S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 4, Стр. 292–295 (2007) УДК 519.172.2
MSC 05C15

СОВЕРШЕННЫЕ 2-РАСКРАСКИ 12-МЕРНОГО КУБА, ДОСТИГАЮЩИЕ ГРАНИЦЫ КОРРЕЛЯЦИОННОЙ ИММУННОСТИ

Д.Г. ФОН-ДЕР-ФЛААС

Abstract. We construct perfect 2-colorings of the 12-hypercube that attain our recent bound on the dimension of arbitrary correlation immune functions. We prove that such colorings with parameters $(x, 12-x, 4+x, 8-x)$ exist if $x = 0, 2, 3$ and do not exist if $x = 1$.

Пусть H_n – гиперкуб размерности n. Его вершины – двоичные векторы длины n; вершины смежны, если их векторы различаются ровно в одной координате. Раскраска его вершин в черный и белый цвета называется совершенной раскраской с параметрами (a, b, c, d), если каждая черная вершина имеет a черных и b белых соседей, а каждая белая вершина c черных и d белых соседей. (Общее определение совершенной раскраски и основные свойства см. в [1], [3].)

В работе [2] получена *граница корреляционной иммунности*: там доказано, что для любой совершенной 2-раскраски H_n с $b \neq c$ выполняется неравенство

$$c - a \leq n/3.$$

Известны две серии раскрасок, достигающих этой границы. Они получаются из совершенного кода в трехмерном кубе и из раскраски Таранникова с параметрами $(1, 5, 3, 3)$ (см. [4]) операцией умножения (см. [1], предложение 1(c)) и имеют параметры, соответственно, $(0, 3k, k, 2k)$ и $(k, 5k, 3k, 3k)$.

Любая раскраска, достигающая границы корреляционной иммунности, имеет параметры $(i, 3x-i, i+x, 2x-i)$; размерность куба при этом равна $3x$. Без ограничения общности можно считать, что $i < x$. В настоящей работе

Fon-Der-Flaass D.G., Perfect colorings of the 12-cube that attain the bound on correlation immunity.

Работа поддержана грантами РФФИ 05-01-00816 и 06-01-00694.

Поступила 15 мая 2007 г., опубликована 29 июня 2007 г.

мы определим, при каких значениях i существуют такие раскраски 12-мерного куба ($x = 4$).

При $i = 0$ и $i = 2$ мы получаем параметры, принадлежащие указанным выше известным сериям; следовательно, в этих случаях раскраска существует.

Теорема 1. *Не существует совершенной раскраски графа* $H = H_{12}$ *с параметрами* $(1, 11, 5, 7)$.

Доказательство. Пусть, напротив, такая раскраска существует. Как в работе [2], определим на H вещественную функцию q, равную 11 в черных вершинах и -5 в белых. Из определения совершенной раскраски следует, что q является собственной функцией матрицы смежности графа H с собственным значением -4.

Мы используем подход из [2]. Напомним введенные там обозначения для граней H_n, и базис $\{f^x\}$ из собственных функций.

Для $x, y \in H$, $x \cap y = \emptyset$, определим множество $[x] + y = \{z \cup y \mid z \subseteq x\}$. Это просто k-грань гиперкуба для $k = |x|$.

Для каждого $x \in H$, функция f^x определяется так:

$$f^x(z) = (-1)^{|z \setminus x|}.$$

Набор функций $\{f^x \mid x \in H\}$ есть ортогональный базис пространства всех вещественных функций на H. Разложим q по базису $\{f^x\}$:

$$q = \sum_x w_x f^x,$$

где суммирование идет по векторам x веса 4. Для любых векторов x, y легко проверить, что $\langle \chi^{[x]}, f^y \rangle = 2^{|x|}$, если $x \subseteq y$; а в противном случае $\langle \chi^{[x]}, f^y \rangle = 0$. (Напомним, что $[x]$ – это наименьшая грань, содержащая вершины x и 0, и $\chi^{[x]}$ – ее характеристическая функция.) Отсюда мы можем найти коэффициенты w_x:

$$\langle \chi^{[x]}, q \rangle = 16 w_x = \sum_{v \in [x]} q(v) = 11m - 5(16 - m),$$

$$w_x = -5 + m,$$

где m – количество вершин черного цвета в грани $[x]$. В частности, все коэффициенты целые.

Значение $\langle q, q \rangle$ может быть вычислено двумя способами. С одной стороны, оно равно $2^{12} \sum w_x^2$, с другой стороны, из подсчета числа черных и белых вершин, оно равно $5 \cdot 2^8 \cdot 11^2 + 11 \cdot 2^8 \cdot 5^2 = 55 \cdot 2^{12}$. Отсюда $\sum w_x^2 = 55$.

Следовательно, среди коэффициентов w_x не более 55 ненулевых. Обозначим $S = \{x \mid w_x \neq 0\}$; $|S| \leq 55$.

Рассмотрим теперь произвольную 3-грань $[y]$. Имеем:

$$\langle \chi^{[y]}, q \rangle = \sum_{[y] \subset [x]} 8 w_x = 11m - 5(8 - m),$$

$$\sum_{[y] \subset [x]} w_x = 2m - 5 \neq 0,$$

где m – количество вершин черного цвета в грани $[y]$. В частности, это означает, что каждый вектор y веса 3 содержится хотя бы в одном векторе $x \in S$. Отсюда $|S| \geq \binom{12}{3}/4 = 55$.

Итак, $|S| = 55$, и каждый 3-вектор содержится ровно в одном векторе из S. Но это невозможно, поскольку тогда каждая из 12 координат должна содержаться ровно в $55 \cdot 4/12$ векторах из S, а это число – не целое. Теорема доказана. $\square$

Теорема 2. *Существуют совершенные раскраски 12-мерного гиперкуба с параметрами* $(3, 9, 7, 5)$.

Доказательство. Мы приведем явную конструкцию таких раскрасок, идейно близкую к конструкции из [1].

Начнем построение с вспомогательного 6-мерного куба X. Будем обозначать координаты в X символами из множества $\Omega = \{a_1, a_2, a_3, b_1, b_2, b_3\}$. Для удобства, мы будем иногда обозначать элемент Ω списком его ненулевых координат, опуская знак "+"между ними. 12-мерный куб H мы представим как объединение попарно непересекающихся слоев L_x, $x \in X$. Элементы каждого слоя также помечены векторами из X: $L_x = \{y_x \mid y \in X\}$. Слои L_x в кубе H являются независимыми множествами. Два слоя L_x, $L_{x'}$ для смежных в X векторов x, x' индуцируют двудольный граф степени 2; а именно: если $x' = x + a$, $a \in \Omega$, то $y_{x'}$ смежна с y_x и с $(y + a)_x$.

Разобьем все вершины X на 4 черные вершины, 12 белых вершин и 12 попарно непересекающихся 2-граней (их вершины назовем серыми). Разбиение будет инвариантно относительно группы $A = \langle \alpha, \beta \rangle$ автоморфизмов X, порожденной автоморфизмом перестановки координат $\alpha = (a_1a_2a_3)(b_1b_2b_3)$ и аффинным автоморфизмом $\beta(x) = a_1a_2a_3 + \sigma(x)$, где $\sigma = (a_1b_1)(a_2b_2)(a_3b_3)$.

Черными будут четыре вершины орбиты 0^A, а именно: 0, $a_1a_2a_3$, $a_1a_2a_3b_1b_2b_3$, $b_1b_2b_3$.

Белыми будут 12 вершин орбиты a_1^A, а именно: $0 + a_i$, $a_1a_2a_3 + b_i$, $a_1a_2a_3b_1b_2b_3 + a_i$, $b_1b_2b_3 + b_i$.

Наконец, остальные вершины X разбиваются на 2-грани, являющиеся образами под действием A грани $b_1 + \langle a_2, a_3 \rangle$, а именно:

$b_i + \langle a_j, a_k \rangle$,
$a_ja_k + \langle b_j, b_k \rangle$,
$a_1a_2a_3b_jb_k + \langle a_j, a_k \rangle$,
$a_ib_1b_2b_3 + \langle b_j, b_k \rangle$,
где i, j, k - произвольная перестановка индексов $1, 2, 3$.

Теперь определим раскраску $c : L_x \to \{0, 1\}$ для каждого слоя L_x. Если x – черная вершина, то положим $c(L_x) = 1$. Аналогично, $c(L_x) = 0$ для белых вершин x.

Для каждой серой грани $G = x + \langle p, q \rangle$ из нашего разбиения (здесь x – образ вершины b_1 под действием некоторого автоморфизма из A, а p, q – элементы Ω, определяющие направление грани) пусть $L_G = \{y_z \mid y \in X, z \in G$ – объединение соответствующих ей слоев. Выберем произвольно значение $c(G) = c(0_x)$ для одной вершины из L_x. Остальные значения $c(y_z)$ при $y_z \in L_G$ определим, исходя из нее, по таким правилам:

Для $r \in \Omega$, положим $c((y+r)_z) = c(y_z)$, если $r \in \{p, q\}$, и $c((y+r)_z) = 1-c(y_z)$ в противном случае;

положим $c(y_{z+r}) = 1 - c(y_z)$ при любом $r \in \{p, q\}$.

Легко видеть, что эти правила однозначно определяют цвета всех вершин $c(y_z)$ при $y \in X$, $z \in G$, и что любые две смежные вершины из этого множества окрашены различно.

Заметим также, что

($*$) *любая вершина вне L_G, смежная с L_G, имеет в L_G ровно двух соседей, и цвета этих соседей различны.*

Теперь нетрудно для каждой вершины H сосчитать число ее соседей цветов 0 и 1.

Если $z \in X$ — черная вершина, то у нее в X три белых и три серых соседа. Каждая вершина $y_z \in L_z$ имеет цвет 1, и у нее, по ($*$), три соседа цвета 1 и $3 + 3 \cdot 2 = 9$ соседей цвета 0.

Если $z \in X$ — белая вершина, то у нее в X один черный и пять серых соседей. Каждая вершина $y_z \in L_z$ имеет цвет 0, и у нее, по ($*$), пять соседей цвета 0 и $5 + 1 \cdot 2 = 7$ соседей цвета 1.

Если z принадлежит серой грани G, то у нее два соседа внутри грани, и либо один черный, два белых и один серый, либо один белый и три серых соседа вне грани. Следовательно, каждая вершина y_z имеет внутри L_G четырех соседей отличного от нее цвета, а вне L_G, подсчитывая, как выше, с использованием ($*$) – трех соседей цвета 1 и пять соседей цвета 0, независимо от цвета самой y_z.

Итак, у каждой вершины H ровно столько соседей каждого цвета, сколько требуется, и нужная нам раскраска построена. $\square$

В заключение заметим, что произвольный выбор двенадцати значений $c(G)$ в последней конструкции позволяет строить неизоморфные совершенные раскраски с параметрами $(3, 9, 7, 5)$. Однако остается неизвестным как точное число попарно неизоморфных таких раскрасок, так и то, все ли раскраски с этими параметрами могут быть получены нашей конструкцией.

Список литературы

[1] D. Fon-Der-Flaass, Perfect colorings of a hypercube, to appear in Siberian Math. J.

[2] D.G. Fon-Der-Flaass. A bound on correlation immunity, Siberian Electronic Mathematical Reports 4 (2007) 133–135.

[3] C. Godsil. Equitable partitions. In: Combinatorics, Paul Erdős is Eighty (Vol. 1). Keszthely (Hungary), 1993, 173–192.

[4] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity. Cryptology ePrint archive (`http://eprint.iacr.org`), Report 2000/005, March 2000, 18 p.

Д.Г. Фон-Дер-Флаасс
Институт математики им. С.Л. Соболева СО РАН,
пр. академика Коптюга 4,
630090, Новосибирск, Россия
E-mail address: `d.flaass@gmail.com`