О разделимости n-арных квазигрупп и их ретрактов

Д. С. Кротов, В. Н. Потапов

Институт математики им. С.Л.Соболева,

Новосибирский государственный университет, Новосибирск

Определение

Пусть Σ — некоторое непустое множество. Функция $f : \Sigma^n \to \Sigma$ называется n-арной квазигруппой (n-квазигруппой) если f действует взаимно однозначно при любой фиксации любого набора из $n-1$ аргумента.

Уравнение $x_0 = f(x_1, \dots, x_n)$ задаёт n неявных функций $f^{(i)}$, каждая из которых является обращением n-квазигруппы f по i-ой переменной.

$$x_i = f^{(i)}(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n) \quad \Leftrightarrow \quad y = f(x_1, \dots, x_i, \dots, x_n)$$

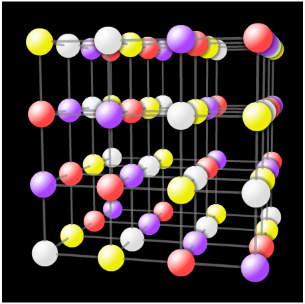
Порядком n-квазигруппы называется мощность множества Σ.

Пусть $\Sigma = \{0, 1, \ldots, k-1\}$ — конечное множество. Условие обратимости можно записать в виде $f(\overline{x}) \neq f(\overline{y})$ для любых $\overline{x}, \overline{y} \in \Sigma^n$ таких, что $d(\overline{x}, \overline{y}) = 1$, где $d(\overline{x}, \overline{y})$ — расстояние Хэмминга.

Определение

Таблица значений n-квазигруппы называется латинским гиперкубом (n-мерное обобщение латинского квадрата).

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



Определение

Если у n-квазигруппы f или у функции, обратной ей по некоторому аргументу, зафиксировать $n - m$ аргументов, то мы получим m-квазигруппу, называемую ретрактом n-квазигруппы f.

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

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

является n-квазигруппой.

Таким образом, класс квазигрупп замкнут относительно операций суперпозиции, обращения по переменной и взятия ретракта.

Определение

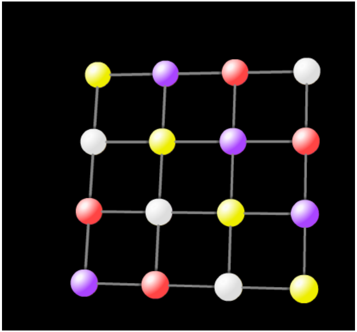
n-Квазигруппа f называется **разделимой** (**приводимой**), если имеются целое число m, $2 \leq m < n$, $(n-m+1)$-квазигруппа h, m-квазигруппа g и перестановка $\sigma \in S_n$ такие, что

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

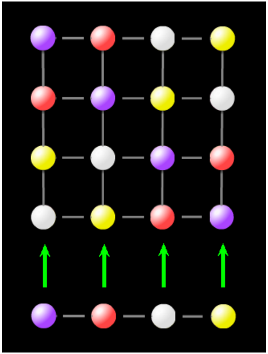
Геометрический критерий разделимости

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

Внутренняя квазигруппа:



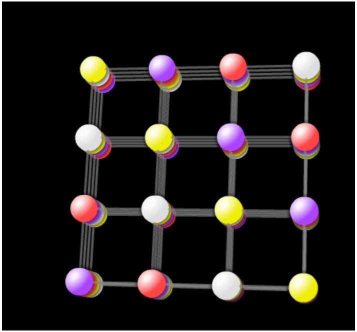
Внешняя квазигруппа:



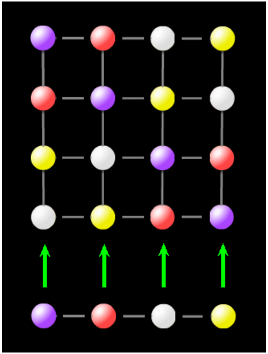
Геометрический критерий разделимости

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

Внутренняя квазигруппа $\to$ Композиция:



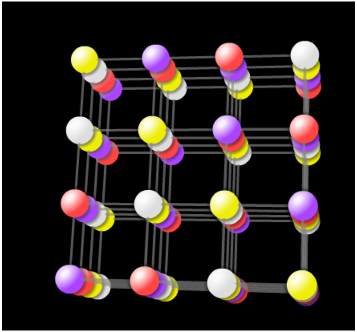
Внешняя квазигруппа:



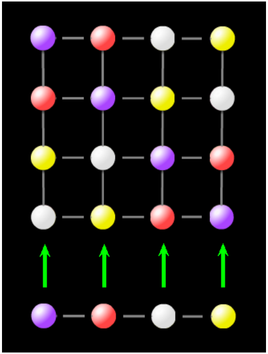
Геометрический критерий разделимости

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

Внутренняя квазигруппа $\rightarrow$ Композиция:



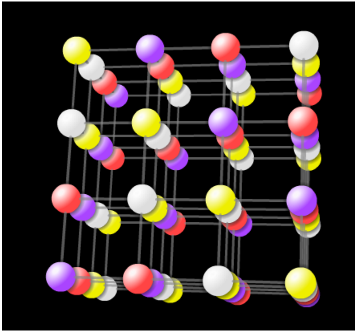
Внешняя квазигруппа:



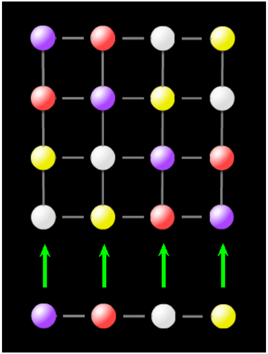
Геометрический критерий разделимости

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

Внутренняя квазигруппа $\rightarrow$ Композиция:



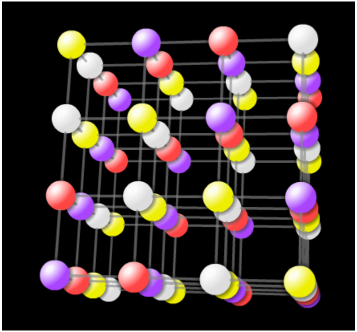
Внешняя квазигруппа:



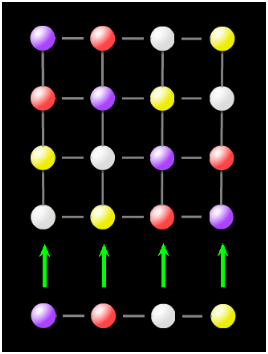
Геометрический критерий разделимости

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

Внутренняя квазигруппа $\rightarrow$ Композиция:



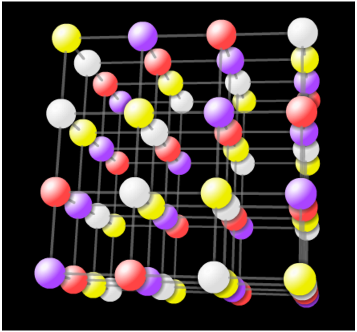
Внешняя квазигруппа:



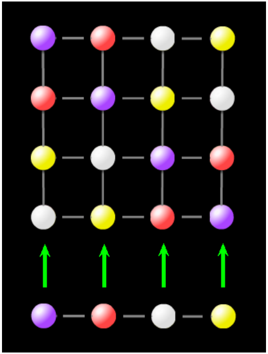
Геометрический критерий разделимости

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

Композиция:



Внешняя квазигруппа:



Теорема

1.Если разделимы все ретракты размерностей $n-2$ и $n-1$ n-квазигруппы f, то f разделима.
2.Если k — простое и разделимы все ретракты размерности $n-1$ n-квазигруппы f порядка k, то 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.

Кротов Д. С. Совершенные коды и n-арные квазигруппы: конструкции и классификация, *Дисс.. . . доктора физ.-мат.наук*, Новосибирск, 2010.

Каноническое представление

Разделимую n-квазигруппу f можно представить в виде

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

где q_j суть n_j-квазигруппы при любом j, $1 \leq j \leq m$, q_0 есть неразделимая m-квазигруппа, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,\dots,m}$ — разбиение множества $\{1, \dots, n\}$ на наборы мощности $n_1, \dots, n_m$, причём при $m \geq 3$ в данном представлении разбиение $\{I_j\}_{j=1,\dots,m}$ единственно.

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

Следствие

Если разделимая n-квазигруппа f имеет неразделимый ретракт размерности $m \geq 2$, который не содержится в неразделимых ретрактах большей размерности, то

$$\{\overline{x} \in \Sigma^{n+1} \mid x_{n+1} = f(x_1, \ldots, x_n))\} =$$
$$= \{\overline{x} \in \Sigma^{n+1} \mid q_{m+1}(x_{n+1}, \tilde{x}_{m+1}) = q_0(q_1(\tilde{x}_1), \ldots, q_m(\tilde{x}_m))\},$$

где q_j суть n_j-квазигруппы при $j, 1 \leq j \leq m+1$, q_0 есть неразделимая m-квазигруппа, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,\ldots,m+1}$ — разбиение множества $\{1, \ldots, n\}$ на наборы мощности $n_1, \ldots, n_{m+1}$.

Пусть m — максимальная размерность неразделимого ретракта n-квазигруппы f. Нужно доказать, что если $m < n-2$, то f разделима.

Произвольный порядок

1. $m = 2$
2. $2 < m < n-2$

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

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

Простой порядок

3.1. $m = n - 2,\ n > 4.$

3.2. $m = n - 2,\ n = 4.$

Определение

n-Квазигруппа порядка k называется сублинейной, если все её ретракты размерности 2 эквивалентны группе Z_k.

Следствие

Все сублинейные n-квазигруппы порядков 5 и 7 разделимы при $n \geq 4$.