В. Н. Потапов, Д. С. Кротов, О числе n-арных квазигрупп конечного порядка, *Дискрет. матем.*, 2012, том 24, выпуск 1, 60–69

DOI: 10.4213/dm1172

Дискретная математика

том 24 выпуск 1 * 2012

УДК 519.143

О числе n-арных квазигрупп конечного порядка

© 2012 г. В. Н. Потапов, Д. С. Кротов

Пусть $Q(n,k)$ — число n-арных квазигрупп порядка k. Получена рекуррентная формула для чисел $Q(n,4)$. Доказано, что при любых $n \geqslant 2$ и $k \geqslant 5$ справедливы неравенства

$$((k-3)/2)^{n/2}((k-1)/2)^{n/2} < \log_2 Q(n,k) \leqslant c_k(k-2)^n,$$

где c_k не зависит от n. Таким образом, верхняя асимптотическая граница для чисел $Q(n,k)$ улучшена при любых $k \geqslant 5$, нижняя — при нечетных $k \geqslant 7$.

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0429) и Российского фонда фундаментальных исследований, проекты 08–01–00671, 08–01–00673, 10–01–00616.

1. Введение

Алгебраическая система из множества Σ мощности $|\Sigma| = k$ и n-арной операции $f\colon \Sigma^n \to \Sigma$ называется n-арной квазигруппой порядка k, если унарная операция, полученная фиксацией любых $n-1$ аргументов операции f любыми значениями из Σ, всегда является биекцией. Принято называть n-арной квазигруппой порядка k или n-квазигруппой порядка k также и соответствующую функцию f (таблица значений такой функции известна под названием латинский гиперкуб, в случае $n = 2$ — латинский квадрат).

Зафиксируем множество элементов $\Sigma = \{0, 1, \dots, k-1\}$. Обозначим через $Q(n,k)$ число различных n-арных квазигрупп порядка k (при фиксированном Σ). Иногда под числом квазигрупп подразумевают число попарно неизоморфных квазигрупп. Известно, что для каждого n существует только две n-арных квазигруппы порядка 2. Имеется $Q(n,3) = 3 \cdot 2^n$ различных n-арных квазигрупп порядка 3, которые составляют единственный класс эквивалентности. В [1] доказано асимптотическое равенство

$$Q(n,4) = 3^{n+1}2^{2^n+1}(1+o(1))$$

при $n \to \infty$. В настоящей работе (в разделе 4) предложен рекуррентный способ вычисления чисел $Q(n,4)$, выписаны первые 8 значений этой величины. Ранее были известны только пять первых значений $Q(n,4)$, кроме того, известны числа $Q(n,5)$ и $Q(n,6)$ для $n \leqslant 5$ и $n \leqslant 3$ соответственно (см. [9]) и число $Q(2,k)$ при $k \leqslant 11$ (см. [8] и библиографию в ней).

Асимптотика числа и даже логарифма числа (и даже логарифма логарифма числа) n-арных квазигрупп порядков, больших 4, неизвестна. В [7] получены следующие нижние оценки:

$$
\begin{aligned}
&Q(n,5) \geqslant 2^{3^{n/3}-c}, && c < 0{,}072;\\
&Q(n,k) \geqslant 2^{(k/2)^n}, && k \text{ четно};\\
&Q(n,k) \geqslant 2^{n(k/3)^n}, && k \text{ кратно трем};\\
&Q(n,k) \geqslant 2^{\frac{3}{2}\lfloor k/3\rfloor^n}.
\end{aligned}
$$

В [4] для числа n-арных квазигрупп порядка k была предложена верхняя оценка

$$Q(n,k) \leqslant 3^{(k-2)^n} 2^{n(k-2)^{n-1}}.$$

В разделе 2 настоящей статьи усилена верхняя оценка числа n-арных квазигрупп конечного порядка и в раздел 3 усилена нижняя оценка числа n-арных квазигрупп нечетного порядка

$$\left(\frac{k-3}{2}\right)^{n/2}\left(\frac{k-1}{2}\right)^{n/2} \log_2 Q(n,k) \leqslant c_k(k-2)^n,$$

где c_k не зависит от n, точнее,

$$c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

2. Верхняя оценка

Будем говорить, что множество $M \subseteq \Sigma^n$ удовлетворяет свойству (A), если для любого элемента $\bar{x}$ из M и каждой позиции $i = 1,\dots,n$ найдется другой элемент $\bar{y}$ из M, отличающийся от $\bar{x}$ только в позиции i. По индукции легко получить следующее утверждение.

Предложение 1. *Любое непустое подмножество $C \subseteq \Sigma^n$, удовлетворяющее свойству* (A)*, имеет мощность не менее 2^n.*

Частичной n-арной квазигруппой порядка $|\Sigma|$ называется функция $g\colon \Omega \to \Sigma$, где $\Omega \subset \Sigma^n$, удовлетворяющая следующему свойству: $g(\bar{x}) \neq g(\bar{y})$ для любых двух наборов $\bar{x}, \bar{y} \in \Omega$, отличающихся ровно в одной позиции. Будем говорить, что n-арная квазигруппа $f\colon \Sigma^n \to \Sigma$ является продолжением частичной n-арной квазигруппы $g\colon \Omega \to \Sigma$, где $\Omega \subset \Sigma^n$, если $f|_\Omega \equiv g$.

Лемма 1. *Пусть $|\Sigma| = k$, $B = \Sigma \setminus \{a,b\}$, $k \geqslant 3$, $a,b \in \Sigma$. Тогда частичная n-арная квазигруппа $g\colon \Sigma^{n-1} \times B \to \Sigma$ имеет не более чем $2^{(k/2)^{n-1}}$ различных продолжений.*

Доказательство. Пусть P — множество неупорядоченных пар элементов множества Σ. Рассмотрим частичную n-арную квазигруппу $g\colon \Sigma^{n-1} \times B \to \Sigma$. Определим функцию $G\colon \Sigma^{n-1} \to P$ равенством

$$G(\bar{x}) = \Sigma \setminus \{g(\bar{x}c)\colon c \in \Sigma \setminus \{a,b\}\}.$$

Определим граф $\Gamma = \langle \Sigma^{n-1}, E\rangle$, в котором две вершины $\bar{x}$ и $\bar{y}$ соединены ребром тогда и только тогда, когда наборы $\bar{x}$ и $\bar{y}$ отличаются только в одной позиции и $G(\bar{x}) \cap G(\bar{y}) \neq \varnothing$. Нетрудно видеть, что компоненты связности графа Γ удовлетворяют свойству (A).

Пусть n-арные квазигруппы f_1 и f_2 являются продолжениями частичной n-арной квазигруппы g. Нетрудно видеть, что

$$\{f_1(\bar{x}a), f_1(\bar{x}b)\} = G(\bar{x})$$

для любого $\bar{x} \in \Sigma^{n-1}$, причем, если $f_1(\bar{x}a) = f_2(\bar{x}a)$, то продолжения f_1 и f_2 совпадают на всей компоненте связности графа Γ, содержащей вершину $\bar{x} \in \Sigma^{n-1}$. Таким образом, для однозначного определения продолжения частичной n-арной квазигруппы g достаточно зафиксировать одно из двух возможных значений в каждой компоненте связности графа Γ. Из предложения 1 следует, что каждая компонента связности имеет мощность не менее 2^{n-1}. Тогда число компонент связности графа Γ не превосходит $(k/2)^{n-1}$. Значит, g имеет не более $2^{(k/2)^{n-1}}$ продолжений.

Теорема 1. *Если $k \geqslant 5$ и $n \geqslant 2$, то*

$$Q(n,k) \leqslant 2^{c_k(k-2)^n},$$

где

$$c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

Доказательство. Число частичных n-арных квазигрупп $g\colon \Sigma^{n-1} \times B \to \Sigma$, где $|\Sigma| = k$, $B = \Sigma \setminus \{a,b\}$, не превосходит $Q(n,k)^{k-2}$. Из леммы 1 следует неравенство

$$Q(n+1,k) \leqslant Q(n,k)^{k-2} 2^{(k/2)^n}. \tag{1}$$

Введем обозначение

$$\alpha_n = \frac{\log_2 Q(n,k)}{(k-2)^n}.$$

Тогда из неравенства (1) следует, что

$$\alpha_{n+1} \leqslant \alpha_n + \left(\frac{k}{2(k-2)}\right)^n.$$

Поскольку

$$\alpha_1 = \frac{\log_2 k!}{k-2},$$

$$\sum_{n=1}^{\infty} \left(\frac{k}{2(k-2)}\right)^n = \frac{k}{k-4},$$

справедливо неравенство

$$\alpha_n \leqslant \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

3. Нижняя оценка

Пусть a и b — два различных элемента из Σ. Будем называть $\{a,b\}$-компонентой n-арной квазигруппы f такое множество $S \subset \Sigma^n$, что

(1) $f(S) = \{a,b\}$ и

(2) функция

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

также является n-арной квазигруппой.

В этом случае будем говорить, что g получена из f свитчингом компоненты S. Заметим, что в определении $\{a, b\}$-компоненты условие 2 можно заменить свойством (A) из предыдущего раздела. Очевидно, что свитчинг непересекающихся компонент можно производить независимо.

Предложение 2. *Пусть S и S' — непересекающиеся $\{a, b\}$- и $\{c, d\}$-компоненты n-арной квазигруппы f соответственно, и n-арная квазигруппа g получена из f свитчингом компоненты S. Тогда S' также является $\{c, d\}$-компонентой квазигруппы g.*

Следующее предложение нетрудно получить из определения $\{a, b\}$-компоненты, аналогичное утверждение имеется в [7].

Предложение 3. *Пусть множество $C = \{c_1, d_1\} \times \{c_2, d_2\}$ является $\{a, b\}$-компонентой 2-квазигруппы g. Пусть множество C_i является $\{c_i, d_i\}$-компонентой n_i-арной квазигруппы q_i при $i = 1, 2$. Тогда множество $C_1 \times C_2$ является $\{a, b\}$-компонентой $(n_1 + n_2)$-арной квазигруппы f, где*

$$f(\bar{x}_1, \bar{x}_2) \equiv g(q_1(\bar{x}_1), q_2(\bar{x}_2)).$$

Назовем 2-квазигруппу $\varphi\colon \Sigma \to \Sigma$ идемпотентной, если $\varphi(x, x) = x$ для любого $x \in \Sigma$. Известно (см., например, [2]), что верно следующее утверждение.

Предложение 4. *Для любого $m \geqslant 3$ имеется идемпотентная 2-квазигруппа порядка m.*

В следующем предложении приведена конструкция 2-квазигрупп, которая будет использована при доказательстве нижней оценки числа n-арных квазигрупп нечетного порядка.

Предложение 5. *Для любого $m \geqslant 3$ найдется 2-квазигруппа ψ порядка $2m + 1$, имеющая m $\{2i, 2i + 1\}$-компонент для каждого $i \in \{0, \dots, m - 1\}$, причем все, кроме одной, $\{2i, 2i + 1\}$-компоненты имеют вид $\{2j, 2j + 1\} \times \{2l, 2l + 1\}$.*

Доказательство. По предложению 4, найдется идемпотентная 2-квазигруппа φ_m порядка m. Для любых $a, b \in \{0, \dots, m - 1\}$, $a \neq b$, и $\delta, \sigma \in \{0, 1\}$ положим

$$\begin{aligned}
\psi(2a + \delta, 2b + \sigma) &= 2\varphi_m(a, b) + (\delta + \sigma \bmod 2);\\
\psi(2a + \delta, 2a + \delta) &= 2a + 1 - \delta;\\
\psi(2a + \delta, 2a + 1 - \delta) &= k - 1;\\
\psi(k - 1, 2a + \delta) &= \psi(2a + \delta, k - 1) = 2a + \delta;\\
\psi(k - 1, k - 1) &= k - 1.
\end{aligned}$$

Непосредственная проверка показывает, что ψ есть 2-квазигруппа, обладающая требуемыми свойствами.

Ниже приведен пример таблиц значений 2-квазигруппы φ_4 и соответствующей ψ:

φ_4:

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

ψ:

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

Из предложения 1 нетрудно заключить, что 2-квазигруппа нечетного порядка k, построенная в предложении 5, имеет максимальное число непересекающихся компонент среди всех 2-квазигрупп порядка k.

Теорема 2. *Если $k \geqslant 5$ — нечетное число и $n \geqslant 2$, то*

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

Доказательство. Пусть ψ — 2-квазигруппа порядка k, построенная в предложении 5. Определим рекуррентно n-арную квазигруппу Ψ^n равенствами

$$\Psi^2 \equiv \psi;$$
$$\Psi^{2m+1}(\bar{x}, y) = \psi(\Psi^{2m}(\bar{x}), y);$$
$$\Psi^{2m+2}(\bar{x}, y, z) = \psi(\Psi^{2m}(\bar{x}), \psi(y, z)).$$

Обозначим через α_n число $\{2i, 2i+1\}$-компонент n-арной квазигруппы Ψ^n, где $i \in \{0, \ldots, (k-3)/2\}$. Из предложений 3 и 5 следуют соотношения $\alpha_2 = (k-1)/2$, $\alpha_{2m+1} \geqslant \alpha_{2m}(k-3)/2$, $\alpha_{2m+2} \geqslant \alpha_{2m}((k-3)/2)((k-1)/2)$. Тогда

$$\alpha_{2m} \geqslant ((k-3)2)^{m-1}((k-1)/2^m, \qquad \alpha_{2m+1} \geqslant ((k-3)/2)^m((k-1)/2)^m.$$

Поскольку $\{2i, 2i+1\}$-компоненты при различных i не пересекаются, всего непересекающихся компонент не меньше, чем $(k-1)\alpha_n/2$. Из предложения 2 следует, что из n-арной квазигруппы Ψ^n свитчингами непересекающихся компонент можно получить требуемое число различных n-арных квазигрупп порядка k.

4. Число n-арных квазигрупп порядка 4

Введем обозначение $[n] = \{1, \ldots, n\}$; n-арная квазигруппа f называется n-арной лупой, если существует такой элемент $e \in \Sigma$, называемый единичным, что для всех $i \in [n]$ и $a \in \Sigma$ имеет место равенство $f(e \ldots e\underset{i}{a}e \ldots e) = a$. Далее мы всегда будем подразумевать, что 0 является единичным элементом n-арной лупы (в общем случае могут быть и другие единичные элементы). Особо отметим, что данное соглашение существенно в интерпретации понятия числа n-арных луп. В частности, справедлив следующий простой и хорошо известный факт.

Предложение 6. *Пусть $Q'(n,k)$ — число n-арных луп порядка k. Тогда*

$$Q(n,k) = k((k-1)!)^n Q'(n,k).$$

Разделимой (приводимой) называется n-арная квазигруппа f, если найдутся целое число m, $2 \leqslant m < n$, $(n-m+1)$-арная квазигруппа h, m-арная квазигруппа g и перестановка $\sigma : [n] \to [n]$, такие, что

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

В дальнейшем будем предполагать, что $\Sigma = \{0,1,2,3\}$, то есть речь пойдет только об n-арных квазигруппах порядка 4. Известно (см., например, [2]), что имеется ровно четыре бинарные лупы порядка 4 (одна изоморфна группе $Z_2 \times Z_2$ и три изоморфны группе Z_4).

Следующее утверждение является прямым следствием теоремы из [3].

Лемма 2. *Для разделимой n-арной лупы f порядка 4 справедливо одно и только одно из двух представлений:*

$$f(\bar{x}) = q_0(q_1(\tilde{x}_1),\dots,q_m(\tilde{x}_m)), \tag{2}$$

где q_j есть n_j-арные лупы при $j=1,\dots,m$, q_0 есть неразделимая m-арная лупа, $m \geqslant 3$, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}$ — разбиение множества $[n]$, причем в данном представлении разбиение $\{I_j\}$ единственно, и

$$f(\bar{x}) = q_1(\tilde{x}_1) * \dots * q_k(\tilde{x}_k), \tag{3}$$

где $*$ есть бинарная операция в одной из 4 луп, q_j есть n_j-арные лупы при j, $1 \leqslant j \leqslant k$, непредставимые 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 $\{I_j\}$ — разбиение множества $[n]$, причем в данном представлении разбиение $\{I_j\}$ единственно.

Корневой операцией n-арной квазигруппы f будем называть m-арную квазигруппу q_0, если имеет место представление (2), и бинарную операцию $*$, если имеет место представление (3).

Простой комбинаторный подсчет показывает, что число $F_{\bar{j},\bar{k}}$ различных разбиений множества $[n]$ на k подмножеств, из которых k_i подмножеств имеет мощность j_i, $1 \leqslant i \leqslant t$, $0 < j_1 < \dots < j_t$, удовлетворяет равенству

$$F_{\bar{j},\bar{k}} = \frac{n!}{(j_1!)^{k_1}\dots(j_t!)^{k_t}}\frac{1}{k_1!\dots k_t!}, \tag{4}$$

где

$$k_1 + k_2 + \dots + k_t = k,$$
$$k_1 j_1 + k_2 j_2 + \dots + k_t j_t = n.$$

Пусть $f\colon \Sigma^n \to \Sigma$ — n-арная квазигруппа, определим множество

$$S_{a,b}(f) \triangleq \{\bar{x} \in \Sigma^n : f(\bar{x}) \in \{a,b\}\}.$$

Назовем n-арную лупу f a-полулинейной, где $a \in \{1,2,3\}$ если характеристическая функция $\chi_{S_{0,a}(f)}$ множества $S = S_{0,a}(f)$ имеет вид

$$\chi_{S_{0,a}(f)}(x_1,\dots,x_n) \equiv \sum_{i=1}^{n} \chi_{\{0,a\}}(x_i) \bmod 2. \tag{5}$$

Будем называть линейной n-арную квазигруппу f, если она одновременно является a-полулинейной и b-полулинейной, где $a \neq b$, $a,b \in \{1,2,3\}$. Непосредственной проверкой нетрудно убедиться, что справедливо следующее утверждение.

Предложение 7. *Из четырех бинарных луп порядка* 4 *одна (изоморфная группе* $Z_2 \times Z_2$*) является линейной, а три остальных —* 1-*,* 2- *и* 3-*полулинейными соответственно.*

Справедливо следующее утверждение (см. [1]).

Предложение 8. *Линейная* n*-арная лупа единственна и является одновременно* 1-*,* 2- *и* 3-*полулинейной.*

Нетрудно видеть (см. также [1]), что справедливо следующее утверждение.

Предложение 9. *Пусть* f *— разделимая* a*-полулинейная* n*-арная лупа, тогда* f *можно представить как суперпозицию* a*-полулинейных луп вида* (2) *или* (3)*.*

Обозначим через l_n^a мощность множества a-полулинейных n-арных луп и через l_n — мощность множества полулинейных n-арных луп.

Как было установлено в [1], мощность множества всех n-арных луп асимптотически совпадает с мощностью множества полулинейных n-арных луп, которая легко вычисляется.

Лемма 3 ([1])**.** *Справедливы равенства*

$$l_n = 3 \cdot 2^{2^n - n - 1} - 2, \quad l_n^a = 2^{2^n - n - 1}, \quad a \in \{1, 2, 3\}.$$

В [6] получено описание n-арных квазигрупп порядка 4 в определенных выше терминах, а именно, доказана следующая теорема.

Теорема 3. *Каждая* n*-арная лупа порядка* 4 *является разделимой или полулинейной.*

На этом описании по-существу основывается вывод рекуррентной формулы для числа n-арных луп (и квазигрупп) порядка 4.

Введем следующие обозначения:

v_n — число n-арных луп (порядка 4);

r_n^* — число разделимых n-арных луп с бинарной корневой операцией $*$;

r_n^0 — число разделимых n-арных луп с корневой операцией арности, большей либо равной 3;

r_n^{a*} — число разделимых a-полулинейных n-арных луп с a-полулинейной бинарной корневой операцией $*$;

r_n^{a0} — число разделимых a-полулинейных n-арных луп с корневой операцией арности, большей либо равной 3;

p_n^a — число неразделимых a-полулинейных n-арных луп;

p_n — число неразделимых n-арных луп.

Из леммы 2 и предложения 9 вытекают следующие соотношения:

$$r_n^{a*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (l_{j_1}^a - r_{j_1}^{a*})^{k_1} \cdots (l_{j_t}^a - r_{j_t}^{a*})^{k_t},$$

$$r_n^{*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1} - r_{j_1}^{*})^{k_1} \cdots (v_{j_t} - r_{j_t}^{*})^{k_t},$$

$$r_n^{a0} = \sum_{i=3}^{n-1} p_i^a \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (l_{j_1}^a)^{k_1} \cdots (l_{j_t}^a)^{k_t},$$

$$r_n^{0} = \sum_{i=3}^{n-1} p_i \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1})^{k_1} \cdots (v_{j_t})^{k_t},$$

где вторая сумма берется по наборам $\bar{k} = (k_1, \ldots, k_t)$ и $\bar{j} = (j_1, \ldots, j_t)$ положительных целых чисел, удовлетворяющих равенствам

$$k_1 + \ldots + k_t = i,$$
$$k_1 j_1 + k_2 j_2 + \ldots + k_t j_t = n$$

и неравенствам $j_1 < \ldots < j_t$. Из теоремы 3 и предложения 8 вытекают соотношения

$$v_n = p_n + r_n^0 + 4 r_n^*,$$
$$p_n^a = l_n^a - r_n^{a0} - 2 r_n^{a*},$$
$$p_n = 3 p_n^a.$$

Из леммы 3 следует, что

$$l_n^a = 2^{2^n - n - 1}, \qquad a \in \{1, 2, 3\}.$$

Из предложения 7 получаем начальные значения для перечисленных выше величин:

$$r_2^{a*} = 2,$$
$$r_2^{*} = 4,$$
$$r_2^{a0} = r_2^{0} = 0.$$

Нетрудно видеть, что приведенные выше равенства и предложение 6 обеспечивают рекуррентный способ вычисления числа n-арных квазигрупп порядка 4.

Наконец, выпишем первые восемь значений величины $Q'(n, 4)$:
1,
4,
64,
7132,
201538000,
432345572694417712,
3987683987354747642922773353963277968,
67846927287489958255998624028528071036486706348977951042703872222975027683 2,
и $Q(n, 4)$:

24,
576,
55296,
36972288,
6268637952000,
80686060158523011084288,
44651852187365545446769179264602567250000192,
455827138491618934904429539585200818248078623084179800874168428190657696388582604 8.

5. Заключение

В заключение скажем несколько слов о связи тематики настоящей статьи с известным понятием латинского трэйда. Частичная n-арная квазигруппа $t\colon \Omega \to \Sigma$, $\Omega \subset \Sigma^n$, называется многомерным латинским трэйдом, далее просто трэйдом, если существует другая частичная n-арная квазигруппа $t'\colon \Omega \to \Sigma$ такая, что

(1) $t(\bar{x}) \neq t'(\bar{x})$ для всех $\bar{x} \in \Omega$;

(2) для любого i, $i = 1, \ldots, n$, и любых допустимых значений $x_1, \ldots, x_n$ множества $\{t(x_1, \ldots, x_{i-1}, y, x_{i-1}, \ldots, x_n) \mid y \in \Sigma\}$ и $\{t'(x_1, \ldots, x_{i-1}, y, x_{i-1}, \ldots, x_n) \mid y \in \Sigma\}$ совпадают.

В этом случае пара (t, t') называется битрэйдом (в зависимости от контекста, битрэйд рассматривают как упорядоченную, либо как неупорядоченную пару), а трэйд t' называется партнером трэйда t. Исследованию битрэйдов в случае $n = 2$ (латинских битрэйдов) уделяется значительное внимание, см. обзор [5].

Будем говорить, что n-арная квазигруппа f содержит трэйд t, если $t = f|_\Omega$ для некоторого Ω. При этом из определений следует, что замена значений f на множестве Ω значениями партнера t' трэйда t приводит к другой n-арной квазигруппе. Трэйды $t = f|_\Omega$ и $s = f|_\Theta$ назовем независимыми, если их носители (области определения) Ω и Θ не пересекаются. Максимальное число попарно независимых трэйдов, которые содержит n-арная квазигруппа f, назовем ее трэйдовым числом $\mathrm{trd}(f)$. Максимум $\mathrm{trd}(f)$ по всем n-арным квазигруппам f порядка k обозначим через $\mathrm{Trd}(n, k)$. Поскольку независимые трэйды в n-арной квазигруппе можно независимо заменять на партнеров, число $Q(n, k)$ различных n-арных квазигрупп порядка k удовлетворяет неравенству

$$Q(n, k) \geqslant 2^{\mathrm{Trd}(n,k)}. \tag{6}$$

Легко понять, что нижняя оценка в разделе 3 (как и все оценки в [7]) получена именно таким образом: $\{a, b\}$-компонента по определению является носителем некоторого трэйда. Поскольку носитель трэйда обладает свойством (A), из предложения 1 вытекает соотношение

$$\mathrm{Trd}(n, k) \leqslant k^n / 2^n = 2^{(\log_2 k - 1)n},$$

причем для четных k легко доказать равенство. Для нечетных k из результатов раздела 3 следует оценка

$$\mathrm{Trd}(n, k) \geqslant 2^{c(k)n},$$

где

$$c(k) \xrightarrow[k\to\infty]{} \log_2 k - 1.$$

Однако для фиксированных k, в частности, для малых значений $5, 7, \ldots$ вопрос об асимптотическом поведении величины $\mathrm{Trd}(n,k)$ остается открытым.

Проблема 1. При $n \to \infty$ вычислить асимптотику логарифма и асимптотику величины $\mathrm{Trd}(n,k)$ для нечетных $k \geqslant 5$.

Другой вопрос состоит в том, насколько оценка (6) близка к истинной. Для порядка 4 оценка (6) асимптотически точна после логарифмирования. Для большего фиксированного порядка асимптотика двукратного логарифма величины $Q(n,k)$ неизвестна. Кажется естественным предположить, что асимптотика двукратного логарифма величины $Q(n,k)$ и логарифма величины $\mathrm{Trd}(n,k)$ совпадают.

Проблема 2. Верно ли, что

$$\lim_{n\to\infty}\left(\frac{\log_2\log_2 Q(n,k)}{n}\right) = \lim_{n\to\infty}\left(\frac{\log_2 \mathrm{Trd}(n,k)}{n}\right)?$$

В частности, верно ли, что

$$\lim_{n\to\infty}\left(\frac{\log_2\log_2 Q(n,k)}{n}\right) \leqslant \log_2 k - 1?$$

Существование этих пределов также не доказано.

Список литературы

1. Потапов В. Н., Асимптотика числа n-квазигрупп порядка 4. *Сибирский матем. журнал* (2006) **47**, №4, 873–887.
2. Белоусов В. Д., *Основы теории квазигрупп*. Наука, Москва, 1967.
3. Черемушкин А. В., *Каноническая декомпозиция n-арных квазигрупп*. Штиинца, Кишинев, 1988.
4. Потапов В. Н., Верхняя оценка числа n-квазигрупп конечного порядка. В сб.: *Труды XVII международной школы-семинара «Синтез и сложность управляющих систем»*. Новосибирск, 2008, с. 135–137.
5. Cavenagh N. J., The theory and application of latin bitrades: A survey. *Mathematica Slovaca* (2008) **58**, 691–718.
6. Krotov D. S., Potapov V. N., n-ary quasigroups of order 4. *SIAM J. Discrete Math.* (2009) **23**, 561–570.
7. Krotov D. S., Potapov V. N., Sokolova P. V., On reconstructing reducible n-ary quasigroups and switching subquasigroups. *Quasigroups Relat. Syst.* (2008) **16**, 55–67.
8. McKay B. D., Wanless I. M., On the number of Latin squares. *Ann. Comb.* (2005) **9**, 335–344.
9. McKay B. D., Wanless I. M., A census of small Latin hypercubes. *SIAM J. Discrete Math.* (2008) **22**, 719–736.

Статья поступила 2.12.2009.