О мощности компонент корреляционно-иммунных функций, совершенных раскрасок и кодов

В. Н. Потапов

Институт математики им. С.Л.Соболева,

Новосибирский государственный университет, Новосибирск

XVI Международная конференция
<ПРОБЛЕМЫ ТЕОРЕТИЧЕСКОЙ КИБЕРНЕТИКИ>,

г. Нижний Новгород, 20-25 июня 2011 г.

Пусть $E = \{0, 1\}$. Булев n-куб E^n естественным образом наделяется структурой векторного пространства над полем $GF(2)$. Пусть $S \subseteq E^n$.

Определение

Булева функция χ^S называется корреляционно-иммунной порядка $n - m$, если для любой грани размерности m её пересечения с множеством S имеют одинаковую мощность.

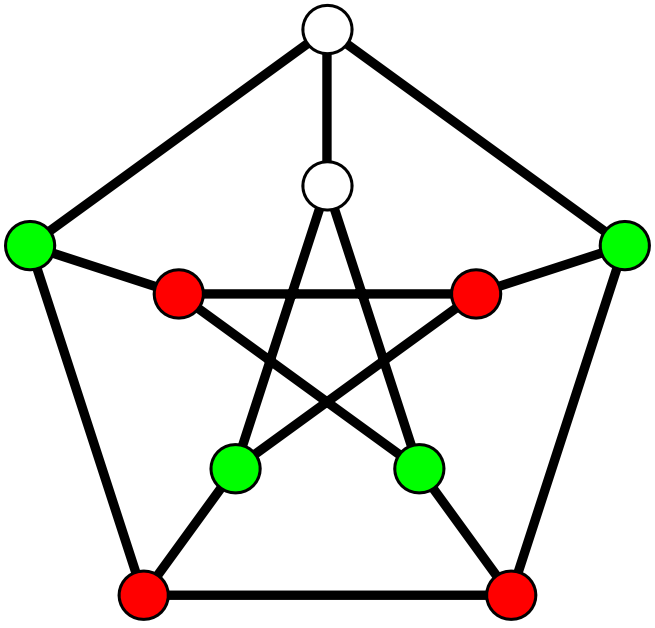
Сферой радиуса 1 с центром в вершине x называется множество $F(x) = \{y \in E^n : d(x, y) = 1\}$, где d — расстояние Хэмминга.

Определение

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 $x \in E^n$.

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 двуцветном $\{0, 1\}$ случае функция Col является булевозначной и $Col = \chi^S$, где S — множество вершин цвета 1.



$$S = \begin{array}{c|ccc} & \circ & \color{green}{\bullet} & \color{red}{\bullet} \\ \hline \circ & 1 & 2 & 0 \\ \color{green}{\bullet} & 1 & 0 & 2 \\ \color{red}{\bullet} & 0 & 2 & 1 \end{array}$$

Утверждение

Совершенная раскраска булева n-куба с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ является корреляционно-иммунной функцией порядка $\frac{b+c}{2} - 1$.

Fon-Der-Flaass D.G. A bound of correlation immunity // Siberian Electronic Mathematical Reports. 2007.

Тарапников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Выпуск 11. М.: Физматлит. 2002.

Определение

Совершенным кодом (с расстоянием 3) $C \subset E^n$ называется подмножество булева n-куба, пересекающееся с любым шаром радиуса 1 ровно по одной вершине.

Характеристической функцией совершенного кода $C \subset E^n$ является совершенная раскраска χ^C с матрицей параметров вида $\begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$.

Пусть $S_1, S_2 \subset E^n$ и функции χ^{S_1}, χ^{S_2} являются совершенными раскрасками с одинаковыми параметрами или корреляционно-иммунными функциями одного порядка и одной мощности.

Определение

Множества $S_1 \setminus S_2$ и $S_2 \setminus S_1$ будем называть компонентами (альтернативными) совершенных раскрасок (корреляционно-иммунных функций) χ^{S_1} и χ^{S_2} соответственно. Объединение альтернативных компонент, т. е. симметрическую разность $S_1 \triangle S_2$ будем называть двойной компонентой.

Статьи о проблеме мощности компонент кодов

Etzion T., Vardy A. Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998.

Avgustinovich S. V., Lobstein A. C., Soloveva F. I. Intersection matrices for partitions by binary perfect codes // IEEE Trans. Inform. Theory. 2001.

Avgustinovich S. V., Heden O., Solov'eva F. I. On intersections of perfect binary codes // Bayreuth. Math. Schr. 2005.

Avgustinovich S. V., Heden O., Solov'eva F. I. On intersection problem for perfect binary codes // Des. Codes Cryptogr. 2006.

Васильев Ю. Л., Августинович С. В., Кротов Д. С. О подвижных множествах в двоичном гиперкубе // Дискретн. анализ и исслед. операций. 2008.

Потапов В.Н. О совершенных раскрасках булева n-куба и корреляционно-иммунных функциях малой плотности // Сибирские электронные математические известия. 2010.

Теорема

Пусть множество $S \subset E^n$ есть компонента корреляционно-иммунной функции порядка $n - m$ и $2^{n-m+1} > |S|$. Тогда $|S| = 2^{n-m+1} - 2^p$, где $p \in \{0, \ldots, n - m\}$. Более того, компонента мощности 2^{n-m} является линейным кодом.

Следствие

Пусть f — совершенная раскраска с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$, множество $S \subset E^n$ есть компонента f и $2^{\frac{b+c}{2}} > |S|$. Тогда $|S| = 2^{\frac{b+c}{2}} - 2^p$, где $p \in \{0, \ldots, \frac{b+c}{2} - 1\}$. Более того, компонента мощности $2^{\frac{b+c}{2}-1}$ является линейным кодом.

Следствие

Пусть множество $S \subset E^n$ есть компонента совершенного кода $C \subset E^n$ и $2^{\frac{n+1}{2}} > |S|$. Тогда $|S| = 2^{\frac{n+1}{2}} - 2^p$, где $p \in \{1, \ldots, \frac{n-1}{2}\}$. Более того, компонента мощности $2^{\frac{n-1}{2}}$ является линейным кодом.

Каждая булева функция $f : E^n \to E$ может быть представлена в виде многочлена Жегалкина

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in E^n} G[f](y) x_1^{y_1} \ldots x_n^{y_n},$$

где $a^0 = 1, a^1 = a$, $G[f] : E^n \to E$ — булева функция.

Утверждение

Для любой булевой функции f справедливо равенство
$G[f](y) = \bigoplus_{x \in E^n, [x,y]=x} f(x), \quad [x, y] = (x_1 y_1, \ldots, x_n y_n).$

Определение

Алгебраической степенью $\deg(f)$ называется максимальная степень слагаемого в многочлене Жегалкина функции f.

Утверждение

Пусть $f : E^n \to E$ — корреляционно-иммунная функция порядка $n - m$. Тогда
(a) $\deg(f) \leq m$ (неравенство Зигенталлера);
(b) алгебраическая степень двойной компоненты корреляционно-иммунной функции f не превосходит $m - 1$.

Замечание

Если корреляционно-иммунная функция f порядка $n - m$ имеет чётное число единиц в каждой грани размерности m, то $\deg(f) \leq m - 1$.

Теорема (Мак-Вильямс , Слоэн; глава 13, теоремы 3 и 5)

Для любой не тождественно нулевой булевой функции $f = \chi^S$ справедливо неравенство $|S| \geq 2^{n-\deg(f)}$. Если $|S| = 2^{n-\deg(f)}$, то множество S является линейным кодом.

Теорема (Мак-Вильямс , Слоэн; глава 15, теорема 10)

Пусть $f = \chi^S$ — булева функция в E^n, $\deg(f) \geq 2$ и $2^{n-\deg(f)+1} > |S|$. Тогда $|S| = 2^{n-\deg(f)+1} - 2^{n-\deg(f)+1-p}$, где $p \in \{1, \ldots, \mu\}$, где
$\mu = \max\{(n - \deg(f) + 2)/2, \min\{n - \deg(f), \deg(f)\}\}$.

Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки, М.: Связь. 1979.

Kasami T., Tokura N. On the weight structure of Reed—Muller codes // IEEE Trans. Inform. Theory. 1970

Kasami T., Tokura N., Azumi S. On the weight enumeration of weights less than 2.5d of Reed—Muller codes // Inform. and Control. 1976

Теорема

Пусть $p \in \{0, \ldots, km-1\}$, $n = (2^s - 1)k$, $m = 2^{s-2}$, $s \geq 2$, $km \geq 3$. Существует совершенная раскраска f с матрицей параметров $\begin{pmatrix} k & k(2^s-2) \\ 2k & k(2^s-3) \end{pmatrix}$, имеющая компоненту мощности $(2^{km} - 2^p)2^{km}$.

При $k = 1$ такую совершенную раскраску рассматривают как двукратный совершенный код.

Следствие

Пусть $n = 3k + n'$, $r = 2k + n' - 1$, $k \geq 3$. Для любого $p \in \{0, \ldots, k-1\}$ найдётся корреляционно-иммунная функция $g : E^{n+n'} \to E$ порядка r, имеющая компоненту мощности $(2^k - 2^p)2^{k+n'}$.

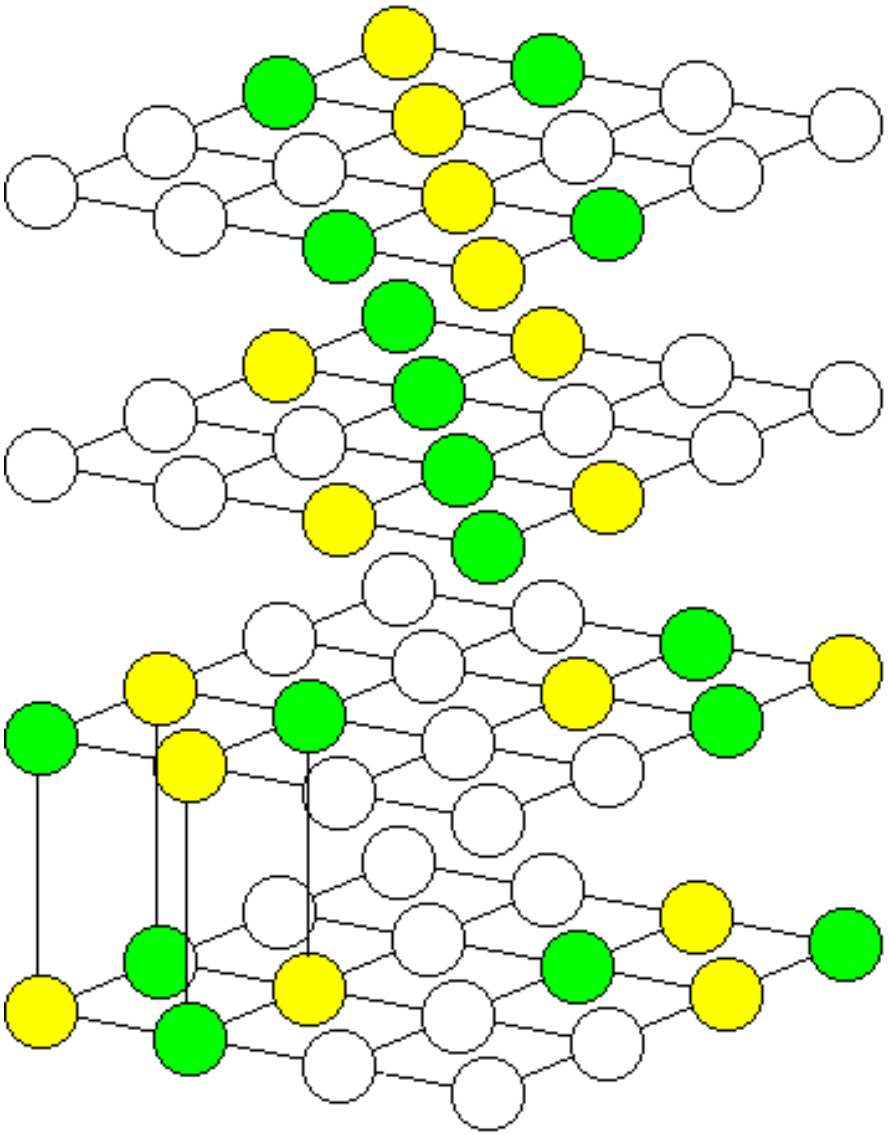
Определение

Множество $M \subset Q_4^n$ называется двукратным МДР-кодом , если M пересекается с каждой 1-мерной гранью куба Q_4^n по двум вершинам.

Утверждение

Для любого $p \in \{0, \ldots, n-1\}$, $t \geq 3$, существует двукратный МДР-код $B_n^p \subset Q_4^n$, имеющий компоненту мощности $2^n - 2^p$.

Potapov V.N. Latin bitrade // arXiv:1104.1295v1 [math.CO]



Зафиксируем $R \subset E^n$ — расширенный код Хэмминга. Определим разбиение E^4 на коды равенством
$C_a^r = C_0 + (1 + r)\overline{e}_4 + \overline{e}_a$, где $r \in \{0, 1\}$, $a \in \Sigma$, $C_0 = \{\overline{0}, \overline{1}\} \subset E^4$, $\overline{e}_i \in E^4$ — единичные вектора с 1 на i-м месте.

Утверждение

Множество

$$C = \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in B_n^p} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_n}^{r_n}.$$

является двукратным расширенным совершенным кодом.

Зиновьев В. А. Обобщённые каскадные коды // *Проблемы передачи информации*. 1976.

Phelps K. T. A general product construction for error correcting codes // *SIAM J. Algebraic Discrete Methods*. 1984.