

## $Z_4$ -ЛИНЕЙНЫЕ СОВЕРШЕННЫЕ КОДЫ\*)

Д. С. Кротов

Показано, что при любом  $n = 2^k \geq 16$  число попарно неэквивалентных  $Z_4$ -линейных расширенных совершенных кодов с расстоянием 4 равно  $\lfloor (k+1)/2 \rfloor$ . Все эти коды имеют различный ранг.

### Введение

Многие известные нелинейные двоичные коды, такие как коды Кердока, Препараты, Гёталса, Дельсарта-Гёталса, представимы при помощи отображения  $0 \rightarrow 00, 1 \rightarrow 01, 2 \rightarrow 11, 3 \rightarrow 10$  как линейные коды в алфавите  $\{0, 1, 2, 3\}$  с операциями по модулю 4 (см. [6, 10, 4, 5, 9]). Представимые таким образом коды называются  $Z_4$ -линейными. В [9] показано, что расширенные совершенные код Голея и коды Хемминга с параметрами  $(n, 2^{n-\log_2 n-1}, 4)$  (длины  $n$ , мощности  $2^{n-\log_2 n-1}$  и с расстоянием 4) при  $n > 16$  не являются  $Z_4$ -линейными. Там же для любого  $n = 2^k$  описан  $Z_4$ -линейный  $(2, 2^{n-\log_2 n-1}, 4)$ -код (приведено циклическое представление кодов  $C^{0,r_2}$ , определённых в § 2). Целью настоящей работы является полное описание  $Z_4$ -линейных совершенных и расширенных совершенных кодов.

Известно [1, 12], что не существует нетривиальных совершенных двоичных кодов, кроме  $(23, 2^{12}, 7)$ -кодов Голея и  $(2^k - 1, 2^{2^k-k-1}, 3)$ -кодов. Совершенные  $(23, 2^{12}, 7)$ -коды единственны с точностью до эквивалентности. Линейные  $(2^k - 1, 2^{2^k-k-1}, 3)$ -коды (Хемминга) также единственны. Однако при  $n = 2^k - 1 \geq 15$  существует более  $2^{2^{(n+1)/2-k}}$  (последнюю нижнюю оценку см. в [13]) нелинейных кодов с теми же параметрами (обзор некоторых конструкций см. в [11, 7]). Весь класс  $(2^k - 1, 2^{2^k-k-1}, 3)$ -кодов на данный момент не описан.

В настоящей статье показано, что не очень большое, но растущее по  $k$  число расширенных совершенных  $(2^k, 2^{2^k-k-1}, 4)$ -кодов могут быть представлены как линейные коды над кольцом  $Z_4$ . В § 2 в терминах

---

\*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 00-01-00822).

проверочных матриц описаны  $\lfloor (\log_2 n + 1)/2 \rfloor$  расширенных совершенных  $(n, 2^n/2n, 4)$ -кодов, являющихся  $Z_4$ -линейными.

В § 3 показано, что такие коды попарно неэквивалентны. В § 4 доказывается несуществование  $Z_4$ -линейных  $(n, 2^n/2n, 4)$ -кодов, неэквивалентных ни одному из построенных. В § 5 предложен индуктивный способ построения  $Z_4$ -линейных расширенных совершенных кодов.

Итак, все  $Z_4$ -линейные  $(n, 2^n/2n, 4)$ -коды описаны с точностью до эквивалентности. По определению коды нечётной длины не могут быть  $Z_4$ -линейными. Код Голея длины 24, как уже было отмечено, тоже не является  $Z_4$ -линейным. Очевидно, что все тривиальные совершенные и расширенные совершенные двоичные коды, т. е. код из одной нулевой вершины,  $(n, 2, n)$ -код с повторением,  $(n, 2^{n-1}, 2)$ -код с проверкой на чётность и полный  $(n, 2^n, 1)$ -код, являются  $Z_4$ -линейными при условии чётности длины. Таким образом, вопрос описания всех  $Z_4$ -линейных совершенных и расширенных совершенных кодов получил исчерпывающий ответ.

### § 1. Основные понятия и обозначения

Обозначим через  $E^n$  множество всех двоичных слов длины  $n$ . Расстоянием Хемминга  $d(x, y)$  между словами  $x, y \in E^n$  называется число позиций, в которых  $x$  и  $y$  различаются. Двоичным  $(n, K, d)$ -кодом называется такое множество  $C \subset E^n$ , что  $|C| = K$  и расстояние Хемминга между любыми двумя различными словами из  $C$  не меньше  $d$ . Код  $C$  называется *линейным*, если он замкнут относительно сложения по модулю 2.

Код  $C$  с параметрами  $(n, K, 2\rho + 1)$  называется *совершенным*, если расстояние от любого слова из  $E^n$  до  $C$  не превосходит  $\rho$ . Код с параметрами  $(n, K, 2\rho + 2)$  называется *расширенным совершенным*, если после удаления из каждого кодового слова последнего символа получается совершенный  $(n - 1, K, 2\rho + 1)$ -код. Код с параметрами  $(n, K, 4)$  является расширенным совершенным тогда и только тогда, когда  $K = 2^{n-1}/n$ .

Обозначим через  $Z_4^n$  множество слов длины  $n$  в алфавите  $Z_4 = \{0, 1, 2, 3\}$  с заданным по mod 4 сложением и умножением на константу. Будем говорить, что слово  $s \in Z_4^n$  имеет *состав*  $1^{n_1}2^{n_2}3^{n_3}$ , если в  $s$  содержится  $n_1$  единиц,  $n_2$  двоек,  $n_3$  троек и  $n - n_1 - n_2 - n_3$  нулей, расположенных в произвольном порядке. Аддитивную подгруппу  $Z_4^n$  назовём *кватернарным кодом*. Два кватернарных кода называются *эквивалентными*, если один код можно получить из другого перестановкой координат и (или) заменой элемента на противоположный по mod 4 (т. е. 0 на 0, 1 на 3, 2 на 2 и 3 на 1) в некоторых координатах. Если при этом

достаточно только перестановки координат, коды называются *перестановочно эквивалентными*.

*Весом Ли*  $wt_L(a)$  слова  $a$  из  $Z_4^n$  называется обычная (над  $Z$ ) сумма весов Ли всех координат слова  $a$ , где  $wt_L(0) = 0$ ,  $wt_L(1) = wt_L(3) = 1$  и  $wt_L(2) = 2$ . Эта весовая функция определяет на  $Z_4^n$  метрику Ли  $d_L(a, b) = wt_L(b - a)$ . Кватернарный код  $\mathcal{C} \subset Z_4^n$  назовём *кватернарным кодом длины  $n$  с расстоянием  $d$* , или  $(n, |\mathcal{C}|, d)_4$ -кодом, если  $d_L(a, b) \geq d$  для любых различных  $a, b \in \mathcal{C}$ , что эквивалентно условию  $wt_L(a) \geq d$  для любого ненулевого  $a \in \mathcal{C}$ .

Любой кватернарный код  $\mathcal{C}$  можно задать *порождающей матрицей* вида

$$G = \begin{bmatrix} G_1 \\ 2G_2 \end{bmatrix}, \quad (1)$$

где  $G_1$  есть  $Z_4$ -матрица размера  $k_1 \times n$ ,  $G_2$  есть  $Z_2$ -матрица размера  $k_2 \times n$ ,  $|\mathcal{C}| = 2^{2k_1 + k_2}$  и каждое слово  $c$  из  $\mathcal{C}$  представимо в виде

$$c = (v_1, v_2) \begin{bmatrix} G_1 \\ 2G_2 \end{bmatrix} \pmod{4}, \quad v_1 \in Z_4^{k_1}, \quad v_2 \in Z_2^{k_2}.$$

Код  $\mathcal{C}$ , заданный порождающей матрицей (1), является элементарной абелевой группой типа  $4^{k_1}2^{k_2}$ . Будем обозначать это следующим образом:  $|\mathcal{C}| = 4^{k_1}2^{k_2}$ .

Говорят, что слова  $x = (x_0, \dots, x_{n-1})$  и  $x' = (x'_0, \dots, x'_{n-1})$  из  $Z_4^n$  (из  $E^n$ ) *ортогональны* (обозначение  $x \perp x'$ ), если  $x_0x'_0 + \dots + x_{n-1}x'_{n-1} = 0 \pmod{4}$  (соответственно по  $\pmod{2}$ ). Отношение ортогональности естественным образом расширяется на ортогональность слова и множества слов и ортогональность двух множеств слов из  $Z_4^n$  (из  $E^n$ ).

Кватернарный код  $\mathcal{C}$  типа  $4^{k_1}2^{k_2}$  может быть задан посредством *проверочной матрицы*

$$A = \begin{bmatrix} A_1 \\ 2A_2 \end{bmatrix}$$

такой, что

$$Ac^T = 0 \text{ для любого } c \in \mathcal{C},$$

где  $A_1$  есть  $Z_4$ -матрица размера  $(n - k_1 - k_2) \times n$  и  $A_2$  есть  $Z_2$ -матрица размера  $k_2 \times n$ . Матрица  $A$  является порождающей для *дуального* к  $\mathcal{C}$  кватернарного кода  $\mathcal{C}^*$ , который можно определить так же, как множество слов, ортогональных коду  $\mathcal{C}$ .

Определим два отображения  $\beta(c)$  и  $\gamma(c)$  из  $Z_4$  в  $Z_2 = \{0, 1\}$ :

$$\begin{array}{ccc} c & \beta(c) & \gamma(c) \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \end{array},$$

покоординатно расширив их на отображения из  $Z_4^n$  в  $Z_2^n$ . Отображение Грея  $\phi: Z_4^n \rightarrow E^{2n}$  определяется соотношением

$$\phi(c) = (\beta(c), \gamma(c)), \quad c \in Z_4^n,$$

(таким образом,  $i$ -й координате слова  $c$  соответствует  $i$ -я и  $(i+n)$ -я координаты двоичного слова  $\phi(c)$ ). Применив  $\phi(\cdot)$  к каждому кодовому слову, произвольному кватернарному коду можно поставить в соответствие двоичный код вдвое большей длины и той же мощности. Следуя [9], кватернарные коды будем обозначать прописными буквами, а соответствующие им двоичные коды — обычными латинскими: например,  $C = \phi(\mathcal{C})$ ,  $B = \phi(\mathcal{B})$ ,  $C^{2,3} = \phi(\mathcal{C}^{2,3})$ . Двоичный код  $C$ , полученный применением отображения Грея ко всем словам некоторого кватернарного кода  $\mathcal{C}$ , а также все коды, которые можно получить из  $C$  при помощи перестановки координат, называются  $Z_4$ -линейными.

Два двоичных кода  $C$  и  $C'$  длины  $n$  называются эквивалентными, если существуют такое слово  $y \in E^n$  и такая перестановка  $\pi$  порядка  $n$ , что  $C = \pi(C' \oplus y)$ . Если кватернарные коды  $\mathcal{C}$  и  $\mathcal{C}'$  эквивалентны, то соответствующие двоичные коды  $C$  и  $C'$  также эквивалентны (смене знака в  $i$ -й координате кода  $\mathcal{C}$  длины  $n$  соответствует транспозиция  $(i, i+n)$  координат кода  $C$ ).

Непосредственно из определений метрик Хемминга  $d(\cdot, \cdot)$  и Ли  $d_L(\cdot, \cdot)$  и отображения Грея  $\phi(\cdot)$  следует, что

$$d_L(a, b) = d(\phi(a), \phi(b)), \quad a, b \in Z_4^n.$$

Таким образом, справедлива

**Лемма 1** [9]. Отображение  $\phi$  является изометрией между пространством  $Z_4^n$  с метрикой Ли и пространством  $E^{2n}$  с метрикой Хемминга.

$(n, 4^n/4n, 4)_4$ -код назовём совершенным кватернарным кодом. Из леммы 1 следует, что кватернарный код  $\mathcal{C}$  является совершенным тогда и только тогда, когда  $C$  является расширенным совершенным двоичным кодом с расстоянием 4.

## § 2. Конструкция $Z_4$ -линейных расширенных совершенных кодов

Пусть  $r_1$  и  $r_2$  — неотрицательные целые числа. Из всевозможных столбцов вида  $z^T$ ,  $z \in \{1\} \times \{0, 1, 2, 3\}^{r_1} \times \{0, 2\}^{r_2}$ , упорядоченных лексикографически, составим матрицу  $A^{r_1, r_2}$ . Например,

$$A^{0,0} = [1], \quad A^{0,1} = \begin{bmatrix} 11 \\ 02 \end{bmatrix},$$

$$\begin{aligned}
 A^{1,0} &= \begin{bmatrix} 1111 \\ 0123 \end{bmatrix}, & A^{0,2} &= \begin{bmatrix} 1111 \\ 0022 \\ 0202 \end{bmatrix}, \\
 A^{1,1} &= \begin{bmatrix} 11 & 11 & 11 & 11 \\ 00 & 11 & 22 & 33 \\ 02 & 02 & 02 & 02 \end{bmatrix}, & A^{0,3} &= \begin{bmatrix} 11 & 11 & 11 & 11 \\ 00 & 00 & 22 & 22 \\ 00 & 22 & 00 & 22 \\ 02 & 02 & 02 & 02 \end{bmatrix}, \\
 A^{2,0} &= \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 0000 & 1111 & 2222 & 3333 \\ 0123 & 0123 & 0123 & 0123 \end{bmatrix}.
 \end{aligned}$$

**Теорема 1.** *Кватернарный код*

$$\mathcal{C}^{r_1, r_2} = \{c \in Z_4^{2^{r_1+r_2}} : A^{r_1, r_2} c^T = 0\}$$

является совершенным.

**Доказательство.** Длина  $n$  кода  $\mathcal{C}^{r_1, r_2}$  равна  $4^{r_1} 2^{r_2}$  — числу элементов в  $Z_4^{r_1} \times Z_2^{r_2}$ . Код  $\mathcal{C}^{r_1, r_2*}$  с порождающей матрицей  $A^{r_1, r_2}$  имеет тип  $4^{r_1+1} 2^{r_2}$ . Поэтому  $|C^{r_1, r_2}| = 4^n / |C^{r_1, r_2*}| = 4^{n-r_1-r_2-1} 2^{r_2} = 4^n / 4n$ .

Покажем, что вес любого ненулевого слова из  $\mathcal{C}^{r_1, r_2}$  не меньше 4. Слова состава 1, 3, 2,  $1^2$ ,  $3^2$ , 12, 23,  $1^3$ ,  $1^2 3$ ,  $13^2$ ,  $3^3$  противоречат первой строке матрицы  $A^{r_1, r_2}$ . Слово состава 13 не может принадлежать  $\mathcal{C}^{r_1, r_2}$ , так как это означало бы, что разность двух различных столбцов матрицы  $A^{r_1, r_2}$  равна нулю, т. е. эти столбцы равны между собой, а это противоречит построению матрицы  $A^{r_1, r_2}$ . Теорема 1 доказана.

### § 3. Попарная неэквивалентность построенных кодов

Две  $Z_4$ -матрицы  $A$  и  $A'$  с одинаковым числом столбцов будем называть *эквивалентными*, если любая строка матрицы  $A$  является линейной комбинацией строк матрицы  $A'$  и, наоборот, любая строка матрицы  $A'$  является линейной комбинацией строк матрицы  $A$ .

Определяемые ниже функции Even, Odd, even и odd понадобятся для доказательства утверждений методом индукции.

Пусть  $n$  чётно. Если  $a_0, a_1, \dots, a_{n-1}$  — столбцы матрицы  $A = (a_0, a_1, \dots, a_{n-1})$ , то через Even( $A$ ) и Odd( $A$ ) будем обозначать матрицы  $(a_0, a_2, \dots, a_{n-2})$  и  $(a_1, a_3, \dots, a_{n-1})$ , составленные соответственно из чётных и нечётных столбцов  $A$  (т. е. столбцов с чётными и нечётными номерами). Аналогично определим Even( $x$ ) и Odd( $x$ ) для  $x = (x_0, \dots, x_{n-1}) \in Z_4^n$  или  $x = (x_0, \dots, x_{n-1}) \in E^n$ .

**Утверждение 1.**

а) При любых  $r_1 \geq 0$  и  $r_2 > 0$  матрицы  $\text{Even}(A^{r_1, r_2})$  и  $\text{Odd}(A^{r_1, r_2})$  эквивалентны матрице  $A^{r_1, r_2-1}$ .

б) При любом  $r_1 > 0$  матрицы  $\text{Even}(A^{r_1, 0})$  и  $\text{Odd}(A^{r_1, 0})$  эквивалентны матрице  $A^{r_1-1, 1}$ .

ДОКАЗАТЕЛЬСТВО. а) Матрица  $A^{r_1, r_2-1}$  получается из матрицы  $\text{Even}(A^{r_1, r_2})$  или  $\text{Odd}(A^{r_1, r_2})$  удалением последней строки. Последняя строка матрицы  $\text{Even}(A^{r_1, r_2})$  состоит из нулей, а последняя строка матрицы  $\text{Odd}(A^{r_1, r_2})$  состоит из двоек и получается умножением на 2 первой строки матрицы  $A^{r_1, r_2-1}$ .

б) Матрица  $A^{r_1-1, 1}$  совпадает с  $\text{Even}(A^{r_1, 0})$  и получается из  $\text{Odd}(A^{r_1, 0})$  вычитанием первой строки из последней, состоящей из единиц и троек. Утверждение 1 доказано.

Если  $\mathcal{C} \subset Z_4^n$ , то пусть

$$\text{even}(\mathcal{C}) \stackrel{\text{def}}{=} \{(c_0, c_2, \dots, c_{n-2}) \in Z_4^{n/2} \mid (c_0, 0, c_2, 0, \dots, c_{n-2}, 0) \in \mathcal{C}\},$$

$$\text{odd}(\mathcal{C}) \stackrel{\text{def}}{=} \{(c_1, c_3, \dots, c_{n-1}) \in Z_4^{n/2} \mid (0, c_1, 0, c_3, \dots, 0, c_{n-1}) \in \mathcal{C}\}.$$

Аналогично определим  $\text{even}(C)$  и  $\text{odd}(C)$  для  $C \subset E^n$ .

Следующие три утверждения вытекают непосредственно из определений.

**Утверждение 2.** Пусть  $\mathcal{C}$  и  $\mathcal{B}$  — кватернарные коды длины  $n$  и  $n/2$  соответственно. Тогда

а)  $\mathcal{B} = \text{even}(\mathcal{C})$  если и только если  $B = \text{even}(C)$ ,

б)  $\mathcal{B} = \text{odd}(\mathcal{C})$  если и только если  $B = \text{odd}(C)$ .

**Утверждение 3.** Пусть  $C \subset E^n$ ,  $y \in E^n$  и  $y \perp C$ . Тогда  $\text{Even}(y) \perp \text{even}(C)$  и  $\text{Odd}(y) \perp \text{odd}(C)$ .

**Утверждение 4.** Пусть  $A$  — проверочная матрица кватернарного кода  $\mathcal{C}$ . Тогда  $\text{Even}(A)$  является проверочной матрицей кода  $\text{even}(\mathcal{C})$ , а  $\text{Odd}(A)$  — проверочной матрицей кода  $\text{odd}(\mathcal{C})$ .

Из утверждений 1, 4 и 2 вытекает

**Следствие 1.** а)  $\text{even}(C^{r_1, r_2}) = \text{odd}(C^{r_1, r_2}) = C^{r_1, r_2-1}$  при любых  $r_1 \geq 0$  и  $r_2 > 0$ ,

б)  $\text{even}(C^{r_1, 0}) = \text{odd}(C^{r_1, 0}) = C^{r_1-1, 1}$  при любом  $r_1 > 0$ .

Рангом двоичного кода  $C$  (обозначается  $\text{rank}(C)$ ) называется максимальное число линейно независимых векторов из  $C$ . Ранг кода  $C$  равен его длине минус максимальное число линейно независимых векторов, ортогональных коду  $C$ . Если два кода, содержащие слово из одних нулей, имеют различный ранг, то они неэквивалентны.

Двоичное слово  $y = (y_0, \dots, y_{n-1})$  чётной длины  $n$  назовём *повторным*, если  $y_i = y_{n/2+i}$  при любом  $i$ ,  $0 \leq i \leq n/2 - 1$ . Другими словами,  $y$  повторно, если  $\phi^{-1}(y) \in \{0, 2\}^{n/2}$ . Очевидно, что сумма повторных слов повторна.

**Утверждение 5.** Если  $x, x' \in \{0, 2\}^n \subset Z_4^n$ , то  $\phi(x + x') = \phi(x) \oplus \phi(x')$ .

**Доказательство.** Поскольку сложения слов из  $Z_4^n$  и  $E^{2n}$  заданы покоординатно, достаточно убедиться только в том, что  $\phi(x_0 + x'_0) = \phi(x_0) \oplus \phi(x'_0)$  для  $x_0, x'_0 \in \{0, 2\}$ . Последнее проверяется непосредственно. Утверждение 5 доказано.

**Утверждение 6.** Пусть  $\mathcal{C}$  — кватернарный код длины  $n$  и  $x \in \{0, 2\}^n$ . Тогда соотношения  $x \perp \mathcal{C}$  и  $\phi(x) \perp C$  эквивалентны.

**Доказательство.** Достаточно показать эквивалентность  $x \perp c$  и  $\phi(x) \perp \phi(c)$  для произвольного  $c \in \mathcal{C}$ . Пусть  $k$  — число двоек в слове  $x$  и  $i_1, \dots, i_k$  — номера позиций слова  $x$ , в которых содержится 2. Тогда соотношение  $x \perp c$  означает  $\sum_{j=1}^k 2c_{i_j} = 0 \pmod{4}$  и эквивалентно чётности суммы всех  $c_{i_j}$ ,  $j = 1, \dots, k$ , что эквивалентно чётности суммы всех  $\beta(c_{i_j})$  и  $\gamma(c_{i_j})$ ,  $j = 1, \dots, k$ , что, в свою очередь, эквивалентно соотношениям  $\sum_{j=1}^k (\phi(c)_{i_j} \oplus \phi(c)_{n+i_j}) = 0 \pmod{2}$  и  $\phi(x) \perp \phi(c)$ . Утверждение 6 доказано.

**Утверждение 7.** При любых целых  $r_1 \geq 0, r_2 \geq 0$  размерность подпространства повторных слов из  $E^{2^{2r_1+r_2+1}}$ , ортогональных коду  $C^{r_1, r_2}$ , равна  $r_1 + r_2 + 1$ .

**Доказательство.** Пусть  $a_0, a_1, \dots, a_{r_1+r_2}$  — соответственно  $1, 2, \dots, (r_1 + r_2 + 1)$ -я строки матрицы  $A^{r_1, r_2}$ . Тогда слова  $2a_0, 2a_1, \dots, 2a_{r_1}, a_{r_1+1}, \dots, a_{r_1+r_2}$  состоят из нулей и двоек и по утверждению 6 повторные линейно независимые слова

$$\phi(2a_0), \phi(2a_1), \dots, \phi(2a_{r_1}), \phi(a_{r_1+1}), \dots, \phi(a_{r_1+r_2}) \quad (2)$$

ортогональны коду  $C^{r_1, r_2}$ .

С другой стороны, если  $y$  — повторное слово, ортогональное коду  $C^{r_1, r_2}$ , то  $\phi^{-1}(y) \in \{0, 2\}^{2^{2r_1+r_2}}$  ортогонально коду  $\mathcal{C}^{r_1, r_2}$ . Следовательно,  $\phi^{-1}(y)$  является линейной комбинацией строк матрицы  $A^{r_1, r_2}$ . Так как  $2\phi^{-1}(y)$  — нулевое слово, то коэффициенты при первых  $r_1 + 1$  строках в этой линейной комбинации чётны. Таким образом,  $\phi^{-1}(y)$  является линейной комбинацией слов  $2a_0, 2a_1, \dots, 2a_{r_1}, a_{r_1+1}, \dots, a_{r_1+r_2}$  и по утверждению 5 слово  $y$  является линейной комбинацией слов (2). Утверждение 7 доказано.

**Следствие 2.** При любых целых  $r_1 \geq 0, r_2 \geq 0$

$$\text{rank}(C^{r_1, r_2}) \leq n - r_1 - r_2 - 1,$$

где  $n = 2^{2r_1+r_2+1}$  — длина кода  $C^{r_1, r_2}$ .

**Утверждение 8.** При любом целом  $r_2 \geq 4$

$$\text{rank}(C^{0, r_2}) = 2^{r_2+1} - r_2 - 1 = n - \log_2 n,$$

где  $n = 2^{r_2+1}$  — длина кода  $C^{0, r_2}$ .

**Доказательство.** В [9] показано, что линейные расширенные совершенные коды Хемминга длины больше 16 не являются  $Z_4$ -линейными. Следовательно, при  $r_2 \geq 4$  код  $C^{0, r_2}$  нелинеен и его ранг больше  $n - \log_2 n - 1$ , т. е. размерности кода Хемминга. Но по следствию 2 ранг кода  $C^{0, r_2}$  не превосходит  $n - \log_2 n$ . Утверждение 8 доказано.

**Замечание 1.** Утверждение 8 можно доказать аналогично следствию 4, установив нелинейность кода  $C^{0, 4}$  и используя индукцию. Тогда «не- $Z_4$ -линейность» кодов Хемминга не будет использоваться в доказательствах и будет являться следствием нелинейности  $Z_4$ -линейных кодов  $C^{r_1, r_2}$ .

**Утверждение 9.** Ранг кода  $C^{1, 1}$  равен 13.

**Доказательство.** По следствию 2 ранг кода  $C^{1, 1}$  не превосходит 13. Укажем 13 линейно независимых векторов из  $C^{1, 1}$ :

$$\begin{aligned} b_1 &= \phi(2200\ 0000) = 1100\ 0000\ 1100\ 0000 \\ b_2 &= \phi(0000\ 2200) = 0000\ 1100\ 0000\ 1100 \\ b_3 &= \phi(2000\ 2000) = 1000\ 1000\ 1000\ 1000 \\ b_4 &= \phi(1100\ 1100) = 0000\ 0000\ 1100\ 1100 \\ b_5 &= \phi(0022\ 0000) = 0011\ 0000\ 0011\ 0000 \\ b_6 &= \phi(0000\ 0022) = 0000\ 0011\ 0000\ 0011 \\ b_7 &= \phi(0020\ 0020) = 0010\ 0010\ 0010\ 0010 \\ b_8 &= \phi(0011\ 0011) = 0000\ 0000\ 0011\ 0011 \\ b_9 &= \phi(0000\ 1313) = 0000\ 0101\ 0000\ 1010 \\ b_{10} &= \phi(0101\ 0303) = 0000\ 0101\ 0101\ 0000 \\ b_{11} &= \phi(0101\ 3030) = 0000\ 1010\ 0101\ 0000 \\ b_{12} &= \phi(1000\ 0111) = 0000\ 0000\ 1000\ 0111 \\ b_{13} &= \phi(0100\ 0102) = 0000\ 0001\ 0100\ 0101 \end{aligned}$$



Набор векторов  $b_1, \dots, b_{11}$  является базисом кода Хемминга с проверочной матрицей

$$B = \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 0000 & 0000 & 1111 & 1111 \\ 0000 & 1111 & 0000 & 1111 \\ 0011 & 0011 & 0011 & 0011 \\ 0101 & 0101 & 0101 & 0101 \end{bmatrix}.$$

Вектор  $b_{12}$  ортогонален всем строкам матрицы  $B$ , кроме третьей, и, следовательно, линейно независим от  $b_1, \dots, b_{11}$ . Вектор  $b_{13}$  не ортогонален второй строке матрицы  $B$ , следовательно, является линейно независимым от  $b_1, \dots, b_{12}$ . Утверждение 9 доказано.

**Следствие 3.** Все слова из  $E^{16}$ , ортогональные коду  $C^{1,1}$ , являются повторными.

**Доказательство.** В противном случае существует по крайней мере четыре линейно независимых слова, ортогональных коду  $C^{1,1}$ : три повторные (утверждение 7) и одно неповторное. Это означает, что ранг кода  $C^{1,1}$  не превосходит  $16 - 4 = 12$ , что противоречит утверждению 9. Следствие 3 доказано.

**Утверждение 10.** Пусть  $r_1 \geq 1$  и  $r_2 \geq 0$  — такие целые числа, что  $2r_1 + r_2 \geq 3$ . Тогда все слова из  $E^{2^{2r_1+r_2+1}}$ , ортогональные коду  $C^{r_1, r_2}$ , являются повторными.

**Доказательство** проведём индукцией по  $r = 2r_1 + r_2$ .

При  $r = 3$  утверждение верно по следствию 3.

Пусть утверждение верно при  $r = k - 1 \geq 3$ . Пусть  $2r_1 + r_2 = k$  и  $y \perp C^{r_1, r_2}$ . Тогда по утверждению 3 имеем  $\text{Even}(y) \perp \text{even}(C^{r_1, r_2})$  и  $\text{Odd}(y) \perp \text{odd}(C^{r_1, r_2})$ . Так как по следствию 1  $\text{odd}(C^{r_1, r_2}) = \text{even}(C^{r_1, r_2}) = C^{r_1, r_2-1}$  при  $r_2 > 0$  и  $\text{odd}(C^{r_1, r_2}) = \text{even}(C^{r_1, r_2}) = C^{r_1-1, r_2+1}$  при  $r_2 = 0$ , то по индукционному предположению слова  $\text{Even}(y)$  и  $\text{Odd}(y)$  повторные и по определению  $y$  также является повторным. Утверждение 10 доказано.

Из утверждений 10 и 7 вытекает

**Следствие 4.** Пусть  $r_1 \geq 1$ ,  $r_2 \geq 0$  — такие целые числа, что  $2r_1 + r_2 \geq 3$ . Тогда

$$\text{rank}(C^{r_1, r_2}) = 2^{2r_1+r_2} - r_1 - r_2 - 1.$$

**Теорема 2.** Если  $2r_1 + r_2 = 2r'_1 + r'_2 \geq 3$ , то коды  $C^{r_1, r_2}$  и  $C^{r'_1, r'_2}$  эквивалентны тогда и только тогда, когда  $r_1 = r'_1$ .

**Доказательство.** Если  $r = 2r_1 + r_2 = 2r'_1 + r'_2 \geq 4$ , то по утверждению 8 и следствию 4 коды  $C^{r_1, r_2}$  и  $C^{r'_1, r'_2}$  имеют ранги  $2^r - r + r_1 - 1$  и  $2^r - r + r'_1 - 1$  соответственно. В случае  $r_1 \neq r'_1$  ранги не равны и коды неэквивалентны.

При  $r = 3$  достаточно показать, что коды  $C^{0,3}$  и  $C^{1,1}$  неэквивалентны. Это следует из соотношений  $\text{rank}(C^{0,3}) \leq 12$  и  $\text{rank}(C^{1,1}) = 13$  (см. следствие 2 и утверждение 9). Теорема 2 доказана.

ЗАМЕЧАНИЕ 2. На самом деле код  $C^{0,3}$  линейный и его ранг равен 11.

#### § 4. Несуществование $(n, 4^n/4n, 4)_4$ -кодов, неэквивалентных построенным

Нам понадобятся следующие два вспомогательных утверждения.

**Утверждение 11.** Если  $C$  — расширенный совершенный двоичный код длины  $n$  с расстоянием 4 и  $x$  — двоичное слово, ортогональное коду  $C$ , то  $wt(x) = 0$ ,  $wt(x) = n/2$  или  $wt(x) = n$ .

Это утверждение эквивалентно тому факту, что совершенный двоичный код длины  $n$  с расстоянием 3 ортогонален только векторам веса  $(n+1)/2$  или 0 (доказательство последнего см., например, в [8]).

**Утверждение 12.** Если  $n$  — степень двойки и  $D$  — линейный двоичный код длины  $n$ , все ненулевые слова которого имеют вес  $n/2$ , то найдётся координата, в которой все слова кода  $D$  содержат 0.

Доказательство проведём по индукции. В случае  $n = 2$  утверждение очевидно (в качестве базы индукции можно взять также тривиальный случай  $n = 1$ ).

Пусть утверждение верно при  $n = m/2$ . Покажем, что оно верно при  $n = m$ . Не теряя общности, предположим, что в коде  $D$  имеется слово  $b = (0, 1, 0, 1, \dots, 0, 1)$  с нулями в чётных координатах и единицами в нечётных. Любое другое ненулевое слово  $b'$  из  $D$  содержит  $m/4$  единиц в чётных координатах и столько же в нечётных, поскольку  $wt(b \oplus b') = m/2$ . Следовательно, все ненулевые слова линейного кода  $D' = \{\text{Even}(d) \mid d \in D\}$  длины  $m/2$  имеют вес  $m/4$ . По индукционному предположению все слова из  $D'$  содержат нуль в некоторой  $i$ -й координате,  $0 \leq i \leq m/2 - 1$ . Поэтому все слова  $D$  содержат нуль в  $2i$ -й координате. Утверждение 12 доказано.

**Теорема 3.** Пусть множество  $\mathcal{C} \subset Z_4^n$  является  $(n, 4^n/4n, 4)_4$ -кодом и  $|\mathcal{C}| = 4^{n-r_0-r_2}2^{r_2}$ . Тогда  $r_0 > 0$  и код  $\mathcal{C}$  эквивалентен коду  $\mathcal{C}^{r_0-1, r_2}$ .

Доказательство. Поскольку  $4^n/4n = 4^{n-r_0-r_2}2^{r_2}$ , то

$$n = 2^{r_0+r_2-2}. \quad (3)$$

Пусть матрица  $A$  размера  $(r_0+r_2) \times n$  является проверочной для кода  $\mathcal{C}$ , а  $a^0, a^1, \dots, a^{r_0+r_2-1}$  — её строки, причём  $a^{r_0} \dots, a^{r_0+r_2-1} \in \{0, 2\}^n$ . Рассмотрим повторные слова  $b^i = \phi(2a^i)$ ,  $i = 0, \dots, r_0-1$ , ортогональные коду  $C$  по утверждению 6. Пусть  $D$  — линейная оболочка множества

слов  $\{b^i\}_{i=0}^{r_0-1}$ . По утверждению 11 линейный код  $D$  длины  $2n$  состоит из слов веса 0,  $n$  и  $2n$ . Пусть  $\bar{1} \in E^{2n}$  — слово веса  $2n$ , состоящее только из единиц. Покажем, что  $\bar{1} \in D$ .

Пусть, от противного,  $D$  содержит только слова веса  $n$  или 0. Тогда по утверждению 12 найдётся такое  $j$ ,  $0 \leq j \leq 2n-1$ , что  $d_j = 0$  для любого  $d = (d_0, \dots, d_{2n-1}) \in D$ . Так как все слова из  $D$  повторяющиеся, то для любого  $d \in D$  также выполнены равенства  $d_{j+n \pmod{2n}} = 0$ . Следовательно,  $\phi^{-1}(d)_{j'} = 0$ , где  $j' = j \pmod{n}$ . В частности,  $2a_{j'}^i = 0$  для любого  $i = 0, \dots, r_0 - 1$ . Отсюда следует, что матрица  $A$  содержит в  $j'$ -м столбце только нули и двойки, что, в свою очередь, означает, что код  $\mathcal{C}$  содержит слово веса 2 (с двойкой в  $j'$ -й координате и нулями в остальных). Последнее противоречит кодовому расстоянию 4 кода  $\mathcal{C}$ .

Таким образом,  $\bar{1} \in D$  и существуют такие коэффициенты  $\alpha_0, \dots, \alpha_{r_0-1} \in \{0, 1\}$ , что

$$\alpha_0 b^0 \oplus \dots \oplus \alpha_{r_0-1} b^{r_0-1} = \bar{1}. \quad (4)$$

Отсюда следует, что  $r_0 \geq 1$ . Не нарушая общности, будем считать, что  $\alpha_0 = 1$  (в противном случае можно поменять местами строки матрицы  $A$  так, чтобы при  $b_0$  в (4) был ненулевой коэффициент). Рассмотрим матрицу  $A'$ , полученную из  $A$  заменой первой строки  $a^0$  на строку

$$a'^0 = \alpha_0 a^0 + \dots + \alpha_{r_0-1} a^{r_0-1} \pmod{4}.$$

Поскольку  $\alpha_0 = 1$ , то  $a^0$  линейно выражается через  $a^0, a^1, \dots, a^{r_0-1}$ . Поэтому матрицы  $A$  и  $A'$  эквивалентны.

Из (4) следует, что

$$2a'^0 = \alpha_0 2a^0 + \dots + \alpha_{r_0-1} 2a^{r_0-1} = 2 \cdot \bar{1} \pmod{4},$$

т. е. слово  $a'^0$  — первая строка матрицы  $A'$  — состоит из единиц и троек. Пусть матрица  $A''$  получается из  $A'$  заменой элементов на противоположные в тех столбцах, в которых на первой позиции находится тройка.  $A''$  является проверочной матрицей для кватернарного кода  $\mathcal{C}''$ , эквивалентного коду  $\mathcal{C}$  (получающегося из  $\mathcal{C}$  заменой элементов на противоположные в соответствующих координатах). Кроме того, первая строка матрицы  $A''$  состоит из единиц, а последние  $r_2$  строк — из нулей и двоек. Если в  $A''$  есть два одинаковых столбца, скажем,  $j$ -й и  $j'$ -й, то  $C''$  содержит слово веса 2 с единицей в  $j$ -й координате, тройкой в  $j'$ -й и нулями в остальных координатах. Это противоречит кодовому расстоянию 4. Таким образом, все столбцы матрицы  $A''$  различны, а из соотношения (3) следует, что  $A''$  состоит из всевозможных столбцов высоты  $r_0 + r_2$ , у которых в первой позиции находится единица, в последних  $r_2$  позициях — нули или двойки, в оставшихся  $r_0 - 1$  позициях — произвольные числа из множества  $\{0, 1, 2, 3\}$ . Упорядочив столбцы лексикографически, получим матрицу  $A^{r_0-1, r_2}$ , а применив соответствующую

перестановку координат к коду  $\mathcal{C}''$ , получим код  $\mathcal{C}^{r_0-1, r_2}$ . Таким образом, код  $\mathcal{C}''$ , а значит, и код  $\mathcal{C}$  эквивалентны коду  $\mathcal{C}^{r_0-1, r_2}$ . Теорема 3 доказана.

**Теорема 4.** При  $n = 2^k \geq 16$  число попарно неэквивалентных  $Z_4$ -линейных расширенных совершенных кодов с расстоянием 4 равно  $\lfloor (\log_2 n + 1)/2 \rfloor$ .

**ДОКАЗАТЕЛЬСТВО.** Имеется  $\lfloor (\log_2 n + 1)/2 \rfloor$  способов представления числа  $n$  в виде  $n = 2^{2r_1+r_2+1}$ , где  $r_1 \geq 0$  и  $r_2 \geq 0$  — целые числа. Пусть  $\mathcal{C} = \{C^{r_1, \lfloor \log_2 n - 2r_1 - 1 \rfloor}_{r_1=0}^{\lfloor (\log_2 n - 1)/2 \rfloor}\}$  — множество кодов, попарно неэквивалентных по теореме 2. Любой  $Z_4$ -линейный  $(n, 2^n/2n, 4)$ -код эквивалентен одному из кодов множества  $\mathcal{C}$  по теореме 3. Теорема 4 доказана.

### § 5. Индуктивное построение кодов $\mathcal{C}^{r_1, r_2}$

Пусть  $n' = 4^{r'_1} 2^{r'_2}$  и  $n'' = 4^{r''_1} 2^{r''_2}$  являются целыми степенями двойки и

$$c = (c_{0,0}, c_{0,1}, \dots, c_{0,n''-1}, c_{1,0}, c_{1,1}, \dots, c_{n'-1, n''-1}) \in Z_4^{n' n''}.$$

Обозначим

$$p'(c) = \left( \sum_{j=0}^{n''} c_{0,j}, \sum_{j=0}^{n''} c_{1,j}, \dots, \sum_{j=0}^{n''} c_{n'-1,j} \right) \pmod{4},$$

$$p''(c) = \left( \sum_{i=0}^{n'} c_{i,0}, \sum_{i=0}^{n'} c_{i,1}, \dots, \sum_{i=0}^{n'} c_{i,n''-1} \right) \pmod{4}.$$

(Если  $c$  представить в виде матрицы размера  $n' \times n''$ , то  $p'$  есть сумма столбцов и  $p''$  есть сумма строк этой матрицы.)

Пусть  $\mathcal{C}'$  — кватернарный код с проверочной матрицей  $A'$ , перестановочно эквивалентный коду  $\mathcal{C}^{r'_1, r'_2}$ , и  $\mathcal{C}''$  — кватернарный код с проверочной матрицей  $A''$ , перестановочно эквивалентный коду  $\mathcal{C}^{r''_1, r''_2}$ . Пусть  $n = n' n''$ ,  $r_1 = r'_1 + r''_1$  и  $r_2 = r'_2 + r''_2$ . Тогда

**Теорема 5.** Множество

$$\mathcal{C} = \{c \in Z_4^{n' n''} \mid p'(c) \in \mathcal{C}', p''(c) \in \mathcal{C}''\} \quad (5)$$

является кватернарным  $(n, 4^n/4n, 4)_4$ -кодом, перестановочно эквивалентным коду  $\mathcal{C}^{r_1, r_2}$ .

Линейность кода  $\mathcal{C}$  над  $Z_4$  очевидна, кодовое расстояние и мощность показаны в [2] для более общей конструкции, а тип проверочной матрицы кода  $\mathcal{C}$  легко устанавливается, если расписать проверочные соотношения  $A'p'(c)^T = 0$  и  $A''p''(c)^T = 0$ .

С помощью конструкции (5) можно индуктивно получить все коды  $\{\mathcal{C}^{r_1, r_2}\}$ , взяв в качестве базы коды  $\mathcal{C}^{0,1}$  и  $\mathcal{C}^{1,0}$ .

## ЛИТЕРАТУРА

1. **Зиновьев В. А., Леонтьев В. К.** Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. Вып. 2. С. 123–132.
2. **Кротов Д. С.** О совершенном коде, содержащем в качестве подкодов заданный набор совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 1. С. 40–48.
3. **Кротов Д. С.** Нижние оценки числа  $m$ -квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 47–53.
4. **Кузьмин А. С., Нечаев А. А.** Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа // Успехи мат. наук. 1992. Т. 47, вып. 5. С. 183–184.
5. **Кузьмин А. С., Нечаев А. А.** Линейно представимые коды и код Кердока над произвольным полем Галуа характеристики 2 // Успехи мат. наук. 1994. Т. 49, вып. 5. С. 165–166.
6. **Нечаев А. А.** Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1, вып. 4. С. 123–139.
7. **Cohen G. D., Honkala I., Litsyn S., Lobstein A.** Covering codes. Amsterdam: North-Holland Publ. Co., 1997.
8. **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40. N 3. P. 754–763.
9. **Hammons A. R., Jr, Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.** The  $Z_4$ -linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. V. 40, N 2. P. 301–319.
10. **Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.** Linear recurring sequences over rings and modules // J. of Math. Sci. 1995. V. 76, N 6. P. 2793–2915.
11. **Solov'eva F. I.** Constructions of perfect binary codes // Preprint 98–042. Univ. Bielefeld, 1998. 12 p.
12. **Tietavainen A.** On the nonexistence of perfect codes over finite fields // SIAM J. Appl. Math. 1973. V. 24, N 1. P. 88–96.

Адрес автора:

Институт математики  
им. С. Л. Соболева СО РАН,  
пр. Академика Коптюга, 4,  
630090 Новосибирск, Россия.  
E-mail: dkrotov@mail.ru

Статья поступила  
3 июля 2000 г.