

Построение транзитивных МДР-кодов на основе диэдральной группы

Д. С. Кротов, В. Н. Потапов

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

XI Международный научный семинар
<Дискретная математика и её приложения>,
г. Москва, 18-23 июня 2012 г.

Определение

Пусть $Q_q = \{0, \dots, q-1\}$. Множество Q_q^n с определённым на нём расстоянием Хэмминга называется **q -значным n -мерным кубом (гиперкубом)**.

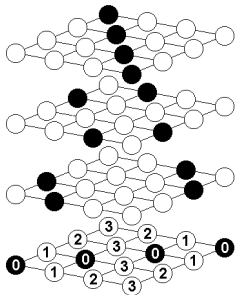
Определение

Множество $M \subset Q_q^n$ называется **МДР-кодом (с расстоянием 2)** если $|M| = q^{n-1}$ и $d(\bar{x}, \bar{y}) \geq 2$ для любых различных $\bar{x}, \bar{y} \in M$.

Определение

Функция $f : Q_q^n \rightarrow Q_q$ называется **n -арной квазигруппой порядка q** , если $f(\bar{x}) \neq f(\bar{y})$ для любых двух соседних вершин $\bar{x}, \bar{y} \in Q_q^n$ ($d(\bar{x}, \bar{y}) = 1$).

График $M[f] = \{(\bar{x}, f(\bar{x})) \mid \bar{x} \in Q_q^n\}$ n -арной квазигруппы f является МДР-кодом. Более того, имеется взаимно однозначное соответствие между n -арными квазигруппами, латинскими гиперкубами и МДР-кодами.



Определение

Изотопией гиперкуба называется преобразование $\bar{x} \mapsto \bar{\tau x}$, где $\bar{x} = (x_1, \dots, x_n) \in Q_q^n$, $\bar{\tau x} = (\tau_1 x_1, \dots, \tau_n x_n)$, $\tau_i \in S_q$ — перестановки на множестве Q_q , $i \in \{1, \dots, n\}$.

Определение

Парастрофией гиперкуба называется преобразование $\bar{x} \mapsto \bar{x}_\varepsilon$, где $\bar{x}_\varepsilon = (x_{\varepsilon 1}, \dots, x_{\varepsilon n})$, $\varepsilon \in S_n$ — перестановка координат.

$$A \subseteq Q_q^n, A_\varepsilon = \{\bar{x}_\varepsilon \mid \bar{x} \in A\}, \bar{\tau}A = \{\bar{\tau x} \mid \bar{x} \in A\}.$$

Утверждение (Марков, 1956)

$$\text{Aut}(Q_q^n) = \text{Ist}(Q_q^n) \ltimes \text{Prs}(Q_q^n).$$

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

Определение

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

Определение

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

Определение

Множество $A \subseteq Q_q^n$ называется **изотопно транзитивным**, если группа $\text{Ist}(A)$ 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 Q_q , то n -арная квазигруппа $f(x_1, \dots, x_n) = x_1 \circ \dots \circ x_n$ называется **итерированной группой**.

Утверждение

Итерированная группа является изотопно транзитивной мультиарной квазигруппой.

Определение

Если $f(x, 0) = f(0, x) = x$ для любого $x \in Q_q$, то 2-квазигруппа f называется **лупой**. Изотопно транзитивные лупы называются **G-лупами**.

Рассмотрим следующие лупы порядка $2p$:

1) группа $Z_p \times Z_2$ с операцией $x_\zeta + y_\xi = (x + y \bmod p)_{(\zeta \oplus \xi)}$;

0	1	2	3	4	5
1	2	0	4	5	3
2	0	1	5	3	4
3	4	5	0	1	2
4	5	3	1	2	0
5	3	4	2	0	1

2) **диэдральная группа** D_p с операцией $x_\zeta \circ y_\xi = ((-1)^\xi x + y \bmod p)_{(\zeta \oplus \xi)}$;

0	1	2	3	4	5
1	2	0	4	5	3
2	0	1	5	3	4
3	5	4	0	2	1
4	3	5	1	0	2
5	4	3	2	1	0

3) **лула** C_p с операцией $x_\zeta * y_\xi = ((-1)^\xi x + y + \zeta \xi \bmod p)_{(\zeta \oplus \xi)}$.

0	1	2	3	4	5
1	2	0	4	5	3
2	0	1	5	3	4
3	5	4	1	0	2
4	3	5	2	1	0
5	4	3	0	2	1

Теорема

Пусть f — n -арная квазигруппа, полученная итерированием группы $Z_p \times Z_2$ или лупы C_p , m_i -арные квазигруппы h_i , $i \in \{1, \dots, n\}$ получены итерированием группы D_p . Тогда МДР-код $M = \{(x, \bar{z}_1, \dots, \bar{z}_n) \mid x = f(h_1(\bar{z}_1), \dots, h_n(\bar{z}_n))\}$ является изотопно транзитивным.

Следствие

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

Определение

Обращением n -арной квазигруппы $f(x_1, \dots, x_n)$ по i -ой переменной называется n -арная квазигруппа $f^{(i)}$, определённая формулой

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

Определим рекуррентно понятие **итерирования квазигруппы** для произвольной 2-квазигруппы f . Пусть m -арная и k -арная квазигруппы $f^{(i)}(f_1(\overline{x_1}), f_2(\overline{x_2}))$ и $f^{(i)}(f_3(\overline{z_1}), f_4(\overline{z_2}))$ получены итерированием 2-квазигруппы f , тогда $(m + k - 1)$ -арная квазигруппа g является итерированием f , если и только если она представима как график МДР-кода $\{(\overline{x_1}, \overline{x_2}, \overline{z_1}, \overline{z_2}) \mid f^{(i)}(f_1(\overline{x_1}), f_2(\overline{x_2})) = f^{(i)}(f_3(\overline{z_1}), f_4(\overline{z_2}))\}$.

Каждой n -арной квазигруппе, полученной итерированием 2-квазигруппы f , соответствует некоторое двоичное дерево разложения в суперпозицию.

Утверждение

Если 2-квазигруппа f является изотопно транзитивной, то n -арная квазигруппа, полученная итерированием f также является изотопно транзитивной.

В [1] показано, что при простом q любая G -лупа является группой (циклической), в [3] аналогичный результат был получен для $q = 3p$, где $p > 3$ — простое. С другой стороны в [2] показано, что для любого непростого порядка q , за исключением случая, когда в разложении числа q на простые отсутствует 2 и кратные сомножители, имеются G -лупы порядка q неэквивалентные группам.

1. Wilson R. L. Jr. Isotopy-isomorphy loops of prime order // J. Algebra — 1974.
2. Goodaire E. G., Robinson D. A. A class of loops which are isomorphic to all loop isotopes // Canadian J. Math. — 1982.
3. Kunen K. G -loops and permutation groups // J. Algebra — 1999.

Пусть $G < \text{Ist}(Q_q^n)$, определим $P_i(G) = \{\sigma_i \mid (\sigma_1, \dots, \sigma_n) \in G\}$.

Лемма 1

Пусть n -арная квазигруппа f и m -арная квазигруппа h изотопно транзитивны и $P_{n+1}G_f = P_{m+1}G_h$, $|P_{n+1}G_f| = q$, где G_f — транзитивно действующая подгруппа группы $\text{Ist}(\{\bar{x} \mid x_{n+1} = f(x_1, \dots, x_n)\})$. Тогда МДР-код $\{(\bar{x}, \bar{y}) \in Q_q^{n+m} \mid f(\bar{x}) = h(\bar{y})\}$ является изотопно транзитивным.

Лемма 2

Пусть

- а) m_i -арные квазигруппы h_i , $i \in \{1, \dots, n\}$, суть итерированные группы,
- б) n -арная квазигруппа f изотопно транзитивна с транзитивно действующей подгруппой автотопий G_f ,
- с) для любого $i \in \{1, \dots, n\}$ и $\bar{\sigma} \in G_f$ существует изотопия $\bar{\tau}_i \in S_{n_i}$ такая, что $h_i(\bar{\tau}_i z_i) = \sigma_i h(\bar{z}_i)$, где $\bar{z}_i$ — наборы из n_i переменных.

Тогда m -арная квазигруппа $f(h_1(\bar{z}_1), \dots, h_n(\bar{z}_n))$, где $m = m_1 + \dots + m_n$, является изотопно транзитивной.