Вестник СПбГУ. Математика. Механика. Астрономия. 2020. Т. 7 (65). Вып. 2
УДК 512.573, 512.548.7
MSC 20N05

К 70-летию проф. А. И. Генералова

Автоморфизмы конечных квазигрупп без подквазигрупп*

В. А. Артамонов

Московский государственный университет имени М. В. Ломоносова,
Российская Федерация, 119991, Москва, Ленинские горы, 1
Всероссийская академия внешней торговли,
Российская Федерация, 119285, Москва, Воробьевское шоссе, 6А
Российская академия народного хозяйства и государственной службы,
Российская Федерация, 119571, Москва, пр. Вернадского, 84

Для цитирования: *Артамонов В. А.* Автоморфизмы конечных квазигрупп без подквазигрупп // Вестник Санкт-Петербургского университета. Математика. Механика. Астрономия. 2020. Т. 7 (65). Вып. 2. С. 197–209. https://doi.org/10.21638/11701/spbu01.2020.202

В работе рассматриваются конечные квазигруппы без подквазигрупп. Показано, что полиномиально полные квазигруппы с этим свойством квазитермальны. Исследуется случай, когда группа автоморфизмов действует транзитивно. Кроме того, изучаются квазигруппы примарного порядка, заданные на арифметическом векторном пространстве над конечным полем. Найдены необходимые условия, при которых умножение, заданное в координатной форме, определяет квазигруппу. Более подробно рассмотрен случай векторного пространства над полем из двух элементов. Получен критерий того, что умножение, заданное в координатной форме булевыми функциями, определяет квазигруппу. При некоторых предположениях описываются с точностью до изотопии квазигруппы порядка 4, задаваемые булевыми функциями. Полиномиально полные квазигруппы важны тем, что в них проблема решения полиномиальных уравнений NP-полна. Это свойство подчеркивает необходимость их использования для защиты информации, поскольку криптографические преобразования используют квазигрупповые операции. Отметим, что важную роль играют те квазигруппы, в которых нет подквазигрупп.

Ключевые слова: квазигруппа, автоморфизмы, перестановки.

1. Введение. Полиномиально полные конечные квазигруппы играют важную роль в проблемах передачи информации [1–8]. Квазигруппа Q *полиномиально полна*, если любая операция в Q является производной в смысле А. Г. Куроша, т. е. получается с помощью суперпозиций из операций умножения, взятия левого и правого обратных, переименования переменных, а также добавления всех констант. Известно, что конечная неодноэлементная квазигруппа полиномиально полна тогда и только тогда, когда она проста и неаффинна. Полиномиально полные квазигруппы интересны тем, что в них проблема решения полиномиальных уравнений NP-полна. Это свойство важно с точки зрения защиты информации. Поскольку криптографические

*Работа выполнена по российско-индийскому проекту QGSEC.
© Санкт-Петербургский государственный университет, 2020

преобразования используют квазигрупповые операции, то важную роль играют те квазигруппы, в которых нет подквазигрупп.

В теореме 1 доказывается квазипримальность конечных полиномиально полных квазигрупп без подквазигрупп. Это означает, что операция в квазигруппе термовая (является главной производной операцией в смысле А. Г. Куроша) тогда и только тогда, когда она перестановочна со всеми автоморфизмами квазигруппы. В связи с этим возникает новая задача изучения автоморфизмов полиномиально полных конечных квазигрупп без подквазигрупп.

В таких квазигруппах группа автоморфизмов действует без неподвижных точек. Если дополнительно группа автоморфизмов действует транзитивно, то квазигруппу можно отождествить со своей группой автоморфизмов. Некоторые простейшие факты о строении возникающих квазигрупп рассмотрены в теореме 3.

В теореме 4 изучаются квазигруппы примарного порядка p^n, допускающие автоморфизм порядка p. Указывается вид квазигруппового умножения. Остается обратная задача — выяснить, когда умножение указанного вида задает полиномиально полную квазигруппу без подквазигрупп.

С точки зрения приложений важны квазигруппы порядка 2^n. Они рассматриваются как векторные арифметические пространства над полем из двух элементов, причем умножение задается булевыми функциями от координат. Эти квазигруппы изучаются в разделе 4. Они образуют частный случай квазигрупп, рассмотренных в разделе 3. Пока нет критерия, характеризующего квазигрупповые умножения в $\mathbb{F}_2^n$ в терминах полиномов над $\mathbb{F}_2$. Некоторые необходимые уточнения в этом направлении получены в теореме 5.

Изучается частный случай квазигрупп с умножением (7) (см. раздел 4), навеянный изучением квадрик, и рассмотренный в [9, 10]. В теореме 6 показано, что необходимые условия из теоремы 5 являются достаточными для того, чтобы получалась квазигруппа. В разделе 3 с точностью до изотопии охарактеризованы квазигруппы порядка 4, построенные с помощью умножения (7) на $\mathbb{F}_2^2$.

Напомним основные определения, используемые в работе. Квазигруппа Q *аффинна*, если в ней можно задать таким образом структуру аддитивной абелевой группы $(Q, +)$, что основная операция умножения имеет вид $x * y = \alpha(x) + \beta(y) + c$, где α, β — автоморфизмы группы $(Q, +)$.

Пусть на множестве Q заданы две квазигрупповые операции умножения xy и $x * y$. Скажем, что возникающие квазигруппы *изотопны*, если существуют такие перестановки π, π_1, π_2 на Q, что $x * y = \pi^{-1}(\pi_1(x)\pi_2(y))$ для всех $x, y \in Q$.

Квазигруппа MQQ определена на конечномерном арифметическом пространстве $\mathbb{F}_2^n$, где каждая координата квазигруппового произведения задается многочленом над полем $\mathbb{F}_2$ от координат множителей. Степень по каждой переменной не выше 1.

Конечная универсальная алгебра квазипримальна, если каждая операция, перестановочная с изоморфизмами подалгебр, является термовой, т. е. получается суперпозицией основных операций с помощью переименования переменных.

Целью работы является изучение автоморфизмов полиномиально полных квазигрупп без собственных подквазигрупп, а также рассмотрение способов построения новых квазигрупп с этими свойствами. Обзор результатов в этом направлении приведен в [11].

2. Автоморфизмы. Всюду в работе через Q обозначается конечная квазигруппа без собственных подквазигрупп, а через G — ее группа автоморфизмов. Действие $g \in G$ на $x \in Q$ будем обозначать через gx.

Предложение 1. *Группа G действует в Q без неподвижных точек, т. е. если $g \in G$ и $gx = x$ для некоторого $x \in Q$, то $g = 1$.*

Доказательство. Пусть $g \in G$ и $gx = x$ для некоторого $x \in Q$. Так как g является автоморфизмом, то множество всех таких $y \in Q$, что $gy = y$, образует подквазигруппу. По условию она совпадает с Q, откуда $g = 1$.

Теорема 1. *Пусть Q — конечная полиномиально полная квазигруппа без подквазигрупп. Тогда Q квазипримальна.*

Доказательство. Базисные операции умножения, перехода к левому и правому обратному сюръективны. Следовательно, квазигруппа является сюръективной алгеброй в смысле [12]. По теореме 3.4 из [12] квазигруппа Q в случае неквазипримальности либо аффинна, либо является алгеброй вида $(N; F)^{[m]}$, где N — множество, $Q = N^m$ и F — примитивная группа перестановок на N.

Поскольку полиномиально полная квазигруппа неаффинна, то остается показать, что последний случай невозможен. Напомним, как устроены операции в алгебре $(N; F)^{[m]}$ с носителем N^m. Введем обозначение $\mathfrak{n} = \{0, 1, \ldots, n-1\}$.

Пусть μ — отображение множества $\mathfrak{m}$ в множество $\mathfrak{n}$ и σ — преобразование $\mathfrak{m}$. Для $g_0, \ldots, g_{m-1} \in F$ и

$$x_i = \begin{pmatrix} x_i^0 \\ \vdots \\ x_i^{m-1} \end{pmatrix}, \quad i = 0, \ldots, n-1,$$

вводятся операции

$$h_\mu^\sigma(g_0, \ldots, g_{m-1})\,(x_0, \ldots, x_{n-1}) = \left(g_0(x_{0\mu}^{0\sigma}), \ldots, g_{m-1}(x_{(m-1)\mu}^{(m-1)\sigma})\right).$$

Тогда $(N; F)^{[m]}$ — алгебра, все термовые операции которой имеют указанный вид [12, теорема 3.4].

При $n = 2$ каждая операция $h_\mu^\sigma(g_0, \ldots, g_{m-1})$ не является квазигрупповой, поскольку ее значение при фиксированном x_0 не задает биекцию относительно x_1.

Пусть Q — конечная квазигруппа без подалгебр и π — автоморфизм Q. Предположим, что $\pi = \pi_1 \cdots \pi_m$ — разложение π на независимые циклы.

Предложение 2. *Длины всех циклов $\pi_1, \ldots, \pi_m$ одинаковы. В частности, порядок Q делится на длину цикла.*

Доказательство. Пусть d — минимальная длина цикла в π. Тогда π^d имеет неподвижные элементы и потому $\pi^d = 1$. Таким образом, длины всех циклов делят d. Учитывая выбор d, получаем требуемое утверждение.

Предложение 3. *Зафиксируем $x \in Q$. Предположим, что группа автоморфизмов G действует в Q транзитивно. Тогда отображение $\zeta : G \to Q$, заданное по правилу $g \mapsto gx$, является биекцией.*

Доказательство. В силу транзитивности действия G в Q отображение ζ сюръективно. Пусть $\zeta(g) = \zeta(h)$. Тогда $gx = hx$, откуда $h^{-1}gx = x$. По предложению 1 получаем $h^{-1}g = 1$ и $h = g$.

Итак, можно считать, что $G = Q$, причем элементы $g \in G = Q$ действуют как умножение слева на g в группе G. При этом умножение $*$ в квазигруппе $Q = G$ удовлетворяет условию

$$g(x * y) = gx * gy \tag{1}$$

для всех $x, y \in G$. Другими словами, умножение $*$ является гомоморфизмом левых G-множеств, т. е. $* : G \times G \to G$.

Рассмотрим обратную ситуацию. Пусть G — конечная группа, являющаяся квазигруппой с умножением $*$, причем выполнены равенства (1) для всех $x, y, g \in G$.

Теорема 2. *G совпадает с группой автоморфизмов $(G, *)$.*

Доказательство. Из (1) следует, что каждое отображение $x \mapsto gx$ является автоморфизмом квазигруппы $(G, *)$. Далее нам потребуются следующие леммы.

Лемма 2.1. *Предположим, что Q_0 — подквазигруппа наименьшего порядка в $(G, *)$, и H — множество всех таких $h \in G$, что $h(Q_0) = Q_0$. Тогда $Q_0 = H$ и H является группой автоморфизмов Q_0.*

Доказательство. Если $x \in Q_0$, то $hx \in Q_0$. Обратно, пусть $gx \in Q_0$, где $g \in G$. Так как g — автоморфизм Q, и Q порождается x, то $gy \in Q_0$ для всех $y \in Q_0$. Отсюда $g \in H$.

Пусть ξ — автоморфизм Q_0. Если $x \in Q_0$, то в силу свойства транзитивности действия G получаем, что $\xi(x) = gx$ для некоторого $g \in G$. Так как Q_0 порождается элементом x, то $\xi(y) = gy \in Q_0$ для всех $y \in Q_0$. Отсюда $\xi = g \in H$.

Лемма 2.2. *Если $g \in G$, то $g(Q_0) = gH$ является минимальной подквазигруппой в $Q = G$. При этом Q является объединением непересекающихся минимальных подквазигрупп вида $g(Q_0)$. Это объединение совпадает с разложением G на левые смежные классы G по H.*

Доказательство. Так как отображение $z \mapsto gz$ является в силу (1) автоморфизмом квазигруппы Q, то $g(Q_0)$ также является подквазигруппой минимального порядка в Q. В силу транзитивности действия G в G посредством левого умножения получаем утверждение о разложении G.

Завершим доказательство теоремы. Пусть ψ — произвольный автоморфизм $(G, *)$. Тогда ψ переставляет минимальные подквазигруппы g_iH в силу леммы 2.2.

Пусть $\psi(g_iH) = g_jH$. Если $x \in H = Q_0$, то найдется такой элемент $x' \in Q_0$, что $\psi(g_ix) = g_jx'$. Отсюда $x' = g_j^{-1}\psi g_i(x)$ и сопоставление $x \mapsto x'$ является автоморфизмом Q_0. Следовательно, $g_j^{-1}\psi g_i = h \in H$ по лемме 2.1. Отсюда $\psi = g_jhg_i^{-1} \in G$.

В заключение первого раздела отметим несколько утверждений, носящих общий характер. В них допускается, что в Q есть подквазигруппы.

Предложение 4. *Пусть в квазигруппе Q порядка не менее 3 группа автоморфизмов G действует 2-транзитивно. Тогда $a^2 = a$ для всех $a \in Q$.*

Доказательство. Пусть $a \in Q$, причем $a^2 \neq a$. По условию существует такой автоморфизм σ в Q, что $\sigma(a) = a,\ \sigma(a^2) \neq a^2$. Но $\sigma(a^2) = \sigma(a)^2 = a^2$, противоречие. Отсюда вытекает утверждение.

Предложение 5. *Пусть Q — произвольная конечная квазигруппа, содержащая не менее двух элементов. Тогда группа автоморфизмов G не может действовать 3-транзитивно в Q.*

Доказательство. Пусть G действует 3-транзитивно и $ax = b$ в Q. Тогда для любого $y \neq x \in Q$ найдется такой автоморфизмв $\zeta \in G$, что $\zeta(a) = a,\ \zeta(b) = b,\ \zeta(x) = y$. В этом случае $ay = b$, что противоречит определению квазигруппы.

Пусть Q — произвольная квазигруппа. Рассмотрим операторы левого L_x и правого R_y умножений в квазигруппе Q. Через $G(Q)$ обозначим группу перестановок на Q, порождаемую всеми перестановками $L_x L_y^{-1}, R_x R_y^{-1}$ для всех $x, y \in Q$.

Теорема 3. *Пусть группа $G(Q)$ действует в Q 2-транзитивно и порядок Q не меньше 3. Тогда G полиномиально полна.*

Доказательство. Нам потребуется следующая лемма.

Лемма 3.1. *Пусть группа F действует на множестве X дважды транзитивно и порядок X не меньше 3. Тогда группа F неабелева.*

Доказательство. Пусть группа F абелева. Так как F действует транзитивно, то стабилизаторы любых точек одинаковы. Отсюда следует, что стабилизаторы единичны. Пусть x, y, z — три разные точки из X. В силу 2-транзитивности существует такой элемент $f \in F$, что $f(x) = x$ и $f(y) = z$. Но тогда $f = 1$ и $z = y$, что неверно.

Продолжим доказательство теоремы. Если квазигруппа Q аффинна, то она изотопна абелевой группе и потому $G(Q)$ — абелева группа (теорема 2 из [2]), что неверно.

Пусть квазигруппа Q непроста и ρ — нетривиальная конгруэнция в Q. По определению отношение конгруэнтности по модулю ρ стабильно относительно действия группы $G(Q)$. Если $x \neq y$ конгруэнтны по модулю ρ, а x, z не конгруэнтны, то не может существовать элемента $f \in G(Q)$ с условием $f(x) = x,\ f(y) = z$. Следовательно, Q проста. Остается воспользоваться критерием полиномиальной полноты [13].

3. Примарный случай. Предположим, что Q — конечная квазигруппа без подквазигрупп, причем порядок Q примарен и равен $q = p^n$, где p просто. Пусть в Q группа автоморфизмов нетривиальна. Обозначим через $*$ умножение в Q. Пусть π — нетривиальный автоморфизм Q. По предложению 2 автоморфизм π как перестановка является произведением циклов одинаковой длины, делящей q. Поэтому их длина равна p^m, где $m \leqslant n$. В этом случае $\pi^{p^{m-1}}$ является автоморфизмом порядка p, разлагающимся в произведение циклов длины p.

Зафиксируем автоморфизм π порядка p. В этом случае Q можно отождествить с полем $\mathbb{F}_q$, причем автоморфизм π порядка p имеет вид $\pi(x) = x + 1$ в $\mathbb{F}_q$.

Умножение в Q задается в виде многочлена $x * y = f(X, Y) \in \mathbb{F}_q[X, Y]$, где степень по каждой переменной X, Y не выше $q - 1$. Поскольку π является автоморфизмом, то выполнено равенство

$$f(X + 1, Y + 1) = f(X, Y) + 1. \tag{2}$$

Теорема 4. *Условие* (2) *выполнено тогда и только тогда, когда*

$$f(X,Y) = X + F(X^p - X, Y - X), \tag{3}$$

где $F(X^p - X, Y - X) \in \mathbb{F}_q[X^p - X, Y - X]$.

Доказательство. Если $f(X,Y)$ имеет указанное представление (3), то выполнено и (2).

Обратно, пусть выполнено (2). Переходя к новым переменным $X, Y - X$, можно считать, что

$$f(X,Y) = \sum_{i=0}^{q-1} f_i(X)(Y-X)^i, \quad f_i(X) \in \mathbb{F}_q[X].$$

Тогда в (2) получаем

$$\sum_{i=0}^{q-1} f_i(X+1)(Y-X)^i = 1 + \sum_{i=0}^{q-1} f_i(X)(Y-X)^i.$$

Отсюда $f_i(X+1) = f_i(X) + \delta_{i0}$ при $i = 0, \ldots, q-1$.

Далее используем следующую лемму.

Лемма 4.1. *Пусть* $h(X) \in \mathbb{F}_q[X]$. *Следующие условия эквивалентны:*
1) $h(X+1) = h(X)$;
2) $h(X) = u(X^p - X)$, *где* $u(X) \in \mathbb{F}_q[X]$.

Доказательство. Ясно, что 2 влечет 1. Покажем, что 1 влечет 2.

Пусть ζ — корень $h(X)$. Тогда $\zeta + 1$ также корень $h(X)$. Таким образом, $\zeta, \zeta + 1, \ldots, z + p - 1$ являются корнями $h(X)$. Поэтому $h(X)$ делится на $(X - \zeta)(X - \zeta - 1) \cdots (X - \zeta - p + 1) = (X - \zeta)^p - (X - \zeta) = (X^p - X) - (\zeta^p - \zeta)$. Применяя это к каждому корню ζ, получаем требуемое утверждение.

Продолжая доказательство теоремы, получаем, что $f_i(X) = u_i(X^p - X)$ при $i > 0$. При $i = 0$ имеем $f_0(X+1) = 1 + f_0(x)$. Положим $g_0(X) = f_0(X) - X$. Тогда $g_0(X+1) = f_0(X+1) - X - 1 = 1 + f_0(X) - X - 1 = g_0(X)$. Таким образом, по лемме 4.1 получаем $g_0(X) = u_0(X^p - X)$ и $f_0(X) = X + u_0(X^p - X)$. Отсюда вытекает утверждение.

Следствие. *Если* $f(X,Y)$ *из теоремы 4, то*

$$f(X,Y) = Y + G(X - Y, Y^p - Y) \tag{4}$$

для некоторого многочлена G.

Итак, $Q = \mathbb{F}_q$ имеет вид (3) и (4). Так как Q относительно умножения $f(X,Y)$ является квазигруппой, функции $F(b^p - b, Z), G(Z, a^p - a) \in \mathbb{F}_q[Z]$, являются перестановками в $Q = \mathbb{F}_q$ при любых $a, b \in \mathbb{F}_q$. Другими словами, отображения

$$Z \mapsto F(b^p - b, Z), \quad Z \mapsto G(Z, a^p - a)$$

являются перестановками в $Q = \mathbb{F}_q$.

4. MQQ. Рассмотрим квазигруппы MQQ из работ [9, 10]. Пусть Q является векторным пространством размерности n над полем $\mathbb{F}_q$. Будем считать, что $Q = \mathbb{F}_q^n$ —

арифметическое векторное пространство столбцов высоты n с коэффициентами из поля $\mathbb{F}_q$, и

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},\ z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \in \mathbb{F}_q^n. \tag{5}$$

Обозначим через $\mathcal{O}(\mathbb{F}_q^{2n})$ алгебру функций на $\mathbb{F}_q^{2n}$ со значениями в $\mathbb{F}_q$. Известно, что

$$\mathcal{O}(\mathbb{F}_q^{2n}) \simeq \mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_n]/(x_i^q - x_i, y_j^q - y_j \mid 1 \leqslant i, j \leqslant n).$$

Каждый элемент из $\mathcal{O}(\mathbb{F}_q^{2n})$ однозначно представляется многочленом с коэффициентами из $\mathbb{F}_q$, причем степень по каждой переменной меньше q.

Квазигрупповое умножение в $\mathbb{F}_q^n$ для x, y, z из (5) задается по правилу $x * y = z$, где $z_i = z_i(x, y) \in \mathcal{O}(\mathbb{F}_q^{2n})$, $1 \leqslant i \leqslant n$, представлены многочленами указанного вида. Рассмотрим $(n \times n)$-матрицы якобианов

$$J_x = \left(\frac{\partial z_i}{\partial x_j}\right),\ J_y = \left(\frac{\partial z_i}{\partial y_j}\right). \tag{6}$$

Теорема 5. *Определители* $\det J_x, \det J_y$ *как функции из* $\mathcal{O}(\mathbb{F}_q^{2n})$ *принимают ненулевые значения в* $\mathbb{F}_q$. *В частности, если* $q = 2$, *то* $\det J_x = \det J_y = 1$.

Доказательство. Квазигрупповое умножение обладает тем свойством, что при любом y отображение $x \to z$ биективно в $\mathbb{F}_q^n$. Рассмотрим правое обратное отображение $z \to x$, которое также задается функциями из $\mathcal{O}(\mathbb{F}_q^{2n})$. Оба отображения $x \to z$ и $z \to z$ представляются многочленами степени меньше q по каждой переменной. Якобиан произведения в $\mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_n]$ отображений $x \to z \to x$ является произведением якобиана J_x и аналогичного якобиана J_z. В силу того, что отображения взаимно обратны в $\mathcal{O}(\mathbb{F}_q^{2n})$, получаем, что

$$J_x J_z \equiv E \mod (x_i^q - x_i, y_j^q - y_j \mid 1 \leqslant i, j \leqslant n)$$

в $\mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_n]$. Переходя к $\mathcal{O}(\mathbb{F}_q^{2n})$, получаем, что $\det J_x \cdot \det J_z = 1$. Случай J_y аналогичен. Отсюда вытекает первое утверждение.

Пусть $q = 2$. Тогда $\det J_x, \det J_y$ принимают ненулевые значения в $\mathbb{F}_2$, которые единственны и равны 1.

Перейдем к случаю, когда $q = 2$ и умножение $x * y = z$ задается по правилу

$$z_i = \begin{pmatrix} {}^t x & 1 \end{pmatrix} \begin{pmatrix} A_i & b_i \\ c_i, & d_i \end{pmatrix} \begin{pmatrix} y \\ 1 \end{pmatrix} = {}^t x A_i y + c_i y + {}^t x b_i + d_i, \quad i = 1, \dots, n, \tag{7}$$

где $A_i \in \mathrm{Mat}(n, \mathbb{F}_2)$. Кроме того, b_i, c_i — столбцы и строки высоты n, и $d_i \in \mathbb{F}_2$. Положим

$$C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 & \dots & b_n \end{pmatrix} \in \mathrm{Mat}(n, \mathbb{F}_2), \quad D = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \in \mathbb{F}_2^n.$$

Рассмотрим, при каких условиях Q с умножением (7) является квазигруппой. Это означает, что при произвольных фиксированных x и z система линейных уравнений

$$\left(\begin{pmatrix} {}^txA_1 \\ \vdots \\ {}^txA_n \end{pmatrix} + C\right) y = z + Bx + D \tag{8}$$

относительно y должна иметь единственное решение.

Аналогично для произвольных фиксированных $y, z \in \mathbb{F}_2^n$ система линейных уравнений

$$\left(\begin{pmatrix} {}^ty{}^tA_1 \\ \vdots \\ {}^ty{}^tA_n \end{pmatrix} + {}^tB\right) x = z + Cy + D \tag{9}$$

относительно $x_1, \ldots, x_n$ должна иметь единственное решение.

Заметим, что якобианы J_x, J_y из (6) имеют, соответственно, вид

$$J_x = J_{x,B} = \left(\begin{pmatrix} {}^ty{}^tA_1 \\ \vdots \\ {}^ty{}^tA_n \end{pmatrix} + {}^tB\right), \; J_y = J_{y,C} = \left(\begin{pmatrix} {}^txA_1 \\ \vdots \\ {}^txA_n \end{pmatrix} + C\right). \tag{10}$$

Следующий результат усиливает теорему 2 из [9].

Теорема 6. *Q является квазигруппой в том и только в том случае, когда* $\det C = \det B = 1$ *и для любого $x \in \mathbb{F}_2^n$ выполнены условия*

$$\det\left(\begin{pmatrix} {}^txA_1C^{-1} \\ \vdots \\ {}^txA_nC^{-1} \end{pmatrix} + E\right) = \det\left(\begin{pmatrix} {}^tx\,{}^tA_1({}^tB)^{-1} \\ \vdots \\ {}^tx\,{}^tA_n({}^tB)^{-1} \end{pmatrix} + E\right) = 1. \tag{11}$$

Доказательство. Квадратные системы линейных уравнений (8), (9) должны иметь единственное решение при любых $x, y \in \mathbb{F}_2^n$. В частности, при $x = y = 0$ получаем, что $\det C = \det B = 1$.

Совершая замены переменных

$$y \mapsto C^{-1}y', \quad x \mapsto ({}^tB)^{-1}x' \tag{12}$$

и, переименовывая y на x, получаем над $\mathbb{F}_2$ две квадратные системы линейных уравнений с матрицами из (11). Единственность решений этих систем эквивалентна тому, что их определители равны 1.

Таким образом, необходимое условие из теоремы 5 в случае умножения (7) является и достаточным.

Заметим, что замены (12) задают изотопию на Q. Поэтому переходя к этому изотопу, можно считать, что $C = B = E$. В этом случае уравнения (11) принимают вид

$$\det\left(\begin{pmatrix} {}^txA_1 \\ \vdots \\ {}^txA_n \end{pmatrix} + E\right) = \det\left(\begin{pmatrix} {}^tx\,{}^tA_1 \\ \vdots \\ {}^tx\,{}^tA_n \end{pmatrix} + E\right) = 1. \tag{13}$$

Из (8) следует, что

$$L_x(y) = \left(\begin{pmatrix} {}^t xA_1 \\ \vdots \\ {}^t xA_n \end{pmatrix} + E \right) y + x + D$$

и

$$L_x^{-1}(y) = \left(\begin{pmatrix} {}^t xA_1 \\ \vdots \\ {}^t xA_n \end{pmatrix} + E \right)^{-1} (y + x + D).$$

В частности, $L_0^{-1}(y) = (y + D)$, откуда в силу (10)

$$L_x L_0^{-1}(y) = \left(\begin{pmatrix} {}^t xA_1 \\ \vdots \\ {}^t xA_n \end{pmatrix} + E \right) (y + D) + x + D =$$

$$= \left(\begin{pmatrix} {}^t xA_1 \\ \vdots \\ {}^t xA_n \end{pmatrix} + E \right) y + \begin{pmatrix} {}^t xA_1 \\ \vdots \\ {}^t xA_n \end{pmatrix} D + x = J_{y,E} y + \begin{pmatrix} {}^t xA_1 \\ \vdots \\ {}^t xA_n \end{pmatrix} D + x \quad (14)$$

Аналогично получаем

$$R_y(x) = \left(\begin{pmatrix} {}^t y\, {}^t A_1 \\ \vdots \\ {}^t y\, {}^t A_n \end{pmatrix} + E \right) x + y + D,$$

откуда $R_0(x) = x + D$ и $R_0(x)^{-1}(x) = (x + D)$. Поэтому в силу (10)

$$R_y R_0^{-1}(x) = \left(\begin{pmatrix} {}^t y\, {}^t A_1 \\ \vdots \\ {}^t y\, {}^t A_n \end{pmatrix} + E \right) (x + D) + y + D =$$

$$= \left(\begin{pmatrix} {}^t y\, {}^t A_1 \\ \vdots \\ {}^t y\, {}^t A_n \end{pmatrix} + E \right) x + \begin{pmatrix} {}^t y\, {}^t A_1 \\ \vdots \\ {}^t y\, {}^t A_n \end{pmatrix} D + y = J_{x,E} x + \begin{pmatrix} {}^t y\, {}^t A_1 \\ \vdots \\ {}^t y\, {}^t A_n \end{pmatrix} D + y. \quad (15)$$

Таким образом, в силу теорем 3 и 6 справедлива

Теорема 7. *Квазигруппа $Q = \mathbb{F}_2^n$ с умножением* (7) *полиномиально полна, если подгруппа $G(Q)$ группы аффинных преобразований на $\mathbb{F}_2$, порожденная всеми элементами* (14), (15), *для всех $x, y \in \mathbb{F}_2^n$ действует 2-транзитивно в $\mathbb{F}_2^n$.*

Итак, в силу теоремы 6 требуется описать квадратные матрицы $A_1, \ldots, A_n$ над $\mathbb{F}_2$ с условием (13) для любых $x \in \mathbb{F}_2^n$.

В дальнейшем через e_i будем обозначать строку $(0, \ldots, 0, 1, 0, \ldots, 0)$, где 1 стоит на i-м месте.

Предложение 5. *В равенстве* (13) *все матрицы $A_1, \ldots, A_n$ вырождены.*

Доказательство. Пусть матрица A_i невырождена. Выберем такой вектор x, что ${}^txA_i = e_i$. Тогда в первом определителе из (13) столбец с номером i нулевой, что неверно.

Пусть

$$1 = \det\left(\begin{pmatrix} {}^txA_1 \\ \vdots \\ {}^txA_n \end{pmatrix} + E\right) = 1 + \sum_{k=1}^{n} \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} x_{i_1}\cdots x_{i_k} W_{i_1,\ldots,i_k}, \tag{16}$$

где $W_{i_1,\ldots,i_k} \in \mathbb{F}_2$. Можно заметить, что $W_{i_1,\ldots,i_k}$ равно сумме определителей, получающихся из E заменой части строк на строки матриц $A_1,\ldots,A_n$ с номерами $i_1,\ldots,i_k$, причем все эти строки встречаются, возможно, несколько раз. Например, W_1 равно сумме определителей, где в первой строке стоит строка с номером σ_1 из $A_1,\ldots,$ в последней строке стоит строка с номером σ_n из A_n. Здесь σ — перестановка степени n.

Любая функция от $x_1,\ldots,x_n$ на $\mathbb{F}_2$ однозначно представляется многочленом, в котором степень по каждой переменной не выше 1. Поэтому справедливо

Предложение 6. *Условие* (16) *эквивалентно системе равенств* $W_{i_1,\ldots,i_k} = 0$ *при любых наборах* $1 \leqslant i_1 < \cdots < i_k \leqslant n$. *Аналогичное утверждение верно и для второго определителя из* (13), *т. е. для матриц* ${}^tA_1,\ldots,{}^tA_n$.

Рассмотрим случай $n = 2$. Обе матрицы A_1, A_2 вырождены. Пусть

$$A_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad A_2 = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

По предложению 6 имеем

$$\begin{aligned} W_1 &= a + q + aq + pb = 0, \\ W_2 &= c + s + cs + rd = 0, \\ W_{12} &= as + cq + rb + dp = 0. \end{aligned}$$

Аналогично переходя к транспонированным матрицам

$${}^tA_1 = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, \quad {}^tA_2 = \begin{pmatrix} p & r \\ q & s \end{pmatrix},$$

получаем

$$\begin{aligned} \widehat{W_1} &= a + r + ar + cp = 0, \\ \widehat{W_2} &= b + s + bs + qd = 0, \\ \widehat{W_{12}} &= W_{12}. \end{aligned}$$

Все эти соотношения можно переписать в виде

$$(1 + a)(1 + q) + pb = 1, \tag{17}$$
$$(1 + c)(1 + s) + rd = 1, \tag{18}$$
$$(1 + a)(1 + r) + pc = 1, \tag{19}$$

$$(1+b)(1+s)+qd=1, \tag{20}$$
$$as+cq+rb+dp=0. \tag{21}$$

Если $p=0$, то $a=q=r=0$ по (17), (19). Но тогда $b=s=c=0$ по (18), (20). Отсюда получаем

$$A_1=\begin{pmatrix}0&0\\0&d\end{pmatrix},\ \text{где } d=0,1;\quad A_2=\begin{pmatrix}0&0\\0&0\end{pmatrix}. \tag{22}$$

Пусть $p=1$. Если $d=0$, то $c=s=b=0$ по (18), (20). Поэтому $a=r=q=0$ в силу (18), (20). Отсюда имеем

$$A_1=\begin{pmatrix}0&0\\0&0\end{pmatrix},\quad A_2=\begin{pmatrix}1&0\\0&0\end{pmatrix}. \tag{23}$$

Предположим, что $p=d=1$. Если $b=0$, то $a=q=0$ по (17), откуда $dp=1$ по (21), что неверно.

Рассмотрим случай $p=d=b=1$. Если $c=0$, то $a=r=0$ по (19), что снова противоречит (21).

Пусть $p=d=b=c=1$. Если $q=0$, то $b=0$, что неверно.

Пусть $p=d=b=c=q=1$. Если $r=0$, то получается противоречие с (18).

Предположим, что $p=d=b=c=q=r=1$. Тогда в (21) получаем $a=s=1$. Отсюда

$$A_1=\begin{pmatrix}1&1\\1&1\end{pmatrix},\quad A_2=\begin{pmatrix}1&1\\1&1\end{pmatrix}. \tag{24}$$

Итак, доказана

Теорема 8. *Пусть задана квазигруппа порядка 4 с умножением вида* (7)*. Тогда с точностью до изотопии матрицы A_1, A_2 имеют вид* (22)–(24)*.*

В заключение отметим, что в работе [1] описаны полиномиально полные квазигруппы порядка 4 в терминах их латинских квадратов.

Автор выражает глубокую благодарность рецензентам за многочисленные полезные замечания.

Литература

1. *Artamonov V. A., Chakrabarti S., Gangopadhyay S., Pal S. K.* On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts // Quasigroups and Related Systems. 2013. Vol. 21. P. 201–214.

2. *Artamonov V. A., Chakrabarti S., Pal S. K.* Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations // J. Discrete Applied Mathematics. 2016. Vol. 200. P. 5–17. https://doi.org/10.1016/j.dam.2015.06.033

3. *Artamonov V. A., Chakrabarti S., Pal S. K.* Characterizations of highly non-associative quasigroups and associative triples // Quasigroups and Related Systems. 2017. Vol. 25. P. 1–19.

4. *Dénes J., Keedwell A. D.* Latin Squares and their Applications. Budapest: Akadémiai Kiadó; New York: Academic Press; London: English Universities Press, 1974.

5. *Dénes J., Keedwell A. D.* Latin squares. New developments in the theory and applications. North-Holland, Amsterdam, 1991. (Vol. 46 Annals of Discrete Mathematics).

6. *Gligoroski D., Dimitrova V., Markovski S.* Quasigroups as Boolean Functions, their equation systems and Gröbner Bases / Eds. M. Sala, L. Peret, S. Sakata, C. Traverso. Gröbner Bases, Coding cna Cryptography. Springer-Heidelberg, 2009. P. 415–420.

7. *Horvath G., Nehaniv C. L., Szabo Cs.* An assertion concerning functionally complete algebras and NP-completeness // Theoret. Comput. Sci. 2008. Vol. 407. P. 591–595.

8. *Liu G., Xu Yu.* Cryptographic classification of quasigroups of order 4 // International Workshop on Cloud Computing and Information Security (CCIS). 2013. P. 278–281.

9. *Gligoroski D., Markovski S., Knapskog S. J.* Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups // MATH'08: Proccedings of the Amer. Conference on Applied Mathematics. 2008. P. 44–49. Steven Point, Wisconsin, USA, World Scientific and Engeneering Academy and Society (WSEAS).

10. *Samardjiska S., Chen Ya., Gligoroski D.* Construction of multivariate quadratic quasigoups (MQQs) in arbitrary Galois fields // 7th International conference on Information assurance and security (IAS). 2011. P. 314–319.

11. *Artamonov V. A.* Applications of quasigroups to cryprography // Sarajevo Journal of Mathematics. 2018. Vol. 14(27), no. 2. P. 191–205.

12. *Szendrei A.* Simple surjective algebras having no proper subalgebras // J. Austral Math. Soc., series a. 1990. Vol. 48. P. 434–454.

13. *Hagemann J., Herrmann C.* Arithmetically locally equational classes and representation of partial functions, Universal algebra, Estergom (Hungary), vol. 29, Colloq. Math. Soc. Janos Bolyai, 1982. P. 345–360.

Статья поступила в редакцию 7 ноября 2019 г.;
после доработки 9 декабря 2019 г.;
рекомендована в печать 12 декабря 2019 г.

Контактная информация:

Артамонов Вячеслав Александрович — д-р физ.-мат. наук; artamon@mech.math.msu.su

Automorphisms of finite quasigroups with no subquasigroups*

V. A. Artamonov

Lomonosov Moscow State University, 1, Leninskie Gory, Moscow, 119991, Russian Federation
Russian Foreign Trade Academy, 6A, Vorobiyovskoye shosse, Moscow, 119285, Russian Federation
Russian Academy of National Economy and Public Administration,
84, pr. Vernadskogo, Moscow, 119571, Russian Federation

For citation: Artamonov V. A. Automorphisms of finite quasigroups with no subquasigroups. *Vestnik of Saint Petersburg University. Mathematics. Mechanics. Astronomy*, 2020, vol. 7 (65), issue 2, pp. 197–209. https://doi.org/10.21638/11701/spbu01.2020.202 (In Russian)

It is shown that polynomially complete quasigroups with no subquasigroups are quasitermal. The case of transitive action of the automorphism group on these quasigroups is considered. In particular the case of quasigroup of a prime power order defined on arithmetic vector space over a finite field is considered in details. There are found some necessary conditions under which a multplication in this space given in terms of coordinates corresponds to a quasigroup. The case of the 2-element field is considered in detalis. In this case the quasigroup multiplication is given in terms of Boolean function. The is found a criteria for a quasigroup multiplication. Under some assumptions there are classified up to an isotopy all quasigroups of order 4 in terms of Boolean function. Polynomially complete quasigroups play a significant role because the problem of solutions of polynomial equation in them is NP-complete. This property is important for the securing information, since

*The work is supported Russian-Indian project QGSEC.

crypto-transformations are defined in terms of quasigroup operations. The same argument shows the importance of quasigroups with no proper subquasigroups.

Keywords: quasigroups, automorphism, permutations.

References

1. Artamonov V. A., Chakrabarti S., Gangopadhyay S., Pal S. K., "On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts", *Quasigroups and Related Systems* **21**, 201–214 (2013).

2. Artamonov V. A., Chakrabarti S., Pal S. K. "Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations", *J. Discrete Applied Mathematics* **200**, 5–17 (2016). https://doi.org/10.1016/j.dam.2015.06.033

3. Artamonov V. A., Chakrabarti S., Pal S. K., "Characterizations of highly non-associative quasigroups and associative triples", *Quasigroups and Related Systems* **25**, 1–19 (2017).

4. Dénes J., Keedwell A. D., *Latin Squares and their Applications* (Akadémiai Kiadó, Budapest; Academic Press, New York; English Universities Press, London, 1974).

5. Dénes J., Keedwell A. D., *Latin squares. New developments in the theory and applications* (North-Holland, Amsterdam, 1991, Vol. 46 Annals of Discrete Mathematics).

6. Gligoroski D., Dimitrova V., Markovski S., *Quasigroups as Boolean Functions, their equation systems and Gröbner Bases*, 415–420 (M. Sala, L. Peret, S. Sakata, C. Traverso (eds.), Gröbner Bases, Coding and Cryptography, Springer-Heidelberg, 2009).

7. Horvath G., Nehaniv C. L., Szabo Sz., "An assertion concerning functionally complete algebras and NP-completeness", *Theoret. Comput. Sci.* **407**, 591–595 (2008).

8. Liu G., Xu Yu., "Cryptographic classification of quasigroups of order 4", *International Workshop on Cloud Computing and Information Security (CCIS 2013)*, 278–281 (2013).

9. Gligoroski D., Markovski S., Knapskog S. J., "Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups", *MATH'08: Proccedings of the Amer. Conference on Applied Mathematics*, 44–49 (Steven Point, Wisconsin, USA, World Scientific and Engeneering Academy and Society (WSEAS), 2008).

10. Samardjiska S., Chen Ya., Gligoroski D., "Construction of multivariate quadratic quasigoups (MQQs) in arbitrary Galois fields", *7th International conference on Information assurance and security (IAS)*, 314–319 (2011).

11. Artamonov V. A., "Applications of quasigroups to cryprography", *Sarajevo Journal of Mathematics* **14(27)**(2), 191–205.

12. Szendrei A., "Simple surjective algebras having no proper subalgebras", *J. Austral Math. Soc., series a* **48**, 434–454 (1990).

13. Hagemann J., Herrmann C., "Arithmetically locally equational classes and representation of partial functions", *Universal algebra* **29**, 345–360 (Estergom (Hungary), Colloq. Math. Soc. Janos Bolyai, (1982)).

Received: November 7, 2019
Revised: December 9, 2019
Accepted: December 12, 2019

Author's information:

Viacheslav A. Artamonov — artamon@mech.math.msu.su