Совершенные раскраски и корреляционно-иммунные функции в q-значном гиперкубе

В. Н. Потапов

Институт математики им. С. Л. Соболева,
Новосибирский государственный университет, Новосибирск

Восьмая молодёжная научная школа
по дискретной математике и её приложениям,
г. Москва, 24-29 октября 2011 г.

Пусть $E_q = \{0, 1, \ldots, q-1\}$. Обозначим через E_q^n множество упорядоченных q-ичных наборов (вершин) длины n (*q-значный n-мерный куб*).

Определение

Расстоянием Хэмминга $d(x, y)$ между вершинами $x, y \in E_q^n$ называется число позиций, в которых наборы x и y различаются.

Определение

Шаром радиуса ρ с центром в вершине $x \in E_q^n$ называется множество $B_\rho(x) = \{y \in E_q^n \mid d(x, y) \leq \rho\}$.
$L_\rho(x) = \{y \in E_q^n \mid d(x, y) = \rho\}$ — *сфера* радиуса ρ.

Определение

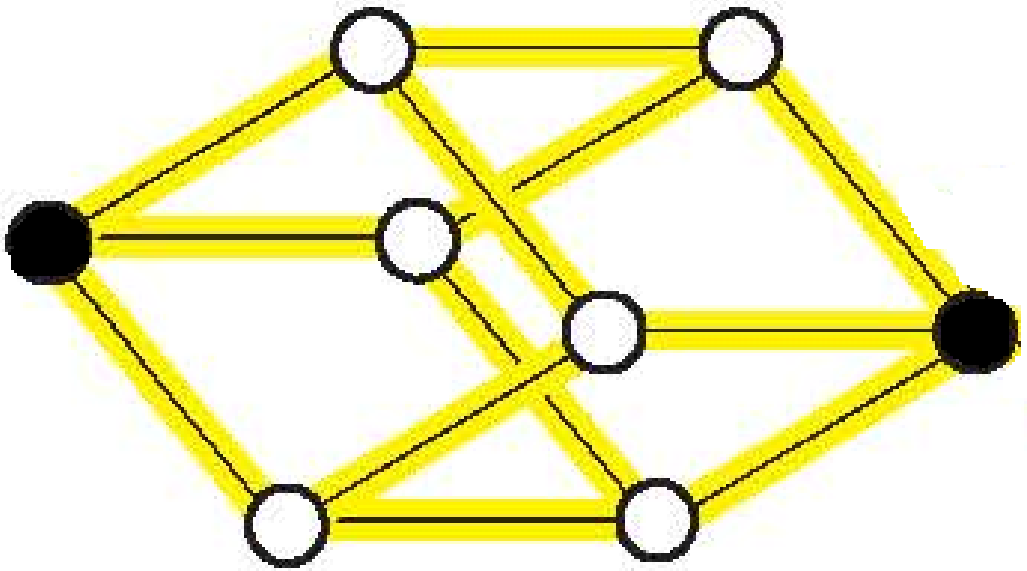
ρ-Совершенным кодом в E_q^n называется такое множество C, $|C| \geq 2$, что $|C \cap B_\rho(x)| = 1$ для любого $x \in E_q^n$.

Утверждение 1.1

Если в E_q^n имеется ρ-совершенный код, то число $\nu(q,n) = \frac{q^n}{1+(q-1)\binom{n}{1}+\cdots+(q-1)^\rho\binom{n}{\rho}}$ целое, где $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Утверждение 1.2

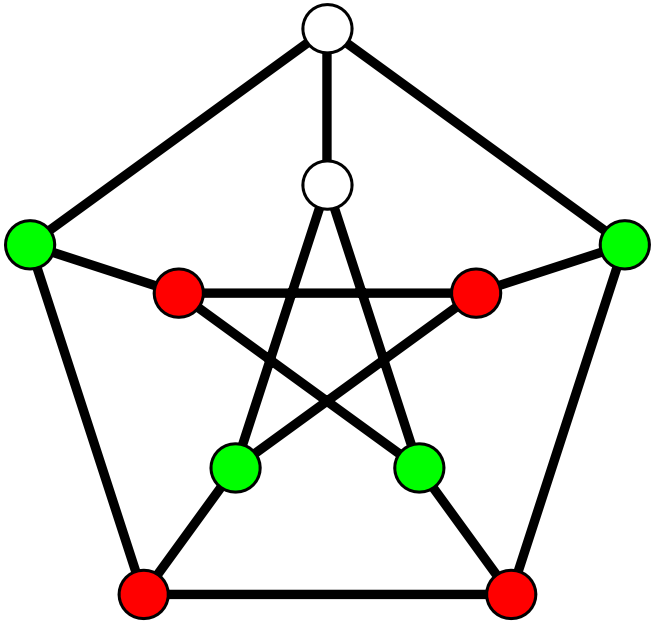
Множество $C \subset E_q^n$ является ρ-совершенным кодом тогда и только тогда, когда $|C| = \nu(q,n)$ и $d(x,y) \geq 2\rho+1$ для любых различных $x, y \in C$.



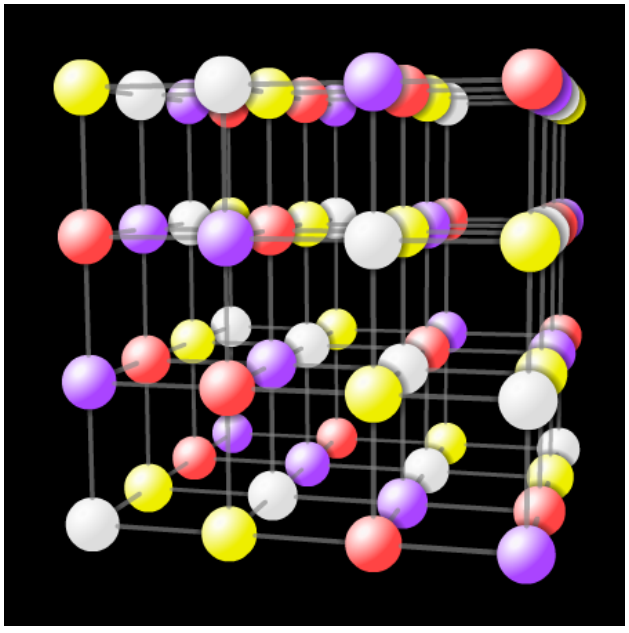
Определение

Совершенной раскраской куба E_q^n в k цветов называется отображение $Col : E_q^n \to \{1, \ldots, k-1, 0\}$, удовлетворяющее следующему условию: мощность пересечения $|Col^{-1}(i) \cap L_1(x)|$ зависит только от цветов i и $Col(x)$, но не от вершины $x \in E_q^n$.

Каждой совершенной раскраске соответствует матрица параметров $S = \{s_{ij}\}$, где s_{ij} — число вершин цвета j в сфере радиуса 1 с центром в вершине цвета i.



$$S = \begin{array}{c} \\ \circ \\ \bullet \\ \bullet \end{array} \begin{array}{c} \circ \quad \bullet \quad \bullet \\ 1 \quad 2 \quad 0 \\ 1 \quad 0 \quad 2 \\ 0 \quad 2 \quad 1 \end{array}$$



$$S = \begin{pmatrix} 0 & 3 & 3 & 3 \\ 3 & 0 & 3 & 3 \\ 3 & 3 & 0 & 3 \\ 3 & 3 & 3 & 0 \end{pmatrix}.$$

Утверждение 1.3

Множество $C \subset E_q^n$ является 1-совершенным кодом тогда и только тогда, когда χ^C — совершенная раскраска куба E_q^n в два цвета с матрицей параметров $\begin{pmatrix} 0 & n(q-1) \\ 1 & n(q-1)-1 \end{pmatrix}$.

Определение

Занумеруем вершины куба E_q^n. Определим $(0,1)$-матрицу M так: $m_{ij} = 1$, если i-я и j-я вершины находятся на расстоянии 1, и $m_{ij} = 0$ в противном случае. Матрица M называется *матрицей смежности* куба E_q^n.

Например, матрица смежности для E_2^2 имеет вид

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

По произвольной раскраске Col куба E_q^n в k цветов определим матрицу F_{col} размера $q^n \times k$, в которой i-я строка равна $\overline{e_j}$, если $Col(i) = j$. Наоборот, по любой $(0,1)$-матрице размера $q^n \times k$ с единственной единицей в каждой строке определяется раскраска куба в k цветов.

Теорема 1 (Августинович)

1) Если Col — совершенная раскраска куба E_q^n с матрицей S, то $MF_{Col} = F_{Col}S$.
2) Если для некоторой раскраски и матрицы S выполнено равенство $MF_{Col} = F_{Col}S$, то раскраска Col совершенная.

Теорема верна для произвольного регулярного графа.

Утверждение 1.4

Пусть S матрица параметров совершенной раскраски куба E_q^n, тогда $n(q-1)$ собственное число матрицы S.

Утверждение 1.5

Пусть S матрица параметров совершенной раскраски куба E_q^n, тогда собственные числа матрицы S являются собственными числами матрицы смежности куба E_q^n.

Утверждение 1.4

Пусть S матрица параметров совершенной раскраски куба E_q^n, тогда $n(q-1)$ собственное число матрицы S.

Утверждение 1.5

Пусть S матрица параметров совершенной раскраски куба E_q^n, тогда собственные числа матрицы S являются собственными числами матрицы смежности куба E_q^n.

Доказательство. Пусть $v \in \mathbb{C}^k$ — собственный вектор матрицы S. Тогда $Sv = \lambda v$ и $MF_{Col}v = F_{Col}Sv = \lambda F_{Col}v$, причём $F_{Col}v \neq \overline{0}$, если $v \neq \overline{0}$. Таким образом, λ — собственное число матрицы M.

Будем рассматривать множество E_q как группу по $\mod q$ и куб E_q^n как абелеву группу $E_q \times \cdots \times E_q$. Для $x, y \in E_q^n$ определим $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n (\mod q)$.
Множество функций $f : E_q^n \to \mathbb{C}$ будем рассматривать как векторное пространство $\mathbb{V}$ над полем $\mathbb{C}$ со скалярным произведением

$$(f, g) = \frac{1}{q^n} \sum_{x \in E_q^n} f(x)\overline{g(x)}.$$

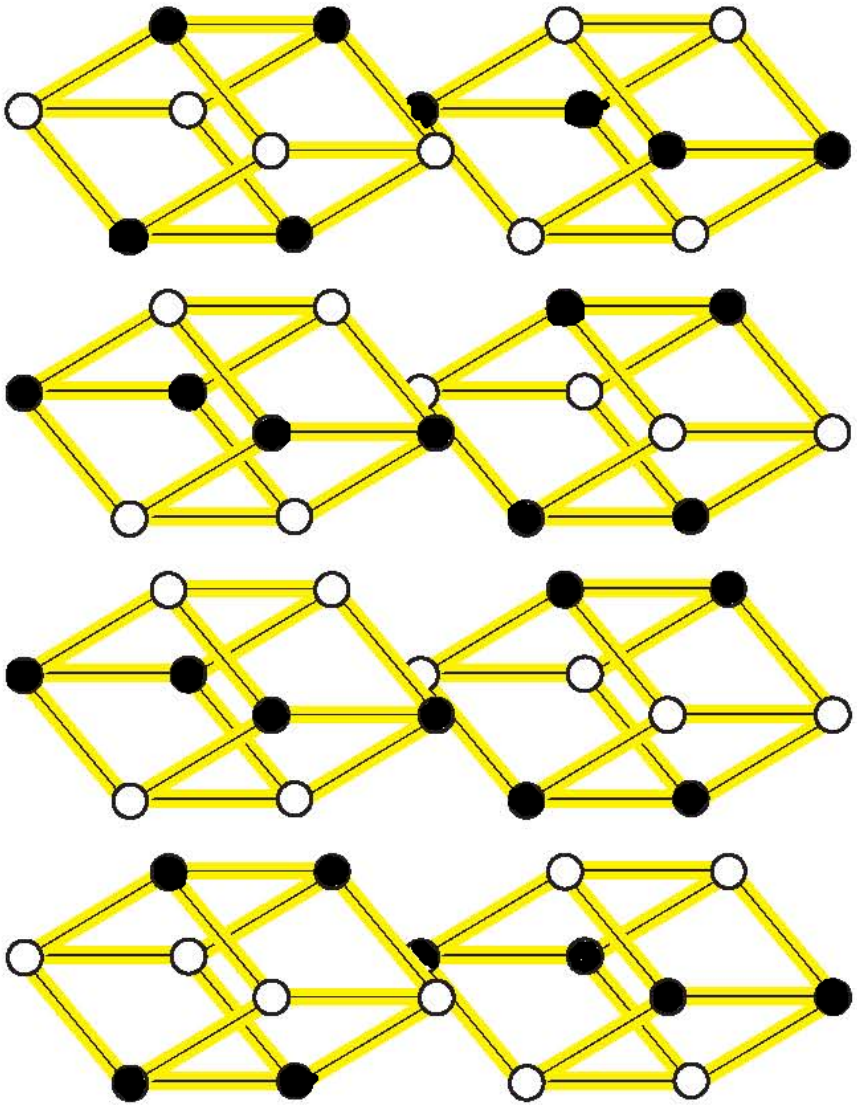
Определение

Пусть $\xi = e^{2\pi i/q}$. *Характером* группы E_q^n называется $\phi_z \in \mathbb{V}$, где $\phi_z(x) = \xi^{\langle x,z\rangle}$, $z \in E_q^n$.

При $q = 2$ можно рассматривать векторное пространство над $\mathbb{R}$ или $\mathbb{Q}$, поскольку $\xi = -1$.

Утверждение 2.1

1) $\phi_z \cdot \phi_y = \phi_{z+y}$;
2) $\sum\limits_{j=0}^{q-1} \xi^{kj} = 0$ при $k \neq 0(\mod q)$;
3) $\sum\limits_{x \in E_q^n} \xi^{\langle x,z\rangle} = 0$ при $z \neq \overline{0}$.



Утверждение 2.2

Характеры образуют ортонормированный базис в $\mathbb{V}$.

Определение

Преобразованием Фурье вектора f называется $\widehat{f}(z) = (f, \phi_z)$. Тогда $f(x) = \sum\limits_{z \in E_q^n} \widehat{f}(z)\phi_z(x)$.

равенство Парсеваля

$$\sum_{x \in E_q^n} |f(x)|^2 = \sum_{z \in E_q^n} |\widehat{f}(z)|^2.$$

Определение

Гранью размерности k называется подмножество куба E_q^n, состоящее из вершин с одинаковыми фиксированными значениями некоторых $n - k$ координат.

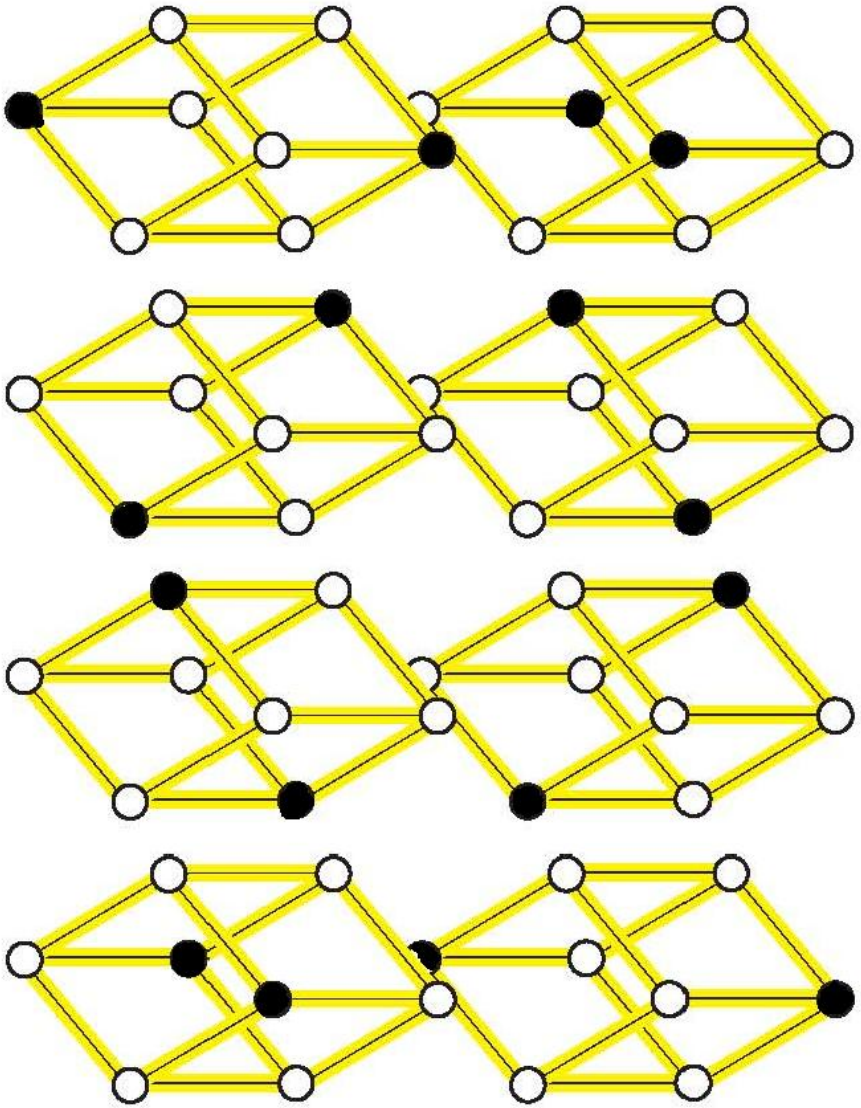
Определение

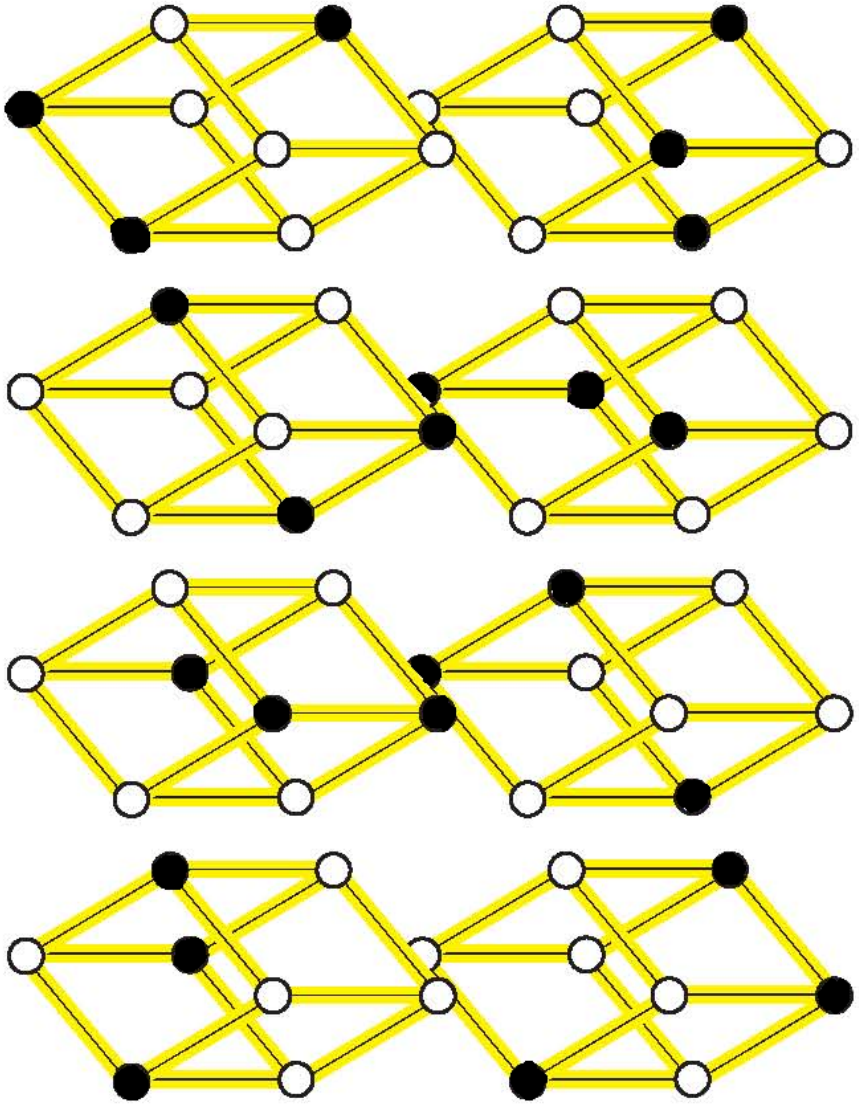
Функция $f : E_q^n \to E_q$ называется *корреляционно-иммунной порядка* $n - m$, если для любого $a \in E_q$ величина $|f^{-1}(a) \cap \Gamma|$ не зависит от выбора m-мерной грани Γ.

Обозначим через $\mathrm{cor}(f)$ максимальный порядок иммунности функции f и через $wt(x)$ — число ненулевых координат вершины $x \in E_q^n$

Пример

Пусть $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n (\mod q)$, тогда $\mathrm{cor}(f) = n - 1$.





Утверждение 2.3

Если f — корреляционно-иммунная функция порядка m, тогда $\widehat{f}(z) = 0$ при $0 < wt(z) \leq m$.

Утверждение 2.3

Если f — корреляционно-иммунная функция порядка m, тогда $\widehat{f}(z) = 0$ при $0 < wt(z) \leq m$.

Доказательство. Рассмотрим $z = (z', \overline{0})$, $wt(z') \leq m$.

$$\widehat{f}(z) = \frac{1}{q^n} \sum_{x \in E_q^n} f(x)\overline{\phi_z(x)} = \frac{1}{q^n} \sum_{x'} (\xi^{-\langle x', z' \rangle} \sum_{x''} f(x)\xi^{-\langle x'', \overline{0} \rangle}) =$$

$$= \frac{const}{q^n} \sum_{x'} \xi^{-\langle x', z' \rangle} = 0.$$

Утверждение 2.4

Если $f \in \mathbb{V}$ такова, что $\widehat{f}(z) = 0$ при $0 \leq wt(z) \leq m$. Тогда $\sum\limits_{x \in \Gamma} f(x) = 0$ для любой грани Γ размерности $n - m$.

Утверждение 2.4

Если $f \in \mathbb{V}$ такова, что $\widehat{f}(z) = 0$ при $0 \leq wt(z) \leq m$. Тогда $\sum\limits_{x \in \Gamma} f(x) = 0$ для любой грани Γ размерности $n - m$.

Доказательство. $f(x) = \sum\limits_{wt(z) > m} \widehat{f}(z)\phi_z(x)$. Если $wt(z) > m$, то $\sum\limits_{x \in \Gamma} \phi_z(x) = 0$ для любой грани Γ размерности $n - m$.

Утверждение 2.4

Если $f \in \mathbb{V}$ такова, что $\widehat{f}(z) = 0$ при $0 \leq wt(z) \leq m$. Тогда $\sum\limits_{x \in \Gamma} f(x) = 0$ для любой грани Γ размерности $n - m$.

Доказательство. $f(x) = \sum\limits_{wt(z) > m} \widehat{f}(z)\phi_z(x)$. Если $wt(z) > m$, то $\sum\limits_{x \in \Gamma} \phi_z(x) = 0$ для любой грани Γ размерности $n - m$.

Утверждение 2.5

Если $f : E_q^n \to \{0, 1\}$ и $\widehat{f}(z) = 0$ при $0 < wt(z) \leq m$, то f — корреляционно-иммунная функция порядка m.

Утверждение 2.6

Характеры $\phi_z(x)$ являются собственными векторами матрицы смежности куба E_q^n с собственными числами $(n - wt(z))(q-1) - wt(z)$.

Утверждение 2.6

Характеры $\phi_z(x)$ являются собственными векторами матрицы смежности куба E_q^n с собственными числами $(n - wt(z))(q-1) - wt(z)$.

Доказательство.

$$M\phi_z(x) = \sum_{y, d(x,y)=1} \xi^{\langle y-x,z\rangle + \langle x,z\rangle} = \xi^{\langle x,z\rangle} \sum_{j=1}^{n} \sum_{k\neq 0} \xi^{kz_j} =$$

$$= ((n - wt(z))(q-1) - wt(z))\phi_z(x).$$

Утверждение 2.7

Пусть $f : E_q^n \to \{0, 1\}$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда $f - \frac{b}{c+b}$ есть собственная функция матрицы смежности гиперкуба E_q^n с собственным числом $n(q-1) - (b+c)$.

Утверждение 2.8

1) Если $f : E_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $\widehat{f}(z) = 0$ при $wt(z) \neq 0, \frac{b+c}{q}$.

2) Если $\widehat{f}(z) = 0$ при $wt(z) \neq 0, s$ для некоторой функции $f : E_q^n \to \{0,1\}$, то f — совершенная раскраска.

Утверждение 2.8

1) Если $f : E_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $\widehat{f}(z) = 0$ при $wt(z) \neq 0, \frac{b+c}{q}$.

2) Если $\widehat{f}(z) = 0$ при $wt(z) \neq 0, s$ для некоторой функции $f : E_q^n \to \{0,1\}$, то f — совершенная раскраска.

Доказательство. Докажем пункт 2). Функция $g = f + t$ является собственным вектором матрицы смежности гиперкуба E_q^n для некоторой константы $t \in \mathbb{Q}$. Пусть $g(x) = t$ и $b(x) = |L_1(x) \cap g^{-1}(1+t)|$. Тогда $b(x)(1+t) + (n(q-1) - b(x))t = \lambda t$, где λ — собственное число соответствующее характерам ϕ_z, $wt(z) = s$. Таким образом, число $b(x)$ не зависит от выбора $x \in E_q^n$.

Утверждение 2.9

Пусть f — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда $\mathrm{cor}(f) = \frac{c+b}{q} - 1$.

Определение

Пусть $f : E_q^n \to \{0, 1\}$, будем называть *плотностью* $\varrho(f) = \frac{|\{x \in E_q^n \mid f(x)=1\}|}{q^n}$.

Утверждение 2.9

Пусть f — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда $\mathrm{cor}(f) = \frac{c+b}{q} - 1$.

Определение

Пусть $f : E_q^n \to \{0, 1\}$, будем называть *плотностью* $\varrho(f) = \frac{|\{x \in E_q^n \mid f(x)=1\}|}{q^n}$.

Теорема 2 (Фридман, 1992, Биербрауэр, 1995)

Для любой функции $f : E_q^n \to \{0,1\}$ справедливо неравенство $\varrho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Теорема 2 (Фридман, 1992, Биербрауэр, 1995)

Для любой функции $f : E_q^n \to \{0,1\}$ справедливо неравенство $\varrho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Доказательство. Пусть $m = \mathrm{cor}(f)$, $\lambda(z)$ — собственное число, соответствующее характеру ϕ_z.

$$f(x) = \varrho(f) + \sum_{wt(z)>m} \widehat{f}(z)\phi_z(x),\ (f,f) = \varrho(f).$$

$$(*) \qquad 0 \leq (Mf,f) = \sum_{z',z''} \lambda(z')\widehat{f}(z')\widehat{f}(z'')(\phi_{z'},\phi_{z''}) =$$

$$= \varrho(f)n(q-1) + \sum_{wt(z)>m} \lambda(z)|\widehat{f}(z)|^2 \leq$$

$$\leq \varrho^2(f)n(q-1) + ((n-(m+1))(q-1)-(m+1))(\varrho(f)-\varrho^2(f)).$$

Теорема 3 (Потапов, 2010)

Функции $f : E_q^n \to \{0, 1\}$ является совершенной раскраской с параметром $s_{11} = 0$ тогда и только тогда, когда справедливо равенство $\varrho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Теорема 3 (Потапов, 2010)

Функции $f : E_q^n \to \{0, 1\}$ является совершенной раскраской с параметром $s_{11} = 0$ тогда и только тогда, когда справедливо равенство $\varrho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Доказательство.

Если функция f является совершенной раскраской в два цвета с параметром $s_{11} = 0$, то $(Mf, f) = 0$. Тогда в цепочке неравенств (*) имеем равенства. Наоборот, если выполнено равенство $\varrho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$, то в цепочке неравенств (*) имеем всюду равенства.

Граница Биербрауэра — Фридмана достигается на счётчике чётности $S = \begin{pmatrix} 0 & n \\ n & 0 \end{pmatrix}$ и 1-совершенном коде $S = \begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$.

Теорема 4 (Дельсарт, 1972, Пулатов, 1976, Остергард, Поттонен, Фелпс, 2010)

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

Определение

Булеву функцию $f : E_2^n \to E_2$ называют *уравновешенной*, если $|f^{-1}(0)| = |f^{-1}(1)|$.

Теорема 5 (Фон-Дер-Флаасс, 2007)

Пусть $f : E_2^n \to E_2$ неуравновешенная и $|f^{-1}(0)|, |f^{-1}(1)| \neq 0$. Тогда $\mathrm{cor}(f) < \frac{2n}{3}$.

Доказательство. Пусть $c = |\{x \in E_2^n \mid f(x) = 0\}|$, $b = |\{x \in E_2^n \mid f(x) = 1\}|$, $c + b = 2^n$, $c \neq b$.

Определим функцию $g(x) = \begin{cases} -c, & \text{при } f(x) = 1, \\ b, & \text{при } f(x) = 0. \end{cases}$

Для любого $x \in E_2^n$ имеем $g^2(x) - (b - c)g(x) - bc = 0$.

Пусть $\widehat{f}(z) = 0$ при $0 < wt(z) \leq \frac{2n}{3} = m$. Тогда $\widehat{g}(z) = 0$ при $wt(z) \leq m$ и

$$\left(\sum_{wt(z)>m} \widehat{g}(z)\phi_z(x) \right) \left(\sum_{wt(z)>m} \widehat{g}(z)\phi_z(x) \right) =$$

$$= cb + (b - c) \left(\sum_{wt(z)>m} \widehat{g}(z)\phi_z(x) \right),$$

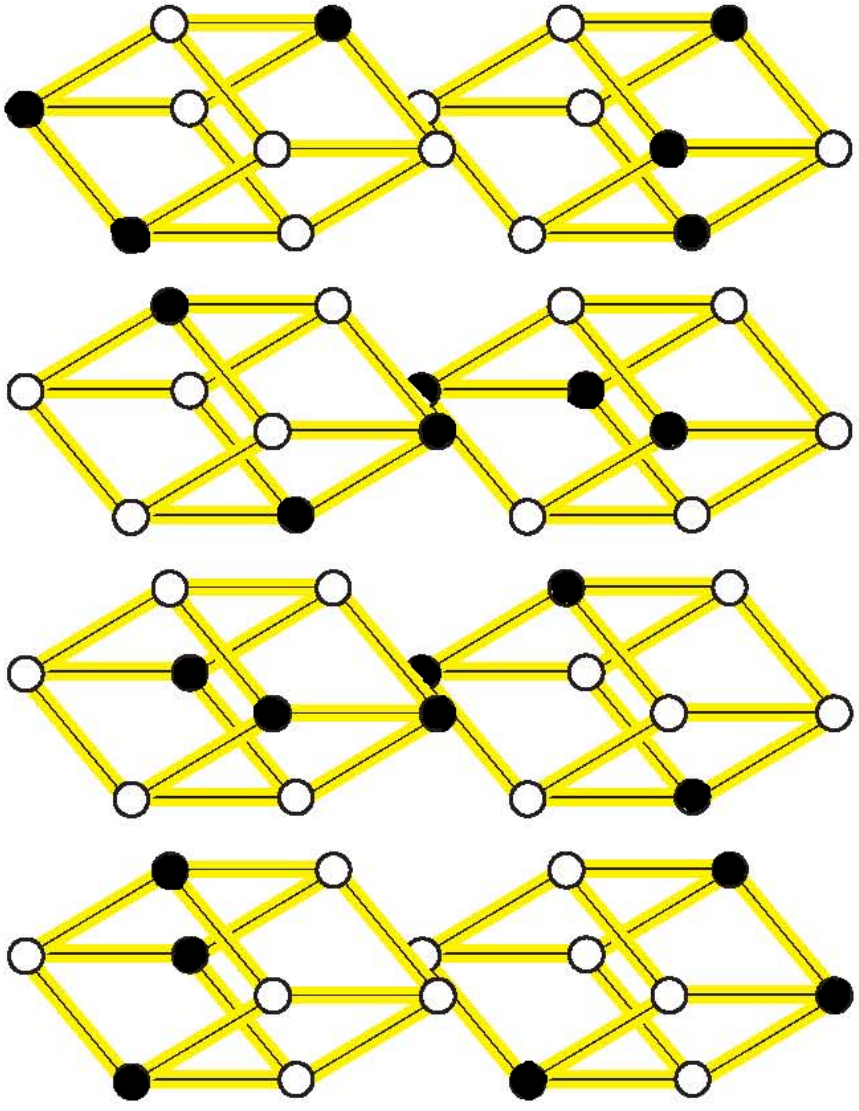
$$\sum_{z' \neq z''} \widehat{g}(z')\widehat{g}(z'')(-1)^{\langle x, z' \oplus z'' \rangle} = (b - c) \sum_{wt(z)>m} \widehat{g}(z)(-1)^{\langle x,z \rangle}.$$

Но $wt(z' \oplus z'') \leq 2n - wt(z') - wt(z'') < m$.

Теорема 6(Фон-Дер-Флаасс, 2007)

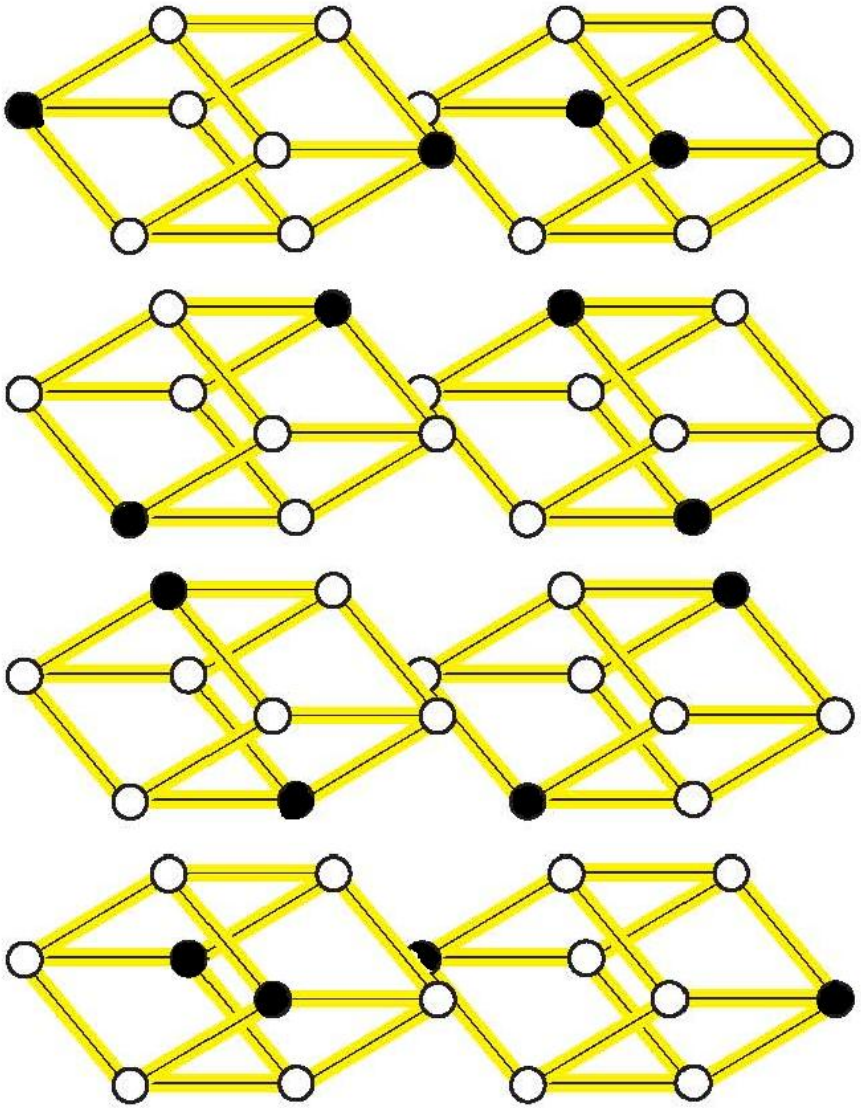
Пусть $f : E_2^n \to E_2$ неуравновешенная корреляционно-иммунная функция порядка $\mathrm{cor}(f) = \frac{2n}{3} - 1$. Тогда f — совершенная раскраска.

Параметры совершенных раскрасок достигающих границы Фон-Дер-Флаасса: $\begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 5 \\ 3 & 3 \end{pmatrix}$.



Утверждение 2.10 (Конструкция удвоения)

Пусть $f : E_2^n \to E_2$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда $g : E_2^{2n} \to E_2$, где $g(x, y) = f(x \oplus y)$, совершенная раскраска с матрицей параметров $2S$.



Проблема 1

Обобщить на q-значный гиперкуб теоремы 5 и 6.

Проблема 2

Существуют ли совершенные раскраски булева гиперкуба с матрицами параметров $\begin{pmatrix} 1 & 23 \\ 9 & 15 \end{pmatrix}$, $\begin{pmatrix} 2 & 22 \\ 10 & 14 \end{pmatrix}$, $\begin{pmatrix} 3 & 21 \\ 11 & 13 \end{pmatrix}$, $\begin{pmatrix} 0 & 25 \\ 7 & 18 \end{pmatrix}$?

Проблема 3

Найти асимптотику логарифма числа совершенных раскрасок булева гиперкуба с параметрами $\begin{pmatrix} 0 & 3n \\ n & 2n \end{pmatrix}$, $\begin{pmatrix} n & 5n \\ 3n & 3n \end{pmatrix}$ и $\begin{pmatrix} 0 & n \\ 1 & n+1 \end{pmatrix}$ при $n \to \infty$.