S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 7, стр. 372–382 (2010) УДК 519.14, 519.174.7
MSC 05B15, 05C15

О СОВЕРШЕННЫХ РАСКРАСКАХ БУЛЕВА n-КУБА И КОРРЕЛЯЦИОННО-ИММУННЫХ ФУНКЦИЯХ МАЛОЙ ПЛОТНОСТИ

В. Н. ПОТАПОВ

Abstract. A coloring of Boolean n-cube is called perfect if, for every vertex, the collection of colors of its neighbors depends only on its own color. Parameters of a perfect coloring are given by an array. A Boolean function is called correlation immune of degree $n-m$ if it takes the value 1 equal number of times on any m-face of Boolean n-cube. It is proved that Boolean function χ^S $(S \subset E^n)$ is a perfect coloring if it satisfies the equality $\rho(S) = 1 - \frac{n}{2(1+\mathrm{cor}(S))}$, where $\mathrm{cor}(S)$ is the maximum degree of the correlation immune of χ^S and $\rho(S) = |S|/2^n$.

It is offered a straightforward concatenative construction for a perfect coloring of Boolean n-cube with array $\begin{matrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{matrix}$. This construction provides a new lower bound on the number of such perfect colorings. Also we give an upper bound for this number. We find the cardinality of the minimal component of perfect coloring with these parameters and prove that any minimal component of such perfect coloring is linear.

Keywords: hypercube, perfect coloring, perfect code, MDS code, correlation-immune function, component.

посвящается памяти Дмитрия Германовича Фон-Дер-Флааса

Potapov, V.N., On perfect colorings of Boolean n-cube and correlation immune functions with small density.

Работа поддержана РФФИ (гранты 10-01-00424-а, 10-01-00616-а).

Поступила 30 июля 2010 г., опубликована 4 ноября 2010 г.

1. Основные определения и результаты

Обозначим через E^n множество упорядоченных двоичных наборов (вершин) длины n. Булев n-куб E^n естественным образом наделяется структурой векторного пространства над полем $GF(2)$. Введём операцию $[x, y] = (x_1y_1, \ldots, x_ny_n)$ и внутреннее произведение $\langle x, y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n$ векторов $x, y \in E^n$. Количество единиц в наборе $y \in E^n$ называется *весом набора* и обозначается через $wt(y) = \langle y, \overline{1}\rangle$. *Гранью размерности* $n - wt(y)$ называется множество $E^n_y(z) = \{x \in E^n : [x, y] = [z, y]\}$.

Пусть $S \subset E^n$, через χ^S будем обозначать характеристическую функцию множества S. Функция χ^S называется *корреляционно-иммунной порядка* $n-m$, если для любой грани $E^n_y(z)$ размерности m пересечения $E^n_y(z)\cap S$ имеют одинаковую мощность. Через $\mathrm{cor}(S)$ будем обозначать максимальный порядок корреляционной иммунности, $\mathrm{cor}(S) = \max\{n - m\}$. *Плотностью* булевой функции χ^S будем называть отношение $\rho(S) = |S|/2^n$. Для корреляционно-иммунной функции χ^S будем всегда считать, что $\rho(S) \leq 1/2$, поскольку $\mathrm{cor}(S) = \mathrm{cor}(E^n \setminus S)$ и в случае $\rho(S) > 1/2$ можно перейти от рассмотрения множества S к его дополнению $E^n \setminus S$. Если $\rho(S) = 1/2$, то корреляционно-иммунную функцию χ^S называют *уравновешенной*.

Расстоянием Хэмминга $d(x, y)$ между вершинами $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ называется число позиций, в которых наборы x и y различаются. Множество вершин, которые находятся от вершины x на расстоянии не более d, называется *шаром* радиуса d с центром в x. *Сферой* радиуса 1 с центром в вершине x называется множество $F(x) = \{y \in E^n : d(x, y) = 1\}$.

Совершенной раскраской булева n-куба в k цветов называется отображение $Col : E^n \to \{1, \ldots, k\}$, удовлетворяющее следующему условию: мощность пересечения $|Col^{-1}(i)\cap F(x)|$ зависит только от цветов i и $Col(x)$, но не от вершины $x \in E^n$. Отметим, что в определении совершенной раскраски сферу можно заменить на шар. Каждой совершенной раскраске соответствует матрица параметров $A = \{a_{ij}\}$, где a_{ij} — число вершин цвета j в сфере радиуса 1 с центром в вершине цвета i. В дальнейшем речь пойдёт только о раскрасках в два цвета, причём для удобства изложения будем считать, что множество цветов есть $\{0, 1\}$. В этом случае функция Col является булевозначной и $Col = \chi^S$, где S — множество вершин цвета 1. *Совершенный код* $C \subset E^n$ можно определить как совершенную раскраску χ^C с матрицей параметров вида $A = \begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$. Раскраски с такими параметрами существуют только при $n = 2^m - 1$ (m — натуральное). Перечисление матриц параметров совершенных раскрасок булева n-куба в 2 цвета и соответствующие конструкции имеются в [1] и [2].

Известно, (см., например, [3, 5]), что совершенная раскраска булева n-куба с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ является корреляционно-иммунной функцией порядка $\frac{b+c}{2} - 1$. Т. е. из регулярной распределённости вершин некоторого множества по шарам радиуса 1 следует равномерная распределение вершин этого множества по граням. Более интересным представляется выяснение возможности обратного следствия.

В [3] доказано, что для любой неуравновешенной неконстантной корреляционно-иммунной функции χ^S ($S \subset E^n$) справедливо неравенство $\mathrm{cor}(S) \leq \frac{2n}{3} - 1$.

Более того, в случае равенства $\operatorname{cor}(S) = \frac{2n}{3} - 1$ функция χ^S является совершенной раскраской. Таким образом, из равномерной распределённости по граням размерности $\frac{n}{3} + 1$ вершин множества S следует регулярная, зависящая только от цвета центра шара, распределённость по шарам радиуса 1.

Для любой булевой[1] функции χ^S ($S \subset E^n$) справедливо неравенство Биербрауэра — Фридмана ([6, 7]) $\rho(S) \geq 1 - \frac{n}{2(1+\operatorname{cor}(S))}$. Это неравенство даёт следующую оценку корреляционной иммунности

$$\operatorname{cor}(S) \leq \frac{n}{2(1-\rho(S))} - 1. \tag{1}$$

Ниже будет доказано, что если в соотношении (1) имеет место равенство, то χ^S — совершенная раскраска. В частности, при $n = k(2^s - 1)$ (k, s — натуральные), $\operatorname{cor}(S) = k2^{s-1} - 1$ и $\rho(S) = 2^{-s}$ корреляционно-иммунная функция χ^S ($S \subset E^n$) достигает границы (1) и является совершенной раскраской с матрицей параметров

$$\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}. \tag{2}$$

Для совершенных кодов (при $k = 1$) аналогичное утверждение было ранее доказано в [8]. А именно, если $\operatorname{cor}(S) = \operatorname{cor}(H)$ и $\rho(S) = \rho(H)$, где $S, H \subset E^n$ и H — совершенный код, то S — совершенный код.

В [4] посредством некоторой рекуррентной конструкции получены нижние оценки на число совершенных раскрасок булева n-куба, в частности, с матрицами параметров вида (2). А именно, доказано неравенство

$$N(k,s) \geq \prod_{i=0}^{s-1} 2^{2^{k(2^i-1)-i}},$$

где $N(k,s)$ — число различных раскрасок с параметрами (2).

В § 4 предложена прямая конструкция совершенных раскрасок с параметрами (2), которая при $k = 1$ совпадает с конструкцией совершенных кодов из [9]. С помощью предлагаемой конструкции улучшена нижняя оценка числа раскрасок с этими параметрами:

$$N(k,s) \geq 2^{2^{k(2^{s-1}-1)-s+1}} \cdot 3^{k2^{k(2^{s-2}-1)}} \cdot 2^{2^{k(2^{s-2}-1)-s+2}}. \tag{3}$$

Отметим, что при $k = 1$ оценка (3) совпадает с ранее известной оценкой числа совершенных кодов (см. [10]). Лучшая на сегодня нижняя оценка числа совершенных кодов получена в [11] с помощью другой конструкции. В § 3 получена также верхняя оценка

$$N(k,s) \leq k2^s 2^{k2^s - s - k}. \tag{4}$$

Компонентой совершенной раскраски χ^S булева n-куба E^n называется такое множество $C \subset S$, что для некоторого множества $C' \subset E^n \setminus C$ функция $\chi^{(S \cap C') \setminus C}$ является совершенной раскраской с теми же параметрами, что и χ^S. Проще говоря, подмножество $C \subset S$ можно заменить на C' без изменения свойств раскраски χ^S.

[1] Биербрауэр обобщил неравенство Фридмана на q-значный n-куб, где q — произвольное натуральное число.

В § 2 показано, что мощность компоненты совершенной раскраски χ^S с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ не может быть меньше $2^{\mathrm{cor}(S)} = 2^{\frac{b+c}{2}-1}$. Кроме того, если компонента C имеет минимальную возможную мощность, то она является аффинным подмножеством булева n-куба (*линейным кодом*). В случае совершенного кода данное утверждение было доказано ранее С.В.Августиновичем. Для совершенных раскрасок с параметрами вида (4) в § 4 будет предложена явная конструкция компонент минимальной мощности.

2. Свойства совершенных раскрасок и корреляционно-имунных функций

Множество функций $a : E^n \to \mathbb{Q}$ можно рассматривать как 2^n-мерное векторное пространство $\mathbb{V}$ над $\mathbb{Q}$. Известно, что функции вида $f^v(u) = (-1)^{\langle u,v\rangle}$, $v \in E^n$, составляют ортогональный базис пространства $\mathbb{V}$. *Преобразованием Фурье* функции a называется функция $\widehat{a}$, значения которой

$$\widehat{a}(v) = \sum_{u\in E^n} a(u)(-1)^{\langle u,v\rangle}$$

являются скалярными произведением векторов a и f^v в $\mathbb{V}$. Поскольку $\langle f^v, f^v\rangle = 2^n$ для любой вершины $v \in E^n$, имеем равенства

$$a(u) = \frac{1}{2^n}\sum_{v\in E^n} \widehat{a}(v)(-1)^{\langle u,v\rangle}, \qquad \text{(формула обращения)} \tag{5}$$

$$2^n \sum_{u\in E^n} a^2(u) = \sum_{v\in E^n} \widehat{a}^2(v). \qquad \text{(равенство Парсеваля)} \tag{6}$$

Нам понадобятся несколько известных утверждений.

Предложение 1. *(см.* [5, 12]*) Булева функция $a = \chi^S$ является корреляционно-иммунной порядка m тогда и только тогда, когда $\widehat{a}(v) = 0$ при любых $v \in E^n$ таких, что $0 < wt(v) \le m$.*

Предложение 2. *(см.* [1]*)*

(a) *Пусть $a = \chi^S$ — совершенная раскраска с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$, тогда $\widehat{a}(v) = 0$ при любых $v \in E^n$, таких что $wt(v) \ne 0, \frac{b+c}{2}$.*

(b) *Пусть булева функция $a = \chi^S$ такова, что $\widehat{a}(v) = 0$ при любых $v \in E^n$, $wt(v) \ne 0, k$, тогда a является совершенной раскраской.*

Известно, что любую булеву функцию $a = \chi^S$ можно представить в *алгебраической нормальной форме* (*полиномом Жегалкина*). Через $\deg(S)$ будем обозначать максимальную степень этого полинома.

Предложение 3. *(см.* [5, 12]*) (неравенство Зигенталлера) Для любой булевой функции $a = \chi^S$ справедливо неравенство* $\deg(S) + \mathrm{cor}(S) \le n$.

Предложение 4. *(см.* [13]*) Для любой булевой функции $a = \chi^S$ справедливо неравенство $|S| \ge 2^{n-\deg(S)}$. Если $|S| = 2^{n-\deg(S)}$, то множество S — линейный код.*

Следствие 1. *Пусть $a = \chi^S$ — совершенная раскраска с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$, тогда $\operatorname{cor}(S) = \frac{b+c}{2} - 1$, $\deg(S) \le n - \frac{b+c}{2} + 1$ и мощность компоненты совершенной раскраски $a = \chi^S$ не может быть меньше $2^{\operatorname{cor}(S)} = 2^{\frac{b+c}{2}-1}$. Более того, компонента мощности $2^{\frac{b+c}{2}-1}$ является линейным кодом.*

Поскольку количество мономов степени не более m равняется $\sum\limits_{i=0}^{m} \binom{n}{i}$, из следствия 1 имеем верхнюю оценку числа совершенных раскрасок.

Следствие 2. *Число совершенных раскрасок с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ не превышает $2^{\sum\limits_{i=0}^{m} \binom{n}{i}}$, где $m = n - \frac{b+c}{2} + 1$.*

Предложение 5. *(см. [5, 6, 7]) (неравенство Биербрауэра — Фридмана) Для любой булевой функции χ^S справедливо неравенство $\rho(S) \ge 1 - \frac{n}{2(1+\operatorname{cor}(S))}$.*

Ниже будет показано, что если для некоторой булевой функции χ^S в неравенстве Биербрауэра — Фридмана достигается равенство, то функция χ^S является совершенной раскраской.

Пусть $a = \chi^S$ — некоторая булева функция. Введём обозначение $a'(v) = \widehat{a}(v)/|S|$. Из (6) имеем

$$\sum_{v \in E^n} (a'(v))^2 = \frac{2^n}{|S|^2} \sum_{u \in E^n} a^2(u) = 2^n/|S|. \tag{7}$$

Наборы $(A_0(a), \dots, A_n(a))$ и $(A'_0(a), \dots, A'_n(a))$, где $A_i(a) = \sum\limits_{wt(u)=i} a(u)$ и $A'_i(a) = \sum\limits_{wt(v)=i} a'(v)$, называются соответственно весовым распределением кода a и весовым распределением дуального к a кода, второе — в случае когда a — характеристическая функция линейного кода (аффинного подмножества) в E^n.

Справедливы равенства

$$A'_k(a) = \frac{1}{|S|} \sum_{wt(v)=k} \sum_{u \in E^n} a(u)(-1)^{\langle u,v \rangle} = \frac{1}{|S|} \sum_{u \in E^n} a(u) \sum_{wt(v)=k} (-1)^{\langle u,v \rangle} =$$

$$= \frac{1}{|S|} \sum_{i=0}^{n} A_i(a) P_k(i), \tag{8}$$

где сумма $P_k(i) = \sum\limits_{wt(v)=k} (-1)^{\langle u,v \rangle}$ зависит только от веса $wt(u) = i$ вектора $u \in E^n$. Известно (см, например, [12], [13]), что величины $P_k(i)$ являются значениями в целых точках *полиномов Кравчука*. Аналогично имеем

$$A_k(a) = \frac{|S|}{2^n} \sum_{i=0}^{n} A'_i(a) P_k(i). \tag{9}$$

Для произвольной булевой функции $a = \chi^S$ определим *весовое распределение*

$(B_0(a), \dots, B_n(a))$, где

$$B_i(a) = \frac{1}{|S|}|\{v, u \in S \mid wt(u+v) = i\}|.$$

Нетрудно видеть, что $\sum\limits_{i=0}^{n} B_i(a) = |S|$ и $B_i(a) = A_i(a)$, если a — характеристическая функция линейного кода S и $\overline{0} \in S$.

Преобразованием Мак-Вильямс набора $(B_0(a), \dots, B_n(a))$ называется набор $(B'_0(a), \dots, B'_n(a))$, где $B'_k(a) = \frac{1}{|S|} \sum\limits_{i=0}^{n} B_i(a) P_k(i)$. Как видно из (8) и (9) преобразование Мак-Вильямс (как линейное отображение в $\mathbb{Q}^{n+1}$) обратимо, причём

$$B_k(a) = \frac{|S|}{2^n} \sum_{i=0}^{n} B'_i(a) P_k(i). \tag{10}$$

В [13] доказано равенство

$$B'_k(a) = \sum_{wt(v)=k} (a'(v))^2 \tag{11}$$

и из равенств (7) и (11) получены следующие следствия.

Следствие 3. *Пусть $\overline{0} \in S$ и $a = \chi^S$, тогда*
(a) $B'_k(a) \geq 0$ *при* $i = 0, \dots, n$;
(b) $B'_k(a) = 0 \Leftrightarrow a'(v) = 0$ *для любой вершины* $v \in E^n$ *веса* $wt(v) = k$;
(c) $B'_0(a) = 1$;
(d) $\sum\limits_{i=0}^{n} B'_k(a) = 2^n/|S|$.

Используя предложения 1 и 2 и следствие 3 (b), нетрудно получить нужные нам формулировки следующих известных (см., например, [3] и [8]) утверждений.

Следствие 4. *Пусть $\overline{0} \in S$ и $a = \chi^S$, тогда $B'_k(a) = 0$ при $0 < k \leq \operatorname{cor}(S)$.*

Следствие 5. *Пусть $\overline{0} \in S$ и $a = \chi^S$ и $B'_i(a) = 0$ при $i \neq 0, k$. Тогда χ^S — совершенная раскраска.*

Приведённое ниже доказательство фактически повторяет рассуждения из [6] и [8].

Следствие 6. *Если для булевой функции $a = \chi^S$, где $S \subset E^n$ и $\rho(S) \leq 1/2$, справедливо равенство $\rho(S) = 1 - \frac{n}{2(1+\operatorname{cor}(S))}$, то χ^S — совершенная раскраска.*

Доказательство. Без ограничения общности считаем, что $\overline{0} \in S$. Пусть $t = \operatorname{cor}(S)$. Из условия имеем

$$n = (2(t+1) - n)\left(\frac{1}{\rho(S)} - 1\right) \tag{12}$$

Из равенства (10), следствия 3(c) и следствия 4 имеем

$$B_1(a)/\rho(S) = P_1(0) + \sum_{i=t+1}^{n} B'_i(a) P_1(i).$$

Поскольку $B_1(a) \geq 0$ и $P_1(i) = n - 2i$ (см., [8] или [12]), получаем неравенство

$$0 \leq n + \sum_{i=t+1}^{n} B'_i(a)(n-2i).$$

Из следствия 3 (a),(c),(d) имеем $\sum\limits_{i=1}^{n} B'_k(a) = \left(\frac{1}{\rho(S)} - 1\right)$ и $B'_k(a) \geq 0$. Ясно, что равенство (12) возможно только в случае, когда $B'_i(a) = 0$ при $i \geq t+2$. Тогда из следствия 5 следует, что χ^S — совершенная раскраска. ▲

Из доказательства следствия 6 видно, что равенство (12) достигается только в случае $B_1(a) = 0$, т. е. когда матрица параметров совершенной раскраски χ^S имеет вид $\begin{pmatrix} 0 & n \\ c & n-c \end{pmatrix}$. В [3] предложены конструкции совершенных раскрасок с параметрами (2), а также раскраски с параметрами $c = 3, b = n = 13$ и $c = 3, b = n = 29$. Тем самым показано, что имеются корреляционно-иммунные функции χ^S, достигающие границы (1) (т. е. удовлетворяющие равенству 12)) при $\rho(S) = \frac{1}{2^s}$, s — натуральное, $\rho(S) = \frac{3}{16}$ и $\rho(S) = \frac{3}{32}$.

Нетрудно видеть, что для булевой функции $a = \chi^S$ ($S \subset E^n$) величина $\rho(S)$ может принимать значения вида только $k/2^n$. В [1] показано, что если $\rho(S) \neq 1/2$, то $\mathrm{cor}(S) \leq \frac{2n}{3} - 1$, т. е. равенство в неравенстве Биербрауэра — Фридмана (1) может быть достигнуто только при $\rho(S) \leq 1/4$. Вопрос о возможности достижения границы (1) при любых двоично-рациональных значениях плотности $\rho \in (0, \frac{1}{4})$ остаётся открытым.

3. Верхняя оценка числа совершенных раскрасок

Как и ранее через $N(k,s)$ обозначаем число различных совершенных раскрасок булева n-куба с матрицей параметров $\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}$. При минимальном значении $s = 1$ совершенная раскраска с такой матрицей параметров является счётчиком чётности и $N(k,s) = 2$. Из следствия 2 имеем

$$\log N(k,s) \leq 2^{nh\ \frac{2^{s-1}-1}{2^s-1}\ (1+o(1))} \tag{13}$$

при $s \geq 2$, $n = k(2^s-1) \to \infty$, где $h(p) = -p\log p - (1-p)\log(1-p)$ — энтропия Шеннона.

Докажем другую верхнюю оценку на число совершенных раскрасок булева n-куба. Идея доказательства этой оценки взята из [2].

Теорема 1. *Пусть $N(k,s)$ — число различных совершенных раскрасок с матрицей параметров $\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}$. Тогда $\ln N(k,s) \leq 2^{k2^s-2k-s}k^2(k+s)(1+o(1))$ при $n = k(2^s-1) \to \infty$.*

Доказательство. Пусть χ^S — совершенная раскраска с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. Вычислив количество пар соседних вершин разных цветов (0 и 1), нетрудно видеть, что $|S| = \frac{c}{b+c}2^n$. Отметим, что $b + c = c'2^t$, где c' — нечётный делитель числа c. Определим функцию $a(u) = \begin{cases} b & \text{при } u \in S; \\ -c & \text{при } u \notin S, \end{cases}$ т. е. $a = b\chi^S - c(1-\chi^S) = (b+c)\chi^S - c$. Тогда $\widehat{a}(\overline{0}) = 0$ по построению. Из предложения 2(a) и определения функции a имеем равенство

$\widehat{a}(v) = 0$ для любых $v \in E^n$ веса $wt(v) \neq 0, \frac{b+c}{2}$. Из равенства Парсеваля (6) имеем

$$\sum_{wt(v)=\frac{b+c}{2}} \widehat{a}^2(v) = 2^n \left(b^2 \frac{c}{b+c} 2^n + c^2 \frac{b}{b+c} 2^n \right). \tag{14}$$

Зафиксируем вершину $w \in E^n$, $wt(w) = (b+c)/2$ и возьмём содержащую $\overline{0}$ грань E размерности $l = n - (b+c)/2$, т. е. $E = E_w^n(\overline{0}) = \{x \in E^n \mid [x, w] = \overline{0}\}$. Ясно, что скалярное произведение векторов $f^v(u) = (-1)^{\langle u,v\rangle}$ и χ^E в $\mathbb{V}$ равно 0, если $v \neq w$ и $wt(v) = (b+c)/2$. Рассмотрим скалярное произведение векторов a и χ^E в $\mathbb{V}$. Из формулы обращения (5) имеем

$$\widehat{a}(w)2^{l-n} = \langle a(u), \chi^E(u)\rangle = bm(w) - c(2^l - m(w)) = (b+c)m(w) - c2^l, \tag{15}$$

где $m(w) = |S \cap E_w^n(\overline{0})|$. Очевидно, что числа $\widetilde{a}(w) = \widehat{a}(w)2^{l-n-t}$ целые для любой вершины $w \in E^n$, $wt(w) = (b+c)/2$. Из (14) имеем

$$\sum_{wt(v)=\frac{b+c}{2}} \widetilde{a}^2(v) = 2^{2l-2t} \left(b^2 \frac{c}{b+c} + c^2 \frac{b}{b+c} \right) = 2^{2l-2t} bc.$$

Подставляя в это равенство $n = b = k(2^s - 1)$, $l = n - k2^{s-1}$, $c = k$, $t = s$ получаем

$$\sum_{wt(v)=k2^{s-1}} \widetilde{a}^2(v) = 2^{k(2^s-2)-2s} k^2 (2^s - 1). \tag{16}$$

Оценим мощность $N(M, R)$ множества целочисленных наборов $\{(\alpha_1, \ldots, \alpha_M) \mid \sum\limits_{i=1}^{M} \alpha_i^2 = R\}$ при $R \leq M$. Нетрудно видеть, что $N(M, R) \leq \binom{M}{R} C^R$, где C — некоторая константа. Применяя асимптотическое равенство $\ln \binom{M}{R} = R \ln \frac{M}{R}(1 + o(1))$, получаем что $\ln N(M, R) = R \ln \frac{M}{R}(1 + o(1))$ при $\frac{M}{R} \to \infty$. Тогда из равенства (16) заключаем, что

$$\ln N(k, s) \leq 2^{k2^s - 2k - s} k^2 (k + s)(1 + o(1))$$

при $n = k(2^s - 1) \to \infty$.▲

Оценка (13) может быть переписана в виде $\log\log N(k, s) \leq nh(\frac{1}{2}(1 - \frac{k}{n}))(1 + o(1))$, а оценка из теоремы 1 в виде $\log\log N(k, s) \leq n(1 - \frac{k}{n})(1 + o(1))$. Вторая оценка сильнее, поскольку неравенство $h(\alpha/2) > \alpha$ следует из выпуклости вверх функции $h(\alpha/2)$ при $0 < \alpha < \frac{1}{2}$. В частности, при $s = 2$ из теоремы 1 вытекает следующая оценка на число совершенных раскрасок $\log\log N(k, s) \leq \frac{2n}{3}(1 + o(1))$ при $3k = n \to \infty$.

4. Конструкции совершенных раскрасок

Пусть Σ — некоторое непустое множество конечной мощности q. *МДР-кодом с расстоянием* $d+1$ называется подмножество $M \subset \Sigma^n$, которое пересекается с каждой d-мерной гранью q-значного n-куба Σ^n ровно по одной вершине. Если в каждой d-мерной грани ровно по t элементов множества M, то M называется *t-кратным* МДР-кодом. Таким образом, понятие кратного МДР-кода являются обобщением понятия корреляционно-иммунной функции на q-значные гиперкубы. МДР-коды с расстоянием 2 иногда называют тривиальными, поскольку они существуют при любой размерности пространства n и любой мощности

алфавита q. В дальнейшем рассматриваются только однократные МДР-коды с расстоянием 2 при $q = 4$.

Конструкция, предложенная в работе [9], связывает МДР-коды и совершенные коды. Рассмотрим обобщение этой конструкции, позволяющее строить совершенные раскраски с матрицей параметров

$$\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}. \tag{17}$$

Пусть $m = 2^{s-2}$, $n = (2^s-1)k$, $s \geq 2$. Зафиксируем $\widetilde{R} \subset E^{m-1}$ — линейный совершенный код (код Хэмминга). Пусть $r \in E^{k(m-1)}$, определим $\widetilde{r} = \left(\bigoplus_{i=1}^{k} r_i, \ldots, \bigoplus_{i=k(m-2)+1}^{k(m-1)} r_i \right)$ и $R = \{r \in E^{k(m-1)} \mid \widetilde{r} \in \widetilde{R}\}$. Для каждого $r \in R$ зададим МДР-код $M_r \subset \Sigma^{km}$ (с расстоянием 2). Обозначим

$$\begin{array}{llll} C_0^0 = \{0000, 1111\}, & C_1^0 = \{1001, 0110\}, & C_2^0 = \{0101, 1010\}, & C_3^0 = \{0011, 1100\}; \\ C_0^1 = \{0001, 1110\}, & C_1^1 = \{1000, 0111\}, & C_2^1 = \{0100, 1011\}, & C_3^1 = \{0010, 1101\}; \\ C_0 = \{000\ , 111\ \}, & C_1 = \{100\ , 011\ \}, & C_2 = \{010\ , 101\ \}, & C_3 = \{001\ , 110\ \}. \end{array}$$

Определим множество $S \subset E^n$, где $n = (2^s-1)k$, равенством

$$S = \bigcup_{r \in R} \bigcup_{\alpha \in M_r} Q_{\alpha,r}, \qquad Q_{\alpha,r} = C_{\alpha_1}^{r_1} \times C_{\alpha_2}^{r_2} \times \cdots \times C_{\alpha_{k(m-1)}}^{r_{k(m-1)}} \times C_{\alpha_{k(m-1)+1}} \times \cdots \times C_{\alpha_{km}}. \tag{18}$$

Теорема 2. *Пусть множество $S \subset E^n$ определено равенством* (18)*, тогда χ^S — совершенная раскраска с матрицей параметров* (17).

Доказательство. Достаточно доказать, что
(a) если $u, v \in S$, то $d(u, v) \geq 2$;
(b) $|F(u) \cap S| \geq k$ для любой вершины $u \notin S$;
(c) $|S| = 2^{n-s}$.

Докажем пункт (a). Если $u \in Q_{\alpha,r}$, $v \in Q_{\alpha',r'}$ и $\alpha \neq \alpha'$, то $d(\alpha, \alpha') \geq 2$ по определению МДР-кода. Поскольку множества C_i^δ попарно не пересекаются и множества C_i попарно не пересекаются, то $d(u, v) \geq 2$.

Пусть $u \in Q_{\alpha,r}$, $v \in Q_{\alpha,r'}$. Если $\widetilde{r} \neq \widetilde{r}'$, то из определения совершенного кода следует, что $d(r, r') \geq 3$ и, следовательно, $d(u, v) \geq 3$. Если же $\widetilde{r} = \widetilde{r}'$, но $r \neq r'$, то $d(r, r') \geq 2$ из определения $\widetilde{r}$. Тогда $d(u, v) \geq 2$.

Пусть $u, v \in Q_{\alpha,r}$. Тогда $d(u, v)$ не меньше расстояния между различными вершинами одного из множеств C_i^δ или C_i, т. е. $d(u, v) \geq 3$.

Докажем пункт (b). Рассмотрим произвольный вектор $u \in E^n$. Ясно, что найдутся единственные $\alpha \in \Sigma^{km}$ и $r \in E^{m-1}$, что $u \in Q_{\alpha,r}$. Поскольку $u \notin S$, то возможны следующие случаи (b1) $r \notin R$; (b2) $r \in R$ и $\alpha \notin M_r$.

В случае (b1) по определению совершенного кода имеется ровно один вектор $\widetilde{q} \in \widetilde{R}$, что $d(\widetilde{r}, \widetilde{q}) = 1$. Без ограничения общности можно считать, что вектора $\widetilde{r}, \widetilde{q} \in E^{m-1}$ различаются в 1-й координате. Тогда имеется ровно k таких векторов $q^i \in E^{k(m-1)}$, $i = 1, \ldots, k$, что $\widetilde{q^i} = \widetilde{q}$ и вектора r и q^i отличаются в i-й координате. Пусть $i = 1$, $q_1^1 = 1$, $r_1 = 0$. По определению МДР-кода найдётся такое $\beta_1 \in \Sigma$, что $(\beta_1, \alpha_2, \ldots, \alpha_{km}) \in M_{q^1}$ и вершина $(v_1, v_2, v_3, v_4) \in C_{\beta_1}^1$ находящаяся на расстоянии 1 от вершины $(u_1, u_2, u_3, u_4) \in C_{\alpha_1}^0$. Тогда $d(u, v^1) = 1$, где $v^1 = (v_1, v_2, v_3, v_4, u_5, \ldots, u_n) \in S$. Аналогично определяются вершины $v^i \in S$, соответствующие векторам q^i при $i = 1, \ldots, k$.

В случае (b2) для каждого $i = k(m-1)+1, \ldots, km$ по определению МДР-кода M найдётся ровно одно $\beta_i \in \Sigma$, что $(\alpha_1, \ldots, \alpha_{i-1}, \beta_i, \alpha_{i+1}, \ldots, \alpha_{km}) \in M$. При $\alpha_i \neq \beta_i$ для любой вершины из C_{α_i} найдётся единственная вершина из C_{β_i}, находящаяся на расстоянии 1.

Докажем (c). Известно, что

$$|\widetilde{R}| = 2^{m-s+1}, |R| = |\widetilde{R}|2^{(k-1)(m-1)} \text{ и } |M_{\widetilde{r}}| = 4^{km-1}. \tag{19}$$

Из (18) имеем равенство

$$|S| = |C_0|^{km}|R||M_r| = 2^{km} \cdot 2^{m-s+1} \cdot 4^{km-1} \cdot 2^{(k-1)(m-1)} = 2^{n-s}.$$

▲

Оценим число тех совершенных раскрасок с параметрами (17), которые могут быть получены с помощью конструкции (18). Следующая теорема является обобщением теоремы из [10] на случай $k > 1$.

Теорема 3. $N(k,s) \geq 2^{2^{k(2^{s-1}-1)-s+1}} \cdot 3^{k2^{k(2^{s-2}-1)}} \cdot 2^{2^{k(2^{s-2}-1)-s+2}}$.

Доказательство. Для любого $u \in Q_{\alpha,r}$ наборы $\alpha \in \Sigma^{km}$ и $r \in E^{k(m-1)}$ определяются единственным образом. Тогда по совершенной раскраске χ^S, удовлетворяющей равенству (18), можно однозначно восстановить множество R и МДР-коды M_r. Отсюда вытекает оценка $N(k,s) \geq \#R(\#M)^{|R|}$, где $\#R$ — число совершенных кодов в E^{m-1}, а $\#M$ — число МДР-кодов в Σ^{km}.

В работе [14] доказаны неравенства $3^{km}2^{2^{(km-1)}+1} \leq \#M \leq (3^{km}+1)2^{2^{(km-1)}+1}$ при $km \geq 5$. Тогда из (19) получаем неравенство

$$N(k,s) \geq \left(3^{km}2^{2^{(km-1)}+1}\right)^{2^{k(m-1)-s+2}} = 2^{2^{k(2^{s-1}-1)-s+1}} \cdot 3^{k2^{k(2^{s-2}-1)}} \cdot 2^{2^{k(2^{s-2}-1)-s+2}}.$$

▲

Рассмотрим совершенную раскраску S, удовлетворящую равенству (18). Из следствия 1 видно, что компоненты совершенной раскраски S имеют мощность не менее 2^{2km-1}. Пусть K — компонента МДР-кода M_r. Тогда множество $C = \bigcup\limits_{\alpha \in K} Q_{\alpha,r} \subset S$ является компонентой совершенной раскраски S по определению. В [14], в частности, исследованы МДР-коды $M \subset \Sigma^{km}$, состоящие из непересекающихся компонент мощности 2^{km-1}. Нетрудно видеть, что $|C| = |K|2^{km} = 2^{2km-1}$. Таким образом, нижняя оценка мощности компоненты совершенной раскраски с параметрами (17) достигается. Более того, существуют совершенные раскраски, состоящие из непересекающихся компонент минимальной мощности. В соответствии со следствием 1, компоненты минимальной мощности являются линейными кодами.

Автор благодарит рецензента за ценные замечания.

Список литературы

[1] Д.Г. Фон-Дер-Флаасс, *Совершенные 2-раскраски гиперкуба*, Сибирский математический журнал, **48**: 4 (2007), 923–930.

[2] Д.Г. Фон-Дер-Флаасс, *Совершенные 2-раскраски 12-мерного куба, достигающие границы корреляционной иммунности*, Сибирские Электронные Математические Известия, **4** (2007), 292–295.

[3] D.G.Fon-Der-Flaass, *A bound of correlation immunity*, Сибирские Электронные Математические Известия, Siberian Electronic Mathematical Reports, **4** (2007), 133–135.

[4] К.В. Воробьёв, Д.Г. Фон-Дер-Флаасс, *О совершенных 2-раскрасках гиперкуба* , Сибирские Электронные Математические Известия, **7** (2010), 65–75.
[5] Ю.В. Тарannиков, *О корреляционно-иммунных и устойчивых булевых функциях*, Математические вопросы кибернетики, Выпуск 11, М.: Физматлит, 2002, 91–148.
[6] J. Friedman, *On the bit extraction problem*, Proc.33rd IEEE Symposium on Foundations of Computer Science (1992), 314–319.
[7] J. Bierbrauer, *Bounds on orthogonal arrays and resilient functions*, Journal of Combinatorial Designs, **3** (1995), 179–183.
[8] P.R.J. Ostergard, O. Pottonen, and K.T. Phelps, *The perfect binary one-error-correcting codes of length 15: Part II-Properties*, IEEE Transactions on Information Theory, **56** (2010), 2571–2582.
[9] K.T. Phelps, *A general product construction for error correcting codes*, SIAM J. Algebraic Discrete Methods, **5**: 2 (1984), 224–228.
[10] Д.С. Кротов, *Нижние оценки числа m-квазигрупп порядка* 4 *и числа совершенных двоичных кодов*, Дискрет. анализ и исслед. операций. Сер. 1. **7**: 2 (2000), 47–53.
[11] D.S. Krotov, S.V. Avgustinovich, *On the number of 1-perfect binary codes: a lower bound*, IEEE Trans. Inform. Theory **54**: 4 (2008), 1760–1765.
[12] О.А. Логачёв, А.А. Сальников, В.В. Ященко, *Булевы функции в теории кодирования и криптологии*, М.: Изд-во МЦНМО, 2004.
[13] Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн, *Теория кодов, исправляющих ошибки*, М.: Связь, 1979.
[14] В.Н. Потапов, Д.С. Кротов, *Асимптотика числа n-квазигрупп порядка 4*, Сибирский математический журнал, **47**:4 (2006), 873–887.

Владимир Николаевич Потапов
Институт математики им. С. Л. Соболева СО РАН,
пр. академика Коптюга 4,
630090, Новосибирск, Россия
E-mail address: vpotapov@math.nsc.ru