Совершенные комбинаторные структуры

В. Н. Потапов

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

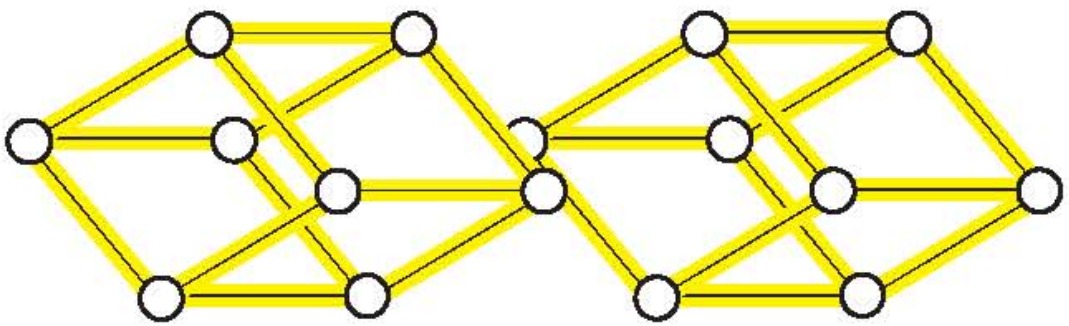
XI летняя школа <Современная математика>,
г. Дубна, 18-29 июля 2011 г.

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*).

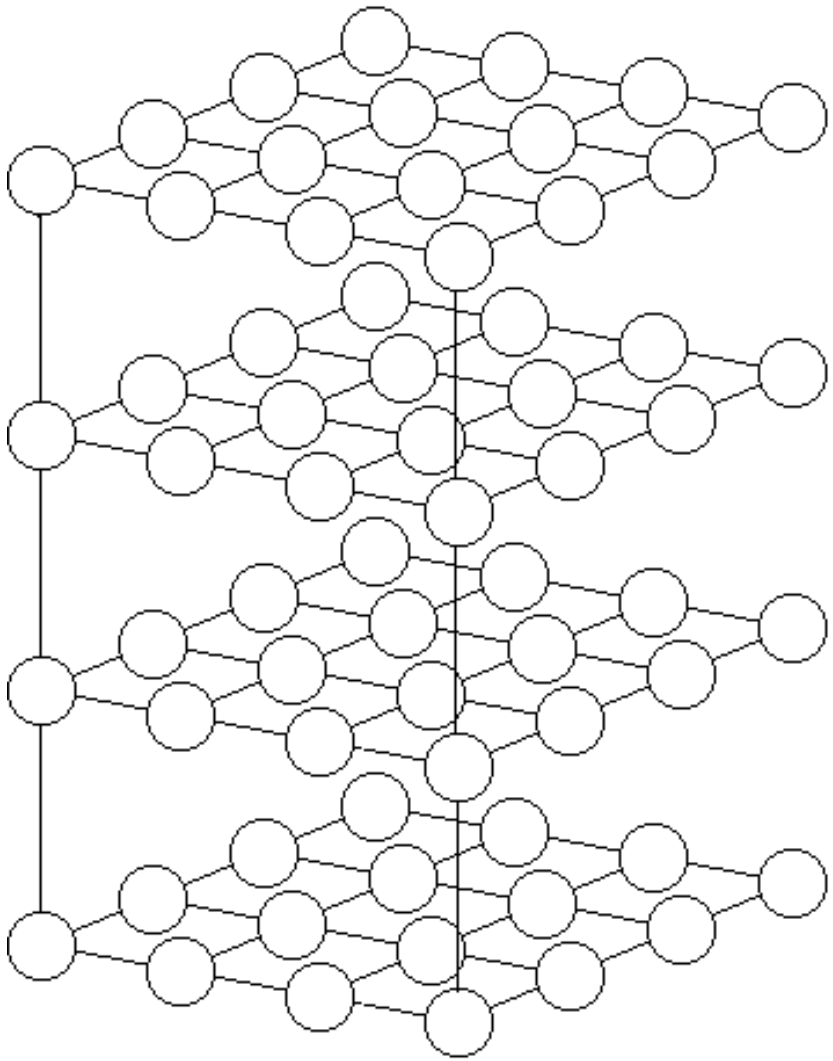
Определение

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

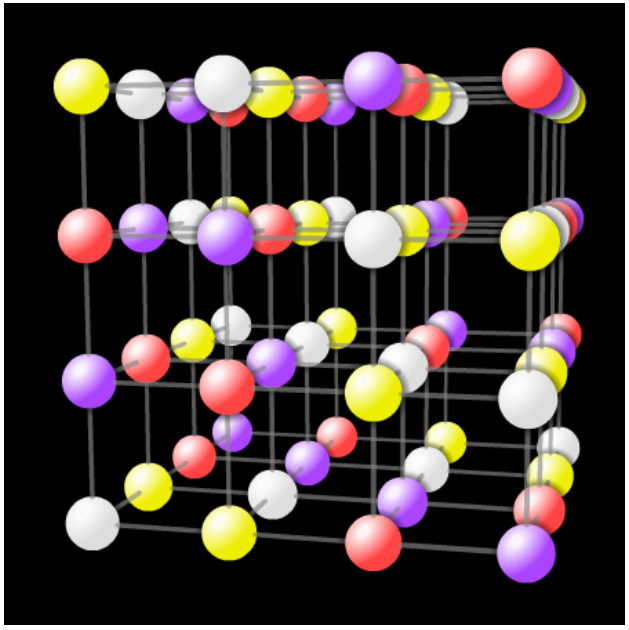
E_2^4



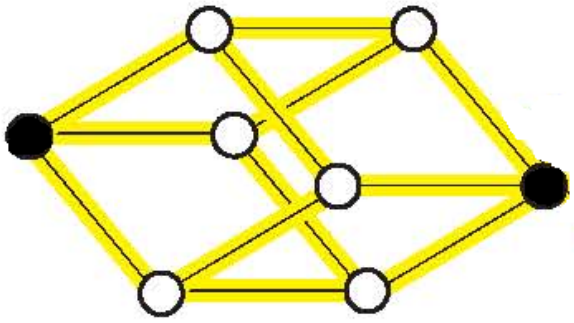
E_4^3

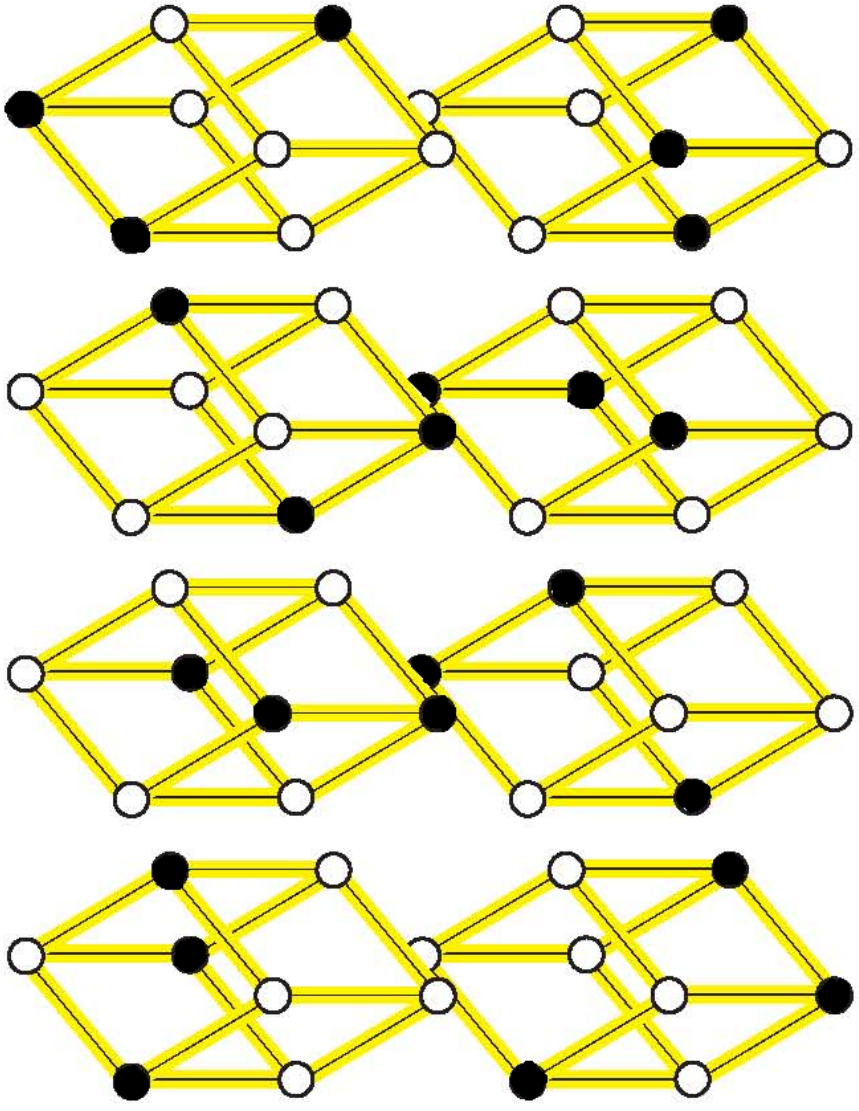


$f : E_q^n \to \{0, \ldots, k-1\}$.
Латинский куб. $q = k$.



Совершенный код $k = 2$.





Теорема (Фон-Дер-Флаасс, 2007)

Пусть $f : E_2^n \to E_2$ неуравновешенная непостоянная булева функция. Тогда $\mathrm{cor}(f) \leq \frac{2n}{3} - 1$ и если $\mathrm{cor}(f) = \frac{2n}{3} - 1$, то f — совершенная раскраска.

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 $x \in E_q^n$.

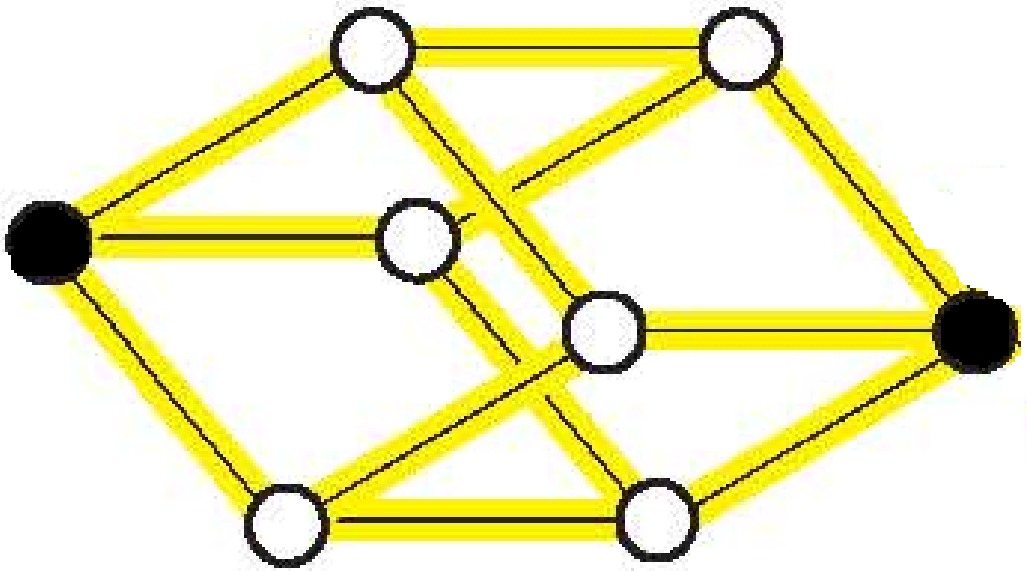
Утверждение 1.1

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 $x, y \in C$.

Заметим, что если $d(x,y) \geq 2\rho+1$ для любых различных $x, y \in C$, то $|C| \leq \nu(q,n)$.



Конструкция кода Хэмминга

Пусть $q = 2$, $n = 2^t - 1$. Пусть β_i — двоичная запись длины t числа i, $i \in \{0, \ldots, 2^t - 1\}$. Пусть матрица $D_t = (\beta_1, \ldots, \beta_n)$ составлена из векторов $i = 1, \ldots, n$. Например,

$$D_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Утверждение 1.3

Множество $C = \{x \in E_2^n \mid D_t x = \overline{0}\}$ является 1-совершенным кодом.

Здесь множество E_2^n рассматривается как векторное пространство над $GF(2)$.

Подобным образом можно построить 1-совершенный код Хэмминга в E_q^n, где $q = p^s$ — степень простого, $n = \frac{q^t-1}{q-1}$.

Заметим, что при нечётном n множество $\{\overline{0}, \overline{1}\}$ является $(n-1)/2$-совершенным кодом в E_2^n.

Теорема 1.1 (Зиновьев, Леонтьев, Тиетвайнен, 1972)

Нетривиальный совершенный код в E_q^n при $q = p^s$ должен иметь одни из следующих параметров:
1) $q = p^s$, $\rho = 1$, $n = \frac{q^t-1}{q-1}$;
2) $q = 3$, $\rho = 2$, $n = 11$;
3) $q = 2$, $\rho = 2$, $n = 23$.

Коды с параметрами 2) и 3) построены М.Голеем. Все коды с параметрами 2) и 3) являются линейными.

Определение

Множество $R \subset E_2^n$ называется *расширенным 1-совершенным кодом* , если $|R| = \frac{2^n}{2n}$, $d(x, y) \geq 4$ для любых различных $x, y \in R$.

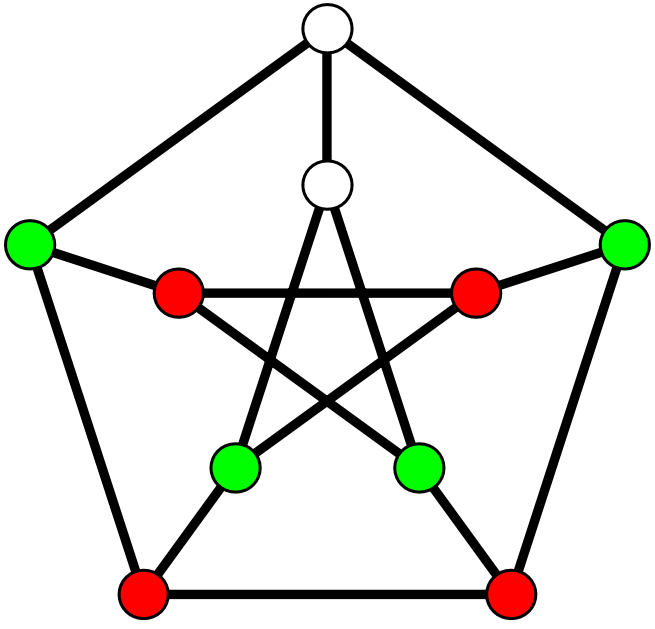
Утверждение 1.4

1) Пусть $R \subset E_2^n$ — расширенный 1-совершенный код, тогда множество
$\{(x_1, \ldots, x_{n-1}) \mid x \in R\}$ есть 1-совершенный код.
2) Пусть $C \subset E_2^n$ — 1-совершенный код, тогда множество
$\{(x_1, \ldots, x_n, |x|) \mid x \in C\}$ есть расширенный 1-совершенный код.

Определение

Совершенной раскраской куба E_q^n в k цветов называется отображение $Col : E^n \to \{1, \ldots, k-1, 0\}$, 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.



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

Утверждение 1.5

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: $m_{i,j} = 1$, если i-я и j-я вершины находятся на расстоянии 1, и $m_{i,j} = 0$ 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 1.2 (Августинович, 2000)

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 1.6

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

Утверждение 1.7

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 1.8

Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ матрица параметров совершенной раскраски булева куба E_2^n. Тогда число $\frac{2^n b}{b+c}$ целое.

Утверждение 1.9

Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ матрица параметров совершенной раскраски булева куба E_2^n. Тогда существует совершенная раскраска булева куба E_2^{n+1} с матрицей параметров $\begin{pmatrix} a+1 & b \\ c & d+1 \end{pmatrix}$.

Теорема 1.3 (Шапиро, Злотник, 1959)

Для любой совершенной раскраски $Col : E^n \to \{1, \ldots, k-1, 0\}$ и $t \in \mathbb{N}$ мощность пересечения $|Col^{-1}(i) \cap L_t(x)|$ зависит только от цветов i и $Col(x)$.

Теорема 1.3 (Шапиро, Злотник, 1959)

Для любой совершенной раскраски $Col : E^n \to \{1, \ldots, k-1, 0\}$ и $t \in \mathbb{N}$ мощность пересечения $|Col^{-1}(i) \cap L_t(x)|$ зависит только от цветов i и $Col(x)$.

Доказательство. Без ограничения общности считаем, что $x = \overline{0}$. Пусть r_t — число вершин из $L_{t-1}(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$; l_t — число вершин из $L_{t+1}(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$.
Пусть M_t — матрица смежности расстояний t в кубе E_q^n.

$$M_t M = M_{t+1} r_{t+1} + M_{t-1} l_{t-1},$$

$M_1 = M$, $M_0 = E$, $M_t = p_t(M)$.

$$M_t F_{col} = p_t(M) F_{col} = F_{col} p_t(S).$$

F_{col} — совершенная раскраска графа расстояний t по теореме 1.2.

Определение

Подмножество $C \subseteq E_2^n$ называется *антиподальным*, если из $x \in C$ следует, что $x \oplus \overline{1} \in C$.

Утверждение 1.10

Любой 1-совершенный код $C \subseteq E_2^n$ антиподальный.

Теорема 1.4 (Августинович, 1995)

Пусть C_1 и C_2 1-совершенные коды в E_2^n. Если $C_1 \cap L_{(n-1)/2} = C_2 \cap L_{(n-1)/2}$, то $C_1 = C_2$.

Определение

Множество $L_{(n-1)/2}$ и любое другое удовлетворяющее условию теоремы 1.4 называется *тестовым* для 1-совершенных кодов.

Проблема 1.1

Найти тестовое для 1-совершенных кодов множество меньшей мощности.

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

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

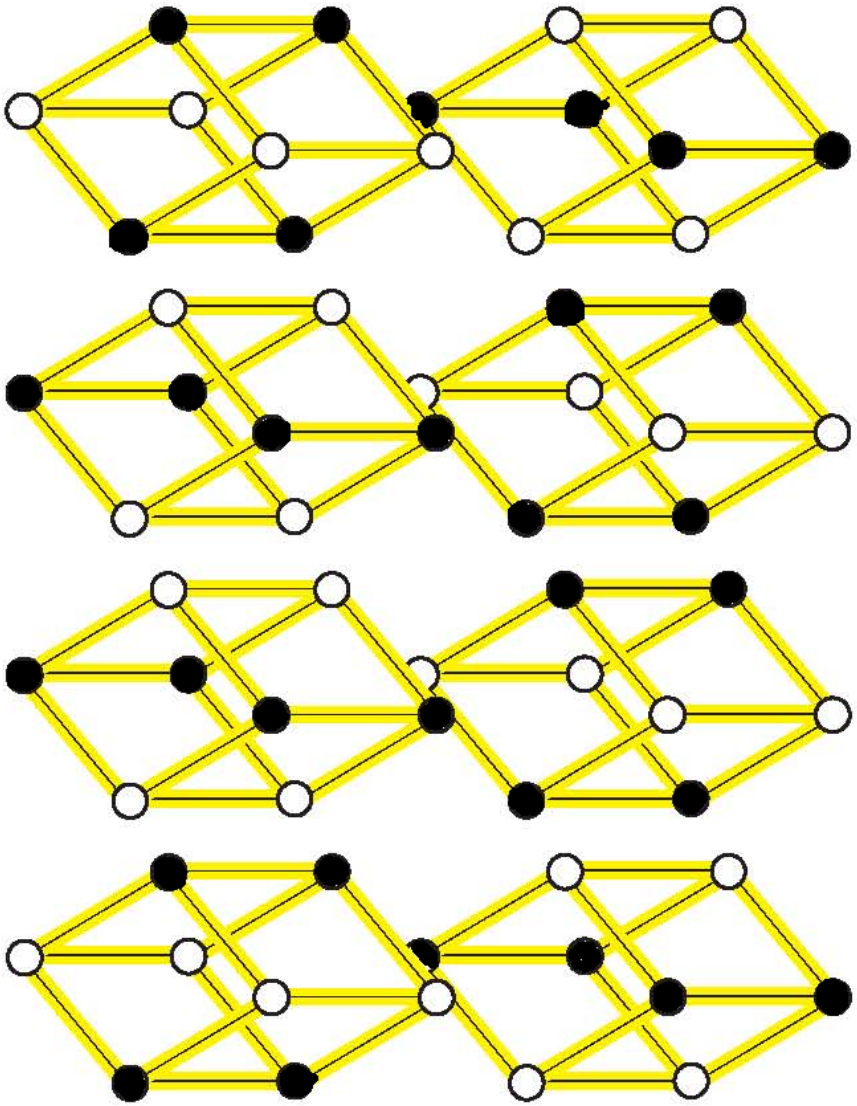
Определение

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 ортонормальный 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 $|f^{-1}(j) \cap \Gamma|$ 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 $z = (z', \overline{0})$, $|z'| \leq m$.

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

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

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 2.5

Если $f : E_q^n \to E_2$ и $\widehat{f}(z) = 0$ при $0 < wt(z) \leq m$, то f — корреляционно-иммунная функция порядка 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 $f : E_q^n \to E_2$ и $\widehat{f}(z) = 0$ при $0 < wt(z) \leq m$, то f — корреляционно-иммунная функция порядка m.

Определение

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

Теорема 2.1 (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 $wt(z' \oplus z'') \leq 2n - wt(z') - wt(z'') < m$.

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 2.7

Пусть $f : E_2^n \to E_2$ — 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 булева куба E_2^n с собственным числом $n - (b + c)$.

Утверждение 2.8

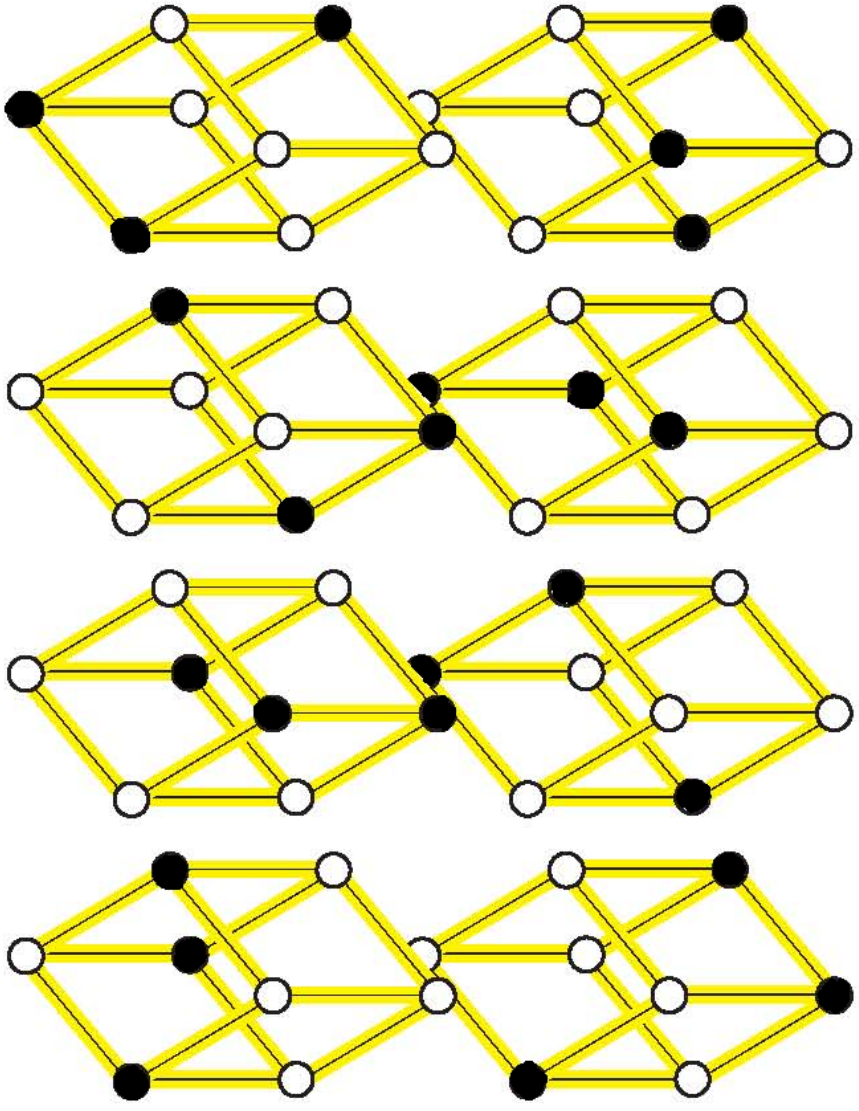
1) Если $f : E_2^n \to E_2$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $\widehat{f}(z) = 0$ при $wt(z) \neq 0, \frac{b+c}{2}$.

2) Если $\widehat{f}(z) = 0$ при $wt(z) \neq 0, s$ для некоторой функции $f : E_2^n \to E_2$, то f — совершенная раскраска.

Теорема 2.2 (Фон-Дер-Флаасс, 2007)

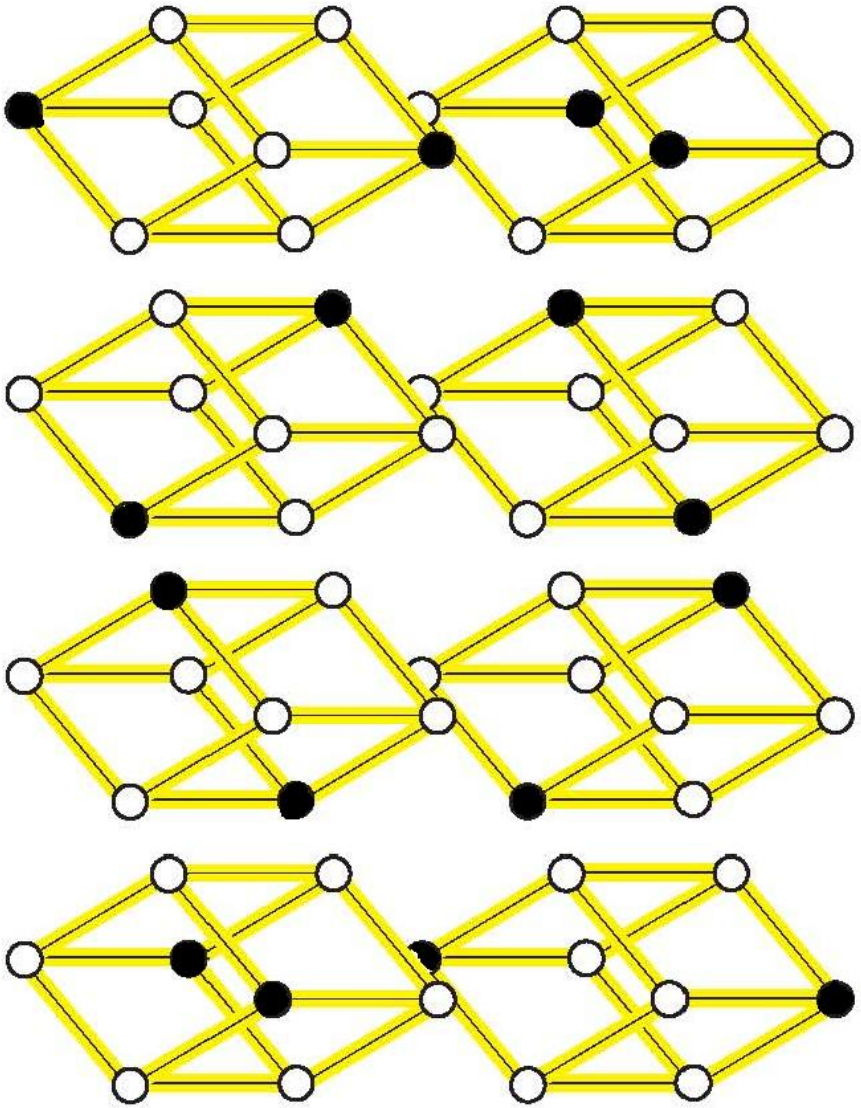
Пусть $f : E_2^n \to E_2$ неуравновешенная корреляционно-иммунная функция порядка $\mathrm{cor}(f) = \frac{2n}{3} - 1$. Тогда f — совершенная раскраска.

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 2.9 (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 $2S$.



Определение

Пусть $f : E_2^n \to E_2$, будем называть *плотностью*
$\varrho(f) = \frac{|\{x \in E_q^n \mid f(x)=1\}|}{2^n}$.

Теорема 2.3 (Фридман, 1992, Биербрауэр, 1995)

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

Определение

Пусть $f : E_2^n \to E_2$, будем называть *плотностью* $\varrho(f) = \frac{|\{x \in E_q^n \mid f(x)=1\}|}{2^n}$.

Теорема 2.3 (Фридман, 1992, Биербрауэр, 1995)

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

Доказательство. Пусть $m = \mathrm{cor}(f)$.

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

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

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

Теорема 2.4 (Потапов, 2010)

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

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

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

Теоремы 2.3–2.5 обобщаются на q-значный куб.

Проблема 2.1

Обобщить на q-значный куб теоремы 2.1, 2.2.

Проблема 2.2

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

Пусть $A = \{a_{ij}\}$ — матрица размера $n \times n$.

Определение

Перманентом матрицы A называется

$$\mathrm{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}.$$

Число $\mathrm{per}(A)$ не изменяется при перестановке строк и столбцов матрицы A. Перманент матрицы можно вычислить, используя разложение по строке (аналогично определителю).
Если A — $(0,1)$-матрица, то неравенство $\mathrm{per}(A) \neq 0$ эквивалентно наличию диагонали из 1.

Теорема 3.1 (Ф.Холл, 1935)

Для неотрицательной матрицы A размера $n \times n$ имеем $\mathrm{per}(A) = 0$ тогда и только тогда, когда A содержит нулевую подматрицу размера $k_1 \times k_2$, где $k_1 + k_2 > n$.

Доказательство. Индукция по n. Докажем для $n+1$. Пусть сумма $k_1 + k_2$ максимальна, возможны два случая:
1) $k_1 + k_2 \leq n$. Выберем ненулевой элемент a_{ij}. Вычеркнем i-ю строку и j-й столбец. У оставшейся матрицы положительный перманент по предположению индукции.
2) $k_1 + k_2 = n + 1$. Без ограничения общности считаем, что подматрица из нулей размера $k_1 \times k_2$ находится в правом верхнем углу. Тогда матрица A имеет блочную структуру и $\mathrm{per}(A) = \mathrm{per}(A_1) \cdot \mathrm{per}(A_2)$, где A_1 имеет размер $k_1 \times k_1$, A_2 имеет размер $k_2 \times k_2$. Пусть $\mathrm{per}(A_1) = 0$, тогда по предположению индукции A_1 имеет подматрицу из нулей размера $m_1 \times m_2$, $m_1 + m_2 > k_1$. Тогда матрица A имеет подматрицу из нулей размера $m_1 \times (k_2 + m_2)$ и $m_1 + m_2 + k_2 > n + 1$.

Теорема 3.2 (Кёниг, 1916)

Если $(0,1)$-матрица A содержит t единиц в каждом столбце и строке, то $\mathrm{per}(A) \neq 0$.

Теорема 3.2 (Кёниг, 1916)

Если $(0,1)$-матрица A содержит t единиц в каждом столбце и строке, то $\mathrm{per}(A) \neq 0$.

Доказательство. Без ограничения общности считаем, что максимальная подматрица из нулей размера $k_1 \times k_2$ находится в правом верхнем углу. Пусть A_1 левая верхняя подматрица из первых k_1 строк и $n - k_2$ столбцов. Подсчитаем число единиц в A_1 по строкам и по столбцам: $k_1 t \leq (n - k_2)t$. Тогда $k_1 + k_2 \leq n$.

Определение

Функция $f : X^n \to X$ называется *n-арной квазигруппой*, если она обратима по каждой своей переменной.

Утверждение 3.1

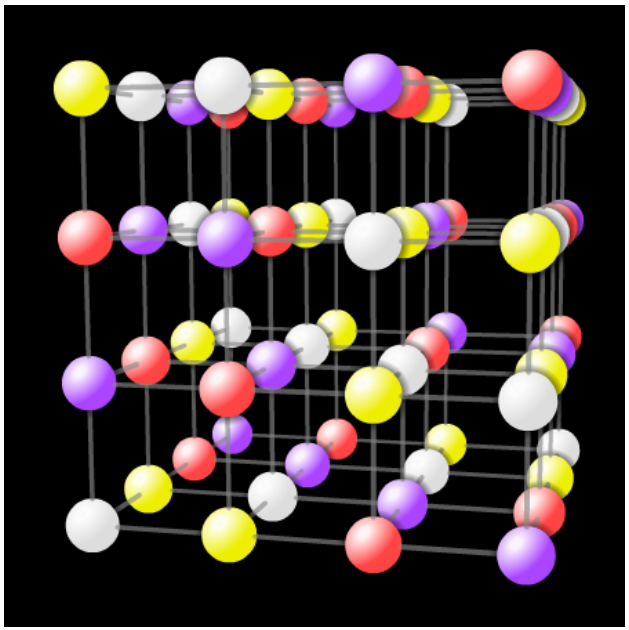
Функция $f : E_q^n \to E_q$ является *n-арной квазигруппой* тогда и только тогда, когда из $d(x, y) = 1$ следует, что $f(x) \neq f(y)$.

Определение

Число q называется *порядком* n-арной квазигруппы.

Определение

Таблица значений n-арной квазигруппы называется *латинским n-кубом*, при $n = 2$ — *латинским квадратом*.



0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Утверждение 3.2

Каждый латинский прямоугольник размера $q \times m$ дополняется до латинского квадрата $q \times q$ ($m \leq q$).

Утверждение 3.3

Каждый латинский параллелепипед размера $q \times \cdots \times q \times 1$ дополняется до латинского n-куба.

Утверждение 3.4

Каждый латинский параллелепипед размера $q \times \cdots \times q \times (q-1)$ дополняется до латинского n-куба.

Утверждение 3.2

Каждый латинский прямоугольник размера $q \times m$ дополняется до латинского квадрата $q \times q$ ($m \leq q$).

0	1	2	3
1	3	0	2
x	x	x	x
x	x	x	x

1	0	1	0
1	1	0	0
0	0	1	1
0	1	0	1

Утверждение 3.3

Каждый латинский параллелепипед размера $q \times \cdots \times q \times 1$ дополняется до латинского n-куба.

Утверждение 3.4

Каждый латинский параллелепипед размера $q \times \cdots \times q \times (q-1)$ дополняется до латинского n-куба.

Определение

Множество $C \subset E_q^n$ называется МДР-*кодом с расстоянием* ρ, если $|C \cap \Gamma| = 1$ для каждой грани размерности $\rho - 1$.

В частности, если C есть МДР-код кодом с расстоянием ρ, то $\mathrm{cor}(\chi^C) = n - \rho + 1$.

Утверждение 3.5

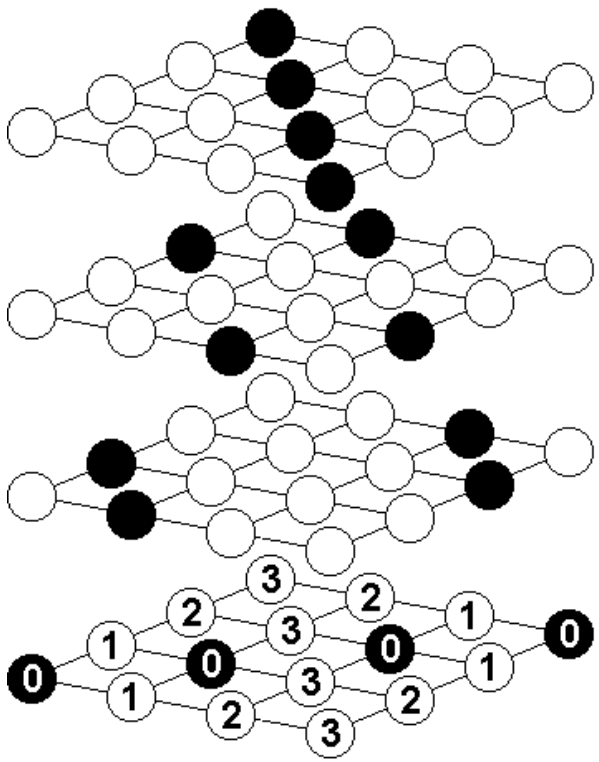
Если C есть МДР-код код с расстоянием 2, то χ^C — совершенная раскраска в 2 цвета.

Утверждение 3.6

Функция $f : E_q^n \to E_q$ является *n-арной квазигруппой* тогда и только тогда, когда её график $C = \{(x, f(x)) \mid x \in E_q^n\}$ является МДР-кодом с расстоянием 2.

Утверждение 3.7

Куб E_q^n содержит МДР-коды с расстоянием 2 при любых натуральных n и q.



Определение

Булевозначная корреляционно-иммунная функция $f : E_q^n \to E_2$ называется *расщепляемой*, если множество $\{x \in E_q^n \mid f(x) = 1\}$ является объединением не пересекающихся МДР-кодов.

Утверждение 3.8

Пусть $C \subset E_4^n$, $|C \cap \Gamma| = 2$ для каждой одномерной грани Γ, т. е. C есть 2-кратный МДР-код. Тогда

1) 2-МДР-код C — расщепляем, если и только если он определяется латинским параллелепипедом размера $4 \times \cdots \times 4 \times 2$;

2) 2-МДР-код $E_4^n \setminus C$ расщепляем, если и только если этот параллелепипед продолжаем до латинского куба;

3) 2-МДР-коды C и $E_4^n \setminus C$ расщепляемы одновременно.

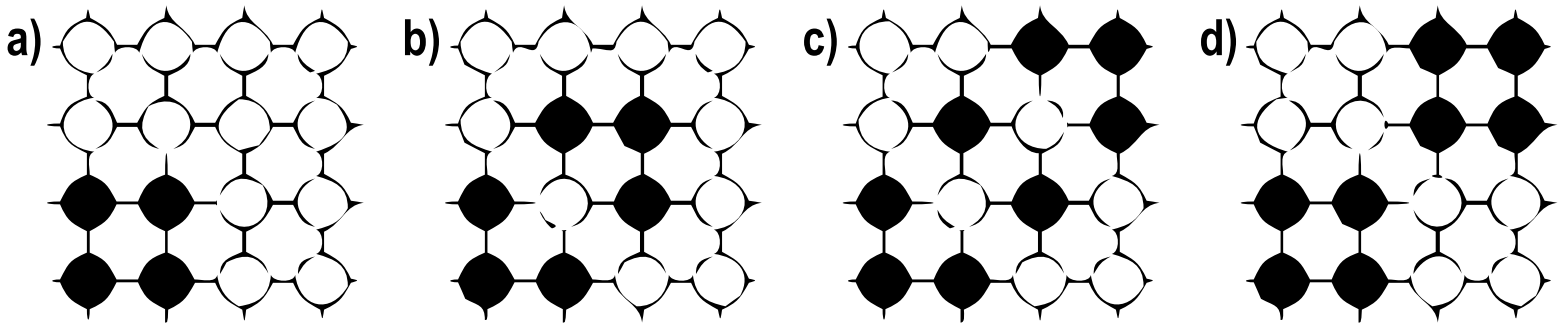


Рис.:

Задачи.

1) Найти число таких подмножеств $C \subset E_3^n$, что $|C \cap \Gamma| = 2$ для любой одномерной грани Γ.

2) Найти число таких подмножеств $C \subset E_3^n$, что $|C \cap \Gamma| \in \{0, 2\}$ для любой одномерной грани Γ.

3) Найти число таких расщепляемых подмножеств $C \subset E_3^n$, что $|C \cap \Gamma| \in \{0, 2\}$ для любой одномерной грани Γ.

Используя неравенство Биербрауэра — Фридмана $\varrho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$, можно доказать

Утверждение 3.9

Пусть $C \subset E_q^n$ МДР-код с расстоянием 3. Тогда $n \leq q + 1$.

Утверждение 3.10

Пусть $C \subset E_q^n$ МДР-код с расстоянием $\rho > 2$. Тогда $n \leq q + \rho - 2$.

Утверждение 3.11

Пусть $C \subset E_q^n$ МДР-код с расстоянием 3 и $n = q + 1$. Тогда C — 1-совершенный код.

Утверждение 3.12

Пусть $C \subset E_q^n$ МДР-код с расстоянием $\rho = m + 1$. Тогда

$$C = \{(x_1, \ldots, x_{n-m}, f_1(x), \ldots, f_m(x)) \mid x \in E_q^{n-m}\},$$

где f_i — $(n-m)$-квазигруппы.

Определение

Система из N n-квазигрупп $f_1, \ldots, f_N$ называется *ортогональной*, если для любого поднабора из n n-квазигрупп имеем

$$\{(f_{i_1}(x), \ldots, f_{i_n}(x)) \mid x \in E_q^n\} = E_q^n.$$

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

00	11	22	33
12	03	30	21
23	32	01	10
31	20	13	02

Определение

Ретрактом n-квазигруппы f называется подфункция, полученная фиксацией нескольких переменных.

Утверждение 3.13

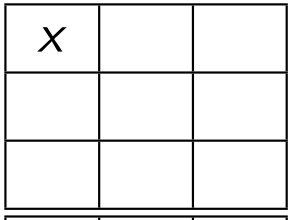
Подмножество $C \subset E_q^n$ является МДР-код с расстоянием $\rho = m + 1$ тогда и только тогда, когда

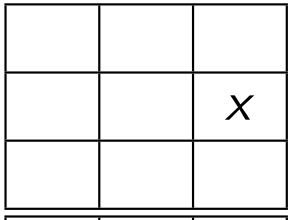
$$C = \{(x_1, \ldots, x_{n-m}, f_1(x), \ldots, f_m(x)) \mid x \in E_q^{n-m}\}$$

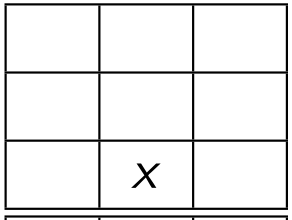
и набор $f_1, \ldots, f_m$, а также все его ретракты (полученные одинаковой фиксацией переменных) являются ортогональными.

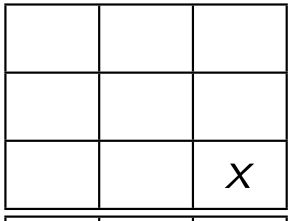
0	1	2
1	2	0
2	0	1

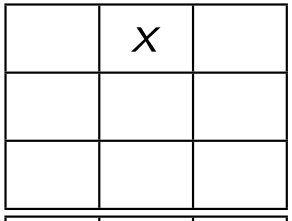
0	1	2
2	0	1
1	2	0

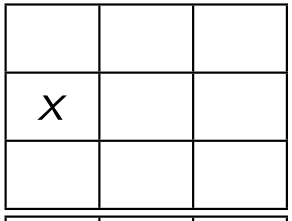


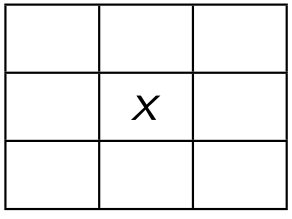


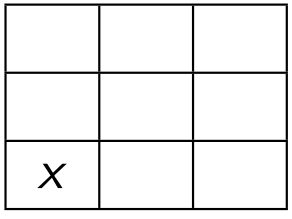


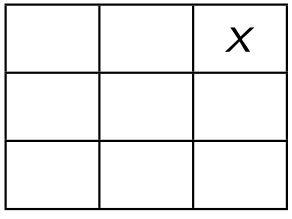












Утверждение 3.14

В E_2^n не существует МДР-кодов с расстоянием ρ при $2 < \rho < n$.

Утверждение 3.15

Если $f_1, \ldots, f_m$ — система ортогональных латинских квадратов (2-квазигрупп) на E_q, то $m \leq q - 1$.

Утверждение 3.16

Если $q = p^s$ — степень простого числа, то на E_q имеется система $f_1, \ldots, f_{q-1}$ ортогональных латинских квадратов.

Утверждение 3.14

В E_2^n не существует МДР-кодов с расстоянием ρ при $2 < \rho < n$.

Утверждение 3.15

Если $f_1, \ldots, f_m$ — система ортогональных латинских квадратов (2-квазигрупп) на E_q, то $m \leq q - 1$.

Утверждение 3.16

Если $q = p^s$ — степень простого числа, то на E_q имеется система $f_1, \ldots, f_{q-1}$ ортогональных латинских квадратов.

Доказательство Рассмотреть $f_i(x, y) = x + iy$, где арифметические операции выполняются в поле $GF(q)$.

Утверждение 3.17

Если $q \neq 4k + 2$, $k \in \mathbb{N}$, то на E_q найдётся пара ортогональных латинских квадратов.

Теорема 3.3 (Паркер, Боус, Шрикхенд, 1960)

При $q \neq 1, 2, 6$ на E_q найдётся пара ортогональных латинских квадрата.

Определение

Изометрией метрического пространства X называется отображение $\varphi : X \to X$ сохраняющее расстояние: $d(x, y) = d(\varphi(x), \varphi(y))$ для любых $x, y \in X$.

Изометрии образуют группу относительно композиции отображений. Группу изометрий обозначают через $\mathrm{Aut}(X)$.

Утверждение 4.1

Изометрия E_q^n переводит ρ-совершенный код в ρ-совершенный код и совершенную раскраску в совершенную раскраску.

Утверждение 4.2

Изометрия E_q^n переводит МДР-код в МДР-код.

Определение

Коды и раскраски, переводимые друг в друга изометриями куба, называют *эквивалентными*.

Определение

Изотопией в E_q^n называется упорядоченный набор из n перестановок $\theta_i : E_q \to E_q$, $\theta x = (\theta_1 x_1, \ldots, \theta_n x_n)$.

Множество $\theta M \triangleq \{\theta x \,|\, x \in M\}$ называют изотопным множеству M.

Изотопии E_q^n образуют группу $\Theta_{nq} \simeq (S_q)^n$.

Определение

Парастрофией в E_q^n называется перестановка координат $\tau \in S_n$, $x_\tau = (x_{\tau(1)}, \ldots, x_{\tau(n)})$.

Множество $M_\tau \triangleq \{x_\tau \,|\, x \in M\}$ парастрофным множеству M.

Теорема 4.1 (Марков, 1956)

$\mathrm{Aut}(E_q^n) = \Theta_{nq} \rtimes S_n$.

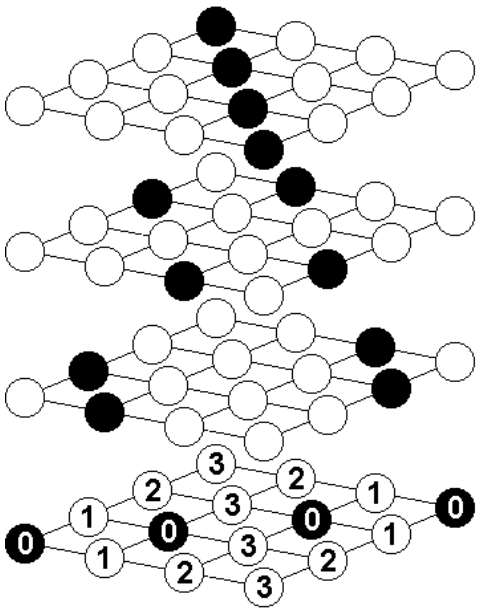
$\varphi(x) = (\theta, \tau)(x) = \theta(x_\tau)$,
$\varphi_1 \circ \varphi_2 = (\theta^1, \tau^1) \circ (\theta^2, \tau^2) = (\theta^1 \circ \theta', \tau^1 \circ \tau^2)$, где θ' зависит от θ^2 и τ^1.

Определение

Функция $f : X^n \to X$ называется *n-арной квазигруппой*, если она обратима по каждой своей переменной.

Утверждение 3.1

Функция $f : E_q^n \to E_q$ является *n-арной квазигруппой* тогда и только тогда, когда из $d(x, y) = 1$ следует, что $f(x) \neq f(y)$.



Определение

Парастрофией и изотопией n-квазигруппы называются, соответственно, парастрофия и изотопия её графика (МДР-кода). n-Квазигруппы называются эквивалентными, если эквивалентны их графики.

$g(x_1, \ldots, x_n) = f(x_{\tau(1)}, \ldots, x_{\tau(n)})$ перестановка координат,
$x_i = g(x_1, \ldots x_{i-1}, x_0, x_{i+1}, \ldots, x_n) \Leftrightarrow x_0 = f(x_1, \ldots, x_n)$
обращение по i-ой переменной,
$g(x_1, \ldots, x_n) = f(\theta_1 x_1, \ldots, \theta_n x_n)$ главная изотопия,
$g(x_1, \ldots, x_n) = \theta_0 f(x_1, \ldots, x_n)$ переименование значений.

Определение

Если у n-арной квазигруппы f или у функции, обратной ей по некоторому аргументу, зафиксировать один или более аргументов, то мы получим квазигруппу некоторой меньшей размерности k, называемую *ретрактом* n-квазигруппы f.

Пусть имеется $(n-m+1)$-квазигруппа h и m-квазигруппа g, тогда их суперпозиция

$$f(x_1,\ldots,x_n) \equiv h(g(x_1,\ldots,x_m),x_{m+1},\ldots,x_n)$$

является n-арной квазигруппой.

Утверждение 4.3

Класс квазигрупп замкнут относительно изометрии куба, операций суперпозиции и взятия ретракта.

Утверждение 4.4

При любом n все n-арные квазигруппы порядка 3 эквивалентны.
Имеется ровно $3 \cdot 2^n$ различных n-арных квазигрупп порядка 3.

0	1	2
1		
2		

1		

2		

Утверждение 4.4

При любом n все n-арные квазигруппы порядка 3 эквивалентны.
Имеется ровно $3 \cdot 2^n$ различных n-арных квазигрупп порядка 3.

0	1	2
1	2	0
2	0	1

1	2	0
2	0	1
0	1	2

2	0	1
0	1	2
1	2	0

Утверждение 4.5

Имеется два класса эквивалентности 2-квазигрупп порядка 4. Каждая 2-квазигрупп порядка 4 изотопна группе.

Утверждение 4.5

Имеется два класса эквивалентности 2-квазигрупп порядка 4.
Каждая 2-квазигрупп порядка 4 изотопна группе.

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Определение

Объединение двух не пересекающихся МДР-кодов называется *2-кратным МДР-кодом*.

Определение

2-Кратный МДР-код называется *линейным*, если он эквивалентен 2-кратному МДР-коду $L \subset \Sigma^n$ с линейной характеристической функцией

$$\chi^L(x_1, \ldots, x_n) \equiv \chi^{\{0,1\}}(x_1) \oplus \cdots \oplus \chi^{\{0,1\}}(x_n).$$

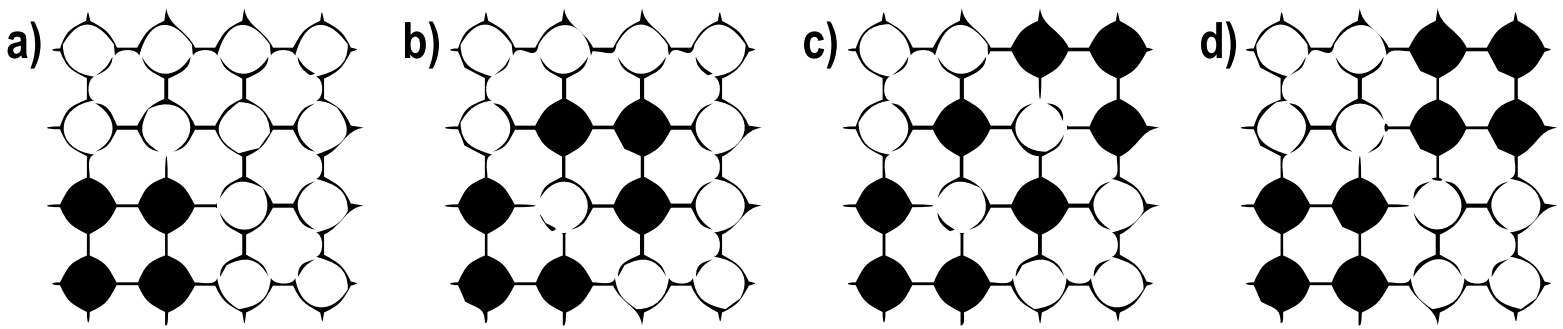
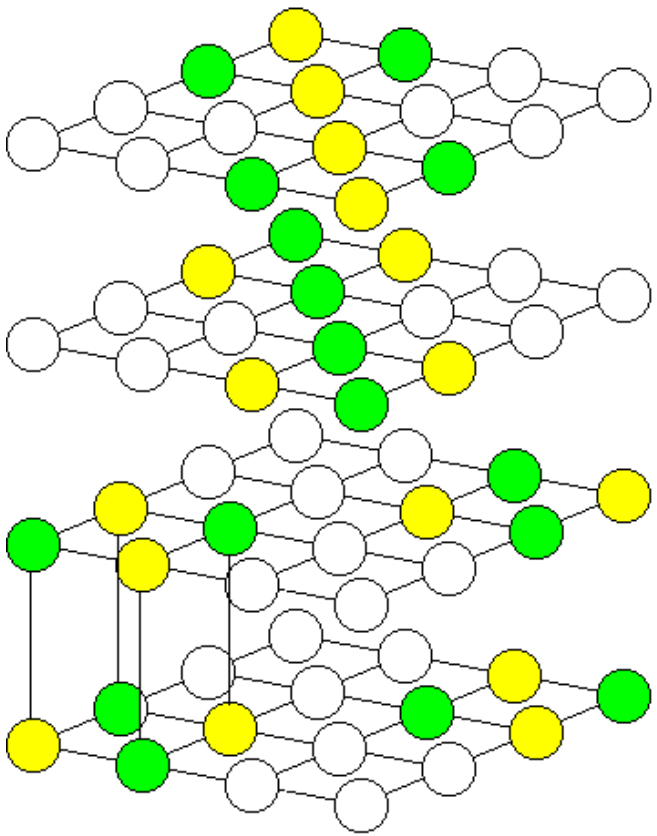


Рис.:

Пусть f — n-арная квазигруппа порядка 4 и $a, b \in E_4, a \neq b$. Множество

$$S_{a,b}(f) = \{(x_1, \ldots, x_n) \in E_4^n \mid f(x_1, \ldots, x_n) \in \{a, b\}\}$$

является 2-кратным МДР-кодом.



Определение

n-Арная квазигруппа f порядка 4 называется *полулинейной*, если для некоторых $a, b \in E_4$ множество $S_{a,b}(f)$ линейно.

Теорема 4.2 (Кротов, 2000)

Имеется ровно $3^{n+1}2^{2^{2^n}+1} - 3^n 2^{n+3}$ различных n-арных квазигрупп порядка 4.

Конструкция совершенных кодов

Зафиксируем $R \subset E_2^n$ — расширенный код Хэмминга. Пусть $M_{\overline{r}} \subset E_4^n$ — МДР-код с расстоянием 2. Определим разбиение E_2^4 на коды равенством $C_a^r = C_0 + (1 + r)\overline{e}_4 + \overline{e}_a$, где $r \in \{0, 1\}$, $a \in \Sigma$, $C_0 = \{\overline{0}, \overline{1}\} \subset E_2^4$, $\overline{e}_i \in E_2^4$ — единичные вектора с 1 на i-м месте (считаем, что $\overline{e}_0 = \overline{e}_4$).

$C_0^0 = \{(0000), (1111)\}$, $C_1^0 = \{(0110), (1001)\}$, $C_2^0 = \{(0101), (1010)\}$, $C_3^0 = \{(0011), (1100)\}$, $C_0^1 = \{(0001), (1110)\}$, $C_1^1 = \{(0111), (1000)\}$, $C_2^1 = \{(0100), (1011)\}$, $C_3^1 = \{(0010), (1101)\}$.

Теорема 4.3 (Фелпс, 1984)

Множество

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

является расширенным 1-совершенным кодом.

Утверждение 4.6

Имеется не менее $2^{2^{1+n/2}/n}$ расширенных 1-совершенных кодов в E_2^n.

Теорема 4.4 (Васильев, 1962)

Существуют нелинейные 1-совершенные коды.

Определение

n-Арная квазигруппа f называется *разделимой*, если имеются целое число m, $2 \leq m < n$, $(n-m+1)$-арная квазигруппа h, m-арная квазигруппа g и перестановка $\sigma \in S_n$ такие, что

$$f(x_1, \ldots, x_n) \equiv h\big(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}\big).$$

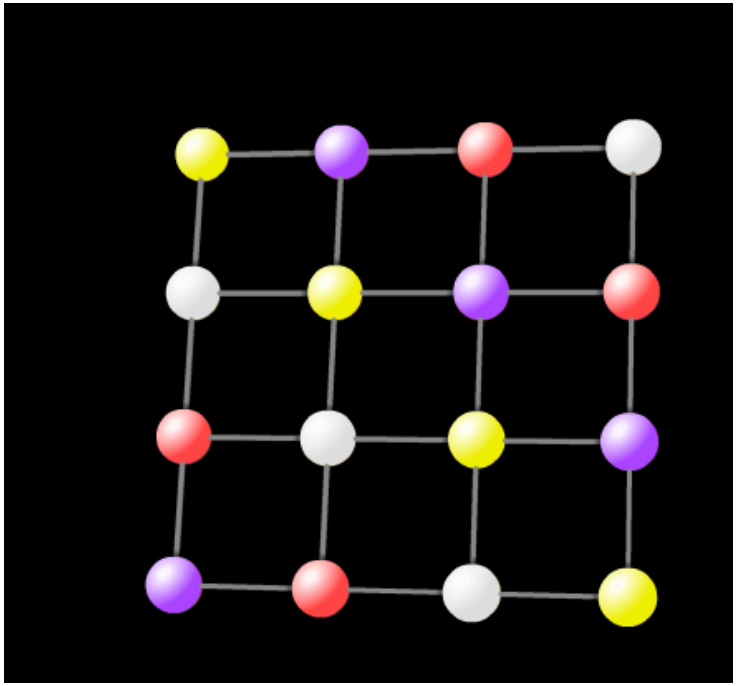
Утверждение 4.7

Пусть f — n-арная квазигруппа. Если из $f(x, \overline{0}) = f(x', \overline{0})$ следует $f(x, y) = f(x', y)$ для любого $y \in E_q^k$, то $f(x, y) \equiv g(h(x), y)$.

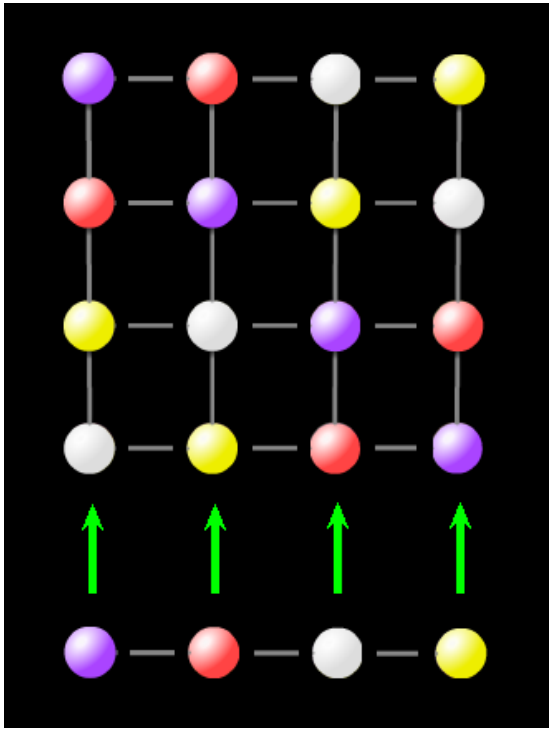
Утверждение 4.8

n-Арная квазигруппа порядка q является разделимой тогда и только тогда, когда произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, у неё имеется только q различающихся ретракта.

Внутренняя квазигруппа:



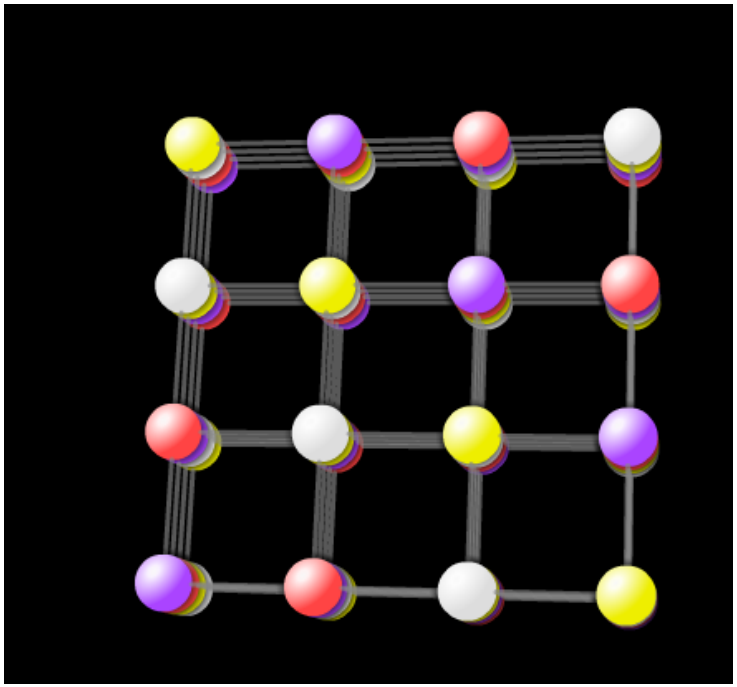
Внешняя квазигруппа:



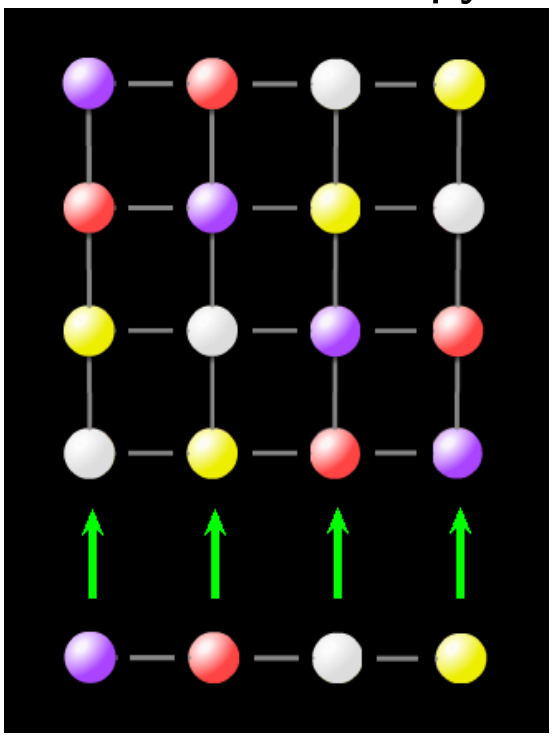
Утверждение 4.8

n-Арная квазигруппа порядка q является разделимой тогда и только тогда, когда произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, у неё имеется только q различающихся ретракта.

Внутренняя квазигруппа $\rightarrow$ Композиция:



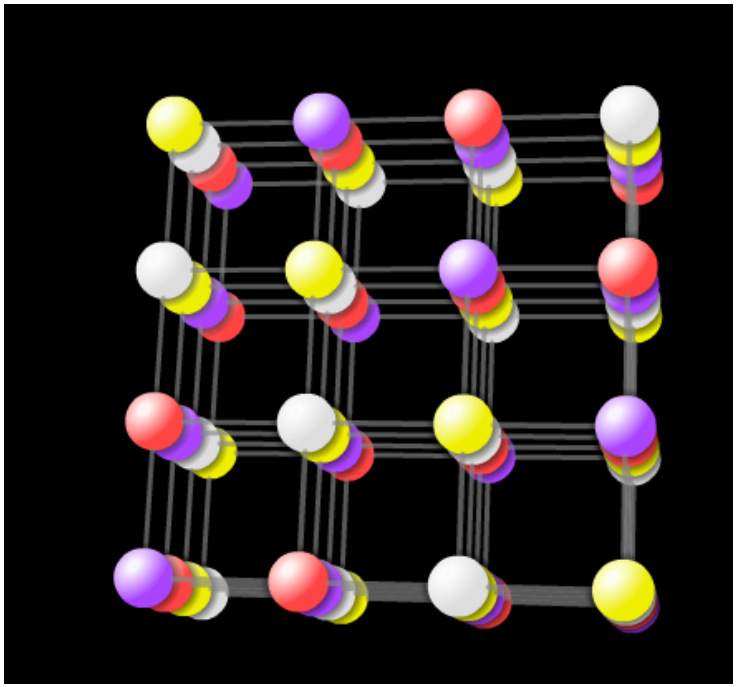
Внешняя квазигруппа:



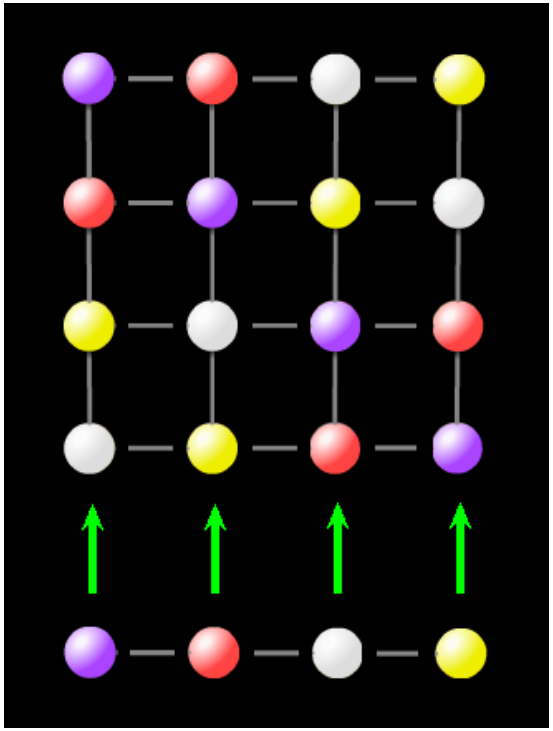
Утверждение 4.8

n-Арная квазигруппа порядка q является разделимой тогда и только тогда, когда произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, у неё имеется только q различающихся ретракта.

Внутренняя квазигруппа $\rightarrow$ Композиция:



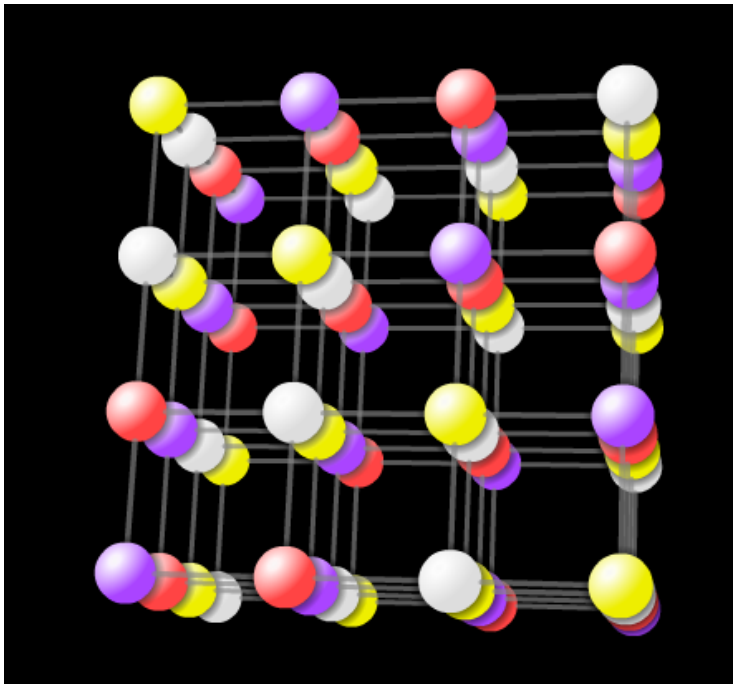
Внешняя квазигруппа:



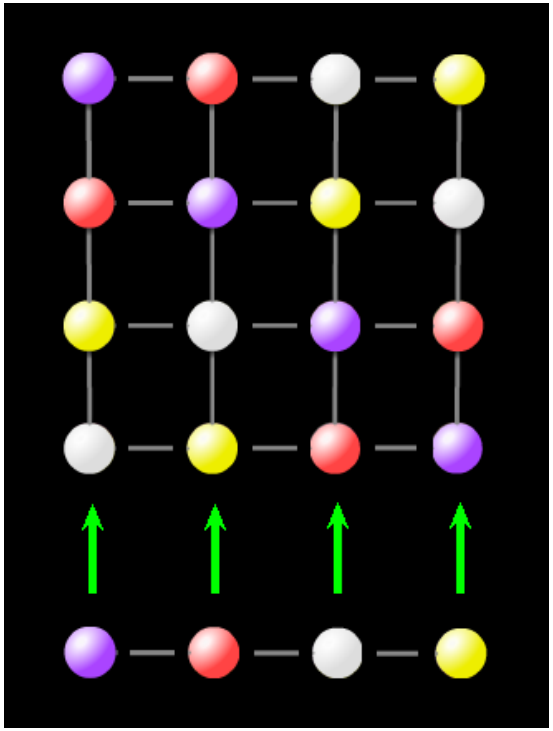
Утверждение 4.8

n-Арная квазигруппа порядка q является разделимой тогда и только тогда, когда произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, у неё имеется только q различающихся ретракта.

Внутренняя квазигруппа $\rightarrow$ Композиция:



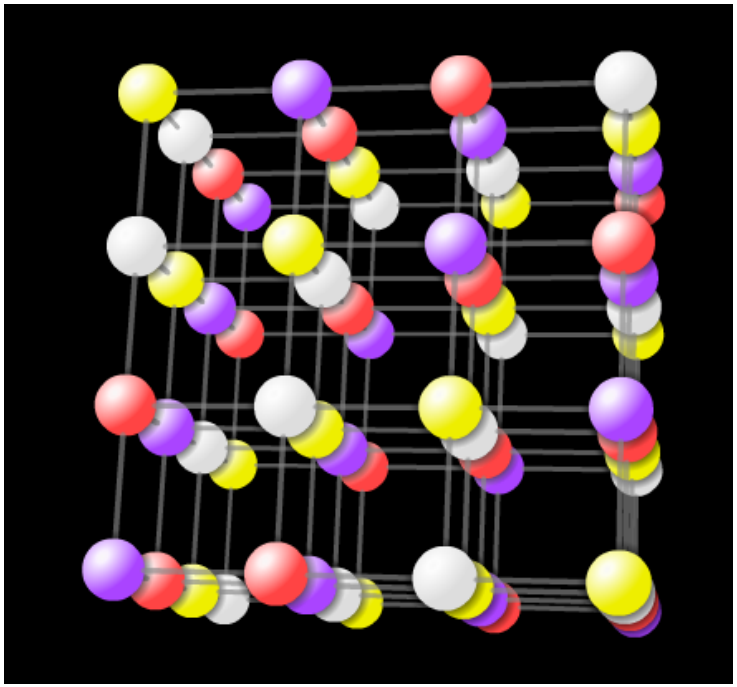
Внешняя квазигруппа:



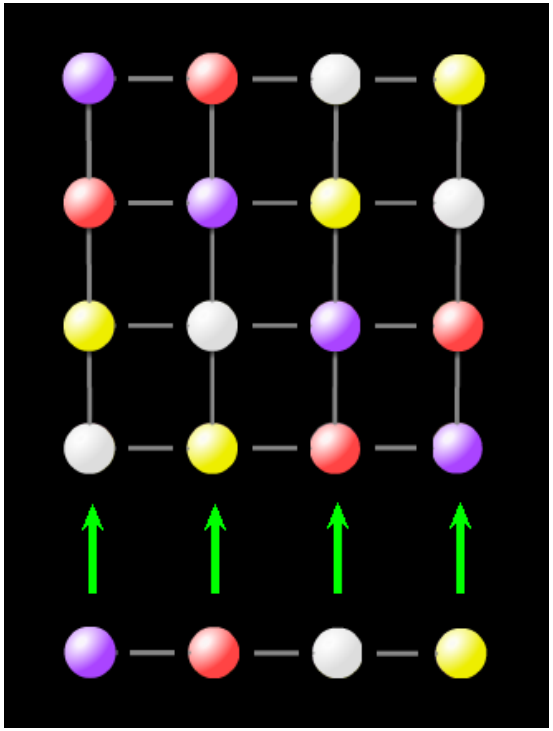
Утверждение 4.8

n-Арная квазигруппа порядка q является разделимой тогда и только тогда, когда произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, у неё имеется только q различающихся ретракта.

Внутренняя квазигруппа $\rightarrow$
Композиция:



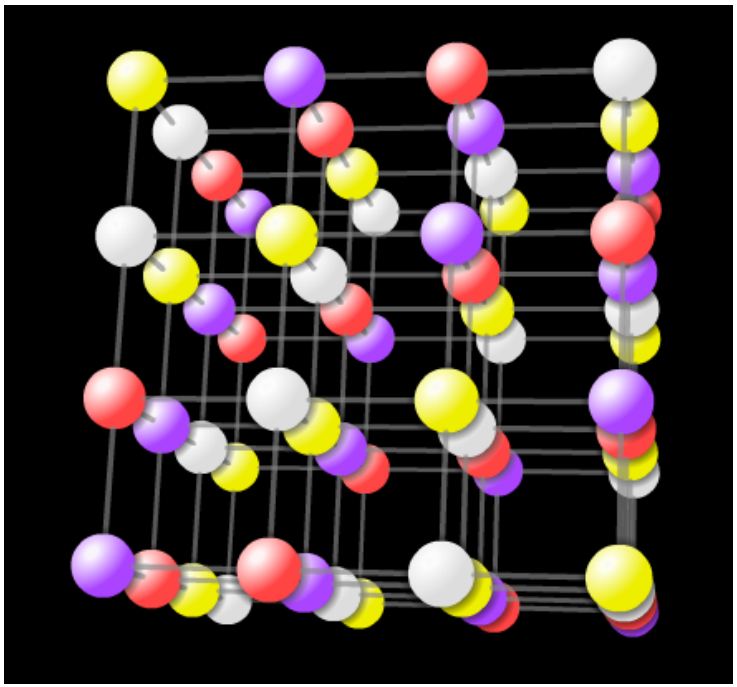
Внешняя квазигруппа:



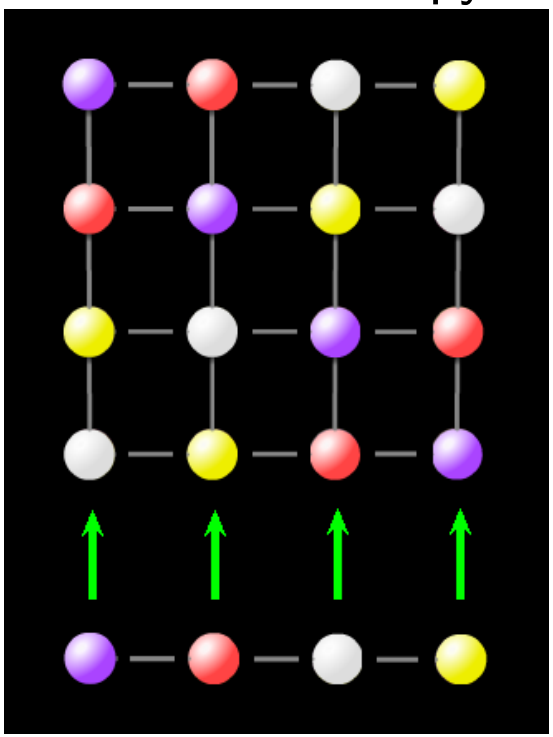
Утверждение 4.8

n-Арная квазигруппа порядка q является разделимой тогда и только тогда, когда произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, у неё имеется только q различающихся ретракта.

Композиция:



Внешняя квазигруппа:



Теорема 4.5 (Кротов, Потапов, Соколова, 2008)

Пусть $n \geq 4$, n-арные квазигруппы f и g разделимы и $f(x) = g(x)$ когда набор x содержит 0. Тогда $f = g$.

Контрпример при $n = 3$: $x_1 * (x_2 * x_3) \neq (x_1 * x_2) * x_3$.

Теорема 4.6 (Кротов, Потапов, Соколова, 2008)

Для любых $n > 2$ и $k > 3$ имеются неразделимые n-квазигруппы порядка k.

Теорема 4.6 (Кротов, Потапов, Соколова, 2008)

Для любых $n > 2$ и $k > 3$ имеются неразделимые n-квазигруппы порядка k.

0	1	2	3	4
1	0	4	2	3
2	3	1	4	0
4	2	3	0	1
3	4	0	1	2

Теорема 4.6 (Кротов, Потапов, Соколова, 2008)

Для любых $n > 2$ и $k > 3$ имеются неразделимые n-квазигруппы порядка k.

Доказательство. Для любого $n \geq 4$ имеется 2-квазигруппа f такая, что $f(E_2^2) = E_2^2$. Пусть $F(x) = f(x_1, f(x_2, f \dots f(x_{n-1}, x_n) \dots))$. Тогда $F(E_2^n) = E_2^n$. Рассмотрим

$$G(x) = \begin{cases} F(x) & x \notin E_2^n; \\ F(x) \oplus 1 & x \in E_2^n. \end{cases}$$

Если G разделима, то $F = G$.

Проблема 4.1

Доказать, что при $k \geq 4$ почти все n-арные квазигруппы неразделимы при $n \longrightarrow \infty$.

Проблема 4.2

Доказать или опровергнуть монотонность числа n-арных квазигрупп порядка k по k при любом n.