

УДК 519.72

## О НЕСИСТЕМАТИЧЕСКИХ СОВЕРШЕННЫХ КОДАХ НАД КОНЕЧНЫМИ ПОЛЯМИ<sup>\*)</sup>

С. А. Малюгин

**Аннотация.** Построены несистематические совершенные  $q$ -значные коды над конечными полями  $F_q$  длины  $n = (q^m - 1)/(q - 1)$  при  $m \geq 4$  и  $q \geq 2$ , а также при  $m = 3$  и при  $q$ , не являющимся простым числом. Показано, что при  $q \neq 3, 5$  такие коды можно строить сдвигами семи непересекающихся компонент, а при  $q = 3, 5$  — сдвигами восьми непересекающихся компонент кода Хемминга  $H_q^n$ .

**Ключевые слова:** совершенный код, код Хемминга, поле Галуа, несистематический код, проективная геометрия, компонента.

### Введение

Пусть  $F_q$  — поле Галуа из  $q$  элементов. Через  $F_q^n$  обозначим  $n$ -мерное векторное пространство над полем  $F_q$ . Множество ненулевых координат вектора  $x \in F_q^n$  называется его *носителем* и обозначается через  $[x]$ . Число элементов в любом множестве  $A$  обозначаем через  $|A|$ . *Весом* вектора  $x$  называется число его ненулевых координат. Введём в пространстве  $F_q^n$  метрику Хемминга  $d(x, y) = |[x - y]| = |\{i \mid x_i \neq y_i\}|$ . Шар радиуса  $r$  с центром в точке  $x \in F_q^n$  обозначаем через  $B_r(x)$ . Базисный вектор пространства  $F_q^n$ , у которого  $i$ -я координата равна 1, а все остальные координаты нулевые, обозначим через  $e_i$ .

**Определение 1.** *Совершенный  $q$ -значный код*  $C \subset F_q^n$  — это такое подмножество в пространстве  $F_q^n$ , что  $\bigcup_{x \in C} B_1(x) = F_q^n$  и

$$x \neq y \implies B_1(x) \cap B_1(y) = \emptyset.$$

Из определения 1 следует, что расстояние Хемминга между любыми различными векторами кода  $C$  не меньше трёх, при этом  $|C| = q^{n-m}$ , где  $n = (q^m - 1)/(q - 1)$ ,  $m = 2, 3, \dots$

---

<sup>\*)</sup>Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 08-01-00671).

Совершенный код  $C$  называется  $q$ -значным кодом Хемминга, если  $C$  является линейным подпространством в  $F_q^n$  размерности  $n - m$ . Имеется следующее представление кода Хемминга. Рассмотрим в пространстве  $F_q^m$  подмножество  $N$ , состоящее из  $n = (q^m - 1)/(q - 1)$  ненулевых попарно не коллинеарных векторов. Далее будем рассматривать  $N$  как множество индексов для векторов  $x = (x_i)_{i \in N} \in F_q^N$ . Тогда совершенный  $q$ -значный код Хемминга  $H_q^n$  можно определить как множество всех таких векторов  $x = (x_i)_{i \in N}$ , что  $\sum_{i \in N} x_i \cdot i = 0$ . Если координаты векторов  $i \in N$  записывать столбцами, то множество  $N$  представляет собой проверочную матрицу кода  $H_q^n$ . Для конкретизации выбора множества  $N$  можем считать, что первая ненулевая координата каждого вектора  $i \in N$  равна единице.

**Определение 2.** Совершенный код  $C \subset F_q^N$  называется *систематическим*, если существуют такие  $(n - m)$ -элементное множество индексов  $I = \{i_1, \dots, i_{n-m}\} \subset N$  и отображение  $f : F_q^I \rightarrow F_q^{N \setminus I}$ , что

$$x = (x_i)_{i \in N} \in C \iff x_i = f_i(x_{i_1}, \dots, x_{i_{n-m}})$$

для всех  $i \in N \setminus I$ , т. е. код  $C$  является графиком отображения  $f$  в пространстве  $F_q^N = F_q^I \times F_q^{N \setminus I}$ .

Очевидно, код Хемминга  $H_q^n$  является систематическим.

Несистематические совершенные двоичные ( $q = 2$ ) коды длины  $n \geq 255$  ( $n = 2^m - 1$ ) были впервые построены в 1996 г. С. В. Августинovichем и Ф. И. Соловьевой [1]. Усовершенствовав конструкцию из [1], Фелпс и Ле-Ван [9] в 1999 г. построили несистематические совершенные двоичные коды для всех длин  $n \geq 31$ . Оказалось, что такой метод неприменим для кодов длины 15. Несистематические коды длины 15 были построены с помощью компьютерных вычислений в 1997 г. А. М. Романовым [6], а также Фелпсом и Ле-Ваном [9]. Нами было показано [4, 5], что задача построения несистематических кодов сводится к задаче нахождения несистематических орбит векторов пространства  $F_2^n$  относительно группы перестановочных автоморфизмов кода Хемминга. Этот факт даёт возможность строить несистематические коды, сдвигая всего семь непересекающихся компонент в коде Хемминга любой длины  $n = 2^m - 1$  ( $m \geq 4$ ), что даёт ответ на вопрос Фелпса и Ле-Вана [9].

Теперь мы рассмотрим аналогичную задачу для  $q$ -значных кодов.

### 1. Построение несистематических $q$ -значных кодов

Следуя [10], рассмотрим в коде Хемминга  $H_q^n$  подпространство  $R_i$ , порождённое всеми векторами веса 3 с ненулевой  $i$ -й координатой.

Для  $u \in H_q^n$  смежные классы  $R_i^u = R_i + u$  называются *компонентами кода*  $H_q^n$ . Впервые такие компоненты применялись в [12] для построения нелинейных  $q$ -значных кодов Васильева.

Рассмотрим семейство  $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_s}^{u_s}\}$ , состоящее из  $s$  попарно не пересекающихся компонент кода  $H_q^n$ . В [10] было показано, что для любого  $\alpha = (\alpha_1, \dots, \alpha_s) \in F_q^s$  множество

$$H_q^n(\mathcal{B}, \alpha) = \left( H_q^n \setminus \bigcup_{k=1}^s R_{i_k}^{u_k} \right) \cup \left( \bigcup_{k=1}^s (R_{i_k}^{u_k} + \alpha_k e_{i_k}) \right)$$

является совершенным  $q$ -значным кодом. Мы будем далее говорить, что код  $C = H_q^n(\mathcal{B})$  получен из кода Хемминга  $H_q^n$  сдвигами непересекающихся компонент  $R_{i_1}^{u_1}, \dots, R_{i_s}^{u_s}$ . Эту конструкцию рассматривали также А. В. Лось [2] и А. М. Романов [7] для получения нижних оценок числа нелинейных совершенных  $q$ -значных кодов и для построения разбиений кода Хемминга  $H_q^n$  на непересекающиеся компоненты. Как мы сейчас покажем, с помощью этой конструкции можно строить и несистематические коды.

Пусть  $J = \{j_1, \dots, j_m\} \subset N$  — некоторый базис в пространстве  $F_q^m$ . Обозначим

$$L_2(J) = \{i \in N \mid \exists \beta, \gamma \in F_q, \exists j, j' \in J \text{ такие, что } i = \beta j + \gamma j'\}.$$

На языке проективной геометрии  $L_2(J)$  — это объединение всех прямых, проходящих через любые пары точек из  $J$ .

Пусть  $I_{\mathcal{B}} = \{i \in N \mid \text{существует } r, 1 \leq r \leq s, \text{ при котором } i = i_r\}$  (множество индексов  $i$ , для которых существуют  $i$ -компоненты, принадлежащие семейству  $\mathcal{B}$ ).

**Теорема 1.** *Если существует такой базисный набор индексов*

$$J = \{j_1, \dots, j_m\} \subset N,$$

что  $I_{\mathcal{B}} \subset L_2(J)$ , то совершенный код  $C = H_q^n(\mathcal{B}, \alpha)$  является систематическим при любом  $\alpha \in F_q^s$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $I = N \setminus J$ . Нам достаточно доказать, что если  $u, v \in C$  и  $u \neq v$ , то  $[u - v] \not\subset J$ , так как отсюда сразу будет

следовать, что множество  $C$  является графиком некоторого отображения  $f : F_q^I \rightarrow F_q^J$ . Возможны следующие варианты.

1.  $u, v \in C \cap H_q^n$ . Тогда  $u - v \in H_q^n$  и в силу определения кода  $H_q^n$  получаем линейную зависимость  $\sum_{i \in N} (u_i - v_i) \cdot i = 0$ . Так как множество индексов  $J$  линейно независимо, то  $[u - v] \not\subset J$ .

2.  $u, v \in C \setminus H_q^n$ . Существуют такие номера  $k, k'$ ,  $1 \leq k, k' \leq s$ , что  $u - \alpha_k e_{i_k} \in R_{i_k}^{u_k}$ ,  $v - \alpha_{k'} e_{i_{k'}} \in R_{i_{k'}}^{u_{k'}}$ . Допустим, что  $i_k \neq i_{k'}$ . Предполагая противное, допустим  $[u - v] \subset J$ . Пусть  $i_k, i_{k'} \notin J$ . Тогда при некоторых  $\beta, \gamma, \beta', \gamma' \in F_q$  и  $j_1, j_2, j'_1, j'_2 \in J$  имеем  $i_k = \beta j_1 + \gamma j_2$ ,  $i_{k'} = \beta' j'_1 + \gamma' j'_2$ . Рассмотрим векторы

$$w = \alpha_k e_{i_k} - \alpha_k \beta e_{j_1} - \alpha_k \gamma e_{j_2}, \quad w' = \alpha_{k'} e_{i_{k'}} - \alpha_{k'} \beta' e_{j'_1} - \alpha_{k'} \gamma' e_{j'_2}$$

веса 3 из  $H_q^n$ . Пусть  $z = u - v - \alpha_k \beta e_{j_1} - \alpha_k \gamma e_{j_2} + \alpha_{k'} \beta' e_{j'_1} + \alpha_{k'} \gamma' e_{j'_2}$ . Так как  $z = u - \alpha_k e_{i_k} - v + \alpha_{k'} e_{i_{k'}} + w - w'$ , то  $z \in H_q^n$  и  $[z] \subset J$ . Поэтому  $z = 0$ . Значит,  $u - v - \alpha_k e_{i_k} + \alpha_{k'} e_{i_{k'}} = w' - w \in R_{i_k} + R_{i_{k'}}$ . Так как  $u - \alpha_k e_{i_k} - u_k \in R_{i_k}$  и  $v - \alpha_{k'} e_{i_{k'}} - u_{k'} \in R_{i_{k'}}$ , то  $u_k - u_{k'} \in R_{i_k} + R_{i_{k'}}$ , а это противоречит непересекаемости компонент  $R_{i_k}^{u_k}$  и  $R_{i_{k'}}^{u_{k'}}$ . Поэтому  $[u - v] \not\subset J$ .

Рассмотрим теперь случай, когда  $i_k \notin J$ ,  $i_{k'} \in J$ . Тогда для некоторых  $\beta, \gamma \in F_q$  и  $j_1, j_2 \in J$  имеем  $i_k = \beta j_1 + \gamma j_2$ . Рассмотрим в коде  $H_q^n$  вектор  $w = \alpha_k e_{i_k} - \alpha_k \beta e_{j_1} - \alpha_k \gamma e_{j_2}$  веса 3. Аналогичным образом получаем, что вектор  $z = u - v - \alpha_k \beta e_{j_1} - \alpha_k \gamma e_{j_2} + \alpha_{k'} e_{i_{k'}}$  принадлежит  $H_q^n$  и его носитель входит в  $J$ . Поэтому  $z = 0$  и  $u - \alpha_k e_{i_k} - v + \alpha_{k'} e_{i_{k'}} = -w \in R_{i_k}$ . Это означает, что  $u_{i_k} - u_{i_{k'}} \in R_{i_k} + R_{i_{k'}}$ , и опять пришли к противоречию с непересекаемостью компонент  $R_{i_k}$  и  $R_{i_{k'}}$ . Если  $i_k, i_{k'} \in J$ , то из включения  $[u - \alpha_k e_{i_k} - v + \alpha_{k'} e_{i_{k'}}] \subset J$  следует, что  $u - v = \alpha_k e_{i_k} - \alpha_{k'} e_{i_{k'}}$ . Это противоречит тому, что вес вектора  $u - v$  должен быть не меньше трёх. Для нерассмотренного ещё случая  $i_k = i_{k'}$  вышеприведённое доказательство сохраняется практически без изменений.

3.  $u \in C \cap H_q^n$ ,  $v \in C \setminus H_q^n$ . В этом случае доказательство аналогично доказательству случаев 1 и 2, поэтому мы его опускаем.

Теорема 1 доказана.

В связи с этим результатом введём следующие определения.

**Определение 3.** Множество индексов  $I = \{i_1, \dots, i_s\} \subset N$  называем *несистематическим*, если  $I \not\subset L_2(J)$  при любом базисном наборе  $J \subset N$ .

**Определение 4.** Говорим, что семейство непересекающихся компонент  $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_s}^{u_s}\}$  не содержит кратных компонент, если  $i_k \neq i_{k'}$  при  $k \neq k'$ .

Для построения несистематических кодов необходимо ввести следующие условия на число компонент  $s$  в семействе  $\mathcal{B}$ :

$$s|R_i| < \frac{1}{2}|H_q^n|, \quad (1)$$

$$s|R_i \cap R_j| \leq |R_i| \quad (i \neq j). \quad (2)$$

**Теорема 2.** Пусть в семействе непересекающихся компонент  $\mathcal{B}$  нет кратных компонент и для числа компонент  $s$  семейства  $\mathcal{B}$  выполняются неравенства (1) и (2). Тогда если множество индексов  $I_{\mathcal{B}}$  является несистематическим, то совершенный код  $H_q^n(\mathcal{B}, \alpha)$  несистематический для любых  $\alpha \in F_q^s, \alpha_i \neq 0$  ( $i = 1, \dots, s$ ).

**ДОКАЗАТЕЛЬСТВО.** Достаточно доказать, что для любого множества индексов  $J = \{j_1, \dots, j_m\} \subset N$  существуют такие векторы  $u, v \in C$ ,  $u \neq v$ , что  $[u-v] \subset J$ . Допустим сначала, что векторы  $j_1, \dots, j_m$  являются линейно зависимыми в пространстве  $F_q^m$ . Тогда существуют такие числа  $x_j \in F_q$  ( $j \in J$ ), не все равные нулю, что  $\sum_{j \in J} x_j \cdot j = 0$ . Полагая  $x_j = 0$  при  $j \notin J$ , мы получим вектор  $x = (x_j) \in H_q^n$ , носитель которого входит в  $J$ . Из условия (1) следует, что  $|C \cap H_q^n| > \frac{1}{2}|H_q^n|$ , поэтому существуют такие два вектора  $u, v \in C \cap H_q^n$ , что  $x = u - v$ . Следовательно,  $[u-v] \subset J$ .

Пусть множество  $J = \{j_1, \dots, j_m\}$  состоит из линейно независимых векторов. По условию теоремы  $I_{\mathcal{B}} \not\subset L_2(J)$ , поэтому существует такой номер  $k$  ( $1 \leq k \leq s$ ), что  $i_k \notin L_2(J)$ . Значит, в разложении

$$i_k = \beta_1 j_1 + \dots + \beta_m j_m$$

по базису  $j_1, \dots, j_m$  имеем  $\beta_r \neq 0$  по крайней мере для трёх различных значений индекса  $r$ . Рассмотрим в коде Хемминга  $H_q^n$  вектор

$$v = e_{i_k} - \beta_1 e_{j_1} - \dots - \beta_m e_{j_m}.$$

Докажем, что  $v \notin R_{i_k}$ . Без ограничения общности можно считать, что  $\beta_1 \neq 0$ . Для любого  $\beta \in F_q^* = F_q \setminus \{0\}$  вектор  $i_k + \beta j_1$  кратен некоторому индексному вектору  $j'_\beta$ ,  $\beta \in N$ . Пусть  $i_k + \beta j_1 = \gamma_\beta j'_\beta$  для некоторого  $\gamma_\beta \in F_q^*$ . Рассмотрим в пространстве  $F_q^n$  вектор  $h = e_{j_1} + \sum_{\beta \in F_q^*} (\beta/\gamma_\beta) e_{j'_\beta}$ .

Для любого  $\beta \in F_q^*$  вектор  $h$  ортогонален вектору  $w_\beta = e_{i_k} + \beta e_{j_1} - \gamma_\beta e_{j'_\beta}$  веса 3 из компоненты  $R_{i_k}$  относительно скалярного произведения

$$\langle u, v \rangle = \sum_{i \in N} u_i v_i \quad (u, v \in F_q^N).$$

Как известно [2, 10], векторы  $w_\beta$  ( $\beta \in F_q^*$ ) являются частью базиса компоненты  $R_{i_k}$ . Множество индексов  $N$  можно рассматривать как конечное проективное пространство размерности  $m-1$  над полем  $F_q$ . При этом  $i_k$ ,  $j_1$  и  $j'_\beta$  ( $\beta \in F_q^*$ ) являются точками прямой в этой геометрии [2]. Носители остальных векторов  $w$  веса 3, составляющих базис компоненты  $R_{i_k}$ , являются подмножествами других прямых в этой геометрии, поэтому скалярное произведение  $\langle h, w \rangle$  равно нулю. Это означает, что  $h \perp R_{i_k}$ . С другой стороны, из  $j'_\beta \in J$  будет следовать, что  $i_k = -\beta j_1 + \gamma_\beta j'_\beta \in L_2(J)$ , а это противоречит нашему предположению, поэтому  $j'_\beta \notin J$  для всех  $\beta \in F_q^*$ . Значит,  $\langle h, v \rangle = -\beta_1 \neq 0$ , и, следовательно,  $v \notin R_{i_k}$ .

Из только что доказанного следует, что  $R_{i_k}^{u_k} \cap R_{i_k}^{u_k + \alpha_k v} = \emptyset$ . В силу условия (2) множество  $R_{i_k}^{u_k + \alpha_k v} \setminus \bigcup_{j=1}^s R_{i_j}^{u_j}$  непусто. Пусть вектор  $w$  принадлежит этому множеству. Тогда  $w \in C \cap R_{i_k}^{u_k + \alpha_k v}$ . Так как  $w - \alpha_k v \in R_{i_k}^{u_k}$ , то вектор  $w' = w - \alpha_k v + \alpha_k e_{i_k}$  принадлежит коду  $C$ . Так как

$$w - w' = \alpha_k v - \alpha_k e_{i_k} = -\alpha_k \beta_1 e_{j_1} - \dots - \alpha_k \beta_m e_{j_m},$$

то  $[w - w'] \subset J$ . Теорема 2 доказана.

В силу теоремы 2 задача о существовании несистематических кодов сводится к задаче о существовании семейства непересекающихся компонент  $\mathcal{B}$ , без кратных компонент и удовлетворяющего условиям (1) и (2), а также к задаче о существовании несистематических множеств. Так как  $|H_q^n| = q^{n-m}$  и  $|R_i| = q^{q^{m-1}-1}$  (см. [2, 10]), то условия (1) и (2) удовлетворяются для всех  $q$  при  $m \geq 5$ , для  $q \geq 3$  при  $m = 4$  и для  $q \geq 4$  при  $m = 3$ .

Семейство непересекающихся компонент  $\mathcal{B}$  можно строить индуктивно. Если набор попарно не пересекающихся компонент  $\{R_{i_1}^{u_1}, \dots, R_{i_k}^{u_k}\}$  уже построен, то выбираем индекс  $i_{k+1} \neq i_j$  ( $j = 1, \dots, k$ ) и рассматриваем множество  $S = \bigcup_{j=1}^k (R_{i_j}^{u_j} + R_{i_{k+1}})$ , которое является объединением некоторого множества смежных классов по компоненте  $R_{i_{k+1}}$ . Так как при  $i \neq j$  имеем  $|R_i + R_j| = q^{q^{m-1} + q^{m-2} - 2}$  (см. [2]), то при  $k < n$  и достаточно больших  $n$  будет выполняться строгое неравенство  $|S| < |H_q^n|$ , поэтому существует еще один смежный класс  $R_{i_{k+1}}^{u_{k+1}}$ , не пересекающийся с  $S$ . Добавляя эту компоненту  $R_{i_{k+1}}^{u_{k+1}}$  к первоначальному семейству, мы получаем новое семейство непересекающихся компонент  $\{R_{i_j}^{u_j}\}_{j=1}^{k+1}$ .

Если  $m \geq 6$ , либо  $m = 5$  и  $q \geq 3$ , либо  $m = 4$  и  $q \geq 5$ , то вышеописанным способом можно построить такое семейство непересекающихся

компонент  $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_n}^{u_n}\}$ , для которого  $I_{\mathcal{B}} = N$ . Для двоичных кодов этот способ построения непересекающихся компонент применялся в [1, 9] (причём в случае  $m = 5$  такое семейство было найдено в [9] с помощью компьютера). При  $m = 4$  и  $q = 4$  этим методом можно построить семейство из 64 непересекающихся компонент, а если  $q = 3$ , то только из 9 непересекающихся компонент.

Теперь нам осталось только решить вопрос о существовании несистематических множеств.

## 2. Описание несистематических множеств

Из определения множества  $L_2(J)$  следует, что

$$|L_2(J)| = \frac{2m + m(m-1)(q-1)}{2} < n = \frac{q^m - 1}{q - 1}. \quad (3)$$

Тем самым, если число компонент  $s$  в семействе  $\mathcal{B}$  удовлетворяет неравенству  $s > |L_2(J)|$ , то любое множество индексов  $I = \{i_1, \dots, i_s\}$  является несистематическим. В частности, из оценок в конце предыдущего раздела следует, что несистематические совершенные коды над полем  $F_q$  существуют при всех  $q$  и всех  $m \geq 5$ , а также при  $m = 4$  и  $q \geq 5$ . Если  $m = q = 4$ , то  $|L_2(J)| = 22$ , при этом можно построить вышеописанным методом семейство из 64 непересекающихся компонент, т. е. и при  $m = q = 4$  существуют несистематические коды.

Рассмотрим вопрос о минимальном несистематическом множестве. Систематичность множества индексов  $I = \{i_1, \dots, i_s\}$  означает, что можно найти такое базисное множество  $J = \{j_1, \dots, j_m\} \subset N$ , что  $I \subset L_2(J)$ , т. е. в разложении по этому базису

$$\begin{aligned} i_1 &= \beta_{1,1}j_1 + \dots + \beta_{m,1}j_m, \\ &\vdots \\ i_s &= \beta_{1,s}j_1 + \dots + \beta_{m,s}j_m, \end{aligned} \quad (4)$$

столбцы матрицы  $B = (\beta_{i,j})$  содержат не более двух ненулевых элементов. Мы будем называть такие матрицы *бидиагональными*.

*Рангом*  $\text{Rank}(I)$  множества индексов  $I = \{i_1, \dots, i_s\} \subset N$  называется число линейно независимых (в пространстве  $F_q^m$ ) векторов из  $I$ . Очевидно,  $r \leq \min\{m, s\}$ . Пусть  $\text{Rank}(I) = r$  и  $i_1, \dots, i_r$  — линейно независимые векторы из  $I$ . Остальные векторы  $i_k$  ( $r < k \leq s$ ) можно представить

линейными комбинациями векторов  $i_1, \dots, i_r$ , т. е.

$$\begin{aligned} i_{r+1} &= \alpha_{1,r+1} i_1 + \dots + \alpha_{r,r+1} i_r, \\ &\vdots \\ i_s &= \alpha_{1,s} i_1 + \dots + \alpha_{r,s} i_r. \end{aligned} \quad (5)$$

Рассмотрим матрицу коэффициентов

$$A = \begin{pmatrix} 1 & \dots & 0 & \alpha_{1,r+1} & \dots & \alpha_{1,s} \\ & & & \dots & & \\ 0 & \dots & 1 & \alpha_{r,r+1} & \dots & \alpha_{r,s} \end{pmatrix}. \quad (6)$$

Сопоставляя системы (4) и (5), видим, что задача теперь сводится к нахождению такой  $(m \times r)$ -матрицы  $C$  ранга  $r$ , после умножения которой слева на матрицу  $A$  получается bidiagonalная  $(m \times s)$ -матрица  $B$ . Так как  $B = CA$  и  $A$  содержит единичную подматрицу, то матрица  $C$  тоже обязана быть bidiagonalной.

Пусть  $N' = L(I)$  — подмножество всех индексов из  $N$ , являющихся линейными комбинациями элементов из  $I$ . Возьмём  $N'$  в качестве индексного множества для кода Хемминга  $H_q^{n'}$  длины  $n' = (q^r - 1)/(q - 1)$ .

**Лемма 1** (о ранге). *Множество индексов  $I$ , удовлетворяющее системе линейных соотношений (5), является систематическим в коде  $H_q^n$  ( $n = (q^m - 1)/(q - 1)$ ) тогда и только тогда, когда оно является систематическим в коде  $H_q^{n'}$ .*

**ДОКАЗАТЕЛЬСТВО.**  $\Leftarrow$  Эта импликация очевидна.

$\Rightarrow$  Пусть  $(m \times s)$ -матрица  $A$  из (6) приводится к bidiagonalному виду домножением слева на  $(m \times r)$ -матрицу  $C$  ранга  $r$ . Рассмотрим в  $C$   $(r \times r)$ -подматрицу  $C'$ , имеющую ненулевой определитель. Тогда  $(r \times s)$ -матрица  $C'A$  тоже будет bidiagonalной, так как она получается путём вычёркивания  $m - r$  строк из bidiagonalной матрицы  $CA$ . Лемма 1 доказана.

Из этой леммы следует, что свойство систематичности множества  $I$ , удовлетворяющего уравнениям (5), не зависит от того, в каком коде Хемминга  $H_q^n$  изучается этот вопрос. Другими словами, без ограничения общности можно считать, что  $m = r$ .

**Лемма 2** (о расширении поля). *Пусть поле  $F'$  является расширением поля  $F$ . Пусть  $(r \times s)$ -матрица  $A$  с элементами из поля  $F$  приводится к bidiagonalному виду над полем  $F'$ . Тогда она приводится к такому виду и над полем  $F$ .*



ДОКАЗАТЕЛЬСТВО. Пусть невырожденная  $(r \times r)$ -матрица  $C'$  с элементами из поля  $F'$  приводит матрицу  $A$  к bidiagonalному виду, т. е. каждый столбец матрицы  $C'A$  содержит по крайней мере  $r - 2$  нулевых элементов. Пусть  $i$ -я строка  $c'_i$  матрицы  $C'$  ортогональна  $k$  столбцам  $a_1, \dots, a_k$  матрицы  $A$ . Запишем эти условия ортогональности в виде системы линейных уравнений  $(c'_i, a_1) = 0, \dots, (c'_i, a_k) = 0$  (здесь  $(c, a)$  означает обычное скалярное произведение строки на столбец). Если  $x_1, \dots, x_t$  — базисный набор решений системы уравнений

$$(x, a_1) = 0, \dots, (x, a_k) = 0$$

над полем  $F$ , то он останется базисным набором решений и над полем  $F'$ . В частности, для некоторых  $\xi_1, \dots, \xi_t \in F'$  имеем  $c'_i = \xi_1 x_1 + \dots + \xi_t x_t$ . Заменяя в определителе  $\det(C')$   $i$ -ю строку на это выражение, приходим к равенству  $\det(C') = \xi_1 \det(C''_1) + \dots + \xi_t \det(C''_t)$ , где матрица  $C''_j$  получается из матрицы  $C'$  заменой строки  $c_i$  строкой  $x_j$  ( $j = 1, \dots, t$ ). Так как  $\det(C') \neq 0$ , то для некоторого  $j$  получим  $\det(C''_j) \neq 0$ . У матрицы  $C''_j$  элементы  $i$ -й строки лежат в поле  $F$ , и по-прежнему матрица  $C''_j A$  является bidiagonalной, так как у неё те же самые нулевые элементы, что и у  $C'A$ . Таким образом, заменяя строку за строкой, мы через конечное число шагов получим такую матрицу  $C$  с элементами из поля  $F$ , что  $\det(C) \neq 0$  и матрица  $CA$  bidiagonalная. Лемма 2 доказана.

Из лемм 1 и 2 следует, что если множество индексов  $\{i_1, \dots, i_s\}$ , удовлетворяющее уравнениям (5) с коэффициентами  $\alpha_{i,j} \in F_q$ , является несистематическим в коде Хемминга  $H_q^n$ ,  $q = p^k$ , где  $p$  — простое число, то оно будет несистематическим в любом другом коде Хемминга  $H_{q'}^{n'}$  длины  $n'$ , где  $q' = p^{k'}$  и  $k'$  делится на  $k$ .

**Лемма 3.** Если  $s \leq r + 1$  либо  $s \leq 6$ , то любая  $(r \times s)$ -матрица  $A$  вида (6) приводится к bidiagonalному виду.

ДОКАЗАТЕЛЬСТВО. При  $s = r$  матрица  $A$  единичная, т. е. она уже bidiagonalна. При  $s = r + 1$  система (5) сводится к одному уравнению  $i_{r+1} = \alpha_{1,r+1}i_1 + \dots + \alpha_{r,r+1}i_r$ . Переставляя строки матрицы  $A$ , можно считать, что  $\alpha_{k,r+1} \neq 0$  при  $1 \leq k \leq r'$  и  $\alpha_{k,r+1} = 0$  при  $r' < k \leq s$  для некоторого  $r' \leq r$ . В этом случае матрица

$$A = \begin{pmatrix} 1 & \dots & 0 & \alpha_{1,r+1} \\ & \dots & & \\ 0 & \dots & 1 & \alpha_{r,r+1} \end{pmatrix}$$

приводится к бидиагональному виду при помощи  $(r \times r)$ -матрицы

$$C = \begin{pmatrix} \alpha_{2,r+1} & -\alpha_{1,r+1} & 0 & \dots & 0 & \cdot & \dots & 0 \\ 0 & \alpha_{3,r+1} & -\alpha_{2,r+1} & \dots & 0 & \cdot & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & \alpha_{r',r+1} & -\alpha_{r'-1,r+1} & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Пусть  $s = 6$ . Из только что доказанного следует, что необходимо рассмотреть только случаи  $r = 4$  и  $r = 3$ . При  $r = 4$  матрица  $A$  имеет следующий вид:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \alpha_{1,5} & \alpha_{1,6} \\ 0 & 1 & 0 & 0 & \alpha_{2,5} & \alpha_{2,6} \\ 0 & 0 & 1 & 0 & \alpha_{3,5} & \alpha_{3,6} \\ 0 & 0 & 0 & 1 & \alpha_{4,5} & \alpha_{4,6} \end{pmatrix}.$$

Рассмотрим  $(2 \times 2)$ -миноры  $\gamma_{i,j} = \alpha_{i,5}\alpha_{j,6} - \alpha_{i,6}\alpha_{j,5}$ . Допустим, что существуют два равных нулю минора, скажем,  $\gamma_{1,3} = 0$  и  $\gamma_{2,3} = 0$ . В каждом из этих миноров есть хотя бы один ненулевой элемент (иначе сама матрица  $A$  будет бидиагональной). Допустим, что  $\alpha_{3,5} \neq 0$ . Тогда, если  $m = r$ , то при умножении слева на матрицу  $A$  невырожденной матрицы

$$C = \begin{pmatrix} \alpha_{3,5} & 0 & -\alpha_{1,5} & 0 \\ 0 & \alpha_{3,5} & -\alpha_{2,5} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

получим бидиагональную матрицу. Другие варианты равенства нулю двух миноров рассматриваются аналогично. Если только один минор  $\gamma_{1,2}$  равен нулю, причём  $\alpha_{2,5} \neq 0$ , а все остальные миноры ненулевые, то мы рассмотрим векторное произведение векторов  $(\alpha_{2,5}, \alpha_{3,5}, \alpha_{4,5})$  и  $(\alpha_{2,6}, \alpha_{3,6}, \alpha_{4,6})$ , которое равно  $(\gamma_{3,4}, \gamma_{4,2}, \gamma_{2,3})$ . Тогда с помощью матрицы

$$C = \begin{pmatrix} \alpha_{2,5} & -\alpha_{1,5} & 0 & 0 \\ 0 & \gamma_{3,4} & \gamma_{4,2} & \gamma_{2,3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

можно привести матрицу  $A$  к бидиагональному виду. Если все мино-

ры  $\gamma_{i,j}$  ненулевые, то матрица

$$C = \begin{pmatrix} \gamma_{2,3} & \gamma_{3,1} & \gamma_{1,2} & 0 \\ \gamma_{2,4} & \gamma_{4,1} & 0 & \gamma_{1,2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

будет приводить матрицу  $A$  к bidiagonalному виду. Определитель матрицы  $C$  равен  $\gamma_{2,3}\gamma_{4,1} - \gamma_{2,4}\gamma_{3,1}$ . Если он равен нулю, то  $\gamma_{1,2}\gamma_{3,4} = 0$ , что противоречит нашему предположению. Поэтому  $\det(C) \neq 0$ . Мы опускаем доказательство для более простых случаев  $s = 5, 6$  и  $r = 3$ . Лемма 3 доказана.

Из леммы 3 и теоремы 1 следует, что если сдвигать в коде Хемминга  $H_q^n$  не более шести непересекающихся компонент, то будем получать только систематические коды. Несколько неожиданным является тот факт, что существуют семиэлементные несистематические множества индексов. Рассмотрим  $(3 \times 7)$ -матрицу

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & \alpha_{1,4} & \alpha_{1,5} & \alpha_{1,6} & \alpha_{1,7} \\ 0 & 1 & 0 & \alpha_{2,4} & \alpha_{2,5} & \alpha_{2,6} & \alpha_{2,7} \\ 0 & 0 & 1 & \alpha_{3,4} & \alpha_{3,5} & \alpha_{3,6} & \alpha_{3,7} \end{pmatrix}. \quad (7)$$

**Лемма 4.** Пусть у матрицы  $A_1$  все элементы  $\alpha_{i,j}$  не равны нулю. В этом случае  $A_1$  не приводится к bidiagonalному виду, если у неё все миноры порядка 2 и 3, составленные из элементов  $\alpha_{i,j}$ , не равны нулю.

**ДОКАЗАТЕЛЬСТВО.** Невырожденная bidiagonalная  $(3 \times 3)$ -матрица  $C$  после перестановки строк и столбцов приводится к одной из следующих «тестовых» матриц:

$$C_1 = \begin{pmatrix} c_1 & 0 & 0 \\ 0 & c_2 & c_3 \\ 0 & 0 & c_4 \end{pmatrix}, \quad C_2 = \begin{pmatrix} c_1 & c_2 & c_3 \\ 0 & c_4 & 0 \\ 0 & 0 & c_5 \end{pmatrix}, \quad C_3 = \begin{pmatrix} c_1 & c_2 & 0 \\ 0 & c_3 & c_4 \\ 0 & 0 & c_5 \end{pmatrix},$$

$$C_4 = \begin{pmatrix} c_1 & c_2 & 0 \\ c_3 & c_4 & 0 \\ 0 & 0 & c_5 \end{pmatrix}, \quad C_5 = \begin{pmatrix} c_1 & c_2 & 0 \\ c_3 & c_4 & c_5 \\ 0 & 0 & c_6 \end{pmatrix}, \quad C_6 = \begin{pmatrix} c_1 & c_2 & 0 \\ c_3 & 0 & c_4 \\ 0 & c_5 & c_6 \end{pmatrix},$$

где все  $c_i \neq 0$  (мы не рассматриваем тривиальный случай, когда  $C$  диагональна). Если при умножении матрицы  $C_1$  на четвёртый и пятый столбцы матрицы  $A_1$  получаются столбцы только с двумя ненулевыми элементами, то её вторая строка должна быть ортогональна этим двум

столбцам, а это противоречит тому, что все миноры порядка 2, взятые из этих двух столбцов, ненулевые. Если при умножении матрицы  $C_2$  на четвёртый, пятый и шестой столбцы матрицы  $A_1$  получаются столбцы только с двумя ненулевыми элементами, то её первая строка ортогональна этим трём столбцам матрицы  $A_1$ . Это противоречит тому, что минор порядка 3 матрицы  $A_1$ , составленный из этих столбцов, равен нулю. Если одна из матриц  $C_3, C_4$  приводит матрицу  $A_1$  к bidiagonalному виду, то либо первая, либо вторая её строка ортогональна сразу двум столбцам матрицы  $A_1$ , начиная с четвёртого. Это противоречит тому, что все миноры порядков 2 и 3 ненулевые. В случае матрицы  $C_5$  либо первая её строка ортогональна двум столбцам, либо вторая строка ортогональна трём столбцам матрицы  $A_1$ , а в случае матрицы  $C_6$  одна из её строк ортогональна двум столбцам матрицы  $A_1$ , что в любом из этих случаев приводит к противоречию. Лемма 4 доказана.

**Лемма 5.** Если  $q$  нечётно и у матрицы  $A_1$  вида (7) три элемента  $\alpha_{i,j}$  равны нулю, то она приводима к bidiagonalному виду. Если  $q = 2^k$  ( $k \geq 1$ ), то матрица  $A_1$  неприводима к bidiagonalному виду над полем  $F_q$  тогда и только тогда, когда перестановкой строк и столбцов, а также умножением их на подходящие ненулевые элементы из  $F_q$  её можно преобразовать к матрице

$$A_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}. \quad (8)$$

**Доказательство.** Рассмотрим матрицу  $A_1$ , у которой три элемента  $\alpha_{i,j}$  нулевые. Случай, когда в одной и той же строке таких нулевых элементов более одного, довольно прост, и мы его не рассматриваем, поэтому допустим, что перестановкой строк и столбцов и домножением их на ненулевые элементы можно привести матрицу  $A_1$  к виду

$$A_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & \alpha_1 \\ 0 & 0 & 1 & 1 & \alpha_2 & \alpha_3 & 0 \end{pmatrix}. \quad (9)$$

Каждая из трёх матриц

$$C_1 = \begin{pmatrix} 1 & -1 & 0 \\ \alpha_3 & \alpha_2 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ \alpha_1 & -1 & \alpha_2^{-1} \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ -\alpha_1 & 1 & \alpha_1 \alpha_3^{-1} \end{pmatrix}$$

приводит матрицу  $A_3$  вида (9) к бидиагональному виду. Для приводимости достаточно, чтобы определитель одной из этих матриц был ненулевым. Пусть  $\det(C_1) = \alpha_2 + \alpha_3 = 0$ ,  $\det(C_2) = \alpha_1 + \alpha_2^{-1} = 0$  и  $\det(C_3) = 1 + \alpha_1 \alpha_3^{-1} = 0$ . Из этих уравнений получим  $\alpha_1 = \alpha_2 = -\alpha_3$ ,  $\alpha_1^2 = -1$ . Пусть теперь  $q$  нечётно. Тогда  $-1 \neq 1$  и поэтому  $\alpha_1 \neq \pm 1$ . Это значит, что матрица

$$C_4 = \begin{pmatrix} \alpha_1 - 1 & -\alpha_1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

невыврожденна и приводит матрицу  $A_3$  к бидиагональному виду. В случае  $q = 2^k$  поле  $F_q$  имеет характеристику 2. Поэтому  $\alpha_1^2 = 1$ , откуда  $\alpha_1 = \alpha_2 = \alpha_3 = 1$ , и матрица  $A_3$  совпадает с матрицей  $A_2$  из (8).

В силу леммы 2 о расширении поля проверку того, что матрица  $A_3$  неприводима к бидиагональному виду, достаточно провести для поля  $F_2$ . Это было сделано ранее в [4], [5, следствие 1]). Лемма 5 доказана.

Переходим к изучению несистематических семиэлементных множеств ранга 4. Для этого требуется рассмотреть вопрос о приводимости к бидиагональному виду матрицы

$$A_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & \alpha_{1,5} & \alpha_{1,6} & \alpha_{1,7} \\ 0 & 1 & 0 & 0 & \alpha_{2,5} & \alpha_{2,6} & \alpha_{2,7} \\ 0 & 0 & 1 & 0 & \alpha_{3,5} & \alpha_{3,6} & \alpha_{3,7} \\ 0 & 0 & 0 & 1 & \alpha_{4,5} & \alpha_{4,6} & \alpha_{4,7} \end{pmatrix}. \quad (10)$$

**Лемма 6.** Пусть у матрицы  $A_4$  все элементы  $\alpha_{i,j}$  не равны нулю. Пусть  $A_4$  имеет не более одного нулевого минора порядка 2 или 3, составленного из элементов  $\alpha_{i,j}$ . Тогда  $A_4$  неприводима к бидиагональному виду.

**Доказательство.** Невыврожденная бидиагональная  $(4 \times 4)$ -матрица  $C$  после перестановки строк и столбцов приводится к одной из следующих «тестовых» матриц:

$$C_1 = \begin{pmatrix} c_1 & c_2 & 0 & 0 \\ 0 & c_3 & c_4 & 0 \\ c_5 & 0 & 0 & c_6 \\ 0 & 0 & c_7 & c_8 \end{pmatrix}, \quad C_2 = \begin{pmatrix} c_1 & c_2 & 0 & 0 \\ c_3 & c_4 & 0 & 0 \\ 0 & 0 & c_5 & c_6 \\ 0 & 0 & c_7 & c_8 \end{pmatrix},$$

$$\begin{aligned}
C_3 &= \begin{pmatrix} c_1 & c_2 & c_3 & 0 \\ 0 & 0 & c_4 & c_5 \\ c_6 & 0 & 0 & c_7 \\ 0 & c_8 & 0 & 0 \end{pmatrix}, & C_4 &= \begin{pmatrix} c_1 & c_2 & c_3 & 0 \\ 0 & 0 & c_4 & c_5 \\ c_6 & c_7 & 0 & 0 \\ 0 & 0 & 0 & c_8 \end{pmatrix}, \\
C_5 &= \begin{pmatrix} c_1 & c_2 & c_3 & 0 \\ 0 & c_4 & c_5 & c_6 \\ c_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & c_8 \end{pmatrix}, & C_6 &= \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ c_5 & c_6 & 0 & 0 \\ 0 & 0 & c_7 & 0 \\ 0 & 0 & 0 & c_8 \end{pmatrix},
\end{aligned} \tag{11}$$

где некоторые из элементов  $c_i$  могут быть нулевыми, если это не противоречит невырожденности матрицы. Попробуем привести матрицу  $A_4$  к bidiagonalному виду с помощью матрицы  $C'$ , получаемой перестановкой столбцов матрицы  $C_1$  или  $C_2$  вида (11). Каждая строка матрицы  $C'$  содержит не более двух ненулевых элементов и может быть ортогональна не более чем двум столбцам матрицы  $A_1$  (так как у  $A_4$  может быть равен нулю только один минор порядка 2). При этом только одна строка матрицы  $C'$  может быть ортогональна сразу двум столбцам матрицы  $A_4$ , поэтому в последних трёх столбцах матрицы  $C'A_4$  может быть не более пяти нулевых элементов. А для bidiagonalности матрицы  $C'A_1$  необходимо, чтобы в каждом её столбце было не менее двух нулевых элементов. Попробуем привести  $A_4$  к bidiagonalному виду с помощью матрицы  $C''$ , получаемой перестановкой столбцов одной из матриц  $C_3, C_4, C_5$ . В этом случае только одна строка матрицы  $C''$ , имеющая три ненулевых элемента, может быть ортогональна сразу трём последним столбцам матрицы  $A_4$ . В этом случае ровно один минор порядка 3 у матрицы  $A_4$  нулевой, а все миноры порядка 2 в последних трёх столбцах ненулевые. Это означает, что другая строка матрицы  $C''$ , содержащая три ненулевых элемента (в случае, если  $C''$  получена из  $C_5$ ), ортогональна не более чем двум столбцам (из последних трёх) матрицы  $A_4$ , иначе матрица  $C''$  будет вырожденной. Строки матрицы  $C''$ , содержащие два ненулевых элемента, ортогональны не более чем одному столбцу (из последних трёх) матрицы  $A_4$ , а строки, имеющие один ненулевой элемент, не ортогональны ни одному столбцу. Тем самым и в этом случае матрица  $C''A_4$  имеет не более пяти нулевых элементов в последних трёх столбцах. Осталось рассмотреть матрицу  $C'''$ , получаемую перестановкой столбцов матрицы  $C_6$ . Её первая строка может быть ортогональна последним трём столбцам матрицы  $A_4$ , вторая строка имеет не более двух ненулевых элементов и может быть ортогональна не более чем двум столбцам из последних трёх, третья и четвёртая строки не ортогональны ни одному столбцу (из последних трёх). Значит, и в этом случае мы не

набираем шести нулевых элементов в последних трёх столбцах матрицы  $C'''A_4$ . Лемма 6 доказана.

**Следствие 1.** В любом коде Хемминга  $H_q^n$  длины  $n = (q^m - 1)/(q - 1)$  при  $m \geq 3$  и  $q \geq 2$ ,  $q \neq 3, 5$ , существуют семиэлементные несистематические множества индексов. Не существует семиэлементных несистематических множеств над полями  $F_3$  и  $F_5$ . При  $m \geq 3$  и  $q = 3, 5$  существуют восьмиэлементные несистематические множества.

**Доказательство.** Если  $q \geq 8$ , то в качестве примера матрицы, неприводимой к bidiagonalному виду можно рассмотреть

$$A_5 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \lambda & \mu & \nu \\ 0 & 0 & 1 & 1 & \lambda^2 & \mu^2 & \nu^2 \end{pmatrix},$$

где  $0, 1, \lambda, \mu, \nu$  и  $1, \lambda^2, \mu^2, \nu^2$  — различные элементы поля  $F_q$ . Все миноры третьего порядка в этом примере являются определителями Вандермонда, поэтому они не равны нулю. Если взять за  $\lambda$  примитивный элемент поля  $F_q$  и положить  $\mu = \lambda^2, \nu = \lambda^3$ , то все условия леммы 4 о неприводимости удовлетворяются в любом поле  $F_q$  при  $q \geq 8$ . В случае  $q = 7$  рассмотрим матрицу

$$A_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 4 \\ 0 & 0 & 1 & 0 & 1 & 5 & 3 \\ 0 & 0 & 0 & 1 & 1 & 6 & 2 \end{pmatrix}.$$

По модулю 7 все миноры порядка 2 и 3 из последних трёх столбцов этой матрицы, кроме одного, ненулевые, и поэтому по лемме 6 она не приводится к bidiagonalному виду.

В случае  $q = 3$  рассмотрим  $(3 \times 8)$ -матрицу

$$A_7 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 1 & 2 & 0 \end{pmatrix}.$$

Прямой проверкой убеждаемся, что она не приводится над полем  $F_3$  к bidiagonalному виду.

Если  $q = 5$ , то в качестве неприводимой матрицы над полем  $F_5$  можно рассмотреть  $(3 \times 8)$ -матрицу

$$A_8 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 1 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

При  $q = 2$  можно использовать матрицу  $A_2$  вида (8). В силу леммы 5 она тоже неприводима (см. также [4], [5, следствие 1]).

Довольно утомительная непосредственная проверка показывает, что над полями  $F_3$  и  $F_5$  все  $(3 \times 7)$ -матрицы,  $(4 \times 7)$ -матрицы и  $(5 \times 7)$ -матрицы приводятся к bidiagonalному виду. В силу леммы 3 все  $(m \times 7)$ -матрицы при  $m \geq 6$  также приводимы над этими полями к bidiagonalному виду, поэтому не существует семиэлементных несистематических множеств над полями  $F_3$  и  $F_5$ . Следствие 1 доказано.

Из теоремы 1, леммы 3 и следствия 1 сразу вытекает

**Следствие 2.** Если совершенный  $q$ -значный код  $C$  получен из кода Хемминга  $H_q^n$  сдвигами не более шести его попарно не пересекающихся компонент, то он является систематическим. Если при  $q = 3, 5$  совершенный  $q$ -значный код  $C$  получен из кода Хемминга  $H_q^n$  сдвигами не более семи попарно не пересекающихся компонент, то он тоже является систематическим.

Как следует из мощностных оценок, приведённых в конце предыдущего раздела, если  $m \geq 4$  и  $q \geq 3$ , то для любого набора индексов  $\{i_1, \dots, i_9\} \subset N$  в коде Хемминга  $H_q^n$  можно найти семейство девяти попарно не пересекающихся компонент  $\{R_{i_1}^{u_1}, \dots, R_{i_9}^{u_9}\}$  (при  $m = 4$  и  $q = 2$  семейство из восьми непересекающихся компонент было впервые построено в [6, 9]). В частности, при этих условиях можно взять семиэлементное или восьмиэлементное несистематическое множество индексов и по нему найти в коде Хемминга соответствующее число попарно не пересекающихся компонент. Следовательно, из теоремы 2 и предыдущих замечаний можно вывести следующее усиление теоремы 3 из [5].

**Теорема 3.** Для любого  $m \geq 4$  и  $q \geq 2$ ,  $q \neq 3, 5$ , существуют несистематические  $q$ -значные коды длины  $n = (q^m - 1)/(q - 1)$ , которые строятся из кода Хемминга  $H_q^n$  сдвигами семи попарно не пересекающихся компонент. Для любого  $m \geq 4$  и  $q = 3, 5$  существуют несистематические  $q$ -значные коды, которые строятся из кода Хемминга  $H_q^n$  сдвигами восьми попарно не пересекающихся компонент.

### 3. Случай $m = 3$

В этом случае сумма двух компонент  $R_i + R_j$  при  $i \neq j$  совпадает со всем кодом Хемминга  $H_q^n$ , поэтому при  $i \neq j$  не существует ни одной пары непересекающихся компонент  $R_i^{u_i}$  и  $R_j^{u_j}$ . Требуется некоторая модификация рассматриваемого выше подхода. В работе Фелпса, Рифы и



Виллануевой [11], а также в работе А. В. Лося [3] изучались так называемые минимальные компоненты  $P_i$  кода Хемминга  $H_q^n$ .

Пусть  $q = p^k$ . Рассмотрим в  $F_q$  простое подполе  $F_p$ . Минимальная компонента  $P_i$  определяется как подпространство, порождённое линейными комбинациями с коэффициентами из подполя  $F_p$  всех троек кода Хемминга  $H_q^n$ , у которых  $i$ -я координата равна единице.

Пусть  $\mathcal{P} = \{P_{i_1}^{u_1}, \dots, P_{i_s}^{u_s}\}$  — семейство, состоящее из  $s$  попарно не пересекающихся минимальных компонент кода  $H_q^n$ .

Если  $q = p^k$ , где  $p$  — простое число, то для любого  $\alpha = (\alpha_1, \dots, \alpha_k) \in F_p^s$  множество

$$H_q^n(\mathcal{P}, \alpha) = \left( H_q^n \setminus \bigcup_{j=1}^s P_{i_j}^{u_j} \right) \cup \left( \bigcup_{j=1}^s (P_{i_j}^{u_j} + \alpha_j e_{i_j}) \right)$$

является совершенным  $q$ -значным кодом.

**Теорема 2'.** Пусть  $m \geq 4$ , либо  $m = 3$  и  $q = p^k \geq 4$ , где  $p$  — простое число. Если в семействе непересекающихся минимальных компонент  $\mathcal{P}$  нет кратных компонент и множество индексов  $I_{\mathcal{P}}$  является несистематическим, то совершенный код  $H_q^n(\mathcal{P}, \alpha)$  несистематический для любых  $\alpha \in F_p^s, \alpha_i \neq 0$  ( $i = 1, \dots, s$ ).

**Теорема 3'.** В случае  $m = 3$  и  $q = p^k$ , где  $p$  — простое число и  $k \geq 2$ , существуют несистематические совершенные  $q$ -значные коды, которые строятся из кода Хемминга  $H_q^n$  сдвигами семи его непересекающихся компонент.

**ДОКАЗАТЕЛЬСТВО.** В [11, предложение 3.6] найдены размерности над полем  $F_p$  компонент  $P_i$  и их пересечений  $P_i \cap P_j$  при  $i \neq j$ :

$$\dim_p(P_i) = \frac{q^{m-1} - 1}{q - 1}(k(q - 2) + 1), \quad \dim_p(P_i \cap P_j) = (kq - 3k + 2)q^{m-2}.$$

Поэтому для размерности суммы  $P_{ij} = P_i + P_j$  над полем  $F_p$  имеем выражение

$$\dim_p(P_{ij}) = \frac{kq^m - (3k - 2)q^{m-2} - 2(kq - 2k + 1)}{q - 1}.$$

Отсюда следует, что размерность фактор-пространства равна

$$\dim_p(H_q^n / P_{ij}) = \frac{(3k - 2)q^{m-2} - (m - 2)kq - 5k + mk + 2}{q - 1}.$$

При  $m = 3$  ( $n = q^2 + q + 1$ ) эта размерность равна  $2(k - 1)$ , т. е. в этом случае код  $H_q^n$  разбивается на  $p^{2(k-1)}$  смежных классов по подпространству  $P_{ij}$ . Если  $q$  не является простым числом и  $q \geq 8$ , то минимальное число таких смежных классов равно 9 при  $q = 9$ . Тем самым при  $q \geq 8$  в коде Хемминга  $H_q^n$  без особого труда можно найти семь попарно не пересекающихся компонент  $P_{i_1}^{u_1}, \dots, P_{i_7}^{u_7}$  с несистематическим множеством индексов  $i_1, \dots, i_7$ , что в силу теоремы 2' гарантирует существование несистематических кодов, поэтому нам осталось разобрать единственный случай, когда  $q = 4$ . В этом случае  $p = 2$ ,  $n = 21$ , а размерность фактор-пространства равна  $\dim_2(H_4^{21}/P_{ij}) = 4$ . Мощностным методом, изложенным в конце первого раздела, можно найти в коде  $H_4^{21}$  только четыре непересекающиеся компоненты. Поэтому необходимо усовершенствовать метод поиска непересекающихся компонент.

Из [11, предложение 3.6] следует, что если  $i, j, k$  независимы (в пространстве  $F_4^3$ ), то  $\dim_2(P_i \cap P_j \cap P_k) = 9$ . Отсюда сразу следует, что  $\dim_2(P_{ij} \cap P_{ik}) = 32$ . В частности, для любых  $u, v \in H_4^{21}$  пересечение смежных классов  $P_{ij}^u$  и  $P_{ik}^v$  непусто, причём  $|P_{ij}^u \cap P_{ik}^v| = 2^{32}$ . Если же  $i, j, k$  зависимы над полем  $F_2$ , то  $P_{ij} = P_{ik} = P_{jk}$  и любые два смежных класса  $P_{ij}^u, P_{ik}^v$  либо не пересекаются, либо совпадают. Рассмотрим теперь семиэлементное несистематическое множество индексов  $\{i_1, \dots, i_7\}$ , где  $i_1, i_2, i_3$  независимы в пространстве  $F_4^3$  и  $i_4 = i_1 + i_2$ ,  $i_5 = i_1 + i_3$ ,  $i_6 = i_2 + i_3$ ,  $i_7 = i_1 + i_2 + i_3$ . Это множество является плоскостью Фано и соответствует последнему критерию несистематичности, сформулированному в лемме 5. Допустим, что мы уже нашли в коде  $H_4^{21}$  с помощью мощностного метода четыре непересекающиеся минимальные компоненты  $P_{i_1}^{u_1}, \dots, P_{i_4}^{u_4}$ . Для нахождения пятой компоненты следует рассмотреть при  $l = 4$  объединение

$$S_l = \bigcup_{j=1}^l (P_{i_j}^{u_j} + P_{i_{l+1}}). \quad (12)$$

Так как индексы  $i_1, i_2, i_5$  независимы над  $F_4$ , то смежные классы  $P_{i_1 i_5}^{u_1}$  и  $P_{i_2 i_5}^{u_2}$  имеют непустое пересечение, поэтому объединение  $S_4$  является собственным подмножеством кода  $H_4^{21}$ . Взяв любой вектор  $u_5 \in H_4^{21} \setminus S_4$ , мы найдём пятую компоненту  $P_{i_5}^{u_5}$ , которая не будет пересекаться с предыдущими четырьмя компонентами. Для поиска шестой компоненты необходимо рассмотреть множество  $S_l$ , определяемое формулой (12), при  $l = 5$ . Так как  $i_2, i_3, i_6$  зависимы над полем  $F_2$ , то смежные классы  $P_{i_2 i_6}^{u_2}$  и  $P_{i_3 i_6}^{u_3}$  не пересекаются. В противном случае мы получили бы равенство  $P_{i_2 i_6}^{u_2} = P_{i_3 i_6}^{u_3}$  и включение  $u_2 - u_3 \in P_{i_2 i_6} = P_{i_2 i_3}$ , из которого сразу сле-

дует пересекать ранее построенных компонент  $P_{i_2}^{u_2}$  и  $P_{i_3}^{u_3}$ . В силу независимости оставшиеся три смежных класса пересекаются с каждым из смежных классов  $P_{i_2 i_6}^{u_2}$  и  $P_{i_3 i_6}^{u_3}$ . Тем самым объединение  $S_5$  тоже является собственным подмножеством кода  $H_4^{21}$ , и мы имеем возможность выбрать шестую компоненту  $R_{i_6}^{u_6}$ , которая не будет пересекаться с выбранными ранее пятью компонентами. Для нахождения седьмой компоненты необходимо сначала определить размерность тройного пересечения  $P_{ij} \cap P_{jk} \cap P_{ik}$  для независимых индексов  $i, j, k$  над полем  $F_4$ . Это легко делается методами линейной алгебры, и мы выпишем только ответ:

$$\dim_2(P_{ij} \cap P_{jk} \cap P_{ik}) = 30. \quad (13)$$

Теперь следует положить в формуле (12)  $l = 6$ . Так как тройка  $i_3, i_4, i_7$  является зависимой над  $F_2$ , то смежные классы  $P_{i_3 i_7}^{u_3}$  и  $P_{i_4 i_7}^{u_4}$  не пересекаются друг с другом, а оставшиеся четыре смежных класса пересекаются с каждым из этих двух. Смежные классы  $P_{i_1 i_7}^{u_1}$  и  $P_{i_2 i_7}^{u_2}$  имеют непустое пересечение, так как множество индексов  $\{i_1, i_2, i_7\}$  является независимым над полем  $F_4$ . Объединение  $S_6$  может совпасть со всем кодом  $H_4^{21}$  только в случае, когда

$$P_{i_1 i_7}^{u_1} \cap P_{i_2 i_7}^{u_2} \subset P_{i_3 i_7}^{u_3} \cup P_{i_4 i_7}^{u_4}.$$

Так как  $|P_{i_1 i_7}^{u_1} \cap P_{i_2 i_7}^{u_2}| = 2^{32}$ , то должно быть

$$|P_{i_1 i_7}^{u_1} \cap P_{i_2 i_7}^{u_2} \cap P_{i_3 i_7}^{u_3}| \geq 2^{31} \text{ либо } |P_{i_1 i_7}^{u_1} \cap P_{i_2 i_7}^{u_2} \cap P_{i_4 i_7}^{u_4}| \geq 2^{31},$$

что противоречит формуле (13). Итак,  $S_6 \neq H_4^{21}$  и есть возможность выбрать седьмую компоненту  $P_{i_7}^{u_7}$ , не пересекающуюся с найденными ранее шестью компонентами. Теорема 3' доказана.

При  $q = 2$  и  $n = 7$  все совершенные коды являются линейными, следовательно, все они систематические. Остался открытым вопрос о существовании несистематических совершенных  $q$ -значных кодов длины  $n = q^2 + q + 1$  в случае, когда  $q$  является нечётным простым числом.

## ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** О несистематических совершенных двоичных кодах // Проблемы передачи информации. — 1996. — Т. 32, вып. 3. — С. 47–50.
2. **Лось А. В.** Построение совершенных  $q$ -значных кодов последовательными сдвигами  $\tilde{\alpha}$ -компонент // Проблемы передачи информации. — 2004. — Т. 40, вып. 1. — С. 40–47.

3. Лось А. В. Построение совершенных  $q$ -значных кодов свитчингами простых компонент // Проблемы передачи информации. — 2006. — Т. 42, вып. 1. — С. 34–42.
4. Малюгин С. А. О критерии несистематичности совершенных двоичных кодов // Докл. РАН. — 2000. — Т. 375, № 1. — С. 13–16.
5. Малюгин С. А. Несистематические совершенные двоичные коды // Дискрет. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 1. — С. 55–76.
6. Романов А. М. О несистематических совершенных кодах длины 15 // Дискрет. анализ и исслед. операций. Сер. 1. — 1997. — Т. 4, № 4. — С. 75–78.
7. Романов А. М. О разбиениях  $q$ -значных кодов Хемминга на непересекающиеся компоненты // Дискрет. анализ и исслед. операций. Сер. 1. — 2004. — Т. 11, №3. — С. 80–87.
8. Los' A. Construction of perfect  $q$ -ary codes // Proc. of Ninth Int. Workshop "Algebraic and combinatorial coding theory" (Kranevo, Bulgaria, June 19–25, 2004). — P. 272–276.
9. Phelps K. T., Le Van M. J. Non-systematic perfect codes // SIAM J. Discrete Math. — 1999. — V. 12, N 1. — P. 27–34.
10. Phelps K. T., Villanueva M. Ranks of  $q$ -ary 1-perfect codes // Designs, Codes and Cryptography. — 2002. — V. 27, N 1–2. — P. 139–144.
11. Phelps K. T., Rifá J., Villanueva M. Kernels of  $q$ -ary 1-perfect codes // Proc. of Ninth Int. Workshop on Coding and Cryptography (Versailles, France, March 24–28, 2003). — P. 375–381.
12. Schönheim J. On linear and nonlinear single-error-correcting  $q$ -ary perfect codes // Information and Control. — 1968. — V. 12, N 1. — P. 23–26.

Малюгин Сергей Артемьевич,  
e-mail: malugin@math.nsc.ru

Статья поступила  
31 июля 2008 г.