

УДК 519.725

## О НИЖНЕЙ ОЦЕНКЕ ЧИСЛА ТРАНЗИТИВНЫХ СОВЕРШЕННЫХ КОДОВ<sup>\*)</sup>

В. Н. Потапов

При  $n \rightarrow \infty$  построено не менее  $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1 + o(1))$  попарно неэквивалентных транзитивных расширенных совершенных кодов длины  $4n$ .

### Введение

Автоморфизмами произвольного подмножества  $A$  булева  $n$ -куба называются изометрии булева  $n$ -куба, переводящие множество  $A$  в себя. Множество называется транзитивным, если оно является орбитой относительно действия своей группы автоморфизмов. Транзитивные совершенные коды длины 15 рассматривались в работе [1]. В [2] построено  $\lfloor \frac{1}{2} \log_2 n \rfloor^2$  неэквивалентных транзитивных совершенных (и расширенных совершенных) кодов с разными парами параметров: размерность линейной оболочки (ранг) кода и размерность ядра кода.

Используя конструкцию из [5], в настоящей статье доказано, что имеется не менее  $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1 + o(1))$  (при  $n \rightarrow \infty$ ) попарно неэквивалентных транзитивных расширенных совершенных кодов длины  $4n$ . Все построенные транзитивные расширенные совершенные коды длины  $n$  имеют ранг  $n - \log_2 n$ .

### 1. Основные определения

Пусть  $E_k = \{0, 1, \dots, k - 1\}$ . Через  $E_k^n$  обозначим множество упорядоченных наборов (вершин) длины  $n$ . Расстоянием Хемминга  $d(\bar{x}, \bar{y})$  между наборами  $\bar{x} = (x_1, x_2, \dots, x_n)$  и  $\bar{y} = (y_1, y_2, \dots, y_n)$  называется число позиций, в которых наборы  $\bar{x}$  и  $\bar{y}$  различаются. Множество вершин, которые находятся от вершины  $\bar{x}$  на расстоянии не более единицы, называется шаром радиуса 1 с центром в  $\bar{x}$  и обозначается через  $\mathcal{B}(\bar{x})$ . Ребрам направления  $i$  называется множество вершин, отличающихся друг

---

<sup>\*)</sup>Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00364).

от друга только в  $i$ -й позиции. Ребро направления  $i$ , содержащее вершину  $\bar{x} \in E_k^n$ , обозначим через  $\mathcal{E}_i(\bar{x})$ .

Через  $E_{2,0}^n$  и  $E_{2,1}^n$  будем обозначать подмножества  $E_2^n$ , каждое из которых состоит из вершин с чётным и нечётным числом единиц соответственно. Множество  $C \subset E_{2,0}^n$  ( $C \subset E_{2,1}^n$ ) называется *расширенным совершенным кодом* (с расстоянием 4) длины  $n$ , если  $|\mathcal{B}(\bar{x}) \cap C| = 1$  для любой вершины  $\bar{x} \in E_{2,1}^n$  ( $\bar{x} \in E_{2,0}^n$ ). Множество  $M \subset E_k^n$  называется *МДР-кодом* (с расстоянием 2) длины  $n$ , если  $|\mathcal{E}_i(\bar{x}) \cap M| = 1$  при любом  $i = 1, \dots, n$  и  $\bar{x} \in E_k^n$ . Из определений видно, что расширенный совершенный код является максимальным по мощности подмножеством в  $E_2^n$  с расстоянием не менее 4 между вершинами, а МДР-код является максимальным подмножеством в  $E_k^n$  с расстоянием не менее 2 между вершинами. Известно, что расширенные совершенные коды длины  $n$  существуют при  $n = 2^t$ , где  $t$  — натуральное, а МДР-коды с расстоянием 2 при любых натуральных  $n$  и  $k$ .

Функция  $f : E_k^n \rightarrow E_k$  называется  *$n$ -квазигруппой порядка  $k$* , если  $f(\bar{x}) \neq f(\bar{y})$  для любых двух вершин  $\bar{x}, \bar{y} \in E_k^n$  таких, что  $d(\bar{x}, \bar{y}) = 1$ . Пусть  $G(f) = \{(\bar{x}, f(\bar{x})) \mid \bar{x} \in E_k^n\}$  — график функции  $f$ . Очевидно, отображение  $G(\cdot)$  осуществляет взаимно однозначное соответствие между  $n$ -квазигруппами и МДР-кодами длины  $n + 1$ .

Пусть  $\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  — перестановка, т. е.  $\tau \in S_n$ ,  $\bar{\sigma} = (\sigma_1, \dots, \sigma_n)$  — набор перестановок вида  $\sigma_i : E_k \rightarrow E_k$ , т. е.  $\bar{\sigma} \in S_k^n$ . Для произвольной вершины  $\bar{x} \in E_k^n$  определим  $\bar{x}_\tau = (x_{\tau(1)}, \dots, x_{\tau(n)})$  и  $\bar{\sigma}\bar{x} = (\sigma_1(x_1), \dots, \sigma_n(x_n))$ . Пусть  $A \subseteq E_k^n$ . Введём обозначения

$$A_\tau = \{\bar{x}_\tau \mid \bar{x} \in A\}, \quad \bar{\sigma}A = \{\bar{\sigma}\bar{x} \mid \bar{x} \in A\}.$$

Множество (код)  $A \subseteq E_k^n$  будем называть *транзитивным*, если для любых двух вершин  $\bar{x}, \bar{y}$  из  $A$  найдутся перестановка  $\tau \in S_n$  координат и перестановки  $\bar{\sigma} \in S_k^n$  символов в каждой координате такие, что  $\bar{\sigma}\bar{y} = \bar{x}_\tau$  и  $\bar{\sigma}A = A_\tau$ . Ясно, что одну из вершин в определении транзитивности можно зафиксировать.

Основной целью настоящей статьи является доказательство следующего утверждения.

**Теорема.** При  $n \rightarrow \infty$  имеется не менее  $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1 + o(1))$  попарно неэквивалентных транзитивных расширенных совершенных кодов длины  $4n$ .

В дальнейшем мы будем рассматривать *приведённые* коды, т. е. такие, что  $\bar{0} \in A$ . В случае  $k = 2$  определение транзитивности кода  $A$

можно записать так: код  $A \subseteq E_2^n$  транзитивный, если для любой вершины  $\bar{x} \in A$  найдётся перестановка  $\tau \in S_n$  такая, что  $\bar{x} + A = A_\tau$ . Здесь и далее сложение осуществляется по модулю 2.

Приведённый код  $A \subseteq E_k^n$  будем называть *изотопно транзитивным*, если для любой вершины  $\bar{x} \in A$  найдётся такой набор перестановок  $\bar{\sigma} \in S_k^n$ , что  $\bar{\sigma}(\bar{0}) = \bar{x}$  и  $A = \bar{\sigma}A$ . При  $k = 2$  это понятие совпадает с понятием линейности кода:  $A + \bar{x} = A$  для любого  $\bar{x} \in A$ .

Будем называть  $n$ -квазигруппу *приведённой*, если  $f(\bar{0}) = 0$ . Приведённую  $n$ -квазигруппу будем называть *изотопно транзитивной*, если для любой вершины  $\bar{a} \in E_k^n$  найдутся такие перестановки  $\bar{\sigma} \in S_k^n$  и  $\sigma_{n+1} \in S_k$ , что  $\bar{\sigma}(\bar{0}) = \bar{a}$ ,  $\sigma_{n+1}(0) = f(\bar{a})$  и  $f(\bar{\sigma}\bar{x}) = \sigma_{n+1}(f(\bar{x}))$  при всех  $\bar{x} \in E_k^n$ . Из определений следуют

**Утверждение 1.**  $n$ -Квазигруппа  $f$  является изотопно транзитивной тогда и только тогда, когда МДР-код  $G(f)$  длины  $n + 1$  является изотопно транзитивным.

Коды  $A, B \subseteq E_k^n$  называются *эквивалентными*, если найдутся такие перестановки  $\tau \in S_n$  и  $\bar{\sigma} \in S_k^n$ , что  $A_\tau = \bar{\sigma}B$  (в случае  $A, B \subseteq E_2^n$  найдётся такая перестановка  $\tau \in S_n$  и вершина  $\bar{x} \in E_2^n$ , что  $A_\tau = \bar{x} + B$ ).

**Утверждение 2.** Эквивалентные коды являются транзитивными (изотопно транзитивными) одновременно.

Конструкция, предложенная в [5] и [6], связывает МДР-коды и расширенные совершенные коды. Рассмотрим частный случай этой конструкции. Зафиксируем  $R \subset E_2^n$  — линейный расширенный совершенный код (код Хемминга). Пусть  $M \subset E_4^n$  — приведённый МДР-код (не зависящий от  $\bar{r}$ ). Определим разбиения множеств  $E_{2,0}^4$  и  $E_{2,1}^4$  на коды равенством

$$C_a^r = C_0 + (1 + r)\bar{e}_4 + \bar{e}_a,$$

где  $r \in \{0, 1\}$ ,  $a \in E_4$ ,  $C_0 = \{\bar{0}, \bar{1}\} \subset E_2^4$ ,  $\bar{e}_i \in E_2^4$  — единичные вектора с 1 на  $i$ -м месте (считаем, что  $\bar{e}_0 = \bar{e}_4$ ). Таким образом,  $C_0^0 = \{(0000), (1111)\}$ ,  $C_1^0 = \{(0110), (1001)\}$ ,  $C_2^0 = \{(0101), (1010)\}$ ,  $C_3^0 = \{(0011), (1100)\}$ ,  $C_0^1 = \{(0001), (1110)\}$ ,  $C_1^1 = \{(0111), (1000)\}$ ,  $C_2^1 = \{(0100), (1011)\}$ ,  $C_3^1 = \{(0010), (1101)\}$ .

Определим приведённый расширенный совершенный код  $C \subset E_{2,0}^{4n}$  равенством

$$C = \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in M} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_n}^{r_n}. \quad (1)$$

## 2. Транзитивные коды

Нетрудно заметить, что все совершенные расширенные коды длины 4 можно представить в виде  $\{\bar{v}, \bar{v} + \bar{1}\}$ , т. е. как смежные классы  $C_a^r$  кода  $C_0^0 = \{\bar{0}, \bar{1}\} \subset E_2^4$ . Покажем, что при  $k = 4$  перестановка координат соответствует перестановке смежных классов.

**Утверждение 3.** (а) Для любого  $b \in E_k$  найдётся такая перестановка  $\sigma \in S_4$ , что  $C_a^r + \bar{e}_b + \bar{e}_4 = C_{\sigma(a)}^r$  для всех  $a \in E_4$  и  $r \in \{0, 1\}$ .

(б) Для любой перестановки  $\tau \in S_4$  найдётся такая перестановка  $\sigma \in S_4$ , что  $(C_a^0)_\tau = C_{\sigma(a)}^0$  для всех  $a \in E_4$ .

(с) Для любой перестановки  $\sigma \in S_4$  найдётся перестановка  $\tau \in S_4$  такая, что  $C_{\sigma(a)}^r + \bar{e}_{\sigma(0)} + \bar{e}_4 = (C_a^r)_\tau$  для всех  $a \in E_4$  и  $r \in \{0, 1\}$ .

**ДОКАЗАТЕЛЬСТВО.** (а), (б). Рассмотрим разбиение  $J$  множества  $E_{2,0}^4$  на коды  $C_0^0, C_1^0, C_2^0, C_3^0$ . Очевидно, что перестановка координат и прибавление вершины с чётным числом единиц переводит элементы из  $J$  в элементы из  $J$ , т. е. порождает их перестановку. Так как  $C_a^r = r\bar{e}_4 + C_a^0$ , то перестановка  $\sigma$  не зависит от  $r \in \{0, 1\}$ .

(с) Из (а) получаем равенство  $C_{\sigma(a)}^r + \bar{e}_{\sigma(0)} + \bar{e}_4 = C_{\tau(a)}^r$ , в котором перестановка  $\tau$  не зависит от  $r \in \{0, 1\}$ . Так как  $C_{\sigma(0)}^r + \bar{e}_{\sigma(0)} + \bar{e}_4 = C_0^r$ , то  $\tau(0) = 0$ . Тогда, как нетрудно видеть,  $C_{\tau(a)}^r = (C_a^r)_\tau$  при  $a \neq 0$ . Кроме того,  $C_0^r = (C_0^r)_\pi$  для произвольной перестановки  $\pi$ , оставляющей на месте последнюю координату. Утверждение 3 доказано.

**Лемма 1.** Пусть  $M$  — изотопно транзитивный МДР-код длины  $n$ . Тогда расширенный совершенный код  $C$  длины  $4n$ , заданный равенством (1), является транзитивным.

**ДОКАЗАТЕЛЬСТВО.** Представим вершину  $\bar{y} \in C$  в виде  $\bar{y} = (\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_n)$ , где  $\tilde{y}_i = (1 + r_i)\bar{e}_4 + \bar{e}_{b_i} + \delta\bar{1}$ ,  $\delta \in \{0, 1\}$ ,  $\bar{r} \in R$ . Из линейности кода  $R$  вытекает, что если  $\bar{y} = (\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_n) \in C$ , то  $(\tilde{y}_1 + r_1\bar{e}_4, \tilde{y}_2 + r_2\bar{e}_4, \dots, \tilde{y}_n + r_n\bar{e}_4) \in C$  при любом  $\bar{r} \in R$ . Из определения  $C_a^r$  вытекает, что если  $\bar{y} = (\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_n) \in C$ , то  $(\tilde{y}_1 + \delta_1\bar{1}, \tilde{y}_2 + \delta_2\bar{1}, \dots, \tilde{y}_n + \delta_n\bar{1}) \in C$  при любом  $\bar{\delta} \in E_2^n$ . Следовательно,

$$\bar{y} + C = v(\bar{b}) + C, \quad (2)$$

где  $v(\bar{b}) = (\bar{e}_4 + \bar{e}_{b_1}, \dots, \bar{e}_4 + \bar{e}_{b_n})$  и  $\bar{b} \in M$ . Так как код  $M$  изотопно транзитивный, то найдётся набор перестановок  $\bar{\sigma}$ , удовлетворяющий равенствам  $\bar{\sigma}M = M$  и  $\bar{\sigma}\bar{0} = \bar{b}$ . Из пункта (с) утверждения 3 следует, что найдутся перестановки  $\tau_i \in S_4$ ,  $i = 1, \dots, n$  такие, что

$$C_{\sigma_i(a)}^r + \bar{e}_{b_i} + \bar{e}_4 = (C_a^r)_{\tau_i}, \quad (3)$$

при всех  $a \in E_4$  и  $r \in \{0, 1\}$ . Из равенств (1)–(3) имеем

$$\begin{aligned}
 \bar{y} + C &= v(\bar{b}) + \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in M} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_n}^{r_n} \\
 &= v(\bar{b}) + \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in \bar{\sigma}M} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_n}^{r_n} \\
 &= \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in M} (\bar{e}_4 + \bar{e}_{b_1} + C_{\sigma_1(a_1)}^{r_1}) \times (\bar{e}_4 + \bar{e}_{b_2} + C_{\sigma_2(a_2)}^{r_2}) \times \cdots \times (\bar{e}_4 + \bar{e}_{b_n} \\
 &\quad + C_{\sigma_n(a_n)}^{r_n}) = \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in M} \left( C_{a_1}^{r_1} \right)_{\tau_1} \times \left( C_{a_2}^{r_2} \right)_{\tau_2} \times \cdots \times \left( C_{a_n}^{r_n} \right)_{\tau_n} = C_\pi
 \end{aligned}$$

для соответствующей перестановки  $\pi \in S_{4n}$ . Лемма 1 доказана.

### 3. Эквивалентные коды

Обозначим через  $I = \{I(1), I(2), \dots, I(n)\}$  разбиение множества  $\{1, 2, \dots, 4n\}$  на четвёрки вида  $I(j) = \{4j - 3, 4j - 2, 4j - 1, 4j\}$ . Пусть  $\tau \in S_{4n}$ . Обозначим через  $I_\tau$  разбиение, состоящее из множеств  $\{\tau(4j - 3), \tau(4j - 2), \tau(4j - 1), \tau(4j)\}$ . Пусть перестановка  $\tau \in S_{4n}$  такова, что  $I = I_\tau$ . Тогда перестановка  $\tau$  порождается перестановкой  $\tau^* \in S_n$  элементов разбиения  $I$  и набором перестановок  $\tau_1, \tau_2, \dots, \tau_n \in S_4$ , где  $\tau_i$  — перестановка на множестве  $I(j)$ .

**Утверждение 4.** Пусть  $C$  и  $C'$  — расширенные совершенные коды длины  $4n$ , удовлетворяющие равенству (1) с МДР-кодами  $M$  и  $M'$  соответственно, причём коды  $C$  и  $C'$  эквивалентны, т. е.  $C'_\tau = \bar{y} + C$  для некоторых  $\tau \in S_{4n}$  и  $\bar{y} \in E_2^{4n}$ . Если  $I = I_\tau$ , то МДР-коды  $M$  и  $M'$  эквивалентны.

**Доказательство.** Поскольку коды  $C$  и  $C'$  приведённые,  $\bar{y} \in C$ . Представим вершину  $\bar{y} \in C$  в виде  $\bar{y} = (\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_n)$ , где  $\tilde{y}_i = (1 + r_i)\bar{e}_4 + \bar{e}_{b_i} + \delta \bar{1}$ ,  $\delta \in \{0, 1\}$ . По пункту (а) утверждения 3 найдутся перестановки  $\sigma_i \in S_4$ ,  $i = 1, \dots, n$ , такие, что

$$C_{a_i}^r + \bar{e}_{b_i} + \bar{e}_4 = C_{\sigma_i(a_i)}^r,$$

где  $r \in \{0, 1\}$ . Тогда из равенств (1)–(2) получаем

$$\begin{aligned}
 \bar{y} + C &= \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in M} (\bar{e}_4 + \bar{e}_{b_1} + C_{a_1}^{r_1}) \times (\bar{e}_4 + \bar{e}_{b_2} + C_{a_2}^{r_2}) \times \cdots \times (\bar{e}_4 + \bar{e}_{b_n} + C_{a_n}^{r_n}) \\
 &= \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in \bar{\sigma}M} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_n}^{r_n}. \quad (4)
 \end{aligned}$$

Поскольку  $C'_\tau = \bar{y} + C$  и  $I = I_\tau$ , из (4) следует равенство  $\bar{r}_{\tau^*} = \bar{r}$  для всех  $\bar{r} \in R$ .

Рассмотрим вершины кодов  $C$  и  $C'$ , у которых в каждом из четырёх координатах с номерами вида  $4i + 1, 4i + 2, 4i + 3, 4i + 4$  (где  $i$  — натуральное) содержится чётное число единиц. Из равенств  $C'_\tau = \bar{y} + C$  и (4) имеем

$$\bigcup_{\bar{a} \in \bar{\sigma}M} C_{a_1}^0 \times C_{a_2}^0 \times \cdots \times C_{a_n}^0 = \bigcup_{\bar{a} \in M'} (C_{a_{\tau^*(1)}}^0)_{\tau_1} \times (C_{a_{\tau^*(2)}}^0)_{\tau_2} \times \cdots \times (C_{a_{\tau^*(n)}}^0)_{\tau_n}.$$

Тогда из пункта (b) утверждения 3 получаем

$$\begin{aligned} \bigcup_{\bar{a} \in \bar{\sigma}M} C_{a_1}^0 \times C_{a_2}^0 \times \cdots \times C_{a_n}^0 \\ = \bigcup_{\bar{a} \in M'} C_{\sigma'_1(a_{\tau^*(1)})}^0 \times C_{\sigma'_2(a_{\tau^*(2)})}^0 \times \cdots \times C_{\sigma'_n(a_{\tau^*(n)})}^0 \\ = \bigcup_{\bar{a} \in \bar{\sigma}'(M'_{\tau^*})} C_{a_1}^0 \times C_{a_2}^0 \times \cdots \times C_{a_n}^0. \end{aligned}$$

Таким образом,  $\bar{\sigma}M = \bar{\sigma}'(M'_{\tau^*})$ , т. е. МДР-коды  $M$  и  $M'$  эквивалентны. Утверждение 4 доказано.

Ортогональным дополнением кода  $A \subseteq E^n$  называется линейное пространство  $A^\perp = \{\bar{x} \in E^n \mid \langle \bar{x}, \bar{y} \rangle = 0 \text{ для всех } \bar{y} \in A\}$ . Известно, что ортогональное дополнение  $R^\perp$  линейного кода  $R \subseteq E^n$  является кодом Адамара и имеет размерность  $\log_2 n + 1$ . Здесь и далее  $\log n = \log_2 n$ .

Введём обозначения  $r^4 = (rrrr)$ , где  $r \in \{0, 1\}$ , и  $\bar{p}^4 = (p_1^4, p_2^4, \dots, p_n^4)$  для вершины  $\bar{p} \in E^n$ . Пусть  $\bar{p} \in R^\perp$ , тогда  $\bar{p}^4 \in C^\perp$ , где код  $C$  определяется равенством (1). Очевидно, что множество  $R^{\perp 4} = \{\bar{p}^4 \mid \bar{p} \in R^\perp\}$  является линейным подпространством пространства  $C^\perp$  размерности  $\log n + 1$ . В [4] показано, что размерность  $C^\perp$  может равняться  $\log n + 1$ ,  $\log n + 2$  или  $\log n + 3$ , причём в последнем случае расширенный совершенный код  $C$  является линейным.

**Утверждение 5.** Пусть  $\tau, \pi \in S_{4n}$ . Если  $(R^{\perp 4})_\tau = (R^{\perp 4})_\pi$ , то  $I_\tau = I_\pi$ .

**Доказательство.** Без ограничения общности можно считать, что  $\pi$  — тождественная подстановка.

Пусть  $I_\tau \neq I$ . Без ограничения общности можно считать, что при перестановке  $\tau$  на первое и второе места перемещаются члены из разных элементов разбиения, т. е.  $\tau^{-1}(1) \in I(i)$ ,  $\tau^{-1}(2) \in I(j)$ , где  $i \neq j$ . По известному свойству кода Адамара найдётся такая вершина  $\bar{p} \in R^\perp$ , что

$p_i \neq p_j$ . Пусть  $\bar{v} = \bar{p}_\tau^4$ , тогда из выбора  $\bar{p}$  следует, что  $v_1 \neq v_2$ . Поэтому  $\bar{v} \notin R^{\perp 4}$ . Утверждение 5 доказано.

Пусть  $M(C)$  — множество МДР-кодов, соответствующих кодам, эквивалентным расширенному совершенному коду  $C$ , т. е.  $M' \in M(C)$ , если найдётся расширенный совершенный приведённый код  $C'$ , который эквивалентен коду  $C$  и удовлетворяет равенству (1) с МДР-кодом  $M'$ .

Доказательство и формулировка следующей леммы принадлежат Д. С. Кротову.

**Лемма 2.** Пусть  $C$  — нелинейный расширенный совершенный код длины  $4n$ , удовлетворяющий равенству (1). Тогда в множестве  $M(C)$  содержится не более  $2n - 1$  классов эквивалентности МДР-кодов.

ДОКАЗАТЕЛЬСТВО. Пусть  $M'$  и  $M''$  — неэквивалентные МДР-коды из  $M(C)$ . Тогда имеются коды  $C'$  и  $C''$ , удовлетворяющие равенству (1) с МДР-кодами  $M'$  и  $M''$  соответственно, причём

$$C'_{\tau'} + \bar{y} = C = C''_{\tau''} + \bar{z}, \quad (5)$$

для некоторых перестановок  $\tau', \tau'' \in S_{4n}$  и вершин  $\bar{y}, \bar{z} \in C$ .

Из утверждения 4 следует, что  $I_{\tau'} \neq I_{\tau''}$ , а из утверждения 5 следует неравенство

$$(R^{\perp 4})_{\tau''} \neq (R^{\perp 4})_{\tau'}. \quad (6)$$

Из равенства (5) видно, что  $(C'^{\perp})_{\tau'} = (C''^{\perp})_{\tau''} = C^{\perp}$ . Поэтому  $(R^{\perp 4})_{\tau''} \subseteq C^{\perp}$  и  $(R^{\perp 4})_{\tau'} \subseteq C^{\perp}$ , причём, как было замечено выше, размерность пространства  $(R^{\perp 4})$  равна  $\log n + 1$ , а размерность пространства  $C^{\perp}$  равна  $\log n + 2$  (размерность  $\log n + 1$  невозможна из-за (6), а  $\log n + 3$  — из-за нелинейности кода  $C$ ). Линейный код  $R$  содержится в  $E_{2,0}^n$ , поэтому  $\bar{1} \in R^{\perp}$ . Число способов, которыми можно выбрать различные гиперподпространства в  $C^{\perp}$ , содержащие вершину  $\bar{1}$ , равняется половине мощности множества  $C^{\perp}$  без единицы, т. е. равно  $2n - 1$ . Поскольку для пары неэквивалентных МДР-кодов  $M'$  и  $M''$  найдётся пара различных гиперподпространств в  $C^{\perp}$ , то множество  $M(C)$  разбивается не более чем на  $2n - 1$  классов эквивалентности. Лемма 2 доказана.

#### 4. Число транзитивных кодов

На множестве  $E_4$  введём бинарные операции: через  $\oplus$  будем обозначать сложение, изоморфное сложению в группе  $Z_2 \times Z_2$ , а через  $*$  — сложение, изоморфное сложению в группе  $Z_4$ . Таблицы этих операций имеют следующий вид:

$*$	0	1	2	3	$\oplus$	0	1	2	3
0	0	1	2	3	0	0	1	2	3
1	1	2	3	0	1	1	0	3	2
2	2	3	0	1	2	2	3	0	1
3	3	0	1	2	3	3	2	1	0

Известно и легко проверяемо

**Утверждение 6.** Не существует перестановок  $\sigma_0, \sigma_1, \sigma_2 \in S_4$  таких, что  $\sigma_0(\sigma(x_1) * \sigma(x_2)) = x_1 \oplus x_2$ .

**Утверждение 7.** (а)  $n$ -Квазигруппа  $f(x_1, x_2, \dots, x_n) = x_1 * x_2 * \dots * x_n$  является изотопно транзитивной.

(б)  $n$ -Квазигруппа  $h(x_1, x_2, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$  является изотопно транзитивной. Более того, для любой вершины  $\bar{a} \in E_4^n$  и любой перестановки  $\sigma_0 \in S_4$  такой, что  $\sigma_0(0) = h(\bar{a})$ , найдётся набор перестановок  $\bar{\sigma} \in S_4^n$ , для которого выполнены равенства  $\bar{\sigma}\bar{0} = \bar{a}$  и  $h(\bar{\sigma}\bar{x}) = \sigma_0(h(\bar{x}))$ .

**ДОКАЗАТЕЛЬСТВО.** (а) Пусть  $a_1 * a_2 * \dots * a_n = a_0$ . Определим  $\sigma_i(y) = y * a_i$  для всех  $i = 0, \dots, n$ . Из ассоциативности и коммутативности операции  $*$  следует равенство

$$f(\bar{\sigma}\bar{x}) = (x_1 * a_1) * (x_2 * a_2) * \dots * (x_n * a_n) = x_1 * x_2 * \dots * x_n * a_0 = \sigma_0(f(\bar{x})).$$

(б) Пусть  $\varphi \in S_4$  такова, что  $\varphi(0) = 0$ . Покажем, что при любых  $a, b \in E_4$  справедливо равенство

$$\varphi(a) \oplus \varphi(b) = \varphi(a \oplus b). \quad (7)$$

Рассмотрим три случая.

1) Если  $a = 0$  ( $b = 0$ ), то  $\varphi(0) \oplus \varphi(b) = \varphi(b \oplus 0)$ .

2) Если  $a = b$ , то  $\varphi(a) \oplus \varphi(a) = 0 = \varphi(0) = \varphi(a \oplus a)$ .

3) Пусть  $a \neq 0, b \neq 0$  и  $a \neq b$ . Оставшийся элемент из  $E_4$  обозначим через  $c$  ( $a \neq c, b \neq c, 0 \neq c$ ). Из таблицы для операции  $\oplus$  видно, что  $a \oplus b \notin \{a, b, 0\}$  и  $\varphi(a) \oplus \varphi(b) \notin \{\varphi(a), \varphi(b), 0\}$ , т. е.  $a \oplus b = c$  и  $\varphi(a) \oplus \varphi(b) = \varphi(c)$ .

Пусть  $a_1 \oplus a_2 \oplus \dots \oplus a_n = a_0$ . Для перестановки  $\sigma_0 \in S_4$ , ( $\sigma_0(0) = a_0$ ) определим перестановку  $\varphi(y) = \sigma_0(y) \oplus a_0$ . Очевидно, что  $\varphi(0) = 0$ . Пусть  $\sigma_i(y) = \varphi(y) \oplus a_i$  при всех  $i = 1, \dots, n$ . Тогда из равенства (7) имеем

$$\begin{aligned} h(\bar{\sigma}\bar{x}) &= (\varphi(x_1) \oplus a_1) \oplus (\varphi(x_2) \oplus a_2) \oplus \dots \oplus (\varphi(x_n) \oplus a_n) \\ &= \varphi(h(\bar{x})) \oplus a_0 = \sigma_0(h(\bar{x})). \end{aligned}$$

Утверждение 7 доказано.



**Утверждение 8.** Пусть  $f$  — изотопно транзитивная  $n$ -квазигруппа и  $h(y_1, y_2, \dots, y_m) = y_1 \oplus y_2 \oplus \dots \oplus y_m$ . Тогда  $(n + m - 1)$ -квазигруппа  $f(x_1, \dots, x_{i-1}, h(\bar{y}), x_{i+1}, \dots, x_n)$  является изотопно транзитивной.

**ДОКАЗАТЕЛЬСТВО.** Без ограничения общности будем считать, что  $i = n$ . Пусть  $\bar{b} \in E_4^m$ ,  $h(\bar{b}) = a_n$  и  $\bar{a} \in E_4^n$ . Из условия следует, что найдутся перестановки  $\bar{\sigma} \in S_4^n$  и  $\sigma_0 \in S_4$ , удовлетворяющие равенствам  $\bar{\sigma}\bar{b} = \bar{a}$ ,  $\sigma_0(0) = f(\bar{a})$  и  $f(\bar{\sigma}x) = \sigma_0(f(x))$  для всех  $x \in E_4^n$ . Из утверждения 7 следует, что найдётся набор перестановок  $\bar{\tau} \in S_4^m$  такой, что  $h(\bar{\tau}\bar{y}) = \sigma_n(h(\bar{y}))$  и  $\bar{\tau}\bar{b} = \bar{b}$ . Тогда

$$\begin{aligned} f(\sigma_1(x_1), \dots, \sigma_{n-1}(x_{n-1}), h(\bar{\tau}\bar{y})) &= f(\sigma_1(x_1), \dots, \sigma_{n-1}(x_{n-1}), \sigma_n(h(\bar{y}))) \\ &= \sigma_0(f(x_1, \dots, x_{n-1}, h(\bar{y}))). \end{aligned}$$

Утверждение 8 доказано.

**Лемма 3.** Пусть  $p(n)$  — число различных представлений числа  $n$  в виде неупорядоченной суммы натуральных слагаемых. Тогда число классов эквивалентности изотопно транзитивных МДР-кодов длины  $n + 1$  не меньше  $p(n)$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\{x_1, x_2, \dots, x_n\}$  — множество координат. Рассмотрим его разбиения  $J = \{J(1), J(2), \dots, J(k)\}$ . Спектром разбиения будем называть величину  $Sp(J) = (|J(i_1)|, |J(i_2)|, \dots, |J(i_k)|)$ , где  $|J(i_1)| \leq |J(i_2)| \leq \dots \leq |J(i_k)|$ . Определим функции

$$h(\tilde{x}_{J(i)}) = x_{j_1} \oplus \dots \oplus x_{j_{|J(i)|}},$$

где  $J(i) = \{j_1, \dots, j_{|J(i)|}\}$  и  $g_J(\bar{x}) = h(\tilde{x}_{J(1)}) * h(\tilde{x}_{J(2)}) * \dots * h(\tilde{x}_{J(k)})$ . Покажем от противного, что из неравенства спектров  $Sp(J) \neq Sp(I)$  следует неэквивалентность МДР-кодов  $G(g_J)$  и  $G(g_I)$ . Пусть найдутся перестановки  $\tau \in S_{n+1}$  и  $\bar{\sigma} \in S_4^{n+1}$  такие, что

$$\begin{aligned} \{(x_1, x_2, \dots, x_{n+1}) \mid g_J(\bar{\sigma}x) = \sigma_{n+1}(x_{n+1})\} \\ = \{(x_1, x_2, \dots, x_{n+1}) \mid g_I(\bar{x}_\tau) = x_{\tau(n+1)}\}. \end{aligned} \quad (8)$$

Без ограничения общности положим, что  $|I| \leq |J|$ . Поскольку  $Sp(J) \neq Sp(I)$ , найдутся такие переменные  $x_i$  и  $x_j$ , содержащиеся в разных элементах разбиения  $J$ , что  $x_{\tau^{-1}(i)}$  и  $x_{\tau^{-1}(j)}$  содержатся в одном элементе разбиения  $I$ . Подставим в равенства  $g_J(\bar{\sigma}x) = \sigma_{n+1}(x_{n+1})$  и  $g_I(\bar{x}_\tau) = x_{\tau(n+1)}$  нули вместо всех переменных, кроме  $x_i$ ,  $x_j$ ,  $x_{n+1}$ . Из первого равенства получаем  $\sigma_i(x_i) * \sigma_j(x_j) * c = \sigma_{n+1}(x_{n+1})$ , где  $c \in E_4$  или в преобразованном виде

$$\sigma_0(\sigma_i(x_i) * \sigma_j(x_j)) = x_{n+1}, \quad (9)$$

где  $\sigma_0 \in S_4$ . Из второго равенства, в зависимости от того, в каком элементе разбиения  $I$  содержится переменная  $x_{\tau^{-1}(n+1)}$ , получаем

$$x_i \oplus x_j = x_{n+1} \text{ или } x_i \oplus x_j \oplus x_{n+1} = 0 \text{ или } (x_i \oplus x_j) * x_{n+1} = 0.$$

По утверждению 6 любое из этих равенств противоречит равенству (9). Отсюда следует, что равенство (8) неверно.

Из утверждений 7 и 8 следует трансляционная транзитивность МДР-кодов  $G(g_I)$  для произвольного разбиения  $I$ . МДР-коды, соответствующие различным спектрам, неэквивалентны. Очевидно, что число различных спектров  $Sp(I)$  равно  $p(n)$ . Лемма 3 доказана.

Теперь оценим число неэквивалентных транзитивных расширенных совершенных кодов.

**ДОКАЗАТЕЛЬСТВО теоремы.** Из леммы 3 следует, что имеется  $p(n-1)$  попарно неэквивалентных изотопно транзитивных МДР-кодов длины  $n$ . Из леммы 1 следует, что, подставив любой из этих МДР-кодов в формулу (1), получим транзитивный расширенный совершенный код длины  $4n$ . Нетрудно проверить, что среди этих кодов только совершенный расширенный код, соответствующий  $n$ -квазигруппе  $h(\bar{x}) = x_1 \oplus x_2 \oplus \dots \oplus x_{n-1}$ , линеен. Тогда из леммы 2 следует, что не более  $2n-1$  построенных расширенных совершенных кодов могут попасть в один класс эквивалентности. Как показано в [3],  $p(n) = \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}} (1+o(1))$  при  $n \rightarrow \infty$ . Тогда при  $n \rightarrow \infty$  имеется не менее  $\frac{p(n-1)-1}{2n-1} = \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}} (1+o(1))$  попарно неэквивалентных транзитивных расширенных совершенных кодов длины  $4n$ . Теорема доказана.

## ЛИТЕРАТУРА

1. **Малюгин С. А.** Транзитивные совершенные коды длины 15 // Труды конференции "Дискретный анализ и исследование операций". Новосибирск: Изд-во Ин-та математики СО РАН, 2004. С. 96.
2. **Соловьёва Ф. И.** О построении транзитивных кодов // Проблемы передачи информации. 2005. Т. 41, вып. 3. С. 23–31.
3. **Эндрюс Г.** Теория разбиений. М.: Наука. 1982.
4. **Avgustinovich S. V., Heden O., Solov'eva F. I.** The classification of some perfect codes // DesIgn Codes Cryptogr. 2004. V. 31, N 3. P. 313–318.
5. **Phelps K.** A general product construction for error correcting codes // SIAM J. Algebraic and Discrete Methods. 1984. V. 5, N 2. P. 224–228.

- 6. Zinoviev V. A.** On generalized concatenated codes // Topic in Information Theory. Colloq. Math. Soc. Janos Boliai. Amsterdam: North-Holland, 1977. P. 587–592.

Адрес автора:

Статья поступила  
9 марта 2006 г.

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