ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 41 2005 Вып. 2

УДК 621.391.15

 Н.Н. Токарева

ПРЕДСТАВЛЕНИЕ $\mathbb{Z}_4$-ЛИНЕЙНЫХ КОДОВ ПРЕПАРАТЫ С ПОМОЩЬЮ ВЕКТОРНЫХ ПОЛЕЙ[1]

Двоичный код называется $\mathbb{Z}_4$-линейным, если его четверичный прообраз относительно отображения Грея линеен. Показано, что множество всех четверичных линейных кодов Препараты длины $n = 2^m$, где m нечетно, $m \geq 3$, исчерпывается кодами вида $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ для

$$\mathcal{H}_{\lambda,\psi} = \{\, y + T_\lambda(y) + S_\psi(y) \,|\, y \in H^n\}, \quad \mathcal{M} = 2H^n,$$

где $T_\lambda(\cdot)$, $S_\psi(\cdot)$ – векторные поля специального вида, определенные на двоичном расширенном линейном коде Хэмминга H^n длины n. Получена верхняя оценка числа неэквивалентных четверичных линейных кодов Препараты длины n, равная $2^{n\log_2 n}$. Предложено представление для двоичных кодов Препараты, содержащихся в совершенных кодах Васильева.

§ 1. Введение

Все известные к настоящему времени коды Препарата содержатся в совершенных кодах, относящихся к классу кодов Васильева [1]. Действительно, оригинальный код Препарата [2] и серия кодов [3, 4] разбивают на смежные классы линейный код Хэмминга, который принадлежит классу кодов Васильева. Любой $\mathbb{Z}_4$-линейный расширенный код Препарата [5, 6] также является подкодом специального $\mathbb{Z}_4$-линейного расширенного кода Васильева (см. предложение 8). Структура совершенных кодов Васильева и строение их минимальных i-компонент хорошо известны. Используя связь между i-компонентами кодов Препараты и совершенных кодов [7], можно получить общее представление для кодов Препараты, содержащихся в кодах Васильева (см. теорему 1).

Отдельно рассмотрены $\mathbb{Z}_4$-линейные коды Препарата. Для их исследования удобно перейти к четверичным прообразам этих кодов относительно отображения Грея. В статье показано, что совокупность четверичных линейных кодов Препараты длины $n = 2^m$, где m нечетно, $m \geq 3$, исчерпывается кодами вида $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ для

$$\mathcal{H}_{\lambda,\psi} = \{\, y + T_\lambda(y) + S_\psi(y) \,|\, y \in H^n\}, \quad \mathcal{M} = 2H^n,$$

где $T_\lambda(\cdot)$, $S_\psi(\cdot)$ – векторные поля специального вида, определенные на двоичном расширенном линейном коде Хэмминга H^n длины n (см. теоремы 2, 3). Использование векторных полей удобно для описания различных комбинаторных объектов (см. [8]). В частности, представление в терминах векторных полей предлагалось и для некоторых кодов Препараты (см. [9]). В работе [10] установлена связь между

[1] Работа выполнена при финансовой поддержке программы Рособразования "Развитие научного потенциала высшей школы" (номер проекта 512).

диаметрально совершенными троичными кодами и кодами Препараты; конструкция, предложенная в [10], в которой используются векторные поля, имеет сходство с предлагаемой в данной статье.

В §§2, 3 приводятся необходимые определения и утверждения для двоичных и четверичных кодов. В §4 исследуются двоичные коды Препарата, содержащиеся в кодах Васильева; §5 посвящен представлению четверичных линейных кодов Препараты с помощью векторных полей; в §6 предложен пример такого представления для одного известного кода Препараты.

§ 2. Двоичные и четверичные коды

Рассмотрим поле $\mathbb{Z}_2$ целых чисел по модулю 2 и кольцо $\mathbb{Z}_4$ целых чисел по модулю 4. Множество $\mathbb{Z}_2^n$ состоит из всех *двоичных* векторов длины n, т.е.

$$\mathbb{Z}_2^n = \{ (x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}_2, i = 1, \ldots, n\},$$

и является n-мерным векторным пространством над полем $\mathbb{Z}_2$. Пусть операция $\oplus$ означает сложение двоичных векторов. Множество $\mathbb{Z}_4^n$ состоит из всех *четверичных* векторов длины n, т.е.

$$\mathbb{Z}_4^n = \{ (x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}_4, i = 1, \ldots, n\},$$

и является модулем с операцией сложения $+$ над кольцом $\mathbb{Z}_4$.

Вес Хэмминга $w_H(\cdot)$ произвольного двоичного вектора равен числу его ненулевых координат. *Расстояние Хэмминга* $d_H(\cdot,\cdot)$ между двумя двоичными векторами равно числу позиций, в которых они различаются. *Весом Ли* $w_L(\cdot)$ четверичного вектора называется сумма весов его координат, которые определяются соотношениями $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, $w_L(2) = 2$. *Расстояние Ли* $d_L(\cdot,\cdot)$ между четверичными векторами x, y задается равенством $d_L(x,y) = w_L(x-y)$.

Множества $\mathbb{Z}_2^n$ и $\mathbb{Z}_4^n$ являются метрическими пространствами относительно метрик Хэмминга и Ли соответственно. Элементы этих пространств будем называть векторами или вершинами. Заметим, что любой двоичный вектор может рассматриваться как четверичный. Конкатенация двоичных или четверичных векторов x, y обозначается через (x, y).

Двоичным кодом длины n называется любое подмножество метрического пространства $\langle \mathbb{Z}_2^n, d_H\rangle$. *Четверичным кодом длины* n называется произвольное подмножество метрического пространства $\langle \mathbb{Z}_4^n, d_L\rangle$. Далее используем обозначения, принятые в [5]. Двоичные коды будем обозначать прописными буквами C, P, H, R, M и т.д., четверичные коды – рукописными прописными буквами $\mathcal{C}$, $\mathcal{P}$, $\mathcal{H}$, $\mathcal{R}$, $\mathcal{M}$ и т.д.

Кодовыми параметрами (n, M, d) двоичного, или четверичного, кода являются *длина* кода n, его *мощность* M и минимальное *расстояние* d (в соответствующей метрике) между различными кодовыми словами. Код, содержащий нулевой вектор $\mathbf{0}$, называется *приведенным.*

Стандартные отображения β, γ из $\mathbb{Z}_4$ в $\mathbb{Z}_2$ определяются следующим образом:

$\mathbb{Z}_4$	β	γ
0	0	0
1	0	1
2	1	1
3	1	0

и покоординатно продолжаются до отображений $\mathbb{Z}_4^n \to \mathbb{Z}_2^n$. *Отображение Грея* $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ задается равенством

$$\phi(x) = (\beta(x), \gamma(x)) \text{ для любого } x \in \mathbb{Z}_4^n.$$

Известно (см. [5]), что ϕ является изометрией метрических пространств $\langle \mathbb{Z}_4^n, d_L\rangle$ и $\langle \mathbb{Z}_2^{2n}, d_H\rangle$.

Множество координат $\{1, 2, \dots, n\}$ обозначим через I. Для двоичных векторов x, y длины n вектор $x * y$ равен $(x_1y_1, \dots, x_ny_n)$. Вектор x *предшествует* вектору y (обозначается $x \prec y$), если $x \neq y$ и $x_i \leq y_i$ для всех $i \in I$, где $\leq$ является обычным порядком на $\mathbb{Z}_2$. Через $|x|$ обозначается сумма $x_1 \oplus \ldots \oplus x_n$. Для четверичных векторов x, y определим $x \prec y$, если $\phi(x) \prec \phi(y)$.

Рассмотрим группу S_n перестановок порядка n и группу J_n инверсий на n координатах (под *инверсией* четверичного вектора понимаем замену в некоторых его координатах элементов кольца $\mathbb{Z}_4$ на обратные к ним, т.е. 0 на 0, 1 на 3, 2 на 2, 3 на 1). Заметим, что группы J_n и $\mathbb{Z}_2^n$ изоморфны. Два двоичных кода C и C' длины n называются *эквивалентными*, если существуют вектор $x \in \mathbb{Z}_2^n$ и перестановка $\pi \in S_n$, такие что $C = \pi(C') \oplus x$. Два четверичных кода C и C' длины n *эквивалентны*, если существуют вектор $x \in \mathbb{Z}_4^n$, перестановка $\pi \in S_n$ и инверсия $\tau \in J_n$, такие что $C = \pi(\tau(C')) + x$. Двоичный (четверичный) код длины n называется *линейным*, если он образует подгруппу аддитивной группы поля $\mathbb{Z}_2^n$ (кольца $\mathbb{Z}_4^n$). Двоичный код называется $\mathbb{Z}_4$*-линейным*, если существует эквивалентный ему код C, такой что его прообраз $\phi^{-1}(C)$ линеен.

§ 3. Вспомогательные определения и утверждения

3.1. Понятие $\{i, j\}$-компоненты. Приведем несколько определений для расширенных двоичных кодов (в работах [11, 12] аналогичные определения были введены для кодов с нечетными расстояниями).

Через e_i обозначается вектор длины n, имеющий единицу в i-й координате и нули в остальных. Подмножество M двоичного кода C называется $\{i, j\}$*-компонентой* кода для некоторых различных координат i и j, если коды C и $C' = (C \setminus M) \cup$ $\cup (M \oplus e_i \oplus e_j)$ имеют одинаковые кодовые параметры. Пусть два вектора некоторого двоичного кода находятся на минимальном кодовом расстоянии и различаются в координатах i и j. Такие кодовые векторы называются $\{i, j\}$*-близкими*. Любое множество кодовых слов, замкнутое относительно включения $\{i, j\}$-близких вершин, является $\{i, j\}$-компонентой. Рассмотрим граф на множестве вершин кода, ребрами в котором соединены $\{i, j\}$-близкие вершины. Каждая его компонента связности однозначно соответствует некоторой минимальной (т.е. неразложимой на меньшие) $\{i, j\}$-компоненте кода и называется *характеристическим графом* этой $\{i, j\}$-компоненты. Характеристический граф G^R компоненты R является метрическим пространством с естественной метрикой: расстояние $d_G(\cdot, \cdot)$ между вершинами равно длине кратчайшего пути между ними.

3.2. Совершенные коды и коды Препарата. Подмножество некоторого метрического пространства называется *совершенным кодом с расстоянием* 3 (кратко *совершенным*), если расстояние между любыми двумя его элементами не меньше 3 и шары радиуса 1 с центрами в кодовых вершинах, не пересекаясь, покрывают все пространство. Хорошо известно, что двоичные совершенные коды существуют только для длин $n = 2^m - 1$, $m \geq 2$, и имеют мощность $M = 2^n/(n + 1)$. Среди них только один код с точностью до эквивалентности обладает свойством линейности – *код Хэмминга.* Максимальный по мощности двоичный код с расстоянием 5 длины $n = 2^{m+1} - 1$, m нечетно, $m \geq 3$, называется *кодом Препараты*, его мощность M равна $2^{n+1}/(n + 1)^2$. Для расширенного двоичного совершенного кода C его прообраз $\phi^{-1}(C)$ относительно отображения Грея будем называть *четверичным совершенным* кодом (опуская термин расширенный). Прообраз $\phi^{-1}(P)$ расширенного двоичного кода Препараты P будем называть *четверичным кодом Препараты.* Исходя из определений, четверичный совершенный код имеет парамет-

ры ($n = 2^m, M = 4^n/4n, d = 4$) для любого целого $m \geq 1$, а четверичный код Препарата – ($n = 2^m, M = 4^n/4n^2, d = 6$) для нечетного целого $m \geq 3$. Справедливо

Предложение 1 (см. [13]). *Любой код Препарата содержится в некотором совершенном коде и притом единственном.*

Для кода Препараты P соответствующий ему совершенный код обозначим через $C(P)$ и будем называть его в дальнейшем *базовым.* Далее потребуется

Предложение 2 (см. [14]). *Для произвольного двоичного кода Препараты P длины n каждая вершина кода $C(P) \setminus P$ находится на расстоянии 3 в точности от $n/3$ вершин кода P.*

Отметим, что множество векторов веса 4 расширенного двоичного совершенного кода C длины n образует *систему четверок Штейнера* порядка n (см. [14]). Обозначим это множество через $SQS(C)$.

Предложение 3 (см. [15, лемма Глаголева]). *Базис расширенного кода Хэмминга H^n длины n может быть выбран среди векторов $SQS(H^n)$.*

§ 4. Коды Препарата, содержащиеся в кодах Васильева

В этом параграфе изучаются общие свойства кодов Препараты с базовым совершенным кодом Васильева. Речь пойдет только о двоичных кодах.

Приведем конструкцию широко известных расширенных совершенных кодов Васильева [1], используя их представление, предложенное в [16]. Пусть $n = 2^m$, $m \geq 2$; пусть i – фиксированная координата из I. Множество E_0^n состоит из всех двоичных векторов длины n четного веса. Пусть дан произвольный расширенный приведенный совершенный код C^n длины n и некоторая функция $\lambda : C^n \to \{0, 1\}$, причем $\lambda(\mathbf{0}) = 0$. Рассмотрим множества

$$R = \{\, (x, x) \mid x \in E_0^n\},$$
$$C_\lambda = \{\, (\lambda(y)e_i, \lambda(y)e_i \oplus y) \mid y \in C^n\}.$$

Если в качестве кода C^n выбран расширенный линейный код Хэмминга H^n, то множество C_λ обозначим через H_λ. Множество

$$V_C^\lambda = C_\lambda \oplus R$$

является расширенным совершенным *кодом Васильева* длины $2n$ (см. [16]). Обозначим через R^y смежный класс множества R, соответствующий вектору y из C^n, т.е.

$$R^y = R \oplus v^y, \text{ где } v^y = (\lambda(y)e_i, \lambda(y)e_i \oplus y).$$

Легко заметить, что множество $R^\mathbf{0}$ совпадает с R. Непосредственно из определения кода V_C^λ следует, что каждое множество R^y составляет его минимальную $\{i, n+i\}$-компоненту.

Предложение 4. *Для любого вектора y из C^n метрические пространства $\langle G^{R^y}, d_G\rangle$ и $\langle \mathbb{Z}_2^{n-1}, d_H\rangle$ изометричны.*

Доказательство. Достаточно показать изометричность пространств $\langle G^R, d_G\rangle$ и $\langle \mathbb{Z}_2^{n-1}, d_H\rangle$. Зададим отображение $f : R \to \mathbb{Z}_2^{n-1}$ следующим образом: для вектора $x \in E_0^n$ положим $f((x, x)) = \widehat{x}$, где $\widehat{x}$ – проекция вектора x по i-й координате. Нетрудно проверить, что f взаимно-однозначно. Покажем, что это отображение сохраняет расстояние 1. Пусть для векторов $x^1, x^2 \in E_0^n$ выполнено равенство $d_G((x^1, x^1), (x^2, x^2)) = 1$, тогда векторы (x^1, x^1) и (x^2, x^2) являются $\{i, n+i\}$-близкими, т.е. различаются в позициях $i, n+i$, и расстояние $d_H((x^1, x^1), (x^2, x^2))$ равно 4. Отсюда имеем $d_H(x^1, x^2) = 2$, и следовательно, $d_H(\widehat{x}^1, \widehat{x}^2) = 1$. Изометрии $f_y : R^y \to \mathbb{Z}_2^{n-1}$ определяются аналогично: $f_y((x, x) \oplus v^y) = \widehat{x}$. ▲

В работе [7] было доказано следующее утверждение, которое сформулируем в терминах расширенных кодов.

Предложение 5. *Пусть P – произвольный расширенный код Препарата. Тогда для любой $\{i,j\}$-компоненты R базового расширенного совершенного кода $C(P)$ множество $P \cap R$ является совершенным кодом с расстоянием 3 в метрическом пространстве $\langle G^R, d_G \rangle$.*

Справедлива

Теорема 1. *Произвольный двоичный расширенный код Препарата P, содержащийся в расширенном совершенном коде Васильева*

$$V_C^\lambda = \{\, (x \oplus \lambda(y)e_i, x \oplus y \oplus \lambda(y)e_i) \,|\, x \in E_0^n, y \in C^n \},$$

однозначно представляется в виде

$$P = \{\, (x \oplus \lambda(y)e_i, x \oplus y \oplus \lambda(y)e_i) \,|\, x \in C_y^n, y \in C^n \},$$

где для каждого $y \in C^n$ специальным образом выбирается расширенный совершенный код C_y^n длины $n = 2^m$, m нечетно, $m \geq 3$.

Доказательство. Пусть код P содержится в коде V_C^λ. Для любого вектора $y \in C^n$ обозначим через M^y множество $P \cap R^y$. Поскольку код V_C^λ разбивается на непересекающиеся $\{i, n+i\}$-компоненты R^y, имеем

$$P = P \cap V_C^\lambda = P \cap \left(\bigcup_{y \in C^n} R^y \right) = \bigcup_{y \in C^n} (P \cap R^y) = \bigcup_{y \in C^n} M^y.$$

Согласно предложению 5 множество M^y образует совершенный код в пространстве $\langle G^{R^y}, d_G \rangle$. Пусть $f_y : R^y \to \mathbb{Z}_2^{n-1}$ – изометрия, определенная в предложении 4. Тогда множество $f_y(M^y)$ является совершенным кодом в пространстве $\langle \mathbb{Z}_2^{n-1}, d_H \rangle$. Через C_y^n обозначим расширенный совершенный код длины n, выкалывание i-й координаты в котором приводит к коду $f_y(M^y)$. Тогда очевидно равенство

$$M^y = v^y \oplus \{\, (x, x) \,|\, x \in C_y^n \},$$

подставив в которое вектор

$$v^y = (\lambda(y)e_i, \lambda(y)e_i \oplus y),$$

получим искомое представление кода P. ▲

Все известные в настоящий момент коды Препарата содержатся в совершенных кодах Васильева, и следовательно, могут быть представлены с помощью конструкции теоремы 1. Например, для функции $\lambda(\cdot) \equiv 0$ и $C^n = H^n$ код Васильева V_H^λ является линейным расширенным кодом Хэмминга. Он содержит серию кодов Препараты [3, 4]. В §5 будет показано, что произвольный $\mathbb{Z}_4$-линейный расширенный код Препарата содержится в единственном с точностью до эквивалентности коде Васильева со специальной функцией λ. Кодами C^n, C_y^n в терминах теоремы 1 для него являются смежные классы расширенного линейного кода Хэмминга H^n. За выбор смежных классов отвечает некоторая функция ψ. Далее как частный случай теоремы 1 будет приведено представление для $\mathbb{Z}_4$-линейных расширенных кодов Препараты и установлено взаимно-однозначное соответствие между всеми такими кодами и специальными *функциями сдвига* φ, определенными на блоках $SQS(H^n)$. Будет показано, что построение функции сдвига эквивалентно построению $\mathbb{Z}_4$-линейного расширенного кода Препараты.

§ 5. Линейные четверичные коды Препарата

5.1. Базовый совершенный код. Рассмотрим произвольный линейный четверичный код Препарата $\mathcal{P}$ длины $n = 2^m$, m нечетно, $m \geq 3$, и его базовый четверичный совершенный код $\mathcal{C}(\mathcal{P})$. Напомним, что *рангом* множества двоичных векторов называется размерность натянутого на него линейного подпространства. Рангом множества четверичных векторов назовем ранг его образа относительно отображения Грея.

Предложение 6 (см. [17]). *Справедливы следующие утверждения:*

i. *Ранг любого кода Препараты равен рангу содержащего его совершенного кода;*

ii. *Ранг любого четверичного линейного кода Препараты длины $n = 2^m$ равен $2^{m+1} - m - 1$ при $m > 3$ и 11 при $m = 3$;*

iii. *Для произвольного четверичного линейного кода Препараты $\mathcal{P}$ его базовый четверичный код $\mathcal{C}(\mathcal{P})$ также линеен.*

Предложение 7 (см. [18, 19]). *Число попарно неэквивалентных четверичных линейных совершенных кодов длины $n = 2^m$, $m \geq 3$, равно $\lfloor m/2 \rfloor + 1$. Все эти коды имеют различный ранг.*

Пусть выбраны некоторый расширенный двоичный линейный код Хэмминга H^n и координата $i \in I$. Для записи конструкции четверичного кода Васильева удобно функции $\lambda : H^n \to \{0, 1\}$ сопоставить четверичное векторное поле на коде H^n

$$T_\lambda : H^n \to \{\, \mathbf{0}, 2e_i \,\}$$

по правилу

$$T_\lambda(y) = 2\lambda(y)e_i \text{ для } y \in H^n.$$

Четверичные множества

$$\mathcal{R} = 2E_0^n, \quad \mathcal{H}_\lambda = \{\, y + T_\lambda(y) \mid y \in H^n \}$$

являются прообразами относительно отображения Грея двоичных множеств R и H_λ.

Следующий результат принадлежит Д.С. Кротову.

Предложение 8 ([20]). *Любой четверичный линейный код Препарата содержится в четверичном совершенном коде, эквивалентном коду $\mathcal{V}_\mathcal{H}^\lambda = \mathcal{H}_\lambda + \mathcal{R}$ с функцией λ вида*

$$\lambda(y) = \begin{cases} 0, & \text{если } w_H(y) \equiv 0 \,(\mathrm{mod}\, 4), \\ 1, & \text{если } w_H(y) \equiv 2 \,(\mathrm{mod}\, 4) \ \text{ для } y \in H^n. \end{cases}$$

Доказательство. Из предложения 6 следует, что код $\mathcal{C}(\mathcal{P})$ линеен и имеет ранг $2^{m+1} - m - 1$ при $m > 3$ и 11 при $m = 3$. Согласно предложению 7 такой код единствен с точностью до эквивалентности. Покажем, что этим кодом является $\mathcal{V}_\mathcal{H}^\lambda$ с указанной функцией λ. Из определения отображения ϕ очевидно следует равенство

$$\phi(x + 2y) = \phi(x) \oplus \phi(2y) \ \text{ для любых } x, y \in \mathbb{Z}_4^n. \tag{1}$$

Тогда имеем

$$\mathcal{V}_\mathcal{H}^\lambda = \phi^{-1}(H_\lambda) + \phi^{-1}(R) = \phi^{-1}(H_\lambda \oplus R) = \phi^{-1}(V_H^\lambda),$$

т.е. код $\mathcal{V}_\mathcal{H}^\lambda$ – прообраз относительно отображения Грея расширенного двоичного совершенного кода Васильева. Несложно проверить, что его ранг равен $2^{m+1} - m - 1$ при $m > 3$ и 11 при $m = 3$ (подробнее см. [21, 22]). Покажем, что сумма $v^1 + v^2$ двух

любых векторов v^1, v^2 совершенного кода $\mathcal{V}_{\mathcal{H}}^{\lambda}$ также принадлежит коду. Пусть

$$v^k = y^k + T_\lambda(y^k) + 2x^k, \text{ где } x^k \in E_0^n,\ y^k \in H^n,\ k = 1, 2.$$

Используем равенства

$$y^1 + y^2 = (y^1 \oplus y^2) + 2y^1 * y^2, \tag{2}$$
$$\lambda(y^1 \oplus y^2) = \lambda(y^1) \oplus \lambda(y^2) \oplus |y^1 * y^2|, \tag{3}$$

первое из которых очевидно, а второе несложно получить из тождеств

$$w_H(y^1 \oplus y^2) = w_H(y^1) + w_H(y^2) - 2w_H(y^1 * y^2),$$
$$w_H(y) \equiv 2\lambda(y) (\mathrm{mod}\, 4) \text{ для любого } y \text{ из } H^n.$$

Тогда выполнено

$$v^1 + v^2 = (y^1 \oplus y^2) + T_\lambda(y^1) + T_\lambda(y^2) + 2(y^1 * y^2 \oplus x^1 \oplus x^2) =$$
$$= (y^1 \oplus y^2) + T_\lambda(y^1 \oplus y^2) + 2(y^1 * y^2 \oplus x^1 \oplus x^2 \oplus |y^1 * y^2|\, e_i).$$

откуда следует равенство $v^1 + v^2 = y + T_\lambda(y) + 2x$ для некоторых $x \in E_0^n$, $y \in H^n$. Следовательно, вектор $v^1 + v^2$ принадлежит коду $\mathcal{V}_{\mathcal{H}}^{\lambda}$. Таким образом, линейность, кодовые параметры и соответствующий ранг кода $\mathcal{V}_{\mathcal{H}}^{\lambda}$ показаны. ▲

Всюду далее $\lambda(\cdot)$ будет функцией, определенной в предложении 8. Без ограничения общности можно считать, что код $\mathcal{P}$ содержится непосредственно в четверичном коде Васильева $\mathcal{V}_{\mathcal{H}}^{\lambda}$.

5.2. Представление четверичных линейных кодов Препараты. Прообраз относительно отображения Грея четверичного линейного кода Препараты имеет представление из теоремы 1. Кодом C^n является код H^n. В качестве кодов C_y^n выберем с помощью функции $\psi : H^n \to I$ смежные классы кода H^n. Удобно функции ψ сопоставить четверичное векторное поле на коде H^n

$$S_\psi : H^n \to \{\, 2e_i + 2e_1, \dots, 2e_i + 2e_n \,\}$$

по правилу

$$S_\psi(y) = 2e_i + 2e_{\psi(y)} \text{ при } y \in H^n.$$

Заметим, что вектор $S_\psi(y)$ содержится в $\mathcal{R}$. Рассмотрим четверичные множества

$$\mathcal{M} = 2H^n, \quad \mathcal{H}_{\lambda,\psi} = \{\, y + T_\lambda(y) + S_\psi(y) \mid y \in H^n \}.$$

Теорема 2. *Произвольный четверичный линейный код Препарата однозначно представим в виде $\mathcal{P} = \mathcal{H}_{\lambda,\psi} + \mathcal{M}$ для некоторых расширенного линейного кода Хэмминга H^n и функции $\psi : H^n \to I$.*

Доказательство. Из предложения 8 следует, что любой код $\mathcal{P}$ содержится в коде

$$\mathcal{V}_{\mathcal{H}}^{\lambda} = \bigcup_{y \in H^n} (y + T_\lambda(y) + \mathcal{R}),$$

поэтому

$$\mathcal{P} = \bigcup_{y \in H^n} (\mathcal{P} \cap (y + T_\lambda(y) + \mathcal{R})).$$

Покажем, что для каждого y из H^n можно однозначно определить $S_\psi(y)$ как вектор наименьшего веса, такой что $y + T_\lambda(y) + S_\psi(y)$ принадлежит коду $\mathcal{P}$. Для этого

зададим функцию ψ следующим образом. Если вектор $y + T_\lambda(y)$ содержится в $\mathcal{P}$, положим $\psi(y) = i$, тогда $S_\psi(y) = \mathbf{0}$. Пусть $y+T_\lambda(y)$ содержится в $\mathcal{C}(\mathcal{P}) \setminus \mathcal{P}$. Из предложения 2 следует, что найдется единственный двоичный вектор v длины $2n$ веса 4 с ненулевыми координатами $i, n+i$, такой что вектор $\phi(y + T_\lambda(y)) \oplus v$ принадлежит коду $\phi(\mathcal{P})$. Прообраз $\phi^{-1}(v)$ содержит двойку в i-й координате. В силу изометричности отображения Грея его вес равен 4. Из определения кода $\mathcal{V}_{\mathcal{H}}^{\lambda}$ следует, что вектор $\phi^{-1}(v)$ имеет вид $2e_i + 2e_j$ для некоторой координаты j, отличной от i. Положим $\psi(y) = j$, тогда $S_\psi(y) = \phi^{-1}(v)$. Используя (1), получаем равенство

$$\phi(y + T_\lambda(y)) \oplus \phi(S_\psi(y)) = \phi(y + T_\lambda(y) + S_\psi(y)),$$

и следовательно, вектор $y+T_\lambda(y)+S_\psi(y)$ содержится в коде $\mathcal{P}$ для любого y из H^n.

Поскольку векторы $y + T_\lambda(y) + S_\psi(y)$ и $S_\psi(y)$ принадлежат линейным кодам $\mathcal{P}$ и $\mathcal{R}$ соответственно, для y из H^n имеем

$$\begin{aligned}
&\mathcal{P} \cap (y + T_\lambda(y) + \mathcal{R}) = \\
&= (y + T_\lambda(y) + S_\psi(y) + \mathcal{P}) \cap (y + T_\lambda(y) + S_\psi(y) + S_\psi(y) + \mathcal{R}) = \\
&= y + T_\lambda(y) + S_\psi(y) + (\mathcal{P} \cap (S_\psi(y) + \mathcal{R})) = \\
&= y + T_\lambda(y) + S_\psi(y) + (\mathcal{P} \cap \mathcal{R}).
\end{aligned}$$

Тогда справедливо

$$\mathcal{P} = \bigcup_{y \in H^n} (y + T_\lambda(y) + S_\psi(y) + (\mathcal{P} \cap \mathcal{R})).$$

Осталось показать, что множества $\mathcal{P} \cap \mathcal{R}$ и $\mathcal{M}$ совпадают. Действительно, из теоремы 1 следует, что их мощности равны, а из очевидных включений $\mathcal{M} \subset \mathcal{R}$ и $\mathcal{M} = 2\mathcal{P} \subset \mathcal{P}$ следует включение $\mathcal{M} \subseteq \mathcal{P} \cap \mathcal{R}$. ▲

Предложение 9. *Четверичный код $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ линеен тогда и только тогда, когда для любых y^1, y^2 из H^n функция ψ удовлетворяет условию*

$$S_\psi(y^1) + S_\psi(y^2) + S_\psi(y^1 \oplus y^2) + 2\,y^1 * y^2 + 2\,|y^1 * y^2|\, e_i \in \mathcal{M}. \tag{4}$$

Доказательство. Рассмотрим два произвольных кодовых вектора

$$v^k = y^k + T_\lambda(y^k) + S_\psi(y^k) + 2x^k, \text{ где } x^k, y^k \in H^n,\ k = 1, 2.$$

Определим, когда их сумма v^1+v^2 принадлежит коду. Используя равенства (2) и (3), получаем

$$\begin{aligned}
&v^1+v^2 = (y^1 \oplus y^2) + T_\lambda(y^1) + T_\lambda(y^2) + S_\psi(y^1) + S_\psi(y^2) + (2\,y^1 * y^2 + 2x^1 + 2x^2) = \\
&= (y^1 \oplus y^2) + T_\lambda(y^1 \oplus y^2) + S_\psi(y^1 \oplus y^2) + (S_\psi(y^1) + S_\psi(y^2) + S_\psi(y^1 \oplus y^2) + \\
&+ 2\,y^1 * y^2 + 2\,|y^1 * y^2|\, e_i + 2x^1 + 2x^2).
\end{aligned}$$

Отсюда вектор v^1+v^2 является кодовым только в том случае, когда вектор $S_\psi(y^1) + S_\psi(y^2) + S_\psi(y^1 \oplus y^2) + 2\,y^1 * y^2 + 2\,|y^1 * y^2|\, e_i$ принадлежит множеству $\mathcal{M}$. ▲

Заметим, что не всякий четверичный линейный код $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ является кодом Препараты.

Предложение 10. *Четверичный линейный код $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ является кодом Препараты тогда и только тогда, когда для любых $y^1, y^2 \in SQS(H^n)$, таких что*

$y^1 \oplus y^2 \in SQS(H^n)$, *функция* ψ *удовлетворяет условиям:*

$$\begin{aligned} &1. \quad S_\psi(y^1) \neq \mathbf{0}; \\ &2. \quad S_\psi(y^1) \not\prec 2y^1; \\ &3. \quad S_\psi(y^1 \oplus y^2) \neq 2y^1 * y^2. \end{aligned} \tag{5}$$

Доказательство. Проверим, что перечисленные условия являются необходимыми и достаточными для того, чтобы кодовое расстояние кода $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ было равным 6.

Необходимость проверяется непосредственно. Вес любого кодового вектора

$$v = y + T_\lambda(y) + S_\psi(y) + 2x, \text{ где } x \in H^n,\, y \in SQS(H^n),$$

не меньше 6. Заметим, что согласно определению векторного поля T_λ выполнено $T_\lambda(y) = \mathbf{0}$. Тогда, если $S_\psi(y) = \mathbf{0}$ или $S_\psi(y) \prec 2y$, то при $x = \mathbf{0}$ имеем $w_L(v) = 4$, противоречие. Если выполняется $S_\psi(y) = 2y^1 * y^2$ для некоторых $y^1, y^2 \in SQS(H^n)$, таких что $y = y^1 \oplus y^2$, то при $x = y^1$ также получаем $w_L(v) = 4$.

Проверим достаточность условий 1–3. Поскольку код $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ линеен, достаточно показать, что минимальный ненулевой вес его кодовых векторов равен 6. Произвольный кодовый вектор

$$v = y + T_\lambda(y) + S_\psi(y) + 2x, \text{ где } x, y \in H^n,$$

имеет четный вес. Справедливо неравенство

$$w_L(v) \geq w_L(y).$$

Поэтому далее ограничимся случаями $w_L(y) = 0$ и $w_L(y) = 4$, в каждом из которых выполнено $T_\lambda(y) = \mathbf{0}$. Несложно проверить, что справедливо неравенство

$$w_L(v) \geq w_L(x).$$

Действительно, если $w_L(y) = 0$, или $w_L(y) = 4$ и $x = y$, то неравенство очевидно. Если $w_L(y) = 4$ и $x \neq y$, имеем

$$\begin{aligned} &w_L(v) \geq w_L(y + 2x) - 4 = w_L(y) + 2w_L(x) - 2w_L(x * y) - 4 = \\ &= w_L(x) + w_L(x \oplus y) - 4 \geq w_L(x). \end{aligned}$$

Поэтому будем рассматривать только те векторы x, для которых $w_L(x) \leq 4$. Таким образом, проверка кодового расстояния сводится к следующим случаям.

Случай 1. Если $w_L(x) = 0$, $w_L(y) = 0$, то вектор v нулевой.

Случай 2. Для $w_L(x) = 4$, $w_L(y) = 0$ справедливо $w_L(v) = 8$.

Случай 3. При $w_L(x) = 0$, $w_L(y) = 4$ из условий 1, 2 следует $w_L(v) \geq 6$.

Случай 4. Пусть $w_L(x) = 4$, $w_L(y) = 4$. Если $x = y$, то аналогично случаю 3, имеем $w_L(v) \geq 6$. При $x \neq y$ используем неравенство $w_L(v) \geq 4$. Предположим, что $w_L(v) = 4$. Тогда векторы x, $x \oplus y$ веса 4 таковы, что выполнено равенство $S_\psi(y) = 2(x * (x \oplus y))$, и следовательно, условие 3 нарушается. Поэтому, в силу четности веса $w_L(x \oplus y)$, имеем $w_L(v) \geq 6$. ▲

Из предложений 9, 10 вытекает

Следствие 1. *Четверичный код* $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ *является линейным кодом Препараты тогда и только тогда, когда функция* ψ *удовлетворяет условиям* (4) *и* (5).

Предложение 11. *Пусть выбран некоторый базис линейного кода* H^n. *Тогда произвольный набор значений функции* ψ, *заданный на базисе, однозначно определяет функцию* ψ *так, что она удовлетворяет условию* (4).

Доказательство. Пусть множество D состоит из всех векторов кода H^n, на которых значения функции ψ определены. Изначально D содержит только базовые векторы. Расширим D до кода H^n с помощью условия (4). Используя тот факт, что вектор $e_{\psi(y^1)} \oplus e_{\psi(y^2)} \oplus e_{\psi(y^1 \oplus y^2)} \oplus y^1 * y^2 \oplus (|y^1 * y^2| \oplus 1)\, e_i$ принадлежит H^n для любых векторов $y^1, y^2 \in D$, однозначно определим $\psi(y^1 \oplus y^2)$. Действительно, вектор $e_{\psi(y^1)} \oplus$ $\oplus\, e_{\psi(y^2)} \oplus y^1 * y^2$ после выкалывания i-й координаты в коде H^n будет находиться на расстоянии, меньшем либо равном 1 от некоторого кодового слова. Если расстояние равно 1, пусть значение $\psi(y^1 \oplus y^2)$ указывает направление к этому кодовому слову. Если равно 0, положим $\psi(y^1 \oplus y^2) = i$. Вектор $y^1 \oplus y^2$ добавим в множество D. Продолжая таким образом, однозначно доопределим ψ на всем коде H^n. ▲

5.3. Четверичные линейные коды Препарата и функции сдвига. Пусть для фиксированных координаты $i \in I$ и двоичного расширенного кода Хэмминга H^n функция $\psi : H^n \to I$ удовлетворяет условиям (4) и (5). Из предложений 3 и 11 следует, что ψ однозначно восстанавливается по своим значениям на множестве векторов H^n веса 4. Поэтому имеет смысл рассматривать сужение φ функции ψ на $SQS(H^n)$, которое назовем *функцией сдвига*. Подставим в (4) и (5) выражения для векторов $T_\lambda(\cdot)$ и $S_\psi(\cdot)$. Тогда для φ имеет место эквивалентное определение: функция $\varphi : SQS(H^n) \to I \backslash \{i\}$ является *функцией сдвига*, если для любых y^1, y^2 из $SQS(H^n)$, таких что $y^1 \oplus y^2$ принадлежит $SQS(H^n)$, выполнены условия:

1. $e_i \oplus e_{\varphi(y^1)} \not\prec y^1$;
2. $e_i \oplus e_{\varphi(y^1 \oplus y^2)} \neq y^1 * y^2$;
3. $e_i \oplus e_{\varphi(y^1)} \oplus e_{\varphi(y^2)} \oplus e_{\varphi(y^1 \oplus y^2)} \oplus y^1 * y^2 \in H^n$.

Теорема 3. *Для любой координаты i существует взаимно-однозначное соответствие между множеством всех различных четверичных линейных кодов Препараты длины n и множеством всевозможных пар (H^n, φ), где H^n – двоичный расширенный линейный код Хэмминга длины n и $\varphi : SQS(H^n) \to I \setminus \{i\}$ – функция сдвига.*

Доказательство. Согласно теореме 2 и следствию 1 множество всех четверичных линейных кодов Препараты длины n исчерпывается кодами вида $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$, где H^n – расширенный код Хэмминга, функция ψ удовлетворяет условиям (4), (5). При фиксированном H^n между множеством таких функций ψ и множеством функций сдвига φ существует взаимно-однозначное соответствие. Тогда произвольному линейному четверичному коду Препараты однозначно сопоставим пару (H^n, φ).

Осталось проверить, что различным парам (H_1^n, φ_1) и (H_2^n, φ_2) соответствуют различные коды Препарата $\mathcal{P}_1$ и $\mathcal{P}_2$. Если выполнено $H_1^n = H_2^n$ и $\varphi_1 \neq \varphi_2$, то коды $\mathcal{P}_1$ и $\mathcal{P}_2$ очевидно различны. Если $H_1^n \neq H_2^n$, то в силу равенств $2\mathcal{P}_1 = 2H_1^n$ и $2\mathcal{P}_2 = 2H_2^n$ коды $\mathcal{P}_1$ и $\mathcal{P}_2$ также различны. ▲

Следствие 2. *Для числа неэквивалентных четверичных линейных кодов Препараты длины n справедлива верхняя оценка $2^{n \log_2 n}$.*

Доказательство. Согласно предложению 11 число различных функций сдвига для фиксированных расширенного кода Хэмминга и координаты i не превышает числа $(n - 1 - \log_2 n)^{n-1}$. ▲

§ 6. Пример описания одного четверичного линейного кода Препараты с помощью функции сдвига

Приведем конструкцию известного четверичного линейного кода Препараты [5] и определим соответствующую ему согласно теореме 3 пару (H^n, φ).

С помощью стандартного отображения $\bar{\ }: \mathbb{Z}_4 \to \mathbb{Z}_2$ по правилу $\overline{0} = \overline{2} = 0$ и $\overline{1} = \overline{3} = 1$ (см. [23]) задается следующий гомоморфизм кольца $\mathbb{Z}_4[X]$ в $\mathbb{Z}_2[X]$:

$$\bar{\ } : \mathbb{Z}_4[X] \to \mathbb{Z}_2[X],$$

при котором многочлен $a_0 + a_1X + \ldots + a_nX^n$ переходит в многочлен $\overline{a}_0 + \overline{a}_1X + \ldots + \overline{a}_nX^n$. Для любого натурального числа m существует приведенный многочлен $h(X) \in \mathbb{Z}_4[X]$ степени m, такой что $h(X)$ делит $(X^{2^m-1} - 1)$ в кольце $\mathbb{Z}_4[X]$, и $\overline{h}(X)$ – примитивный многочлен степени m в кольце $\mathbb{Z}_2[X]$. Пусть $(h(X))$ обозначает идеал, порожденный многочленом $h(X)$. Тогда факторкольцо $\mathbb{Z}_4[X]/(h(X))$ является кольцом Галуа $GR(4^m)$ и совпадает с кольцом $\mathbb{Z}_4[\xi]$, где $\xi = X + (h(X))$. Отметим, что элемент ξ является корнем многочлена $h(X)$. Рассмотрим гомоморфизм

$$\bar{\ } : \mathbb{Z}_4[X]/(h(X)) \to \mathbb{Z}_2[X]/(\overline{h}(X)).$$

Тогда элемент $\overline{\xi}$ равен $X + (\overline{h}(X))$ и является корнем примитивного многочлена $\overline{h}(X)$. Кольцо $\mathbb{Z}_2[\overline{\xi}]$ является полем Галуа $GF(2^m)$. Таким образом, отображение

$$\bar{\ } : \mathbb{Z}_4[\xi] \to \mathbb{Z}_2[\overline{\xi}]$$

задает гомоморфизм, при котором элемент $a_0 + a_1\xi + \ldots + a_n\xi^{m-1}$ переходит в $\overline{a}_0 + \overline{a}_1\overline{\xi} + \ldots + \overline{a}_n\overline{\xi}^{m-1}$ (см. [23, глава 6]).

Произвольный элемент кольца $GR(4^m)$ можно однозначно представить в виде

$$a + 2b \text{ для } a, b \in \mathcal{T}, \text{ где } \mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}.$$

Четверичный линейный код Препарата $\mathcal{P}(m)$ длины $n = 2^m$, m нечетно, $m \geq 3$, задается проверочной матрицей

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \xi & \xi^2 & \ldots & \xi^{n-2} \end{pmatrix}.$$

Базовый четверичный код Васильева $\mathcal{V}_{\mathcal{H}}^{\lambda}$ имеет проверочную матрицу

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 2 & 2\xi & 2\xi^2 & \ldots & 2\xi^{n-2} \end{pmatrix}.$$

По теореме 2 коду $\mathcal{P}(m)$ соответствует двоичный расширенный линейный код Хэмминга H^n, однозначно определяемый равенством $2\mathcal{P} = 2H^n$. Он имеет проверочную матрицу

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \overline{\xi} & \overline{\xi}^2 & \ldots & \overline{\xi}^{n-2} \end{pmatrix}.$$

Пусть координаты занумерованы следующим образом:

$$I = \{\infty, 0, 1, 2, \ldots, n-2\}.$$

Условимся считать, что $\xi^\infty = 0$. Тогда между множествами I и $\mathcal{T}$ легко провести соответствие, сопоставив элементу i элемент ξ^i. Выделим координату ∞ и определим функцию сдвига $\varphi : SQS(H^n) \to I \setminus \{\infty\}$. Для произвольного вектора y из $SQS(H^n)$, имеющего ненулевыми координаты j, k, l, m, справедливо равенство

$$\overline{\xi}^j + \overline{\xi}^k + \overline{\xi}^l + \overline{\xi}^m = 0.$$

Следовательно,

$$\xi^j + \xi^k + \xi^l + \xi^m = 2\xi^r$$

для некоторого r из множества I. Заметим, что $\xi^r \neq 0$, т.е. $r \neq \infty$, поскольку в противном случае код $\mathcal{P}(m)$ содержал бы вектор y веса 4. Тогда из равенства $\xi^j + \xi^k + \xi^l + \xi^m + 2\xi^r = 0$ следует, что четверичный вектор

$$y + 2e_\infty + 2e_r$$

принадлежит коду $\mathcal{P}(m)$. Положим $\varphi(y) = r$. Таким образом, вектор $y + T_\lambda(y) + S_\psi(y)$ является кодовым. Соответствующая коду $\mathcal{P}(m)$ пара (H^n, φ) определена.

Автор глубоко признателен Ф.И. Соловьевой за полезные обсуждения и ряд ценных замечаний.

СПИСОК ЛИТЕРАТУРЫ

1. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337–339.
2. *Preparata F.P.* A Class of Optimum Nonlinear Double-Error-Correcting Codes // Inform. Control. 1968. V. 13. № 4. P. 378–400.
3. *Думер И.И.* Некоторые новые равномерно упакованные коды // Тр. Московского ин-та физики и технологии. М., 1976. С. 72–78.
4. *Baker R.D., van Lint J.H., Wilson R.M.* On the Preparata and Goethals Codes // IEEE Trans. Inform. Theory. 1983. V. 29. № 3. P. 342–345.
5. *Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319.
6. *Calderbank A.R., Cameron P.J., Kantor W.M., Seidel J.J.* $\mathbb{Z}_4$-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets // Proc. London Math. Soc. 1997. V. 75. P. 436–480.
7. *Токарева Н.Н.* О компонентах кодов Препараты // Пробл. передачи информ. 2004. Т. 40. № 2. С. 63–69.
8. *Васильев Ю.Л.* Векторные поля на множестве вершин n-мерного единичного куба // Дискретный анализ. Новосибирск: Ин-т математики СО АН СССР, 1967. Вып. 11. С. 21–59.
9. *Кротов Д.С.* Векторные поля, коды Препарата и разбиения булева куба на цилиндры // Тр. XII Междунар. конф. "Проблемы теоретической кибернетики". Нижний Новгород. Май 17–22, 1999. М.: Изд-во мех.-мат. фак-та МГУ, 1999. С. 122.
10. *Krotov D.S.* On Diameter Perfect Constant-Weight Ternary Codes // Discrete Mathematics (submitted).
11. *Соловьева Ф.И.* О факторизации кодообразующих д.н.ф. // Методы дискретного анализа в исследовании функциональных систем. Новосибирск: Ин-т математики СО АН СССР, 1988. Вып. 47. С. 66–88.
12. *Августинович С.В., Соловьева Ф.И.* Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Пробл. передачи информ. 1997. Т. 33. № 3. С. 15–21.
13. *Semakov N.V., Zinoviev V.A., Zaitsev G.V.* Interrelation of Preparata and Hamming Codes and Extension of Hamming Codes to New Double-Error Correcting Codes // Proc. 2nd Int. Sympos. Information Theory. Tsakhadsor, Armenia, 1971. Budapest: Akademia Kiado, 1973. P. 257–263.
14. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. № 1. С. 38–50.
15. *Курляндчик Я.М.* О логарифмической асимптотике длины максимального цикла разброса $r > 2$ // Методы дискретного анализа. Новосибирск: Ин-т математики СО АН СССР, 1971. Вып. 19. С. 48–55.

16. *Avgustinovich S. V., Solov'eva F.I., Heden O.* On Group of Symmetries of Vasil'ev Codes // Proc. 9th Int. Workshop "Algebraic and Combinatorial Coding Theory". Kranevo, Bulgaria. June 19–25, 2004. P. 27–33.
17. *Borges J., Phelps K.T., Rifa J., Zinoviev V.A.* On $\mathbb{Z}_4$-Linear Preparata-Like and Kerdock-Like Codes // IEEE Trans. Inform. Theory. 2003. V. 49. № 11. P. 2834–2843.
18. *Кротов Д.С.* $\mathbb{Z}_4$-линейные совершенные коды // Дискретный анализ и исследование операций. Сер. 1. 2000. Т. 7. № 4. С. 78–90.
19. *Krotov D.S.* $\mathbb{Z}_4$-Linear Hadamard and Extended Perfect Codes // Proc. Int. Workshop on Coding and Cryptography WCC'2001. Paris, France. January 8–12, 2001. P. 329–334.
20. *Кротов Д.С.* Частное сообщение. 2003.
21. *Avgustinovich S.V., Heden O., Solov'eva F.I.* The Classification of Some Perfect Codes. Preprint. Stockholm: Royal Institute of Technology, 2001.
22. *Avgustinovich S.V., Heden O., Solov'eva F.I.* The Classification of Some Perfect Codes // Designs, Codes Cryptography. 2004. V. 31. № 3. P. 313–318.
23. *Wan Z.-X.* Quaternary Codes. Singapore: World Scientific, 1997.

Токарева Наталья Николаевна
Новосибирский государственный университет
toknn@ngs.ru

Поступила в редакцию
08.12.2004
После переработки
14.03.2005