]_q$-код C_2 имеет веса $r-1$ и r. Обозначая через β_w число кодовых слов веса w, получаем, что

$$\beta_{r-1} = (q-1)r, \quad \beta_r = (q-1)(q+1-r). \tag{8}$$

Таким образом, конкатенация этих двух кодов C_1 и C_2 должна была бы быть кодом C с по крайней мере тремя расстояниями d, $d+1$ и $d+2$, где $d \leqslant q+r-1$, т.е. получаем противоречие. Значит, код C_1 длины $(q+1)s$ должен быть эквидистантным. Следовательно, любой $[n,2,d]_q$-код C с двумя расстояниями d и $d+1$ может быть получен одной из двух конструкций, а именно конструкцией 2 или 5.

Теперь для завершения доказательства нам остается лишь показать, что всякий $[n,3,d]_q$-код с двумя расстояниями d и $d+1$ может быть получен только конструкцией 2. Предположим противное – пусть C_1 является $[n_1,3,d_1]_q$-кодом с двумя расстояниями d_1 и d_1+1 длины n_1 в интервале $2 \leqslant n_1 \leqslant q^2+q-1$. Это означает, что существует $[n_2,3,d_2]_q$-код C_2 (дополнительный к C_1) с двумя расстояниями d_2 и d_2+1 длины $n_2 = q^2+q+1-n_1$. Следовательно, существует q-ичный эквидистантный $[n,3,q^2]_q$-код C длины $n = q^2+q+1$, который можно представить в виде конкатенации кодов C_1 и C_2. Но согласно лемме это невозможно. Так как любой $[n,k \geqslant 4,d]_q$-код с двумя расстояниями d и $d+1$ укорочением сводится к $[n',3,d]_q$-коду с двумя расстояниями d и $d+1$, то это и завершает доказательство. ▲

Замечание 1. Рассматриваемые коды с весами d и $d+1$ являются подклассом более широкого класса кодов с двумя весами – классического объекта алгебраической теории кодирования. Однако такие коды с весами d и $d+1$ ранее не рассматривались в литературе (см., например, дающий исчерпывающую информацию обзор [9]). Таким образом, теорема 3 является результатом о классификации для линейных кодов с весами d и $d+1$. Как хорошо известно [9,10], двойственный код любого линейного проективного кода с двумя весами равномерно упакован (и следовательно, полностью регулярен – см. [11,12]). Коды с двумя весами, получаемые удалением одной позиции из линейных эквидистантных кодов, также индуцируют полностью регулярные коды и хорошо известны [11,12].

Замечание 2. Доказательство леммы, приведенное выше, можно обобщить на любой эквидистантный код C, обладающий следующим свойством: для любых двух координатных позиций, скажем, i и j, $1 \leqslant i,j \leqslant n$, существуют λ кодовых слов $\boldsymbol{c} = (c_1, \ldots c_n)$ кода C с двумя нулями в этих двух позициях, т.е. $c_i = c_j = 0$, где λ одинаково для всех i и j. Это означает, например, что никакой двоичный нелинейный $(n,N,d) = (4m-1,4m,2m)$-код Адамара нельзя представить в виде конкатенации двух кодов C_1 и C_2 (длин $n_i \geqslant 2$) с двумя последовательными расстояниями d_1, d_1+1 и d_2, d_2+1 соответственно. Но эту лемму нельзя использовать для доказательства соответствующей теоремы, где линейность весьма существенна. Заметим также, что это сведение к квадратному уравнению не дает никакого результата для кодов с расстояниями d и $d+\delta$, где $\delta \geqslant 2$. Даже для следующего случая $\delta = 2$ соответствующие коды существуют (в случае $q = 2^m$ [9]), а решение квадратного уравнения сводится к решению диофантова уравнения, что выходит за рамки настоящей статьи.

§ 5. Верхние границы

Нас интересуют верхние границы на величину

$$A_q(n; \{d, d+1\}) = \max\{|C| : C \text{ является } (n, |C|, \{d, d+1\})\text{-кодом}\},$$

максимальную возможную мощность кода в Q^n с двумя расстояниями d и $d+1$.

Общая граница гармонического анализа Дельсарта [10]

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

и ее улучшение Барга – Мусина [13]

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

(при $(2d+1)q < 2n(q-1) + 2 - q$) кажутся слишком общими, в то время как наша ситуация довольно специфическая.

5.1. Границы линейного программирования. Для фиксированных n и q (нормированные) многочлены Кравчука определяются как

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

где

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

– (обычные) многочлены Кравчука. Если многочлен $f(t) \in \mathbb{R}[t]$ имеет степень $m \geqslant 0$, то он имеет единственное разложение вида

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

Следующая теорема является адаптацией для оценки $A_q(n; \{d, d+1\})$ общей границы линейного программирования Дельсарта. Доказательства таких границ обычно считаются фольклорными (см., например, [10, 14]).

Теорема 4. *Пусть $n \geqslant q \geqslant 2$, и пусть $f(t)$ – вещественный многочлен степени $m \leqslant n$, такой что*

(A1) $f(t) \leqslant 0$ *для* $t \in \{1 - 2d/n, 1 - 2(d+1)/n\}$;

(A2) *Коэффициенты в разложении по многочленам Кравчука* $f(t) = \sum_{i=0}^{m} f_i Q_i^{(n,q)}(t)$ *удовлетворяют условию* $f_i \geqslant 0$ *для всех* i.

Тогда $A_q(n; \{d, d+1\}) \leqslant f(1)/f_0$. Если эта граница достигается для некоторого $(n, N, \{d, d+1\})_q$-кода C и многочлена $f(t)$, то $f(1 - 2(d+i)/n) = 0$, $i = 0, 1$, когда существуют точки кода C на расстоянии $d+i$, $i = 0, 1$, и при этом $f_i M_i(C) = 0$, где

$$M_i(C) = \sum_{x,y \in C} Q_i^{(n,q)}(1 - 2d(x,y)/n) = 0$$

– *i-й момент кода C.*

Большинство верхних границ, приведенных в таблицах ниже, получены согласно теореме 4 симплексным методом (т.е. получены наилучшие возможные границы из теоремы 4). Теперь опишем некоторые случаи, когда возможен аналитический вид хороших границ.

Многочлен первой степени $f(t) = t - 1 + 2d/n$ дает границу Плоткина, достигающуюся для многих больших значений d. Оптимизация по многочленам второй степени дает следующий результат.

Теорема 5. *Если $d \geqslant (n-1)(q-1)/q$, то*

$$A_q(n; \{d, d+1\}) \leqslant \frac{q^2 d(d+1)}{n^2(q-1)^2 - n(q-1)(2dq+q-1) + dq^2(d+1)}. \tag{9}$$

Если некоторый $(n, N, \{d, d+1\})_q$-код C достигает этой границы, то $M_2(C) = 0$, и кроме того, $M_1(C) = 0$ при $d > (n-1)(q-1)/q$.

Доказательство. Рассмотрим многочлен второй степени

$$f(t) = \left(t - 1 + \frac{2d}{n}\right)\left(t - 1 + \frac{2d+2}{n}\right) = f_0 + f_1 Q_1^{(n,q)}(t) + f_2 Q_2^{(n,q)}(t),$$

где

$$f_0 = \frac{4(n^2(q-1)^2 - n(q-1)(2dq+q-1) + dq^2(d+1))}{n^2q^2},$$
$$f_1 = \frac{8(q-1)(dq-(q-1)(n-1))}{nq^2},$$
$$f_2 = \frac{4(q-1)^2(n-1)}{nq^2}.$$

Условие (A1), очевидно, выполнено.

Условие $f_0 > 0$ равносильно квадратичному по dq неравенству, которое выполнено при $n \geqslant q$. Условие $f_1 \geqslant 0$ равносильно $dq \geqslant (n-1)(q-1)$, а $f_2 > 0$ очевидно. Таким образом, $f(t)$ удовлетворяет (A1) и (A2) при условии, что $d \geqslant (n-1)(q-1)/q$. Вычисляя теперь $f(1)/f_0$, получаем границу (9).

Условия достижимости границы (9) вытекают из общих условий теоремы 4. ▲

В некоторых случаях граница (9) достигается. В частности, $A_q(n; \{d, d+1\}) \leqslant q^2$ для $d = n-1$, что достигается при $(q, n) = (3,3)$, $(3,4)$, $(4,5)$ и $(5,6)$. Далее, в силу (9) имеем $A_2(7; \{4,5\}) = A_2(7; \{3,4\}) = 8$, $A_2(10; \{5,6\}) = 12$, $A_3(12, \{8,9\}) = A_3(13, \{9,10\}) = 27$. Случаи, когда граница (9) достигается, в приведенных ниже таблицах отмечены знаком $d2$.

Кроме того, если граница (9) достигается для некоторого кода C и при этом $d > (n-1)(q-1)/q$ (т.е. $f_1 > 0$), то $M_1(C) = M_2(C) = 0$. Таким образом, C является ортогональной таблицей силы 2. В частности, мощность C кратна q^2. Это соображение позволяет улучшить границу (9) на единицу, приводя к точным значениям $A_2(12, \{5,6\}) = A_2(12, \{6,7\}) = A_2(13, \{6,7\}) = 13$ и границе $13 \leqslant A_3(6, \{4,5\}) \leqslant 14$. Эти случаи отмечены в таблицах знаком n. Еще один интересный случай – это $A_3(7, \{4,5\}) = 15$, где граница (9) достигается при $d = (n-1)(q-1)/q$.

Дальнейшие границы можно получить с помощью специально подобранных многочленов. Например, многочлен

$$f(t) = 1 + (q-1)nQ^{(n,q)}_{(n(q-1)+1)/q}(t)$$

дает $A_q(n,\{1,2\}) = (q-1)n+1$ (см. конструкцию 1a), когда q кратно $n-1$. В частности, получаем $A_2(n,\{1,2\}) = n+1$ при нечетном n. Аналогично, многочлен

$$f(t) = 1 + \frac{n+2}{2} Q_{n/2}^{(n,2)}(t) + \frac{n}{2} Q_{1+n/2}^{(n,2)}(t),$$

где n четно, дает $A_2(n,\{1,2\}) \leqslant f(1)/f_0 = n+2$. Если эта граница достигается, то условия дополняющей нежесткости линейного программирования теоремы 4 дают уравнения $M_{n/2} = M_{1+n/2} = 0$, которые вместе с тривиальным уравнением $A_d(x) + A_{d+1}(x) = |C| - 1$ позволяют вычислить (используя Maple) распределения расстояний кодов (с двумя расстояниями), достигающих этой границы. Здесь $A_{d+i}(x) = |\{y \in C :\ d(x,y) = d+i\}|$, $i = 0, 1$, $x \in C$. Поскольку это распределение расстояний оказывается не целочисленным, получаем противоречие. Таким образом, оба многочлена доказывают, что $A_2(n,\{1,2\}) = n+1$ (что достигается конструкцией 1a). Такие случаи отмечены в таблицах знаком a.

Дальнейшее тщательное изучение условий достижения границ линейного программирования могут, возможно, привести к другим улучшениям в таблицах.

5.2. Границы через сферические коды. Коды в Q^n можно естественным образом отобразить на сферу $\mathbb{S}^{(q-1)n-1}$. Вначале биективно отобразим символы алфавита $0, 1, \ldots, q-1$ в вершины правильного симплекса размерности $q-1$, а затем покоординатно отобразим кодовые слова q-ичного кода $C \subset Q^n$ в $\mathbb{R}^{(q-1)n}$. Нетрудно видеть, что все векторы имеют одинаковую норму, и после нормировки получаем сферический код на сфере $\mathbb{S}^{(q-1)n-1}$. Этот сферический код имеет мощность $|C|$ и максимальное скалярное произведение $1 - 2dq/(q-1)n$ (т.е. минимальный квадрат расстояния $2dq/(q-1)n$). Очевидно, q-ичные коды с расстояниями d и $d+1$ отображаются в сферические коды с двумя расстояниями с квадратами расстояний $2dq/(q-1)n$ и $2(d+1)q/(q-1)n$. Из этого вытекает следующая верхняя граница на $A_q(n,\{d,d+1\})$.

Т е о р е м а 6. *Если* $d > (\sqrt{2(q-1)n} - 1)/2$, *то*

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

Д о к а з а т е л ь с т в о. В [15] было доказано, что если мощность множества в $\mathbb{R}^n$ с двумя расстояниями a и b, $a < b$, больше чем $2n+3$, то отношение a^2/b^2 равно $(k-1)/k$, где k – положительное целое число, такое что $2 \leqslant k \leqslant (\sqrt{2n}+1)/2$. В работе [16] ограничение $2n+3$ было улучшено до $2n+1$.

В нашей ситуации $a^2/b^2 = d/(d+1) = (k-1)/k$, откуда следует, что $d = k-1$ должно принадлежать интервалу $[1, (\sqrt{2(q-1)n} - 1)/2]$. Иными словами, не существует q-ичных кодов с расстояниями d и $d+1$ и мощностью, большей $2(q-1)n+1$, если $d > (\sqrt{2(q-1)n} - 1)/2$, и таким образом, $A_q(n,\{d,d+1\}) \leqslant 2(q-1)n+1$. ▲

Граница теоремы 6, как правило, лучше, чем симплексный метод, для достаточно больших n и средних значений d. В первый раз это происходит при $(n,d) = (13,4)$ для $q = 2$, $(9,3)$ для $q = 3$, $(8,3)$ для $q = 4$ и $(7,4)$ для $q = 5$.

Мы не нашли границ линейного или полуопределенного программирования для сферических кодов, которые давали бы хорошие границы для наших кодов.

§ 6. Таблицы

Мы приводим таблицы для $q = 2, 3, 4, 5$. По горизонтали даются значения d, по вертикали – значения n. Нижние границы показывают наилучший из найденных на компьютере случайных кодов и кодов по конструкциям из § 3. Все найденные случайные коды предоставляются авторами по запросу.

Таблица 1

Границы для $q = 2$

n	d																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
7	8	7–10	8^{d2}	8^{d2}	2*	2*											
8	9^a	8–12	8–10	8–10	4*	2*	2*										
9	10	9–14	8–16	8–10	6*	4*	2*	2*									
10	11^a	10–16	8–16	10–16	12^{d2}	6^{d2}	2–3	2*	2*								
11	12	11–18	8–19	10–20	12^{d2}	12^{d2}	4*	2*	2*	2*							
12	13^a	12–20	8–25	10–21	13^n	13^n	4*	4*	2*	2*	2*						
13	14	13–22	8–26	10–27	13–19	13^n	8^{d2}	4*	2*	2*	2*	2*					
14	15^a	14–24	$8–29^{t6}$	$10–29^{t6}$	14–27	14–19	16^{d2}	8*	4*	2–3	2*	2*	2*				
15	16	15–26	$8–31^{t6}$	$11–31^{t6}$	14–29	14–30	16	16*	4*	4*	2*	2*	2*	2*			
16	17^a	16–28	$8–33^{t6}$	$11–33^{t6}$	$14–33^{t6}$	$15–33^{t6}$	16–18	16–18	6*	4*	2*	2*	2*	2*	2*		
17	18	17–30	$9–35^{t6}$	$12–35^{t6}$	$14–35^{t6}$	$15–35^{t6}$	17–22	16–18	10*	6*	4*	2*	2*	2*	2*	2*	
18	19^a	18–32	$9–37^{t6}$	$12–37^{t6}$	$14–37^{t6}$	$15–37^{t6}$	17–35	18–22	20*	10	4*	2–4	2*	2*	2*	2*	2*

Таблица 2

Границы для $q = 3$

n	d												
	1	2	3	4	5	6	7	8	9	10	11	12	13
3	9	9											
4	9^a	9	9										
5	11–13	9–17	11–13	6									
6	13–15	11–18	11–16	$13–14^n$	4								
7	15^a	13–27	11–27	15^{d2}	10	3							
8	17–19	15–31	11–30	15–31	18–19	9	3						
9	19–21	17–33	$11–37^{t6}$	15–36	18–25	18–21	6	3					
10	21^a	19–45	$11–41^{t6}$	$15–41^{t6}$	$18–41^{t6}$	18–21	13–14	3					
11	23–25	21–45	$11–45^{t6}$	$15–45^{t6}$	18–45	18–45	18–25	12*	4*	3*			
12	25–27	23–51	$12–49^{t6}$	$15–49^{t6}$	$18–49^{t6}$	$18–49^{t6}$	18–30	27^{d2}	9*	4*	3*		
13	27^a	25–63	$13–53^{t6}$	$15–53^{t6}$	$18–53^{t6}$	$18–53^{t6}$	$18–53^{t6}$	18–27	27^{d2}	6*	3*	3*	
14	29–31	27–63	$14–57^{t6}$	$15–57^{t6}$	$18–57^{t6}$	$18–57^{t6}$	$18–57^{t6}$	18–45	27–31	12–13	6*	3*	3*

Таблица 3

Границы для $q = 4$

n	d										
	1	2	3	4	5	6	7	8	9	10	11
5	16^a	16–25	16	16*							
6	19–22	16–37	16–37	18–22	9*						
7	22–26	19–41	16–43	18–41	21–26	8*					
8	25–28	22–50	$16–49^{t6}$	$18–49^{t6}$	21–32	19–28	5*				
9	28^a	25–67	16–86	$18–55^{t6}$	$21–55^{t6}$	19–28	15–20*	5*			
10	31–34	28–72	16–90	$18–61^{t6}$	$20–61^{t6}$	$19–61^{t6}$	21–34	16*	5*		
11	34–38	31–78	16–134	$18–67^{t6}$	$21–67^{t6}$	$19–67^{t6}$	20–56	22–38	12*	4*	
12	37–40	34–97	18–152	$18–73^{t6}$	$21–73^{t6}$	$19–73^{t6}$	$20–73^{t6}$	22–43	21–40	9*	4*

Верхние границы берутся из наилучших границ линейного программирования, получаемых симплексным методом (без пометок в таблицах), с помощью специальных многочленов из п. 5.1 (помечены знаками $d2$, n и a соответственно), соответствующих наилучших известных границ на $A_q(n, d)$ [17] (помечены знаком $*$) и границ теоремы 6 (помечены знаком $t6$).

Таблица 4

Границы для $q = 5$

n	d								
	1	2	3	4	5	6	7	8	9
5	25	25–30	25–30	19–25*					
6	25^a	25–51	25–51	19–25	15–25*				
7	29–34	25–66	25–81	19–57^{t6}	25–34	12–15*			
8	33–40	29–75	25–88	19–65^{t6}	22–65^{t6}	26–40	10*		
9	37–43	33–83	25–130	21–73^{t6}	22–73^{t6}	26–65	25–43	8–10*	
10	41–45	37–114	25–177	21–81^{t6}	22–81^{t6}	26–81^{t6}	25–49	25–45	7*

Авторы благодарят рецензента за подробные и вдумчивые замечания относительно первоначальной версии настоящей статьи, а также Г. Кабатянского за полезные обсуждения, касающиеся рассматриваемых кодов.

СПИСОК ЛИТЕРАТУРЫ

1. *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, Russia. Sept. 2–8, 2018. P. 40–45. Available at `https://www.dropbox.com/s/h7u89lh8vyirww9/Proceedings\%20final.pdf?dl=0`.
2. *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.
3. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44.
4. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Об m-квазиразрешимых блок-схемах и q-ичных равновесных кодах // Пробл. передачи информ. 2018. Т. 54. № 3. С. 54–61.
5. *Бассалыго Л.А., Зиновьев В.А.* Замечание об уравновешенных неполных блок-схемах, почти разрешимых блок-схемах и q-ичных равновесных кодах // Пробл. передачи информ. 2017. Т. 53. № 1. С. 55–59.
6. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87.
7. *Beth T., Jungnickel D., Lenz H.*, Design Theory. Cambridge: Cambridge Univ. Press, 1986.
8. *Богданова Г.Т., Зиновьев В.А., Тодоров Т.Й.* О построении q-ичных эквидистантных кодов // Пробл. передачи информ. 2007. Т. 43. № 4. С. 13–36.
9. *Calderbank R., Kantor W.M.* The Geometry of Two-Weight Codes // Bull. London Math. Soc. 1986. V. 18. № 2. P. 97–122.
10. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10.
11. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. № 1. С. 38–50.
12. *Боржес Ж., Рифа Ж., Зиновьев В.А.* О полностью регулярных кодах // Пробл. передачи информ. 2019. Т. 55. № 1. С. 3–50.
13. *Barg A., Musin O.* Bounds on Sets with Few Distances // J. Combin. Theory Ser. A. 2011. V. 118. № 4. P. 1465–1474.
14. *Levenshtein V.I.* Krawtchouk Polynomials and Universal Bounds for Codes and Designs in Hamming Spaces // IEEE Trans. Inform. Theory. 1995. V. 41. № 5. P. 1303–1321.
15. *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.
16. *Neumaier A.* Distance Matrices, Dimension, and Conference Graphs // Nederl. Akad. Wetensch. Indag. Math. 1981. V. 43. № 4. P. 385–391.
17. *Brouwer A.E.* Tables of Bounds for q-ary Codes. Published electronically at `www.win.tue.nl/~aeb/`.

Бойваленков Петър
Институт математики и информатики
Болгарской академии наук, София, Болгария
Юго-западный университет, Благоевград, Болгария,
технический факультет
peter@math.bas.bg
Делчев Константин
Институт математики и информатики
Болгарской академии наук, София, Болгария
math_k_delchev@yahoo.com
Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
zinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
29.05.2019
После доработки
27.10.2019
Принята к публикации
29.11.2019