n-Арные квазигруппы конечного порядка

В. Н. Потапов

Семинар "Дискретная математика и теоретическая кибернетика"

ВМиК МГУ, 15 марта 2013 г.

Определения

Пусть F_q — конечное множество из q элементов. Множество F_q^n, состоящее из наборов длины n называется q-ичным n-мерным гиперкубом.

Определение

Расстоянием Хэмминга $d(x, y)$ между векторами $x, y \in F_q^n$ называется число координат, в которых наборы x и y различаются.

Определение

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

Определение

Функция $f : F_q^n \to F_q$ называется n-арной квазигруппой поорядка q, если она обратима по каждой своей переменной, т.е. отображение, полученное из f произвольной фиксацией всех переменных кроме одной является биекцией.

Утверждение

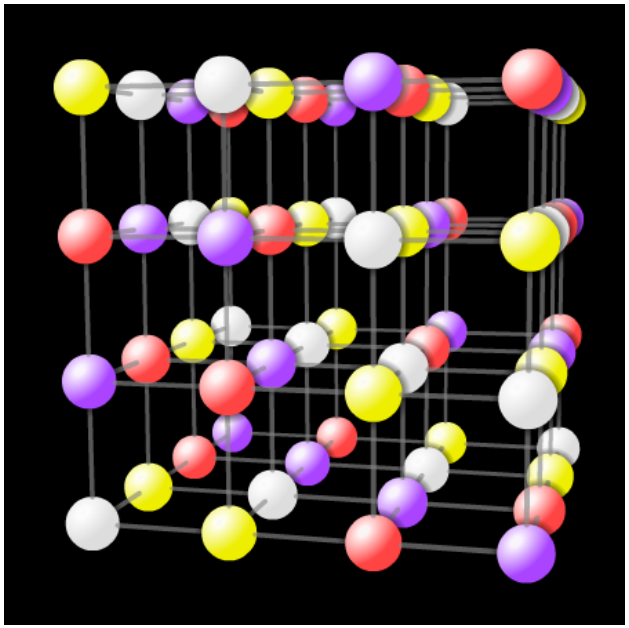
Функция $f : F_q^n \to F_q$ является n- арной квазигруппой тогда и только тогда, когда из $d(x, y) = 1$ следует, что $f(x) \neq f(y)$.

Пример

$f(x_1, \ldots, x_n) = x_1 + \cdots + x_n (\mod q)$.

Определение

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



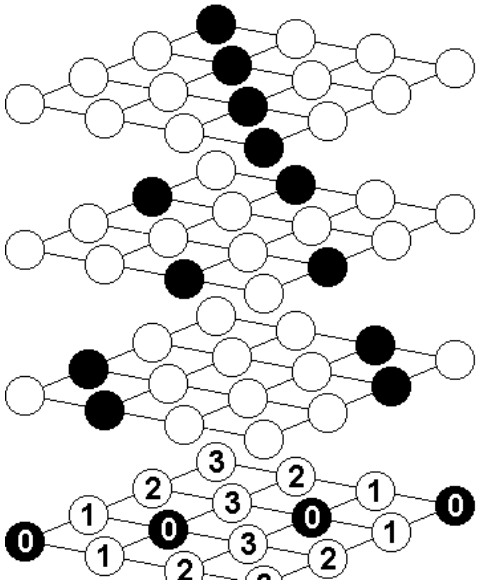
0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Определение

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

Утверждение

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



Определение

Изотопией в F_q^n называется упорядоченный набор из n перестановок $\theta_i : F_q \to F_q$, $i \in [n]$. Пусть $\bar{\theta} = (\theta_1, \ldots, \theta_n)$ является изотопией и $M \subseteq F_q^n$.

$$\bar{\theta}M \triangleq \{(\theta_1 x_1, \ldots, \theta_n x_n) \,|\, (x_1, \ldots, x_n) \in M\}.$$

Определение

Парастрофией в F_q^n называется перестановка координат $\tau \in S_n$.

$$M_\tau \triangleq \{(x_{\tau(1)}, \ldots, x_{\tau(n)}) \,|\, (x_1, \ldots, x_n) \in M\}.$$

Изотопия

0	1	2
3	4	5
6	7	8

1	2	0
4	5	3
7	8	6

4	5	3
1	2	0
7	8	6

Парастрофия

0	1	2
3	4	5
6	7	8

0	3	6
1	4	7
2	5	8

Рассмотрим n-мерный q-ичный куб (F_q^n, d) как метрическое пространство с метрикой Хэмминга. Его группа изометрий является полупрямым произведением группы изотопий Θ_{nk} на группу парастрофий S_n.

$$\mathrm{Aut}(F_q^n) = \Theta_{nk} \rtimes S_n$$

Определение

Мультиарные квазигруппы $f_1, f_2 : F_q^n \to F_q$ называются эквивалентными , если МДР-коды $M[f_1], M[f_2] \subseteq F_q^{n+1}$ эквивалентны, т. е. переводятся друг в друга изометрией куба F_q^{n+1}.

Определение

Ретрактом размерности $n-1$ МДР-кода $M \subset F_q^n$ называется множество $M|_{x_i=a} = \{\overline{x} \in M \mid x_i = a\}$, где $a \in F_q$.
Если зафиксировать значения m переменных в МДР-коде $M \subset F_q^n$, то полученное множество называется ретрактом размерности $n-m$, $1 \leq m \leq n-2$.

Определение

Функция f_1 называется ретрактом мультиарной квазигруппы f_2, если $M[f_1]$ — ретракт $M[f_2]$.

Утверждение

Ретракт МДР-кода является МДР-кодом. Ретракт мультиарной квазигруппы является мультиарной квазигруппой.

Утверждение

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-квазигруппой.

Таким образом, класс квазигрупп замкнут относительно операций суперпозиции и взятия подфукции.

Разделимость мультиарных квазигрупп

Определение

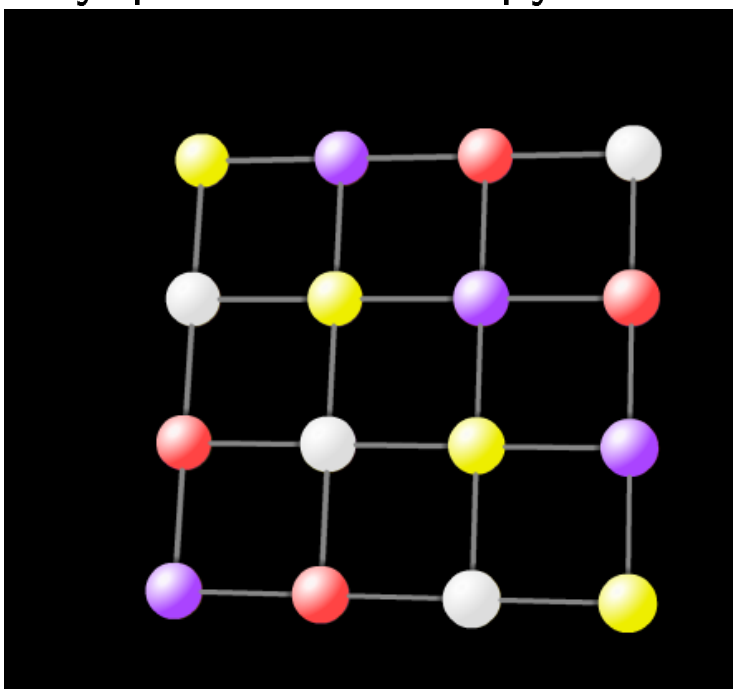
Мультиарная квазигруппа f называется разделимой (приводимой), если имеются целое число m, $2 \leq m < n$, $(n-m+1)$-арная квазигруппа h, m-арная квазигруппа g и перестановка $\sigma \in S_n$ такие, что

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

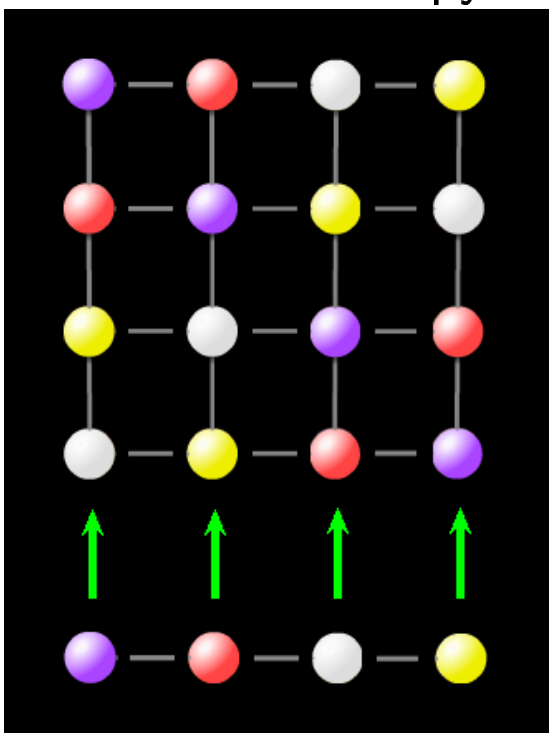
Геометрический критерий разделимости

Если n-квазигруппа порядка q при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только q различающихся ретрактов, то она является разделимой.

Внутренняя квазигруппа:



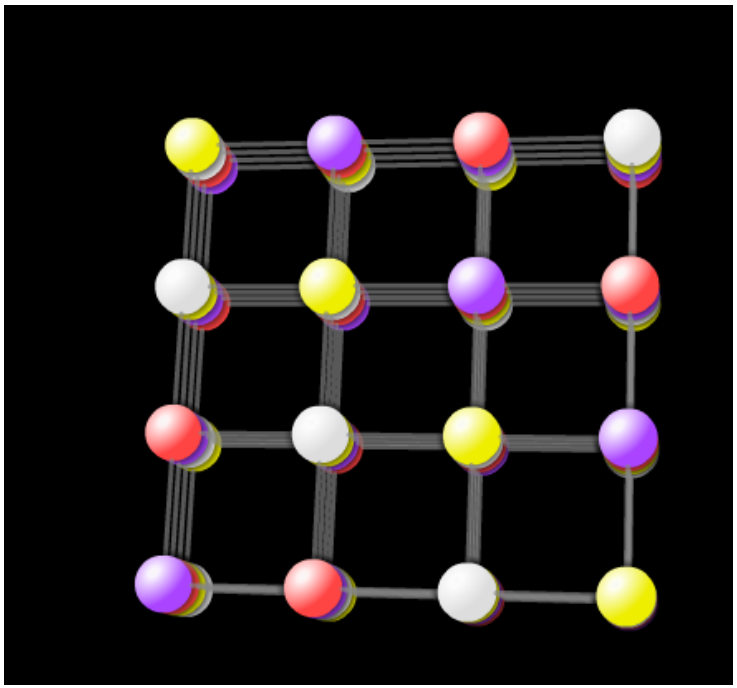
Внешняя квазигруппа:



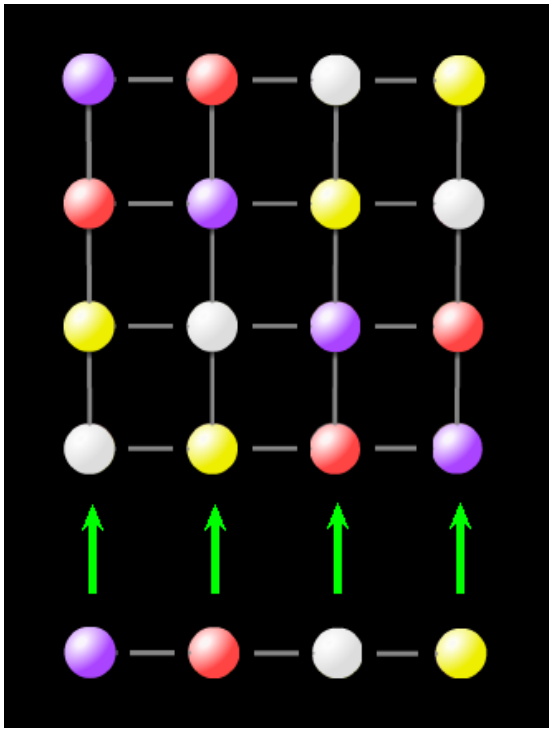
Геометрический критерий разделимости

Если n-квазигруппа порядка q при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только q различающихся ретрактов, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$ Композиция:



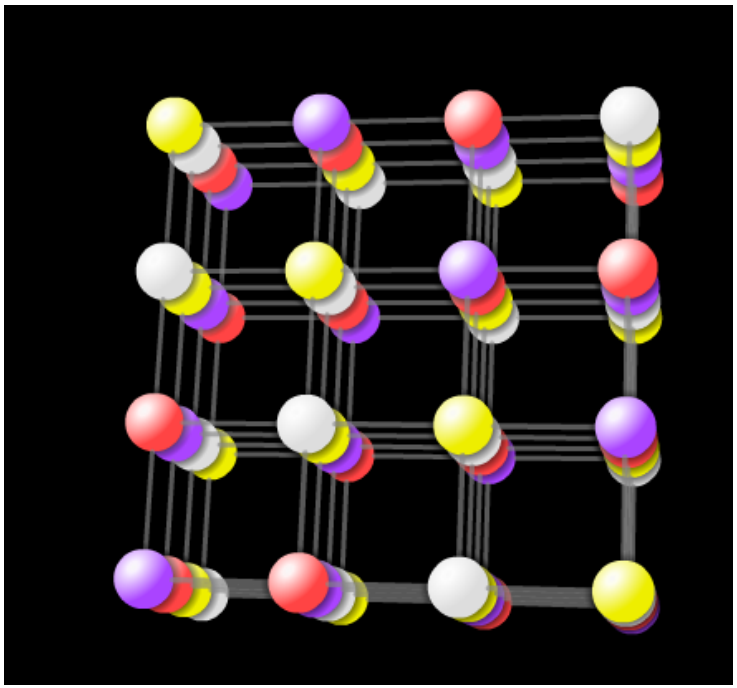
Внешняя квазигруппа:



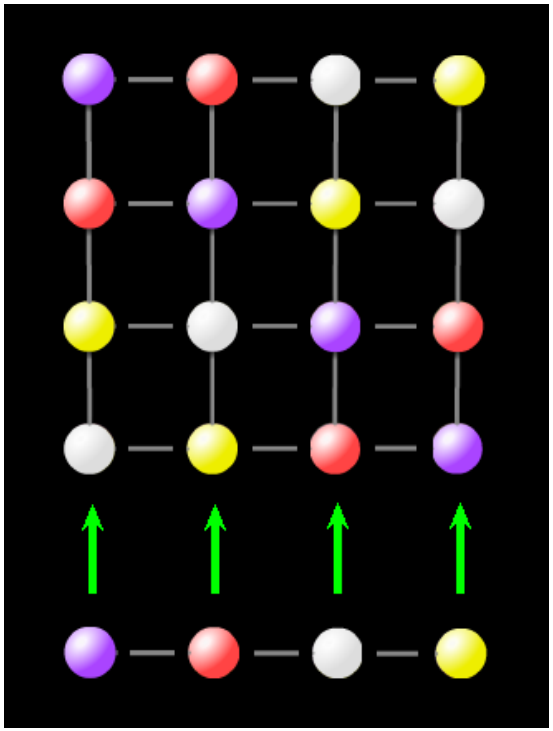
Геометрический критерий разделимости

Если n-квазигруппа порядка q при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только q различающихся ретрактов, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$ Композиция:



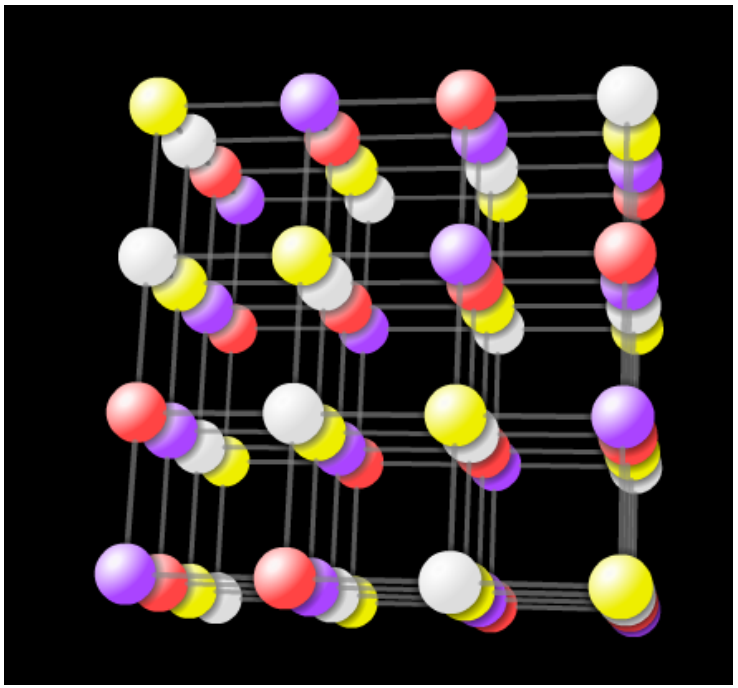
Внешняя квазигруппа:



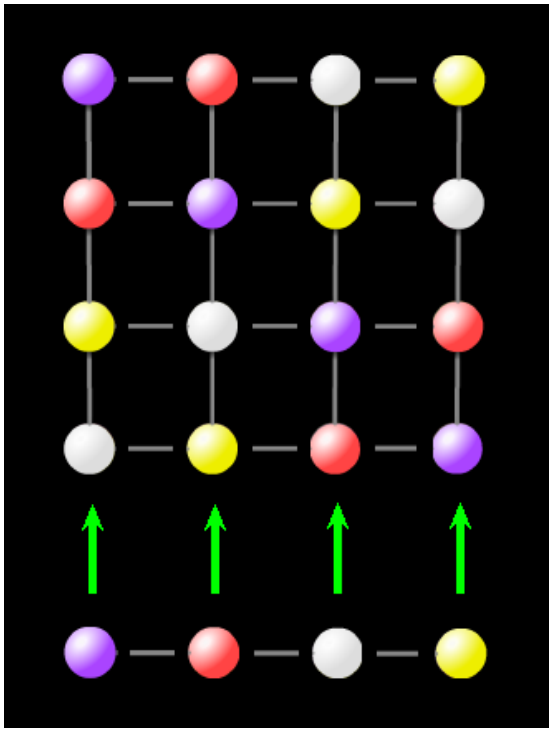
Геометрический критерий разделимости

Если n-квазигруппа порядка q при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только q различающихся ретрактов, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$ Композиция:



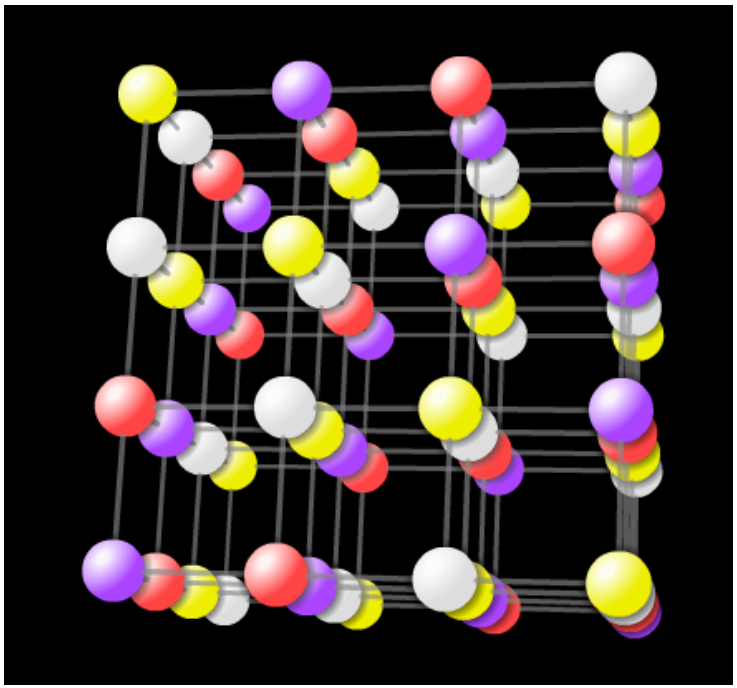
Внешняя квазигруппа:



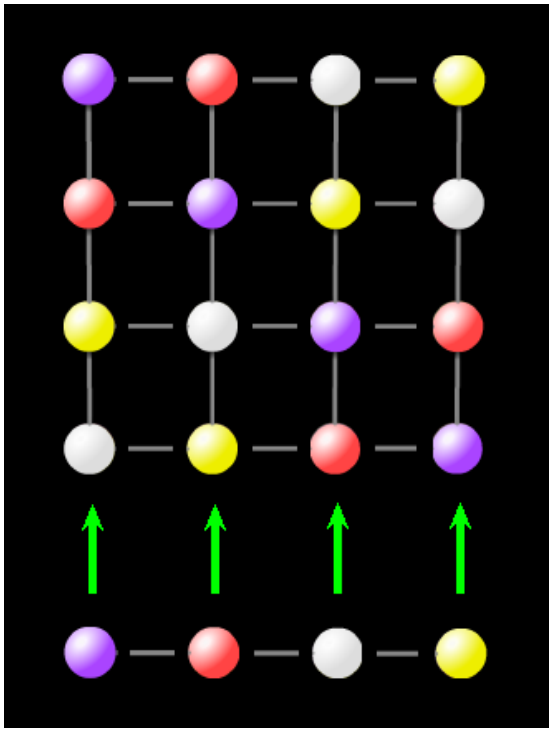
Геометрический критерий разделимости

Если n-квазигруппа порядка q при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только q различающихся ретрактов, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$ Композиция:



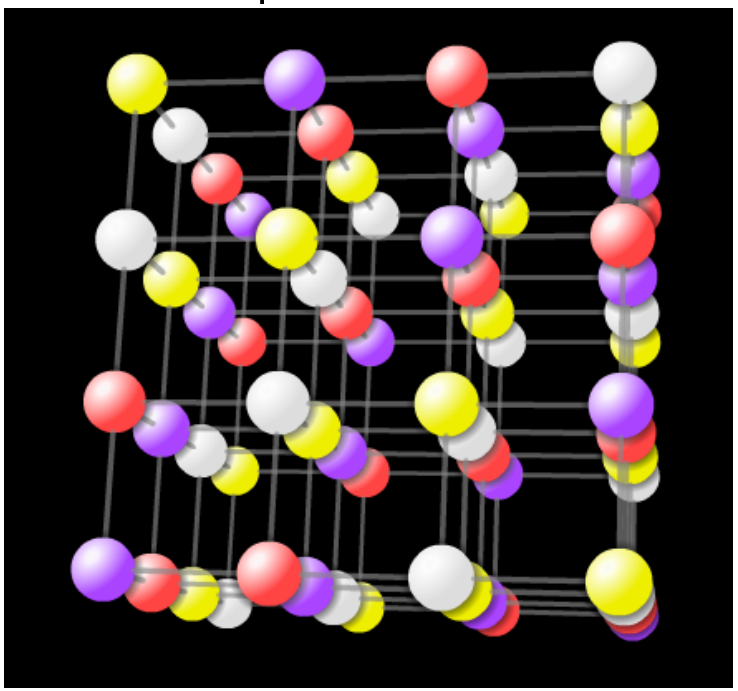
Внешняя квазигруппа:



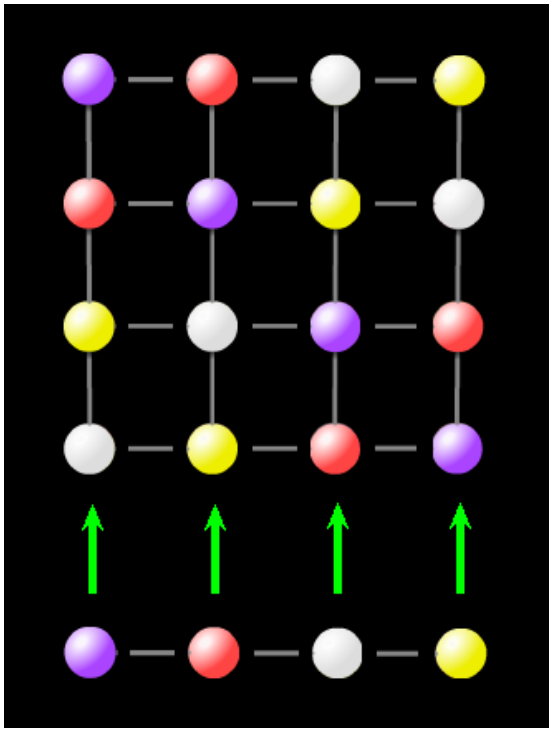
Геометрический критерий разделимости

Если n-квазигруппа порядка q при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только q различающихся ретрактов, то она является разделимой.

Композиция:



Внешняя квазигруппа:



Теорема

n-Арную квазигруппу f можно представить в виде суперпозиции ровно одним из двух способов

$$f(\overline{x}) \equiv q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)), \tag{1}$$

где q_j суть n_j-арные квазигруппы при любом $j, 1 \leq j \leq m$, q_0 есть неразделимая m-арная квазигруппа не эквивалентная группе, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,...,m}$ — разбиение множества $[n]$ на наборы мощности $n_1, \ldots, n_m$; либо

$$f(\tilde{x}_1, \ldots, \tilde{x}_m) \equiv q_1(\tilde{x}_1) * ... * q_m(\tilde{x}_m), \tag{2}$$

где $*$ есть ассоциативная квазигрупповая операция, q_j суть n_j-арные квазигруппы, $1 \leq j \leq k$, не представимые в виде $q_j(\tilde{x}_j) = q'(\tilde{x}'_j) * q''(\tilde{x}''_j)$, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,...,m}$ — разбиение множества $[n]$ на наборы мощности $n_1, \ldots, n_m$.
Причём в представлениях (1) и (2) разбиение $\{I_j\}_{j=1,...,m}$ единственно, m-арная квазигруппа q_0 и квазигрупповая операция $*$ определяются единственным образом с точностью до эквивалентности и набор мультиарных квазигрупп $q_1, \ldots, q_m$ единственный с точностью до эквивалентности и перестановки элементов.

Черёмушкин А. В. Каноническое разложение n-арных квазигрупп // *Матем. исследования*. Кишинёв:"Штиинца 1988.

Теорема

1.Пусть $3 < m+1 < n$ и разделимы все ретракты размерностей m и $m+1$ n-арной квазигруппы f порядка q, тогда f разделима.
2.Пусть $3 \leq m < n$, q — простое и разделимы все ретракты размерности m n-арной квазигруппы f порядка q, тогда f разделима.

Krotov D. S., Potapov V. N. On connection between reducibility on an n-ary quasigroup and that of its retracts // *Discrete Math.* 2011.

Krotov D. S. On irreducible n-ary quasigroups with reducible retracts // *European J. Combin.* 2008.

Zaslavsky T. Associativity in multary quasigroups: the way of biased expansions: eprint math.CO/0411268: arXiv.org, 2004.

Доказательство.

Обозначим через $\kappa(f)$ максимальную арность неразделимого ретракта n-арной квазигруппы f.

Лемма

Случай $\kappa(f) = 2$. Из разделимости 3- и 4-арных ретрактов следует разделимость мультиарной квазигруппы.

Лемма

Если $\kappa(f) \in \{3, \ldots, n-3\}$, то эта n-арная квазигруппа f разделимая.

Krotov D. S. On reducibility of n-ary quasigroups // *Discrete Math.* 2008.

Лемма

Пусть $n \geq 4$. Для n-арной квазигруппы f конечного простого порядка из $\kappa(f) = n-2$ следует, что f — разделимая.

Определение

n-Арная квазигруппа порядка k называется сублинейной, если все ее бинарные ретракты изотопны циклической группе Z_k.

Теорема

Все сублинейные n-арные квазигруппы порядка 5 разделимы при $n \geq 4$. Все сублинейные n-арные квазигруппы порядка 7 разделимы при $n \geq 3$.

Существует пример неразделимой сублинейной 3-квазигруппы порядка 5.

Проблема Белоусова

Для каких n и q имеются неразделимые n-арные квазигруппы порядка q?

Ответ

При любых $n > 2$ и $q > 3$.

Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n-ary quasigroups and switching subquasigroups // *Quasigroups and Related Systems* 2008.

Борисенко В. В. Неприводимые n-квазигруппы на конечных множествах составного порядка // *Мат. Исслед.* Квазигруппы и лупы. Кишинев: Штиинца, 1979.

Глухов М. М. К вопросу о приводимости главных парастрофов n-квазигрупп // *Мат. Исслед.* Квазигруппы и их системы. Кишинев: Штиинца, 1990.

Akivis M. A., Goldberg V. V. Solution of Belousov's problem // *Discuss. Math., Gen. Algebra Appl.* 2001.

Определение

Опорным будем называть ретракт, в котором все фиксированные переменные принимают значение $0 \in F_q$.

В следующей лемме доказано, что разделимая n-арная квазигруппа однозначно определяется своими 3-х арными опорными ретрактами.

лемма

Пусть $q, f : F_q^n \to F_q$ — разделимые n-арные квазигруппы, $n \geq 4$. Пусть множество $A_4 \subset F_q^n$ состоит из наборов, в которых не более 3-х элементов не равны 0. Предположим, что для всех $\bar{a} \in A_4$ справедливо равенство

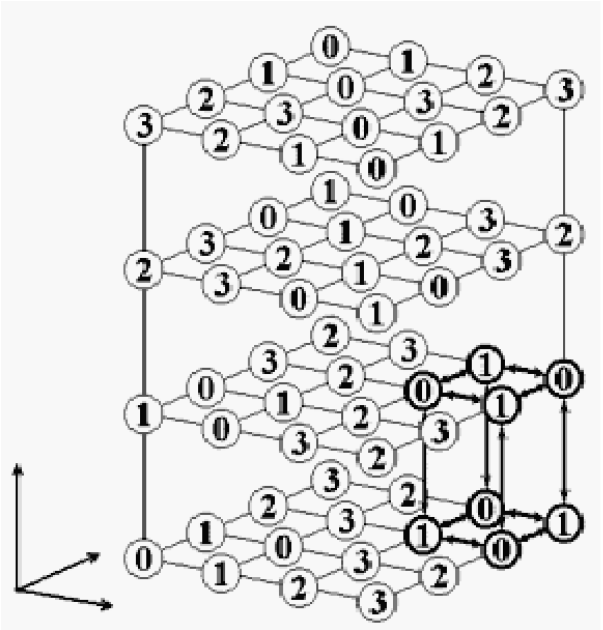
$$q(\bar{a}) = f(\bar{a}). \tag{3}$$

Тогда $q(\bar{x}) = f(\bar{x})$ для всех $\bar{x} \in F_q^n$.

По опорным двумерным ретрактам n-арная квазигруппа, вообще говоря, не восстанавливается. Например, разделимые 3-квазигруппы $q(x) \equiv (x_1 * x_2) * x_3$ и $f(x) \equiv x_1 * (x_2 * x_3)$, где операция $*$ не ассоциативна.

Определение

$\{a, b\}$-Компонентой n-арной квазигруппы f будем называть такое непустое подмножество $S \subset F_q^n$, что $f(S) = \{a, b\}$ $(a \neq b)$ и для любых $\overline{x}$ из S и $i \in [n]$ найдётся ровно один набор $\overline{y}$ из S, отличающийся от $\overline{x}$ только в i-й координате.



Будем говорить, что функция g получается из n-арной квазигруппы f свитчингом $\{a, b\}$-компоненты S, если

$$g(\overline{x}) = \begin{cases} f(\overline{x}) & \text{при } x \notin S; \\ a & \text{при } x \in S, f(\overline{x}) = b; \\ b & \text{при } x \in S, f(\overline{x}) = a. \end{cases}$$

Из определения $\{a, b\}$-компоненты следует, что функция g является n-арной квазигруппой.

Доказательство.

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

Для любого $n \geq 4$ имеется 2-квазигруппа f такая, что $f(F_2^2) = F_2^2$. Пусть $H(x) = f(x_1, f(x_2, f \dots f(x_{n-1}, x_n) \dots)$. Тогда $H(F_2^n) = F_2^n$. Рассмотрим

$$G(x) = \begin{cases} H(x) & x \notin F_2^n; \\ H(x) \oplus 1 & x \in F_2^n. \end{cases}$$

Если G разделима, то $H = G$.

Классификация n-квазигрупп порядка 4

Определение

Объединение двух непересекающихся МДР-кодов называется 2-кратным МДР-кодом. 2-Кратный МДР-код называется линейным, если он эквивалентен 2-кратному МДР-коду $L \subset F_4^n$ с линейной характеристической функцией

$$\chi_L(x_1, \ldots, x_n) \equiv \chi_{\{0,1\}}(x_1) \oplus \cdots \oplus \chi_{\{0,1\}}(x_n).$$

Утверждение

Пусть f — n-арная квазигруппа и $a, b \in F_4, a \neq b$. Множество $S_{a,b}(f) = \{(x_1, \ldots, x_n) \in F_4^n \mid f(x_1, \ldots, x_n) \in \{a, b\}\}$ является 2-кратным МДР-кодом.

Определение

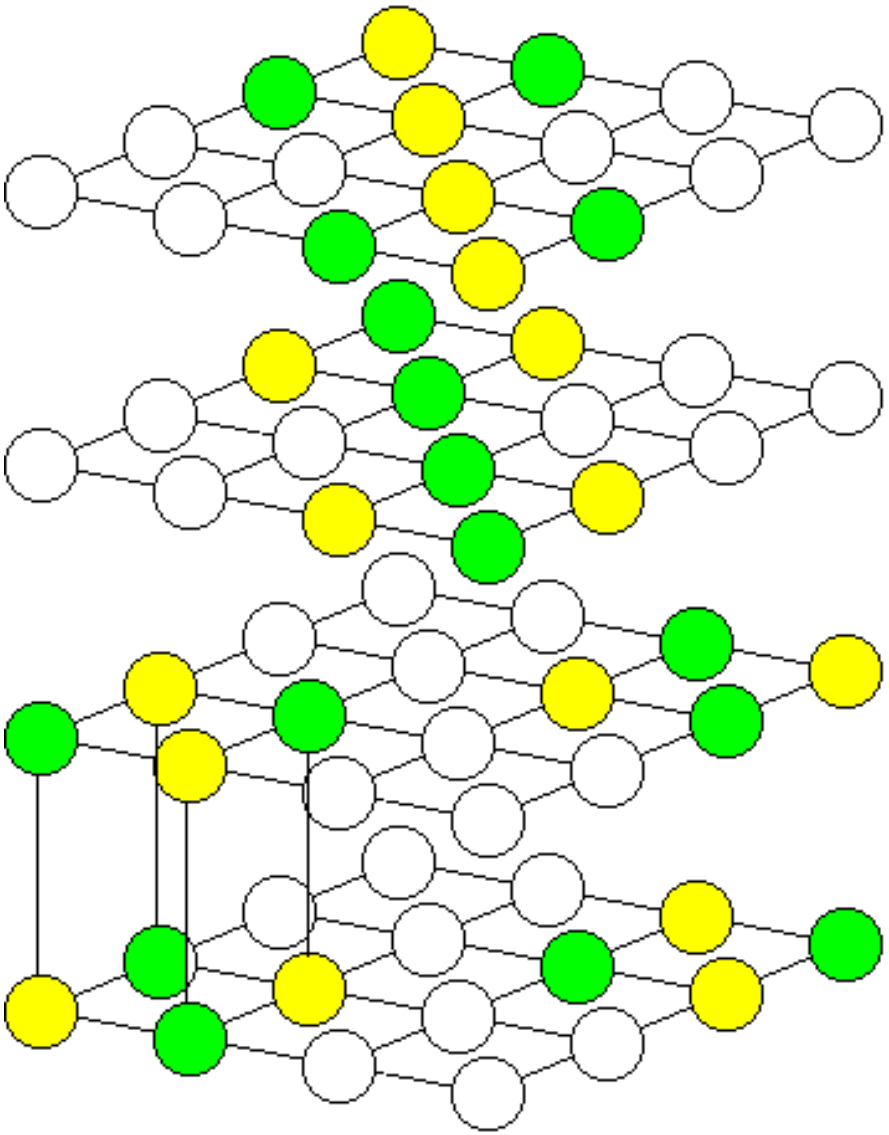
n-Арная квазигруппа f порядка 4 называется полулинейной, если для некоторых $a, b \in F_4$ множество $S_{a,b}(f)$ линейно.

Определение

МДР-код называется полулинейным, если он содержится в некотором линейном 2-МДР-коде.

Утверждение

n-Арная квазигруппа полулинейна тогда и только тогда, когда её график является полулинейным.



Элементы группы $(F_4, +)$ удобно представлять в виде двумерных двоичных векторов $\overline{(\mu^1, \mu^2)}$, $\mu^i \in \{0, 1\}$ с естественным отождествлением $\underline{0 = \overline{(0,0)}, 1 = \overline{(1,0)}, 2 = \overline{(1,1)}, 3 = \overline{(0,1)}}$, причём $\overline{(\mu^1, \mu^2)} + \overline{(\nu^1, \nu^2)} = \overline{(\mu^1 \oplus \nu^1, \mu^2 \oplus \nu^2)}$. Пусть

$$S = \{(\overline{(\mu_1^1, \mu_1^2)}, \ldots, \overline{(\mu_n^1, \mu_n^2)}) : \bigoplus_{i=1}^{n} \mu_i^2 = \delta\},$$

где $\delta \in \{0, 1\}$. Любой полулинейный МДР-код $M \subset S$ можно представить в виде

$$M = \{(\overline{(\mu_1^1, \mu_1^2)}, \ldots, \overline{(\mu_n^1, \mu_n^2)}) : \bigoplus_{i=1}^{n} \mu_i^2 = \delta, \bigoplus_{i=1}^{n} \mu_i^1 = \lambda_M(\mu_1^2, \ldots, \mu_n^2)\}, \tag{4}$$

где λ_M — некоторая булева функция, определённая на множестве $E_\delta^n = \{(\mu_1^2, \ldots, \mu_n^2) : \bigoplus_{i=1}^{n} \mu_i^2 = \delta\}$ булевых векторов чётности δ.

Теорема

Каждая n-арная квазигруппа порядка 4 разделима или полулинейна.

Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4// *SIAM J. Discrete Math.*, 2009.

Следствие

$Q(n,4) = 3^{n+1}2^{2^n+1}(1+o(1))$ при $n \to \infty$. $Q(n,k)$ — число n-квазигрупп порядка k.

Krotov D. S. On decomposability of 4-ary distance 2-MDS codes, double-codes, and n-quasigroups of order 4 // Discrete Math. 2008.

Потапов В. Н., Кротов Д. С. Асимптотика числа n-квазигрупп порядка 4 // *Сиб. матем. журн.* 2006.

Кротов Д. С. Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // *Дискрет. анализ и исслед. операций* Сер. 1. 2000.

Доказательство.

Обозначим через $\kappa(f)$ максимальную арность неразделимого ретракта n-арной квазигруппы f.

При $2 \leq \kappa(f) \leq n-3$ утверждение следует из теоремы о разделимости.

Лемма

Пусть $n \geq 5$. Если $\kappa(f) = n-2$, то f является разделимой или полулинейной.

Лемма

Пусть $n \geq 4$. Если $\kappa(f) = n-1$, то f — разделимая или полулинейная.

Определение

n-Арные квазигруппы f и g называют свитчингово эквивалентными, если одна получается из другой конечным числом последовательных свитчингов $\{a, b\}$-компонент, где пары элементов $a, b \in F_q$ могут быть различными для разных свитчингов.

Теорема

Для любого $n \in \mathbb{N}$ все n-арные квазигруппы порядка 4 с.-эквивалентны.

Кротов Д.С., Потапов В.Н. О свитчинговой эквивалентности n-арных квазигрупп порядка 4 и совершенных двоичных кодов // Пробл. передачи информ. 2010.

Число n-арных квазигрупп

$Q'(n,k) = Q(n,k)/k((k-1)!)^n$ — число n-арных луп порядка k.

$n \setminus k$	3	4	5	6
2	1	4	56	9408
3	1	64	40256	95909896152
4	1	7132	31503556	— — —
5	1	201538000	50490811256	— — —

McKay B. D., Wanless I. M. A census of small Latin hypercubes // *SIAM J. Discrete Math.* 2008.

Потапов В. Н., Кротов Д.С. О числе n-арных квазигрупп конечного порядка // Дискрет. матем. 2012.

$Q'(6,4) = 4323455726944177 12,$

$Q'(7,4) = 39876839873547476429227735 3963277968$

$Q'(8,4) =$ 67846927287489958255998624028528071036486706348977951042703872222975027 6832

$Q'(9,4) =$

392806872947537024401582763619311898265997045525167774737994964171536055569 1

715689315798207034124864743631547346499445406013494396046681627805987607270 4

Определение

2-Квазигруппа $\varphi : F_q \to F_q$ называется идемпотентной, если $\varphi(x, x) = x$ для любого $x \in F_q$.

Утверждение

Для любого $m \geq 3$ имеется идемпотентная 2-квазигруппа порядка m.

Утверждение

Для любого $m \geq 3$ найдётся 2-квазигруппа ψ порядка $2m + 1$, имеющая m $\{2i, 2i + 1\}$-компонент для каждого $i \in \{0, \ldots, m - 1\}$, причём все кроме одной $\{2i, 2i + 1\}$-компоненты имеют вид $\{2j, 2j + 1\} \times \{2l, 2l + 1\}$.

Доказательство

Пусть φ_m идемпотентная 2-квазигруппа φ_m порядка m. Для любых $a, b \in \{0, \ldots, m-1\}$, $a \neq b$, и $\delta, \sigma \in \{0, 1\}$ определим
$\psi(2a+\delta, 2b+\sigma) = 2\varphi_m(a, b) + (\delta + \sigma \bmod 2)$;
$\psi(2a+\delta, 2a+\delta) = 2a+1-\delta$;
$\psi(2a+\delta, 2a+1-\delta) = 2m-1$;
$\psi(2m-1, 2a+\delta) = \psi(2a+\delta, 2m-1) = 2a+\delta$;

$\psi(2m-1, k-1) = 2m-1$.

φ_4 :

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

ψ :

8	0	4	5	6	7	2	3	1
1	8	5	4	7	6	3	2	0
6	7	8	2	0	1	4	5	3
7	6	3	8	1	0	5	4	2
2	3	6	7	8	4	0	1	5
3	2	7	6	5	8	1	0	4
4	5	0	1	2	3	8	6	7
5	4	1	0	3	2	7	8	6
0	1	2	3	4	5	6	7	8

Теорема

Если $k \geq 5$ — нечётное и $n \geq 2$, то

$$Q(n,k) \geq 2^{\left(\frac{k-3}{2}\right)^{\left\lfloor \frac{n-1}{2} \right\rfloor}\left(\frac{k-1}{2}\right)^{\left\lceil \frac{n+1}{2} \right\rceil}} > 2^{\left(\frac{k-3}{2}\right)^{n/2}\left(\frac{k-1}{2}\right)^{n/2}}.$$

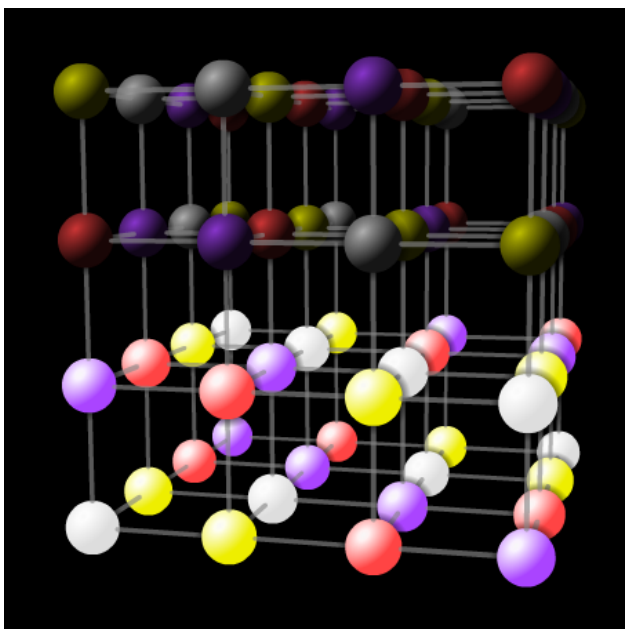
Доказательство. Определим рекуррентно n-арную квазигруппу Ψ^n равенствами:
$\Psi^2 \equiv \psi$;
$\Psi^{2m+1}(\overline{x}, y) = \psi(\Psi^{2m}(\overline{x}), y)$;
$\Psi^{2m+2}(\overline{x}, y, z) = \psi(\Psi^{2m}(\overline{x}), \psi(y, z))$.
Обозначим через α_n — число $\{2i, 2i+1\}$-компонент n-арной квазигруппы Ψ^n, где $i \in \{0, \ldots, \frac{k-3}{2}\}$. Имеем соотношения $\alpha_2 = \frac{k-1}{2}$, $\alpha_{2m+1} \geq \alpha_{2m}\frac{k-3}{2}$, $\alpha_{2m+2} \geq \alpha_{2m}\frac{k-3}{2}\frac{k-1}{2}$. Тогда $\alpha_{2m} \geq \left(\frac{k-3}{2}\right)^{m-1}\left(\frac{k-1}{2}\right)^{m}$ и $\alpha_{2m+1} \geq \left(\frac{k-3}{2}\right)^{m}\left(\frac{k-1}{2}\right)^{m}$.
Поскольку $\{2i, 2i+1\}$-компоненты при различных i не пересекаются, всего непересекающихся компонент не меньше, чем $\frac{k-1}{2}\alpha_n$.

Дополняемость частичных n-арных квазигрупп

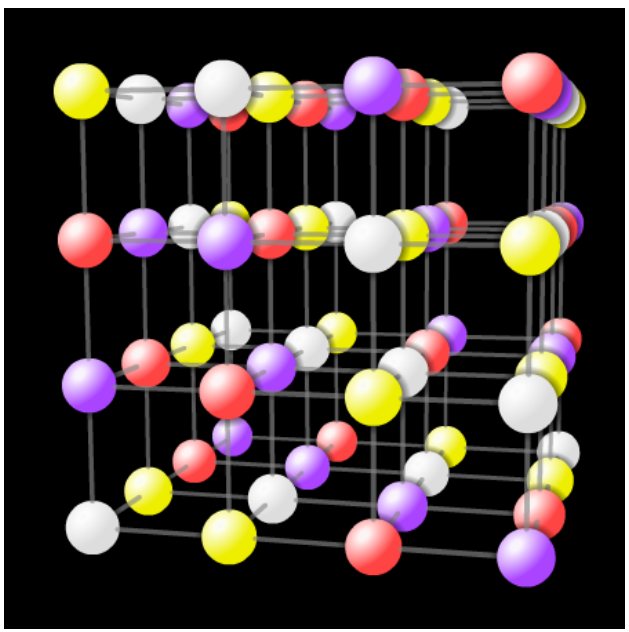
Определение

Частичная n-арная квазигруппа f дополняема, если f есть сужение некоторой n-арной квазигруппы g.

Рассмотрим задачу о возможности дополнения частичных n-арных квазигрупп или о дополнении латинского гиперкубоида до латинского куба.



$\rightarrow$



Известно, что дополняемость латинского прямоугольника до латинского квадрата является прямым следствием теоремы Кёнига.

Теорема

Любая n-квазигруппа $f : F_q^{n-1} \times F_{q'} \to F_q$ дополняема при $q' = 1$ или $q' = q - 1$.

Теорема

Для любых t и m при $m/2 < t < m - 2$ существует $m \times m \times t$ латинский кубоид, который не дополняется до латинского куба.

Kochol M. Relatively narrow latin parallelepipeds that cannot be extended to a latin cube // *Ars Comb.*, 1995.

Kochol M. Latin $(n \times n \times (n-2))$-parallelepipeds not completing to a latin cube // *Math. Slovaka*, 1989.

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

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

являются таблицами 2-квазигрупп f_0, f_1, f_2. Пусть 2-квазигруппы f_3, f_4 дополняют этот набор. Тогда $\{f_3(0,0), f_4(0,0)\} = \{1,2\}$, $\{f_3(0,1), f_4(0,1)\} = \{1,2\}$, $\{f_3(1,0), f_4(1,0)\} = \{3,2\}$, $\{f_3(1,1), f_4(1,1)\} = \{1,3\}$. Нетрудно видеть, что таких 2-квазигрупп f_3 и f_4 не существует.

Теорема

1. Для любых $m \geq 4$ существует $2m \times 2m \times m$ латинский кубоид, который не дополняется до $2m \times 2m \times 2m$ латинского куба.
2. Для любых чётных $m \notin \{2, 6\}$ существует $(2m-1) \times (2m-1) \times (m-1)$ латинский кубоид, который не дополняется до $(2m-1) \times (2m-1) \times m$ латинского куба.

McKay B. D., Wanless I. M. A census of small Latin hypercubes // *SIAM J. Discrete Math.*, 2008.

Bryant D., Cavenagh N. J., Maenhaut B., Pula K., Wanless I. M. Non-extendible Latin cuboids. SIAM J. of Discrete Math. 2012.

Теорема

Любой латинский кубоид размера $4 \times 4 \times \cdots \times 4 \times k$, где $k = 1, 2, 3$, дополняется до латинского гиперкуба.

Потапов В. Н. О дополняемости частичных n-квазигрупп порядка 4// Математические труды. 2011.

Доказательство

Доказательство проводится по индукции (при $n = 4$ утверждение теоремы проверено с помощью компьютера) и состоит из рассмотрения нескольких случаев:
(a) когда n-арные квазигруппы f_1 и f_2 неразделимы;
(b) когда хотя бы одна из n-арных квазигрупп f_1 и f_2 разделима, причём разделимость не синхронна;
(c) когда n-арные квазигруппы f_1 и f_2 не полностью синхронно разделимы;
(d) когда одна из одна из n-арных квазигрупп f_1 и f_2 разделима полностью, а другая нет;
(e) когда n-арные квазигруппы f_1 и f_2 полностью разделимы.

Транзитивные мультиарные квазигруппы

Определение

Подгруппа группы изометрий гиперкуба, переводящая множество $A \subseteq F_q^n$ в себя, называется группой изометрий множества A и обозначается через $\mathrm{Aut}(A)$.

Определение

Множество $A \subseteq F_q^n$ называется транзитивным, если для любых двух вершин $\overline{x}, \overline{y}$ из A найдутся парастрофия $\varepsilon \in \mathrm{Prs}(F_q^n)$ и изотопия $\overline{\tau} \in \mathrm{Ist}(F_q^n)$ такие, что $\overline{\tau y} = \overline{x}_\varepsilon$ и $\overline{\tau} A = A_\varepsilon$, т. е. группа изометрий $\mathrm{Aut}(A)$ действует транзитивно на A.

Определение

Множество $A \subseteq F_q^n$ называется изотопно транзитивным, если группа $\mathrm{Ist}(A)$ действует транзитивно на A.

Определение

n-Арную квазигруппу будем называть транзитивной (изотопно транзитивной), если её график (МДР-код) является транзитивным (изотопно транзитивным).

Определение

Если $\circ$ — групповая операция на F_q, то n-арная квазигруппа $f(x_1, \ldots, x_n) = x_1 \circ \cdots \circ x_n$ называется итерированной группой.

Утверждение

Итерированная группа является изотопно транзитивной мультиарной квазигруппой.

Теорема

При $q = 2p$ число попарно не эквивалентных изотопно транзитивных n-арных квазигрупп порядка q растёт почти экспоненциально при $n \to \infty$.

Потапов В. Н. О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2006.

Теорема

Пусть $q = p^k$, где p — простое. В гиперкубе F_{2q}^n, имеется не менее $q^{\binom{n}{2}(1+o(1))}$ изотопно транзитивных МДР-кодов.

Теорема

МДР-код $M \subset F_4^n$ является изотопно транзитивным тогда и только тогда, когда он является полулинейным с квадратичной функцией λ.

Krotov D.S., Potapov V.N. Construction of transitive MDS codes // arXiv:1303.0004

Применение в теории кодирования

Кротов Д.С., Потапов В.Н. О кратных МДР- и совершенных кодах, не расщепляемых на однократные // Пробл. передачи информ. 2004.

Потапов В.Н. Бесконечномерные квазигруппы конечного порядка// Мат. заметки. 2013.

Heden, Olof; Krotov, Denis S. On the structure of non-full-rank perfect q-ary codes. Adv. Math. Commun. 5 (2011)

J. Borges, I. Yu. Mogilnykh, J. Rifa, F. I. Solov'eva. On the number of nonequivalent propelinear extended perfect codes. arXiv:1303.0680 [math.CO]