Сибирский математический журнал
Март—апрель, 2008. Том 49, № 2

УДК 519.725

О ПЕРЕСЕЧЕНИЯХ q–ЗНАЧНЫХ СОВЕРШЕННЫХ КОДОВ

Ф. И. Соловьева, А. В. Лось

Аннотация. Исследуются пересечения q-значных совершенных кодов. Доказано, что существуют два q-значных совершенных кода C_1 и C_2 длины $N = qn+1$ такие, что $| C_1 \cap C_2 | = k \cdot |P_i|/p$ для каждого $k \in \{0, \dots, p \cdot K - 2, p \cdot K\}$, где $q = p^r$, p простое, $r \geq 1$, $n = \frac{q^{m-1}-1}{q-1}$, $m \geq 2$, $|P_i| = p^{nr(q-2)+n}$, $K = p^{n(2r-1)-r(m-1)}$. Показано, что существуют два q-значных совершенных кода длины N, пересекающиеся по $p^{nr(q-3)+n}$ кодовым словам.

Ключевые слова: совершенные q-значные коды, пересечение кодов, метод свитчинга компонент, код Хэмминга.

§ 1. Введение

Работа посвящена исследованию проблемы пересечения q-значных совершенных кодов: *какие возможны мощности пересечения $\eta(C_1, C_2)$ двух совершенных кодов C_1 и C_2 длины N?* Этот вопрос впервые сформулирован Этционом и Варди в работе [1]. Они предложили полное решение проблемы пересечения двоичных кодов Хэмминга, нашли наименьшее пересечение для совершенных двоичных кодов любой допустимой длины, которое состоит из двух кодовых слов, а также получили возможные пересечения совершенных двоичных кодов, используя свитчинги i-компонент двоичных кодов Хэмминга (см. [1]). Бар-Яшалом и Этцион решили проблему пересечения для любых необязательно совершенных q-значных циклических кодов (см. [2]), $q \geq 2$.

В статье [3] установлено, что для любых двух чисел k_1 и k_2 таких, что

$$1 \leq k_i \leq 2^{(n+1)/2 - \log(n+1)}, \quad i = 1, 2,$$

существуют совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geq 4$, удовлетворяющие

$$\eta(C_1, C_2) = 2k_1k_2.$$

В [4] доказано, что для всякого четного k_3, удовлетворяющего неравенствам $0 \leq k_3 \leq 2^{n+1-2\log(n+1)}$, найдутся совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geq 4$, такие, что

$$\eta(C_1, C_2) = k_3.$$

Работа первого автора выполнена при частичной финансовой поддержке Шведской Королевской академии. Работа второго автора выполнена при финансовой поддержке Фонда содействия отечественной науке, а также при частичной финансовой поддержке в рамках интеграционного проекта СО РАН № 35 «Древовидный каталог математических Интернет-ресурсов». Работа обоих авторов выполнена при частичной финансовой поддержке Новосибирского государственного университета.

Стоит заметить, что число кодовых слов в пересечении любых двух совершенных двоичных кодов всегда четно и согласно [1] удовлетворяет

$$0 \le \eta(C_1, C_2) \le 2^{n-\log(n+1)} - 2^{(n-1)/2}. \tag{1}$$

Сравнивая результаты работ [1, 3] и [4], убеждаемся, что результаты статьи [4] наилучшие возможные на сегодняшний день, покрывающие достаточно большую часть интервала (1), но не перекрывающие результатов работы [3]. Условие четности пересечения необязательно выполняется для q-значных совершенных кодов, $q > 2$, в частности, пересечение троичных кодов не всегда будет четным. Более того, существуют совершенные троичные коды Хэмминга длины 4, пересечение которых составляет единственное кодовое слово. Эти коды могут быть заданы следующими проверочными матрицами:

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}, \quad H_2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 0 \end{bmatrix}.$$

В работе [5] исследованы пересечения кодов Адамара. В статье [6] (см. также [7]) полностью изучены пересечения аддитивных (расширенных и нерасширенных) совершенных кодов, охарактеризована структура абелевых групп — пересечений таких кодов, а также приведены конструкции всех возможных кодов-пересечений этих совершенных кодов.

Приведем необходимые определения. Пусть V_q^N — векторное пространство размерности N над полем Галуа $GF(q)$, где q — степень простого числа, по отношению к метрике Хэмминга. Расстояние Хэмминга между двумя произвольными векторами пространства равно числу координат, в которых они различаются. Подмножество C пространства V_q^N называется *совершенным q-значным кодом длины N с расстоянием* 3 (далее *совершенным кодом*), если $|C| = q^{N-\log_q(qN-N+1)}$ и расстояние между любыми двумя *кодовыми словами* (так в дальнейшем будем называть элементы кода) не менее 3. Эти условия эквивалентны плотной упаковке пространства V_q^N шарами единичного радиуса с центрами в кодовых словах. Согласно широко известной теореме В. А. Зиновьева и В. К. Леонтьева, полученной независимо Титвайненом (см. [8–10]), такой код существует только для $N = (q^m - 1)/(q - 1)$, где m — любое натуральное число, не меньшее двух. Код C *линеен*, если он является подпространством V_q^N. Совершенный линейный код в пространстве V_q^N называется *кодом Хэмминга.* Будем обозначать его через $\mathcal{H}_q^N$. Два кода $C, C' \subset V_q^N$ *изоморфны*, если существует перестановка σ на N координатах такая, что $C' = \sigma(C)$. Код Хэмминга единствен с точностью до изоморфизма. Всюду далее $N = qn + 1$, $n = (q^{m-1} - 1)/(q - 1)$ и $m \ge 2$.

§ 2. Пересечение q-значных кодов Хэмминга

Согласно [11] существуют циклические q-значные коды Хэмминга для любых допустимых параметров. С другой стороны, всякий q-значный, $q \ge 2$, код Хэмминга единствен с точностью до изоморфизма, значит, существует описание этого кода в циклическом виде. Напомним, что в работе [2] была решена проблема пересечения циклических q-значных кодов. Следовательно, эта проблема решена и для q-значных кодов Хэмминга.

В настоящем параграфе приведем более короткое, чем в [2], доказательство существования возможных мощностей пересечения кодов Хэмминга. Развитая в этом параграфе для линейного q-значного кода Хэмминга техника будет существенно использована нами в следующем параграфе для исследования пересечений уже нелинейных q-значных кодов. Следует отметить, что для доказательства теоремы 1 использовались модификация и обобщение на q-значный случай идей, рассмотренных Этционом и Варди в работе [1] (см. теорему 6) для двоичных кодов Хэмминга.

Напомним, что q-значный код Хэмминга $\mathcal{H}_q^N$ может быть задан проверочной матрицей, столбцами которой являются всевозможные q-значные векторы длины m, первая ненулевая координата которых равна 1. Таким образом, любые два столбца являются линейно независимыми, и найдутся три линейно зависимых столбца, т. е. кодовое расстояние равно трем.

Теорема 1. *Для каждого $m \geq 3$ и $l = m+1, m+2, \dots, 2m$ существуют два линейных q-значных кода Хэмминга $\mathcal{H}_1$, $\mathcal{H}_2$ длины $N = \frac{q^m-1}{q-1}$ такие, что $\eta(\mathcal{H}_1, \mathcal{H}_2) = q^{N-l}$.*

Доказательство проведем индукцией по m. В качестве базы индукции при $m = 3$ имеем следующие четыре проверочные матрицы кодов Хэмминга, столбцами которых являются все ненулевые векторы длины 3 над $GF(q)$ с первым ненулевым элементом, равным 1. Нетрудно видеть, что при этом столбцы могут быть упорядочены таким образом, что последние $N - 7 = q^2 + q - 6$ столбцов у всех матриц совпадут, обозначим эту матрицу через W:

$$H_1 = \left[\begin{array}{ccccccc|c} 0 & 0 & 0 & 1 & 1 & 1 & 1 & \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & W \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & \end{array}\right]; \quad H_2 = \left[\begin{array}{ccccccc|c} 0 & 0 & 1 & 1 & 0 & 1 & 1 & \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & W \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & \end{array}\right];$$

$$H_3 = \left[\begin{array}{ccccccc|c} 0 & 0 & 1 & 1 & 0 & 1 & 1 & \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & W \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & \end{array}\right]; \quad H_4 = \left[\begin{array}{ccccccc|c} 0 & 0 & 0 & 1 & 1 & 1 & 1 & \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & W \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & \end{array}\right].$$

Проверочной матрицей для кода-пересечения $\mathcal{H}_1 \cap \mathcal{H}_2$ является матрица $H = \left[\dfrac{H_1}{H_2}\right]$. Для удобства будем, следуя [1], кратко писать $H = H_1 \parallel H_2$. Очевидно, что ранг $\operatorname{rank}(H)$ матрицы H удовлетворяет неравенству $\operatorname{rank}(H) \leq 2m$ и, следовательно, $|\mathcal{H}_1 \cap \mathcal{H}_2| \geq q^{N-2m}$. Нетрудно проверить, что $\operatorname{rank}(H_1 \parallel H_i)$ равен 6, 5 и 4 для $i = 2, 3, 4$ соответственно. Заметим, что, отбросив у матриц H_i подматрицу W, получим двоичный случай, рассмотренный в работе [1].

Положим, что для каждого $l = m, m+1, \dots, 2(m-1)$ существуют проверочные матрицы H_1' и H_2' двух кодов Хэмминга длины $n = (q^{m-1}-1)/(q-1)$ такие, что $\operatorname{rank}(H_1' \parallel H_2') = l$. Рассмотрим следующие матрицы:

$$H_1 = \left[\begin{array}{c|c|c|c|c} \mathbf{0} & H_1' & H_1' & \dots & H_1' \\ \hline 1 & 0\dots0 & 1\dots1 & \dots & q-1\dots q-1 \end{array}\right],$$

$$H_2 = \left[\begin{array}{c|c|c|c|c} \mathbf{0} & H_2' & H_2' & \dots & H_2' \\ \hline 1 & 0\dots0 & 1\dots1 & \dots & q-1\dots q-1 \end{array}\right],$$

здесь $\mathbf{0}$ является столбцом из нулей длины $m-1$. Нетрудно показать, что H_1 и H_2 являются проверочными матрицами изоморфных кодов Хэмминга длины $N = (q^m-1)/(q-1)$ и

$$\operatorname{rank}(H_1 \parallel H_2) = \operatorname{rank}(H_1' \parallel H_2') + 1 = l + 1.$$

Следовательно, все значения рангов вида $l+1 = m+1, m+2, \dots, 2m-1$ достижимы. Остается заметить, что ранг $2m$ также достигается, например, в случае, когда $\mathrm{rank}(H_1' \parallel H_2') = 2(m-1)$ и последняя строка матрицы H_2 имеет вид

$$(1 \mid 1\dots 1 \mid 0\dots 0 \mid 2\dots 2 \mid \cdots \mid q-1\dots q-1). \quad \square$$

§ 3. Пересечения q-значных нелинейных совершенных кодов

В данном параграфе предлагаются два свитчинговых способа построения нелинейных совершенных q-значных кодов, имеющих различные непустые пересечения. В п. 3.1 приведен спектр пересечения q-значных совершенных кодов, полученный сдвигами простых компонент. В п. 3.2 описана модификация конструкции Шонхейма из [12], позволяющая получить два совершенных q-значных кода, пересечение которых меньше, чем минимальное непустое пересечение совершенных кодов, достигаемое сдвигами простых компонент.

3.1. Пересечения q-значных совершенных кодов, построенных свитчингами простых компонент. 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 $\mathcal{H}_q^N$ длины $N = nq+1$, где $n = (q^{m-1}-1)/(q-1)$, в свою очередь, является длиной кода Хэмминга $\mathcal{H}_q^n$. Кодовое слово веса 3 будем называть *тройкой*. Подпространство, порожденное совокупностью троек кода $\mathcal{H}_q^N$ с единичной i-й координатой, обозначим через R_i. Известно [13], что множество R_i является i-компонентой и его мощность равна $q^{n(q-1)}$.

Далее, предварительно введя необходимые понятия, рассмотрим строение i-компоненты R_i в терминах проективных геометрий. Это облегчит понимание различия между компонентой R_i и простой i-компонентой P_i, определение которой будет дано ниже, при построении базовых множеств этих компонент. Введенная терминология будет использована в доказательстве леммы 4.

Проверочная матрица кода $\mathcal{H}_q^N$ состоит из N попарно линейно независимых векторов пространства V_q^m. С помощью кода Хэмминга $\mathcal{H}_q^N$ 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 $\mathcal{H}_q^N$ и три точки лежат на одной прямой, если соответствующие им столбцы являются линейно зависимыми. Через любые две различные точки $a = (a_1, a_2, \dots, a_m)$ и $b = (b_1, b_2, \dots, b_m)$ 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, [11]).

В проективной геометрии каждой i-компоненте R_i из кода $\mathcal{H}_q^N$ соответствуют прямые, проходящие через точку i (см. [13]). Каждая такая прямая задает некоторый подкод $\mathcal{H}_l$, его база состоит из $q-1$ троек кода Хэмминга вида

$$T_s = e_i + s \cdot e_j + a_s \cdot e_{k_s}, \quad s \in GF^*(q), \tag{2}$$

где $GF^*(q)$ — ненулевые элементы поля $GF(q)$, $j = j(l)$ и паре элементов $1, s$, стоящих в i-й, j-й позициях вектора веса 3 кода $\mathcal{H}_q^N$, отвечает в силу плотной упакованности кода Хэмминга единственный элемент $a_s \in GF^*(q)$, 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, база компоненты R_i является объединением баз $\mathcal{B}(\mathcal{H}_i)$ соответствующих подкодов $\mathcal{H}_i$, т. е.

$$R_i = \langle \mathcal{B}(\mathcal{H}_1) \cup \mathcal{B}(\mathcal{H}_2) \cup \cdots \cup \mathcal{B}(\mathcal{H}_n) \rangle. \quad (3)$$

Рассмотрим подкод $\mathcal{H}_1$, его база состоит из $q-1$ троек кода Хэмминга вида (2). Вычитая первую тройку $T = e_i + e_j + a_1 \cdot e_{k_1}$ из оставшихся $q-2$ троек, получим тройки

$$T'_s = 0 \cdot e_i + (s - \alpha^0) \cdot e_j + (-a_1) \cdot e_{k_1} + a_s \cdot e_{k_s}, \quad s \in GF^*(q) \backslash \{\alpha^0\},$$

здесь α — примитивный элемент поля $GF(q)$. Рассмотрим $r(q-2)$ кодовых слов вида $T + \alpha^{tp} \cdot T'_s$ для всех $s \in GF^*(q) \backslash \{\alpha^0\}$ и $t \in \{0, 1, \ldots, r-1\}$, вместе с тройкой T добавим их к формирующейся над простым полем $GF(p)$ базе нового множества.

Аналогично действуем с оставшимися подкодами $\mathcal{H}_l$ компоненты R_i, $l \in \{2, 3, \ldots, n\}$. В результате получим базу, мощность которой равна $n \cdot (r(q-2)+1)$, напомним, что $q = p^r$.

Обозначим через P_i подпространство, порожденное над простым полем $GF(p)$ полученным множеством. Следует отметить, что в i-й позиции кодовых слов множества P_i находятся элементы простого поля $GF(p)$, в остальных же позициях могут встретиться элементы всего поля $GF(q)$. Множество P_i называется *простой* i-компонентой, и его мощность равна $p^{nr(q-2)+n}$. Впервые такое множество было рассмотрено в [13], в работе [14] свитчинги простых компонент позволили получить нижнюю оценку числа различных совершенных q-значных кодов, являющуюся на сегодняшний день лучшей.

Теорема 2. *Для любого $k \in \{0, \ldots, p \cdot K - 2, p \cdot K\}$ существуют два q-значных совершенных кода $\mathcal{H}_q^N$ и C длины $N = nq + 1$ такие, что $\eta(\mathcal{H}_q^N, C) = k \cdot |P_i|/p$, где $|P_i| = p^{nr(q-2)+n}$, $q = p^r$.*

Доказательство. Рассмотрим разбиение q-значного кода Хэмминга $\mathcal{H}_q^N$ на простые компоненты:

$$\mathcal{H}_q^N = \bigcup_{j=1}^{K} P_i^j, \quad \text{где } K = p^{n(2r-1)-r(m-1)}, \ N = nq + 1$$

(см. [14]). Используя свитчинги по i-й координате, легко получить следующее достаточно богатое множество чисел пересечений q-значных совершенных кодов: $k \cdot |P_i|/p$ для каждого $k \in \{0, 1, \ldots, p \cdot K - 2, p \cdot K\}$.

Минимальная мощность непустого пересечения равна $|P_i|/p$. Это значение достигается при пересечении кода C с кодом, полученным свитчингами всех простых компонент кода C, за исключением единственной простой компоненты, на которую действуем свитчингом по перестановке, не изменяющей только один элемент поля $GF(p)$ в i-й координате.

Следует отметить, что пересечение двух кодов мощности $(p \cdot K - 1) \cdot |P_i|/p$ невозможно в силу того, что единичный свитчинг одной компоненты не может изменить только один элемент поля $GF(p)$ в некоторой координате кодовых слов компоненты, он переставит как минимум два элемента поля. $\square$

3.2. О пересечениях q-значных совершенных кодов, полученных с использованием конструкции Шонхайма. В этом пункте для произвольного допустимого $N = nq+1$, $n \geq 1$, описываются конструкции двух q-значных совершенных кодов длины N, пересечение которых меньше, чем минимальное непустое пересечение свитчинговых совершенных кодов той же длины, данное теоремой 2.

Пусть C_q^n — q-значный совершенный код длины $n = (q^{m-1}-1)/(q-1)$, $n \geq 1$, элементы множества $F^0 = \{1, 2, \ldots, q-1\}$ сопоставим во взаимно однозначное соответствие с ненулевыми элементами поля $GF(q)$. Рассмотрим следующую модификацию известной конструкции совершенных q-значных кодов Шонхайма (см. [12]):

$$C_q^N = \left\{ \left(v_1, v_2, \ldots, v_{q-1}, \sum_{t=1}^{q-1} |v_t| + \lambda(c), \sum_{t=1}^{q-1} \alpha_t v_t + c \right) \right.$$
$$\left. \mid v_t \in V_q^n, c \in C_q^n, \alpha_t \in F^0, \alpha_t \neq \alpha_s, t \neq s \right\},$$

где $|v_t| = v_{t1}+v_{t2}+\cdots+v_{tn}$ для $v_t = (v_{t1}, v_{t2}, \ldots, v_{tn})$, λ — произвольная функция, действующая из кода C_q^n длины n во множество элементов поля $GF(q)$.

Множество C_q^N является q-значным совершенным кодом длины $N = nq+1$, доказательство этого факта аналогично доказательству основного результата статьи [12].

Вместо кода C_q^n в приведенной выше конструкции рассмотрим код Хэмминга $\mathcal{H}_q^n$ и линейную функцию $\lambda(c) = -|\,c\,|$, $c \in \mathcal{H}_q^n$. Обозначим полученный код через C. Легко убедиться, что код C является линейным, т. е. кодом Хэмминга. Рассмотрим подмножество $A = \{(e_s^t, 1, \alpha e_s) \mid \alpha \in F^0\}$ кода C, где e_s^t и e_s — векторы длины $n(q-1)$ и n только с одной ненулевой координатой, равной 1, в $(tn+s)$-й и s-й позициях соответственно, $t \in \{1, \ldots, q-1\}$, $s \in \{1, \ldots, n\}$. Обозначим через $\langle A \rangle$ подпространство, порожденное векторами множества A.

Лемма 1. *Множество $\langle A \rangle$ является i-компонентой кода C, где $i = (q-1)n+1$.*

Доказательство. Непосредственно из определения i-компоненты R_i, где $i = (q-1)n+1$, и определения множества A следует $\langle A \rangle \subseteq R_i$. Используя этот факт вместе с линейной независимостью всех векторов множества A, получаем, что мощности $\dim(\langle A \rangle)$ и $\dim(R_i)$ равны и, следовательно, подпространство $\langle A \rangle$ совпадает с компонентой R_i. $\square$

Поскольку $R_i \subset C$, множество $C \setminus R_i$ также является i-компонентой. Пусть далее $q > 2$. Рассмотрим следующие множества:

$$B_1 = (C \setminus R_i) + \beta \cdot e_i, \quad B_2 = (C \setminus R_i) + \gamma \cdot e_i, \quad \beta, \gamma \in F^0 \text{ и } \beta \neq \gamma.$$

Пусть

$$C_1 = R_i \cup B_1 \quad \text{и} \quad C_2 = \pi(R_i \cup B_2), \tag{4}$$

где π — циклический сдвиг на одну позицию влево последних $n+1$ координат во всех кодовых словах кода $R_i \cup B_2$, т. е.

$$\pi(z_1, \ldots, z_{n(q-1)}, z_{n(q-1)+1}, \ldots, z_N)$$
$$= (z_1, \ldots, z_{n(q-1)}, z_{n(q-1)+2}, \ldots, z_N, z_{n(q-1)+1}).$$

Легко видеть, что C_1 и C_2 являются q-значными совершенными кодами.

Лемма 2. *Справедливо* $B_1 \cap \pi(B_2) = R_i \cap \pi(B_2) = \pi(R_i) \cap B_1 = \varnothing$.

Доказательство. Докажем, что $B_1 \cap \pi(B_2) = \varnothing$. Пусть два вектора

$$x = \left(u_1, u_2, \dots, u_{q-1}, \sum_{j=1}^{q-1} |u_j| - |\,c\,| + \beta, \sum_{j=1}^{q-1} \alpha_j u_j + c \right),$$

$$y = \left(v_1, v_2, \dots, v_{q-1}, \sum_{j=1}^{q-1} \alpha_j v_j + c', \sum_{j=1}^{q-1} |v_j| - |\,c'\,| + \gamma \right),$$

принадлежащие кодам B_1 и $\pi(B_2)$ соответственно, равны. Тогда $u_j = v_j$ для каждого $j \in \{1, 2, \dots, q-1\}$ и $|\,x\,| = |\,y\,|$. Рассмотрим разность

$$|x| - |y| = \sum_{j=1}^{q-1} |u_j| + \sum_{j=1}^{q-1} |u_j| - |c| + \beta + \sum_{j=1}^{q-1} |\alpha_j u_j| + |c|$$
$$- \sum_{j=1}^{q-1} |u_j| - \sum_{j=1}^{q-1} |u_j| + |c'| - \gamma - \sum_{j=1}^{q-1} |\alpha_j u_j| - |c'| = \beta - \gamma.$$

Но по построению множеств B_1 и B_2 выполняется $\beta \neq \gamma$ и, следовательно, $x \neq y$. Остальные случаи доказываются аналогичным образом. □

Теорема 3. *Существуют два q-значных совершенных кода длины $N = qn + 1$, пересекающихся по $p^{nr(q-2)}$ кодовым словам, где $q = p^r$, $n \geq 1$.*

Доказательство. Докажем, что искомыми кодами являются коды C_1 и C_2, определенные выше. Легко видеть, что

$$|C_1 \cap C_2| = |R_i \cap \pi(R_i)| + |B_1 \cap \pi(B_2)| + |R_i \cap \pi(B_2)| + |\pi(R_i) \cap B_1|.$$

По лемме 2 имеем $|C_1 \cap C_2| = |R_i \cap \pi(R_i)|$.

Рассмотрим порождающие матрицы $G(R_i)$ и $G(\pi(R_i))$ множеств R_i и $\pi(R_i)$ соответственно:

$$G(R_i) = \left(\begin{array}{c|c|c} E_{(q-1)n} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} & \begin{array}{c} E_n \\ \hline 2E_n \\ \hline \dots \\ \hline (q-1)E_n \end{array} \end{array} \right),$$

$$G(\pi(R_i)) = \left(\begin{array}{c|c|c} E_{(q-1)n} & \begin{array}{c} E_n \\ \hline 2E_n \\ \hline \dots \\ \hline (q-1)E_n \end{array} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{array} \right).$$

Заметим, что обе матрицы даны в канонической форме, следовательно, отсюда легко получить проверочные матрицы $H(R_i)$ и $H(\pi(R_i))$, также заданные в канонической форме. Поскольку множества R_i и $\pi(R_i)$ линейны, множество $R_i \cap \pi(R_i)$ также является линейным кодом. Проверочная матрица этого множества имеет вид

$$H(R_i \cap \pi(R_i)) = H(R_i) \parallel H(\pi(R_i)).$$

Нетрудно видеть, что $\mathrm{rank}(H(R_i \cap \pi(R_i))) = 2n + 1$. Тогда для $q = p^r$ имеем

$$|R_i \cap \pi(R_i)| = q^{N-(2n+1)} = q^{n(q-2)} = p^{nr(q-2)}. \quad \square$$

Минимальная мощность пересечения $|P_i|/p$, данная теоремой 2, больше, чем мощность пересечения $\eta(C_1, C_2)$ из теоремы 3, что демонстрирует

Следствие 1. *Для любого* $N = qn + 1$, $q > 2$, *выполняется*

$$\frac{|P_i|/p}{\eta(C_1, C_2)} = p^{n-1}.$$

Покажем теперь, что, используя технику свитчингов простых компонент, можно получить пересечение совершенных q-значных кодов, меньшее, чем данное теоремой 3.

Пусть далее $q = p^r$ и $r > 1$. Рассмотрим в конструкции кодов (4) вместо компоненты R_i простую компоненту P_i, вместо множеств B_1 и B_2 следующие два множества:

$$B_1' = (C \setminus P_i) + \beta \cdot e_i, \quad B_2' = (C \setminus P_i) + \gamma \cdot e_i, \quad \beta, \gamma \in F^0 \text{ и } \beta \neq \gamma,$$

соответственно. Тогда аналогично кодам C_1 и C_2 получаем коды $C_1' = P_1 \cup B_1'$ и $C_2' = \pi(P_2 \cup B_2')$ и аналогично доказательству леммы 2 доказывается следующее утверждение.

Лемма 3. *Справедливо* $B_1' \cap \pi(B_2') = P_i \cap \pi(B_2') = \pi(P_i) \cap B_1' = \varnothing$.

Найдем пересечение множеств P_i и $\pi(P_i)$.

Лемма 4. *Справедливо* $\dim(P_i \cap \pi(P_i)) = n(r(q-3)+1)$.

Доказательство. Поскольку компоненты P_i и $\pi(P_i)$ являются линейными подпространствами над полем $GF(p)$, их пересечение также линейное подпространство. Для вычисления мощности пересечения простых компонент воспользуемся подсчетом его размерности из равенства

$$\dim(P_i \cap \pi(P_i)) = \dim(P_i) + \dim(\pi(P_i)) - \dim(P_i \cup \pi(P_i)). \tag{5}$$

Для этого найдем ранг порождающей матрицы объединения $P_i \cup \pi(P_i)$, предварительно построив ее. Рассмотрим порождающую матрицу $G(P_i)$ простой компоненты P_i как пополнение порождающей матрицы компоненты R_i некоторой подматрицей X порядка $n(r-1)(q-2) \times N$, т. е. $G(P_i) = G(R_i) \parallel X$. Здесь стоит отметить, что порождающая матрица меньшей простой компоненты P_i содержит строки порождающей матрицы большей компоненты R_i. Такое происходит в силу того, что простая компонента P_i получается линейными комбинациями строк порождающей матрицы не над полем $GF(q)$ (как в случае с компонентой R_i), а над простым полем $GF(p)$. Подматрицу X будем формировать следующими линейными преобразованиями матрицы $G(R_i)$ над полем $GF(q)$. Рассмотрим порождающую матрицу произвольного подкода $\mathcal{H}_l$, $l \in \{1, 2, \ldots, n\}$, из представления (3), строки которой содержатся в матрице $G(R_i)$, для краткости приведем только $q + 1$ столбцов, остальные столбцы порождающей матрицы $G(\mathcal{H}_l)$ данного подкода длины N являются нулевыми:

$$G(H_l) = \left(\begin{array}{c|c|c} \multirow{4}{*}{E_{q-1}} & 1 & 1 \\ & 1 & 2 \\ & \vdots & \vdots \\ & 1 & q-1 \end{array} \right).$$

Вычитая произвольную, например, первую строку из остальных, получим следующую матрицу с $q - 2$ строками:

$$\left(\begin{array}{c|c|c|c} -1 & \multirow{4}{*}{E_{q-2}} & 0 & 1 \\ -1 & & 0 & 2 \\ \vdots & & \vdots & \vdots \\ -1 & & 0 & q-2 \end{array} \right).$$

Затем, поочередно умножая полученную матрицу на $r-1$ линейно независимых элементов поля $GF(q)$ (напомним, что $q = p^r$), например на первые $r-1$ степеней примитивного элемента α поля $GF(q)$, сформируем из этих $r-1$ матриц матрицу X_l размера $(r-1)(q-2) \times (q+1)$, приписывая каждую новую матрицу снизу к полученной ранее матрице. И, наконец, к каждой строке матрицы X_l прибавляем по одной строке порождающей матрицы $G(\mathcal{H}_l)$ так, чтобы последний столбец стал нулевым. В итоге имеем матрицу с $(r-1)(q-2)$ строками:

$$X'_l = \left(M_l \;\middle|\; \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \;\middle|\; \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \right),$$

где M_l — некоторая подматрица порядка $(r-1)(q-2) \times (q-1)$. Нетрудно проверить, что матрица $G(\mathcal{H}_l) \parallel X'_l$ имеет $r(q-2)+1$ линейно независимых над простым полем $GF(p)$ строк.

Дополняя полученные матрицы X'_l для всех $l \in \{1, 2, \ldots, n\}$ опущенными нулевыми столбцами и приписывая одну под другой, объединяем их в матрицу, которую обозначим через X, т. е.

$$X = \left(M \;\middle|\; \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \;\middle|\; \Theta_{n(r-1)(q-2),n} \right),$$

где $\Theta_{n(r-1)(q-2),n}$ — нулевая $n(r-1)(q-2) \times n$-матрица и M — матрица порядка $n(r-1)(q-2) \times (N-n-1)$, полученная из матриц M_l.

Таким образом, объединение $P_i \cup \pi(P_i)$ компонент P_i и $\pi(P_i)$ будет иметь порождающую матрицу, состоящую из строк матрицы

$$G(P_i) \parallel G(\pi(P_i)) = (G(R_i) \parallel X) \parallel (G(\pi(R_i)) \parallel \pi(X)),$$

исключая линейно зависимые строки над простым полем $GF(p)$. Порождающие матрицы $G(P_i)$ и $G(\pi(P_i))$ имеют вид

$$\left(\begin{array}{c|c|c} & 1 & E_n \\ \cline{3-3} E_{(q-1)n} & \vdots & \vdots \\ \cline{3-3} & 1 & (q-1)E_n \\ \hline & 1 & \\ M & \vdots & \Theta_{n(r-1)(q-2),n} \\ & 1 & \end{array} \right)$$

и

$$\left(\begin{array}{c|c|c} & E_n & 1 \\ \cline{2-2} E_{(q-1)n} & \vdots & \vdots \\ \cline{2-2} & (q-1)E_n & 1 \\ \hline & & 1 \\ M & \Theta_{n(r-1)(q-2),n} & \vdots \\ & & 1 \end{array} \right)$$

соответственно. Проделаем линейные преобразования строк матрицы $G(P_i) \parallel G(\pi(P_i))$ с тем, чтобы вычислить ее ранг, здесь и далее все операции будут производиться над простым полем $GF(p)$. Для этого, рассмотрев разность

$G(\pi(P_i)) - G(P_i)$ и выполнив несложные линейные преобразования, получим матрицу

$$Y = \left(\begin{array}{c|c|c} \Theta_{(q-1)n} & \begin{array}{c} E_n \\ \hline \vdots \\ \hline (q-1)E_n \end{array} & \begin{array}{c} I_n \\ \hline \vdots \\ \hline (q-1)I_n \end{array} \\ \hline \Theta_{n(r-1)(q-2),n} & \begin{array}{c|c} 1 & \\ \vdots & \Theta_{n(r-1)(q-2),n-1} \\ 1 & \end{array} & \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \end{array} \right),$$

где I_n — вектор-столбец длины n, состоящий из единиц. Если положить, что ненулевые элементы поля $GF(q)$, составляющие первые rn строк полученной матрицы, линейно независимы (например, первые r степеней примитивного элемента α поля $GF(q)$ начиная с нулевой степени), то тогда эти строки также линейно независимы, обозначим их через Y'. Заметим, что линейные комбинации строк матрицы Y' порождают все оставшиеся строки матрицы Y. При этом строки матрицы Y' линейно независимы со строками порождающей матрицы $G(P_i)$. Таким образом, ранг порождающей матрицы объединения $P_i \cup \pi(P_i)$ будет равен

$$\operatorname{rank}(G(P_i)) + \operatorname{rank}(Y') = n(r(q-2)+1) + nr = n(r(q-1)+1).$$

Следовательно, согласно равенству (5) размерность пересечения компонент P_i и $\pi(P_i)$ равна

$$\dim(P_i \cap \pi(P_i)) = n(r(q-2)+1) + n(r(q-2)+1) - n(r(q-1)+1) = n(r(q-3)+1). \quad \square$$

Теорема 4. *Существуют два q-значных совершенных кода длины* $N = qn+1$, *пересекающихся по* $p^{nr(q-3)+n}$ *кодовым словам, где* $q = p^r, r > 1$.

Доказательство. Докажем, что построенные выше коды C_1' и C_2' удовлетворяют условию теоремы. Очевидно, что

$$|C_1' \cap C_2'| = |P_i \cap \pi(P_i)| + |B_1' \cap \pi(B_2')| + |P_i \cap \pi(B_2')| + |\pi(P_i) \cap B_1'|.$$

По лемме 3 имеем $|C_1' \cap C_2'| = |P_i \cap \pi(P_i)|$. Следовательно, согласно лемме 4 мощность пересечения кодов C_1' и C_2' равна $p^{nr(q-3)+n}$. $\square$

Во сколько раз мощность пересечения кодов C_1' и C_2' меньше мощности пересечения кодов C_1 и C_2 показывает

Следствие 2. *Для любого* $N = qn+1$, $q = p^r$, $r > 1$, *выполняется*

$$\frac{\eta(C_1, C_2)}{\eta(C_1', C_2')} = p^{n(r-1)}.$$

Результаты настоящей работы частично анонсированы в [15]. Вопросы минимальной мощности пересечения совершенных q-значных кодов и полного спектра пересечения этих кодов остаются открытыми.

ЛИТЕРАТУРА

1. *Etzion T., Vardy A.* Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. V. 11, N 2. P. 205–223.
2. *Bar-Yahalom S. E., Etzion T.* Intersection of isomorphic linear codes // J. Combin. Theory. Ser. A. 1997. V. 80, N 1. P. 247–256.

3. *Avgustinovich S. V., Heden O., Solov'eva F. I.* On intersections of perfect binary codes // Bayreuth. Math. Schr. 2005. N 74. P. 1–6.
4. *Avgustinovich S. V., Heden O., Solov'eva F. I.* On intersection problem for perfect binary codes // Des. Codes Cryptogr. 2006. V. 39, N 3. P. 317–322.
5. *Phelps K. T., Villanueva M.* Intersection of Hadamard codes // IEEE Trans. Inform. Theory. 2007. V. 53, N 5. P. 1924–1928.
6. *Rifá J., Solov'eva F. I., Villanueva M.* On the intersection of additive perfect codes // IEEE Trans. Inform. Theory. 2008. V. 54, N 3.
7. *Rifá J., Solov'eva F. I., Villanueva M.* On the intersection of additive extended and non-extended perfect codes // Proc. Intern. Workshop on Coding and Cryptography. Versailles, France. April, 16–20, 2007. Rocquencourt: INRIA, 2007. P. 333–341.
8. *Зиновьев В. А., Леонтьев В. К.* Теорема о несуществовании совершенных кодов над полями Галуа. 1972. (Препринт / ИППИ АН СССР).
9. *Зиновьев В. А., Леонтьев В. К.* Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. № 2. С. 123–132.
10. *Tietäväinen A.* On the nonexistence of perfect codes over finite fields // SIAM J. Appl. Math. 1973. V. 24. P. 88–96.
11. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
12. *Schönheim J.* On linear and nonlinear single-error-correcting q-nary 1 perfect codes // Inform. Control. 1968. V. 12, N 1. P. 23–26.
13. *Phelps K. T., Villanueva M.* Ranks of q-ary 1 perfect codes // Des. Codes Cryptogr. 2002. V. 27, N 1–2. P. 139–144.
14. *Лось А. В.* Построение совершенных q-ичных кодов свитчингами простых компонент // Проблемы передачи информации. 2006. Т. 42, № 1. С. 34–42.
15. *Solov'eva F. I., Los' A. V.* On intersections of q-ary perfect codes // Proc. Tenth Intern. Workshop "Algebraic and Combinatorial Coding Theory". Zvenigorod, Russia. September, 3–9. 2006. Moscow: IITP RAS, 2006. P. 244–247.

Статья поступила 9 апреля 2007 г.

Соловьева Фаина Ивановна, Лось Антон Васильевич
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
`sol@math.nsc.ru, sozercatel@gmail.com`