S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 7, стр. 425–434 (2010) УДК 519.72
MSC 94B25

О РАЗБИЕНИЯХ ПРОСТРАНСТВА F_q^N НА АФФИННО НЕЭКВИВАЛЕНТНЫЕ СОВЕРШЕННЫЕ q-ЗНАЧНЫЕ КОДЫ

А. В. ЛОСЬ, Ф. И. СОЛОВЬЕВА

Abstract. It is proved that there exists a partition of the set F_q^N of all q-ary vectors of length N into pairwise affine nonequivalent perfect q-ary codes of length N with the Hamming distance 3 for any $N = (q^m - 1)/(q - 1)$, where $q = p^r$, p is prime.

Keywords: perfect q-ary code, partition into perfect codes, switching, affine nonequivalence of codes.

1. Введение

Данная работа посвящена построению разбиения N-мерного векторного пространства F_q^N над полем Галуа $GF(q)$, по отношению к метрике Хэмминга, на попарно аффинно неэквивалентные совершенные q-значные коды длины N с кодовым расстоянием 3. Здесь и далее $N = (q^m - 1)/(q - 1)$, $q = p^r$, p — простое. Полученная конструкция обобщает аналогичный результат для совершенных двоичных кодов из [1]. Проблема перечисления всех разбиений пространства F_q^N на совершенные q-значные коды тесно связана с классической проблемой классификации всех совершенных q-значных кодов. Конструкции разбиений пространств на коды могут быть использованы для построения новых q-значных кодов с хорошими свойствами, в том числе совершенных. Например, в [2], гл. 11, приведено несколько конструкций совершенных q-значных кодов, использующих разбиения пространств на коды.

Напомним необходимые определения. Расстояние Хэмминга между двумя произвольными векторами пространства равно числу координат, в которых

Los', A.V., Solov'eva, F.I., On partitions into affine nonequivalent perfect q-ary codes.

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 10-01-00424-а).

Поступила 4 ноября 2010 г., опубликована 18 ноября 2010 г.

они различаются. Произвольное подмножество C пространства F_q^N называется *совершенным q-значным кодом длины N с кодовым расстоянием 3* (далее называемым *совершенным кодом*) если для любого вектора $x \in F_q^N$ существует единственный вектор y из кода C, такой что $d(x,y) \le 1$. Хорошо известно, что такой код существует только для $N = (q^m - 1)/(q-1)$, где m — любое натуральное число не меньшее двух. Код называется *линейным*, если он является линейным подпространством пространства F_q^N. Совершенный линейный q-значный код называется *кодом Хэмминга*, далее такой код длины N будем обозначать через $\mathcal{H}$. Два кода $C, C' \subset F_q^N$ называются *изоморфными*, если существует перестановка π на N координатах, такая что $C' = \pi(C)$. Два кода называются *эквивалентными*, если существует изометрия пространства F_q^N, отображающая один код в другой. Если такая изометрия является перестановкой координатных позиций в композиции со сдвигом на некоторый вектор пространства F_q^N, то коды назовем *аффинно эквивалентными*. Следует отметить, что при $q = 3$ определения эквивалентности и аффинной эквивалентности совпадают. Код будем называть *приведенным*, если он содержит вектор $\mathbf{0}$, состоящий из одних нулей. Код Хэмминга единственен с точностью до изоморфизма и по определению является приведенным. Всюду далее $N = qn + 1$, $n = (q^{m-1} - 1)/(q-1)$ и $m \ge 2$.

2. Нелинейность совершенных q-значных кодов

Пусть R — некоторое подмножество совершенного кода C и R' — множество векторов, полученное действием некоторой нетождественной перестановки на элементах от 0 до $q-1$ в i-й позиции кодовых слов множества R. Множество R называется *i-компонентой* совершенного кода C, если множество $C' = (C \backslash R) \cup (R')$ является совершенным кодом. Будем говорить, что код C' получен из кода C *свитчингом* i-компоненты R.

Рассмотрим q-значный код Хэмминга $\mathcal{H}$ длины $N = nq + 1$, $n = (q^{m-1} - 1)/(q-1)$. Кодовое слово веса 3 будем называть *тройкой*. Подпространство, порожденное совокупностью троек кода $\mathcal{H}$ с единичной i-й координатой, обозначим через R_i. Известно [4], что множество R_i является i-компонентой и его мощность равна $q^{n(q-1)}$.

Проверочная матрица q-значного кода Хэмминга $\mathcal{H}$ длины N состоит из N попарно линейно независимых столбцов пространства F_q^m. С помощью кода Хэмминга $\mathcal{H}$ можно построить конечную $(m-1)$-мерную проективную геометрию $PG(m-1, q)$ над полем $GF(q)$. В этой геометрии точкам соответствуют столбцы проверочной матрицы кода $\mathcal{H}$ и три точки лежат на одной прямой, если соответствующие им столбцы являются линейно зависимыми. Через любые две различные точки $a = (a_1, a_2, \ldots, a_m)$ и $b = (b_1, b_2, \ldots, b_m)$ проходит только одна прямая (ab), состоящая из точек вида $\beta a + \gamma b$, где β, γ из $GF(q)$ и не равны одновременно нулю. Прямая состоит из $q+1$ точек, так как всего имеется $q^2 - 1$ возможностей выбора ненулевой пары (β, γ) и каждой точке соответствует $q-1$ попарно линейно зависимых пар, см., например, [5].

В проективной геометрии каждой i-компоненте R_i из кода $\mathcal{H}$ соответствуют прямые, проходящие через точку i, см. [4]. Каждая такая прямая задает некоторый подкод $\mathcal{H}_l$, его база состоит из $q-1$ троек кода Хэмминга вида

$$T_s = e_i + s \cdot e_j + a_s \cdot e_{k_s}, \qquad s \in F^0, \tag{1}$$

где F^0 — ненулевые элементы поля $GF(q)$, $j = j(l)$ и паре элементов $1, s$, стоящих в i-й, j-й позициях вектора веса 3 кода $\mathcal{H}$ соответственно отвечает в силу плотной упакованности кода Хэмминга единственный элемент $a_s \in F^0$, стоящий на позиции с номером k_s. Таким образом координаты $i, j, k_1, k_2, \ldots, k_{q-1}$ соответствуют $q+1$ точкам прямой L в проективной геометрии $PG(m-1, q)$. Другими словами, носители кодовых слов такого подкода $\mathcal{H}_l$ будут содержаться в соответствующей подкоду прямой L в проективной геометрии $PG(m-1, q)$. Поскольку через одну точку проходит n прямых, то база компоненты R_i является объединением баз $\mathcal{B}(\mathcal{H}_i)$ соответствующих подкодов $\mathcal{H}_i$, то есть

$$R_i =< \mathcal{B}(\mathcal{H}_1) \cup \mathcal{B}(\mathcal{H}_2) \cup \cdots \cup \mathcal{B}(\mathcal{H}_n) > . \tag{2}$$

Введем понятие степени нелинейности кода. Для кодов, построенных из исходного q-значного кода Хэмминга методом сдвига компонент, несложно вычислить как и в двоичном случае, см. [1], степень нелинейности. Данное свойство является инвариантом при исследовании вопроса об эквивалентности двух совершенных q-значных кодов. Отметим, что в общем случае степень нелинейности кода установить не просто.

Обозначим через $\mathcal{H}_q(N)$ совокупность кодов вида $\mathcal{H}+\beta\cdot e_i$ длины N, где $\mathcal{H}$ — код Хэмминга, $\beta \in F_q$, а e_i — вектор, содержащий в единственной ненулевой i-й координате единицу. Для произвольного совершенного q-значного кода C длины N определим величину

$$\mathcal{NL}(C) = \min_{\mathcal{H}\in\mathcal{H}_q(N)} d(C, \mathcal{H}), \tag{3}$$

называемую *степенью нелинейности* совершенного q-значного кода C, где $d(C, \mathcal{H})$ — расстояние между множествами C и $\mathcal{H}$:

$$d(C, \mathcal{H}) = \frac{1}{2}(|\, C| + |\, \mathcal{H}|) - |\, C \cap \mathcal{H}|. \tag{4}$$

Полагая $q = 2$, получим определение степени нелинейности для двоичного случая, введенное в работе [1].

Нетрудно убедиться в справедливости следующего утверждения.

Лемма 1. *Если для двух совершенных q-значных кодов C_1 и C_2 выполняется*

$$\mathcal{NL}(C_1) \neq \mathcal{NL}(C_2),$$

то эти коды аффинно неэквивалентны.

Лемма 2. *Мощность пересечения произвольного q-значного кода Хэмминга $\mathcal{H}$ и любого отличного от него аффинно эквивалентного ему кода не превосходит $|\mathcal{H}|/q$.*

Доказательство. Рассмотрим произвольный код Хэмминга $\mathcal{H}$ и аффинно эквивалентный ему код $\mathcal{H}' + \beta \cdot e_i$, где $\mathcal{H}'$ — некоторый код Хэмминга отличный от $\mathcal{H}$, $\beta \in F_q$ и $i \in \{1, 2, \ldots, N\}$.

Для некоторого фиксированного вектора $x \in \mathcal{H} \cap (\mathcal{H}' + \beta \cdot e_i)$ рассмотрим произвольный вектор $y \in \mathcal{H} \cap (\mathcal{H}' + \beta \cdot e_i)$. Очевидно, что их сумма $x+y$ принадлежит коду $\mathcal{H}$, так как $\mathcal{H}$ — код Хэмминга — линейное подпространство в F_q^N. С другой стороны, векторы x и y принадлежат $\mathcal{H}' + \beta \cdot e_i$, то есть $x = x' + \beta \cdot e_i$ и $y = y' + \beta \cdot e_i$ для некоторых $x', y' \in \mathcal{H}'$. Отсюда

$$x + y = x' + y' + \beta \cdot e_i + \beta \cdot e_i = x' + y' + \gamma \cdot e_i,$$

где $\gamma = \beta + \beta \in F_q$ и $\gamma = \beta$ тогда и только тогда, когда $\beta = 0$. Следовательно, $x + y \notin \mathcal{H}' + \beta \cdot e_i$, то есть $x + y \in \mathcal{H} \setminus (\mathcal{H} \cap (\mathcal{H}' + \beta \cdot e_i))$, а значит

$$|\mathcal{H} \setminus (\mathcal{H} \cap (\mathcal{H}' + \beta \cdot e_i))| \geq |\mathcal{H} \cap (\mathcal{H}' + \beta \cdot e_i)|.$$

Поскольку β — произвольный элемент из F_q, отсюда получаем

$$|\mathcal{H} \cap (\mathcal{H}' + \beta \cdot e_i)| \leq \mathcal{H}/q. \qquad \square$$

Лемма 3. *Для произвольного совершенного q-значного кода C длины N справедливо*

$$0 \leq \mathcal{NL}(C) \leq \frac{N(q-1)}{N(q-1)+1} |\, C|.$$

Доказательство. Нижняя оценка очевидна. Докажем верхнюю оценку. Рассмотрим разбиение пространства F_q^N на q-значный код Хэмминга $\mathcal{H}$ длины N и его смежные классы $\mathcal{H}_i^\beta = \mathcal{H} + \beta \cdot e_i$:

$$F_q^N = \mathcal{H} \cup \bigcup_{i=1}^{N} \bigcup_{\beta \in F^0} \mathcal{H}_i^\beta. \tag{5}$$

Для любого совершенного q-значного кода C найдутся такие $i \in \{1, 2, \ldots, N\}$ и элемент β из F_q, что выполняется

$$|\, C \cap \mathcal{H}_i^\beta| \geq \frac{1}{N(q-1)+1} |\, C|.$$

Отсюда, используя определение (4), а также тот факт, что $|\, C| = |\, \mathcal{H}|$, получаем

$$d(C, \mathcal{H}_i^\beta) = |\, C| - |\, C \cap \mathcal{H}_i^\beta| \leq \frac{N(q-1)}{N(q-1)+1} |\, C|. \qquad \square$$

Рассмотрим семейство $\mathcal{F} = \{R_{i_1}, R_{i_2}, \ldots, R_{i_t}\}$ попарно непересекающихся линейных i_s-компонент q-значного кода Хэмминга $\mathcal{H}$, $s = 1, 2, \ldots, t$. Заметим, что в множестве $\{i_1, i_2, \ldots, i_t\}$ необязательно все элементы являются различными. Следуя [1], обозначим через $S_{\mathcal{F}}(\mathcal{H})$ код, полученный из кода $\mathcal{H}$ сдвигами компонент семейства $\mathcal{F}$:

$$S_{\mathcal{F}}(\mathcal{H}) = \left(\mathcal{H} \setminus \bigcup_{s=1}^{t} R_{i_s}\right) \bigcup \left(\bigcup_{s=1}^{t} R_{i_s} + \beta_s e_{i_s}\right). \tag{6}$$

Обозначим через $T = |\, \mathcal{H}|/|R_i|$ максимальное число попарно непересекающихся линейных компонент в коде $\mathcal{H}$. Иначе говоря, T — число смежных классов в коде Хэмминга $\mathcal{H}$ по линейной компоненте R_i, являющейся по определению линейным подпространством. Для кода Хэмминга длины $N = \frac{q^m - 1}{q-1} = qn + 1$ справедливо $|\, \mathcal{H}| = q^{N-m}$, $|\, R_i| = q^{(q-1)n}$ и, следовательно, выполняется $T = q^{n-m+1}$.

Лемма 4. *Пусть T — максимальное число попарно непересекающихся линейных компонент в коде Хэмминга $\mathcal{H}$ и $t \leq \frac{(q-1)}{2q} T$, тогда выполняется*

$$\mathcal{NL}(S_{\mathcal{F}}(\mathcal{H})) = t |\, R_i|.$$

Доказательство. Используя определения (4) и (6), нетрудно проверить выполнение

$$d(S_{\mathcal{F}}(\mathcal{H}), \mathcal{H}) = t |\, R_i|.$$

Пусть найдется такой класс смежности $\mathcal{H}' \in \mathcal{H}_q(N)$ некоторого кода Хэмминга, что $\mathcal{H}' \neq \mathcal{H}$ и $d(S_{\mathcal{F}}(\mathcal{H}), \mathcal{H}') < t|\,R_i|$. Тогда $|\,\mathcal{H} \cap \mathcal{H}'| > |S_{\mathcal{F}}(\mathcal{H})| - 2t|R_i| \geq |\,\mathcal{H}|/q$, что противоречит лемме 2, согласно которой любые два различных класса смежности некоторых кодов Хэмминга пересекаются не более чем по $|\mathcal{H}|/q$ кодовым словам. □

Следствие 1. *Если* $\mathcal{NL}(C) < \frac{(q-1)}{2q}|\,C|$, *то код из семейства кодов* $\mathcal{H}_q(N)$, *ближайший к коду* C, *определяется однозначно.*

3. Конструкция разбиений на аффинно неэквивалентные совершенные q-значные коды

В настоящем параграфе приведена конструкция разбиений пространства F_q^N на аффинно неэквивалентные совершенные q-значные коды длины N. Построение начинается с тривиального разбиения (5) пространства F_q^N на классы смежности некоторого кода Хэмминга. В таком разбиении выделяются подмножества кодов, для которых предложены способы осуществления попарных обменов компонентами между кодами одного подмножества так, что в каждом коде этого подмножества производится различное число сдвигов компонент. Метод сдвига компонент линейного кода развит в работах [6,7,8]. Кроме того, описана возможность внесения в любое из таких подмножеств кодов так называемых циклических свитчингов компонент с той целью, чтобы в каждом коде этого подмножества можно было нарастить количество преобразованных компонент на одно и то же число. Цель всех этих преобразований заключается в том, чтобы из исходного разбиения пространства на классы смежности кода Хэмминга построить разбиение на коды с различным числом преобразованных компонент и при этом минимизировать число преобразований так, чтобы даже для максимально преобразованного кода ближайшим к нему из множества кодов $\mathcal{H}_q(N)$ остался исходный код тривиального разбиения. Что в результате позволяет легко определять степень нелинейности кодов полученного разбиения.

Рассмотрим пространство F_q^m всех q-значных вектор-столбцов длины m, упорядочим их лексикографически, пронумеруем от 0 до $N(q-1) = q^m - 1$ и обозначим i-й столбец через M_i. Очевидно, что каждому ненулевому столбцу M_i можно однозначно сопоставить столбец h_j проверочной матрицы H кода $\mathcal{H}$, такой что $M_i = \alpha_j \cdot h_j$ для некоторого элемента α_j поля $GF(q)$. Определим с помощью равенств $M_i = \alpha_j \cdot h_j$ функцию $f : M_i \to \alpha_j \cdot e_j$, где $f(M_0) = \mathbf{0}$. Пусть столбцы проверочной матрицы H также будут упорядочены лексикографически, и пусть L — прямая в проективной геометрии $PG(m-1, q)$, состоящая из $q+1$ точек, которым без ограничения общности соответствуют первые $q+1$ столбцов проверочной матрицы кода $\mathcal{H}$. Рассмотрим следующее объединение из $q^2 = (q+1)(q-1)+1$ кодов:

$$U = \mathcal{H} \cup \bigcup_{i=1}^{q+1} \bigcup_{\beta \in F^0} \mathcal{H}_i^{\beta},$$

где $\mathcal{H}_i^{\beta} = \mathcal{H} + \beta e_i$. Напомним, что F^0 — множество ненулевых элементов поля $GF(q)$. Подчеркнем, что объединение U в свою очередь является кодом, а любые два слагаемых в этом объединении не пересекаются. С целью облегчить

изложение в дальнейшем данный код U и его смежные классы будем рассматривать как объединение непересекающихся кодов, а именно кодов, аффинно эквивалентных коду Хэмминга. Нетрудно заметить, что здесь использованные $q+1$ координатных позиций соответствуют первым $q+1$ столбцам проверочной матрицы H и, соответственно, прямой L в проективной геометрии $PG(m-1,q)$. Если вместе с этими координатными позициями учесть ненулевые элементы поля, то кодам из объединения U соответствуют первые q^2 упорядоченных столбцов пространства F_q^m, образующие подпространство V. Профакторизуем пространство F_q^m по выбранному подпространству V и выберем представителей классов смежности v_k так, чтобы индекс k был минимальным. В таком случае представителем исходного пространства V будет нулевой столбец. Заметим, что описанным выше способом в качестве представителей классов смежности будут выбраны столбцы с номерами $k = sq^2 + 1$, $s \in \{0, \dots, q^{m-2} - 1\}$.

Рассмотрим следующее объединение

$$W = \bigcup_{s=0}^{q^{m-2}-1} (U + f(v_k)), \tag{7}$$

где $k = sq^2 + 1$, а v_k — лидер класса смежности пространства F_q^m по подпространству V.

Лемма 5. *Коды объединения W задают разбиение пространства F_q^N на совершенные q-значные коды.*

Доказательство. Покажем, что никакие два кода объединения (7) не пересекаются. Пустота пересечения произвольной пары кодов внутри одного объединения $U + f(v_k)$ очевидна.

Рассмотрим два произвольных кода $C_1 = \mathcal{H}_i^\beta + f(v_k)$ и $C_2 = \mathcal{H}_j^\gamma + f(v_t)$ из разных объединений $U + f(v_k)$ и $U + f(v_t)$. Преобразуем пространство F_q^N добавлением вектора $-\gamma e_j$ ко всем векторам. А также, не теряя общности, положим, что $f(v_t) = 0$. Тогда коды будут иметь вид: $C_1 - \gamma e_j = \mathcal{H} + \beta e_i - \gamma e_j + f(v_k)$ и $C_2 - \gamma e_j = \mathcal{H}$. Пусть $f(v_k) = \delta e_{k'}$. Поскольку точки i и j принадлежат прямой L в проективной геометрии $PG(m-1,q)$, а точка k' не принадлежит, то коду Хэмминга не принадлежит вектор веса 3 с ненулевыми позициями i, j и k'. Следовательно код $C_1 - \gamma e_j$ является смежным классом кода $C_2 - \gamma e_j$, то есть они не пересекаются также как и коды C_1 и C_2.

Остается убедиться, что общее количество векторов равно $|F_q^N| = q^N$. Действительно,

$$q^{m-2} \cdot q^2 \cdot |\mathcal{H}| = q^m \cdot q^{N-m} = q^N. \qquad \square$$

Лемма 6. *Для любой пары кодов объединения U существует обмен компонентами с помощью свитчингов по одному из направлений, соответствующих точкам прямой $L \subset PG(m-1,q)$, такой что объединение преобразованных кодов совпадает с объединением исходных.*

Доказательство. Рассмотрим произвольную пару кодов C_1 и C_2 объединения U. Возможны два случая.

Случай 1. При $C_1 = \mathcal{H}_i^\alpha$ и $C_2 = \mathcal{H}_i^\beta$ таким обменом является свитчинг компоненты $R_i + \alpha e_i$ на элемент $\beta - \alpha$ для первого кода и компоненты $R_i + \beta e_i$ на элемент $\alpha - \beta$ для второго, то есть

$$C_1' = (\mathcal{H}_i^\alpha \setminus (R_i + \alpha e_i)) \cup ((R_i + \alpha e_i) + (\beta - \alpha) e_i),$$

$$C_2' = (\mathcal{H}_i^\beta \setminus (R_i + \beta e_i)) \cup ((R_i + \beta e_i) + (\alpha - \beta)e_i).$$

Случай 2. При $C_1 = \mathcal{H}_i^\alpha$ и $C_2 = \mathcal{H}_j^\beta$ необходимым обменом будет являться свитчинг компоненты $R_k + \alpha e_i$ на элемент γ для первого кода и компоненты $R_k + \beta e_j$ на элемент $-\gamma$ для второго, где $k \in L$ и $\gamma \in F^0$ такие, что тройка $\alpha e_i - \beta e_j + \gamma e_k$ принадлежит коду Хэмминга $\mathcal{H}$. При помощи таких свитчингов получим коды

$$C_1' = (\mathcal{H}_i^\alpha \setminus (R_k + \alpha e_i)) \cup ((R_k + \alpha e_i) + \gamma e_k) = (\mathcal{H}_i^\alpha \setminus (R_k + \alpha e_i)) \cup (R_k + \beta e_j),$$

$$C_2' = (\mathcal{H}_j^\beta \setminus (R_k + \beta e_j)) \cup ((R_k + \beta e_j) - \gamma e_k) = (\mathcal{H}_j^\beta \setminus (R_k + \beta e_j)) \cup (R_k + \alpha e_i).$$

Очевидно, что объединение кодов C_1 и C_2 после действия указанных преобразований не изменяется, поскольку объединение кодов C_1' и C_2' состоит из тех же самых подмножеств. □

Если в обмене компонентами участвует множество A, состоящее из не менее чем трех кодов, и при этом нельзя выделить подмножество кодов из множества A так, чтобы свитчинг их компонент оставался обменом, то такой обмен будем называть *циклическим свитчингом длины* $|A|$. Всюду в определениях обмена компонентами подразумевается, что в каждом коде, принимающем участие в обмене, сдвигается только одна компонента. Таким образом, чтобы в каждом коде множества A можно было преобразовать одинаковое число компонент, достаточно осуществить требуемое количество циклических свитчингов длины $|A|$.

Следствие 2. *Для фиксированного $i \in L$ и любого числа классов смежности кода Хэмминга вида $\mathcal{H}_i^\alpha$, $\alpha \in GF(q)$ существует циклический обмен компонентами с помощью свитчингов i-компонент.*

Доказательство непосредственно следует из случая 1 доказательства леммы 6, где аналогичным способом может быть осуществлен циклический свитчинг компонент необходимого числа кодов от 2 до q. □

Следующая лемма с целью облегчения изложения сформулирована в терминах взвешенных цепей, вершины которых отождествляются с кодами, а ребра соединяют вершины, если соответствующие вершинам коды участвуют в обмене компонентами. Кроме того, вес вершины будет обозначать количество компонент данного кода, участвующих в обменах, а вес ребра — сколькими компонентами обменялись соответствующие коды. Таким образом, данная терминология используется только для описания схемы последующих преобразований компонент кодов исходного разбиения (5) пространства F_q^N.

Лемма 7. *Для любого целого $t > 0$ существует цепь из $4t-1$ вершин с весами вершин от 1 до $4t-1$ и весами ребер из множества $\{1, 2, \ldots, 4t-1\}$, такая что вес любой вершины равен сумме весов инцидентных ей ребер.*

Доказательство. Очевидно, что порядок вхождения вершин в цепь определит ее однозначно. Поскольку вес каждого ребра дает свой вклад в вес двух вершин, то сумма весов вершин должна быть четна. Действительно сумма весов вершин от 1 до $4t-1$ является четной:

$$\frac{1 + (4t-1)}{2}(4t-1) = 2t(4t-1).$$

Рассмотрим цепь из вершин всех весов от 1 до $2t-1$, которые будут следовать в порядке возрастания их весов, из оставшихся вершин с весами от $2t$ до $4t-1$

также построим цепь в порядке возрастания весов вершин. Покажем, что если при соответствующей нумерации ребер соединить концы этих цепей, то есть вершины с весами $2t-1$ и $4t-1$, то получим цепь с необходимыми свойствами. Для этого пронумеруем, начиная с единицы, ребра обеих цепей и отметим, что вес ребра первой цепи с номером $2s-1$ или $2s$ равен s, а вес ребра второй цепи с номером $2w-1$ равен $((4t-1)-1)/2+w = 2t-1+w$ и с номером $2w$ равен w. Если добавить ребро между вершинами с весами $2t-1$ и $4t-1$, то в первой цепи оно должно иметь номер $2t-1$ и, следовательно, вес t, а во второй цепи — номер $2t$ и, следовательно, вес t, см. рис. 1. Так как при распределении

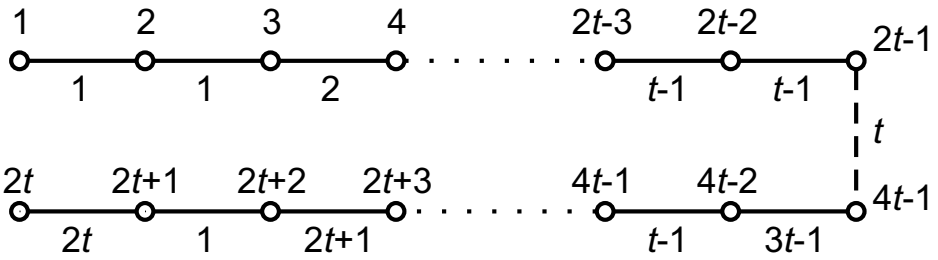

Рис. 1. Соединение двух цепей.

весов ребер с двух концов цепи вес соединительного ребра совпал, то такая цепь полностью отвечает заявленным условиям. □

Теорема 1. *Для всех $N = (q^m-1)/(q-1)$, $q = p^r > 2$, $m \geq 4$ существует разбиение пространства F_q^N на попарно аффинно неэквивалентные совершенные q-значные коды длины N.*

Доказательство. Искомое разбиение будем строить, исходя из разбиения W пространства F_q^N на смежные классы кода Хэмминга $\mathcal{H}$.

Рассмотрим коды объединения U и покажем, что с помощью попарных обменов компонентами можно построить коды D_s, имеющие различное число $s \in \{0, \ldots, q^2-1\}$ сдвинутых компонент. Упорядочим произвольным образом все q^2 кодов объединения U и обозначим их через C_s, $s \in \{0, 1, \ldots, q^2-1\}$. Построим для каждого кода C_s с помощью свитчингов некоторых его компонент код D_s. Для этого рассмотрим следующие 4 случая :

Случай 1. Если $q = 4t+2$, то конечное поле $GF(q)$ существует только при $t = 0$, то есть $q = 2$. Задача разбиения пространства F_2^N на попарно неэквивалентные совершенные двоичные коды решена в [1].

Случай 2. Если $q = 4t-1$, то $q+1$ координатных позиций, соответствующих точкам прямой L, можно разбить на четверки равно как и $q^2-1 = (q+1)(q-1)$ кодов объединения U (без кода $C_0 = D_0$) разбиваются на четверки кодов $\mathcal{H}_{i_l}^{\alpha_l}$ для некоторых $\alpha_l \in GF(q)$ и различных $i_l \in L$, $l = 1, 2, 3, 4$. Между кодами такой четверки и вершинами цепи длины 4 установим соответствие, такое что вес вершины будет равен числу сдвинутых компонент соответствующего кода, а вес ребра будет равен числу обменов компонентами кодов, соответствующих инцидентным вершинам. Очевидно, что в таком случае вес вершины должен совпадать с суммой весов инцидентных ей ребер.

Рассмотрим для каждого $s = 0, 1, \ldots, (q^2-1)/4-1$ цепи с вершинами весов $4s+1$, $4s+3$, $4s+4$ и $4s+2$, расположенных в порядке следования, и тремя ребрами, соединяющими эти вершины в указанном выше порядке, то есть с весами $4s+1$, 2 и $4s+2$. Нетрудно заметить, что в совокупности для всех $s = 0, 1, \ldots, (q^2-1)/4-1$ такие цепи отвечают описанным выше условиям и дают вершины всех различных весов от 1 до q^2-1.

Поскольку в четверках кодов вида $\mathcal{H}_{i_l}^{\alpha_l}$ все индексы i_l различны, то компоненты этих кодов будем обменивать с помощью свитчингов компонент согласно случаю 2 доказательства леммы 6 по схеме, заданной построенными цепями.

Случай 3. При $q = 4t+1$ множество из q^2-1 кодов объединения U (без кода $C_0 = D_0$) можно представить в виде объединений по $q-1$ смежных классов кода $\mathcal{H}$, отвечающих одному параллельному классу, которые также допускают разбиения на четверки смежных классов кода $\mathcal{H}$. Как и в предыдущем случае цепи длины 4 задают необходимые обмены компонентами с тем лишь отличием, что тип свитчингов компонент описан в случае 1 доказательства леммы 6.

Случай 4. При $q = 4t$, то есть $q = 2^r, r > 1$ необходимая схема обменов дана в доказательстве леммы 7, при этом используются свитчинги компонент всех типов.

Таким образом, построены q^2 кодов D_s, $s \in \{0, 1, \ldots, q^2-1\}$, таких что их объединение D совпадает с объединением U.

Заметим, что согласно следствию 2 внутри полученного объединения D можно устроить циклические обмены длины $q-1$ (то есть между $q-1$ кодами) компонент кодов по любой из q координатных позиций, отвечающих прямой L. Кроме того, по оставшейся $(q+1)$-й координате осуществляется циклический сдвиг длины q, то есть вместе с кодом D_0. Причем число таких циклических обменов может быть произвольным и ограничено только максимальным числом T непересекающихся компонент исходного кода Хэмминга $\mathcal{H}$. Тогда из объединения D, наращивая число циклических сдвигов на значение sq^2, $s = 0, 1, \ldots, q^{m-2}-1$, получим объединения D^s, такие что как совокупности векторов пространства F_q^N они будут совпадать с объединением U. Следовательно, согласно лемме 5, объединение

$$\bigcup_{s=0}^{q^{m-2}-1} (D^s + f(v_k)), \qquad k = sq^2 + 1,$$

является разбиением пространства F_q^N на совершенные q-значные коды D_t длины N, $t = 0, 1, \ldots, q^m-1$. По условию теоремы имеем $m \geq 4$, откуда следует, что $q^m < \frac{q-1}{2q} T$, где T — максимальное число попарно непересекающихся компонент кода Хэмминга длины N. Но поскольку $t < q^m$, то согласно лемме 4 степень нелинейности $\mathcal{NL}(D_t)$ кодов D_t равна $t|\,R_i\,|$ и по лемме 1 все коды D_t попарно аффинно неэквивалентны.

Заметим, что при $m = 3$ теорема справедлива для всех $q > 4$, а при $m \geq 5$ верна и для двоичных кодов, см. [1]. $\square$

В заключение отметим, что интерес также представляет изучение свойства сильной степени нелинейности кодов, где в отличии от определения (3) в качестве семейства кодов $\mathcal{H}_q(N)$ рассматривается совокупность всех кодов, эквивалентных коду Хэмминга. Зная минимальное расстояние между двумя кодами, эквивалентными коду Хэмминга, изложенная выше конструкция, как полагают

авторы, позволит построить разбиение пространства F_q^N на попарно неэквивалентные совершенные q-значные коды длины N.

Авторы выражают благодарность С. В. Августиновичу за ценные замечания.

Список литературы

[1] Августинович С. В., Соловьева Ф. И., Хеден У., *О разбиениях n-куба на неэквивалентные совершенные коды*, Пробл. передачи информ. **43**: 4 (2007), 45–50.
[2] Cohen G., Honkala I., Lobstein A., Litsyn S., *Covering codes*, Elsevier, 1998.
[3] Schönheim J., *On linear and nonlinear single-error-correcting q-nary 1 perfect codes*, Inform. Control. **12** (1986), 23–26.
[4] Phelps K. T., Villanueva M., *Ranks of q-ary 1 perfect codes*, Des. Codes Cryptogr. **27** (2002), 139–144.
[5] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А., *Теория кодов, исправляющих ошибки*, М: 1979.
[6] Августинович С. В., Соловьева Ф. И., *Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент*, Пробл. передачи информ. **33**: 3 (1997), 15–21.
[7] Лось А. В., *Построение совершенных q-значных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент*, Пробл. передачи информ. **40**: 1 (2004), 33–39.
[8] Лось А. В., *Построение совершенных q-значных кодов свитчингами простых компонент*, Пробл. передачи информ. **42**: 1 (2006), 34–42.

Антон Васильевич Лось
Институт математики им. С. Л. Соболева СО РАН,
пр. академика Коптюга 4,
Новосибирский государственный университет,
ул. Пирогова, 2,
630090, Новосибирск, Россия
E-mail address: sozercatel@gmail.com

Фаина Ивановна Соловьева
Институт математики им. С. Л. Соболева СО РАН,
пр. академика Коптюга 4,
Новосибирский государственный университет,
ул. Пирогова, 2,
630090, Новосибирск, Россия
E-mail address: sol@math.nsc.ru