ЧЕБЫШЕВСКИЙ СБОРНИК
Том 19. Выпуск 2

УДК 512.57, 512.54 DOI 10.22405/2226-8383-2018-19-2-111-122

Квазигруппы и их приложения[1]

Артамонов Вячеслав Александрович — доктор физико-математических наук, профессор, заведующий кафедрой высшей алгебры механико-математического факультета Московского государственного университета имени М. В. Ломоносова; заведующий кафедрой информатики и математики, Всероссийская академия внешней торговли; профессор, Российская академия народного хозяйства и государственной службы при Президенте РФ.
e-mail: viacheslav.artamonov@gmail.com

Аннотация

В работе приводится обзор результатов, полученных в ходе работы по теме 0АААА-А16-116070810025-5 и по завершившемуся совместному проекту с индийскими алгебраистами С. Чакрабарти, С. Гангопапдуем, С. Палом. В работе приняли участие российские алгебраисты В.Т. Марков и А.Е. Панкратьев.

Цель работы состоит в изучении алгебраических свойств конечных полиномиально полных квазигрупп, проблемы их расознавания по латинскому квадрату и в построении полиномиально полных квазигрупп квазигрупп достаточно большого порядка. Кроме того, нас интересуют полиномиально полные квазигруппы без подквазигрупп. Приведены достаточные условия полиномиально полноты квазигруппы Q в терминах группы $G(Q)$. Например, достаточно, чтобы $G(Q)$ действовала дважды транзитивно на Q. Отмечено поведение $G(Q)$ при изотопиях. Показано что любую конечную квазигруппу можно вложить в полиномиально полную. Рассмотрена конструкция бипроизведения квазигрупп. Результаты применяются для защиты информации.

Ключевые слова: квазигруппы, латинские квадраты, группы перестановок, транзитивность.

Библиография: 10 названий.

Для цитирования:
В. А. Артамонов. Квазигруппы и их приложения // Чебышевский сборник, 2018, т. 19, вып. 2, с. 111–122.

[1]Работа выполнена в рамках темы 0АААА-А16-116070810025-5 "Алгебраические системы: группы, кольца, универсальные алгебры; алгебраическая геометрия; группы Ли и теория инвариантов; компьютерная алгебра, теория кодирования"

CHEBYSHEVSKII SBORNIK
Vol. 19. No. 2

UDC 512.57, 512.54 DOI 10.22405/2226-8383-2018-19-2-111-122

Quasigroups and their applications

Artamonov Vyacheslav Alexandrovich — doctor of physical and mathematical sciences, professor, head of the department higher algebra's of the mechanics and mathematics faculty of the M. V. Lomonosov Moscow State University; head of the department of informatics and mathematics, Russian foreign trade academy; professor, The Russian Presidential Academy of National Economy and Public Administration.
e-mail: viacheslav.artamonov@gmail.com

Abstract

A survey of results obtained within the project 0AAAA-A16-116070810025-5 and the recent joint project with Indian algebraists S.Chakrabarti, S. Gangopahyay, S. Pal and also with Russian participants V.T. Markov, A.E. Pankratiev.

The aim of projects is a study of algebraic properties of finite polynomially complete quasigroups, the problem of their recognition from its Latin square and constructions of polynomially complete quasigroups of sufficiently large order. We are also interested in poly nomially complete quasigroups with no subquasigroups. There are found sufficient conditions of polynomial completeness of a quasigroups Q in terms of a group $G(Q)$. For example it suffices if $G(Q)$ acts doubly transitive in Q. There is found a behaviour of $G(Q)$ under isotopies.

It is shown that any finite quasigroup can be embedded into a polynomial complete one. The results are applied for securing an information.

Keywords: quasigroups, Latin squres, permutation groups, transitivity

Bibliography: 10 titles.

For citation:
V. A. Artamonov, 2018, "Quasigroups and their applications" , *Chebyshevskii sbornik*, vol. 19, no. 2, pp. 111–122.

1. Введение

В работе исследуется вопрос о выборе класса конечных квазигрупп, применимого для криптографических преобразование. В качестве такого класса предлагается выбрать класс полиномиально полных квазигрупп, в которых вопрос о разрешимости уравнение является NP-полным.

В работе рассматривается вопрос о распознавании полиномиальной полноты конечным квазигрупп, заданных латинскими квадратами. Показывается, что это можно сделать с помощью группы $G(Q)$.

Далее рассматривается вопрос о построении полиномиально полных квазигрупп достаточно большого порядка. Это делается с помощью вложения любой конечной квазигруппы в полиномиально полную, а также с помощью конструкции бипроизведения.

Устанавливается свзязь с переходом к изотопу, не имеющему подквазигрупп.

2. Системы операций

Для непустого множества A через A^n, $n \geqslant 0$, обозначим n-ую декартову степень множества A. В частности, при $n = 0$ под A^0 будм понимать одноэлементное множество $\{*\}$.

Под *n-арной алгебраической операцией* на A будет понимать произвольное отображение $f : A^n \to A$. В частности, *нульарная* операция $f : \{*\} = A^0 \to A$ фиксирует элемент $f(*) \in A$.

Через $\mathcal{O}_n(A)$ обозначим множество всех n-арных алгебраических операций на A. Пусть $\mathcal{O}(A)$ — семейство всех $\{\mathcal{O}_n(A) \mid n \geqslant 0\}$.

Рассмотрим семейство множеств $F = \{F_n \mid n \geqslant 0\}$, которое будет называть *сигнатурой*. Непустье множество A называется *алгеброй сигнатуры* Fили *F-алгеброй*, если задано такое отображение $\alpha : F \to \mathcal{O}(A)$, что $\alpha(F_n) \subseteq \mathcal{O}_n(A)$. Это одначает, что каждый элемент $f \in F_n$ реализуется с помощью α как n-арная операция в A.

Например, *квазигруппой* называется непустое множество Q с умножением xy, причем для любых $a, b \in Q$ каждое из уравнений $ax = b$, $ya = b$ имеет и притом единственное решение $a \diagdown b$, и $a \diagup b$, соответственно.

Если $f \in \mathcal{O}_n(A)$ и $g_1, \dots, g_n \in \mathcal{O}_m(A)$, то можно определить *суперпозицию (композицию)* $f(g_1, \dots, g_n) \in \mathcal{O}_m(A)$ по правилу

$$[f(g_1, \dots, g_n)]\,(x_1, \dots, x_m) = f\left(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)\right) \qquad (1)$$

для всех $x_1, \dots, x_m \in A$.

Композиция удовлетворяет закону *суперассоциативности*

$$[f(g_1, \dots, g_n)]\,(h_1, \dots, h_m) = f\left(g_1(h_1, \dots, h_m), \dots, g_n(h_1, \dots, h_m)\right) \qquad (2)$$

для любых $f \in \mathcal{O}_n(A)$, $\quad g_1, \dots, g_n \in \mathcal{O}_m(A)$, $\quad h_1, \dots, h_m \in \mathcal{O}_r(A)$.

Заметим, что если операции $g_1, \dots g_n$ из (1) нульарны, и $g_i(*) = a_i \in A$, то

$$[f(g_1, \dots, g_n)]\,(*) = f(a_1, \dots, a_n)$$

значение f в точке $(a_1, \dots, a_n)$.

Семейство $\mathcal{O}(A)$ содержит операции проекции $p_{in}(x_1, \dots, x_n) = x_i$.

Легко видеть, что если $f \in \mathcal{O}_n(A)$, то $f = f(p_{1n}, \dots, p_{nn})$.

Семейство $\mathcal{C} = \{\mathcal{C}_n \subseteq \mathcal{O}_n(A) \mid n \geqslant 0\}$ называется *клоном операций* на A, если $\mathcal{C}$ содержит все проекции и замкнуто относительно суперпозиций.

Предложение 1. *Если $f \in \mathcal{C}_n$ и операция g получена из f с помощью перестановки или отождествления некоторых аргументов, то $g \in \mathcal{C}$.*

Если $F = \{F_n \mid n \geqslant 0\}$ — сигнатура и A является F-алгеброй. Без ограничения общности можно считать, что $F_n \subseteq \mathcal{O}_n(A)$ для любого индекса $n \geqslant 0$.

Обозначим через $T(F)$ наименьший клое операций на A содержащий F. Операции из $T(F)$ называются *термовыми* относительно F. Операции из $T(F)$ получаются m F с помощью композиции, отождествления или перестановки аргументов, а также присоединением всех проекций.

Определение 1. *Пусть задана сигнатура F. Операция $f \in \mathcal{O}_n(A)$ называется* полиномиальной*, ели существует такая термовая операция $g \in \mathcal{O}_{n+m}(A)$ и элементы $a_1, \ldots, a_m \in A$ такие, что*

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, a_1, \ldots, a_m).$$

для всех $x_1, \ldots, x_n \in A$.

Клон $Pol(F)$ всех полиномиальных операций является наименьшим клоном, содержащим F и все нульарные операции.

Определение 2. *Алгебра A сигнатуры F is* полиномиально (функционально) полна*, если $\mathcal{O}(A) = Pol(F)$.*

Основным примпером полиномиально полных коммутативных ассоциативных колец является конечное поле.

Отображение π из F-алгебры A в F-алгебру B называется *гомоморфизмом*, для любого $n \geqslant 0$, любого $f \in F_n$ и любых элементов $a_1, \ldots, a_n \in A$ выполнено равенство

$$\pi\left(f(a_1, \ldots, a_n)\right) = f\left(\pi(a_1), \ldots, \pi(a_n)\right).$$

F-алгебра A *проста*, если люююй гомоморфизм из A в любюую F-алгебру либо инъективен, либо имеет одноэлементный образ.

3. Мальцевские операции

Тернарной мальцевской операцией m на множестве A называется тернарная операция, удовлетворяющая тождествам

$$m(x, x, y) = m(y, x, x) = y \tag{3}$$

Например, на любой группе существует тернарная мальцевская операция $m(x, y, z) = xy^{-1}z$. Обобщая эту ситуацию можно показать, что любая квазигруппа обладает тернарной мальцевской операцией.

F-алгебра A *аффинна*, если в A можно так ввести структуру аддитивной абелевой группы, что любая термовая операция $f \in F_n$ имеет вид $f(x_1, \ldots, x_n) = a_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n$, где $a_0 \in A$ и $\alpha_1, \ldots, \alpha_n$ — эндоморфизмы этой абелевой группы.

Теорема 1 ([1]). *Пусть A — конечная неодноэлементная алгебра. Следующие утверждения эквивалентны:*

(i) *A полиномиально полна;*

(ii) *существует полиномиальная мальцевская операция в A и алгебра A проста и неафинна.*

Теорема 2 ([2]). *Пусть Q — полиномиально полная конечная неодноэлементная алгебра. Тогда проблема существования решения систем полиномиальных уравнение в Q является NP-полной.*

4. Полиномиально полные квазигруппы

Наша цель использовать квазигруппы для защиты информации см, например, [7]. Пусть задан алфавит Q, на котором мы ввели структуру квазигруппы. Будем преобразовывать слова в этом алфавите, используя квазигрупповые операции. Для восстановления исходного сообщения необходимо решать системы полиномиальных уравнений. Теорема 2 показывает, что полиномиально полные квазигруппы подходят для наших целей.

Возникает проблема распознавания полиномиально полных квазигрупп по их заданию латинскими квадратами.

Нетрудно видеть, что аффинность квазигруппы Q означает, что на Q можно така задать структуру аддитивной абелевой группы с автоморфизмами α, β и элементом $c \in Q$, что умножение в Q имеет вид

$$xy = \alpha(x) + \beta(y) + c.$$

В теории квазигрупп такие квазигруппыв называются *T-квазигруппами*, [10].

Рассмотрим способ задание квазигруппы с помощью латинских квадратов. Пусть имеется квазигруппа $Q = \{x_1, \dots, x_n\}$ порядка n. Рассмотрим ее таблицу Кэли

$$\begin{array}{|c|ccc|} \hline & x_1 & \dots & x_n \\ \hline x_1 & a_{11} & \dots & a_{1n} \\ \vdots & \dots & \dots & \dots \\ x_n & a_{n1} & \dots & a_{nn} \\ \hline \end{array} \tag{4}$$

размера n, где у $a_{ij} = x_i x_j$ в Q. Из определения квазигруппы следует, что для всех $i, j = 1, \dots, n$

$$\sigma_i = \begin{pmatrix} x_1 & \dots & x_n \\ a_{i1} & \dots & a_{in} \end{pmatrix}, \quad \tau_j = \begin{pmatrix} x_1 & \dots & x_n \\ a_{1j} & \dots & a_{nj} \end{pmatrix} \tag{5}$$

являются перестановками элементов $x_1, \dots, x_n$.

Под *мультипликативной группой* $MultQ$ понимается подгруппа группы переставновок на Q, порождаемая

$$\sigma_1, \dots, \sigma_n, \quad \tau_1, \dots, \tau_n \tag{6}$$

Через $G(Q)$ обозначим подгруппу в $MultQ$, порождаемую всеми перестановками

$$\sigma_j \sigma_1^{-1}, \quad \tau_j \tau_1^{-1}, \quad i, j = 2, \dots, n. \tag{7}$$

Определение 3. *Две квазигруппы с умножениями $x \cdot y$, $x * y$, определенными на одном множестве Q* изотопны, *если существуют такие перестановки π, π_1, π_2 на Q , что для любых $x, y \in Q$ выполнено равенство $x * y = \pi^{-1}(\pi_1(x) \cdot \pi_2(y))$.*

В терминах латинского квадрата (4) это означает, что с помощью π_1 переставлояются строки, с помощью π_2 переставляются столбцы, а с помощью π переставляются элементы матрицы (a_{ij}).

Например, любая аффинная квазигруппа Q изотопна абелевой группе $\langle Q, + \rangle$

Непосредственно проверяеюся следующие теоремы.

Теорема 3. *При изотопии π,π_1,π_2 группа $G(Q)$ переходит в сопряженную группу $\pi G(Q) \pi^{-1}$.*

Квазигруппа Q по теореме Альберта изотопна группе Q'. Тогда $G(Q)$ сопряжена с группой $G(Q')$, которая в свою очередь совпадает с $MultQ'$.

Теорема 4. *Следующие условия эквивалентны:*

(i) *любые пары перестановок* $\sigma_i\sigma_1^{-1}$, $\tau_j\tau_1^{-1}$ *из* (7) *коммутируют между собой;*

(ii) Q *изотопна группе.*

Теорема 5. *Следующие условия эквивалентны:*

(i) *любая пара перестановок из* (7) *перестановочна;*

(ii) Q *изотопна абелевой группе;*

(iii) $G(Q)$ *является абелевой группой.*

(iv) Q *изотопна абелевой группе* $G(Q)$.

Поскольку любая квазигруппа, как отмпечалось, обладает термовым мальцевским термом, то справепдлива

Теорема 6. *Конечная квазигруппа полиномиально полна в том и только в том случае, если она проста и не аффинна.*

Отметим, что по [3, Теорема 2] диэдральные: симметрическин, альтернативные, общие линейные, проективные общие линейные группы, группы Матье M_{11}, M_{12} как группы перестановок множества Q реализуются как $Mult(Q)$ для некоторой структуры квазигруппы на Q.

В силу определения квазигруппы группа перестановок $Mult(Q)$ дей ствует в Q транзитивно.

Напомним необходимое определение. Пусть группа G действует транзитивно перестановками на множестве Q. *Стабилизатор* St_x точки $x \in Q$ состоит из всех таких $g \in G$, что $gx = x$. Группа G действует *примитивна*, если St_x является максимальной подгруппой в G. Приведем известный факт.

Теорема 7. *Квазигруппа* Q *проста в том и только в том случае, если* $MultQ$ *действует примитивно в* Q.

Ряд авторов выделяет еще одно свойство квазигрупп. Квазигруппа Q обладает *высокой неассоциативностью*, если $Mult(Q) = Sym(Q)$, [9].

Предложение 2. *Пусть квазигруппа* Q *порядка* $n > 3$ *обладает тем свойством, что* $Mult(Q)$ *действует дважды транзитивно в* Q. *Тогда* Q *полиномиально полна. В частности, квазигруппа с высокой неассоциативностью полиномиально полна.*

Если $G(Q)$ *действует дважды транзитивно в* Q, *то квазигруппа* Q *и все ее изотопы полиномиально полны.*

Теорема 8 ([6])**.** *Пусть конечная квазигруппа* Q *порядка* n *обладает тем свойством, что* $Mult(Q)$ *содержит группу, изоморфную* $\mathbf{A}_m$, *где*

$$m = \max\left(\left[\frac{n}{2}\right] + 1, 5\right). \tag{8}$$

Тогда Q *полиномиально полна.*

Предложение 3 ([5])**.** *Пусть квазигруппа* Q *имеет порядок* $|Q| \geqslant 5$. *Пусть существует элемент из* $Mult(Q)$ *с циклическим разложением, в который входит цикл простой длины* $p > \frac{|Q|}{2}$. *Толда квазигруппа* Q *проста и* $MultQ$ *содержит* $\mathbf{A}_n$, *если выполнено одно из следующих условий:*

(i) $|Q| \geqslant p+3$

(ii) $|Q| = p+2$ *и* $|Q|-1$ *не является степенью 2.*

Теорема 9 ([5])**.** *Пусть в латинском квадрате* (4) *группа* $G(Q)$ *обладает одним из следующих свойств* ($n = |Q|$)*:*

(i) $G(Q) \supseteq \mathbf{A}_n$;

(ii) $G(Q)$ *содержит подгруппу, изоморфную* $\mathbf{A}_m$, *где* m *из* (8).

Эти свойства сохраняются при изотопии.

Тройка элементов x, y, z из квазигруппы Q *ассоциативна*, если $(xy)z = x(yz)$.

Теорема 10 ([5])**.** *Если Q имеет порядок 4, то число ассоциативных троек не меньше 16. Если Q полиномиально полная квазигруппа порфдка 4, то число ассоциативных троек равно 16.*

5. Криптографические преобразования

Пусть $Q = \{x_1, \ldots, x_n\}$ — конечный алфавит и $Q^\dagger = \{x_1x_2\cdots x_t \mid x_i \in Q,\ t \geqslant 1\}$ — множество слов в этом алфавите, т.е. свободная полугруппа с базой A. Предположим, что в Q введена структура квазигруппы. Тогда множеством сообщений $\mathcal{M}$ является $\mathcal{C} = Q^\dagger$. Зафиксируем элемент $l \in Q$, который называется *лидером*, и определим элементарное преобразование $E_l : \mathcal{M} \to \mathcal{C}$ по правилу:

$$E_l(x_1x_s\cdots x_t) = y_1y_2\cdots y_t, \quad \forall M = x_1x_2\cdots x_t \in \mathcal{M} = Q^\dagger$$
$$\text{где } y_i = \begin{cases} l\cdot x_i, & i=1 \\ y_{i-1}\cdot x_i, & 2 \leqslant i \leqslant t). \end{cases}$$

Приведем пример применения элементарных преобразований для полиномиально полной квазигрппы порядка 4, заданной латинским квадратом (см. [5])

	1	2	3	4
1	2	1	3	4
2	4	3	1	2
3	3	2	4	1
4	1	4	2	3

.

Будем брать слова M, лидеры l и применять степени E_l^k. Получаем

$$M = 11111111111111111111, \quad l = 1; k = 5;$$
$$E_1^1(M) = C_1 = 24124124124124124124;$$
$$E_1^2(M) = C_2 = 14114114114114114114;$$
$$E_1^3(M) = C_3 = 22414122414122414122;$$
$$E_1^4(M) = C_4 = 11414111414111414111;$$
$$E_1^5(M) = C_5 = 24331241414124331241.$$

$$
\begin{aligned}
&M = 22222222222222222222, \quad l = 2; k = 5;\\
&E_2^1(M) = C_1 = 32323232323232323232;\\
&E_2^2(M) = C_2 = 11321132113211321132;\\
&E_2^3(M) = C_3 = 41324132413241324132;\\
&E_2^4(M) = C_4 = 24231211413224231211;\\
&E_2^5(M) = C_5 = 31133241413231133241.
\end{aligned}
$$

$$
\begin{aligned}
&M = 33333333333333333333, \quad l = 3; k = 5;\\
&E_3^1(M) = C_1 = 42134213421342134213;\\
&E_3^2(M) = C_2 = 11214413112144131121;\\
&E_3^3(M) = C_3 = 3324312124441433412 3;\\
&E_3^4(M) = C_4 = 42313324431221312342;\\
&E_3^5(M) = C_5 = 11334231424441332144.
\end{aligned}
$$

$$
\begin{aligned}
&M = 44444444444444444444, \quad l = 4; k = 5;\\
&E_4^1(M) = C_1 = 31431431431431431431;\\
&E_4^2(M) = C_2 = 24341424341424341424;\\
&E_4^3(M) = C_3 = 4343311422432214144;\\
&E_4^4(M) = C_4 = 34342414443444141434;\\
&E_4^5(M) = C_5 = 22144331434314141422.
\end{aligned}
$$

Видно, что происходят достаточно хорошие перемешивания элементов в преобразованном слове.

6. Конструкции полиномиально полных квазигрупп

Цель этого раздела — показать способы построения полиномиально полных квазигрупп достаточно большого размера.

Пусть заданы две квазигруппы K иQ. Через $\mathbf{S}_K, \mathbf{S}_Q$ обозначи группы перестановок на K, Q, соответственно. Предположим, что заданы отображения $\Phi, \Lambda, \Gamma : K \to \mathbf{S}_Q,\ \Psi, \Omega, \Theta : Q \to \mathbf{S}_K$ переводящие $a \in K$ в $\Phi_a, \Lambda_a, \Gamma_a \in \mathbf{S}_Q$ и $\alpha \in Q$ в $\Psi_\alpha, \Omega_\alpha, \Theta_\alpha \in \mathbf{S}_K$, соответственно. Зададим в $K \times Q$ новую операцию умножения по правилу

$$
(a, \alpha) * (b, \beta) = \left(\Psi_\alpha \left(\Omega_\alpha(a)\Theta_\alpha(b)\right),\ \Phi_b \left(\Lambda_b(\alpha)\Gamma_b(\beta)\right)\right), \tag{9}
$$

где $a, b \in K$ and $\alpha, \beta \in Q$. Непосредственно проверяется

Теорема 11. *Множество $K \times Q$ с умножением (9) является квазигруппой. Она называется бипроизведением (бискрещенным произведением) $K \bowtie Q$ квазигрупп K и Q.*

Теорема 12. *Пусть группы $G(K)$, $G(Q)$ действуют 2-транзитивно на K и на Q, соответственно. Предположим, что отображения Φ_u, Ψ_α не зависят от u и от α, соответственно. Пусть $|K| \leqslant (|Q|-1)!$ и $|Q| \leqslant (|K|-1)!$. Тогда существует $(|Q|-1)! \cdot (|K|-1)!$ вариантов для отображений $\Lambda, \Gamma, \Omega, \Theta$, для которых $G(K \bowtie Q)$ действует 2-транзитивно на $K \bowtie Q$. В частности, по предложению 2 в этих случаях бипроизведение $K \bowtie Q$ полиномиально полно.*

Рассмотрим пример 8-элементной квазигруппы K_3 с латинским квадратом

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

В ней

$$\sigma_2\sigma_1^{-1} = (1,2,3,4,5,6,7,8), \quad \sigma_2\sigma_2^{-1} = (2,3,1,6,7)(4,5,8).$$

Заметим, что $(\sigma_3\sigma_2^{-1})^5 = (4,5,8)^2$. Поэтому группа, порождаемая $\sigma_2\sigma_1^{-1}, \sigma_3\sigma_2^{-1}$ содержит $(4,5,8)$,и, следовательно,

$$(\sigma_2\sigma_2^{-1})(4,5,8)(\sigma_2\sigma_2^{-1})^{-1} = (6,7,2).$$

Кроме того, эта подгруппа содержит

$$(6,7,2)^{-1}(2,3,1,6,7) = (1,2,3).$$

Итак, рассматриваемая подгруппа содержит $(1,2,3,4,5,6,7,8)$ и $(1,2,3)$. Отсюда $G(K_3) = \mathbf{S}_8$.

Разберем пример 16-элементной квазигруппы K_4 с латинским квадратом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	1	6	7	8	9	10	11	12	13	14	15	16	5
3	3	1	2	6	7	8	9	10	11	12	13	14	15	16	5	4
4	4	5	6	7	8	9	10	11	12	13	14	15	16	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	1	4	3	2
6	6	7	8	9	10	11	12	13	14	15	16	5	2	3	4	1
7	7	8	9	10	11	12	13	14	15	16	2	3	4	5	1	6
8	8	9	10	11	12	13	14	15	16	5	4	1	3	2	6	7
9	9	10	11	12	13	14	15	16	4	3	1	2	5	6	7	8
10	10	11	12	13	14	15	16	5	1	2	3	4	6	7	8	9
11	11	12	13	14	15	16	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	5	4	3	2	1	6	7	8	9	10	11
13	13	14	15	16	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	5	4	3	2	1	6	7	8	9	10	11	12	13
15	15	16	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	4	5	3	2	1	6	7	8	9	10	11	12	13	14	15

Как и выше можно показать, что $G(K_4) = \mathbf{S}_{16}$. Применяя итеративно конструкцию бипроизведения $\bowtie$ к K_3, K_4 можно построить последовательность квазигрупп K_n of порядка 2^n для $n \geqslant 3$, $n \neq 5$, причем $G(K_n)$ действует 2-транзитивно в K_n. Таким образом, все построенные K_n iполиномиально полны.

Теорема 13 ([8]). *Счтеная квазигруппа порядка не менее 3 изотопна квазигруппе без подквазигрупп.*

Итак, можно построить сперию полиномиально полных квазигрупп Q любого порядка 2^n, $n \geqslant 3$, $n \neq 5$ с дважды транзитивной группой $G(Q)$. Беря изотоп приходим к квазигруппt, без подквазигрупп, но свойство 2-транзитивности сохраняется. Тем самым получаем требуюмую серию квазигрупп.

Приведем еще серии полиномиально полных полных квазигрупп.

Теорема 14. *Пусть p — простое число и $q = p^r$. Пусть $m \notin \{1, p, \dots, p^{r-1}\} \mod (q-1)$ и β — полрождающий мультипликативной циклической группы $\mathbb{F}_q^*$. Предположим, что $1 < m < q-1$ взаимно просто в $q-1$. Тогда найдется такой элемент $c \in \mathbb{F}_p^*$, что $Q = \mathbb{F}_p$ с умножением*

$$x * y = (1-\beta)x^m + \beta y + c$$

не имеет подквазигрупп и полиномиально полно.

Теорема 15. *Пусть квазигруппа Q имеет простой порядок и не имеет подквазигрупп. Если ее группа автоморфизмов нетривиальна, то Q аффинна. Если Q полиномиально полна, то любая операция в Q является термовой относительно умножения, взятия левого и правого обратных.*

Рассмотрим связь с тернарными полиномиально полными квазигруппами. Пусть Q — тернарная квазигруппа с умножением xyz. Если зафиксировать одну переменную, то получается полиномиальная бинарная квазигруппа of Q, называемая редуктом.

Теорема 16. *Пусть L — конечная квазигруппа порядка $n \geqslant 3$, причем $G(L) \supseteq \mathbf{A}_n$. Тогда существует такая тернарная квазигруппа Q, что один из ее редуктов равен L и группа G любого редукта Q содержит $\mathbf{A}_n$.*

Теорема 17 (В.Т.Марков). *Пусть $\sigma \in \mathbf{S}_n$ — нетождественная перестановка степени n. Тогда сущетсвует высоко неассоциативная квазигруппа порядка n, такая, что первая строка ее латинского квадрата равна σ. Эта квазигруппа проста при любом n и полиномиально полна, если $n \geq 5$.*

Теорема 18 (В.Т.Марков). *Пусть Q — конечная квазигруппа порядка $|Q| = k \geq 1$ и p наименьшее простое нечетное число с условием $p > k$ (если $p = 3$, то $k = 1$, в противном случае $p < 2k$ по теореме Чебышева). Тогда для любого $n \geq 2k + p$ существует такая квазигруппа R, $|R| = n$, $R \supseteq Q$ и $Mult(R) = \mathbf{S}_n$.*

7. Заключение

В разделе 4 приведены достаточные условия полиномиальной полноты Q в терминах дважды транзитивности действия группы $G(Q)$. В терминах этой же группы дан ответ на вопрос, когда квазигруппа изотопна (абелевой) группе.

В разделе 5 приведены примеры криптографических преобразований на основе квазигрупп и влияние на них полиномиальной полноты.

В разделе 6 приведены способы построения полиномиально полных квазигрупп достаточно большого порядка.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

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

2. G. Horvath, C. L. Nehaniv, Cs. Szabo. An assertion concerning functionally complete algebras and NP-completeness. Theoret. Comput. Sci., 407:591–595, 2008.

3. Ihringer T.: On multiplication groups of quasigroups, European J. Combin. 5, 1984, 137-141.

4. V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S. K. Pal, On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts, Quasigroups and related systems, 21 (2013), 201-214.

5. V.A. Artamonov, S. Chakrabarti, S. K. Pal, Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations, Discrete Applied Mathematics (2016), pp. 5-17

6. V.A. Artamonov , S. Chakrabarti, S.K. Pal, Characterizations of highly non-associative quasigroups and associative triples, Quasigroups and related systems, 25(2017) 1-19.

7. M.M. Glukhov, On applications of quasigroups in cryptography, Appl. Discrete Math. 2(2008), 28-32.

8. Kepka T., A note on simple quasigroups. Acta Univ. Carolin. Math. Phys., 19(2):59–60, 1978.

9. Otokar Grošek, Peter Horák, On quasigroups with few associative triples, Des. Codes Cryptogr. (2012), 64, 221–227.

10. Belyavskaya G.B., Tabarov A.H. A characterization of linear and a linear quasigroups, Discrete Math., 4(1992), N 2, 142-147.

REFERENCES

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

2. Horvath, G. Nehaniv, C.L. Szabo, Cs., 2008, "An assertion concerning functionally complete algebras and NP-completeness". *Theoret. Comput. Sci.*, vol. 407, pp. 591–595.

3. Ihringer T., 1984, On multiplication groups of quasigroups, *European J. Combin.* vol 5, pp. 137-141.

4. Artamonov, V.A. Chakrabarti, S. Gangopadhyay, S. Pal, S. K., 2013, "On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts *Quasigroups and related systems,* vol. 21, pp. 201-214.

5. [2016] Artamonov, V.A. Chakrabarti, S. Pal, S.K. 2016, "Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations *Discrete Applied Mathematics* vol. 200, pp. 5-17

6. [2017] Artamonov, V.A. Chakrabarti, S. Pal, S.K. 2017, "Characterizations of highly non-associative quasigroups and associative triples *Quasigroups and related systems*, vol. 25, pp. 1-19.

7. Glukhov,M.M., 1978, "On applications of quasigroups in cryptography *Appl. Discrete Math.* vol. 2, pp. 28-32.

8. Kepka T., 1978, "A note on simple quasigroups". *Acta Univ. Carolin. Math. Phys.* vol. 19, no. 2, pp. 59–60.

9. Grošek, Otokar Peter Horák, Peter, 2012, "On quasigroups with few associative triples *Des. Codes Cryptogr.*, vol. 64, pp. 221–227.

10. Belyavskaya G.B., Tabarov A.H. 1992, "A characterization of linear and a linear quasigroups *Discrete Math.*, vol. 4, no 2, pp. 142-147.

Получено 12.06.2018
Принято в печать 17.08.2018