Math-Net.Ru

Общероссийский математический портал

В. Н. Поталов, Бесконечномерные квазигруппы конечных порядков, *Матем. заметки*, 2013, том 93, выпуск 3, 457–465

DOI: <https://doi.org/10.4213/mzm9141>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.196.121.252

26 апреля 2023 г., 15:03:03

Бесконечномерные квазигруппы конечных порядков

В. Н. Потапов

Пусть Σ – конечное множество мощности $k > 0$, $\mathbb{A}$ – некоторое конечное или бесконечное множество индексов, $\mathcal{F} \subseteq \Sigma^{\mathbb{A}}$ – подмножество, состоящее из наборов с конечным носителем. Функция $f: \Sigma^{\mathbb{A}} \rightarrow \Sigma$ называется $\mathbb{A}$ -квазигруппой (если $|\mathbb{A}| = n$, то n -арной квазигруппой) порядка k , когда $f(\bar{y}) \neq f(\bar{z})$ для упорядоченных наборов $\bar{y}$ и $\bar{z}$, различающихся ровно в одной позиции. Доказано, что $\mathbb{A}$ -квазигруппа f порядка 4 является разделимой (представимой в виде суперпозиции) или полулинейной на каждом смежном классе по $\mathcal{F}$.

Показано, что квазигруппы, определенные на $\Sigma^{\mathbb{N}}$, где $\mathbb{N}$ – натуральные числа, порождают неизмеримые по Лебегу подмножества отрезка $[0, 1]$.

Библиография: 6 названий.

DOI: 10.4213/mzm9141

1. Бесконечномерные квазигруппы и неизмеримые множества. Пусть Σ – некоторое непустое конечное множество, $\mathbb{A}$ – некоторое конечное или бесконечное множество, элементами которого нумеруются аргументы функций, действующих из $\Sigma^{\mathbb{A}}$ в Σ . Определим функцию $d: \Sigma^{\mathbb{A}} \times \Sigma^{\mathbb{A}} \rightarrow [0, \infty]$ так, что $d(\bar{y}, \bar{z})$ – число различающихся координат в $\bar{y}, \bar{z} \in \Sigma^{\mathbb{A}}$. Функция $f: \Sigma^{\mathbb{A}} \rightarrow \Sigma$ называется $\mathbb{A}$ -квазигруппой (далее просто квазигруппой или, если $|\mathbb{A}| = n$, то n -арной квазигруппой, см., например, [1]) порядка $|\Sigma|$, когда $f(\bar{y}) \neq f(\bar{z})$ при $d(\bar{y}, \bar{z}) = 1$.

Без ограничения общности можно положить $\Sigma = \{0, \dots, k-1\}$. Пусть $\mathbb{N}$ – множество натуральных чисел. Элементы множества $\Sigma^{\mathbb{N}}$ можно рассматривать как k -ичные представления вещественных чисел $\delta \in [0, 1]$. отождествим вещественные числа и их k -ичные представления¹.

ПРЕДЛОЖЕНИЕ 1. Для любой квазигруппы $f: \Sigma^{\mathbb{N}} \rightarrow \Sigma$ конечного порядка k и элемента $a \in \Sigma$ множество $\{\delta \in [0, 1] \mid f(\delta) = a\}$ неизмерно по Лебегу.

ДОКАЗАТЕЛЬСТВО. Предположим, что множество $B = \{\delta \in [0, 1] \mid f(\delta) = a\}$ измеримо. Пусть $\tau \in [0, 1]$ – некоторое k -ично рациональное число, в k -ичной записи которого не более начальных m символов отличны от нуля. Рассмотрим полуинтервал $[\tau, \tau + 1/k^{m+1})$. Из определения квазигруппы следует, что

$$(B \cap [\tau, \tau + 1/k^{m+1}) + i/k^{m+1}) \cap B = \emptyset \quad \text{для любого } i = 1, \dots, k-1.$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 10-01-00616) и ФЦП “Научные и научно-педагогические кадры инновационной России” на 2009–2013 гг., гос. контракт № 02.740.11.0362.

¹Для дальнейшего изложения не существенно нарушение взаимной однозначности на счетном множестве.

Тогда, используя инвариантность меры Лебега относительно сдвига множества, получаем неравенство $\mu(B \cap [\tau, \tau + 2/k^{m+1})) \leq \mu([\tau, \tau + 2/k^{m+1}))/2$. Поскольку в сколь угодно малой окрестности любой точки $v \in (0, 1)$ найдутся k -ично рациональные точки, имеем

$$\lim_{\varepsilon \rightarrow 0} \frac{\mu((v - \varepsilon, v + \varepsilon) \cap B)}{\mu((v - \varepsilon, v + \varepsilon))} \leq \frac{1}{2}.$$

По теореме Лебега о плотности для произвольного измеримого множества A этот предел равен 1 для почти всех точек $v \in A$. Тогда $\mu(B) = 0$. Кроме того, из определения квазигруппы имеем $[0, 1] \subset \bigcup_{i=1-k}^{1+k} (B + i/k)$. Тогда $\mu([0, 1]) = 0$. Пришли к противоречию.

Определим $\text{supp } \bar{y} = \{i \in \mathbb{A} \mid y_i \neq 0\}$. Обозначим через $\mathcal{I}$ совокупность конечных подмножеств множества $\mathbb{A}$. Пусть множество $\mathbb{A}$ бесконечно. Рассмотрим $\mathcal{F} = \{\bar{y} \in \Sigma^{\mathbb{A}} \mid \text{supp } \bar{y} \in \mathcal{I}\}$. Ясно, что множество $\Sigma^{\mathbb{A}}$ представимо в виде дизъюнктного объединения подмножеств вида $\mathcal{F}_{\bar{a}} = \bar{a} + \mathcal{F}$. Причем если $\mathcal{F}_{\bar{a}} \neq \mathcal{F}_{\bar{b}}$, то $d(\bar{y}, \bar{z}) = \infty$ для любых $\bar{y} \in \mathcal{F}_{\bar{a}}$ и $\bar{z} \in \mathcal{F}_{\bar{b}}$. Поэтому квазигруппа f может быть независимо определена на каждом $\mathcal{F}_{\bar{a}}$. В дальнейшем будем подразумевать, что $f: \mathcal{F} \rightarrow \Sigma$. Как будет показано ниже, квазигруппы на $\mathcal{F}$ допускают конструктивное определение, в то время как для определения квазигрупп на $\Sigma^{\mathbb{A}}$ необходимо выбирать по представителю из каждого класса $\mathcal{F}_{\bar{a}}$.

Символом x всюду будем обозначать набор аргументов (переменных) квазигруппы, через x_L будем обозначать выборку аргументов с индексами из множества L , $L \subseteq \mathbb{A}$. Ретрактом квазигруппы f называется подфункция, полученная из f подстановкой констант в некоторые аргументы, причем только конечное число констант может быть отлично от нуля. Число переменных ретракта будем называть его *размерностью*. Через $f_L(x_L)$ (или просто $f(x_L)$) будем обозначать ретракт квазигруппы $f: \mathcal{F} \rightarrow \Sigma$, в котором фиксированы нулем все аргументы, кроме имеющих индексы из множества L . Через $f(y_{\{i\}}, x_L)$ будем обозначать квазигруппу, полученную подстановкой функции, переменной или константы y на место аргумента x_i , $i \notin L$. Символами I и J будем обозначать только конечные подмножества в $\mathbb{A}$. Ясно, что ретракт f_J можно рассматривать как $|J|$ -арную квазигруппу.

Обозначим через S_0 группу перестановок на Σ , сохраняющих нуль². *Изотопией* (сохраняющей нуль) называется элемент множества $S_0 \times S_0^{\mathbb{A}}$. Две квазигруппы f и g называются *изотопными*, если $g(x_{\mathbb{A}}) = \theta_0(f(\theta_{\mathbb{A}}x_{\mathbb{A}}))$, $\theta_0 \in S_0$, $\theta_{\mathbb{A}} \in S_0^{\mathbb{A}}$. Если перестановка θ_0 тождественная, то квазигруппы f и g называют *главно изотопными*. Квазигруппа f называется *приведенной*, если при подстановке любого $a \in \Sigma$ в любой аргумент x_i , $i \in \mathbb{A}$, и нулей в остальные аргументы получаем a , т.е. справедливо равенство $f(a_{\{i\}}, \bar{0}_{\mathbb{A} \setminus \{i\}}) = a$.

Целью данной статьи является классификация квазигрупп порядка 4. Для этого ниже будут введены понятия разделимости (представимости в виде суперпозиции) и полулинейности квазигруппы; будет доказано, что все квазигруппы порядка 4 полулинейны или разделимы. Полулинейные квазигруппы допускают описание посредством булевых функций. Разделимые квазигруппы могут быть представлены

²Если множество $\mathbb{A}$ конечно, то нуль не фиксируют.

через собственные ретракты. Однако, в отличие от аналогичного описания квазигрупп конечной размерности (см. [6]), данная работа не обеспечивает конструктивной классификации бесконечномерных квазигрупп, ибо дерево разложения квазигруппы в суперпозиции может оказаться бесконечным.

2. Разделимость. Квазигруппа f называется *разделимой*, если она может быть представлена в виде суперпозиции, т.е. $f(x_{L_1}, x_{L_2}) = g(h(x_{L_1})_{\{j\}}, x_{L_2})$, где g и h – L_1 и $(\{j\} \cap L_2)$ -квазигруппы, $L_1 \cap L_2 = \emptyset$, $|L_1| \geq 2$, $|L_2| \geq 1$, $j \notin L_2^3$. В противном случае квазигруппа называется *неразделимой*.

Известно (см., например, [2]), что любая квазигруппа изотопна приведенной квазигруппе и приведенная разделимая квазигруппа может быть представлена как суперпозиция приведенных квазигрупп.

ПРЕДЛОЖЕНИЕ 2. Квазигруппа f тогда и только тогда представляется в виде суперпозиции $f(x_{L_1}, x_{L_2}) = g(h(x_{L_1})_{\{j\}}, x_{L_2})$, когда для любых наборов аргументов $y_{L_2}, y_{L_1}, y'_{L_1}$ из равенства $f(y_{L_1}, \bar{0}_{L_2}) = f(y'_{L_1}, \bar{0}_{L_2})$ следует равенство $f(y_{L_1}, y_{L_2}) = f(y'_{L_1}, y_{L_2})$.

ДОКАЗАТЕЛЬСТВО. Без ограничения общности считаем квазигруппу f приведенной и $1 = j \in L_1$. Необходимость очевидна, докажем достаточность. Определим $h = f_{L_1}$ и $g = f_{\{1\} \cup L_2}$.

Пусть

$$f(y_{L_1}, \bar{0}_{L_2}) = h(y_{L_1}) = a = f(a_{\{1\}}, \bar{0}_{L_1 \setminus \{1\}}, \bar{0}_{L_2})$$

для некоторого $a \in \Sigma$. Тогда

$$f(y_{L_1}, y_{L_2}) = f(a_{\{1\}}, \bar{0}_{L_1 \setminus \{1\}}, y_{L_2}) = g(a_{\{1\}}, y_{L_2}) = g(h(y_{L_1})_{\{1\}}, y_{L_2}).$$

Следующее утверждение является прямым следствием теоремы из [3].

УТВЕРЖДЕНИЕ 1. Разделимую n -арную квазигруппу f можно представить в виде

$$f(x_J) = F(q_1(x_{J_1}), \dots, q_m(x_{J_m})), \quad (2.1)$$

где q_j суть n_j -арные квазигруппы при $j \in \{1, \dots, m\}$, F есть неразделимая m -арная квазигруппа, $\{J_i\}$ – разбиение множества J на наборы мощности $n_1, \dots, n_m$. Причем, если $m \geq 3$, то в данном представлении разбиение $\{J_i\}$ единственно.

Это утверждение можно переформулировать следующим образом (см. [4; § 2]).

СЛЕДСТВИЕ 1. Если разделимая n -арная квазигруппа f имеет неразделимый ретракт размерности $m > 2$, который не содержится в неразделимых ретрактах большей размерности, то

$$\{x \mid x_0 = f_J(x_J)\} = \{x \mid q_0(x_{J_0}) = F(q_1(x_{J_1}), \dots, q_m(x_{J_m}))\}, \quad (2.2)$$

где q_j суть n_j -арные квазигруппы при $j \in \{0, \dots, m\}$, F есть неразделимая m -арная квазигруппа, $\{J_i\}$ – разбиение множества $J \cup \{0\}$ на наборы мощности $n_0, \dots, n_m$ ⁴.

³Для определенности будем полагать, что $j \in L_1$.

⁴Здесь и далее подразумеваем, что x_0 не является аргументом квазигруппы f .

Зафиксируем некоторую квазигруппу $f: \mathcal{F} \rightarrow \Sigma$. Будем говорить, что множество $M \subseteq \mathbb{A}$ *неразделимое* (относительно f), если $|M| \geq 3$ и для любого конечного набора $J \subseteq M$ найдется такой конечный набор J' , $J \subseteq J' \subseteq M$, что квазигруппа $f_{J'}$ неразделимая.

Система множеств, в которой для каждой пары множеств L_1, L_2 имеется такое множество L , что $L_1 \cup L_2 \subset L$, называется *направлением*. Будем говорить, что направление $S \subseteq \mathcal{I}$ *сходится* к множеству $M \subseteq \mathbb{A}$, если для каждого конечного подмножества в M найдется включающий его элемент направления S . По определению неразделимого множества M найдется сходящееся к M направление S , состоящее из неразделимых конечных наборов.

ПРЕДЛОЖЕНИЕ 3. Если направление $S \subseteq \mathcal{I}$ сходится к множеству $M \subseteq \mathbb{A}$ и $S = \bigcup_{i=1}^m S_i$, то найдется такое $i \in \{1, \dots, m\}$, что множество S_i есть направление, сходящееся к M .

ДОКАЗАТЕЛЬСТВО. Пусть S_i не есть направление, сходящееся к M . Тогда имеется $J_i \in \mathcal{I}$, которое не мажорируется элементами S_i . Рассмотрим $J = \bigcup_{i=1}^m J_i$. Найдется такое $I \in S$, что $J \subseteq I$. По условию $I \in S_i$ для некоторого $i \in \{1, \dots, m\}$. Пришли к противоречию.

ПРЕДЛОЖЕНИЕ 4. Если множество M неразделимое, то квазигруппа f_M неразделимая.

ДОКАЗАТЕЛЬСТВО. Предположим противное, т.е. имеется представление квазигруппы f_M в виде суперпозиции

$$f_M(x_{L_1}, x_{L_2}) = g(h(x_{L_1})_{\{i_0\}}, x_{L_2}), \quad (2.3)$$

где $M = L_1 \cup L_2$, $|L_1| \geq 2$, $|L_2| \geq 1$. Пусть $i_0, i_1 \in L_1$, $i_2 \in L_2$. По определению неразделимого множества найдется такой конечный набор J , $\{i_0, i_1, i_2\} \subset J \subseteq M$, что квазигруппа f_J неразделимая. Однако, это противоречит равенству (2.3).

Обращение этого утверждения, разбитое на два подслучая (леммы 1 и 2), является основным результатом этого и следующего разделов: если квазигруппа $f_{\mathbb{A}}$ неразделима, то множество $\mathbb{A}$ является неразделимым.

Обозначим через $\mathcal{N}(f)$ совокупность неразделимых подмножеств множества $\mathbb{A}$. Отметим, что если $\mathcal{N}(f) \neq \emptyset$, то множество $\mathcal{N}(f)$ содержит конечные элементы.

ПРЕДЛОЖЕНИЕ 5. Пусть $\mathcal{N}(f) \neq \emptyset$. Для любого неразделимого L найдется максимальный элемент M в $\mathcal{N}(f)$, содержащий L .

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольную конечную или бесконечную цепь (по включению) неразделимых множеств $\{L_\beta\}$. Покажем, что множество $K = \bigcup L_\beta$ неразделимо. Пусть $I \subset K$ – некоторый конечный набор. Тогда найдется такое β , что $I \subset L_\beta$ и, следовательно, имеется конечный неразделимый набор J' , $I \subseteq J' \subseteq L_\beta \subseteq K$. Требуемое следует из леммы Цорна.

Предполагая, что множество $\mathcal{N}(f)$ непусто, зафиксируем некоторый максимальный по включению элемент M_f в $\mathcal{N}(f)$.

ПРЕДЛОЖЕНИЕ 6. Пусть $J \in \mathcal{N}(f)$, $J' \in \mathcal{I}$ и $J \subset J'$. Тогда имеется представление

$$\{x \mid x_0 = f_{J'}(x_{J'})\} = \{x \mid q_0(x_{J_0}) = F(q_1(x_{J_1}), \dots, q_m(x_{J_m}))\}, \quad (2.4)$$

где q_i – n_i -арные квазигруппы при $i \in \{0, \dots, m\}$, F есть неразделимая m -арная квазигруппа, $\{J_i\}$ – разбиение множества $J' \cup \{0\} \in \mathcal{I}$ на наборы мощности $n_0, \dots, n_m$. Причем $|(J \cup \{0\}) \cap J_i| \leq 1$ для любого $i, i \in \{0, \dots, m\}$.

ДОКАЗАТЕЛЬСТВО. Если J есть максимальное неразделимое подмножество в J' , то требуемое получаем из следствия 1. В противном случае нужно применить следствие 1 к максимальному неразделимому множеству J'' , $J \subset J'' \subseteq J'$.

Заметим, что $m \geq |J|$ в (2.4), но не утверждается, что неравенство $m \geq |J|$ верно для всех представлений множества $\{x \mid x_0 = f_{J'}(x_{J'})\}$. Будем писать $[i, j]_{f, J' \supset J}$, если в представлении (2.4) для $f_{J'}$ имеем $i, j \in J_l$ для некоторого l , $0 \leq l \leq m$.

ПРЕДЛОЖЕНИЕ 7. Для любого $i \notin M_f$ найдется набор $J(i) \in \mathcal{I}$, $J(i) \subseteq M_f$ и единственное $\alpha(i) \in M_f \cup \{0\}$ такие, что для любых $J \in \mathcal{I}$, $i \in J$, $J(i) \subset J \subseteq M_f \cup \{0, i\}$ имеем $[i, \alpha(i)]_{f, J \supset J(i)}$.

ДОКАЗАТЕЛЬСТВО. Поскольку $i \notin M_f$, для конечных наборов $J' \subset M_f$, больших некоторого $J(i) \subseteq M_f$, квазигруппа $f_{J' \cup \{i\}}$ разделима. Очевидно, что набор индексов $J(i)$ можно выбрать неразделимым. Для определенности выбора будем считать множество индексов упорядоченным, а набор $J(i)$ лексикографически минимальным из возможных. По предложению 6 имеется представление (2.4). Если номер $\alpha(i)$ принимает различные значения $i_1, i_2 \in J(i)$ для различных конечных наборов $J', J'' \subseteq M_f$, то, подставляя нуль во все аргументы кроме аргументов с индексами из $\{0, i\} \cup J(i)$, в представлениях вида (2.4) для квазигрупп $f_{J'}$ и $f_{J''}$ приходим в противоречие с единственностью представления квазигруппы, обеспеченной утверждением 1.

ПРЕДЛОЖЕНИЕ 8. Для любых наборов $J', J'' \in \mathcal{I}$, $i \in J''$, $J' \subset M_f$, $J(i) \subset J' \subset J''$ имеем $[i, \alpha(i)]_{f, J'' \supset J'}$.

ДОКАЗАТЕЛЬСТВО. Из предложения 7 имеем $[i, \alpha(i)]_{f, J' \cup \{i\} \supset J(i)}$. Рассмотрим представление (2.4) для квазигруппы $f_{J''}$. Для того, чтобы убедиться в выполнении $[i, \alpha(i)]_{f, J'' \supset J'}$ достаточно подставить нуль во все аргументы кроме аргументов с индексами из $J' \cup \{0, i\}$ и применить утверждение 1.

СЛЕДСТВИЕ 2. Для любого конечного набора $J \subset \mathbb{A} \setminus M_f$ найдется такой набор $J' \in \mathcal{I}$, $J' \subset M_f$, что для любого набора $J'' \in \mathcal{I}$, $J' \cup J \subset J''$ и любого $i \in J$ имеем $[i, \alpha(i)]_{f, J'' \supset J'}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим конечный набор $J' \subset M_f$ такой, что $f_{J'}$ – неразделимая квазигруппа и $J(i) \subset J'$ для любого $i \in J$. Требуемое следует из предложения 8.

ЛЕММА 1. Если множество $\mathbb{A}$ разделимо и $\mathcal{N}_f \neq \emptyset$, то квазигруппа $f: \mathcal{F} \rightarrow \Sigma$ разделима.

ДОКАЗАТЕЛЬСТВО. Рассмотрим некоторое множество M_f ; по условию $M_f \neq \mathbb{A}$. Для любого $m \in M_f$ определим множество индексов $A_m = \{i \notin M_f \mid \alpha(i) = m\} \cup \{m\}$. Без ограничения общности можно считать, что $1 \in M_f$ и $|A_1| \geq 2$. Пусть $B = \mathbb{A} \setminus A_1$. Покажем, что для любых наборов аргументов y_B, y_{A_1}, y'_{A_1} из равенства $f(y_{A_1}, \bar{0}_B) = f(y'_{A_1}, \bar{0}_B)$ следует равенство $f(y_{A_1}, y_B) = f(y'_{A_1}, y_B)$. Рассмотрим произвольные $y, y' \in \mathcal{F}$ и конечный набор $J = \text{supp } y_B \cup \text{supp } y_{A_1} \cup \text{supp } y'_{A_1}$. По следствию 2

найдется такой набор $J' \subseteq M_f$, $J \cap M_f \subset J'$, что для любого конечного набора J'' , $J' \cup J \subset J''$ и любого $i \in J \setminus M_f$ имеем $[i, \alpha(i)]_{f, J'' \supset J'}$. Тогда $f_{J''}(x_{A_1 \cap J''}, x_{B \cap J''}) = g(h(x_{A_1 \cap J''})_{\{1\}}, x_{B \cap J''})$.

Пусть $f(y_{A_1}, \bar{0}_B) = f(y'_{A_1}, \bar{0}_B)$. Тогда $h(y_{A_1 \cap J''}) = h(y'_{A_1 \cap J''})$ и

$$f(y_{A_1}, y_B) = f_{J''}(y_{A_1 \cap J''}, y_{B \cap J''}) = f_{J''}(y'_{A_1 \cap J''}, y_{B \cap J''}) = f(y'_{A_1}, y_B).$$

Из предложения 2 получаем требуемое.

Методы, подобные использованным выше, применялись в [5] для исследования свойств разделимых n -арных квазигрупп.

3. Полная разделимость. Все 2-арные квазигруппы в соответствии с определением являются неразделимыми. Разделимая n -арная квазигруппа f называется *полностью коммутативно разделимой*, если все ее ретракты размерности, большей 2-х, разделимы и все ретракты размерности 2 изотопны коммутативным группам.

В дальнейшем будем предполагать, что $\Sigma = \{0, 1, 2, 3\}$, т.е. речь пойдет только об n -арных квазигруппах порядка 4. Известно (см., например, [1]), что все 2-арные квазигруппы порядка 4 изотопны либо группе $Z_2 \times Z_2$, либо группе Z_4 . Поэтому разделимые n -арные квазигруппы порядка 4, не содержащие неразделимых ретрактов размерности, большей 2-х, являются полностью коммутативно разделимыми. Следующее утверждение является прямым следствием теоремы из [3].

УТВЕРЖДЕНИЕ 2. *Полностью коммутативно разделимую n -арную квазигруппу $f: \Sigma^n \rightarrow \Sigma$ можно представить в виде*

$$f(x_{J_1}, \dots, x_{J_k}) = q_1(x_{J_1}) * \dots * q_k(x_{J_k}), \quad (3.1)$$

где $*$ есть коммутативная групповая операция, q_j суть n_j -квазигруппы при $j \in \{1, \dots, k\}$, не представимые в виде $q_j(x_{J'_j}, x_{J''_j}) = q'(x_{J'_j}) * q''(x_{J''_j})$. Причем в данном представлении конечные наборы $\{J_j\}$ и операция $*$ определяются единственным (при фиксированном нейтральном элементе группы) образом.

Полностью коммутативно разделимой n -квазигруппе f , имеющей представление (3.1), поставим в соответствие корневое дерево $T(f)$, внутренние вершины которого помечены операциями, а листья аргументами функции. Построим дерево рекуррентно. Предположим, что $T(g_j)$ – дерево, соответствующие функции q_j , $j \in \{1, \dots, k\}$; тогда дерево n -арной квазигруппы f определяется как корень, помеченный операцией $*$, с выходящими из него k ребрами, причем к j -му ребру присоединено дерево $T(q_j)$.

Пусть квазигруппа $f: \mathcal{F} \rightarrow \Sigma$ такова, что множество $\mathcal{N}(f)$ пусто. Будем обозначать $T(f_J)$ через T_J , где $J \in \mathcal{I}$. Рассмотрим в T_J минимальное поддереву, содержащее пару аргументов с индексами $i_1, i_2 \in J$, и обозначим через $C(J, i_1, i_2) \in \mathcal{I}$ множество индексов, соответствующих висячим вершинам этого поддерева. Корректность определения дерева T_J и множества $C(J, i_1, i_2)$ следует из утверждения 2. Множество $C(J, i_1, i_2) \in \mathcal{I}$ можно эквивалентно определить через существование следующего представления:

$$f_J(x_J) = g((h_1(x_{C_1}) * h_2(x_{C_2}))_{\{i_1\}}, x_{J \setminus (C_1 \cup C_2)}),$$

где $C_1 \cup C_2 = C(J, i_1, i_2)$, $i_1 \in C_1$, $i_2 \in C_2$, и квазигруппа $(h_1(x_{C_1}) * h_2(x_{C_2}))$ соответствует минимальному поддереву, содержащему пару аргументов с индексами $i_1, i_2 \in J$.

ПРЕДЛОЖЕНИЕ 9. Пусть $J \subset J' \in \mathcal{I}$, $i_1, i_2 \in J$. Тогда справедливо равенство $C(J, i_1, i_2) = C(J', i_1, i_2) \cap J$.

ДОКАЗАТЕЛЬСТВО. Имеем

$$f_{J'}(x_{J'}) = g((h_1(x_{C_1}) * h_2(x_{C_2}))_{\{i_1\}}, x_{J' \setminus (C_1 \cup C_2)}),$$

где $C_1 \cup C_2 = C(J', i_1, i_2)$, $i_1 \in C_1$, $i_2 \in C_2$. Подставляя нуль во все аргументы из $J' \setminus J$, получаем требуемое представление для квазигруппы f_J .

ЛЕММА 2. Пусть квазигруппа $f: \mathcal{F} \rightarrow \Sigma$ такова, что $\mathcal{N}(f) = \emptyset$. Тогда f разделима.

ДОКАЗАТЕЛЬСТВО. Без ограничения общности будем считать, что f приведенная. Если квазигруппа f линейна или f изотопна итерированной группе Z_4 , то f разделима. Иначе найдется такой набор $J = \{i_1, i_2, i_3\}$, что $f_J(x_J) = (x_{i_1} *_1 x_{i_2}) *_2 x_{i_3}$, где $*_1$ и $*_2$ – различные групповые операции. Рассмотрим множество $C = \bigcup C(J, i_1, i_2)$, где объединение берется по всем конечным наборам J , содержащим i_1, i_2 . Из предложения 9 получаем, что $i_3 \notin C$. Кроме того, для любого конечного набора $J \in \mathcal{I}$, $i_1, i_2 \in J$ имеем $C(J, i_1, i_2) = C \cap J$. Действительно, если $j \in (C \cap J) \setminus C(J, i_1, i_2)$, то $j \in C(J', i_1, i_2)$ для некоторого конечного набора J' . Тогда из предложения 9 имеем $j \in C(J' \cup J, i_1, i_2)$ и, следовательно, $j \in C(J, i_1, i_2)$.

Докажем, что $f(x_{\mathbb{A}}) = g(h(x_C)_{\{i_1\}}, x_{\mathbb{A} \setminus C})$. По предложению 2 достаточно доказать, что для любых аргументов $y_{\mathbb{A} \setminus C}, y_C, y'_C$ из равенства $f(y_C, \bar{0}_{\mathbb{A} \setminus C}) = f(y'_C, \bar{0}_{\mathbb{A} \setminus C})$ следует равенство $f(y_C, y_{\mathbb{A} \setminus C}) = f(y'_C, y_{\mathbb{A} \setminus C})$. Рассмотрим произвольные $y, y' \in \mathcal{F}$; обозначим $J = \text{supp } y \cup \text{supp } y' \cup \{i_1, i_2, i_3\}$. Тогда

$$f(y) = f_J(y_J) = g(h(y_{J \cap C})_{\{i_1\}}, y_{J \setminus C}).$$

Из равенства $f(y_C, \bar{0}_{\mathbb{A} \setminus C}) = f(y'_C, \bar{0}_{\mathbb{A} \setminus C})$ имеем $h(y_{J \cap C}) = h(y'_{J \cap C}) = a$ для некоторого $a \in \Sigma$. Тогда

$$\begin{aligned} f(y_C, y_{\mathbb{A} \setminus C}) &= f_J(y_C, y_{\mathbb{A} \setminus C}) = g(a_{\{i_1\}}, y_{\mathbb{A} \setminus C}) \\ &= g(h(y'_{J \cap C})_{\{i_1\}}, y_{\mathbb{A} \setminus C}) = f_J(y'_C, y_{\mathbb{A} \setminus C}) = f(y'_C, y_{\mathbb{A} \setminus C}). \end{aligned}$$

4. Полулинейность. Квазигруппа $f: \mathcal{F} \rightarrow \Sigma$ порядка 4 называется *полулинейной*, если она удовлетворяет равенству $f(\{0, 1\}^{\mathbb{A}} \cap \mathcal{F}) = \{0, 1\}$ или f изотопна квазигруппе, удовлетворяющей этому равенству. В частности, *приведенная линейная* квазигруппа $f(x_{\mathbb{A}}) = \sum_{\beta \in \mathbb{A}} x_{\beta}$ является полулинейной. Здесь подразумевается сложение, изоморфное групповой операции в $Z_2 \times Z_2$. Квазигруппы, изотопные приведенной линейной квазигруппе, также называют *линейными*.

Нетрудно видеть (см. также [2]), что полулинейные квазигруппы разделяются на три класса Q_1, Q_2, Q_3 , так что в Q_a содержатся квазигруппы, главно изотопные квазигруппам, удовлетворяющим равенству $f(\{0, 1\}^{\mathbb{A}} \cap \mathcal{F}) = \{0, a\}$.

В [2] доказано

УТВЕРЖДЕНИЕ 3. При $a \neq b$ множество $Q_a \cap Q_b$ совпадает с множеством линейных n -арных квазигрупп.

В [6] получено описание n -квазигрупп порядка 4 в определенных выше терминах, а именно, доказано

УТВЕРЖДЕНИЕ 4. *Для любого конечного n каждая n -арная квазигруппа порядка 4 является разделимой или полулинейной.*

Для бесконечномерных квазигрупп, используя утверждение 4, докажем следующую лемму.

ЛЕММА 3. *Пусть f – квазигруппа порядка 4 и $M \in \mathcal{N}(f)$. Тогда квазигруппа f_M полулинейна.*

ДОКАЗАТЕЛЬСТВО. Без ограничения общности считаем, что f приведенная. Если M конечное, то требуемое следует из утверждения 4. Далее полагаем, что множество M бесконечное. Поскольку $M \in \mathcal{N}(f)$, найдется направление $S \subseteq \mathcal{I}$, которое сходится к M . Пусть $B_a = \{J \in \mathcal{I} \mid J \in S, f_J \in Q_a\}$. Из предложения 3 следует, что как минимум одно из множеств B_a , $a \in \{1, 2, 3\}$, образует сходящееся к M направление. Известно (см., например, [2]), что если $J \in B_a$ $J' \subset J$, то $J' \in B_a$. Следовательно, B_a состоит из всех конечных подмножеств в M .

Если найдутся такие $a \neq b$, что направления B_a и B_b сходятся к M , то все квазигруппы f_J , $J \in S$, являются линейными по утверждению 3. Тогда квазигруппа f_M линейна. Если только одно из направлений B_a , $a \in \{1, 2, 3\}$, сходится к M , то определим $c_0 = a$.

Аналогичным образом определим c_i для каждого $i \in M$. А именно, определим квазигруппу $f_M^{(i)}$ как обращение квазигруппы f по i -му аргументу, т.е. так, что

$$\{(x, y) \mid x_i = f_M^{(i)}(x_{M \setminus \{i\}}, y_{\{i\}})\} = \{(x, y) \mid y = f_M(x_M)\}.$$

Затем найдем элемент $c_0 \in \{1, 2, 3\}$ для квазигруппы $f_M^{(i)}$ и обозначим его через c_i .

Пусть $\theta_i = (1, c_i)$. Рассмотрим квазигруппу $g_M(x_M) = \theta_0 f_M(\theta_M x_M)$. Нетрудно видеть, что $g_J(\{0, 1\}^{|J|}) = \{0, 1\}$ для любого $J \subseteq M$, $J \in \mathcal{I}$. Тогда квазигруппы g_M и f_M полулинейные.

Известно (см., например, [2]), что любая n -арная квазигруппа порядка 2 имеет вид

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n + \sigma \pmod{2},$$

где $\sigma \in \{0, 1\}$, и любая n -арная квазигруппа порядка 3 изотопна n -квазигруппе

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n + \sigma \pmod{3}.$$

Отсюда методом, подобным описанному выше, нетрудно доказать следующее

ПРЕДЛОЖЕНИЕ 10. (а) *Пусть $f: \mathcal{F} \rightarrow \{0, 1\}$ – квазигруппа порядка 2. Тогда $f(x_{\mathbb{A}}) = p(x_{\mathbb{A}}) + \sigma$, где $\sigma \in \{0, 1\}$ и $p(x_{\mathbb{A}}) = \sum_{i \in \mathbb{A}} x_i \pmod{2}$.*

(б) *Пусть $f: \mathcal{F} \rightarrow \{0, 1, 2\}$ квазигруппа порядка 3. Тогда f изотопна квазигруппе g , где $g(x_{\mathbb{A}}) = \sum_{i \in \mathbb{A}} x_i \pmod{3}$.*

Функция p называется *счетчиком четности*. Пусть $J \in \mathcal{I}$; определим функцию $\chi: \mathcal{I} \rightarrow \{0, 1\}^{\mathbb{A}}$ равенством $\chi(J) = \bar{\delta}$, где $\delta_i = 1$ тогда и только тогда, когда $i \in J$.

ПРЕДЛОЖЕНИЕ 11. Пусть g – полулинейная квазигруппа порядка 4. Тогда g изотопна некоторой квазигруппе f , сужения которой $f^J = f|_{\{2,3\}^J \times \{0,1\}^{\mathbb{A} \setminus J}}$ имеют вид

$$f^J(x) = 2p(\chi(J)) + (p(x \bmod 2) + \sigma_J) \bmod 2.$$

ДОКАЗАТЕЛЬСТВО. По определению полулинейности квазигруппа g изотопна квазигруппе f , удовлетворяющей равенству $f(\{0,1\}^{\mathbb{A}} \cap \mathcal{F}) = \{0,1\}$. Тогда по определению квазигруппы

$$f(\{2,3\}^J \times \{0,1\}^{\mathbb{A} \setminus J} \cap \mathcal{F}) = \begin{cases} \{0,1\}, & \text{при } p(\chi(J)) = 0, \\ \{2,3\}, & \text{при } p(\chi(J)) = 1. \end{cases}$$

Требуемое следует из предложения 10(а).

5. Основной результат.

ТЕОРЕМА 1. Пусть $f: \mathcal{F} \rightarrow \Sigma$ – квазигруппа порядка 4.

(а) Множество $\mathbb{A}$ неразделимое тогда и только тогда, когда квазигруппа $f_{\mathbb{A}}$ неразделимая.

(б) Квазигруппа f является разделимой или полулинейной.

ДОКАЗАТЕЛЬСТВО. (а) Если $\mathbb{A}$ конечное, то утверждение очевидно. Если $\mathbb{A}$ бесконечное, то утверждение следует из предложения 4 и лемм 1 и 2.

(б) Если $\mathbb{A}$ конечное, то применяем утверждение 4. Если $\mathbb{A}$ бесконечное, то утверждение пункта (б) следует из пункта (а) и леммы 3.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] В. Д. Белоусов, *n*-Арные квазигруппы, Штиинца, Кишинев, 1972.
- [2] В. Н. Потапов, Д. С. Кротов, “Асимптотика числа n -квазигрупп порядка 4”, *Сиб. матем. журн.*, **47:4** (2006), 873–887.
- [3] А. В. Черемушкин, “Каноническое разложение n -арных квазигрупп”, *Исследование операций и квазигрупп*, Матем. исследования, **102**, Штиинца, Кишинев, 1988, 97–105.
- [4] В. Н. Потапов, “О дополняемости частичных n -квазигрупп порядка 4”, *Матем. тр.*, **14:2** (2011), 147–172.
- [5] D. S. Krotov, “On reducibility of n -ary quasigroups”, *Discrete Math.*, **308:22** (2008), 5289–5297.
- [6] D. S. Krotov, V. N. Potapov, “ n -Ary quasigroups of order 4”, *SIAM J. Discrete Math.*, **23:2** (2009), 561–570.

В. Н. Потапов

Институт математики им. С. Л. Соболева СО РАН,
Новосибирский государственный университет
E-mail: vpotapov@math.nsc.ru

Поступило

29.04.2011

Исправленный вариант

26.02.2012