Сибирский математический журнал
Май—июнь, 2008. Том 49, № 3

УДК 519.725

ДИСТАНЦИОННАЯ РЕГУЛЯРНОСТЬ КОДОВ КЕРДОКА

Ф. И. Соловьева, Н. Н. Токарева

Аннотация. Код называется *дистанционно регулярным*, если для любых кодовых слов $\mathbf{x}$, $\mathbf{y}$ и любых целых чисел i, j число кодовых слов $\mathbf{z}$ таких, что расстояния Хэмминга $d(\mathbf{x}, \mathbf{z})$ и $d(\mathbf{y}, \mathbf{z})$ равны i и j соответственно, не зависит от выбора векторов $\mathbf{x}$, $\mathbf{y}$ и зависит только от $d(\mathbf{x}, \mathbf{y})$ и чисел i, j. Приводится новое комбинаторное доказательство (с использованием свойств дискретного преобразования Фурье) того факта, что все коды Кердока дистанционно регулярны. Вычислены параметры дистанционной регулярности произвольного кода Кердока.

Ключевые слова: дистанционно регулярные коды, коды Кердока, коды Рида — Маллера, дискретное преобразование Фурье, максимально нелинейная булева функция, дистанционно регулярный граф, метрическая схема отношений.

§ 1. Введение

В работе, существенно используя свойства дискретного преобразования Фурье, приведем новое комбинаторное доказательство дистанционной регулярности произвольного кода Кердока, более простое и короткое в отличие от сложного алгебраического доказательства, полученного ранее Дельсартом в работе [1] при исследовании регулярных схем отношений Хэмминга. Кроме того, в данной работе определяются параметры δ_{ij}^{k} дистанционной регулярности кода Кердока, не известные ранее. Коды Кердока представляют собой асимптотически оптимальные коды, тесно связанные с такими хорошими кодами, как коды Рида — Маллера, коды Препараты, а также другими комбинаторными и алгебраическими объектами. Эти коды образуют первый бесконечный класс дистанционно регулярных кодов, весовой спектр которых имеет более трех ненулевых значений.

Напомним, что код называется *дистанционно регулярным*, если для любых кодовых слов $\mathbf{x}$, $\mathbf{y}$ и любых целых чисел i, j число кодовых слов $\mathbf{z}$ таких, что расстояния Хэмминга $d(\mathbf{x}, \mathbf{z})$ и $d(\mathbf{y}, \mathbf{z})$ равны i и j соответственно, не зависит от выбора векторов $\mathbf{x}$, $\mathbf{y}$ и зависит только от $d(\mathbf{x}, \mathbf{y})$ и чисел i, j.

Дистанционная регулярность является сильным структурным свойством кодов. Говоря неформально, наличие этого свойства отражает высокую степень симметричности кода: относительно любых двух его векторов, находящихся друг от друга на определенном расстоянии, остальные кодовые векторы

Работа первого автора выполнена при частичной финансовой поддержке Шведской Королевской академии наук, работа второго автора — при финансовой поддержке интеграционного проекта СО РАН № 35 «Древовидный каталог математических Интернет-ресурсов mathtree.ru», Российского фонда фундаментальных исследований (коды проектов 07–01–00248 и 08–01–00671) и Фонда содействия отечественной науке. Работа обеих авторов выполнена при частичной финансовой поддержке Новосибирского гос. университета.

всегда «располагаются» одинаковым образом независимо от выбора исходной пары. Свойство дистанционной регулярности кодов тесно связано с другими регулярными свойствами характеристических графов этих кодов, их метрическими свойствами, а также с метрическими схемами отношений Хэмминга (см. [2, гл. 21]), и дистанционно регулярными графами (см. [3]). Исследование этого свойства кодов было начато в работах Дельсарта [1], Баннаи и Ито [4], В. И. Левенштейна (см. [5]).

На сегодняшний день свойство дистанционной регулярности кодов исследовано недостаточно широко и пока известно небольшое число кодов, обладающих этим свойством. Дистанционно регулярными являются все двоичные коды Адамара (среди них двоичные коды Рида — Маллера первого порядка), двоичный и троичный совершенные коды Голея, а также серия кодов, полученных из них операциями расширения, укорочения и выкалывания (см. [5] и работу Топаловой [6]). В статье [7] показано, что все двоичные совершенные коды с кодовым расстоянием 3 не являются дистанционно регулярными, за исключением кодов Хэмминга длин 3 и 7. Аналогичный результат справедлив для расширенных двоичных совершенных кодов с кодовым расстоянием 4 (см. [8]). В работе [9] установлено, что единственным с точностью до эквивалентности дистанционно регулярным кодом Препараты является код длины 16, называемый кодом Нордстрома — Робинсона.

Рассмотрим структуру статьи. В § 2 приведены необходимые определения и свойства кодов Рида — Маллера, максимально нелинейных булевых функций, кодов Кердока и дискретного преобразования Фурье. В § 3 доказан ряд вспомогательных лемм 1–3, отражающих свойства максимально нелинейных функций и смежных классов по коду Рида — Маллера первого порядка. В § 4 показано, что для проверки свойства дистанционной регулярности кодов Кердока достаточно рассматривать (см. определение) пары кодовых слов $\mathbf{x}$, $\mathbf{y}$ такие, что одно из них является нулевым вектором (лемма 4). Далее для таких пар кодовых слов с использованием леммы из § 3 доказывается, что число кодовых слов $\mathbf{z}$ (см. выше определение дистанционной регулярности) является константой, зависящей только от параметров i, j, k и длины кода (см. леммы 5–8). Отсюда следует основной результат статьи — дистанционная регулярность кодов Кердока (теорема 1). В § 5 содержится ряд дополнительных замечаний о свойстве дистанционной регулярности.

§ 2. Необходимые определения и понятия

Рассмотрим метрическое пространство E^n всех двоичных векторов длины n с метрикой Хэмминга. *Расстояние Хэмминга* $d(\mathbf{x}, \mathbf{y})$ между векторами $\mathbf{x}$ и $\mathbf{y}$ определяется как число координат, в которых эти векторы различаются. *Весом Хэмминга* $w(\mathbf{x})$ вектора $\mathbf{x}$ называется число его ненулевых координат. *Двоичный код длины* n — произвольное непустое подмножество пространства E^n. *Кодовое расстояние* d кода равно минимальному расстоянию между его различными векторами (или *кодовыми словами*). Векторы, имеющие все координаты равными нулю или единице, обозначим через $\mathbf{0}$ и $\mathbf{1}$ соответственно. *Весовым спектром* кода длины n называют набор чисел $A_0, A_1, \ldots, A_n$ такой, что число кодовых слов веса i равно A_i для каждого i.

Дальнейшие определения и понятия приведем, следуя, в основном, [2].

2.1. Коды Рида — Маллера. Рассмотрим множество булевых функций от m переменных $v_1, \ldots, v_m$. Напомним, что любую такую функцию можно единственным образом представить в виде многочлена степени не больше m, именуемого многочленом Жегалкина:

$$\sum_{j=1}^{m} \sum_{1 \le i_1, \dots, i_j \le m} a_{i_1 \dots i_j} v_{i_1} \dots v_{i_j} + a,$$

где $a_{i_1 \dots i_j}$, a равны 0 или 1, числа $i_1, \dots, i_j$ попарно различны и суммирование ведется по модулю 2. Пусть вектор $\mathbf{v} = (v_1, \dots, v_m)$ пробегает все пространство E^m. При этом каждой булевой функции f сопоставляется двоичный вектор $\mathbf{f}$ ее значений длины 2^m.

Двоичный *код Рида — Маллера* $R(r, m)$ *порядка* r длины $n = 2^m$ состоит из всех двоичных векторов $\mathbf{f}$, отвечающих булевым функциям f от m переменных, многочлены которых имеют степени не выше r. Код $R(r, m)$ имеет мощность

$$2^{1+\binom{m}{1}+\dots+\binom{m}{r}}$$

и кодовое расстояние 2^{m-r}, где $\binom{m}{i}$ обозначает, как обычно, число сочетаний из m элементов по i.

Для двух векторов $\mathbf{a} = (a_1, \dots, a_m)$ и $\mathbf{v} = (v_1, \dots, v_m)$ через $\mathbf{a} \cdot \mathbf{v}$ обозначается их скалярное произведение $\mathbf{a} \cdot \mathbf{v} = a_1 v_1 + \dots + a_m v_m$ по модулю 2. Код Рида — Маллера $R(1, m)$ первого порядка описывается всевозможными линейными функциями от $\mathbf{v}$ вида $\mathbf{a} \cdot \mathbf{v} + b$, где $\mathbf{a}$ — произвольный фиксированный вектор длины m, константа b принимает значения 0 и 1. Другими словами, каждое кодовое слово кода $R(1, m)$ имеет вид

$$\sum_{i=1}^{m} a_i \mathbf{v}^i + b \cdot \mathbf{1},$$

где через $\mathbf{v}^i$ обозначается двоичный вектор длины $n = 2^m$, соответствующий функции, равной переменной v_i. Мощность кода Рида — Маллера $R(1, m)$ равна $2n$, кодовое расстояние равно $n/2$. Нетрудно видеть, что весовой спектр этого кода имеет следующие ненулевые значения: $A_0 = A_n = 1$, $A_{n/2} = 2n - 2$.

Почти всем кодовым словам кода Рида — Маллера $R(2, m)$ второго порядка отвечают так называемые *квадратичные* булевы функции, степени многочленов Жегалкина которых равны 2.

2.2. Максимально нелинейные булевы функции. Далее потребуются максимально нелинейные булевы функции — функции, наиболее удаленные (по расстоянию Хэмминга) от множества всех линейных функций. Всюду далее полагаем

$$n = 2^m \text{ для четного } m \ge 4, \quad d = (n - \sqrt{n})/2.$$

Булева функция f от m переменных $v_1, \dots, v_m$ называется *максимально нелинейной* (или *бент-функцией*), если соответствующий ей вектор $\mathbf{f}$ находится на расстоянии Хэмминга d или $n - d$ от любого кодового слова кода Рида — Маллера первого порядка $R(1, m)$. Из этого определения непосредственно следует, что вес вектора $\mathbf{f}$ равен d или $n - d$. Имеет место

Утверждение 1. *Смежный класс* $\mathbf{f} + R(1, m)$ *для произвольной максимально нелинейной функции* f *от* m *переменных имеет* n *векторов веса* d *и* n *векторов веса* $n - d$.

Нетрудно убедиться, что каждому вектору из класса смежности $\mathbf{f} + R(1, m)$ соответствует максимально нелинейная функция.

2.3. Коды Кердока. *Код Кердока* K длины $n = 2^m$ для четного $m \geq 4$ является объединением кода Рида — Маллера первого порядка $R(1,m)$ и $(n-2)/2$ смежных классов кода Рида — Маллера второго порядка $R(2,m)$ по коду $R(1,m)$, причем булевы функции, соответствующие этим смежным классам, являются максимально нелинейными квадратичными функциями такими, что сумма любых двух из них снова является максимально нелинейной.

Из свойств множества максимально нелинейных квадратичных функций от m переменных (см. [2]) следует, что произвольный код Кердока K длины n имеет мощность n^2 и является максимальным подкодом с кодовым расстоянием $(n-\sqrt{n})/2$ кода Рида — Маллера $R(2,m)$ второго порядка. Более того, согласно работе В. М. Сидельникова [10] верхняя оценка мощности произвольного двоичного кода длины n с кодовым расстоянием $(n-\sqrt{n})/2$ эквивалентна функции n^2 при $n \to \infty$. Таким образом, код Кердока является асимптотически оптимальным в классе кодов длины n с таким кодовым расстоянием. Код Кердока имеет следующие ненулевые значения весового спектра:

$$A_0 = A_n = 1, \quad A_d = A_{n-d} = n(n-2)/2, \quad A_{n/2} = 2n-2.$$

Заметим, что каждый код Кердока обладает свойством *антиподальности*: для любого кодового слова $\mathbf{x}$ слово $\mathbf{x}+\mathbf{1}$ также принадлежит коду.

Код называется *дистанционно инвариантным*, если число кодовых слов на расстоянии i от кодового слова $\mathbf{x}$ не зависит от выбора $\mathbf{x}$, а зависит только от i. Согласно [2, гл. 15] имеет место

Утверждение 2. *Произвольный код Кердока дистанционно инвариантен.*

Первый такой код для каждой допустимой длины n построен Кердоком в 1972 г. [11]. Для каждого $n = 2^m$ такого, что $m-1$ — составное нечетное число, Кантором [12] в 1982 г. построена серия из $2^{\sqrt{m}/2}$ попарно неэквивалентных кодов Кердока длины n. В 1989 г. А. А. Нечаевым [13] построен код Кердока длины n (для каждого допустимого значения n), имеющий описание в терминах линейных рекуррентных последовательностей над кольцом $\mathbb{Z}_4$, эквивалентный оригинальному коду Кердока [11]. Позднее в 1994 г. Хэммонс и др. [14] предложили иную конструкцию кодов Кердока для каждой допустимой длины. Ими показано, что относительно отображения Грея оригинальный код Кердока [11] является образом линейного расширенного циклического кода над кольцом $\mathbb{Z}_4$ (см. [14], а также [15]).

Коды Кердока тесно связаны с кодами Препараты (двоичными кодами максимальной мощности длины $n = 2^m$ для четного $m \geq 4$ с кодовым расстоянием 6 (см. [2, гл. 15])). Коды Кердока и Препараты являются формально дуальными в том смысле, что их весовые спектры удовлетворяют соотношению Мак-Вильямс (см. [2, гл. 5]). Отметим, что коды Кердока и Препараты длины 16 совпадают. Этот код единствен с точностью до эквивалентности и называется *кодом Нордстрома — Робинсона* [16].

Каждый код Кердока длины n может быть описан с помощью так называемого множества Кердока, состоящего из $n/2$ кососимметричных двоичных матриц размера $m \times m$ (среди которых содержится нулевая матрица) таких, что разность любых двух из них является невырожденной матрицей. Каждой матрице из множества Кердока сопоставляется квадратичная форма, однозначно определяющая соответствующий смежный класс кода $R(2,m)$ по коду $R(1,m)$, входящий в код Кердока. Такой подход к описанию кодов Кердока связан со специальными вопросами в области конечных геометрий и квадратичных форм.

Большое количество кодов Кердока длины $n = 2^m$ построено с использованием проективных плоскостей и специальных неассоциативных алгебр, определяемых на множестве элементов поля $GF(2^{m-1})$ (см. подробнее [17, 18]).

Пусть $\rho(m-1)$ обозначает число простых делителей числа $m-1$ с учетом их кратностей. В работе [19] доказано, что для четного $m \geq 4$ существует не менее

$$\frac{(2^{m-1}-1)^{\rho(m-1)-3}}{(m-1)^2}$$

попарно неэквивалентных кодов Кердока длины $n = 2^m$.

В настоящей работе для исследования структурного свойства дистанционной регулярности кодов Кердока длины $n = 2^m$ существенно будут использоваться линейные и максимально нелинейные булевы функции от m переменных, а также свойства дискретного преобразования Фурье.

2.4. Дискретное преобразование Фурье. Подробное описание приводимых в данном пункте свойств дискретного преобразования Фурье (его также называют *преобразованием Уолша — Адамара*) может быть найдено в [2, гл. 14].

Пусть вектор $\mathbf{v} = (v_1, \ldots, v_m)$ пробегает все пространство двоичных векторов E^m. Булевой функции f от m переменных $v_1, \ldots, v_m$ однозначно сопоставляется двоичный вектор ее значений $\mathbf{f}$ длины $n = 2^m$. Для булевой функции f определим вещественную функцию F от m переменных $v_1, \ldots, v_m$ следующим образом:

$$F(\mathbf{v}) = (-1)^{f(\mathbf{v})}. \tag{1}$$

Используя равенство (1), можно перейти от двоичного вектора $\mathbf{f}$ к вещественнозначному вектору $\mathbf{F}$ той же длины, отвечающему функции F, заменив в каждой координате вектора $\mathbf{f}$ значения 0 на 1 и 1 на -1. Далее, не оговаривая особо, формулу (1) будем использовать и для других булевых функций. Например, булевым функциям $f_{\mathbf{a}}, h$ по правилу (1) будут сопоставляться вещественные функции $F_{\mathbf{a}}, H$ соответственно.

Дискретное преобразование Фурье вектора $\mathbf{F}$ определяется равенством

$$\widehat{F}(\mathbf{u}) = \sum_{\mathbf{v} \in E^m} (-1)^{\mathbf{u}\cdot\mathbf{v}} F(\mathbf{v}) \quad \text{для всех } \mathbf{u} \in E^m. \tag{2}$$

Для произвольного вектора $\mathbf{u}$ длины m из (2) следуют соотношения

$$\widehat{F}(\mathbf{u}) = n - 2d\left(\mathbf{f}, \sum_{i=1}^{m} u_i \mathbf{v}^i\right), \tag{3}$$

$$\widehat{F}(\mathbf{u}) = -n + 2d\left(\mathbf{f}, \sum_{i=1}^{m} u_i \mathbf{v}^i + \mathbf{1}\right) \tag{4}$$

(см. подробнее [2, гл. 14, п. 3]). Имеет место *формула обращения* дискретного преобразования Фурье

$$F(\mathbf{v}) = \frac{1}{n} \sum_{\mathbf{u} \in E^m} (-1)^{\mathbf{u}\cdot\mathbf{v}} \widehat{F}(\mathbf{u}) \quad \text{для всех } \mathbf{v} \in E^m. \tag{5}$$

§ 3. Вспомогательные леммы

Для доказательства основной теоремы потребуется ряд вспомогательных утверждений, касающихся смежных классов кода Рида — Маллера первого порядка, максимально нелинейных булевых функций и дискретного преобразования Фурье.

Пусть f — произвольная максимально нелинейная булева функция от m переменных (всюду далее f будет обозначать именно такую функцию). В смежном классе $\mathbf{f} + R(1, m)$ кода Рида — Маллера первого порядка содержится согласно утверждению 1 в точности n векторов веса d и n антиподальных к ним векторов веса $n - d$. Каждому вектору $\mathbf{a}$ из E^m сопоставим взаимно однозначно вектор $\mathbf{f_a}$ длины $n = 2^m$ веса d этого смежного класса, описываемый булевой функцией

$$f_{\mathbf{a}}(\mathbf{v}) = f(\mathbf{v}) + \mathbf{a} \cdot \mathbf{v} + b_{\mathbf{a}}, \tag{6}$$

от m переменных; значение $b_{\mathbf{a}}$, равное 0 или 1, каждый раз однозначно определяется из условия $d(\mathbf{f_a}, \mathbf{0}) = d$. Очевидно, что разным векторам $\mathbf{a}$, $\mathbf{a}'$ из E^m отвечают разные векторы $\mathbf{f_a}$, $\mathbf{f_{a'}}$ этого смежного класса. Заметим, что в силу формулы (3) (подставим в качестве аргумента функции $\widehat{F}_{\mathbf{a}}$ нулевой вектор) это условие эквивалентно условию

$$\widehat{F}_{\mathbf{a}}(\mathbf{0}) = n - 2d \tag{7}$$

независимо от выбора вектора $\mathbf{a}$ из E^m.

Из соотношений (1) и (6) следует равенство

$$F_{\mathbf{a}}(\mathbf{v}) = (-1)^{\mathbf{a} \cdot \mathbf{v} + b_{\mathbf{a}}} F(\mathbf{v}). \tag{8}$$

Утверждение 3. *Для любого вектора* $\mathbf{u}$ *длины* m *для дискретного преобразования Фурье вектора* $\mathbf{F_a}$ *справедливо*

$$\widehat{F}_{\mathbf{a}}(\mathbf{u}) = (-1)^{b_{\mathbf{a}}} \widehat{F}(\mathbf{u} + \mathbf{a}). \tag{9}$$

Доказательство этого факта вытекает из последовательности следующих равенств:

$$\widehat{F}_{\mathbf{a}}(\mathbf{u}) \overset{(2)}{=} \sum_{\mathbf{v} \in E^m} (-1)^{\mathbf{u} \cdot \mathbf{v}} F_{\mathbf{a}}(\mathbf{v}) \overset{(8)}{=} \sum_{\mathbf{v} \in E^m} (-1)^{\mathbf{u} \cdot \mathbf{v} + \mathbf{a} \cdot \mathbf{v} + b_{\mathbf{a}}} F(\mathbf{v}) \overset{(2)}{=} (-1)^{b_{\mathbf{a}}} \widehat{F}(\mathbf{u} + \mathbf{a}).$$

Лемма 1. *Пусть* $f_{\mathbf{a}}(\mathbf{v})$ — *произвольная максимально нелинейная функция от* m *переменных, определенная в* (6). *Тогда для любого вектора* $\mathbf{v}$ *из* E^m *справедливо*

$$\sum_{\mathbf{a} \in E^m} F_{\mathbf{a}}(\mathbf{v}) = \frac{n}{n - 2d}.$$

Доказательство. Рассмотрим формулу (5) обращения дискретного преобразования Фурье:

$$F(\mathbf{v}) = \frac{1}{n} \sum_{\mathbf{a} \in E^m} (-1)^{\mathbf{a} \cdot \mathbf{v}} \widehat{F}(\mathbf{a})$$

для любого двоичного вектора $\mathbf{v}$ длины m. Используя соотношение (9), получаем

$$F(\mathbf{v}) = \frac{1}{n} \sum_{\mathbf{a} \in E^m} (-1)^{\mathbf{a} \cdot \mathbf{v} + b_{\mathbf{a}}} \widehat{F}_{\mathbf{a}}(\mathbf{0}).$$

Домножая на $F(\mathbf{v})$ обе части этого равенства, учитывая условие (7) и равенство (8), имеем

$$F^2(\mathbf{v}) = \frac{n-2d}{n} \sum_{\mathbf{a}\in E^m} F_{\mathbf{a}}(\mathbf{v}).$$

Поскольку $F^2(\mathbf{v}) = 1$ для любого двоичного вектора $\mathbf{v}$, приходим к требуемому равенству. $\square$

Лемма 2. *Пусть $f_{\mathbf{a}}(\mathbf{v})$ — произвольная максимально нелинейная функция от m переменных, определенная в (6). Тогда для любого ненулевого вектора $\mathbf{u}$ из E^m выполняется*

$$\sum_{\mathbf{a}\in E^m} \widehat{F}_{\mathbf{a}}(\mathbf{u}) = 0.$$

Доказательство. Используя соотношение (9), представим искомое равенство в виде

$$\sum_{\mathbf{a}\in E^m} (-1)^{b_{\mathbf{a}}} \widehat{F}(\mathbf{u}+\mathbf{a}) = 0.$$

Подставляя в него формулу (2) для дискретного преобразования Фурье, в левой части получим

$$\sum_{\mathbf{a}\in E^m} (-1)^{b_{\mathbf{a}}} \sum_{\mathbf{v}\in E^m} (-1)^{(\mathbf{u}+\mathbf{a})\cdot\mathbf{v}} F(\mathbf{v}).$$

Меняя местами знаки суммирования и используя (8), приходим к выражению

$$\sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{u}\cdot\mathbf{v}} \sum_{\mathbf{a}\in E^m} F_{\mathbf{a}}(\mathbf{v}).$$

Из леммы 1 следует, что полученное выражение равно

$$\frac{n}{n-2d} \sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{u}\cdot\mathbf{v}}.$$

Заметим, что для любого фиксированного ненулевого вектора $\mathbf{u}$ скалярное произведение $\mathbf{u}\cdot\mathbf{v}$ принимает значения 0 и 1 одинаково часто, когда вектор $\mathbf{v}$ пробегает все пространство E^m. Таким образом, имеем

$$\sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{u}\cdot\mathbf{v}} = 0,$$

откуда следует искомое равенство. $\square$

Лемма 3. *Пусть $f_{\mathbf{a}}(\mathbf{v})$ — произвольная максимально нелинейная функция от m переменных, определенная в (6). Тогда для любого двоичного вектора $\mathbf{g}$ длины n веса d сумма всех значений вещественнозначных функций $(-1)^{g(\mathbf{v})}F_{\mathbf{a}}(\mathbf{v})$, где $\mathbf{a}$ из E^m, не зависит от выбора вектора $\mathbf{g}$ и равна константе, а именно*

$$\sum_{\mathbf{a}\in E^m,} \sum_{\mathbf{v}\in E^m} (-1)^{g(\mathbf{v})} F_{\mathbf{a}}(\mathbf{v}) = n.$$

Доказательство. Поменяем местами знаки суммирования:

$$\sum_{\mathbf{v}\in E^m} (-1)^{g(\mathbf{v})} \sum_{\mathbf{a}\in E^m} F_{\mathbf{a}}(\mathbf{v}).$$

Используя лемму 1, получим

$$\frac{n}{n-2d}\sum_{\mathbf{v}\in E^m}(-1)^{g(\mathbf{v})}.$$

Заметим, что выражение $\sum\limits_{\mathbf{v}\in E^m}(-1)^{g(\mathbf{v})}$ равно разности между числом нулей и единиц в двоичном векторе $\mathbf{g}$. Поскольку вектор $\mathbf{g}$ имеет вес d, эта разность равна $n-2d$, откуда следует требуемое равенство. $\square$

§ 4. Дистанционная регулярность кодов Кердока

Рассмотрим произвольный код Кердока K длины $n=2^m$ для четного $m\geq 4$. Обозначим через K_i множество всех кодовых слов кода K веса i. Напомним, что A_i обозначает соответствующее значение весового спектра кода, т. е. $|K_i|=A_i$. Пусть фиксированы целые неотрицательные числа i,j,k. Следуя работе [7], через $\delta_{ij}^k(\mathbf{x})$ обозначим число кодовых слов веса j, находящихся на расстоянии k от кодового слова $\mathbf{x}$ веса i.

Для доказательства дистанционной регулярности произвольного кода Кердока важную роль играет следующий факт.

Лемма 4. *Если для любого кода Кердока длины n при всех допустимых значениях i,j,k функции δ_{ij}^k тождественно равны константам, зависящим только от i,j,k,n, то каждый код Кердока является дистанционно регулярным.*

Доказательство. Пусть K — произвольный код Кердока. Для любых кодовых слов $\mathbf{x},\mathbf{y}$ кода K, находящихся друг от друга на расстоянии i, обозначим через $\Delta_{jk}^i(\mathbf{x},\mathbf{y})$ число кодовых слов $\mathbf{z}$ таких, что $d(\mathbf{x},\mathbf{z})=j$ и $d(\mathbf{y},\mathbf{z})=k$. Убедимся, что значения функций Δ_{jk}^i не зависят от выбора $\mathbf{x}$ и $\mathbf{y}$. Действительно, поскольку сдвиг кода Кердока K на кодовое слово $\mathbf{x}$ является изометричным преобразованием (т. е. сохраняющим расстояние) и код $\mathbf{x}+K$, как нетрудно показать, также является некоторым кодом Кердока, имеем

$$\Delta_{jk}^i(\mathbf{x},\mathbf{y})=\delta_{ij}^k(\mathbf{x}+\mathbf{y}),$$

где по условию леммы функции δ_{ij}^k тождественно равны константам, зависящим только от i,j,k,n. Отсюда следует дистанционная регулярность кода K. $\square$

Далее покажем (см. леммы 5–8), что в произвольном коде Кердока все функции δ_{ij}^k для допустимых значений i,j,k тождественно равны константам, не зависящим от выбора кода, а зависящим лишь от параметров i,j,k и длины n. В силу леммы 4 из этого будет следовать дистанционная регулярность кода Кердока (см. теорему 1), константы δ_{ij}^k играют роль параметров дистанционной регулярности.

Для доказательства потребуются некоторые свойства функций δ_{ij}^k для допустимых значений i,j,k из спектра возможных различных расстояний $\{0,d,n/2,n-d,n\}$ между словами кода Кердока. Опишем эти свойства в следующих ниже утверждениях.

В силу антиподальности кода Кердока справедливо

Утверждение 4. *Для любых значений i,j,k и любого кодового слова $\mathbf{x}$ веса i выполняются равенства*

$$\delta_{ij}^k(\mathbf{x})=\delta_{i,n-j}^{n-k}(\mathbf{x})=\delta_{n-i,n-j}^{k}(\mathbf{x}+1)=\delta_{n-i,j}^{n-k}(\mathbf{x}+1). \tag{10}$$

Для любых i, j, k, подсчитывая различными способами число упорядоченных пар кодовых слов $\mathbf{x} \in K_i$ и $\mathbf{y} \in K_j$ таких, что $d(\mathbf{x}, \mathbf{y}) = k$, получим следующее хорошо известное соотношение:

$$\sum_{\mathbf{x} \in K_i} \delta_{ij}^k(\mathbf{x}) = \sum_{\mathbf{y} \in K_j} \delta_{ji}^k(\mathbf{y}). \tag{11}$$

По утверждению 3 произвольный код Кердока является дистанционно инвариантным, поэтому для любого кодового слова $\mathbf{x}$ веса i число кодовых слов, находящихся от него на расстоянии k, равно A_k. Из свойств весового спектра кода Кердока следует, что каждое из A_j кодовых слов веса j имеет с любым кодовым словом $\mathbf{x}$ веса i одно из пяти возможных расстояний. Отсюда вытекает

Утверждение 5. *Для любых значений i, j, k и произвольного кодового слова $\mathbf{x}$ веса i выполняются равенства*

$$A_k = \delta_{i0}^k(\mathbf{x}) + \delta_{id}^k(\mathbf{x}) + \delta_{i,n/2}^k(\mathbf{x}) + \delta_{i,n-d}^k(\mathbf{x}) + \delta_{in}^k(\mathbf{x}), \tag{12}$$

$$A_j = \delta_{ij}^0(\mathbf{x}) + \delta_{ij}^d(\mathbf{x}) + \delta_{ij}^{n/2}(\mathbf{x}) + \delta_{ij}^{n-d}(\mathbf{x}) + \delta_{ij}^n(\mathbf{x}). \tag{13}$$

Через $\equiv$ далее обозначаем тождественное равенство.

Лемма 5. *Функции δ_{ij}^k, для которых хотя бы один из параметров i, j, k принимает значение 0 или n, тождественно равны константам, зависящим лишь от i, j, k, n.*

Доказательство. Согласно утверждению 3 каждый код Кердока является дистанционно инвариантным. Отсюда несложно следуют тождества

$$\delta_{ij}^0 \equiv \delta_{i0}^j \equiv \begin{cases} 0, & \text{если } i \neq j, \\ 1, & \text{если } i = j; \end{cases} \quad \delta_{ij}^n \equiv \delta_{in}^j \equiv \begin{cases} 0, & \text{если } i + j \neq n, \\ 1, & \text{если } i + j = n. \end{cases} \tag{14}$$

Используя значения весового спектра кода Кердока, имеем

$$\delta_{0j}^k \equiv \begin{cases} 0, & \text{если } j \neq k, \\ A_j, & \text{если } j = k; \end{cases} \quad \delta_{nj}^k \equiv \begin{cases} 0, & \text{если } j + k \neq n, \\ A_j, & \text{если } j + k = n, \end{cases} \tag{15}$$

что и доказывает лемму. □

В последующем будем считать, что возможными значениями каждого из параметров i, j, k могут быть числа $d, n/2$ и $n-d$. В доказательстве приведенных ниже лемм используются свойства (10)–(15) функций δ_{ij}^k.

Лемма 6. *Справедливы тождества $\delta_{n/2,n/2}^{n/2} \equiv 2n-4$, $\delta_{d,n/2}^{n/2} \equiv 0$, $\delta_{dd}^{n/2} \equiv n-1$.*

Доказательство. Поскольку множество $K_0 \cup K_{n/2} \cup K_n$ является кодом Рида — Маллера $R(1, m)$ первого порядка, любое кодовое слово $\mathbf{x}$ кода Кердока веса $n/2$ находится на расстоянии $n/2$ в точности от $A_{n/2} - 2$ кодовых слов веса $n/2$. Отсюда имеем

$$\delta_{n/2,n/2}^{n/2} \equiv 2n - 4.$$

Используя утверждение 5 (см. свойство (12) при $i = k = n/2$) и формулы (14), получаем для произвольного кодового слова $\mathbf{x}$ веса $n/2$ равенство

$$2n - 2 = 1 + \delta_{n/2,d}^{n/2}(\mathbf{x}) + 2n - 4 + \delta_{n/2,n-d}^{n/2}(\mathbf{x}) + 1.$$

Поскольку функции δ_{ij}^k принимают неотрицательные значения, из этого равенства вытекает $\delta_{n/2,d}^{n/2} \equiv \delta_{n/2,n-d}^{n/2} \equiv 0$. Тогда из свойства (11) при $i = k = n/2$,

$j = d$ следует, что $\delta^{n/2}_{d,n/2} \equiv 0$. В утверждении 5 равенство (12) при $i = d$, $k = n/2$ для произвольного кодового слова $\mathbf{x}$ веса d принимает вид $2n - 2 = \delta^{n/2}_{dd}(\mathbf{x}) + \delta^{n/2}_{d,n-d}(\mathbf{x})$. Отсюда и из утверждения 4 получаем тождества $\delta^{n/2}_{dd} \equiv \delta^{n/2}_{d,n-d} \equiv n - 1$. $\square$

Лемма 7. *Имеет место тождество* $\delta^{d}_{n/2,d} \equiv n(n-2)/4$.

Доказательство. Рассмотрим произвольное кодовое слово $\mathbf{g}$ кода Кердока веса $n/2$. Поскольку $\mathbf{g}$ содержится в коде $R(1,m)$, ему соответствует линейная булева функция g от m переменных. Пусть

$$g(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_m v_m$$

для некоторого ненулевого вектора $\mathbf{u} = (u_1, \ldots, u_m)$ длины m (случай $g(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v} + 1$ рассматривается аналогично). Векторы веса d из смежных классов по коду $R(1,m)$, содержащихся в коде Кердока, образуют множество K_d. Число этих смежных классов равно $(n-2)/2$. Рассмотрим векторы веса d одного из таких смежных классов $\mathbf{f} + R(1,m)$, где f — некоторая максимально нелинейная функция. Их число равно n. Каждый такой вектор можно описать с помощью максимально нелинейной булевой функции $f_{\mathbf{a}}(\mathbf{v}) = f(\mathbf{v}) + \mathbf{a} \cdot \mathbf{v} + b_{\mathbf{a}}$, удовлетворяющей (7): $\widehat{F}_{\mathbf{a}}(\mathbf{0}) = n - 2d$, где $\mathbf{a}$ — вектор длины m, а $b_{\mathbf{a}}$ равно 0 или 1 (см. (6)). Из определения максимально нелинейной функции и соотношения (3) следует, что

$$\widehat{F}_{\mathbf{a}}(\mathbf{u}) = \begin{cases} n - 2d, & \text{если } d(\mathbf{f}_{\mathbf{a}}, \mathbf{g}) = d, \\ -n + 2d, & \text{если } d(\mathbf{f}_{\mathbf{a}}, \mathbf{g}) = n - d. \end{cases}$$

По лемме 2 для любого ненулевого вектора $\mathbf{u}$ длины m выполняется

$$\sum_{\mathbf{a} \in E^m} \widehat{F}_{\mathbf{a}}(\mathbf{u}) = 0,$$

откуда вытекает, что расстояния d и $n - d$ между вектором $\mathbf{g}$ и векторами веса d смежного класса $\mathbf{f} + R(1,m)$ встречаются одинаково часто, а именно по $n/2$ раз. Умножая это число на число $(n-2)/2$ нетривиальных смежных классов по коду $R(1,m)$, получаем $\delta^{d}_{n/2,d} \equiv n(n-2)/4$. $\square$

Лемма 8. *Выполняются тождества* $\delta^{d}_{dd} \equiv (n-d)(n-4)/2$, $\delta^{n-d}_{dd} \equiv d(n-4)/2$.

Доказательство. Пусть $\mathbf{g}$ — произвольное кодовое слово кода Кердока веса d. Рассмотрим максимально нелинейную квадратичную функцию f от m переменных такую, что соответствующий ей вектор $\mathbf{f}$ содержится в коде Кердока, а вектор $\mathbf{g}$ не принадлежит смежному классу $\mathbf{f} + R(1,m)$. Множество векторов веса d смежного класса $\mathbf{f} + R(1,m)$ описывается с помощью максимально нелинейных функций $f_{\mathbf{a}}(\mathbf{v}) = f(\mathbf{v}) + \mathbf{a} \cdot \mathbf{v} + b_{\mathbf{a}}$, удовлетворяющих (7): $\widehat{F}_{\mathbf{a}}(\mathbf{0}) = n - 2d$, напомним, что здесь $\mathbf{a}$ так же, как и выше, является вектором длины m, а $b_{\mathbf{a}}$ принимает значение 0 или 1 (см. (6)). Обозначим $h(\mathbf{v}) = g(\mathbf{v}) + f(\mathbf{v})$. Согласно определению кода Кердока функция h является максимально нелинейной. Пусть

$$H(\mathbf{v}) = (-1)^{h(\mathbf{v})}.$$

Покажем, что

$$(-1)^{b_{\mathbf{a}}} \widehat{H}(\mathbf{a}) = \begin{cases} n - 2d, & \text{если } d(\mathbf{g}, \mathbf{f}_{\mathbf{a}}) = d, \\ -n + 2d, & \text{если } d(\mathbf{g}, \mathbf{f}_{\mathbf{a}}) = n - d. \end{cases} \tag{16}$$

Действительно, имеем

$$d(\mathbf{g},\mathbf{f_a}) = d\left(\mathbf{g},\mathbf{f}+\sum_{i=1}^{m} a_i\mathbf{v}^i + b_{\mathbf{a}}\cdot\mathbf{1}\right) = d\left(\mathbf{h},\sum_{i=1}^{m} a_i\mathbf{v}^i + b_{\mathbf{a}}\cdot\mathbf{1}\right).$$

Для значения $\widehat{H}(\mathbf{a})$ воспользуемся формулами (3) при $b_{\mathbf{a}} = 0$ и (4) при $b_{\mathbf{a}} = 1$. Поскольку функция h максимально нелинейна, расстояние $d\left(\mathbf{h},\sum\limits_{i=1}^{m} a_i\mathbf{v}^i + b_{\mathbf{a}}\cdot\mathbf{1}\right)$ может принимать лишь два значения: d и $n-d$, откуда следует равенство (16).

Используя формулу (2) для дискретного преобразования Фурье, представим левую часть равенства (16) в виде

$$(-1)^{b_{\mathbf{a}}}\sum_{\mathbf{v}\in E^m}(-1)^{\mathbf{a}\cdot\mathbf{v}}H(\mathbf{v}).$$

Подставляя $H(\mathbf{v}) = (-1)^{g(\mathbf{v})}F(\mathbf{v})$ и используя $F(\mathbf{v}) = (-1)^{\mathbf{a}\cdot\mathbf{v}+b_{\mathbf{a}}}F_{\mathbf{a}}(\mathbf{v})$ (см. (8)), получаем

$$\sum_{\mathbf{v}\in E^m}(-1)^{g(\mathbf{v})}F_{\mathbf{a}}(\mathbf{v}).$$

Таким образом, из соотношения (16) следует равенство

$$\frac{1}{n-2d}\sum_{\mathbf{v}\in E^m}(-1)^{g(\mathbf{v})}F_{\mathbf{a}}(\mathbf{v}) = \begin{cases} 1, & \text{если } d(\mathbf{g},\mathbf{f_a}) = d,\\ -1, & \text{если } d(\mathbf{g},\mathbf{f_a}) = n-d. \end{cases} \tag{17}$$

По определению кода Кердока функция $g+f_{\mathbf{a}}$ для любого вектора $\mathbf{a}$ является максимально нелинейной, поэтому вес каждого вектора $\mathbf{g}+\mathbf{f_a}$ равен d или $n-d$. Отсюда следует, что расстояние между векторами $\mathbf{g}$ и $\mathbf{f_a}$ принимает два возможных значения: d и $n-d$. Обозначим через $\mu_{d,f}(\mathbf{g})$ и $\mu_{n-d,f}(\mathbf{g})$ количества векторов $\mathbf{f_a}$, находящихся на расстояниях d и $n-d$ соответственно от вектора $\mathbf{g}$. Так как число всех векторов $\mathbf{f_a}$ равно n, то выполняется равенство

$$\mu_{d,f}(\mathbf{g}) + \mu_{n-d,f}(\mathbf{g}) = n.$$

Суммируя обе части равенства (17) по всем векторам $\mathbf{a}$ длины m и применяя лемму 3, получаем соотношение

$$\mu_{d,f}(\mathbf{g}) - \mu_{n-d,f}(\mathbf{g}) = \frac{n}{n-2d}.$$

Решая систему из последних двух уравнений и подставляя $d = (n-\sqrt{n})/2$, имеем

$$\mu_{d,f}(\mathbf{g}) = n-d, \quad \mu_{n-d,f}(\mathbf{g}) = d.$$

Заметим, что полученные значения не зависят от выбора кодового слова $\mathbf{g}$ веса d и максимально нелинейной квадратичной функции f такой, что смежный класс $\mathbf{f}+R(1,m)$ не содержит вектора $\mathbf{g}$. Для фиксированного кодового слова $\mathbf{g}$ веса d число смежных классов кода Кердока по коду Рида — Маллера первого порядка, не содержащих $\mathbf{g}$ и отличных от $R(1,m)$, равно $(n-4)/2$. Поскольку расстояние от кодового слова $\mathbf{g}$ до любого вектора из смежного класса $\mathbf{g}+R(1,m)$, которому слово $\mathbf{g}$ принадлежит, не равно d и $n-d$, заключаем, что

$$\delta_{dd}^{d}(\mathbf{g}) = \mu_{d,f}(\mathbf{g})(n-4)/2, \quad \delta_{dd}^{n-d}(\mathbf{g}) = \mu_{n-d,f}(\mathbf{g})(n-4)/2.$$

Подставляя значения функций $\mu_{d,f}$ и $\mu_{n-d,f}$, получаем искомые тождества для δ_{dd}^{d} и δ_{dd}^{n-d}. $\square$

Теорема 1. *Произвольный код Кердока длины $n = 2^m$ для любого четного $m \geq 4$ является дистанционно регулярным.*

Доказательство. Нетрудно заметить, что, используя леммы 6–8, свойства (10)–(13) функций δ_{ij}^k и формулы (14), (15), можно показать, что каждая функция δ_{ij}^k при параметрах i, j, k из множества $\{d, n/2, n-d\}$ тождественно равна константе, а именно

$$\delta_{dd}^d \equiv \delta_{n-d,n-d}^d \equiv \delta_{d,n-d}^{n-d} \equiv \delta_{n-d,d}^{n-d} \equiv (n-d)(n-4)/2,$$

$$\delta_{d,n-d}^d \equiv \delta_{n-d,d}^d \equiv \delta_{d,d}^{n-d} \equiv \delta_{n-d,n-d}^{n-d} \equiv d(n-4)/2,$$

$$\delta_{n/2,d}^d \equiv \delta_{n/2,n-d}^d \equiv \delta_{n/2,d}^{n-d} \equiv \delta_{n/2,n-d}^{n-d} \equiv n(n-2)/4,$$

$$\delta_{n/2,n/2}^d \equiv \delta_{d,n/2}^{n/2} \equiv \delta_{n/2,d}^{n/2} \equiv \delta_{n/2,n-d}^{n/2} \equiv \delta_{n-d,n/2}^{n/2} \equiv \delta_{n/2,n/2}^{n-d} \equiv 0, \quad \delta_{n/2,n/2}^{n/2} = 2n-4,$$

$$\delta_{d,n/2}^d \equiv \delta_{n-d,n/2}^d \equiv \delta_{dd}^{n/2} \equiv \delta_{d,n-d}^{n/2} \equiv \delta_{n-d,d}^{n/2} \equiv \delta_{n-d,n-d}^{n/2} \equiv \delta_{d,n/2}^{n-d} \equiv \delta_{n-d,n/2}^{n-d} \equiv n-1,$$

и не зависит от выбора кода Кердока длины n. Отсюда и из лемм 4, 5 следует дистанционная регулярность произвольного кода Кердока. $\square$

Коды Кердока образуют бесконечный класс дистанционно регулярных кодов, весовой спектр которых имеет более трех (а именно пять) ненулевых значений.

Более слабым свойством кода по сравнению с дистанционной регулярностью является свойство *сильной дистанционной инвариантности*: число пар кодовых слов $\mathbf{x}$, $\mathbf{y}$ таких, что $d(\mathbf{x}, \mathbf{y}) = k$ и $d(\mathbf{x}, \mathbf{z}) = i$, $d(\mathbf{y}, \mathbf{z}) = j$ для любого кодового слова $\mathbf{z}$, зависит только от чисел i, j, k и не зависит от выбора $\mathbf{z}$.

Следствие 1. *Произвольный код Кердока длины $n = 2^m$ для любого четного $m \geq 4$ является сильно дистанционно инвариантным.*

Заметим, что согласно работе А. Ю. Васильевой [20] все двоичные совершенные коды с кодовым расстоянием 3 обладают свойством сильной дистанционной инвариантности, не будучи при этом ввиду [7] дистанционно регулярными.

§ 5. Комментарии

Приведем несколько соображений относительно методов исследования дистанционной регулярности (нерегулярности) различных кодов.

1. Для исследования дистанционной регулярности произвольного приведенного (т. е. содержащего нулевой вектор) кода иногда полезно использовать информацию о различных группах преобразований, переводящих код в себя. *Группа автоморфизмов* $\mathrm{Aut}(C)$ кода C длины n состоит из всех изометрий пространства E^n (комбинаций подстановок на n координатах и сдвигов на векторы из E^n), оставляющих код на месте. Код C называется *транзитивным*, если группа $\mathrm{Aut}(C)$ действует транзитивно на множестве его кодовых слов. Подгруппа $\mathrm{Sym}(C)$ группы $\mathrm{Aut}(C)$, отвечающая всем подстановкам на n координатах со сдвигом на нулевой вектор, называется *группой симметрий* кода C. Согласно [9] справедливо

Утверждение 6. *Если группа* $\mathrm{Sym}(C)$ *транзитивного кода* C *действует транзитивно на каждом множестве кодовых слов одного веса, то код* C *дистанционно регулярен.*

2. Укажем обобщение леммы 4. Для приведенного кода C длины n пусть $\delta_{ij}^k(\mathbf{x})$ обозначает, как и в § 4, число кодовых слов веса j, находящихся на расстоянии k от кодового слова $\mathbf{x}$ веса i.

Утверждение 7. *Пусть для любого кодового слова* $\mathbf{x}$ *кода* C *длины* n *при всех допустимых значениях* i, j, k *все функции* δ_{ij}^k *для кода* $\mathbf{x}+C$ *тождественно равны константам* c_{ij}^k, *зависящим от* i, j, k, n *и не зависящим от* $\mathbf{x}$. *Тогда код* C *дистанционно регулярен.*

3. Для доказательства дистанционной нерегулярности кода можно воспользоваться свойством (11) функций δ_{ij}^k. Предполагая, что функции δ_{ij}^k тождественно равны константам, иногда удается показать (см., например, [7–9]), что какое-либо из равенств $A_i\delta_{ij}^k = A_j\delta_{ji}^k$, где A_i, A_j обозначают соответствующие значения весового спектра приведенного кода, не выполняется ни при каком целом значении функции δ_{ij}^k.

Результаты статьи анонсированы в [21]. Авторы считают своим приятным долгом выразить благодарность П. Шарпан, Г. М. Керигян и К. Баю за полезные дискуссии.

ЛИТЕРАТУРА

1. *Delsarte P.* An algebraic approach to the association schemes of coding theory // Philips Res. Rep. Suppl. 1973. N 10.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. *Brouwer A. E., Cohen A. M., Neumaier A.* Distance-regular graphs. Berlin: Springer–Verl., 1989.
4. *Баннаи Э., Ито Т.* Алгебраическая комбинаторика. Схемы отношений. М.: Мир, 1987.
5. *Levenshtein V. I.* Universal bounds for codes and designs // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. V. 1. P. 499–648.
6. *Topalova S. T.* Distance regularity of some linear codes // Abstracts of the Annual Workshop on Algebraic and Combinatorial Coding Theory, P. 18.
7. *Августинович С. В., Соловьева Ф. И.* О дистанционной регулярности совершенных двоичных кодов // Пробл. передачи информ. 1998. Т. 34, № 3. С. 47–49.
8. *Августинович С. В., Соловьева Ф. И.* Новые конструкции и свойства совершенных кодов // Тр. Междунар. конф. «Дискретный анализ и исследование операций». Новосибирск: Изд-во Ин-та математики СО РАН, 2000. С. 5–10.
9. *Соловьева Ф. И., Токарева Н. Н.* О дистанционной нерегулярности кодов Препараты // Сиб. мат. журн. 2007. Т. 48, № 2. С. 408–416.
10. *Сидельников В. М.* Об экстремальных многочленах, используемых при оценках мощности кода // Пробл. передачи информ. 1980. Т. 16, № 3. С. 17–30.
11. *Kerdock A. M.* A class of low-rate non-linear binary codes // Inform. Control. 1972. V. 20, N 2. P. 182–187.
12. *Kantor W. M.* An exponential number of generalized Kerdock codes // Inform. Control. 1982. V. 53, N 1–2. P. 74–80.
13. *Нечаев А. А.* Код Кердока в циклической форме // Дискр. математика. 1989. Т. 1, № 4. С. 123–139.
14. *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, N 2. P. 301–319.
15. *Zhe-Xian Wan.* Quaternary codes. Singapore: World Sci. Publ. Co. Pte. Ltd, 1997.
16. *Nordstrom A. W., Robinson J. P.* An optimum nonlinear code // Inform. Control. 1967. V. 11, N 5–6. P. 613–616.

17. *Kantor W. M.* Codes, quadratic forms and finite geometries // Proc. Sympos. Appl. Math. 1995. V. 50. P. 153–177.
18. *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.
19. *Kantor W. M., Williams M. E.* Symplectic semifield planes and $\mathbb{Z}_4$-linear codes // Trans. Amer. Math. Soc. 2004. V. 356, N 3. P. 895–938.
20. *Васильева А. Ю.* Сильная дистанционная инвариантность совершенных двоичных кодов // Дискр. анализ и исслед. операций. Сер. 1. 2002. Т. 9, № 4. С. 33–40.
21. *Solov'eva F. I., Tokareva N. N.* On the property of distance regularity of Kerdock and Preparata codes // Proc. Tenth intern. workshop on algebraic and combinatorial coding theory, 3–9 September 2006. Zvenigorod, Russia. Moscow: IITP, 2006. P. 248–251.

Статья поступила 30 мая 2006 г.

Соловьева Фаина Ивановна, Токарева Наталья Николаевна
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
`sol@math.nsc.ru`, `tokareva@math.nsc.ru`