

УДК 519.8

## АФФИННО НЕСИСТЕМАТИЧЕСКИЕ КОДЫ <sup>\*)</sup>

С. А. Малюгин

**Аннотация.** Совершенный двоичный код  $C$  длины  $n = 2^k - 1$  называется *аффинно систематическим*, если существует  $k$ -мерное подпространство в  $\{0, 1\}^n$  такое, что пересечение кода  $C$  с любым смежным классом по этому подпространству является одноэлементным; в противном случае  $C$  называется *аффинно несистематическим*. Описана конструкция аффинно несистематических кодов.

**Ключевые слова:** совершенный код, код Хемминга, несистематический код, аффинно несистематический код, компонента.

### Введение

Пусть  $\{0, 1\}^n$  — векторное пространство над полем из двух элементов 0 и 1. Сумму векторов  $\mathbf{u}, \mathbf{v} \in \{0, 1\}^n$  обозначим через  $\mathbf{u} + \mathbf{v}$ . Базисный вектор, в котором  $i$ -я координата равна единице, обозначим через  $\mathbf{e}_i$ , а нулевой и единичный векторы — через  $\mathbf{0}$  и  $\mathbf{1}$ . Число ненулевых координат вектора  $\mathbf{u}$  называется его *весом*. *Носитель* вектора  $\mathbf{u} \in \{0, 1\}^n$  (множество индексов  $i$ , для которых  $u_i = 1$ ) обозначается через  $[\mathbf{u}]$ . Совершенный код  $C \subset \{0, 1\}^n$  длины  $n = 2^k - 1$  называется *систематическим*, если существует  $k$ -элементное подмножество  $K \subset \{1, \dots, n\}$  такое, что любые два неравных вектора  $\mathbf{u}, \mathbf{v} \in C$  различаются хотя бы в одной координате с номером, не принадлежащим  $K$ . В противном случае код  $C$  называется *несистематическим*.

В коде Хемминга  $H^n$  рассмотрим подпространство  $R_i$ , порожденное всеми векторами веса 3 с  $i$ -й координатой, равной единице. Все возможные смежные классы вида  $R_i^{\mathbf{u}} = R_i + \mathbf{u}$ ,  $\mathbf{u} \in H^n$ , называются  *$i$ -компонентами* кода  $H^n$ ,  $i = 1, \dots, n$ . Рассмотрим семейство  $\mathcal{B} = \{R_{i_1}^{\mathbf{u}_1}, \dots, R_{i_m}^{\mathbf{u}_m}\}$ , состоящее из попарно не пересекающихся  $i_p$ -компонент, где  $\mathbf{u}_p \in H^n$ ,  $p = 1, \dots, m$ . Одна из основных конструкций нелинейных кодов состоит в том, что в коде  $H^n$  сдвигаются по координатам  $i_p$  все

---

<sup>\*)</sup>Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 10-01-00616 и 11-01-00997).

компоненты из семейства  $\mathcal{B}$ . Тем самым множество

$$H^n(\mathcal{B}) = \left( H^n \setminus \bigcup_{p=1}^m R_{i_p}^{\mathbf{u}_p} \right) \cup \left( \bigcup_{p=1}^m (R_{i_p}^{\mathbf{u}_p} \oplus \mathbf{e}_{i_p}) \right) \quad (1)$$

является совершенным кодом [1, 7, 10, 12].

Хорошо известно, что код Хемминга  $H^n$  систематический, но довольно долго стоял вопрос о существовании несистематических нелинейных совершенных кодов. Такие коды длины  $n \geq 255$  впервые построены в [1] сдвигами  $i$ -компонент кода  $H^n$  для  $i$ , пробегающим все значения из  $\{1, \dots, n\}$ . В [11] предложена модификация конструкции [1], позволяющая строить такие коды для всех  $n \geq 63$ . Для  $n = 15$  и  $n = 31$  несистематические коды найдены с помощью компьютера [7, 11]. В [3, 4] получен критерий, с помощью которого можно устанавливать систематичность или несистематичность нелинейных кодов, получаемых из кода Хемминга сдвигами его непересекающихся компонент. В частности, доказано, что для построения несистематического кода любой длины  $n \geq 15$  достаточно сдвинуть в коде Хемминга всего семь непересекающихся компонент. Этот результат даёт ответ на вопрос, поставленный Фелпсом и Ваном [11].

**Определение 1.** Совершенный код  $C$  длины  $n = 2^k - 1$  называется *аффинно систематическим*, если в пространстве  $\{0, 1\}^n$  существует  $k$ -мерное подпространство  $L$  такое, что любой его смежный класс  $L + \mathbf{u}$  пересекается с кодом  $C$  ровно по одному элементу. В противном случае код  $C$  называем *аффинно несистематическим*.

Из определения 1 следует, что систематичность совершенного кода влечёт его аффинную систематичность.

Определение аффинной систематичности предложено С. В. Августиновичем. Это свойство является аффинным инвариантом кода, т. е. оно сохраняется при невырожденных аффинных преобразованиях пространства  $\{0, 1\}^n$ . Другими наиболее известными аффинными инвариантами являются ранг кода и размерность его ядра. С. В. Августиновичем также поставлен вопрос о существовании аффинно несистематических кодов. Ответ на него анонсирован в [5], а в настоящей работе даётся развёрнутое изложение анонсированных результатов.

### 1. Конструкция аффинно несистематических кодов

На множестве  $\{0, 1, \dots, n\}$  ( $n = 2^k - 1$ ) можно ввести структуру линейного пространства следующим образом. Пусть  $i = i_1 \dots i_k$  — представление числа  $0 \leq i \leq n$  в двоичной системе. *Бинарной суммой*  $i \oplus j$

чисел  $0 \leq i, j \leq n$  называется число, двоичное представление которого есть побитовая сумма двоичных представлений чисел  $i$  и  $j$ . Таким образом на множестве индексов  $\{0, 1, \dots, n\}$  ( $n = 2^k - 1$ ) вводится структура линейного пространства. При этом код Хемминга  $H^n$  определяется как множество всех векторов  $\mathbf{u} = (u_1, \dots, u_n) \in \{0, 1\}^n$ , для которых  $\bigoplus_{i=1}^n u_i i = 0$ .

Дополнительным к коду Хемминга  $H^n$  называем  $k$ -мерное подпространство  $Q \subset \{0, 1\}^n$ , если  $Q \cap H^n = \{\mathbf{0}\}$ . Так как  $Q + H^n = \{0, 1\}^n$ , дополнительное подпространство  $Q$  пересекается с каждым смежным классом  $H^n + \mathbf{e}_i$  по единственному ненулевому элементу  $\mathbf{q}_i$  ( $i = 1, \dots, n$ ).

**Лемма 1.** Пусть  $Q = \{\mathbf{q}_0, \mathbf{q}_1, \dots, \mathbf{q}_n\}$  — дополнительное подпространство к коду Хемминга  $H^n$ , где  $\mathbf{q}_0 = \mathbf{0}$ ,  $\mathbf{q}_i \in H^n + \mathbf{e}_i$  ( $1 \leq i \leq n$ ). Тогда  $\mathbf{q}_{i \oplus j} = \mathbf{q}_i + \mathbf{q}_j$  для всех  $1 \leq i, j \leq n$ .

**ДОКАЗАТЕЛЬСТВО.** По условию  $\mathbf{q}_i = \mathbf{e}_i + \mathbf{u}_i$  для некоторых  $\mathbf{u}_i \in H^n$ . Тогда

$$\mathbf{q}_{i \oplus j} = \mathbf{e}_{i \oplus j} + \mathbf{u}_{i \oplus j} = \mathbf{e}_i + \mathbf{e}_j + \mathbf{w},$$

где  $\mathbf{w} = (\mathbf{e}_i + \mathbf{e}_j + \mathbf{e}_{i \oplus j}) + \mathbf{u}_{i \oplus j} \in H^n$ . Поэтому  $\mathbf{q}_{i \oplus j} + \mathbf{q}_i + \mathbf{q}_j = \mathbf{u}_i + \mathbf{u}_j + \mathbf{w} \in H^n$ . Так как  $Q$  пересекается с  $H^n$  только по нулевому элементу, имеем  $\mathbf{q}_{i \oplus j} + \mathbf{q}_i + \mathbf{q}_j = \mathbf{0}$ . Лемма 1 доказана.

**Определение 2.** Множество индексов  $I = \{i_1, \dots, i_m\} \subset \{1, \dots, n\}$  называем *аффинно систематическим*, если существует такое дополнительное к коду Хемминга  $k$ -мерное подпространство  $Q = \{\mathbf{q}_0, \mathbf{q}_1, \dots, \mathbf{q}_n\}$  ( $\mathbf{q}_0 = \mathbf{0}$ ), что  $\mathbf{q}_i \in H^n + \mathbf{e}_i$  ( $i = 1, \dots, n$ ) и  $\mathbf{q}_{i_s} \in R_{i_s} + \mathbf{e}_{i_s}$  ( $s = 1, \dots, m$ ), где  $R_{i_s}$  —  $i_s$ -компоненты кода Хемминга, содержащие нулевой вектор ( $s = 1, \dots, m$ ). В противном случае называем множество  $I$  *аффинно несистематическим*.

Множество индексов  $I \subset \{1, \dots, n\}$  названо в [3, 4] *систематическим*, если в пространстве  $\{0, 1, \dots, n\}$  существует такой базис  $K$  из  $k$  элементов, что  $I \subset K \oplus K$ .

Множество всех векторов пространства  $\{0, 1\}^n$  разбивается на орбиты относительно группы перестановочных автоморфизмов  $\text{Sym}(H^n)$  кода Хемминга  $H^n$ . В [4] (определение 3) орбита, носители всех векторов которой являются систематическими множествами, названа систематической, а орбита, для которой это свойство не выполняется, несистематической. В согласии с этой терминологией будем называть орбиту, носители всех векторов которой являются аффинно систематическими множествами, *аффинно систематической*, а орбиту, для которой это свойство

не выполнено, *аффинно несистематической*.

**Лемма 2.** *Любое систематическое множество  $I \subset \{1, \dots, n\}$  является аффинно систематическим.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $I$  — систематическое множество, причём  $I \subset K \oplus K$  для некоторого базисного множества  $K = \{i_1, \dots, i_k\}$ . Рассмотрим  $k$ -мерное подпространство  $Q$ , порождённое векторами  $\mathbf{e}_{i_p}$  ( $p = 1, \dots, k$ ) (это  $k$ -мерная грань куба  $\{0, 1\}^n$ ). Пусть  $\sum_{p=1}^k \alpha_p \mathbf{e}_{i_p} \in H^n$  для некоторых  $\alpha_1, \dots, \alpha_k \in \{0, 1\}$ . Из определения кода Хемминга тогда следует, что  $\bigoplus_{p=1}^k \alpha_p i_p = 0$ . В силу независимости множества  $K$  все  $\alpha_p$  равны нулю ( $p = 1, \dots, k$ ). Это доказывает, что пространство  $Q$  является дополнительным к коду Хемминга  $H^n$ . Рассмотрим теперь любое  $i \in I$ . Существуют такие два элемента  $j_1, j_2 \in K$ , что  $i = j_1 \oplus j_2$ , т. е.  $\mathbf{u} = \mathbf{e}_i + \mathbf{e}_{j_1} + \mathbf{e}_{j_2} \in R_i$  и  $\mathbf{u} + \mathbf{e}_i \in Q$ . Лемма 2 доказана.

Рассмотрим любое семейство  $\mathcal{B} = \{R_{i_1}^{\mathbf{u}_1}, \dots, R_{i_m}^{\mathbf{u}_m}\}$  из попарно не пересекающихся компонент кода Хемминга  $H^n$ . Обозначим через  $I(\mathcal{B})$  множество всех индексов  $i$ , для которых существуют  $i$ -компоненты, принадлежащие семейству  $\mathcal{B}$ .

**Теорема 1.** *Если множество индексов  $I(\mathcal{B})$  аффинно систематическое, то код  $H^n(\mathcal{B})$ , получаемый по формуле (1) из кода Хемминга  $H^n$  сдвигами компонент из семейства  $\mathcal{B}$ , аффинно систематический.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $Q = \{\mathbf{q}_0, \dots, \mathbf{q}_n\}$  — дополнительное подпространство к коду Хемминга  $H^n$ , обладающее свойством  $\mathbf{q}_i \in R_i + \mathbf{e}_i$  для любого  $i \in I(\mathcal{B})$ . Если  $\mathbf{u}, \mathbf{v} \in H^n(\mathcal{B}) \cap H^n$ , то из  $\mathbf{u} + \mathbf{v} \in Q$  следует  $\mathbf{u} = \mathbf{v}$ . Пусть  $\mathbf{u} \in H^n(\mathcal{B}) \cap H^n$  и  $\mathbf{v} \in R_{i_p}^{\mathbf{u}_p} + \mathbf{e}_{i_p}$  для некоторой компоненты  $R_{i_p}^{\mathbf{u}_p}$  из семейства  $\mathcal{B}$ . Так как  $\mathbf{u} \in H^n \setminus R_{i_p}^{\mathbf{u}_p}$ , получим  $\mathbf{u} + \mathbf{v} \notin R_{i_p} + \mathbf{e}_{i_p}$ . Поскольку  $i_p \in I(\mathcal{B})$ , тем более  $\mathbf{u} + \mathbf{v} \notin Q$ . Если  $\mathbf{u} \in R_{i_p}^{\mathbf{u}_p} + \mathbf{e}_{i_p}$ ,  $\mathbf{v} \in R_{i_q}^{\mathbf{u}_q} + \mathbf{e}_{i_q}$  и  $i_p = i_q$ , то  $\mathbf{u} + \mathbf{v} \notin R_{i_p}$ , и снова  $\mathbf{u} + \mathbf{v} \notin Q$ . Осталось рассмотреть случай  $\mathbf{u} \in R_{i_p}^{\mathbf{u}_p} + \mathbf{e}_{i_p}$ ,  $\mathbf{v} \in R_{i_q}^{\mathbf{u}_q} + \mathbf{e}_{i_q}$  и  $i_p \neq i_q$ . Так как все компоненты из  $\mathcal{B}$  не пересекаются, имеем

$$\mathbf{u} + \mathbf{v} + \mathbf{e}_{i_p} + \mathbf{e}_{i_q} \notin R_{i_p} + R_{i_q}. \quad (2)$$

Очевидно, что  $\mathbf{u} + \mathbf{v} \in H^n + \mathbf{e}_{i_p \oplus i_q}$ . Допустим, что  $\mathbf{u} + \mathbf{v} \in Q$ . Тогда в силу леммы 1  $\mathbf{u} + \mathbf{v} = \mathbf{q}_{i_p \oplus i_q} = \mathbf{q}_{i_p} + \mathbf{q}_{i_q} \in R_{i_p}^{\mathbf{u}_p} + \mathbf{e}_{i_p} + R_{i_q}^{\mathbf{u}_q} + \mathbf{e}_{i_q}$ , что противоречит включению (2). Теорема 1 доказана.

Говорим, что семейство непересекающихся компонент  $\mathcal{B} = \{R_{i_1}^{\mathbf{u}_1}, \dots, R_{i_m}^{\mathbf{u}_m}\}$  не имеет кратных компонент, если все индексы  $i_1, \dots, i_m$  различны. В этом случае  $I(\mathcal{B}) = \{i_1, \dots, i_m\}$ .

Пусть  $E(\mathcal{B}) = H^n \setminus \left( \bigcup_{p=1}^m R_{i_p}^{\mathbf{u}_p} \right)$  — часть кода  $H^n$ , не занятая компонентами из семейства  $\mathcal{B}$ .

Рассмотрим следующие два условия на семейство компонент  $\mathcal{B}$ :

- (а) для любых индекса  $i_p \in I(\mathcal{B})$  и вектора  $\mathbf{q} \in H^n \setminus R_{i_p}$  пересечение  $E(\mathcal{B}) \cap R_{i_p}^{\mathbf{u}_p + \mathbf{q}}$  непусто;
- (б)  $H^n = E(\mathcal{B}) + E(\mathcal{B})$ .

**Теорема 2.** Пусть семейство попарно не пересекающихся компонент  $\mathcal{B} = \{R_{i_1}^{\mathbf{u}_1}, \dots, R_{i_m}^{\mathbf{u}_m}\}$  не содержит кратных компонент. Если множество индексов  $I(\mathcal{B})$  аффинно несистематическое и для семейства  $\mathcal{B}$  выполнены условия (а) и (б), то код  $H^n(\mathcal{B})$  аффинно несистематический.

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим в  $\{0, 1\}^n$  произвольное  $k$ -мерное подпространство  $Q$ . Допустим, что существует вектор  $\mathbf{0} \neq \mathbf{u} \in H^n \cap Q$ . По условию (б) существуют такие два вектора  $\mathbf{v}, \mathbf{w} \in E(\mathcal{B}) \subset H^n(\mathcal{B})$ , что  $\mathbf{v} + \mathbf{w} = \mathbf{u} \in Q$ . Допустим теперь, что  $Q \cap H^n = \{\mathbf{0}\}$ , т. е.  $Q$  является подпространством, дополнительным к  $H^n$ . Пусть  $Q = \{\mathbf{q}_0, \dots, \mathbf{q}_k\}$ , где  $\mathbf{q}_0 = \mathbf{0}$  и  $\mathbf{q}_{i \oplus j} = \mathbf{q}_i + \mathbf{q}_j$  для всех  $0 \leq i, j \leq k$ . Так как множество  $I(\mathcal{B})$  аффинно несистематическое, найдётся такой индекс  $i_p \in I(\mathcal{B})$ , что  $\mathbf{q}_{i_p} \notin R_{i_p} + \mathbf{e}_{i_p}$ . По условию (а) существует вектор  $\mathbf{v} \in E(\mathcal{B}) \cap R_{i_p}^{\mathbf{u}_p + \mathbf{q}_{i_p} + \mathbf{e}_{i_p}}$ . Поэтому  $\mathbf{v} \in H^n(\mathcal{B})$  и  $\mathbf{w} = \mathbf{v} + \mathbf{q}_{i_p} \in R_{i_p}^{\mathbf{u}_p} + \mathbf{e}_{i_p} \subset H^n(\mathcal{B})$ , т. е.  $\mathbf{v} + \mathbf{w} = \mathbf{q}_{i_p} \in Q$ . Теорема 2 доказана.

Каждая компонента кода  $H^n$  состоит из  $2^{\frac{n-1}{2}}$  элементов [1]. Семейство  $\mathcal{B}$  без кратных компонент может содержать не более  $n$  компонент. Условие (б) при  $n > 15$  следует из неравенства

$$n \cdot 2^{\frac{n-1}{2}} < \frac{1}{2} |H^n| = 2^{n - \log_2(n+1) - 1}.$$

Условие (а) следует из того, что при  $i \neq j$  число элементов в пересечении двух компонент  $R_i$  и  $R_j$  равно  $2^{\frac{n+1}{4}}$  [1]. Таким образом, получаем

**Следствие 1.** Если  $n > 15$ , то для любого семейства непересекающихся компонент  $\mathcal{B}$  кода Хемминга  $H^n$ , не содержащего кратных компонент и такого, что множество индексов  $I(\mathcal{B})$  аффинно несистематическое, код  $H^n(\mathcal{B})$  аффинно несистематический.

## 2. Построение аффинно несистематических множеств и кодов

В разд. 1 задача о построении аффинно несистематических кодов сведена к задаче построения аффинно несистематических множеств. Для окончательного решения этой задачи необходимо указать явные примеры аффинно несистематических множеств.

Напомним, что  $\{0, \dots, n\}$  является линейным пространством размерности  $k$  ( $n = 2^k - 1$ ), которое для краткости будем обозначать символом  $\{0, 1\}^k$ . Возьмём в этом пространстве некоторое подмножество  $I = \{i_1, \dots, i_m\}$ , ранг которого равен  $r < k$ . Выделим в  $I$  некоторый базисный набор  $\{i_1, \dots, i_r\}$  и рассмотрим в  $\{0, 1\}^k$  подпространство  $M$ , порождённое векторами  $i_1, \dots, i_r$ . Пусть  $n' = 2^r - 1$ . В коде Хемминга  $H^n$  можно рассмотреть подкод  $H_M^{n'}$ , состоящий из всех векторов кода  $H^n$ , носители которых входят в  $M \setminus \{0\}$ . Очевидно, что этот подкод эквивалентен стандартному коду Хемминга  $H^{n'}$  длины  $n'$ . Если  $I = \{i_1, \dots, i_m\}$  входит в  $M \setminus \{0\}$ , то можем говорить о его аффинной систематичности (или несистематичности) как относительно кода  $H^n$ , так и относительно кода  $H_M^{n'}$ . Свойство обычной систематичности не зависит от того, в каком коде Хемминга ( $H_M^{n'}$  или  $H^n$ ) рассматривается этот вопрос (см. [4, лемма 5] или [3, лемма 1]). Покажем, что аналогичный факт справедлив и для свойства аффинной систематичности.

**Лемма 3** (о редукции). *Множество  $I$  аффинно систематическое относительно кода  $H_M^{n'}$  тогда и только тогда, когда оно аффинно систематическое относительно кода  $H^n$ .*

**ДОКАЗАТЕЛЬСТВО.** Допустим, что множество  $I = \{i_1, \dots, i_m\}$  (с базисным набором  $\{i_1, \dots, i_r\}$ ) аффинно систематическое относительно кода Хемминга  $H_M^{n'}$ . Пусть  $M \setminus \{0\} = \{i_1, \dots, i_{n'}\}$  ( $m \leq n'$ ). Если через  $R_i(M)$  обозначим  $i$ -компоненты кода  $H_M^{n'}$ , то должно существовать такое  $r$ -мерное подпространство  $Q_M = \{\tilde{\mathbf{q}}_0, \tilde{\mathbf{q}}_{i_1}, \dots, \tilde{\mathbf{q}}_{i_{n'}}\}$  ( $\tilde{\mathbf{q}}_0 = \mathbf{0}$ ), что  $\tilde{\mathbf{q}}_{i_s} \in H_M^{n'} + \mathbf{e}_{i_s}$  ( $s = 1, \dots, n'$ ) и  $\tilde{\mathbf{q}}_{i_s} \in R_{i_s}(M) + \mathbf{e}_{i_s}$  ( $s = 1, \dots, m$ ). Рассмотрим в  $\{0, 1\}^k$  такое базисное множество  $K$ , что  $i_s \in K$  ( $s = 1, \dots, r$ ). Положим  $\mathbf{q}_{i_s} = \tilde{\mathbf{q}}_{i_s}$  при  $s = 1, \dots, r$  и  $\mathbf{q}_j = \mathbf{e}_j$  при  $j \in K \setminus I$ . Если  $j \notin K$ , то для некоторого множества  $J \subset K$  имеем  $j = \bigoplus_{i \in J} i$  и полагаем  $\mathbf{q}_j = \sum_{i \in J} \mathbf{q}_i$ . Легко проверяется, что определённое таким способом множество  $Q = \{\mathbf{q}_0, \dots, \mathbf{q}_n\}$  является дополнительным к коду Хемминга  $H^n$   $k$ -мерным подпространством в  $\{0, 1\}^n$ . Так как  $R_i(M) = H_M^{n'} \cap R_i$  для любого  $i \in M \setminus \{0\}$ , очевидно, что  $\mathbf{q}_{i_s} \in R_{i_s} + \mathbf{e}_{i_s}$  ( $s = 1, \dots, m$ ), откуда следует аффинная систематичность  $I$  относительно кода  $H^n$ .

Наоборот, допустим, что  $I$  является аффинно систематическим относительно кода  $H^n$  и что дополнительное к  $H^n$   $k$ -мерное подпространство  $Q = \{\mathbf{q}_0, \dots, \mathbf{q}_n\}$  ( $\mathbf{q}_0 = \mathbf{0}$ ) обладает свойством  $\mathbf{q}_i \in H^n + \mathbf{e}_i$  ( $i = 1, \dots, n$ ) и  $\mathbf{q}_{i_s} \in R_{i_s} + \mathbf{e}_{i_s}$  ( $s = 1, \dots, m$ ). Так как  $M$  — подпространство в  $\{0, 1\}^k$ , множество  $Q_M = \{\mathbf{q}_0, \mathbf{q}_{i_1}, \dots, \mathbf{q}_{i_{n'}}\}$  является  $r$ -мерным подпространством. Обозначим символом  $(\mathbf{u})_j$   $j$ -ю координату вектора  $\mathbf{u}$ . Теперь для любого  $i \in M$  полагаем

$$(\tilde{\mathbf{u}})_j = \begin{cases} (\mathbf{u})_j, & \text{если } j \in M, \\ 0, & \text{если } j \notin M. \end{cases}$$

Поскольку отображение  $\sim : M \rightarrow \{0, 1\}^n$ , очевидно, линейно, множество  $\tilde{Q} = \{\tilde{\mathbf{q}}_0, \tilde{\mathbf{q}}_{i_1}, \dots, \tilde{\mathbf{q}}_{i_{n'}}\}$  — линейное подпространство. Свойство  $\tilde{\mathbf{q}}_{i_s} \in H_M^{n'} + \mathbf{e}_{i_s}$  ( $s = 1, \dots, n'$ ) сразу следует из определения кода  $H_M^{n'}$  и аналогичного свойства для элементов  $\mathbf{q}_{i_s}$ . Докажем, что  $\tilde{\mathbf{q}}_{i_s} \in R_{i_s} + \mathbf{e}_{i_s}$  при  $s = 1, \dots, m$ . Легко заметить, что вектор  $\mathbf{u} \in H^n$  принадлежит компоненте  $R_i$  тогда и только тогда, когда  $(\mathbf{u})_j = (\mathbf{u})_{i \oplus j}$  для любого индекса  $j \neq i$ ,  $j \in \{0, 1\}^k$ . Пусть  $1 \leq s \leq m$ . Если  $j \notin M$ , то так как  $i_s \in M$  и  $M$  — подпространство, получаем  $j \oplus i_s \notin M$ . Поэтому  $(\tilde{\mathbf{q}}_{i_s})_j = 0 = (\tilde{\mathbf{q}}_{j \oplus i_s})_j$ . Пусть  $j \in M \setminus \{0\}$  и  $j \neq i_s$ . Поскольку по условию  $\mathbf{q}_{i_s} \in R_{i_s} + \mathbf{e}_{i_s}$ , имеем  $(\tilde{\mathbf{q}}_{i_s})_j = (\mathbf{q}_{i_s})_j = (\mathbf{q}_{i_s})_{j \oplus i_s} = (\tilde{\mathbf{q}}_{i_s})_{j \oplus i_s}$ . Тем самым  $\tilde{\mathbf{q}}_{i_s} \in R_{i_s} + \mathbf{e}_{i_s}$ . Кроме того,  $\tilde{\mathbf{q}}_{i_s} \in H_M^{n'} + \mathbf{e}_{i_s}$ . Значит,  $\tilde{\mathbf{q}}_{i_s} \in H_M^{n'} \cap R_{i_s} + \mathbf{e}_{i_s} = R_{i_s}(M) + \mathbf{e}_{i_s}$ . Лемма 3 доказана.

Орбиты векторов пространства  $\{0, 1\}^n$  можно задавать с помощью уравнений. Каждой орбите веса  $m$  и ранга  $r$  сопоставляется матрица  $(b_{pq})$  ( $p = r + 1, \dots, m$ ;  $q = 1, \dots, r$ ) размера  $(m - r) \times r$  над полем  $\{0, 1\}$  с попарно различными строками. При этом носителями векторов из орбиты являются всевозможные множества  $\{i_1, \dots, i_m\}$  такие, что

$$i_p = b_{p1}i_1 \oplus \dots \oplus b_{pr}i_r \quad (p = r + 1, \dots, m), \quad (3)$$

а  $i_1, \dots, i_r$  пробегает все линейно независимые наборы из  $\{0, 1\}^k$ . Если орбита в пространстве  $\{0, 1\}^{n'}$  ( $n' = 2^r - 1$ ) задаётся уравнением (3), то ей соответствует орбита с таким же уравнением в любом пространстве  $\{0, 1\}^n$  большей размерности. Из леммы 3 следует, что при таком соответствии свойство орбиты быть аффинно систематической (аффинно несистематической) сохраняется. Этот факт даёт возможность искать аффинно несистематические орбиты в пространствах небольших размерностей путём непосредственного перебора вариантов. В силу леммы 2 аффинная несистематичность влечёт обычную несистематичность, поэтому среди орбит веса 7 кандидатами в аффинно несистематические орбиты

могут быть только две найденные в [4] (следствие 1) несистематические орбиты  $O_7^1$  и  $O_7^3$ .

**Лемма 4.** Орбиты  $O_7^1$  и  $O_7^3$  аффинно несистематические.

**ДОКАЗАТЕЛЬСТВО.** Носители векторов орбиты  $O_7^1$  задаются следующими уравнениями:  $i_4 = i_1 \oplus i_2$ ,  $i_5 = i_2 \oplus i_3$ ,  $i_6 = i_1 \oplus i_3$ ,  $i_7 = i_1 \oplus i_2 \oplus i_3$ , где тройка  $i_1, i_2, i_3$  линейно независима (см. табл. 1 из [4]). Ранг орбиты равен 3, поэтому в силу леммы о редукции достаточно решить эту задачу в коде Хемминга  $H^7$ , т. е. проверить аффинную несистематичность множества  $\{1, 2, 3, 4, 5, 6, 7\}$ . Рассмотрим базисное множество

$$K = \{i_1, i_2, i_3\} = \{1, 2, 4\}.$$

Выберем произвольным образом векторы  $\mathbf{q}_{i_\alpha} \in R_{i_\alpha} + \mathbf{e}_{i_\alpha}$  ( $\alpha = 1, 2, 3$ ). Остальные векторы подпространства  $Q = \{\mathbf{q}_0, \mathbf{q}_1, \dots, \mathbf{q}_7\}$  ( $\mathbf{q}_0 = \mathbf{0}$ ), порождённого векторами  $\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_4$ , определяются однозначно, т. е.

$$\text{если } J \subset K \text{ и } i = \bigoplus_{j \in J} j, \quad \text{то } \mathbf{q}_i = \sum_{j \in J} \mathbf{q}_j. \quad (4)$$

После этого необходимо проверить, что  $\mathbf{q}_i \notin R_i + \mathbf{e}_i$  хотя бы для одного индекса  $i$ . Каждая компонента кода  $H^7$  состоит из 16 элементов. Поэтому необходимо сделать  $16^3$  таких проверок. Эту работу можно в значительной степени сократить. Во-первых, представим  $\mathbf{q}_j = \mathbf{w}_j + \mathbf{e}_j$ ,  $j = 1, \dots, 7$ . Тогда  $\mathbf{w}_j \in H^7$  и формула (2) имеет вид

$$\text{если } J \subset K \text{ и } i = \bigoplus_{j \in J} j, \quad \text{то } \mathbf{w}_i = \sum_{j \in J} \mathbf{w}_j + \mathbf{e}_i + \sum_{j \in J} \mathbf{e}_j. \quad (4')$$

Теперь необходимо проверить, что  $\mathbf{w}_i \notin R_i$  хотя бы для одного индекса  $i$ . Так как вектор  $\mathbf{1}$  принадлежит всем компонентам, замена  $\mathbf{w}_j$  на  $\mathbf{w}_j + \mathbf{1}$  не меняет свойства принадлежности компоненте  $R_j$ . Тем самым достаточно исследовать случаи, когда векторы  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  либо равны нулю, либо имеют вес 3. Рассмотрим эти случаи.

**СЛУЧАЙ 1:**  $\mathbf{w}_1 = \mathbf{w}_2 = \mathbf{w}_4 = \mathbf{0}$ . Тогда вектор  $\mathbf{w}_7 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_7$  (вычисленный по формуле (4')) не принадлежит компоненте  $R_7$ .

Все случаи, когда только один из векторов  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  ненулевой и его носитель содержит два базисных элемента из  $K$ , сводятся с помощью подходящего автоморфизма кода Хемминга  $H^7$  к следующему.

**СЛУЧАЙ 2:**  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ ,  $\mathbf{w}_2 = \mathbf{w}_4 = \mathbf{0}$ . Здесь вектор  $\mathbf{w}_5 = \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_5$  не принадлежит компоненте  $R_5$ .

Все случаи, когда только один из векторов  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  ненулевой и его носитель содержит два базисных элемента из  $K$ , сводятся с помощью подходящего автоморфизма кода Хемминга  $H^7$  к следующему.

СЛУЧАЙ 3:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_6 + \mathbf{e}_7, \mathbf{w}_2 = \mathbf{w}_4 = \mathbf{0}$ . В этом случае вектор  $\mathbf{w}_5 = \mathbf{e}_4 + \mathbf{e}_5 + \mathbf{e}_6 + \mathbf{e}_7$  не принадлежит компоненте  $R_5$ .

Все случаи, когда имеется только два ненулевых равных между собой вектора из  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$ , сводятся к следующему.

СЛУЧАЙ 4:  $\mathbf{w}_1 = \mathbf{w}_2 \neq \mathbf{0}, \mathbf{w}_4 = \mathbf{0}$ . Тогда (как и в случае 1) вектор  $\mathbf{w}_7 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_7$  не принадлежит компоненте  $R_7$ .

Все случаи, когда имеется только два ненулевых не равных между собой вектора из  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$ , причём носитель каждого из них содержит по два базисных элемента из  $K$ , сводятся к следующему.

СЛУЧАЙ 5:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, \mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_6, \mathbf{w}_4 = \mathbf{0}$ . Здесь вектор  $\mathbf{w}_3 = \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_6$  не принадлежит компоненте  $R_3$ .

Все случаи, когда имеется только два ненулевых не равных между собой вектора из  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$ , причём носитель одного из них содержит два базисных элемента, а носитель другого — только один базисный элемент из  $K$ , сводятся к одному из следующих двух случаев.

СЛУЧАЙ 6:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, \mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7, \mathbf{w}_4 = \mathbf{0}$ . В этом случае вектор  $\mathbf{w}_3 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7$  не принадлежит компоненте  $R_3$ .

СЛУЧАЙ 7:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, \mathbf{w}_4 = \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_7, \mathbf{w}_2 = \mathbf{0}$ . Тогда вектор  $\mathbf{w}_6 = \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_6 + \mathbf{e}_7$  не принадлежит компоненте  $R_6$ .

Все случаи, когда имеется только два ненулевых не равных между собой вектора из  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$ , причём носитель каждого из них содержит по одному базисному элементу из  $K$ , сводятся к следующему.

СЛУЧАЙ 8:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_6 + \mathbf{e}_7, \mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7, \mathbf{w}_4 = \mathbf{0}$ . Здесь  $\mathbf{w}_6 = \mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_6 + \mathbf{e}_7$  не принадлежит компоненте  $R_6$ .

Рассмотрим случаи, когда все векторы  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  ненулевые, причём среди них есть два одинаковых. Применяя автоморфизмы кода Хемминга, можно считать, что  $\mathbf{w}_1 = \mathbf{w}_2 \neq \mathbf{w}_4$ . Если носитель вектора  $\mathbf{w}_4$  содержит два базисных элемента из  $K$ , то с помощью подходящих автоморфизмов кода Хемминга придём к следующему.

СЛУЧАЙ 9:  $\mathbf{w}_1 = \mathbf{w}_2 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, \mathbf{w}_4 = \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_6$ . В этом случае вектор  $\mathbf{w}_6 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$  не принадлежит компоненте  $R_6$ .

Если же носитель вектора  $\mathbf{w}_4$  содержит только один базисный элемент из  $K$ , то получим

СЛУЧАЙ 10:  $\mathbf{w}_1 = \mathbf{w}_2 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ ,  $\mathbf{w}_4 = \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_7$ . Тогда  $\mathbf{w}_7 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_7$  не принадлежит компоненте  $R_7$ .

И, наконец, переходим к случаям, когда все векторы  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  различны и не равны нулю. Все случаи, когда носители каждого из этих векторов содержат по два базисных элемента из  $K$ , с помощью автоморфизмов кода Хемминга сводятся к следующему.

СЛУЧАЙ 11:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ ,  $\mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_6$ ,  $\mathbf{w}_4 = \mathbf{e}_1 + \mathbf{e}_4 + \mathbf{e}_5$ . Здесь вектор  $\mathbf{w}_3 = \mathbf{e}_2 + \mathbf{e}_4 + \mathbf{e}_6$  не принадлежит компоненте  $R_3$ .

Все случаи, когда носители двух векторов из  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  содержат по два базисных элемента, а третий — только один базисный элемент из  $K$ , сводятся к следующему.

СЛУЧАЙ 12:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ ,  $\mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7$ ,  $\mathbf{w}_4 = \mathbf{e}_1 + \mathbf{e}_4 + \mathbf{e}_5$ . В этом случае вектор  $\mathbf{w}_7 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$  не принадлежит компоненте  $R_7$ .

Если носитель только одного вектора из  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  содержит два базисных элемента, а двух других — только по одному базисному элементу из  $K$ , то получаем

СЛУЧАЙ 13:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ ,  $\mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7$ ,  $\mathbf{w}_4 = \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_7$ . Тогда вектор  $\mathbf{w}_3 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7$  не принадлежит компоненте  $R_3$ .

Осталось разобрать последний случай, когда каждый из векторов  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4$  содержит по одному базисному элементу из  $K$ .

СЛУЧАЙ 14:  $\mathbf{w}_1 = \mathbf{e}_1 + \mathbf{e}_6 + \mathbf{e}_7$ ,  $\mathbf{w}_2 = \mathbf{e}_2 + \mathbf{e}_5 + \mathbf{e}_7$ ,  $\mathbf{w}_4 = \mathbf{e}_3 + \mathbf{e}_4 + \mathbf{e}_7$ . В этом случае вектор  $\mathbf{w}_7 = \mathbf{e}_3 + \mathbf{e}_5 + \mathbf{e}_6$  не принадлежит компоненте  $R_7$ .

Носители векторов орбиты  $O_7^3$  задаются следующими уравнениями:

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

где  $i_1, i_2, i_3, i_4$  линейно независимы (см. табл. 1 из [4]). Аффинная несистематичность орбиты  $O_7^3$  установлена с помощью компьютера. Лемма 4 доказана.

**Теорема 3.** *Все несистематические коды, которые получаются из кода Хемминга сдвигами семи непересекающихся компонент, аффинно несистематические.*

**ДОКАЗАТЕЛЬСТВО.** Пусть код  $C = H^n(\mathcal{B})$  — несистематический, где  $\mathcal{B} = \{R_{i_1}^{\mathbf{u}_1}, \dots, R_{i_7}^{\mathbf{u}_7}\}$  — некоторое семейство из семи попарно не пересекающихся  $i_q$ -компонент кода Хемминга  $H^n$  ( $q = 1, \dots, 7$ ;  $\mathbf{u}_1, \dots, \mathbf{u}_7 \in H^n$ ). В силу теоремы 1 из [4] множество  $I(\mathcal{B})$  несистематическое. Так как по

следствию 1 из [4] множества, содержащие менее семи элементов, систематические, семейство  $\mathcal{B}$  не может содержать кратных компонент (т. е. индексы  $i_1, \dots, i_7$  различны). По следствию 1 из [4] существует в точности две несистематические орбиты  $O_7^1$  и  $O_7^3$  веса 7. В силу леммы 5 из [4] и леммы 3 (о редукции), а также леммы 4 получаем аффинную несистематичность множества  $\{i_1, \dots, i_7\}$ . Известно, что для любых двух компонент  $R_i, R_j$  ( $i \neq j$ ) кода Хемминга  $H^n$  имеют место равенства  $|R_i| = 2^{(n-1)/2}$ ,  $|R_i \cap R_j| = 2^{(n-1)/4}$  [1, 2]. Тем самым для всех  $n = 2^k - 1 \geq 15$  справедливы неравенства для мощностей

$$\left| \bigcup_{j=1}^7 (R_{i_j}^{\mathbf{u}_j} \cap R_{i_q}^{\mathbf{u}_q}) \right| = 7 \cdot 2^{(n-1)/4} < 2^{(n-1)/2} = |R_{i_q}^{\mathbf{u}_q}|, \quad q = 1, \dots, 7;$$

$$\left| \bigcup_{j=1}^7 R_{i_j}^{\mathbf{u}_j} \right| = 7 \cdot 2^{(n-1)/2} < 2^{n-k-1} = \frac{1}{2} |H^n|.$$

Это означает, что выполнены условия (а) и (б) теоремы 2. В силу теоремы 2 код  $C$  является аффинно несистематическим. Теорема 3 доказана.

Из этой теоремы и теоремы 3 в [4] следует существование аффинно несистематических кодов любой длины  $n = 2^k - 1 \geq 15$ .

### 3. Примеры несистематических аффинно систематических кодов

Для любого совершенного кода  $C$  длины  $n = 2^k - 1$  можно построить расширенный код  $\tilde{C}$  длины  $n + 1$ , добавляя к векторам  $C$  проверку на чётность в качестве нулевой координаты. Обратно, исходя из расширенного кода  $\tilde{C}$  можно получить нерасширенный (совершенный) код  $\tilde{C}^i$ , вычеркивая  $i$ -ю координату во всех векторах  $\tilde{C}$ . В частности,  $\tilde{C}^0 = C$ . Следуя [4] (определение 1), назовём расширенный код  $\tilde{C}$  *систематическим*, если существует  $(k + 1)$ -элементное множество  $K \subset \{0, 1, \dots, n\}$  такое, что любые два неравных вектора  $\mathbf{u}, \mathbf{v} \in \tilde{C}$  различаются хотя бы в одной координате с номером, не принадлежащим  $K$ . В противном случае  $\tilde{C}$  назовём *несистематическим*.

**Теорема 4.** Пусть расширенный код  $\tilde{C}$  построен из совершенного кода  $C$  длины  $n = 2^k - 1$ . Тогда если код  $\tilde{C}$  систематический, то код  $C$  аффинно систематический.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $(k + 1)$ -элементное множество  $K \subset \{0, 1, \dots, n\}$  такое, что любые два неравных вектора из  $\tilde{C}$  различаются хотя

бы в одной координате с номером, не принадлежащим  $K$ . Пусть  $0 \in K$ . Рассмотрим  $k$ -элементное множество  $K_0 = K \setminus \{0\} \subset \{1, \dots, n\}$  и любые два неравных вектора  $\mathbf{u}, \mathbf{v} \in C$ . Пусть векторы  $\tilde{\mathbf{u}}, \tilde{\mathbf{v}}$  получены из векторов  $\mathbf{u}, \mathbf{v}$  добавлением проверки на чётность в качестве нулевой координаты. Тогда  $\tilde{\mathbf{u}}, \tilde{\mathbf{v}}$  принадлежат  $\tilde{C}$  и различаются в некоторой координате  $i \notin K$ . Из того, что  $0 \in K$ , следует, что  $i \neq 0$ . Поэтому векторы  $\mathbf{u}, \mathbf{v}$  тоже различаются в координате  $i \notin K_0$ . Таким образом, код  $C$  систематический и, в частности, аффинно систематический. Предположим теперь, что  $0 \notin K$ . Пусть  $L$  — подпространство в  $\{0, 1\}^n$ , состоящее из всех векторов  $\mathbf{u}$ , носители которых входят в  $K$  и имеют чётное число элементов. Очевидно, что размерность  $L$  равна  $k$ . Допустим, что код  $C$  аффинно несистематический. Тогда существует смежный класс  $L + \mathbf{w}$ , содержащий два различных вектора  $\mathbf{u}, \mathbf{v} \in C$ . Это означает, что  $\mathbf{u} + \mathbf{w} \in L$  и  $\mathbf{v} + \mathbf{w} \in L$ . В частности,  $\mathbf{u} + \mathbf{v} \in L$  и носители векторов  $\mathbf{u}, \mathbf{v}$  имеют одинаковую чётность. Поэтому нулевые координаты векторов  $\tilde{\mathbf{u}}, \tilde{\mathbf{v}}$ , полученных из  $\mathbf{u}, \mathbf{v}$  добавлением проверки на чётность, совпадают, т. е.  $[\tilde{\mathbf{u}} + \tilde{\mathbf{v}}] = [\mathbf{u} + \mathbf{v}] \subset K$ , что противоречит тому, что любые два неравных вектора  $\tilde{\mathbf{u}}, \tilde{\mathbf{v}} \in \tilde{C}$  различаются хотя бы в одной координате с номером, не принадлежащим  $K$ . Следовательно, код  $C$  должен быть аффинно систематическим. Теорема 4 доказана.

В [4, пример 1] для любого  $k \geq 5$  построены примеры несистематических кодов длины  $n = 2^k - 1$  таких, что построенные из них расширенные коды являются систематическими. Кроме этого, в [8, 9] построены с помощью компьютера все попарно не эквивалентные совершенные коды длины 15, при этом расширение 12 несистематических кодов даёт 12 неэквивалентных расширенных несистематических кодов, а один код становится при расширении систематическим. Из теоремы 4, а также из результатов, полученных в [8, 9], получаем

**Следствие 2.** Для любого  $n = 2^k - 1$  ( $k \geq 4$ ) существуют несистематические аффинно систематические коды длины  $n$ .

**Замечание.** 12 неэквивалентных несистематических кодов длины 15, расширение которых даёт несистематические коды, построены в [4, 6] (два кода найдены в [7, 11]). Компьютерная проверка показала, что эти 12 кодов аффинно несистематические. Поэтому для кодов длины 15 теперь имеем исчерпывающую информацию: среди 13 неэквивалентных несистематических кодов длины 15 только один код (найденный впервые в [8, 9]) является аффинно систематическим.

## 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 критерии несистематичности совершенных двоичных кодов // Докл. РАН. — 2000. — Т. 375, № 1. — С. 13–16.
4. **Малюгин С. А.** Несистематические совершенные двоичные коды // Дискрет. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 1. — С. 55–76.
5. **Малюгин С. А.** Об аффинно несистематических кодах // Сб. докл. междунар. конф., посвящённой 90-летию со дня рождения А. А. Ляпунова (Новосибирск, 8–12 октября 2001 г.). — Новосибирск: Ин-т математики, 2001. — С. 393–394. (<http://www.sbras.nsc.ru/ws/Lyap2001/2288>).
6. **Малюгин С. А.** О перечислении неэквивалентных совершенных двоичных кодов длины 15 и ранга 15 // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 1. — С. 77–98.
7. **Романов А. М.** О несистематических совершенных кодах длины 15 // Дискрет. анализ и исслед. операций. Сер. 1. — 1997. — Т. 4, № 4. — С. 75–78.
8. **Östergård P. R. J., Potttonen O.** The perfect binary one-error-correcting codes of length 15, part I – classification // IEEE Trans. Inform. Theory. — 2009. — Vol. 55, N 10. — P. 4657–4660.
9. **Östergård P. R. J., Potttonen O., Phelps K. T.** The perfect binary one-error-correcting codes of length 15, part II – properties // IEEE Trans. Inform. Theory. — 2009. — Vol. 56, N 6. — P. 2571–2582.
10. **Phelps K. T., LeVan M. J.** Kernels of nonlinear Hamming codes // Des. Codes Cryptography. — 1995. — Vol. 6, N 3. — P. 247–257.
11. **Phelps K. T., LeVan M. J.** Nonsystematic perfect codes // SIAM J. Discrete Math. — 1999. — Vol. 12, N 1. — P. 27–34.
12. **Solov'eva F. I.** Switchings and perfect codes // Numbers, information and complexity. — Dordrecht: Kluwer Acad. Publ., 2000. — P. 311–324.