

## НЕСИСТЕМАТИЧЕСКИЕ СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ\*)

*С. А. Малюгин*

Предлагается новая конструкция несистематических расширенных совершенных двоичных кодов. Получено сведение задачи построения несистематических кодов к задаче нахождения несистематических орбит векторов пространства  $\{0,1\}^n$  относительно группы перестановочных автоморфизмов кода Хемминга. Этот факт дает возможность строить несистематические коды, сдвигая в коде Хемминга  $H^n$  всего семь непересекающихся компонент. Найдены все несистематические совершенные коды длины 15, получающиеся из кода Хемминга сдвигами его непересекающихся компонент, и доказано, что порождаемые ими расширенные коды являются несистематическими. При любом  $k \geq 5$  строятся примеры несистематических совершенных кодов длины  $n = 2^k - 1$  такие, что полученные из них расширенные коды являются систематическими.

### Введение

Несистематические совершенные двоичные коды любой длины  $n = 2^k - 1$  ( $k \geq 8$ ) впервые были построены С. В. Августиновичем и Ф. И. Соловьевой [1]. К. Т. Фелпс и М. Ли-Ван [9] предложили модификацию конструкции из [1], которая позволяет строить такие коды для всех  $n > 31$ . Несистематические коды длины  $n = 15$  и  $n = 31$  были найдены в [9] с помощью компьютера. В [6] дана теоретическая конструкция двух неэквивалентных несистематических кодов длины 15. В настоящей статье дается определение несистематических расширенных кодов (определение 1) и предлагается новая конструкция таких кодов. Дается также определение вполне систематических расширенных кодов (определение 2). Определения  $i$ -компоненты и  $(i, j, k)$ -компоненты кода Хемминга имеются в [2]. Все рассматриваемые коды строятся по следующей схеме. В коде Хемминга  $H^n$  выделяется семейство непересекающихся

---

\*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-00531) и Федеральной целевой программы «Интеграция» (объединенный проект АО-110).

$i$ -компонент  $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_m}^{u_m}\}$ . Затем в  $H^n$  сдвигаются по соответствующим координатам все компоненты выделенного семейства. Полученное таким способом множество

$$H^n(\mathcal{B}) = \left( H^n \setminus \bigcup_{p=1}^m R_{i_p}^{u_p} \right) \bigcup \left( \bigcup_{p=1}^m (R_{i_p}^{u_p} \oplus e_{i_p}) \right)$$

является совершенным кодом [2, 7, 8, 10].

Во втором разделе множество всех орбит пространства  $\{0, 1\}^n$  относительно группы перестановочных автоморфизмов кода  $H^n$  разбивается на класс систематических орбит и на класс несистематических орбит. Доказывается, что если для множества  $I_{\mathcal{B}}$  координат, по которым сдвигаются компоненты семейства  $\mathcal{B}$ , вектор с носителем  $I_{\mathcal{B}}$  принадлежит систематической орбите, то совершенный код  $H^n(\mathcal{B})$  является вполне систематическим (теорема 1). Если же множество  $I_{\mathcal{B}}$  соответствует несистематической орбите, то при выполнении некоторых условий  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$  и  $(\delta)$  совершенный код  $C = H^n(\mathcal{B})$  вместе с полученным из него расширенным кодом  $\tilde{C}$  являются несистематическими (теорема 2).

Таким образом, задача построения несистематических кодов сводится к другой задаче, к поиску несистематических орбит пространства  $\{0, 1\}^n$ . Все орбиты веса больше  $k(k+1)/2$  являются несистематическими. Кроме этого, найдены две несистематические орбиты веса 7 и доказано, что все орбиты веса меньше 7 являются систематическими (следствие 1). Следовательно, несистематический совершенный код любой допустимой длины  $n \geq 15$  можно получить, если сдвинуть в коде Хемминга  $H^n$  только семь непересекающихся компонент. Этот результат дает ответ на вопрос, поставленный К. Т. Фелпсом и М. Ли-Ваном в [9].

В третьем разделе найдены все несистематические коды длины 15, которые получаются из кода  $H^{15}$  сдвигами непересекающихся компонент, и доказано, что получаемые из них расширенные коды являются несистематическими. Ранее несистематичность кодов длины 15 проверялась с помощью компьютера [6, 9]. Из определения следует, что для любого систематического совершенного кода  $C$  построенный из него расширенный код  $\tilde{C}$  также будет систематическим. Обратное утверждение неверно.

В четвертом разделе для любого допустимого  $n \geq 31$  строится пример такого несистематического кода длины  $n$ , что полученный из него расширенный код является систематическим (пример 1). Строится также пример такого систематического кода  $H^n(\mathcal{B})$ , что множество номеров  $I_{\mathcal{B}}$  сдвигаемых координат семейства непересекающихся компонент  $\mathcal{B}$  соответствует несистематической орбите (пример 2). Этот пример

в какой-то мере оправдывает условия  $(\alpha)$ – $(\delta)$ , накладываемые на семейство  $\mathcal{B}$  при построении несистематических кодов. Примеры 3 и 4 дают ответы на вопросы К. Т. Фелпса и М. Ли-Вана [9] о свойствах системы троек  $ST(C)$  несистематического кода  $C$ .

Краткое изложение основных результатов настоящей статьи имеется в [4].

## 1. Предварительные сведения

Большая часть обозначений берется из работ [2, 3]. Пусть  $\{0, 1\}^n$  — векторное пространство над полем из двух элементов 0 и 1. Носитель вектора  $\mathbf{u} \in \{0, 1\}^n$  обозначается через  $[\mathbf{u}]$ . Базисный вектор, в котором  $i$ -я координата равна единице, обозначается через  $\mathbf{e}_i$ . Мы будем пользоваться следующим представлением кода Хемминга длины  $n = 2^k - 1$ . Каждому  $i = 0, \dots, n$  ставится в соответствие вектор  $(i_1, \dots, i_k) \in \{0, 1\}^k$ , представляющий число  $i$  в двоичной системе счисления. Считаем, что код Хемминга  $H^n$  состоит из всех векторов  $\mathbf{u} \in \{0, 1\}^n$  таких, что  $\bigoplus \{i \mid i \in [\mathbf{u}]\} = 0$ . Для  $i \in \{1, \dots, n\}$  минимальная  $i$ -компонента кода  $H^n$ , содержащая вектор  $\mathbf{u} \in H^n$ , обозначается через  $R_i^{\mathbf{u}}$ .

Множество всех векторов пространства  $\{0, 1\}^n$  разбивается на орбиты относительно группы перестановочных автоморфизмов  $\text{Sym}(H^n)$  кода  $H^n$ . Нас будут далее интересовать векторы  $\mathbf{h} \in H^n$  веса  $m = (n - 1)/2$ , которые образуют орбиту  $O_m^1$  длины  $n$ . Носители  $[\mathbf{h}]$  таких векторов  $\mathbf{h}$  являются  $(k - 2)$ -мерными подпространствами в проективной геометрии  $PG_{k-1}(2)$ . Назовем  $i$ -компоненту  $R_i^{\mathbf{u}}$  *антиподальной*  $i$ -компоненте  $R_i^{\mathbf{v}}$ , если существует вектор  $\mathbf{w} \in R_i^{\mathbf{u} \oplus \mathbf{v}} \cap O_m^1$  такой, что  $i \notin [\mathbf{w}]$ . Основное свойство антиподальных компонент состоит в следующем. Если при  $i \neq j$  компоненты  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{w}}$  не пересекаются, а компонента  $R_i^{\mathbf{v}}$  антиподальна к  $R_i^{\mathbf{u}}$ , то компоненты  $R_i^{\mathbf{v}}$  и  $R_j^{\mathbf{w}}$  не пересекаются (см. [3, лемма 8]).

Совершенный код  $C$  длины  $n = 2^k - 1$  называется *систематическим*, если существует  $k$ -элементное подмножество номеров  $K \subset \{1, \dots, n\}$  такое, что для любых двух различных векторов  $\mathbf{u}, \mathbf{v} \in C$  носитель их суммы  $[\mathbf{u} \oplus \mathbf{v}]$  не лежит в  $K$ . Это означает, что множество всех координат векторов  $\mathbf{u}$  кода  $C$  можно разбить на множество из  $n - k$  информационных координат  $u_{i_1} \dots u_{i_{n-k}}$  и множество из  $k$  проверочных координат  $u_{i_{n-k+1}} \dots u_{i_n}$ , которые являются функциями от информационных координат, т. е.  $u_{i_{n-k+1}} = f_1(u_{i_1}, \dots, u_{i_{n-k}}), \dots, u_{i_n} = f_k(u_{i_1}, \dots, u_{i_{n-k}})$ . В противном случае код  $C$  называется *несистематическим*.

Для любого кода  $C$  длины  $n$  можно построить расширенный код  $\tilde{C}$  длины  $n + 1$ , добавляя к векторам кода  $C$  проверку на четность в качестве

нулевой координаты. Обратно, если дан расширенный код  $\tilde{C}$ , то для любого  $i = 0, \dots, n$ , вычеркивая  $i$ -ю координату во всех векторах кода  $\tilde{C}$ , можно получить нерасширенный код  $\tilde{C}^i$ . В частности,  $\tilde{C}^0 = C$ .

**ОПРЕДЕЛЕНИЕ 1.** Расширенный код  $\tilde{C}$  длины  $n = 2^k$  называется *систематическим*, если существует  $(k + 1)$ -элементное подмножество номеров  $K \subset \{0, \dots, n\}$  такое, что для любых двух различных векторов  $u, v \in \tilde{C}$  носитель их суммы  $[u \oplus v]$  не лежит в  $K$ . В противном случае расширенный код  $\tilde{C}$  называется *несистематическим*.

Из этого определения следует, что расширенный код  $\tilde{C}$ , построенный из систематического совершенного кода  $C$ , является систематическим.

Из определения сразу же легко получается следующее утверждение.

**Лемма 1.** Расширенный код  $\tilde{C}$ , построенный из нерасширенного кода  $C$  длины  $n = 2^k - 1$ , является несистематическим тогда и только тогда, когда

- (а) код  $C$  является несистематическим;
- (б) для любого  $(k + 1)$ -элементного множества  $K \subset \{1, \dots, n\}$  существуют два различных вектора  $u, v \in C$  таких, что носитель их суммы  $[u \oplus v]$  содержится в  $K$  и содержит четное число элементов.

Легко устанавливается также взаимосвязь между двумя понятиями несистематичности для расширенных и нерасширенных кодов.

**Лемма 2.** Расширенный код  $\tilde{C}$  является несистематическим тогда и только тогда, когда каждый нерасширенный код  $\tilde{C}^i$ , полученный из  $\tilde{C}$  вычеркиванием  $i$ -й координаты ( $i = 0, \dots, n$ ), несистематичен.

В связи с этим полезно ввести следующее

**ОПРЕДЕЛЕНИЕ 2.** Расширенный код  $\tilde{C}$  длины  $n = 2^k$  называется *вполне систематическим*, если при любом  $i \in \{0, \dots, n\}$  существует  $(k + 1)$ -элементное подмножество  $K \subset \{0, \dots, n\}$  такое, что  $i \in K$  и для любых двух различных векторов  $u, v \in \tilde{C}$  носитель суммы  $[u \oplus v]$  не лежит в  $K$ .

Отличие этого определения от определения 1 состоит в том, что у вполне систематического кода любая наперед заданная координата может быть включена в список  $k + 1$  проверочных координат. Также имеет место связь с понятием систематичности нерасширенных кодов.

**Лемма 3.** Расширенный код  $\tilde{C}$  является вполне систематическим тогда и только тогда, когда каждый нерасширенный код  $\tilde{C}^i$  ( $i = 0, \dots, n$ ), полученный из  $\tilde{C}$  вычеркиванием  $i$ -й координаты, является систематическим.

Данные определения вполне систематичности и несистематичности расширенных кодов оправданы еще и тем, что существуют такие

несистематические коды, что порождаемые ими расширенные коды являются систематическими. Другими словами, существуют систематические, но не вполне систематические расширенные коды (см. пример 1).

Для любого  $i \in \{0, \dots, n\}$  рассмотрим перестановку  $\alpha_i(j) = i \oplus j$  ( $j = 0, \dots, n$ ). Эта перестановка осуществляет аффинный перенос пространства  $\{0, 1\}^k$ . Для любого совершенного кода  $C$  рассмотрим код  $a_i(C) = \alpha_i(\tilde{C})^i$ . Этот код получается из кода  $C$  перестановкой местами каждой  $j$ -й и  $(i \oplus j)$ -й координаты при  $j \neq i$  и заменой  $i$ -й координаты на проверку четности. Следовательно,  $a_i$  является линейным преобразованием с  $(n \times n)$ -матрицей, у которой каждая  $j$ -я строка при  $i \neq j$  содержит только одну единицу на  $(i \oplus j)$ -м месте, а  $i$ -я строка целиком состоит из единиц. Легко понять, что код  $a_i(C)$  можно получить из кода  $\tilde{C}^i$  с помощью некоторой перестановки координат. Кроме этого, очевидно, что  $a_0(C) = C$ . Поэтому имеет место

**Лемма 4.** *Расширенный код  $\tilde{C}$  является несистематическим (вполне систематическим) тогда и только тогда, когда для любого  $i = 0, \dots, n$  код  $a_i(C)$  является несистематическим (систематическим).*

## 2. Конструкция несистематических расширенных кодов

Обозначим через  $I_{\mathcal{B}}$  множество всех номеров  $i$  таких, что существуют  $i$ -компоненты, принадлежащие семейству  $\mathcal{B}$ . Рассмотрим независимое множество  $K \subset \{1, \dots, n\}$ . Положим  $L(K) = K \cup ((K \oplus K) \setminus \{0\})$ , т. е. в  $L(K)$  входят все элементы из  $K$  и все попарные суммы различных элементов из  $K$ . Векторы  $\mathbf{u} \in \{0, 1\}^n$ , носители которых совпадают с некоторым множеством  $L(K)$ , относительно группы перестановочных автоморфизмов кода  $H^n$  образуют одну орбиту веса  $k(k+1)/2$ , которую мы будем называть *максимальной систематической орбитой* кода  $H^n$ .

**Теорема 1.** *Пусть для некоторого независимого множества  $K$  и семейства  $\mathcal{B}$  непересекающихся компонент кода  $H^n$  множество  $I_{\mathcal{B}}$  является подмножеством множества  $L(K)$ . Тогда код  $C = H^n(\mathcal{B})$  является систематическим. Кроме этого, полученный из него расширенный код  $\tilde{C}$  является вполне систематическим.*

**Доказательство.** Для проверки систематичности будем использовать фигурирующее в формулировке теоремы независимое множество  $K$ . Пусть  $\mathbf{u}, \mathbf{v} \in C$  и  $\mathbf{u} \neq \mathbf{v}$ . Возможны три случая.

(i)  $\mathbf{u}, \mathbf{v} \in H^n$ . Тогда  $[\mathbf{u} \oplus \mathbf{v}] \not\subseteq K$ , так как  $K$  независимо.

(ii)  $\mathbf{u} \in H^n$  и  $\mathbf{v} \in C \setminus H^n$ . Это означает, что при некотором  $i \in L(K)$  вектор  $\mathbf{v} \oplus \mathbf{e}_i$  принадлежит  $i$ -компоненте семейства  $\mathcal{B}$ . Допустим, что

$[\mathbf{u} \oplus \mathbf{v}] \subset K$ . Если  $i \notin K$ , то  $i = j_1 \oplus j_2$  при некоторых  $j_1, j_2 \in K$ . Вектор  $\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_i$  принадлежит коду  $H^n$ . Поэтому вектор  $\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_{j_1} \oplus \mathbf{e}_{j_2}$  также принадлежит коду  $H^n$  и его носитель лежит в  $K$ . Значит,  $\mathbf{u} \oplus \mathbf{v} = \mathbf{e}_{j_1} \oplus \mathbf{e}_{j_2}$ , что противоречит тому, что  $H^n$  — код с расстоянием 3. Если  $i \in K$ , то  $[\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_i] \subseteq K$ , что противоречит независимости  $K$ .

(iii)  $\mathbf{u}, \mathbf{v} \in C \setminus H^n$ . В этом случае для некоторых  $i, i' \in L(K)$  вектор  $\mathbf{u} \oplus \mathbf{e}_i$  принадлежит  $i$ -компоненте, а вектор  $\mathbf{v} \oplus \mathbf{e}_{i'}$  принадлежит  $i'$ -компоненте семейства  $\mathcal{B}$ . Пусть  $[\mathbf{u} \oplus \mathbf{v}] \subset K$ . Если  $i, i' \notin K$ , то  $i = j_1 \oplus j_2$  и  $i' = j'_1 \oplus j'_2$  для некоторых  $j_1, j_2, j'_1, j'_2 \in K$ . Рассмотрим вектор  $\mathbf{w} \in H^n$  с носителем  $[\mathbf{w}] = \{i, j_1, j_2\}$  и вектор  $\mathbf{w}' \in H^n$  с носителем  $[\mathbf{w}'] = \{i', j'_1, j'_2\}$ . Вектор  $\mathbf{u} \oplus \mathbf{e}_i \oplus \mathbf{w} \oplus \mathbf{v} \oplus \mathbf{e}_{i'} \oplus \mathbf{w}'$  принадлежит коду  $H^n$ , и его носитель входит в  $K$ . Поэтому вектор  $\mathbf{u} \oplus \mathbf{e}_i \oplus \mathbf{v} \oplus \mathbf{e}_{i'}$  равен вектору  $\mathbf{w} \oplus \mathbf{w}'$ , принадлежащему сумме компонент  $R_i^0 \oplus R_{i'}^0$ . Это противоречит непересекаемости компонент семейства  $\mathcal{B}$ , содержащих соответственно векторы  $\mathbf{u} \oplus \mathbf{e}_i$  и  $\mathbf{v} \oplus \mathbf{e}_{i'}$ . Более простые случаи  $i \notin K, i' \in K$  и  $i, i' \in K$  рассматриваются аналогичным образом.

Осталось доказать, что расширенный код  $\tilde{C}$ , полученный из кода  $C$ , является вполне систематическим. Согласно лемме 4 для этого следует доказать систематичность всех кодов  $a_i(C)$ ,  $i = 1, \dots, n$ . Легко заметить, что  $a_i(H^n) = H^n$  и для любой  $i$ -компоненты  $R_i^{\mathbf{u}}$  из семейства  $\mathcal{B}$  имеет место равенство  $a_i(R_i^{\mathbf{u}}) = R_i^{a_i(\mathbf{u})}$ . Обозначим преобразованное таким образом семейство компонент через  $\mathcal{B}_i$ . Очевидно, что  $I_{\mathcal{B}} = I_{\mathcal{B}_i}$  и  $a_i(C) = H^n(\mathcal{B}_i)$ . Поэтому код  $a_i(C)$ , как только что доказано, является систематическим для каждого  $i = 1, \dots, n$ . Теорема доказана.

**ОПРЕДЕЛЕНИЕ 3.** Говорим, что вектор  $\mathbf{u} \in \{0, 1\}^n$  принадлежит *систематической орбите*, если существует такой вектор  $\mathbf{v}$  из максимальной систематической орбиты, что  $[\mathbf{u}] \subseteq [\mathbf{v}]$ . В противном случае говорим, что  $\mathbf{u}$  принадлежит *несистематической орбите*.

Оказывается, что для любого вектора  $\mathbf{u}$  из несистематической орбиты существует семейство непересекающихся компонент  $\mathcal{B}$  такое, что  $[\mathbf{u}] = I_{\mathcal{B}}$  и код  $C = H^n(\mathcal{B})$  является несистематическим. Приведем условия, которым должно удовлетворять семейство  $\mathcal{B}$ .

( $\alpha$ ) Для любого  $i \in I_{\mathcal{B}}$  существует  $i$ -компонента из семейства  $\mathcal{B}$ , расстояние Хемминга от которой до всех остальных  $i$ -компонент семейства больше  $k + 1$ .

( $\beta$ ) При  $i \in I_{\mathcal{B}}$  множество  $\cup \mathcal{B}$  не содержит ни одной  $i$ -компоненты, отличной от  $i$ -компонент семейства  $\mathcal{B}$ .

( $\gamma$ ) Для множества  $E = H^n \setminus (\cup \mathcal{B})$  сумма  $E \oplus E$  содержит все векторы кода  $H^n$ , вес которых не больше  $k + 1$ .

( $\delta$ ) Существует такой вектор  $\mathbf{u}$  из несистематической орбиты, что  $[\mathbf{u}] = I_{\mathcal{B}}$ .

Идея использования в доказательстве несистематичности условия ( $\beta$ ) применялась ранее в [9].

**Теорема 2.** Пусть семейство  $\mathcal{B}$  непересекающихся  $i$ -компонент кода  $H^n$  удовлетворяет условиям ( $\alpha$ )–( $\delta$ ). Тогда  $C = H^n(\mathcal{B})$  и полученный из него расширенный код  $\tilde{C}$  является несистематическим.

**Доказательство.** Сначала докажем, что код  $C$  является несистематическим. Рассмотрим любое зависимое множество  $K$ , состоящее из  $k$  элементов. В этом случае существует ненулевой вектор  $\mathbf{u} \in H^n$  с носителем  $[\mathbf{u}] \subseteq K$ . По условию ( $\gamma$ ) такой вектор можно представить в виде суммы двух векторов  $\mathbf{u}, \mathbf{v} \in E = C \cap H^n$ . Теперь рассмотрим независимое  $k$ -элементное множество  $K$ . Так как множество  $I_{\mathcal{B}}$  является носителем вектора  $\mathbf{u}$  из несистематической орбиты, то существует  $i \in I_{\mathcal{B}} \setminus L(K)$ . Так как множество  $K$  является базисным, то  $i = j_1 \oplus \dots \oplus j_s$  для некоторых  $j_1, \dots, j_s \in K$ ,  $3 \leq s \leq k$ . Вектор  $\mathbf{v}$  с носителем  $\{i, j_1, \dots, j_s\}$  принадлежит коду  $H^n$ . По условию ( $\alpha$ ) существует такая  $i$ -компонента  $R_i^{\mathbf{w}}$  из семейства  $\mathcal{B}$ , что компонента  $R_i^{\mathbf{v} \oplus \mathbf{w}}$  не принадлежит семейству  $\mathcal{B}$ . По условию ( $\beta$ ) существует вектор  $\mathbf{w}_1 \in R_i^{\mathbf{v} \oplus \mathbf{w}} \setminus (\cup \mathcal{B})$ . Тогда векторы  $\mathbf{w}_1$  и  $\mathbf{w}_2 = \mathbf{w}_1 \oplus \mathbf{v} \oplus \mathbf{e}_i$  принадлежат коду  $C$ , причем  $[\mathbf{w}_1 \oplus \mathbf{w}_2]$  лежит в  $K$ . Следовательно, код  $C$  является несистематическим, причем для доказательства этого факта условия ( $\alpha$ ) и ( $\gamma$ ) можно ослабить, заменив в них  $k+1$  на  $k$ .

Осталось выяснить, будет ли расширенный код  $\tilde{C}$ , полученный из кода  $C$ , несистематическим. Рассмотрим любое  $(k+1)$ -элементное множество координат  $K'$ . Допустим, что в  $K'$  существует по крайней мере два различных непустых подмножества  $L$  и  $M$  с нулевыми суммами. Рассмотрим вектор  $\mathbf{u}$  с носителем  $[\mathbf{u}] = L$  и вектор  $\mathbf{v}$  с носителем  $[\mathbf{v}] = M$ . Очевидно, что  $\mathbf{u}, \mathbf{v} \in H^n$ , причем либо  $[\mathbf{u}]$ , либо  $[\mathbf{v}]$ , либо  $[\mathbf{u} \oplus \mathbf{v}]$  состоит из четного числа элементов. В зависимости от этого полагаем либо  $\mathbf{w} = \mathbf{u}$ , либо  $\mathbf{w} = \mathbf{v}$ , либо  $\mathbf{w} = \mathbf{u} \oplus \mathbf{v}$ . По условию ( $\gamma$ ) вектор  $\mathbf{w} \neq \mathbf{0}$  можно представить суммой двух векторов из множества  $E = C \cap H^n$ .

Рассмотрим случай, когда в зависимом множестве  $K'$  содержится только одно непустое подмножество  $M$  с нулевой суммой. Можно считать, что  $M$  состоит из нечетного числа элементов. Положим  $L'(K') = (K' \oplus K') \setminus \{0\}$ . Рассмотрим любой элемент  $j \in K'$  и определим множество  $K = (K' \setminus \{j\}) \oplus j$ . Множество  $K$  является независимым. В противном случае в множестве  $K'$  содержится непустое подмножество с четным числом элементов и нулевой суммой. Кроме этого, имеем  $L'(K') \setminus K = (K \oplus K) \setminus \{0\}$ . Это означает, что  $L'(K') = L(K)$ .

По условию  $(\delta)$  множество  $I_{\mathcal{Q}}$  не входит в  $L(K)$ . Возьмем любое  $i \in I_{\mathcal{Q}} \setminus L'(K')$ . В множестве  $K'$  имеется  $2^k - 1 = n$  различных непустых подмножеств с четным числом элементов. Так как в  $K'$  нет непустых подмножеств с четным числом элементов и нулевой суммой, то все суммы таких подмножеств различны. Поэтому  $i = j_1 \oplus \dots \oplus j_s$  для некоторых  $j_1, \dots, j_s$  и четного  $s$ ,  $4 \leq s \leq k + 1$ . Вектор  $\mathbf{v}$  с носителем  $\{i, j_1, \dots, j_s\}$  принадлежит коду  $H^n$ . Доказательство можно закончить так же, как и в предыдущем случае. Теорема доказана.

Задача о построении несистематических кодов фактически свелась к задаче перечисления несистематических орбит пространства  $\{0, 1\}^n$ . В частности, любой вектор веса больше  $k(k + 1)/2$  принадлежит несистематической орбите. Орбиты векторов пространства  $\{0, 1\}^n$  можно задавать с помощью уравнений (см. [3, лемма 1]). С каждой орбитой веса  $t$  сопоставляется матрица  $(b_{pq})$  размера  $(m - r) \times r$  над полем  $\{0, 1\}$  с попарно различными строками ( $p = r + 1, \dots, m$ ;  $q = 1, \dots, r$ ). Тогда носителями векторов из данной орбиты являются всевозможные множества  $\{i_1, \dots, i_m\}$  такие, что  $i_p = b_{p1}i_1 \oplus \dots \oplus b_{pr}i_r$  ( $p = r + 1, \dots, m$ ), а  $i_1, \dots, i_r$  пробегает все линейно независимые наборы из  $\{0, 1\}^k$ . Аналогичное представление орбит булевых функций рассматривалось в [5]. В случае  $r < k$  следующая лемма сводит проверку несистематичности орбиты в пространстве  $\{0, 1\}^n$  к проверке несистематичности орбиты с этим же уравнением в пространстве  $\{0, 1\}^{n'}$  для  $n' = 2^r - 1$ .

**Лемма 5.** Если вектор  $\mathbf{u} \in \{0, 1\}^n$  принадлежит систематической орбите и ранг множества  $[\mathbf{u}]$  (в пространстве  $\{0, 1\}^k$ ) равен  $r$ , где  $r < k$ , то существует независимое  $r$ -элементное множество  $R \subset \{1, \dots, n\}$  такое, что  $[\mathbf{u}] \subseteq L(R)$ .

**Доказательство.** Пусть  $[\mathbf{u}] = \{i_1, \dots, i_m\}$ , где элементы  $i_1, \dots, i_r$  линейно независимы, и для некоторых подмножеств  $I_p \subseteq \{i_1, \dots, i_r\}$  имеют место разложения

$$i_p = \bigoplus \{i_q \mid q \in I_p\} \quad (p = r + 1, \dots, m). \quad (1)$$

Так как вектор  $\mathbf{u}$  принадлежит систематической орбите, то существует базисный набор  $\{j_1, \dots, j_k\}$  такой, что любой элемент множества  $\{i_1, \dots, i_m\}$  является либо одним из базисных элементов, либо суммой двух базисных элементов. Так как элементы  $i_1, \dots, i_r$  независимы, то можно переобозначить  $j_1, \dots, j_k$  так, чтобы первые  $r$  уравнений имели вид

$$i_1 = j_1 \oplus j_{p_1}, \dots, i_r = j_r \oplus j_{p_r}, \quad (2)$$

где  $0 \leq p_s \leq r$  при  $1 \leq s \leq r$  (здесь  $j_0 = 0$ ). После подстановки (2) в (1) и проведения сокращений получим задание всех  $i_p$ , где  $p > r$ , через  $j_p$



и  $j_p \oplus j_{p'}$ . Заменяем в уравнениях (2) все  $j_p$ , при  $p > r$  на нули. Допустим, что после этого правые части равенств (2) принимают вид

$$j_1 \oplus j_{q_1}, \dots, j_r \oplus j_{q_r}, \quad (3)$$

где  $0 \leq q_s \leq r$  ( $s = 1, \dots, r$ ). Нужно только убедиться, что все элементы (3) останутся линейно независимыми. Допустим, что для некоторого непустого  $Q \subset \{1, \dots, k\}$  сумма  $\oplus \{j_s \oplus j_{p_s} \mid s \in Q\}$  равна нулю. Сократиться могут только элементы  $j_s$  с элементами  $j_{q_s}$  при некоторых  $t \neq s$ . Поэтому ни одно  $j_{q_t}$  не может быть равно нулю, и мы получили зависимость правых частей первоначальной системы равенств (2), а это противоречит независимости элементов  $i_1, \dots, i_r$ . Существует перестановка из группы  $\text{Sym}(H^n)$ , переводящая набор элементов из (3) в  $i_1, \dots, i_r$ . При этом элементы  $j_1, \dots, j_r$  перейдут в независимые элементы  $j'_1, \dots, j'_r$ . В результате получим равенства

$$i_1 = j'_1 \oplus j'_{q_1}, \dots, i_r = j'_r \oplus j'_{q_r}.$$

После подстановки этих равенств в правые части из (1) мы проведем те же самые сокращения элементов  $j'_{q'}$ , которые проводились с элементами  $j_q$  при  $q \leq r$  после подстановки в (1) первоначальных равенств (2). Тогда получим выражения всех  $i_p$  при  $p > r$  через  $j'_p$  и  $j'_p \oplus j'_{p'}$  ( $1 \leq p \leq r, 1 \leq p' \leq r$ ). Лемма доказана.

Если орбита в пространстве  $\{0, 1\}^{n'}$  задается уравнением (1), то ей соответствует орбита с точно таким же уравнением в любом пространстве  $\{0, 1\}^n$  большей размерности. Из леммы 5 следует, что при таком соответствии свойство орбиты быть систематической (несистематической) сохраняется.

*Рангом* орбиты называем ранг (в пространстве  $\{0, 1\}^k$ ) носителя  $[\mathbf{u}]$  любого вектора  $\mathbf{u}$  из этой орбиты. Легко проверяется справедливость следующего утверждения.

**Лемма 6.** Все орбиты веса больше  $k(k+1)/2$  являются несистематическими. Любая орбита веса  $p$  и ранга  $r \geq p-2$  является систематической.

**Доказательство.** Первое утверждение леммы очевидно в силу того, что для независимого  $k$ -элементного множества  $K$  число элементов в множестве  $L(K)$  равно  $k(k+1)/2$ . Второе утверждение тоже очевидно для орбит ранга  $r = p$ . Пусть  $r = p-1$  и вектор  $\mathbf{u}$  из этой орбиты имеет носитель  $\{i_1, \dots, i_p\}$ , где  $i_1, \dots, i_{p-1}$  линейно независимы, а  $i_p = i_1 \oplus \dots \oplus i_s$  при некотором  $s \leq p-1$ . Полагаем  $j_1 = i_1, j_2 = i_1 \oplus i_2, \dots, j_s = i_1 \oplus \dots \oplus i_s, j_{s+1} = i_{s+1}, \dots, j_{p-1} = i_{p-1}$ . Пусть  $R = \{j_1, \dots, j_{p-1}\}$ . Тогда  $i_1 = j_1, i_2 = j_1 \oplus j_2, \dots, i_s = j_{s-1} \oplus j_s, i_{s+1} = j_{s+1}, \dots, i_{p-1} = j_{p-1}, i_p = j_s$ , т. е.  $[\mathbf{u}] \subseteq L(R)$ . Пусть теперь  $r = p-2$  и  $[\mathbf{u}] = \{i_1, \dots, i_p\}$ , где  $i_1, \dots, i_{p-2}$

линейно независимы, а  $i_{p-1} = i_1 \oplus \dots \oplus i_s$ ,  $i_p = i_q \oplus \dots \oplus i_{p-2}$ . Если  $s < q$ , то определяем  $j_1, \dots, j_s$  через  $i_1, \dots, i_s$  и  $j_q, \dots, j_{p-2}$  через  $i_q, \dots, i_{p-2}$  по формулам, аналогичным предыдущему случаю. Пусть  $s \geq q$ . Тогда делаем следующую замену:  $j_q = i_q$ ,  $j_{q+1} = i_q \oplus i_{q+1}, \dots, j_s = i_q \oplus \dots \oplus i_s$ ,  $j_1 = i_1 \oplus j_s, \dots, j_{q-1} = i_1 \oplus \dots \oplus i_{q-1} \oplus j_s$ ,  $j_{s+1} = i_{s+1} \oplus j_s, \dots, j_{p-2} = i_{s+1} \oplus \dots \oplus i_{p-2} \oplus j_s$ . Пусть  $R = \{j_1, \dots, j_{p-2}\}$ . Легко видеть, что, выразив все  $i_l$  через  $j_l$ , мы опять получим включение  $[u] \subseteq L(R)$ . Лемма доказана.

Лемма 6 дает возможность легко проверять на систематичность орбиты небольшого веса. Совершенно неожиданным оказался следующий факт.

**Следствие 1.** Все векторы веса меньше 7 принадлежат систематическим орбитам. Для любого  $n \geq 15$  ( $n = 2^k - 1$ ) в пространстве  $\{0, 1\}^n$  существуют две различные несистематические орбиты веса 7.

Доказательство. По лемме 6 все орбиты, имеющие вес 3, 4 и 5, и все орбиты веса 6 и ранга больше 3 являются систематическими. В [3, теорема 1] перечислены орбиты в пространстве  $\{0, 1\}^{15}$  и приведены определяющие их уравнения. Среди орбит веса 6 есть только одна орбита ранга 3, задающаяся уравнениями  $i_4 = i_1 \oplus i_2$ ,  $i_5 = i_1 \oplus i_3$ ,  $i_6 = i_2 \oplus i_3$ . Следовательно, все орбиты веса 6 являются систематическими.

Рассмотрим орбиты веса 7. По лемме 6 все орбиты ранга больше 4 являются систематическими. Орбиты ранга не больше 4 перечислены в [3]. Их уравнения приведены в табл. 1. Здесь носитель вектора  $u$  из орбиты  $O_7^l$  имеет вид  $[u] = \{i_1, \dots, i_7\}$ , где выражение элементов  $i_p$  через новые независимые элементы  $j_1, j_2, j_3, j_4$  показывает систематичность данной орбиты.

Т а б л и ц а 1

$i \setminus$	$O_7^1$	$O_7^2$	$O_7^3$	$O_7^4$	$O_7^5$	$O_7^6$
$i_1 =$	$i_1$	$j_1$	$i_1$	$j_1$	$j_1 \oplus j_2$	$j_1$
$i_2 =$	$i_2$	$j_2$	$i_2$	$j_2$	$j_2$	$j_2$
$i_3 =$	$i_3$	$j_3$	$i_3$	$j_3$	$j_3$	$j_2 \oplus j_3$
$i_4 =$	$i_1 \oplus i_2$	$j_4$	$i_4$	$j_4$	$j_4$	$j_4$
$i_5 =$	$i_2 \oplus i_3$	$j_1 \oplus j_2$	$i_1 \oplus i_2 \oplus i_3$	$j_1 \oplus j_2$	$j_2 \oplus j_3$	$j_1 \oplus j_3$
$i_6 =$	$i_1 \oplus i_3$	$j_1 \oplus j_3$	$i_1 \oplus i_2 \oplus i_4$	$j_2 \oplus j_3$	$j_1 \oplus j_3$	$j_3 \oplus j_4$
$i_7 =$	$i_1 \oplus i_2 \oplus i_3$	$j_1 \oplus j_3$	$i_1 \oplus i_3 \oplus i_4$	$j_1 \oplus j_3$	$j_2 \oplus j_4$	$j_1 \oplus j_4$

Рассмотрим орбиту  $O_7^1$ , векторы которой задаются следующими уравнениями:  $i_4 = i_1 \oplus i_2$ ,  $i_5 = i_2 \oplus i_3$ ,  $i_6 = i_1 \oplus i_3$ ,  $i_7 = i_1 \oplus i_2 \oplus i_3$ , а тройка  $i_1, i_2, i_3$  линейно независима. Допустим, что представление, требуемое для доказательства систематичности, удалось найти, т. е.

все элементы  $i_p$  являются либо базисными элементами  $j_p$ , либо суммами двух базисных элементов из нового независимого набора  $\{j_1, j_2, j_3\}$  (в силу леммы 5 можно считать, что орбита  $O_7^1$  лежит в пространстве  $\{0, 1\}^7$ ). Из трехэлементного набора можно получить только шесть различных комбинаций данного типа. Поэтому один из семи элементов  $i_p$  является суммой трех элементов  $j_1, j_2, j_3$ , что доказывает несистематичность орбиты  $O_7^1$ .

Обратимся теперь к орбите  $O_7^3$ , которая задается следующими уравнениями:

$$i_5 = i_1 \oplus i_2 \oplus i_3, \quad i_6 = i_1 \oplus i_2 \oplus i_4, \quad i_7 = i_1 \oplus i_3 \oplus i_4, \quad (4)$$

где  $i_1, i_2, i_3, i_4$  линейно независимы. По лемме 5 несистематичность такой орбиты достаточно доказать в пространстве  $\{0, 1\}^{15}$ . Рассмотрим любую независимую четверку  $K = \{j_1, j_2, j_3, j_4\}$  такую, что каждый элемент  $i_p$  принадлежит либо  $K$ , либо  $K \oplus K$ . Переобозначая элементы из  $K$ , можно добиться того, чтобы первые четыре уравнения приняли вид  $i_1 = j_1 \oplus j_{p_1}, i_2 = j_2 \oplus j_{p_2}, i_3 = j_3 \oplus j_{p_3}, i_4 = j_4 \oplus j_{p_4}$ , где все индексы  $p_s \leq 4$  ( $s = 0, 1, 2, 3, 4$ ). Здесь также используется элемент  $j_0 = 0$ . Теперь следует непосредственно подставлять эти выражения для  $i_1, \dots, i_4$  в уравнения (4) и убеждаться в том, что после всех сокращений хотя бы одна правая часть получающихся равенств будет иметь более двух ненулевых слагаемых. Следствие доказано.

**Лемма 7.** Если число элементов подмножества  $D \subseteq H^n$  больше  $|H^n|/2$ , то  $D \oplus D = H^n$ .

**Доказательство.** Фиксируем любой вектор  $u \in H^n$  и разбиваем код  $H^n$  на пары  $\{v, w\}$  такие, что  $u = v \oplus w$ . По условию леммы найдется хотя бы одна такая пара  $\{v, w\}$ , которая лежит в  $D$ . Поэтому  $u \in D \oplus D$ . Лемма доказана.

Для построения несистематических расширенных кодов достаточно, чтобы множество  $I_{\mathcal{B}}$  состояло из семи номеров. Кроме этого, в силу леммы 6 условия  $(\alpha), (\beta), (\gamma)$  удовлетворяются автоматически, если рассматривать семейство непересекающихся компонент  $\mathcal{B}$ , не содержащих «кратных» компонент, т. е. для любого  $i \in \{1, \dots, n\}$  существует не более одной  $i$ -компоненты из  $\mathcal{B}$ . Именно такие семейства рассматривались ранее в [1, 9] для построения несистематических кодов.

При  $n \geq 31$  семейство из семи непересекающихся компонент кода  $H^n$  легко строится с помощью применяемого в [1, 8, 9] мощностного подхода. Для замкнутости изложения напомним здесь эту конструкцию. Рассмотрим любое множество номеров  $\{i_1, \dots, i_m\} \subseteq \{1, \dots, n\}$ . Компоненту  $R_{i_1}^{u_1}$  выбираем в коде  $H^n$  произвольным образом. Продолжая индуктивно этот процесс, при любом  $p = 2, \dots, m$  выбираем компоненту  $R_{i_p}^{u_p}$  так,

чтобы она не пересекалась с множеством  $\cup \{R_{i_q}^{u_q} \oplus R_{i_p}^0 \mid q = 1, \dots, p-1\}$ . Так как  $m \leq n$ , то при  $n \geq 31$  такой выбор всегда возможен. Для  $n = 15$  семейства непересекающихся  $i$ -компонент, когда  $i$  пробегает семь (или восемь) значений, были впервые построены в [6, 9]. Как оказалось, в этом случае  $i$  принадлежит семиэлементному множеству, являющемуся носителем вектора из орбиты  $O_7^3$ . В [3] перечислены все коды длины 15, которые получаются из кода Хемминга  $H^{15}$  сдвигами по соответствующим координатам его непересекающихся компонент. Исходя из этой классификации, можно, в частности, утверждать, что не существует семейств непересекающихся  $i$ -компонент кода  $H^{15}$  таких, что  $i$  принимает все значения из носителя некоторого вектора орбиты  $O_7^1$ . Такие семейства непересекающихся  $i$ -компонент кода  $H^n$  появляются только начиная с  $n = 31$ .

Теперь, подводя итог, сформулируем следующую теорему.

**Теорема 3.** При любом  $k \geq 4$  существует несистематический совершенный код  $C$  длины  $n = 2^k - 1$ , который может быть получен из кода Хемминга  $H^n$  сдвигами семи непересекающихся  $i$ -компонент, где  $i$  принимает значения из носителя некоторого вектора орбиты  $O_7^3$ . При этом полученный из  $C$  расширенный код  $\tilde{C}$  является несистематическим.

В [9] был поставлен следующий вопрос. Какое наименьшее число компонент для построения несистематического кода необходимо сдвинуть в коде Хемминга  $H^n$ ? Следствие 1 и теорема 3 дают ответ на этот вопрос. Явный вид представителей семи непересекающихся компонент кода  $H^n$  получается просто добавлением соответствующего числа нулевых координат к векторам, которые предлагаются в [6, 9] в качестве представителей компонент для построения несистематического кода длины 15.

### 3. Несистематические расширенные коды длины 16

В [3, теорема 2] перечислены все совершенные коды длины 15, которые могут быть получены из кода Хемминга  $H^{15}$  сдвигами по соответствующим координатам некоторого семейства его непересекающихся  $i$ -компонент. В [3] также доказано, что любое семейство непересекающихся компонент кода  $H^{15}$  является частью либо некоторого  $(k \times l)$ -разбиения кода  $H^{15}$  ( $k = 1, 2, 4, 8$ ;  $l = 16/k$ ), либо тупикового набора из десяти компонент, содержащего по две  $i$ -компоненты, когда  $i$  пробегает пять значений. В соответствии с этим код называется  $(k \times l)$ -кодом, если он получается из  $H^{15}$  сдвигами по соответствующим координатам некоторых компонент либо одного из  $(k \times l)$ -разбиений (при  $k = 1, 2, 4, 8$ ;  $l = 16/k$ ), либо тупикового набора из десяти компонент

(при  $k = 5$ ,  $l = 2$ ). При построении  $(k \times l)$ -кода число сдвигаемых координат не превышает  $k$ . Из теоремы 1 и следствия 1 вытекает следующее

**Следствие 2.** Все  $(k \times l)$ -коды длины 15 при  $k = 1, 2, 4$ ,  $l = 16/k$  и все  $(5 \times 2)$ -коды являются систематическими. Все  $(8 \times 2)$ -коды, которые получены из кода  $H^{15}$  сдвигами непересекающихся  $i$ -компонент, когда  $i$  пробегает меньше семи значений, являются систематическими.

Рассмотрим семейство непересекающихся  $i$ -компонент  $\mathcal{B}$  из некоторого  $(8 \times 2)$ -разбиения кода  $H^{15}$ , удовлетворяющее следующим двум условиям.

(А) Существуют такие четыре  $i$ -компоненты  $R_{i_1}^{u_1}, R_{i_2}^{u_2}, R_{i_3}^{u_3}, R_{i_4}^{u_4}$ , непересекающиеся с компонентами семейства  $\mathcal{B}$ , что множество номеров  $\{i_1, i_2, i_3, i_4\}$  является независимым.

(В) Множество  $I_{\mathcal{B}}$  содержит по крайней мере семь элементов.

Компьютерная проверка показала, что именно такие семейства непересекающихся  $i$ -компонент кода  $H^{15}$  порождают несистематические коды длины 15. Приведем здесь теоретическое подтверждение этих фактов.

**Теорема 4.** Пусть семейство  $\mathcal{B}$  непересекающихся  $i$ -компонент из  $(8 \times 2)$ -разбиения кода  $H^{15}$  удовлетворяет условиям (А) и (В). Тогда совершенный код  $C = H^{15}(\mathcal{B})$  и полученный из него расширенный код  $\tilde{C}$  являются несистематическими. Во всех остальных случаях код  $C$  систематический, а полученный из него расширенный код  $\tilde{C}$  вполне систематический.

**Доказательство.** Достаточно проверить справедливость условий  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$  и  $(\delta)$ . Условие  $(\alpha)$  верно в силу того, что при любом  $i \in I_{\mathcal{B}}$  в  $(8 \times 2)$ -разбиении имеются только две антиподальные друг другу  $i$ -компоненты. Расстояние между ними равно 7, что больше  $k + 1 = 5$ .

Убедимся в справедливости условия  $(\beta)$ . В [3] доказано, что существует 64 различных  $(8 \times 2)$ -разбиения, которые получаются друг из друга переносами на векторы из  $H^{15}$ . Поэтому без ограничения общности можно рассмотреть первое разбиение, которое приведено в [3, табл. 4]. Пусть  $i$ -компонента  $R_i^u$ , не входящая в это разбиение, входит в объединение семейства  $\mathcal{B}$ . Согласно лемме 8 из [3] если компонента из  $\mathcal{B}$  пересекается с компонентой  $R_i^u$ , то антиподальная ей компонента также пересекается с  $R_i^u$ . Всего с компонентой  $R_i^u$  пересекается восемь компонент из семейства  $\mathcal{B}$ , составляющих четыре антиподальные пары. Среди них можно выбрать четыре  $R_{i_p}^{v_p}$  ( $p = 1, 2, 3, 4$ ). Так как компонента  $R_i^u$  не совпадает ни с одной компонентой  $R_{i_p}^{v_p}$  ( $p = 1, 2, 3, 4$ ) и пересекается с каждой из них, то  $i \neq i_1, i_2, i_3, i_4$ . Допустим, что  $i = i_1 \oplus i_2 \oplus i_3$ . С помощью перестановки из группы  $\text{Sym}(H^{15})$ , переноса на подходящий вектор из  $H^{15}$  и замены компонент на антиподальные, можно добиться

того, чтобы выполнялось  $i_1 = 8, i_2 = 10, i_3 = 12, i = 14, \mathbf{v}_1 = \mathbf{0}, [\mathbf{v}_2] = \{2, 3, 4, 5\}, [\mathbf{v}_3] = \{1, 3, 4, 6\}$ . При этом либо  $\mathbf{u} = \mathbf{0}$ , либо  $[\mathbf{u}]$  является кодовой четверкой из  $\{1, \dots, 7\}$ . Мы будем пользоваться следующим критерием непересекаемости компонент. Компоненты  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{v}}$  не пересекаются тогда и только тогда, когда множество  $[\mathbf{u} \oplus \mathbf{v}] \setminus \{i \oplus j\}$  состоит из нечетного числа элементов (см. [3, лемма 5] и [7, лемма 4]).

В силу этого критерия в случае  $\mathbf{u} = \mathbf{0}$  получаем непересекаемость компонент  $R_i^{\mathbf{u}}$  и  $R_{i_3}^{\mathbf{v}_3}$ . Если  $[\mathbf{u}] = \{2, 3, 6, 7\}$ , то компонента  $R_i^{\mathbf{u}}$  попадает в рассматриваемое  $(8 \times 2)$ -разбиение, что противоречит нашему предположению. Если  $[\mathbf{u}] = \{1, 2, 5, 6\}$ , то компоненты  $R_{i_p}^{\mathbf{v}_p}$  ( $p = 1, 2, 3$ ) вместе с  $R_i^{\mathbf{u}}$  попадают в первое  $(4 \times 4)$ -разбиение, которое приведено в [3, табл. 3]. В оставшихся пяти случаях, когда  $[\mathbf{u}]$  равно одному из множеств  $\{1, 3, 5, 7\}, \{2, 3, 4, 5\}, \{1, 2, 4, 7\}, \{4, 5, 6, 7\}, \{1, 3, 4, 6\}$ , компонента  $R_i^{\mathbf{u}}$  не будет пересекаться с одной из компонент  $R_{i_p}^{\mathbf{v}_p}$  ( $p = 1, 2, 3$ ). Поэтому можно считать, что  $i \neq i_1 \oplus i_2 \oplus i_3$ . С помощью перестановки  $\pi \in \text{Sym}(H^{15})$  такой, что  $\pi(8) = 8, \pi(10) = 10, \pi(12) = 12, \pi(i) = 9$ , и переноса на подходящий вектор из  $H^{15}$  можно добиться выполнения равенства  $i = 9$ . Переходя при необходимости к антиподальной компоненте, можно опять считать, что вектор  $\mathbf{u}$  имеет четный вес. Действуя аналогичным образом, мы найдем, что только при  $[\mathbf{u}] = \{2, 3, 6, 7\}$  компонента  $R_i^{\mathbf{u}}$  пересекается со всеми тремя компонентами  $R_{i_p}^{\mathbf{v}_p}$  ( $p = 1, 2, 3$ ). Она также пересекается с компонентой  $R_{i_4}^{\mathbf{v}_4}$  из рассматриваемого  $(8 \times 2)$ -разбиения, где  $\mathbf{v}_4 = \mathbf{u}$ . Итак, мы показали, что  $i_4 = i_1 \oplus i_2 \oplus i_3$ . Поэтому если  $i \in I_{\mathcal{B}}$  и компонента  $R_i^{\mathbf{u}}$  не входит в семейство  $\mathcal{B}$ , то при выполнении условия (А)  $R_i^{\mathbf{u}}$  не будет входить в объединение компонент семейства  $\mathcal{B}$ .

Докажем теперь справедливость условия  $(\gamma)$ . Рассмотрим компоненты  $R_{i_p}^{\mathbf{u}_p}$  ( $p = 1, 2, 3, 4$ ), которые в силу условия (А) не пересекаются с компонентами семейства  $\mathcal{B}$ . Осуществляя соответствующую перестановку координат из группы  $\text{Sym}(H^{15})$ , можно считать, что  $i_p \geq 8$ . Для  $\mathbf{h} = \{1, \dots, 7\}$  рассмотрим в  $H^{15}$  подкод  $H^7(\mathbf{h})$ , состоящий из всех векторов  $\mathbf{v} \in H^{15}$  таких, что  $[\mathbf{v}] \subseteq [\mathbf{h}]$ . При любом  $p = 1, 2, 3$  множества  $R_{j_p}^{\mathbf{u}_p}(\mathbf{h}) = (R_{i_4}^{\mathbf{u}_4} \oplus R_{i_p}^{\mathbf{u}_p}) \cap H^7(\mathbf{h})$  являются  $j_p$ -компонентами кода  $H^7(\mathbf{h})$ , где  $j_p = i_4 \oplus i_p$ . Каждая такая  $j_p$ -компонента не содержит нуля и состоит из всех векторов веса 4, в которых  $j_p$ -я координата равна 1, и векторов веса 3, в которых  $j_p$ -я координата равна 0. В силу независимости множества  $\{i_1, i_2, i_3, i_4\}$  множество  $J = \{j_1, j_2, j_3\}$  также независимо. Поэтому для любого вектора  $\mathbf{v} \in H^7(\mathbf{h})$  веса 4 носитель  $[\mathbf{v}]$  пересекается с  $J$ , т. е. принадлежит некоторой компоненте  $R_{j_p}^{\mathbf{u}_p}(\mathbf{h})$ . То же самое можно сказать про векторы веса 3. Следовательно, компоненты  $R_{i_4}^{\mathbf{u}_4} \oplus R_{i_p}^{\mathbf{u}_p}$  и компонента  $R_{i_4}^{\mathbf{u}_4} \oplus R_{i_4}^{\mathbf{u}_4}$ , являющиеся объединениями  $i_4$ -компонент, содержат все векторы кода  $H^7(\mathbf{h})$ , кроме вектора  $\mathbf{h}$ . Но компонента  $R_{i_4}^{\mathbf{h}}$  состоит только

из векторов веса 7 и 8 (факт существования  $i$ -компоненты, лежащей в двух средних слоях кода Хемминга  $H^n$ , был обнаружен С. В. Августиновичем). Поэтому объединение  $\cup\{R_{i_p}^{u_p} \oplus R_{i_4}^{u_4} \mid p = 1, 2, 3, 4\}$  содержит все векторы кода  $H^{15}$  веса меньше семи.

Условие  $(\delta)$  очевидным образом выполняется, так как из условия (В) следует, что множество  $I_{\mathcal{B}}$  соответствует орбите  $O_7^3$  [3] (лемма 3). Поэтому из теоремы 3 следует несистематичность кода  $C$  и полученного из него расширенного кода  $\tilde{C}$ .

Осталось убедиться в систематичности кода  $C$ , когда условие (А) не выполняется, а условие (В) выполняется. Только этот случай не был рассмотрен в следствии 2. Допустим, что  $R_{i_p}^{u_p}$ ,  $p = 1, \dots, r$  ( $r \leq 4$ ) — это все компоненты из рассматриваемого  $(8 \times 2)$ -разбиения, не пересекающиеся с компонентами семейства  $\mathcal{B}$ . Множество индексов  $i_p$  ( $1 \leq p \leq r$ ) доопределим до четверки  $i_p \in I_{\mathcal{B}}$  ( $p = 1, 2, 3, 4$ ) так, чтобы выполнялось равенство  $i_1 \oplus i_2 \oplus i_3 \oplus i_4 = 0$ . В случае  $r = 0$  семейство компонент  $\mathcal{B}$  совпадает со всем  $(8 \times 2)$ -разбиением, и в этом случае четверка номеров координат с нулевой суммой  $I = \{i_1, i_2, i_3, i_4\} \subset I_{\mathcal{B}}$  выбирается произвольным образом. Применяя соответствующую перестановку координат из  $\text{Sym}(H^{15})$ , можно считать, что все  $i_p \geq 8$  ( $p = 1, 2, 3, 4$ ). Из зависимости множества  $I$  следует существование такого вектора  $\mathbf{v} \in H^7(\mathbf{h})$  веса 3, что  $i_p \oplus i_q \in [\mathbf{v}]$  для любых  $p \neq q$ . Это означает, что  $\mathbf{v} \notin R_{i_p}^{u_p} \oplus R_{i_q}^{u_q}$  при любых  $p, q \leq r$ . Пусть  $\mathbf{u} \in H^{15}$  — вектор с носителем  $[\mathbf{u}] = I$ . Так как  $\mathbf{u} \oplus \mathbf{v} \in R_{i_p}^0$  при каждом  $p \leq r$ , то отсюда также следует, что  $\mathbf{u} \notin R_{i_p}^{u_p} \oplus R_{i_q}^{u_q}$  для любых  $p, q \leq r$ . Для проверки систематичности кода  $C$ , рассматриваемого в условии теоремы, возьмем множество номеров  $I$ . Пусть  $\mathbf{u}, \mathbf{v} \in C$  и  $\mathbf{u} \neq \mathbf{v}$ . Возможны три различных случая.

(а)  $\mathbf{u}, \mathbf{v} \in H^{15}$ . Тогда  $\mathbf{u}, \mathbf{v} \in \cup\{R_{i_p}^{u_p} \mid p \leq r\}$ . Если  $[\mathbf{u} \oplus \mathbf{v}] \subseteq I$ , то  $[\mathbf{u} \oplus \mathbf{v}] = I$ , и в силу вышесказанного это невозможно.

(б)  $\mathbf{u} \in R_{i_p}^{u_p}$  при некотором  $p \leq r$ ,  $\mathbf{v} \in C \setminus H^{15}$ . Допустим, что  $[\mathbf{u} \oplus \mathbf{v}] \subset I$  и  $[\mathbf{u} \oplus \mathbf{v}] = \{j_1, j_2, j_3\}$ . Для  $i = j_1 \oplus j_2 \oplus j_3 \in I$  вектор  $\mathbf{v} \oplus \mathbf{e}_i$  принадлежит либо компоненте  $R_{i_q}^{u_q \oplus \mathbf{h}}$ , антиподальной к  $R_{i_q}^{u_q}$ , либо некоторой компоненте  $R_{i_q}^{u_q}$  из семейства  $\mathcal{B}$  при  $r < q \leq 4$ . Так как  $R_{i_p}^{u_p} \oplus R_{i_q}^{u_q \oplus \mathbf{h}} = R_{i_p}^{u_p} \oplus R_{i_q}^{u_q}$ , то в любом случае получаем включение  $\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_i \in R_{i_p}^{u_p} \oplus R_{i_q}^{u_q}$ . Так как  $[\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_i] = I$ , то приходим к противоречию с вышесказанным.

(с)  $\mathbf{u}, \mathbf{v} \in C \setminus H^{15}$ . Допустим, что  $\mathbf{u} \in (R_i^{y_i} \oplus \mathbf{e}_i)$  и  $\mathbf{v} \in (R_j^{y_j} \oplus \mathbf{e}_j)$  для некоторых компонент  $R_i^{y_i}, R_j^{y_j}$  из семейства  $\mathcal{B}$ . Пусть  $[\mathbf{u} \oplus \mathbf{v}] = \{j_1, j_2, j_3\} \subset I$ . Так как  $\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_i \oplus \mathbf{e}_j \in H^{15}$ , то  $i \oplus j \oplus j_1 \oplus j_2 \oplus j_3 = 0$ . В случае  $i \neq j$  это невозможно, так как все элементы  $i, j, j_1, j_2, j_3$  больше 7 и сумма нечетного числа таких элементов больше 7. В случае  $i = j$  получаем  $[\mathbf{u} \oplus \mathbf{v}] = I$ . Векторы  $\mathbf{u} \oplus \mathbf{e}_i$  и  $\mathbf{v} \oplus \mathbf{e}_i$  не могут принадлежать двум

антиподальным компонентам кода  $H^{15}$ , иначе вес вектора  $\mathbf{u} \oplus \mathbf{v}$  будет больше 6. Следовательно, эти векторы принадлежат одной и той же  $i$ -компоненте. Но при  $i \geq 8$  вектор  $\mathbf{u} \oplus \mathbf{v}$  с носителем  $[\mathbf{u} \oplus \mathbf{v}] = I$  не может принадлежать ни одной компоненте  $R_i^0$ . Это противоречие доказывает систематичность кода  $C$ . Доказательство того, что расширенный код  $\tilde{C}$  является вполне систематическим, проводится в точности так же, как доказательство теоремы 1. Теорема доказана.

Автору известно, что среди несистематических кодов длины 15 из данного класса имеется 12 попарно неэквивалентных.

#### 4. Примеры

Приведем ряд примеров, дополняющих и иллюстрирующих изложенный выше материал.

Для всех известных к настоящему моменту несистематических кодов длины 15 получаемые из них расширенные коды являются несистематическими. Оказывается, что для кодов большей длины ситуация иная. Пример 1 показывает, что для любого  $k \geq 5$  существуют несистематические коды длины  $n = 2^k - 1$  такие, что построенные из них расширенные коды являются систематическими.

**ПРИМЕР 1.** Рассмотрим любое независимое множество номеров  $I = \{i_1, \dots, i_k\} \subset \{1, \dots, n\}$  ( $k = \log(n + 1)$ ). Пусть  $i_{k+1} = i_{k-1} \oplus i_k$ . Для  $(k + 1)$ -элементного множества  $I' = \{i_1, \dots, i_{k+1}\}$  полагаем  $L'(I') = (I' \oplus I') \setminus \{0\} = \{j_1, \dots, j_m\}$ . Число элементов в множестве  $L'(I')$  равно  $m = k(k + 1)/2$ . Пусть  $j_{m+1} = j_{m+2} = i_1 \oplus i_2 \oplus i_3 \oplus i_4$ . Рассмотрим вектор  $\mathbf{u}_{m+1} = \mathbf{0}$  и вектор  $\mathbf{u}_{m+2} \in H^n$  с носителем  $[\mathbf{u}_{m+2}] = \{j_{m+2}, i_1, i_2, i_3, i_4\}$ . Компоненты  $R_{j_{m+1}}^{\mathbf{u}_{m+1}}$  и  $R_{j_{m+2}}^{\mathbf{u}_{m+2}}$  включим в семейство непересекающихся компонент  $\mathcal{B} = \{R_{j_p}^{\mathbf{u}_p} \mid p = 1, \dots, m + 2\}$ . В случае  $n \geq 63$  это легко делается с помощью используемой в [9] мощностной конструкции (она кратко изложена также в предыдущем разделе). В случае  $n = 31$  полагаем

$$I' = \{1, 2, 4, 8, 16, 24\},$$

$$j_1 = 3, j_2 = 5, j_3 = 6, j_4 = 8, j_5 = 9, j_6 = 10, j_7 = 12, j_8 = 16,$$

$$j_9 = 17, j_{10} = 18, j_{11} = 20, j_{12} = 24, j_{13} = 25, j_{14} = 26, j_{15} = 28,$$

$$j_{16} = j_{17} = 15.$$

Представители компонент  $\mathbf{u}_p$  ( $p = 1, \dots, 17$ ) выписаны в табл. 2. При составлении этой таблицы использовалось найденное в [9] семейство из 31 непересекающейся компоненты кода  $H^{31}$ . Непересекаемость компонент семейства  $\{R_{j_p}^{\mathbf{u}_p} \mid p = 1, \dots, 17\}$  была проверена с помощью компьютера.

Совершенный код  $C$ , построенный из кода  $H^n$  сдвигами всех компонент семейства  $\mathcal{B}$  по соответствующим направлениям, является несистематическим, но полученный из него расширенный код  $\tilde{C}$  систематический.



Т а б л и ц а 2

$p$	$j_p$	$[u_p]$	$p$	$j_p$	$[u_p]$
1	3	$\{2, 4, 5, 6, 9, 18, 19, 22, 27\}$	10	18	$\{2, 4, 6, 15, 17, 30\}$
2	5	$\{2, 4, 6, 15, 21, 26\}$	10	20	$\{2, 3, 4, 5, 6, 8, 19, 29\}$
3	6	$\{2, 4, 6, 11, 18, 25\}$	12	24	$\{4, 11, 12, 21, 22\}$
4	8	$\{1, 2, 4, 6, 22, 23\}$	13	25	$\{2, 4, 6, 13, 17, 28\}$
5	9	$\{2, 4, 6, 8, 15, 16, 19, 27, 31\}$	14	26	$\{2, 4, 6, 7, 12, 13, 15, 17, 24\}$
6	10	$\{2, 4, 5, 6, 21, 22, 27, 29\}$	15	28	$\{2, 4, 6, 7, 10, 11, 24, 30\}$
7	12	$\{2, 4, 11, 18, 20, 22, 29\}$	16	15	$\emptyset$
8	16	$\{2, 4, 6, 8, 23, 31\}$	17	15	$\{1, 2, 4, 8, 15\}$
9	17	$\{2, 3, 4, 8, 10, 24, 31\}$			

Для доказательства систематичности расширенного кода  $\tilde{C}$ , полученного из кода  $C$ , рассмотрим проверочное множество номеров координат  $I'$ . Возьмем пару неравных векторов  $u, v \in C$  такую, что веса векторов  $u$  и  $v$  имеют одинаковую четность и  $[u \oplus v] \subseteq I'$ . Возможны три варианта.

(а)  $u, v \in H^n$ . Этот случай невозможен, так как в  $I'$  нет непустых подмножеств с четным числом элементов и нулевой суммой (единственное подмножество с нулевой суммой — это  $\{i_{k-1}, i_k, i_{k+1}\}$ ).

(б)  $u \in H^n, v \in C \setminus H^n$ . Пусть  $i$  равно сумме всех элементов из носителя  $[u \oplus v]$ . Так как вес вектора  $u \oplus v$  не меньше четырех, то  $i$  не может принадлежать множеству  $L'(I')$ . Поэтому  $i = j_{m+1}$  и  $[u \oplus v] = \{i_1, i_2, i_3, i_4\}$ . Это означает, что вектор  $v \oplus e_i$  принадлежит либо компоненте  $R_{j_{m+1}}^{u_{m+1}}$ , либо компоненте  $R_{j_{m+2}}^{u_{m+2}}$ . Тогда вектор  $u \oplus e_i$  должен принадлежать одной из этих компонент, что противоречит предположению о том, что  $u \in H^n$ .

(с)  $u, v \in C \setminus H^n$ . Пусть  $u \in R_{j_p}^{u_p} \oplus e_{j_p}, v \in R_{j_q}^{u_q} \oplus e_{j_q}$ . Для некоторого вектора  $w \in H^n$  имеем  $[w \oplus e_{j_p} \oplus e_{j_q}] = [u \oplus v]$ . Пусть  $p \leq m, q = m+1$  или  $q = m+2$ . В этом случае  $j_q = i_1 \oplus i_2 \oplus i_3 \oplus i_4$  и  $j_p = i_{p'} \oplus i_{p''}$  для некоторых  $i_{p'}, i_{p''} \in I'$ . Пусть  $w_p, w_q$  — векторы с носителями  $\{j_p, i_{p'}, i_{p''}\}$  и  $\{j_q, i_1, i_2, i_3, i_4\}$  соответственно. Так как  $j_q = j_{m+2}$ , то  $w_q = u_{m+2}$ . Поскольку носитель  $[w \oplus w_p \oplus w_q]$  состоит из четного числа элементов и входит в  $I'$ , имеем  $w = w_p \oplus w_q$ . Следовательно,  $w \in R_{j_p}^0 \oplus R_{j_{m+2}}^{u_{m+2}}$ . Поэтому  $u \oplus e_{j_p} \oplus w = v \oplus e_{j_{m+2}} \in R_{j_q}^{u_q}$ . Если  $q = m+2$ , то это противоречит непересекаемости компонент  $R_{j_p}^{u_p}$  и  $R_{j_{m+1}}^{u_{m+1}}$ . Если же  $q = m+1$ , то получается противоречие с непересекаемостью компонент  $R_{j_p}^{u_p}$  и  $R_{j_{m+2}}^{u_{m+2}}$ . Осталось рассмотреть случай, когда  $p, q \leq m$ . Отличие от доказательства

предыдущего случая состоит только в том, что теперь следует положить  $j_q = i_{q'} \oplus i_{q''}$  для некоторых  $i_{q'}, i_{q''} \in I'$ . Пусть  $w_p, w_q$  — векторы с носителями  $\{j_p, i_{p'}, i_{p''}\}$  и  $\{j_q, i_{q'}, i_{q''}\}$  соответственно. Далее доказательство повторяет соответствующий фрагмент доказательства теоремы 1. Поэтому мы его опускаем.

Докажем несистематичность кода  $C$ . Рассмотрим любое  $k$ -элементное множество  $K$ . В случае, когда множество  $K$  является зависимым, поступаем так же, как и в доказательстве теоремы 2. Поэтому считаем, что множество  $K$  независимо. Так как множества  $L(K)$  и  $L'(I')$  равномощны, то при  $L(K) \neq L'(I')$  существует  $i \in L'(I') \setminus L(K)$ . Этот случай рассматривается точно так же, как и в доказательстве теоремы 2. Предположим, что  $L(K) = L'(I')$ . Тогда  $j_{m+1} = k_1 \oplus \dots \oplus k_s$  для некоторых  $k_1, \dots, k_s \in K$  ( $s \geq 3$ ). Рассмотрим вектор  $v \in H^n$  с носителем  $[v] = \{j_{m+1}, k_1, \dots, k_s\}$ . Покажем, что  $(u_{m+2} \oplus v) \notin R_{j_{m+1}}^0$ . В противном случае найдется такой элемент  $k_p$  ( $1 \leq p \leq s$ ), что  $j_{m+1} \oplus i_4 \oplus k_p = 0$ . Подставив сюда определение  $j_{m+1}$ , получим  $k_p = i_1 \oplus i_2 \oplus i_3$ , что противоречит включению  $k_p \in L'(I')$ . Легко проверяется, что  $v \notin R_{j_{m+1}}^0$ . Все это означает, что компонента  $R_{j_{m+1}}^v$  не пересекается с компонентами  $R_{j_{m+1}}^{u_{m+1}}$  и  $R_{j_{m+2}}^{u_{m+2}}$ . В силу условия  $(\beta)$  существует вектор  $w \in R_{j_{m+1}}^v \setminus (\cup \mathcal{B})$ . Доказательство теперь можно закончить так же, как и доказательство теоремы 2.

В следующем примере по семейству непересекающихся компонент  $\mathcal{B}$  строится систематический код; при этом множество номеров координат  $I_{\mathcal{B}}$  соответствует несистематической орбите. Этот пример оправдывает условие  $(\alpha)$ , налагаемое на семейство  $\mathcal{B}$  при построении несистематических кодов.

**ПРИМЕР 2.** Рассмотрим независимое множество  $I = \{i_1, \dots, i_k\}$ . Пусть  $L(I) = \{j_1, \dots, j_m\}$  ( $m = k(k+1)/2$ ). Полагаем  $j_{m+1} = j_{m+2} = i_1 \oplus i_2 \oplus i_3$ . Рассмотрим вектор  $u_{m+1} = 0$  и вектор  $u_{m+2} \in H^n$  с носителем  $[u_{m+2}] = \{j_{m+2}, i_1, i_2, i_3\}$ . Компоненты  $R_{j_{m+1}}^{u_{m+1}}$  и  $R_{j_{m+2}}^{u_{m+2}}$  включим в семейство непересекающихся компонент  $\mathcal{B} = \{R_{j_p}^{u_p} \mid p = 1, \dots, m+2\}$ . При  $n = 31$  положим  $I = \{3, 5, 9, 17, 24\}$ . Тогда получим, что множество  $L(I)$  совпадает с множеством  $L'(I')$  из примера 1. Для  $p = 1, \dots, 16$  возьмем векторы  $u_p$  такие же, как и в примере 1, и положим  $[u_{17}] = \{3, 5, 9, 15\}$ . Компьютерная проверка показала, что все компоненты  $R_{j_p}^{u_p}$  ( $p = 1, \dots, 17$ ) не пересекаются между собой.

При  $n \geq 31$  множество  $I_{\mathcal{B}} = \{j_1, \dots, j_{m+1}\}$  является носителем вектора из несистематической орбиты, но совершенный код  $C$ , построенный из кода  $H^n$  сдвигами всех компонент семейства  $\mathcal{B}$ , является систематическим.

Доказательство систематичности кода  $C$  аналогично доказательству систематичности кода  $\tilde{C}$  в примере 1.

При  $n = 15$  в качестве такого кода можно взять любой код  $H^{15}(\mathcal{B})$ , где семейство непересекающихся компонент  $\mathcal{B}$  удовлетворяет приведенному в третьем разделе условию (В), но не удовлетворяет условию (А).

Для совершенного кода  $C$  длины  $n$  обозначим через  $ST(C)$  множество всех трехэлементных подмножеств  $T \subset \{1, \dots, n\}$ , для которых существует пара векторов  $\mathbf{u}, \mathbf{v} \in C$  таких, что  $[\mathbf{u} \oplus \mathbf{v}] = T$ . Множество  $ST(C)$  обычно называется *системой троек*, а число элементов в  $ST(C)$  называется *числом троек* кода  $C$  [1, 9]. Максимальное число  $r$  такое, что существует  $r$ -элементное подмножество  $R \subseteq \{1, \dots, n\}$ , не содержащее ни одной тройки из  $ST(C)$ , называется *числом стабильности* системы  $ST(C)$  [9].

**Лемма 8.** Если код  $C$  получен из кода  $H^n$  сдвигами всех непересекающихся компонент из семейства  $\mathcal{B}$ , удовлетворяющего условиям  $(\beta)$ , и для множества  $E = H^n \setminus (\cup \mathcal{B})$  сумма  $E \oplus E$  содержит все векторы веса 3 из кода  $H^n$ , то число троек в системе  $ST(C)$  не меньше  $(n(n-1) + |I_{\mathcal{B}}|(n-1)(n-3))/6$ .

**Доказательство.** Рассмотрим произвольную компоненту  $R_i^n$  из семейства  $\mathcal{B}$  и тройку  $\{i_1, i_2, i_3\}$  такую, что  $i = i_1 \oplus i_2 \oplus i_3$ . Пусть  $\mathbf{v} \in H^n$  — вектор с носителем  $[\mathbf{v}] = \{i, i_1, i_2, i_3\}$ . По условию  $(\beta)$  существует вектор  $\mathbf{w} \in (R_i^n \oplus \mathbf{v}) \setminus (\cup \mathcal{B})$ . Векторы  $\mathbf{w}, \mathbf{u} \oplus \mathbf{e}_i$  принадлежат коду  $C$ , причем  $[\mathbf{w} \oplus \mathbf{u} \oplus \mathbf{e}_i] = \{i_1, i_2, i_3\}$ . Очевидно, что таким способом можно получить  $|I_{\mathcal{B}}|(n-1)(n-3)/6$  различных троек. Кроме этого, складывая пары векторов из множества  $E = H^n \setminus (\cup \mathcal{B})$ , можно получить все тройки кода  $H^n$ . Так как число троек кода  $H^n$  равно  $n(n-1)/6$ , то лемму можно считать доказанной.

Именно с помощью системы троек ранее доказывалась несистематичность кодов в [1, 6, 9]. В связи с этим в [9] был поставлен следующий вопрос. Обязательно ли для несистематического кода  $C$  длины  $n = 2^k - 1$  число стабильности системы троек  $ST(C)$  меньше  $k$ ? Этот вопрос можно переформулировать следующим образом. Верно ли, что в несистематическом коде  $C$  для любого  $k$ -элементного множества  $K$  существуют такие векторы  $\mathbf{u}, \mathbf{v} \in C$ , что расстояние Хемминга между ними равно 3 и  $[\mathbf{u} \oplus \mathbf{v}] \subset K$ ? Следующий пример дает отрицательный ответ на этот вопрос.

**ПРИМЕР 3.** Рассмотрим вектор  $\mathbf{u}_7$  с носителем  $[\mathbf{u}_7] = \{9, 10, 12, 15\}$ . Компоненты  $R_7^{u_7}$  и  $R_8^{u_8}$  ( $\mathbf{u}_8 = \mathbf{0}$ ) включим в систему непересекающихся компонент  $R_i^{u_i}$ ,  $i = 1, \dots, 8$ . Это возможно для кодов  $H^n$  любой длины  $n \geq 31$ . Рассмотрим семейство  $\mathcal{B} = \{R_i^{u_i} \mid i = 1, \dots, 7\}$ . Так как вектор  $\mathbf{u}_0$  с носителем  $[\mathbf{u}_0] = \{1, \dots, 7\}$  принадлежит несистематической орбите

$O_7^1$ , то код  $C = H^n(\mathcal{B})$  является несистематическим. Пусть  $i_1 = 8, i_2 = 9, i_3 = 10, i_4 = 12$ . Дополним этот набор до независимого  $k$ -элементного множества  $K = \{i_1, \dots, i_k\}$ . Оказывается, что множество  $K$  не содержит ни одной тройки из системы  $ST(C)$ .

По построению  $\{1, \dots, 6\} \subset L(K)$ , причем  $7 = i_1 \oplus i_2 \oplus i_3 \oplus i_4 \notin L(K)$ . Возьмем любые различные векторы  $\mathbf{u}, \mathbf{v} \in C$  такие, что  $[\mathbf{u} \oplus \mathbf{v}] \subseteq K$ . В случае, когда  $\mathbf{u} \in H^n$  и  $\mathbf{v} \in R_7^{u_7} \oplus \mathbf{e}_7$ , мы получаем, что носитель  $[\mathbf{u} \oplus \mathbf{v}] = \{i_1, i_2, i_3, i_4\}$  не является кодовой тройкой. Так же, как при доказательстве теоремы 1, убеждаемся, что случай  $\mathbf{v} \in R_i^{u_i} \oplus \mathbf{e}_i$  для  $i < 7$  невозможен. Осталось рассмотреть случай, когда  $\mathbf{u}, \mathbf{v} \in C \setminus H^n$ . Пусть  $\mathbf{u} \in R_i^{u_i} \oplus \mathbf{e}_i$  ( $i < 7$ ) и  $\mathbf{v} \in R_7^{u_7} \oplus \mathbf{e}_7$ . Как и при доказательстве примера 2, убеждаемся в том, что  $\mathbf{w} = \mathbf{u} \oplus \mathbf{v} \oplus \mathbf{e}_i \oplus \mathbf{e}_7 \in R_7^{u_7} \oplus R_i^0$ . Это противоречит непересекаемости компонент  $R_7^0$  и  $R_i^{u_i}$ . Случай  $\mathbf{u} \in R_i^{u_i} \oplus \mathbf{e}_i, \mathbf{v} \in R_j^{u_j} \oplus \mathbf{e}_j$ , как и в случае примера 2, тоже невозможен.

В [9] ставился вопрос о минимальном числе троек в  $ST(C)$  для несистематического кода  $C$ . Пользуясь леммой 8, можно утверждать, что для несистематических кодов  $C$  длины  $n \geq 31$ , полученных из кода  $H^n$  сдвигами компонент из семейства  $\mathcal{B}$ , удовлетворяющего условиям  $(\alpha)$ – $(\delta)$ , минимальное число троек в  $ST(C)$  равно  $t_n = (n(n-1) + 7(n-1)(n-3))/6$ . Для доказательства этого факта считаем число троек у кода  $H^n(\mathcal{B})$  из примера 3. Так как для семейства  $\mathcal{B} = \{R_i^{u_i} \mid i = 1, \dots, 7\}$  выполняются все условия  $(\alpha)$ – $(\delta)$ , то по лемме 8 имеем  $|ST(C)| \geq t_n$ . Новые тройки  $\{i_1, i_2, i_3\}$  могут получиться только как носители сумм  $\mathbf{v} \oplus \mathbf{w}$ , где  $\mathbf{v} \in R_i^{u_i} \oplus \mathbf{e}_i$  и  $\mathbf{w} \in R_j^{u_j} \oplus \mathbf{e}_j$  для некоторых  $i \neq j$ . Следовательно, пятерка  $\{i, j, i_1, i_2, i_3\}$  является носителем вектора из кода  $H^n$ . Поэтому  $i_1 \oplus i_2 \oplus i_3 = i \oplus j$ . Так как множество  $I_{\mathcal{B}}$  является носителем вектора из орбиты  $O_7^1$  и  $i, j \in I_{\mathcal{B}}$ , то  $p = i \oplus j \in I_{\mathcal{B}}$ . Поэтому тройку  $\{i_1, i_2, i_3\}$  можно получить как носитель суммы вектора из  $H^n$  и вектора из  $R_p^{u_p}$ . Все такие тройки уже посчитаны в лемме 8. Следовательно,  $|ST(C)| = t_n$ .

Так как сейчас нет полного описания всех конструкций несистематических кодов, то пока можно только утверждать, что  $t_n$  является минимальным числом троек  $ST(C)$  среди всех известных к настоящему моменту несистематических совершенных кодов  $C$  длины  $n \geq 31$ .

Сосчитаем теперь число троек у несистематических кодов длины 15. Из теоремы 4 предыдущего раздела следует, что код  $C = H^{15}(\mathcal{B})$  является несистематическим тогда и только тогда, когда семейство компонент  $\mathcal{B}$  удовлетворяет условиям (А) и (В). Из условия (А) следует, что все 35 троек кода  $H^{15}$  принадлежат  $ST(C)$ . Лемма 8 гарантирует еще  $|I_{\mathcal{B}}|(n-1)(n-3)/6 = 28|I_{\mathcal{B}}|$  троек. Остались неучтенными

только тройки  $\{i_1, i_2, i_3\}$ , для которых  $0 \neq i_1 \oplus i_2 \oplus i_3 \notin I_{\mathcal{B}}$ . Из условия (В) следует, что либо  $|I_{\mathcal{B}}| = 7$ , либо  $|I_{\mathcal{B}}| = 8$ . Перестановкой координат из  $\text{Sym}(H^{15})$  можно добиться того, чтобы выполнялось либо  $I_{\mathcal{B}} = \{8, 9, 10, 11, 12, 13, 14\}$ , либо  $I_{\mathcal{B}} = \{8, 9, 10, 11, 12, 13, 14, 15\}$ . Рассмотрим любую тройку  $\{i_1, i_2, i_3\}$ , для которой  $0 \neq p = i_1 \oplus i_2 \oplus i_3 < 8$ . Можно подобрать два номера  $i, j \in I_{\mathcal{B}}$  такие, что  $i, j \notin \{i_1, i_2, i_3\}$  и  $i \oplus j = p$ . Тогда пятерка  $\{i, j, i_1, i_2, i_3\}$  имеет нулевую сумму и является носителем некоторого вектора  $\mathbf{u}$  из кода  $H^{15}$ . Так как  $(i, j, k)$ -компонента  $R_i^0 \oplus R_j^0$  не содержит векторов веса 5, у которых  $i$ -я и  $j$ -я координаты равны единице, то вектор  $\mathbf{u}$  принадлежит ее смежному классу. Компоненты  $R_i^{\mathbf{u}_i}$  и  $R_j^{\mathbf{u}_j}$ , принадлежащие семейству  $\mathcal{B}$ , не пересекаются, поэтому их сумма и является тем смежным классом по подпространству  $R_i^0 \oplus R_j^0$ . Это означает, что  $\mathbf{u} = \mathbf{v} \oplus \mathbf{w}$  для некоторых  $\mathbf{v} \in R_i^{\mathbf{u}_i}$  и  $\mathbf{w} \in R_j^{\mathbf{u}_j}$ . Поэтому векторы  $\mathbf{v} \oplus \mathbf{e}_i$  и  $\mathbf{w} \oplus \mathbf{e}_j$  принадлежат коду  $C$  и носителем их суммы является тройка  $\{i_1, i_2, i_3\}$ . Всего таким способом можно получить  $7(n-1)(n-3)/6$  новых троек. Окончательно получаем, что число троек для любого несистематического кода  $C = H^{15}(\mathcal{B})$  равно 455, если  $|I_{\mathcal{B}}| = 8$ , и равно 427, если  $|I_{\mathcal{B}}| = 7$ .

Автор выражает благодарность С. В. Августиновичу за обсуждения, которые стимулировали данное исследование.

## 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. **Августинович С. В., Соловьева Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами  $\tilde{\alpha}$ -компонент // Проблемы передачи информации. 1997. Т. 33, вып. 3. С. 15–21.
3. **Малюгин С. А.** О перечислении совершенных двоичных кодов длины 15 // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
4. **Малюгин С. А.** О критерии несистематичности совершенных двоичных кодов // Докл. РАН. 2000. Т. 375, № 1. С. 13–16.
5. **Нечипорук Э. И.** О синтезе схем с помощью линейных преобразований // Докл. АН СССР. 1958. Т. 123, № 4. С. 610–612.
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 построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 46–52.

8. **Phelps K. T., LeVan M. J.** Kernels of nonlinear Hamming codes // Designs, Codes and Cryptogr. 1995. V. 6, N 3. P. 247–257.
9. **Phelps K. T., LeVan M. J.** Nonsystematic perfect codes // SIAM J. Discrete Math. 1999. V. 12, N 1. P. 27–34.
10. **Solov'eva F. I.** Switchings and perfect codes // Numbers, Information and Complexity. Dordrecht: Kluwer Acad. Publ., 2000. P. 311–324.

Адрес автора:

Институт математики  
им. С. Л. Соболева СО РАН,  
пр. Академика Коптюга, 4,  
630090 Новосибирск,  
Россия

Статья поступила

20 июня 1999 г.