APPLICATIONS OF QUASIGROUPS TO CRYPTOGRAPHY

V.A. ARTAMONOV

Dedicated to Professor Mirjana Vuković on the occasion of her 70th birthday

ABSTRACT. The present paper contains a survey of some recent results on polynomially (functionally) complete quasigroups and their application obtained by joint Indo-Russian research group: S. Chakrabarti, S. Gangopadhyay, S. K. Pal, V.T.Markov.

1. INTRODUCTION

Finite quasigroups have important applications in the development of crypto-primitives and cryptographic schemes [15, 8, 8, 10, 17]. Crypto-transformations in these schemes are based on quasigroup operations. So the inverse transformations are reduced to solutions of equations in the language of quasigroups. The most suitable class for these purposes are polynomially complete quasigroups in which the problem solution of equations is NP-complete. So the usage of the mentioned quasigroups presents new perspectives of cryptography and information security. From algebraic point of view polynomial completeness is one of the most important characteristic for cryptographically suitable quasigroups because by Theorem 3.5 it coincides with the class of simple non-affine quasigroups.

In this paper in § 5 we expose different methods to construct polynomially complete quasigroups of any order $n \geq 5$.

For our purposes we also consider quasigroups with no proper subquasigroups. This problem is mentioned in § 5.

The paper is based on results of a joint project foundations RFBR (Russia) and DCT (India).

The paper is organized is follows. In § 2 we expose some basic facts and notions from universal algebra. § 3 shows applications of results from previous section and

2010 Mathematics Subject Classification. 08A30; 20B15; 20B20.

Key words and phrases. universal algebra, quasigroups, Latin squares, polynomial completeness.

Partially supported by NIR AAAA-A16-116070810025-5

This paper was presented at the International Scientific Conference Modern Algebra and Analysis and their Applications, ANUBiH - Sarajevo, September 20 - 22, 2018.
from permutation group theory to classification of polynomially complete quasigroups. § 4 discusses cryptographic transformation based of polynomially complete quasigroups. In the last section we consider constructions of polynomially complete quasigroups of sufficiently large order.

All necessary definition and results related to quasigroups can be found in [5, 7, 21, 20]

2. Systems of operations

For be a nonempty set $A$ denote by $A^n$, $n \geq 0$, the $n$th direct power of the set $A$. In particular if $n = 0$ then $A^0$ denote the one-element set $\{\ast\}$.

$n$-ary algebraic operation on $A$ is a map $f : A^n \rightarrow A$. In particular a nullary operation $f : \{\ast\} = A^0 \rightarrow A$ fixes an element $f(\ast) \in A$.

Denote by $O_n(A)$ the set of all $n$-ary algebraic operations in $A$ and by $O(A)$ the collection of all $\{O_n(A) \mid n \geq 0\}$.

Consider a family of sets $F = \{F_n \mid n \geq 0\}$ which we call a signature. A nonempty set $A$ is an algebra of a signature $F$ or an $F$-algebra if there exists a map $\alpha : F \rightarrow O(A)$ such that $\alpha(F_n) \subseteq O_n(A)$. It means that each $f \in F_n$ is realized via $\alpha$ as an $n$-ary operation in $A$.

For example a quasigroup is a set $Q$ with a multiplication $xy$ such that for any $a,b \in Q$ each of the equations $ax = b$, $ya = b$ have unique solutions which are denoted by $a \setminus b$, and by $a / b$, respectively. So a quasigroup can be considered as an algebra with three binary operations.

If $f \in O_n(A)$ and $g_1,\ldots,g_n \in O_m(A)$ then one can define a composition (superposition) $f(g_1,\ldots,g_n) \in O_m(A)$ by the rule

\[
[f(g_1,\ldots,g_n)](x_1,\ldots,x_m) = f(g_1(x_1,\ldots,x_m),\ldots,g_n(x_1,\ldots,x_m)) \tag{2.1}
\]

for all $x_1,\ldots,x_m \in A$.

The composition satisfies the superassociativity law

\[
[f(g_1,\ldots,g_n)](h_1,\ldots,h_m) = f(g_1(h_1,\ldots,h_m),\ldots,g_n(h_1,\ldots,h_m)) \tag{2.2}
\]

for all $f \in O_n(A)$, $g_1,\ldots,g_n \in O_m(A)$, $h_1,\ldots,h_m \in O_r(A)$.

Observe that if the operations $g_1,\ldots,g_n$ in (2.1) are nullary, then

\[
[f(g_1,\ldots,g_n)](\ast) = f(a_1,\ldots,a_n)
\]

is an evaluation of $f$ at the $n$-tuple $(a_1,\ldots,a_n)$.

The family $O(A)$ is also provided with special operations of projections

\[
p_{in}(x_1,\ldots,x_n) = x_i.
\]

It is easy to check that if $f \in O_n(A)$ and $f_1,\ldots,f_n \in O_m(A)$ then

\[
f = f(p_{1n},\ldots,p_{mn}), \quad p_{in}(f_1,\ldots,f_n) = f_i. \tag{2.3}
\]
2.1. Clones

A family \( C = \{ C_n \subseteq O_n(A) \mid n \geq 0 \} \) is a clone of operations on \( A \) if \( C \) contains all projections and it is closed under composition. It means that if \( f, g_1, \ldots, g_n \in C \), then \( f(g_1, \ldots, g_n) \in C \).

**Proposition 2.1.** Let \( f \in C_n \) and an operation \( g \) is obtained from \( f \) by any change of variables. Then \( g \in C \).

**Proof.** Take variables \( x_{i_1}, \ldots, x_{i_n} \), where \( 1 \leq i_1, \ldots, i_n \leq m \). Then \( f(x_{i_1}, \ldots, x_{i_n}) = f(p_{i_1m}, \ldots, p_{i_nm})(x_1, \ldots, x_m) \).

**Definition 2.2.** An abstract clone is a collection of sets \( C = \{ C_n \mid n \geq 0 \} \) with an operation of composition \( f(g_1, \ldots, g_n) \in C_m \) for all \( f \in C_n \) and \( g_1, \ldots, g_n \in C_n \). Also for all \( 1 \leq i \leq n \) there exist elements \( p_{i_in} \in C_n \) such that (2.2), (2.3) hold.

Each clone is provided with a system of maps \( \Psi_{mn} : C_n \rightarrow C_m \), \( m \geq n \), where \( \Psi_{mn}(f) = f(p_{1m}, \ldots, p_{nm}) \) for any \( f \in C_n \). For a clone of operations it means that \( n \)-ary operation \( f \) can considered as \( m \)-ary operation which does not depend on the last \( m - n \) variables.

**Proposition 2.3.** For any integers \( d \geq m \geq n \) we have \( \Psi_{dn} \Psi_{mn} = \Psi_{dn}, \Psi_{nn} = 1 \).

**Proof.** Let \( f \in C_n \). By (2.3) and (2.2) we get
\[
\Psi_{dn} \Psi_{mn}(f) = f(p_{1m}, \ldots, p_{nm})(p_{1d}, \ldots, p_{md}) = f(p_{1d}, \ldots, p_{md}) = \Psi_{dn}(f).
\]

**Proposition 2.4.** Let \( f \in C_n \) and \( g_1, \ldots, g_n \in C_m \). If \( d \geq \max(n, m) \) then
\[
\Psi_{dm}[f(g_1, \ldots, g_n)] = f(\Psi_{dm}(g_1), \ldots, \Psi_{dm}(g_n)). \tag{2.4}
\]

**Proof.** By (2.3) and (2.2) we get
\[
\Psi_{dm}[f(g_1, \ldots, g_n)] = [f(g_1, \ldots, g_n)](p_{1d}, \ldots, p_{md}) = f(g_1(p_{1d}, \ldots, p_{md}), \ldots, g_n(p_{1d}, \ldots, p_{md})) = f(\Psi_{dm}(g_1), \ldots, \Psi_{dm}(g_n)).
\]

Denote by \( A \) the limit of the diagram \( \{ C_n, \Psi_{mn} \mid m \geq n \} \) in the category of sets. In other words \( A \) can be considered as a factor of the disjoint union of all \( C_n, n \geq 0 \) factorized by binary relation \( f \equiv \Psi_{nn}(f), m \geq n \), where \( f \in C_n \).

**Proposition 2.5.** Let \( f \in C_n \) and \( g_1, \ldots, g_n \in C_m \). If \( d \geq m \) then
\[
f(g_1, \ldots, g_n) \equiv f(\Psi_{dm}(g_1), \ldots, \Psi_{dm}(g_n)).
\]

**Proof.** We have
\[
f(\Psi_{dm}(g_1), \ldots, \Psi_{dm}(g_n)) = f(g_1(p_{1d}, \ldots, p_{md}), \ldots, g_n(p_{1d}, \ldots, p_{md})) = f(g_1, \ldots, g_n)(p_{1d}, \ldots, p_{md}) = \Psi_{dm}(f(g_1, \ldots, g_n)) \equiv f(g_1, \ldots, g_n).
\]
Theorem 2.6. Let \( C \) be an abstract clone. Then it is isomorphic to some clone of operations.

Proof. Let \( A \) be as above. We shall represent \( C \) by functions in \( A \). Let \( f \in C_n, n \geq 0 \). Suppose that \( g_i \in C_{k_i}, 1 \leq i \leq n \) and \( d \geq \max(k_1, \ldots, k_n) \). Set

\[
f * (g_1, \ldots, g_n) = f (\Psi_{d k_1}(g_1), \ldots, \Psi_{d k_n}(g_n)).
\]

(2.5)

By Proposition 2.5 the action (2.5) is correct.

In particular

\[
p_m * (g_1, \ldots, g_n) = p_m (\Psi_{d k_1}(g_1), \ldots, \Psi_{d k_n}(g_n)) = \Psi_{m k_i}(g_i) \equiv g_i.
\]

Moreover if \( f \in C_n \) and \( g_i \in C_{m_i}, h_j \in C_{s_j}, 1 \leq i \leq n, 1 \leq j \leq m \), then for \( d \geq \max(m_i, s_j) \) by (2.5) we have

\[
[f * (g_1, \ldots, g_n)] * (h_1, \ldots, h_m) \equiv \Psi_{d s_1}(h_1), \ldots, \Psi_{d s_m}(h_m)
\]

\[
f[g_1 (\Psi_{d s_1}(h_1), \ldots, \Psi_{d s_m}(h_m)), \ldots, g_n (\Psi_{d s_1}(h_1), \ldots, \Psi_{d s_m}(h_m))] \equiv
\]

\[
f [g_1 * (h_1, \ldots, h_m), \ldots, g_n * (h_1, \ldots, h_m)].
\]

It means that the action (2.5) is compatible with superpositions.

Finally we have to show that the action is faithful. In fact let \( f * (g_1, \ldots, g_n) = h * (g_1, \ldots, g_n) \) for all \( g_i \). Taking \( g_i = p_{m_i} \) we obtain that \( f = h \).

\[\square\]

2.2. Term and polynomial clones of operations

Let \( F = \{F_n \mid n \geq 0\} \) be a signature and a nonempty set \( A \) an \( F \)-algebra. Without loss of generality we can assume that \( F_n \subseteq O_n(A) \) for an any index \( n \geq 0 \).

Denote by \( T(F) \) the least clone of operations on \( A \) containing \( F \). Operations from \( T(F) \) are called term operations in the signature \( F \).

Operations from \( T(F) \) are obtained from \( F \) by compositions, identifications and changes of variables and by adding all projections.

Definition 2.7. Let \( F \) be a signature. An operation \( f \in O_n(A) \) is polynomial if there exist a term operation \( g \in O_{n+m}(A) \) and elements \( a_1, \ldots, a_m \in A \) such that \( f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, a_1, \ldots, a_m) \) for all \( x_1, \ldots, x_n \in A \).

A clone \( \text{Pol}(F) \) of all polynomial operations is the least clone containing \( F \) and all nullary operations. It is obtained from \( F \) by adding all nullary opertations, all projections and all their compositions.

Definition 2.8. An algebra \( A \) of a signature \( F \) is polynomially (functionally) complete if \( O(A) = \text{Pol}(F) \).

For example a commutative associative ring \( A \) with a unit element is polynomially complete if for any \( n \) every \( n \)-are operation \( f \) on \( A \) is a polynomial with coefficients in \( A \).
The main example of polynomially complete commutative associative ring is a finite field.

A map $\pi$ from a $F$-algebra $A$ to $F$-algebra $B$ is a homomorphism if it is compatible with operations from $F$. It means that $\pi(f(a_1, \ldots, a_n)) = f(\pi(a_1), \ldots, \pi(a_n))$, for any $n \geq 0$, any $f \in F_n$ and any elements $a_1, \ldots, a_n \in A$. $F$-algebra $A$ is simple if any homomorphism from $A$ to any $F$-algebra $B$ is either injective or has one-element image.

2.3. Malcev operations

A Malcev ternary operation $m$ on a set $A$ is a ternary operation satisfying the identities $m(x, x, y) = m(y, x, x) = y$. For example in any group there exists a Malcev term operation $m (x, y, z) = xy^{-1}z$.

Each quasigroup has a term Malcev operation [6, Chapter VII.3]

An $F$-algebra $A$ is affine if $A$ is equipped with a structure of an additive Abelian group such that each term operation $f \in F_n$ has the form $f(x_1, \ldots, x_n) = a_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n$, where $a_0 \in A$ and $\alpha_1, \ldots, \alpha_n$ are group endomorphisms.

**Theorem 2.9** ([11]). Let $A$ be a finite algebra containing at least two elements. The following are equivalent:

(i) $A$ is polynomially complete;

(ii) there exists a polynomial Malcev operation in $A$ and the algebra $A$ is simple and non-affine.

**Theorem 2.10** ([12]). Let $Q$ be a polynomially complete finite algebra or order at least 2. Then the problem of a solution of systems of polynomial equations in $Q$ in $NP$-complete.

3. Polynomially complete quasigroups

Our aim is to use quasigroups for security of information. Suppose that we have an alphabet $Q$ which has a structure of a quasigroup. Then one can make some transformation of a word in $Q$ using quasigroup operations. For example we have an element $x$ of a quasigroup $Q$. Then we transform it into an element $xy \in Q$ for some key element $y$.

If someone knows the message $xy$ and a key $y$ he can find the inverse transformation and find the original message $x$.

Theorem 2.10 shows that polynomially complete quasigroups are suitable for our purposes.

Now we shall consider a problem of recognition of polynomial completeness of a quasigroup given by its Latin square.

If $Q$ is an additive abelian group with automorphisms $\alpha, \beta$ and $c \in Q$, then $Q$ with an operation $xy = \alpha(x) + \beta(y) + c$ is a quasigroup. It is called affine or $T$-quasigroup.
Each finite quasigroup $Q = \{x_1, \ldots, x_n\}$ of order $n$ can be given by its Cayley table. This is a square matrix of size $n$ of size $n$, where an entry $a_{ij}$ stands for the product $x_i x_j$ in the quasigroup $Q$. From the definition of a quasigroup it follows that for any $i, j = 1, \ldots, n$

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

are permutations of elements $x_1, \ldots, x_n$. Hence the square (3.1) is a Latin square.

**Definition 3.1.** Multiplication group $\text{Mult} Q$ is the subgroup of permutations in $Q$ generated by $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_n$. $G(Q)$ is the subgroup of $\text{Mult} Q$ generated by permutations

$$\sigma_j \sigma_i^{-1}, \quad \tau_j \tau_i^{-1}, \quad i, j = 2, \ldots, n.$$  

Two quasigroups multiplication $x \cdot y$, $x * y$ defined on the set $Q$ are isotopic if there exist permutations $\pi, \pi_1, \pi_2$ on $Q$ such that for any $x, y \in Q$ we have

$$x * y = \pi^{-1}(\pi_1(x) \cdot \pi_2(y)).$$

In terms of a Latin square (3.1) it means that we permute rows by $\pi_1$, permute columns by $\pi_2$ and then permute entries of the matrix $(a_{ij})$ by $\pi$.

In particular any affine quasigroup $Q$ is isotopic to the abelian group $(Q, +)$.

**Theorem 3.2** ([3]). Under an isotopy $\pi, \pi_1, \pi_2$ the group $G(Q)$ is mapping to $\pi G(Q) \pi^{-1}$.

A quasigroup $Q$ by [1] is isotopic to a loop $Q'$. Then $G(Q)$ is conjugate to the group $G(Q')$ which coincides with $\text{Mult} Q'$.

**Theorem 3.3** ([4]). The following conditions are equivalent:

(i) any pair of permutations $\sigma_i \sigma_i^{-1}, \tau_j \tau_j^{-1}$ from (3.3) commute between themselves;

(ii) $Q$ is isotopic to a group.

**Theorem 3.4** ([4]). The following conditions are equivalent:

(i) any pair of permutations from (3.3) commute;

(ii) $Q$ is isotopic to an abelian group;

(iii) $G(Q)$ is an abelian group;

(iv) $Q$ is isotopic to the abelian group $G(Q)$.

Similar results were obtained in [14].

Since any quasigroup admits Malcev term, we have
**Theorem 3.5** ([11]). A finite quasigroup is polynomially complete if and only if it is simple and non-affine.

By [13] dihedral, symmetric, alternating, general linear, projective general linear groups as well as Mathieu groups $M_{11}, M_{12}$ can occur as $\text{Mult}(Q)$ for some quasigroup $Q$.

It follows from the definition of a quasigroups that the group $\text{Mult}(Q)$ acts transitively on $Q$.

**Definition 3.6.** Let $G$ be a group acting transitively by permutations on the set $Q$. A stabilizer $\text{St}_x$ of an element $x \in Q$ is the set of all $g \in G$ such that $gx = x$. The group $G$ is primitive if $\text{St}_x$ is a maximal subgroup in $G$.

The next results follows immediately from a definition of a congruence.

**Theorem 3.7.** A quasigroup $Q$ is simple if and only if $\text{Mult}(Q)$ is a primitive permutation group on $Q$.

A quasigroup $Q$ is highly non-associative if $\text{Mult}(Q) = \text{Sym}(Q)$.

**Proposition 3.8** ([4]). Let $Q$ be a quasigroup of order $n > 3$ such that $\text{Mult}(Q)$ is a doubly transitive permutation group on $Q$. Then $Q$ is polynomially complete.

**Theorem 3.9** ([4]). Let $Q$ be a finite quasigroup of order $n$ such that $\text{Mult}(Q)$ contains a subgroup isomorphic to an alternative subgroup $A_m$, where

$$m = \max \left( \left\lfloor \frac{n}{2} \right\rfloor + 1, 5 \right).$$

Then $Q$ is polynomially complete. In particular a highly non-associative quasigroup of order $n \geq 5$ is polynomially complete.

**Proposition 3.10** ([4]). Let $Q$ be a quasigroup of order $|Q| \geq 5$. Suppose that there exists an element of $\text{Mult}(Q)$ with a cycle decomposition containing a cycle of prime length $p > \sqrt{|Q|}$. Then $Q$ is simple and $\text{Mult}(Q)$ contains $A_n$ if one of the following conditions is satisfied:

(i) $|Q| \geq p + 3$;
(ii) $|Q| = p + 2$ and $|Q| - 1$ is not a power of 2.

**Theorem 3.11** ([4]). If in the Latin square (3.1) the group $G(Q)$ yields one of the properties ($n = |Q|$):

(i) $G(Q) \supset A_n$;
(ii) $G(Q)$ contains a subgroup isomorphic to $A_m$ where $m$ is from (3.4);

then this property is preserved under isotopy.

A triple $x, y, z$ of elements of a quasigroup $Q$ is associative if $(xy)z = x(yz)$. 

---

**APPLICA TIONS OF QUASIGROUPS TO CRYPTOGRAPHY 197**

**Theorem 3.5** ([11]). A finite quasigroup is polynomially complete if and only if it is simple and non-affine.

By [13] dihedral, symmetric, alternating, general linear, projective general linear groups as well as Mathieu groups $M_{11}, M_{12}$ can occur as $\text{Mult}(Q)$ for some quasigroup $Q$.

It follows from the definition of a quasigroups that the group $\text{Mult}(Q)$ acts transitively on $Q$.

**Definition 3.6.** Let $G$ be a group acting transitively by permutations on the set $Q$. A stabilizer $\text{St}_x$ of an element $x \in Q$ is the set of all $g \in G$ such that $gx = x$. The group $G$ is primitive if $\text{St}_x$ is a maximal subgroup in $G$.

The next results follows immediately from a definition of a congruence.

**Theorem 3.7.** A quasigroup $Q$ is simple if and only if $\text{Mult}(Q)$ is a primitive permutation group on $Q$.

A quasigroup $Q$ is highly non-associative if $\text{Mult}(Q) = \text{Sym}(Q)$.

**Proposition 3.8** ([4]). Let $Q$ be a quasigroup of order $n > 3$ such that $\text{Mult}(Q)$ is a doubly transitive permutation group on $Q$. Then $Q$ is polynomially complete.

**Theorem 3.9** ([4]). Let $Q$ be a finite quasigroup of order $n$ such that $\text{Mult}(Q)$ contains a subgroup isomorphic to an alternative subgroup $A_m$, where

$$m = \max \left( \left\lfloor \frac{n}{2} \right\rfloor + 1, 5 \right).$$

Then $Q$ is polynomially complete. In particular a highly non-associative quasigroup of order $n \geq 5$ is polynomially complete.

**Proposition 3.10** ([4]). Let $Q$ be a quasigroup of order $|Q| \geq 5$. Suppose that there exists an element of $\text{Mult}(Q)$ with a cycle decomposition containing a cycle of prime length $p > \sqrt{|Q|}$. Then $Q$ is simple and $\text{Mult}(Q)$ contains $A_n$ if one of the following conditions is satisfied:

(i) $|Q| \geq p + 3$;
(ii) $|Q| = p + 2$ and $|Q| - 1$ is not a power of 2.

**Theorem 3.11** ([4]). If in the Latin square (3.1) the group $G(Q)$ yields one of the properties ($n = |Q|$):

(i) $G(Q) \supset A_n$;
(ii) $G(Q)$ contains a subgroup isomorphic to $A_m$ where $m$ is from (3.4);

then this property is preserved under isotopy.

A triple $x, y, z$ of elements of a quasigroup $Q$ is associative if $(xy)z = x(yz)$.
Theorem 3.12 ([16]). If \(Q\) is a quasigroup of order 4, then the number of associative triples is at least 16. If \(Q\) is a polynomially complete quasigroup of order 4, then the number of associative triples in \(Q\) is equal to 16.

If \(Q\) is non-simple then the number of associative triples is at least 24.

4. CRYPTOGRAPHIC TRANSFORMATIONS

In this section we consider an example of cryptosystem based on quasigroups which is due to S. Markovsky, see for example [19].

Let \(Q = \{x_1, \ldots, x_n\}\) be a finite set (alphabet) and denote by \(Q^t = \{x_1x_2\cdots x_t \mid x_i \in Q, t \geq 1\}\) the set of all finite strings over \(Q\). Consider a quasigroup \((Q, \cdot)\) and message space \(\mathcal{M} = \text{crypt space} \ C = Q^t\). For each fixed element \(l \in Q\), define an encryption transformation \(E_l : \mathcal{M} \to C\) as follows:

\[
E_l(x_1x_2\cdots x_t) = y_1y_2\cdots y_t, \quad \forall M = x_1x_2\cdots x_t \in \mathcal{M} = Q^t,
\]

where \(y_i = \begin{cases} l \cdot x_i, & i = 1, \\ y_{i-1} \cdot x_i, & 2 \leq i \leq t. \end{cases}\)

We compared results of an action of encryption transformation of a constant string using polynomially complete quasigroups and non-polynomially complete ones. From statistical point of view transformations given by polynomially complete quasigroups looks better. Here we present some experiments from [2].

4.1. Experiment 1.

Consider the quasigroup \((Q, \cdot)\) which is non-simple and non-affine (not polynomially complete) whose Latin square is as follows

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Some of the outcomes of \(e\)-transformation are presented here to show the effect of choice of the quasigroup

\[
M = 2222222222222222222222; \quad l = 1; k = 5;
\]

\[
E_1^1(M) = c_1 = 111111111111111111; \]

\[
E_1^2(M) = c_2 = 2341234123412341; \]

\[
E_1^3(M) = c_3 = 1441441144114411441; \]

\[
E_1^4(M) = c_4 = 22244441222444412223; \]

\[
E_1^5(M) = c_5 = 114444111144441114. \]
\[ M = 22222222222222222222, \quad l = 2; k = 5; \]
\[ E_1^2 (M) = C_1 = 42424242424242424242; \]
\[ E_2^2 (M) = C_2 = 24422442244224422442; \]
\[ E_3^2 (M) = C_3 = 44424442444244424442; \]
\[ E_4^2 (M) = C_4 = 22244442222444422224; \]
\[ E_5^2 (M) = C_5 = 42444442444442442442. \]

\[ M = 22222222222222222222, \quad l = 3; k = 5; \]
\[ E_1^3 (M) = C_1 = 33333333333333333333; \]
\[ E_2^3 (M) = C_2 = 21432143214321432143; \]
\[ E_3^3 (M) = C_3 = 34433443344334433443; \]
\[ E_4^3 (M) = C_4 = 22214443222144432221; \]
\[ E_5^3 (M) = C_5 = 33344443333444333334. \]

\[ M = 22222222222222222222, \quad l = 4; k = 5; \]
\[ E_1^4 (M) = C_1 = 24242424242424242424; \]
\[ E_2^4 (M) = C_2 = 22442244224422442244; \]
\[ E_3^4 (M) = C_3 = 24424442444244424442; \]
\[ E_4^4 (M) = C_4 = 22244442222444422224; \]
\[ E_5^4 (M) = C_5 = 24444442444442444244. \]

\[ M = 24242424242424242424, \quad l = 2; k = 5; \]
\[ E_1^2 (M) = C_1 = 44224422442244224422; \]
\[ E_2^2 (M) = C_2 = 22422422222442222422; \]
\[ E_3^2 (M) = C_3 = 42244422424242424242; \]
\[ E_4^2 (M) = C_4 = 24244422424442242422; \]
\[ E_5^2 (M) = C_5 = 44244442444442444244. \]
It is observed that for this class if messages (plaintexts) consist of elements of unit class of factor quasigroups then ciphertexts of all rounds of e-transformation consist of the same set of elements under two leaders viz. elements of unit class (case (a), (c), (d)). This may turn out to be a weakness as it generates unbalanced cipher texts for all rounds. This might also help the cryptanalyst to find out the algebraic structure of quasigroup used for encryption based on input-output pairs.

4.2. Experiment 2.

Consider the quasigroup \((Q, \cdot)\) which is simple & non-affine (polynomially complete) whose Latin square is shown below

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

\[ M = \begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array} \]

\( l = 1; k = 5; \)

\[ E_1^1(M) = C_1 = 24124124124124124124; \]

\[ E_1^2(M) = C_2 = 14114114114114114114; \]

\[ E_1^3(M) = C_3 = 22414122414122414122; \]

\[ E_1^4(M) = C_4 = 11414111414114141411; \]

\[ E_1^5(M) = C_5 = 24331241414124331241. \]

\[ M = \begin{array}{cccc}
2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 \\
\end{array} \]

\( l = 2; k = 5; \)

\[ E_2^1(M) = C_1 = 32323232323232323232; \]

\[ E_2^2(M) = C_2 = 11321132113211321132; \]

\[ E_2^3(M) = C_3 = 41324132413241324132; \]

\[ E_2^4(M) = C_4 = 24231211413224231211; \]

\[ E_2^5(M) = C_5 = 31133241413231133241. \]
$M = 33333333333333333333, \quad l = 3; k = 5;
E_1^3(M) = C_1 = 42134213421342134213;
E_2^3(M) = C_2 = 11214413112144131121;
E_3^3(M) = C_3 = 332431214414334123;
E_4^3(M) = C_4 = 42313324431221312342;
E_5^3(M) = C_5 = 11334231424441332144.$

$M = 44444444444444444444, \quad l = 4; k = 5;
E_1^4(M) = C_1 = 31431431431431431431;
E_2^4(M) = C_2 = 243412434124341242;
E_3^4(M) = C_3 = 434311422432214144;
E_4^4(M) = C_4 = 343421444441414434;
E_5^4(M) = C_5 = 22144331434314141422.$

In this case, it is observed that there is no leader for which ciphertexts (of all rounds) for any type of message under $e$-transformation consist of same one or two elements only. These are not unbalanced for all rounds. It is due to the fact that there is no non-trivial congruence classes of quasigroup. So it shows the polynomially complete class is most suitable for cryptographic applications from algebraic point of view.

The weakness observed in Experiment-1 can be overcome either by choosing initially the quasigroup from polynomially complete class or applying cryptographic transformation (viz. $e$-transformation) on isotope belonging to polynomially complete class. In the later case we can construct isotopies [Theorem 4, Cor 2] under which the isotopes belong to the above mentioned class, the algebraically most suitable class.

5. Constructions of Polynomially Complete Quasigroups of Large Order

In this section we give some methods of construction of polynomially complete quasigroups of sufficiently large order.

Let $K$ and $Q$ are two quasigroups and $S_K, S_Q$ permutations group of the sets $K, Q$, respectively. Suppose that there are given maps $\Phi, \Lambda, \Gamma : K \to S_Q, \Psi, \Omega, \Theta : Q \to S_K$ sending $a \in K$ to $\Phi(a), \Lambda(a), \Gamma(a) \in S_Q$ and $\alpha \in Q$ to $\Psi(\alpha), \Omega(\alpha), \Theta(\alpha) \in S_K$, respectively. Define in $K \times Q$ new operation of multiplication

$$ (a, \alpha) \ast (b, \beta) = (\Psi(\alpha) (\Omega(a)(\Theta(\beta)) ), \Phi(b) (\Lambda(a)(\Gamma(b)) ) ) \quad (5.1) $$

for all $a, b \in K$ and $\alpha, \beta \in Q$. 
Theorem 5.1. The resulting groupoid \( K \bowtie Q \) with multiplication (5.1) is a quasigroup. It is called a biproduct (bicrossed product) of \( K \) and \( Q \).

A permutation group \( G \) on a set \( X \) acts \( t \)-transitively if for any two ordered collections \( \{ x_1, \ldots, x_t \} \) and \( \{ y_1, \ldots, y_t \} \) of elements from \( X \) there exists an element \( g \in G \) such that \( g(x_i) = y_i \) for any \( i = 1, \ldots, t \).

Theorem 5.2. Suppose that \( G(K), G(Q) \) act \( t \)-transitively on \( K \) and on \( Q \), respectively, where \( t \leq \min(|K|, |Q|) \). Suppose that the maps \( \Phi_u, \Psi_\alpha \) does not depend on \( u \) and on \( \alpha \), respectively. Let \( |K| \leq (|Q| - 1)! \) and \( |Q| \leq (|K| - 1)! \). Then \( G(K \bowtie Q) \) acts \( t \)-transitively on \( K \bowtie Q \). In particular, biproduct \( K \bowtie Q \) is polynomially complete.

Take for example the 8-element quasigroups \( K_3 \) with Latin square

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>7</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>3</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>4</td>
<td>6</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

It is easy to check that \( G(K_3) = S_8 \).

Take 16-element quasigroup \( K_4 \) with Latin square

|   | 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 | 5 | 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 | 5 | 1 | 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 | 5 | 2 | 3 | 4 | 1 | 6 |
| 8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 5 | 2 | 3 | 4 | 1 | 6 | 7 |
| 9 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 5 | 2 | 3 | 4 | 6 | 7 | 8 | 9 |
| 10 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 5 | 2 | 3 | 4 | 6 | 7 | 8 | 9 | 10 |
| 11 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 12 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 3 | 4 | 5 | 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 | 1 | 2 | 3 | 4 | 5 | 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 |
It can be proved that \( G(K_4) = S_{16} \). So \( G(K_3), G(K_4) \) act 8-transitively in \( K_3 \) and in \( K_4 \), respectively. Applying iteratively biproduct \( \diamond \) to \( K_3, K_4 \) one can construct a series of quasigroups \( K_n \) of order \( 2^n \) for \( n \geq 3, n \neq 5 \), such that \( G(K_n) \) acts 8-transitively in \( K_n \). It follows that each \( K_n \) is a polynomially complete quasigroup.

**Theorem 5.3** ([18]). A countable quasigroup with at least three elements is isotopic to a quasigroup which has no proper subquasigroups.

So we can construct a polynomially complete quasigroup \( Q \) of any order \( 2^n \), \( n \geq 3, n \neq 5 \), with 8-transitive group \( G(Q) \). Then we take its Then \( G(Q^p) = \pi G(Q) \pi^{-1} \). So the group \( G(Q^p) \) acts 8-transitive on \( Q \) and therefore \( Q^p \) is a polynomially complete quasigroup with no proper subquasigroups.

**Theorem 5.4.** Let \( p \) be a prime and \( q = p^r \). Suppose that \( m \not\in \{1, p, \ldots, p^{r-1}\} \mod (q - 1) \) and \( \beta \) is a generator of the cyclic group \( \mathbb{F}_q^* \). Suppose that \( 1 < m < q - 1 \) is coprime with \( q - 1 \). Then there exists an element \( c \in \mathbb{F}_p^* \) such that \( Q = \mathbb{F}_p \) with multiplication \( x * y = (1 - \beta)x^m + \beta y + c \) has no subquasigroups and it is polynomially complete.

**Theorem 5.5.** Let \( Q \) be a quasigroup of a prime order with no subquasigroups. If its automorphism group is nontrivial then \( Q \) is affine. If \( Q \) is polynomially complete then any operation in \( Q \) is a term with respect to multiplication, left and right inverses.

Let \( Q \) be a ternary quasigroup with multiplication \( xyz \). If we fix one variable then we obtain a binary reduct of \( Q \) which is a quasigroup.

**Theorem 5.6.** Let \( L \) be a finite quasigroup of order \( n \geq 3 \) such that \( G(L) \subseteq A_n \). There exists a ternary quasigroup \( Q \) such that one of its reducts is \( L \) and the group \( G \) of any binary reduct of \( Q \) contains \( A_n \).

**Theorem 5.7** (V.T. Markov). Let \( \sigma \in S_n \) be any non-identity permutation of degree \( n \). Then there exists a highly non-associative quasigroup with the first row equal to \( \sigma \). This quasigroup is simple for any \( n \) and it is polynomially complete if \( n \geq 5 \).

**Theorem 5.8** (V.T. Markov). Let \( Q \) be a finite quasigroup, \( |Q| = k \geq 1 \) and let \( p \) be the least odd prime number such that \( p > k \) (note that \( p = 3 \) if \( k = 1 \) else \( p < 2k \) by Tschebyscheff theorem). Then for any \( n \geq 2k + p \) there exists a quasigroup \( R \) such that \( |R| = n, R \supseteq Q \) and \( \text{Mult}(R) = S_n \).

The next example is due to V.T. Markov. Let \( Q \) be a loop with the Latin square
Then $\text{Mult}(Q) = S_6$, but subgroups generated by row and by column permutations of the Latin square have order 48, respectively.

Note that classifications of quasigroups of order 6 were obtained by Albert and Fisher could do in the 30-th years of the XX-th century.

REFERENCES


(Received: July 27, 2018) V.A. Artamonov
(Revised: January 18, 2019) Department of Algebra
Faculty of Mechanics and Mathematics
Moscow State University
Department of Informatics Mathematics VAVT
Ranepa, RUSSIA