О совершенных 2-раскрасках q-значного гиперкуба

В. Н. Потапов

Институт математики им. С.Л.Соболева,

Новосибирский государственный университет, Новосибирск

10 СИБИРСКАЯ НАУЧНАЯ ШКОЛА-СЕМИНАР
«КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ И КРИПТОГРАФИЯ» SIBECRYPT'11,

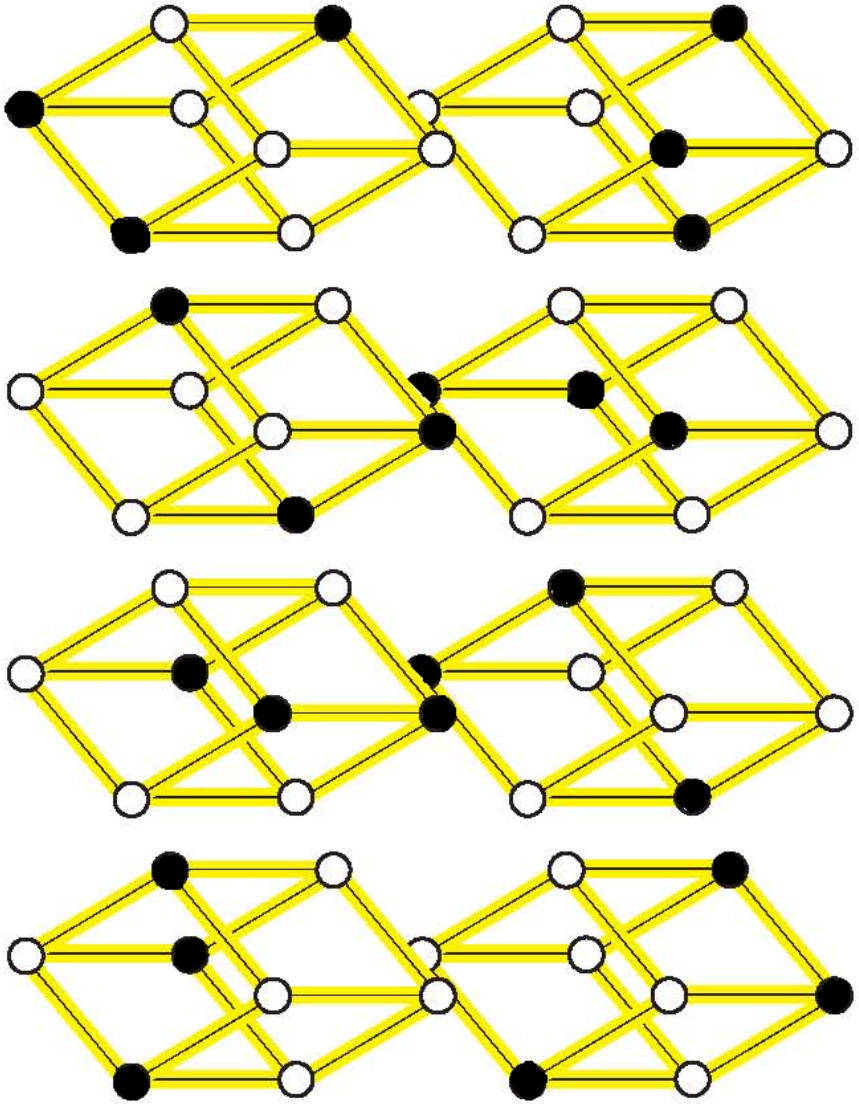
г. Томск, 5-10 сентября 2011 г.

Обозначим через Z_q множество $\{0, \ldots, q-1\}$. Декартово произведение Z_q^n называется q-значным n-мерным кубом (гиперкубом).

Определение

Функция $f : Z_q^n \to Z_q$ называется корреляционно-иммунной порядка $n - m$, если мощность пересечения грани размерности m с множеством $f^{-1}(a)$ зависит только от $a \in Z_q$.

Через $\mathrm{cor}(f)$ будем обозначать максимальный порядок корреляционной иммунности, $\mathrm{cor}(f) = \max\{n - m\}$.

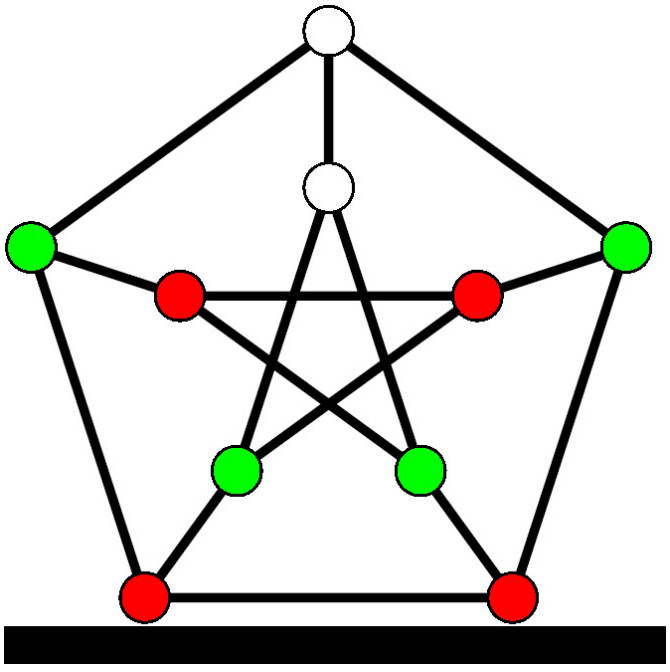


Определение

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

Определение

Отображение $Col : Z_q^n \to \{0, \ldots, k\}$ называется совершенной раскраской с матрицей параметров $M = \{m_{ij}\}$ если для любых i и j, для каждой вершины $x \in Z_q^n$ цвета i число соседей цвета j равняется $m_{ij} = |Col^{-1}(j) \cap F(x)|$.



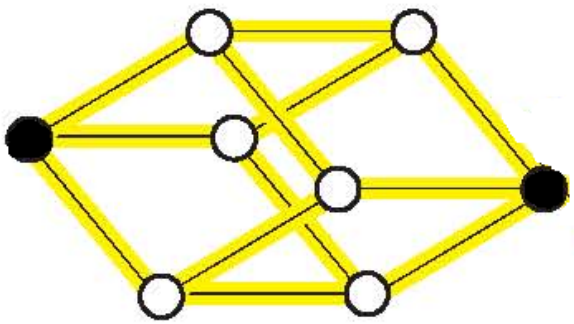
$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

В дальнейшем рассматриваются только раскраски в два цвета (2-раскраски). В двуцветном $\{0, 1\}$ случае функция *Col* является булевозначной и $Col = \chi^S$, где S — множество вершин цвета 1.

Определение

Совершенный код (исправляющий одну ошибку) $C \subset Z_q^n$ можно рассматривать как множество единиц совершенной 2-раскраски с матрицей параметров $M = \begin{pmatrix} n(q-1)-1 & 1 \\ n(q-1) & 0 \end{pmatrix}$.

Если число q является степенью простого числа, то раскраска с такими параметрами существует только при $n = \frac{q^j-1}{q-1}$.



Теорема (Таранников, 2002)

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

Определение

Плотностью функции $f : Z_q^n \to \{0,1\}$ будем называть $\rho(f) = \frac{|\{x \in Z_q^n \mid f(x)=1\}|}{q^n}$.

Теорема (Фон-Дер-Флаасс, 2007)

Пусть $f : Z_2^n \to \{0,1\}$, $0 < \rho(f) < 1/2$. Тогда $\mathrm{cor}(f) \leq \frac{2n}{3} - 1$ и если $\mathrm{cor}(f) = \frac{2n}{3} - 1$, то f — совершенная раскраска.

Теорема (Дельсарт, 1972, Пулатов, 1976, Остергард, Поттонен, Фелпс, 2010)

Булева функции f является характеристической функцией 1-совершенного кода тогда и только тогда, когда $\mathrm{cor}(f) = \frac{n-1}{2}$, $\rho(f) = \frac{1}{n+1}$.

Теорема (Фридман, 1992, Биербрауэр, 1995)

Для любой булевой функции f справедливо неравенство $\rho(f) \geq 1 - \frac{n}{2(\mathrm{cor}(f)+1)}$.

Теорема (Потапов, 2010)

Булева функции f является совершенной 2-раскраской с параметром $m_{11} = 0$ тогда и только тогда, когда справедливо равенство $\rho(f) = 1 - \frac{n}{2(\mathrm{cor}(f)+1)}$.

Определение

Определим величину $A(\chi^S)$ как среднее число вершин из $S \subseteq Z_q^n$, которые находятся на расстоянии 1 от вершины из дополнения $Z_q^n \setminus S$, т. е.
$A(\chi^S) = \frac{1}{q^n - |S|} \sum\limits_{x \notin S} |\{y \in S \mid d(x,y) = 1\}|$.

Теорема

(a) Для каждой булевозначной функции $f = \chi^S$, где $S \subset Z_q^n$, справедливо неравенство

$$\rho(f)q(\mathrm{cor}(f) + 1) \leq A(f).$$

(b) Булевозначная функция $f = \chi^S$ является совершенной 2-раскраской тогда и только тогда, когда

$$\rho(f)q(\mathrm{cor}(f) + 1) = A(f).$$