Quasigroups and Related Systems **25** (2017), 1 − 19

Characterizations of highly non-associative quasigroups and associative triples

Viacheslav A. Artamonov, Sucheta Chakrabarti, Saibal Kumar Pal

Abstract. Number of associative triples of quasigroup plays an important role in development of quasigroup based cryptographic schemes. In this paper we present algebraic properties of highly non-associative quasigroups and derive the criteria for polynomial completeness based on their multiplicative groups. We develop an algorithm to check the polynomial completeness of the quasigroup Q from its Latin square representation, which is based on the criteria derived by using element of $\mathrm{Mult}(Q)$ with specific cycle structure. We also develop and implement an algorithm for deriving associative triples of finite quasigroups based on commutators of their Latin squares. Experimental results on quasigroups of different order and all quasigroups of order 4 of different classes are reported.

1. Introduction

Crypto community has focused on usage of non-commutative and non-associative algebraic structures in cryptography more intensively from the beginning of this century. Quasigroups are good choice of this type of algebraic structures for cryptographic purpose [2, 10, 11, 16]. The security of quasigroup based cryptographic primitives depend on its algebraic properties. Highly non-associative is one of the significant algebraic properties for cryptographic suitable choice of quasigroup [6].

Highly non-associative quasigroups were considered in [13, 18]. It was shown in [4] that almost all finite quasigroups Q have the property that the multiplication group $\mathrm{Mult}(Q)$ contains symmetric or alternative group. In other words, the ratio of number of quasigroups having this property and total number of quasigroups of finite order n tends to 1 as $n \to \infty$. From a practical point of view quasigroups of order n, $4 \leqslant n \leqslant 256$ are frequently used in cryptography.

In the present paper we consider the problem of characterizing the highly non-associative quasigroup Q of finite order from its multiplicative group $\mathrm{Mult}(Q)$. Also one of our main aim is to develop an algorithm for testing polynomial completeness based on these algebraic properties. It is the main algebraic parameter

2010 Mathematics Subject Classification: 20N05, 08A40, 08B10.
Keywords: quasigroup, isotopy, simplicity, Latin square, commutators, polynomially completeness, multiplicative group, highly non-associative
Research supported by DST-RFBR Indo-Russian joint project

for cryptographically suitable choice of quasigroups. Another significant parameter for suitable choice of quasigroups is the number of associative triples. The number of associative triples of different classes of finite quasigroups was studied by different researchers [6, 7, 8, 9]. In this paper we also deal with the problem of development of algorithm for derivation of associative triples of a quasigroup of finite order by algebraic approach from its Latin square. The smallest number of associative triples plays an important role to resist some known cryptographic attacks.

In this paper first we discuss the preliminaries of quasigroups, their Latin squares and polynomial completeness in §2. Some properties of affine quasigroups are discussed in §3. Section 4 deals with the characterization of highly non-associative quasigroups, polynomial completeness and simplicity by using multiplicative group Mult(Q) of a quasigroup Q. Also in this section we present the algorithm for testing the polynomial completeness of a quasigroup from its Latin square by using the cycle structure of permutations of Q which are belong to Mult(Q). Section 5 deals with the development of algorithm and experiments of computation of associative triplets and its total numbers from a given Latin square. Also we present experimental results on associative triples over all quasigroups of order 4.

2. Preliminaries

A *quasigroup* is a set Q with a binary operation of multiplication such that for all $a, b \in Q$ the equations $ax = b, \quad ya = b$ have unique solutions $x = a\backslash b, \quad y = b/a$. Then the class of quasigroups form a variety of algebras with three operations $xy, \; x\backslash y, \quad x/y$ which is defined by identities

$$(xy)/y = x = (x/y)y \quad x\backslash(xy) = y = x(x\backslash y). \tag{1}$$

Each quasigroup Q can be given by a Latin square

	x_1	$\dots$	x_n
x_1	a_{11}	$\dots$	a_{1n}
$\vdots$	$\dots$	$\dots$	$\dots$
x_n	a_{n1}	$\dots$	a_{11}

(2)

of size n. The elements of Q are $\{x_1, \dots, x_n\}$, each entry a_{ij} stands for the product $x_i x_j$ in the quasigroup Q.

Let $x \cdot y, x * y$ be two quasigroup multiplications on a set Q. We say that multiplication $x * y$ is an *isotope* of multiplication $x \cdot y$ if there exists permutations π, π_1, π_2 on Q such that

$$x * y = \pi\left(\pi_1^{-1}(x) \cdot \pi_2^{-1}(y)\right) \tag{3}$$

for all $x, y \in Q$. Here (π, π_1, π_2) is called an *isotopy* and the two quasigroups $(Q,)$ and $(Q, *)$ are said to be *isotopic.* If π is an identity permutation then it is called *principal isotopy.*

In terms of the Latin square (2) it means that we replace it by the square

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

where

$$b_{ij} = \pi\left(\pi_1^{-1}(x_i) \cdot \pi_2^{-1}(x_j)\right) = \pi\left(a_{\pi_1^{-1}(x_i),\pi_2^{-1}(x_j)}\right). \tag{5}$$

It means that we rearrange columns and rows of Q using permutations π_2 and π_1, respectively, and afterwards permute elements of the obtained Latin square using π.

The next Proposition follows from (3) and (5).

Proposition 2.1. *Let Q be a quasigroup of order n with a Latin square* (2)*. Denote the sets of its row and column permutations by*

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

If (π, π_1, π_2) is an isotopy of Q then (6) *is replaced by the sets*

$$\begin{aligned}
\{\pi\sigma_{\pi_1^{-1}(1)}\pi_2^{-1}, \dots, \pi\sigma_{\pi_1^{-1}(n)}\pi_2^{-1}\} &= \{\pi\sigma_r\pi_2^{-1},\ 1 \leqslant r \leqslant n\}, \\
\{\pi\tau_{\pi_2^{-1}(1)}\pi_1^{-1}, \dots, \pi\tau_{\pi_2^{-1}(n)}\pi_1^{-1}\} &= \{\pi\tau_s\pi_1^{-1},\ 1 \leqslant s \leqslant n\}.
\end{aligned} \tag{7}$$

In particular the sets

$$\{\sigma_{ij} = \sigma_i\sigma_j^{-1} \mid 1 \leqslant i, j \leqslant n\}, \quad \{\tau_{ij} = \tau_i\tau_j^{-1} \mid 1 \leqslant i, j \leqslant n\} \tag{8}$$

are replaced by the sets

$$\begin{aligned}
\{\pi\sigma_{\pi_1^{-1}(i)}\sigma^{-1}_{\pi_1^{-1}(j)}\pi^{-1} \mid 1 \leqslant i, j \leqslant n\} &= \{\pi\sigma_{rs}\pi^{-1} \mid 1 \leqslant r, s \leqslant n\}, \\
\{\pi\tau_{\pi_2^{-1}(i)}\tau^{-1}_{\pi_2^{-1}(j)}\pi^{-1} \mid 1 \leqslant i, j \leqslant n\} &= \{\pi\tau_{kl}\pi^{-1} \mid 1 \leqslant k, l \leqslant n\},
\end{aligned} \tag{9}$$

respectively.

The multiplication group $\mathrm{Mult}(Q)$ is the permutation group of the set Q generated by permutations (6). By [13, Theorem 2] dihedral, symmetric, alternating, general linear, projective general linear groups as well as Mathieu groups M_{11}, M_{12} can occur as $\mathrm{Mult}(Q)$ for some quasigroup Q.

Denote by $G(Q)$ the subgroup of $\mathrm{Mult}(Q)$ generated by elements (8). Note that $G(Q)$ is generated by elements σ_{i1}, τ_{i1} where $2 \leqslant i \leqslant n$. Since (4) is a Latin square the elements σ_{i1}, $2 \leqslant i \leqslant n$, are distinct and non-identical. Adding to them the identity element we can conclude that the order of the group $H(Q)$ generated by all elements σ_{i1} where $2 \leqslant i \leqslant n$ is at least $n = |Q|$. Since $G(Q) \supseteq H(Q)$, the order of $G(Q)$ is greater or equal to the order of Q.

The next Theorem is close to [13, Theorem 1].

Theorem 2.2. *Under an isotopy (π, π_1, π_2) the group $G(Q)$ is mapped to $\pi G(Q)\pi^{-1}$. In particular if by Albert theorem Q is isotopic to a loop Q' then $G(Q)$ is conjugate to the group $G(Q')$ which coincides with* $\mathrm{Mult}\, Q'$.

Proof. Let $e = x_i$ be the identity of a loop Q'. Then $\sigma_i = \tau_i$ is the identity permutation. Then $\sigma_j\sigma_i^{-1} = \sigma_j$ and similarly $\tau_j\tau_i^{-1} = \tau_j$ for all j. Hence $\pi G(Q)\pi^{-1} = G(Q') = \mathrm{Mult}\, Q'$. Now we can apply (9). □

Note that σ_i is a permutation L_{x_i} of left multiplication by x_i, and τ_j is a permutation R_{x_j} of right multiplication by x_j.

Theorem 2.3. *The following conditions are equivalent:*

(i) *any pair of permutations σ_{ij}, τ_{rs} from* (8) *commute between themselves;*

(ii) *Q is isotopic to a group;*

(iii) *the order of $H(Q)$ is equal to the order of Q.*

Proof. Suppose that (ii) holds. Using Theorem 2.2 we can replace Q by an isotopic copy Q which is a group. By the associativity law, permutations σ_i, τ_r commute and (i) follows.

Suppose that (i) holds. We can assume that Q is a loop. Taking $x_1 = e$ we see that $\sigma_{i1} = \sigma_i$ and $\tau_{r1} = \tau_r$. So for any $a \in Q$ we have

$$(x_i a)x_r = \tau_r\sigma_{i1}a = \sigma_{i1}\tau_r a = x_i(ax_r).$$

So Q is associative and therefore a group.

Suppose that (iii) holds. Then $H(Q) = \{\sigma_{i1} \mid 1 \leqslant i \leqslant n\}$. By (9), Theorem 2.2 and by Albert theorem we can assume that Q is a loop with unit element $x_1 = e$. Now for any indices i, j there exists an index k such that $\sigma_{i1}\sigma_{j1} = \sigma_{k1}$. Applying these maps to $e = x_1$ we get $x_i x_j = x_k$. It means that the map $x_i \to \sigma_{i1}$ is an isomorphism of Q and the group $H(Q)$. Hence (ii) holds.

Suppose that (ii) holds. Without loss of generality we can assume that Q is a group. Then the map $H(Q)$ is the group of left translations by elements of Q and this group is isomorphic to Q. So (iii) follows. □

Theorem 2.4. *The following conditions are equivalent:*

(i) *any pair of permutations from* (8) *commute;*

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

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

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

(v) *The order of $H(Q)$ is equal to the order of $G(Q)$ and to the order of Q.*

Proof. Note that conditions (i) and (iii) are equivalent since the elements (8) generate $G(Q)$.

Now let (i) and (iii) hold. By Albert's theorem Q is isotopic to a loop Q'. Then $G(Q) = \mathrm{Mult}\, Q'$ by Theorem 2.2 is an abelian group. Hence for any $x, y, a \in Q'$ we have $(xa)y = x(ay)$ and $x(ya) = y(xa)$. It follows that mutiplication in Q' is associative and commutative. Thus Q' is a group and (ii) holds.

Conversely if (ii) holds then $G(Q) = \mathrm{Mult}\, Q'$ is an abelian group by Theorem 2.2.

Finally if equivalent conditions (i) – (iii) hold, then $G(Q)$ is isomorphic to $\mathrm{Mult}\, Q'$ where Q' is an abelian group. In this case $\mathrm{Mult}\, Q' \simeq Q'$. Thus $G(Q) \simeq Q'$ and (iv) holds. Conversely (iv) implies (iii).

Suppose that (v) holds. Then Q is isotopic to a group by Theorem 2.3. So we can assume that Q is a group with a unit element x_1. By (v) we have $\tau_{i1} = \sigma_{j1}$ for some j. It means that $x_i x = x x_j$ for any $x \in Q$. Setting $x = x_1$ we get $x_j = x_i$ and obtain commutativity law in Q. So (ii) holds.

The same argument shows that (v) implies (ii). □

3. Affine quasigroups

A universal algebra Q is *affine* if there exists a structure of additive abelian group on Q such that any basic n-ary operation f on Q has the form

$$f(x_1, \ldots, x_n) = \alpha_1(x_1) + \cdots + \alpha_n(x_n) + c,$$

where $\alpha_1, \ldots, \alpha_n$ are group endomorphisms of $(Q, +)$ and $c \in Q$. Following this definition we call a quasigroup Q is *affine* or a *T-quasigroup* if there exists a structure of an abelian group $< Q, +, 0, - >$ in Q such that

$$xy = \alpha(x) + \beta(y) + c \tag{10}$$

for some automorphisms α, β of the group $< Q, +, 0, - >$ and for some element $c \in Q$. It is easy to see that a quasigroup is affine if and only if the group operations $< Q, +, 0, - >$ are polynomials with respect to the quasigroup operations $< Q, \cdot, /, \backslash >$.

Note that the affine quasigroup is isotopic to the abelian group $\langle Q, + \rangle$. In fact take $\pi_1 = \alpha^{-1}$, $\pi_2 = \beta^{-1}$ and $\pi(x) = x + c$.

Hence we have

Proposition 3.1. *If Q is an affine quasigroup then $G(Q)$ is isomorphic to the group $< Q, +, 0, - >$.*

An equivalence relation $\wp$ in a quasigroup Q is a *congruence* if $\wp$ is a subquasigroup in direct square $Q \times Q$. A quasigroup Q is *simple* if it has only trivial congruences. It means in particular that any quasigroup homomorphism from Q to any other quasigroup is either an embedding or its image is a one-element set.

Proposition 3.2. *Let Q be a finite simple affine quasigroup. Then $(Q, +)$ is an elementary abelian p-group for some prime p and $|Q| = p^d$ for some positive integer d. The group $\mathrm{Mult}(Q)$ is embedded into the group of affine transformations $\mathrm{Aff}(Q)$ of Q as a vector space over the field $\mathbb{F}_p$ with p elements. In particular $G(Q)$ is a normal subgroup in $\mathrm{Mult}(Q)$ isomorphic to $\langle Q, +\rangle$.*

Proof. Let A be a subgroup in $(Q, +)$ which is stable under α, β. Define a relation $u \sim v \iff u - v \in A$. It is easy to check that $\sim$ is a congruence. So if Q is a simple quasigroup then $(Q, +)$ has no non-trivial subgroups stable under α, β. In particular for any divisor p of the order of Q the set $\{x \in Q \mid px = 0\}$ is non-zero and therefore it coincides with $(Q, +)$. Hence Q is a vector space over the field $\mathbb{F}_p$. □

Corollary 3.3. *A simple finite quasigroup Q is polynomially complete if either of conditions is satisfied:*

(i) *the order of Q is not a prime power,*

(ii) *the order of Q is a power of a prime p, and $G(Q)$ is not an elementary abelian p-group whose order is equal to the order of Q,*

(iii) $\mathrm{Mult}(Q)$ *has no normal abelian subgroups.*

The class of quasigroups with the given property is stable under isotopies.

Use Proposition 3.2 and [1, Corollary 3.4]

Proposition 3.4. *Let Q be an affine quasigroup of a prime order p. Then the order of each cycle occurring in permutations τ_j, σ_i is a divisor of $p - 1$. In particular the order of each permutation τ_j, σ_i is a divisor of $p - 1$.*

Proof. Affine quasigroup is defined on residue group $\mathbb{Z}/p$ by (10). So we can conclude that $\alpha(x) = kx$, $\beta(y) = my$, where k, m are coprime with p.

Fix an element $y = x_j$. Then $R_y = \tau_j$. By induction on t we can prove that

$$\tau_j^t(x) = k^t x + \left(k^{t-1} + \cdots + 1\right)(my + c).$$

Let τ_j have a cycle of length t generated by an element x, then

$$x = k^t x + \left(k^{t-1} + \cdots + 1\right)(my + c)$$

and therefore

$$(k^t - 1)x + \left(k^{t-1} + \cdots + 1\right)(my + c) = 0.$$

Suppose first that

$$a = k^{t-1} + \cdots + 1 \in \mathbb{Z}/p \setminus 0.$$

Canceling by a, we obtain $(k-1)x + my + c = 0$ or $\tau_j(x) = x$. So τ_j has a cycle of length 1.

Suppose now that

$$a = k^{t-1} + \cdots + 1 = 0$$

in $\mathbb{Z}/p$. Then $k^t = 1$. Since k is coprime with p we can conclude that t is a divisor of $p-1$. □

Proposition 3.5. *Let Q be an affine quasigroup of a prime order p. Then $\mathrm{Mult}(Q)$ is an extension of an abelian translation group by a cyclic group of order dividing $p-1$.*

Proof. By (10) each map R_y, L_x is an affine transformation of $Q = \mathbb{F}_p$ and therefore it has the form $x \to \alpha x + c$ where α is a non-zero element of $\mathbb{F}_p$.

There exists a surjective group homomorphism $\mathrm{Aff}(\mathbb{F}_p) \to \mathbb{F}_p^*$ sending each map $x \mapsto \alpha x + c$ to $\alpha \in \mathbb{F}_p^*$. The image is a subgroup of the cyclic group $\mathbb{F}_p^*$ and the kernel consists of translations $x \mapsto x + c,\ c \in Q$. □

Proposition 3.6. *Let Q be an affine quasigroup. Then the operations $x\diagdown y$, $x\diagup y$ are also affine. Conversely, if an operation $x\diagdown y$ ($x\diagup y$) is affine then Q is affine.*

Proof. Let (10) holds. Then by (1)

$$y = x(x\diagdown y) = \alpha x + \beta(x\diagdown y) + c$$

and therefore

$$x\diagdown y = -\beta^{-1}\alpha x + \beta^{-1}y - \beta^{-1}c.$$

Similarly

$$x = (x\diagup y)y = \alpha(x\diagup y) + \beta y + c$$

implies

$$x\diagup y = \alpha^{-1}x - \alpha^{-1}\beta y - \alpha^{-1}c.$$

Thus the operations $x\diagdown y$, $x\diagup y$ are affine.

Suppose now that $x\diagdown y = \gamma x + \delta y + d$ is affine. Then

$$y = x\diagdown(xy) = \gamma x + \delta(xy) + d$$

and

$$xy = -\delta^{-1}\gamma x + \delta^{-1}y - \delta^{-1}d$$

is an affine operation. The case of affine operation $x\diagup y$ is similar. □

Take fundamental operations $xy,\ x\diagdown y,\ y\diagup x$ in a quasigroup Q and of all nullary operations fixing elements from Q. Now consider all finitary operations in Q which are obtained from fundamental ones by compositions, identifications and permutations of variables. The operations on Q which are obtained by this process are called *polynomial*. A quasigroup Q is *polynomially complete* if any finitary operation on Q is polynomial.

Theorem 3.7 ([12]). *A finite quasigroup Q is polynomially complete, if and only if Q is simple and non-affine quasigroup.*

It is well known that a quasigroup Q is simple if and only if $\mathrm{Mult}(Q)$ is primitive permutation group of Q. The following section deals with characterization of polynomial completeness of highly non-associative quasigroups and its invariant class under isotopy by using $\mathrm{Mult}(Q)$ and $G(Q)$.

4. Highly non-associative quasigroups

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

By a definition of a quasigroup the group $\mathrm{Mult}(Q)$ of a quasigroup Q acts transitively on the set Q.

Proposition 4.1 ([17]). *Let Q be a quasigroup of order n such that $\mathrm{Mult}(Q)$ is a doubly transitive permutation group on Q. Then Q is simple. In particular, if $n \geqslant 4$ and $\mathrm{Mult}(Q) \supseteq \mathbf{A}_n$ then Q is simple. A highly non-associative quasigroup of any order is simple.*

Proof. Suppose $\wp$ is a congruence in Q. Let $\wp(c)$ be a class containing $c \in Q$ and $d \in \wp(c)\setminus c$. By double transitivity there exists $g \in \mathrm{Mult}(Q)$ such that $g(c) = c$ and $g(d) \notin \wp(c)$. Since $\wp$ is a congruence $(c, d) \in \wp$ implies $(g(c), g(d)) = (c, g(d)) \in \wp$, which is not the class.

If a quasigroup Q is highly non-associative then $\mathrm{Mult}(Q) = \mathrm{Sym}(Q)$ is a doubly transitive group. If $n \geqslant 4$, then $\mathbf{A}_n$ is again a doubly transitive group. □

The next Proposition generalizes [1, Proposition 3.13].

Proposition 4.2. *Let Q be a quasigroup of order n. Suppose that $\mathrm{Mult}(Q)$ contains a simple non-identical subgroup G whose images under any group homomorphisms into any symmetric group $\mathbf{S}_q$ is identical provided $q < n$ and $q \mid n$. Then Q is simple.*

Proof. Suppose that Q has a proper congruence $\wp$. If $x \in Q$ then the maps L_x, R_x permute congruence classes of $\wp$. Hence there exists a group homomorphism π from $\mathrm{Mult}\, Q$ into the group $\mathbf{S}_q$ of permutations of $Q/\wp$. As it was shown in [3] orders of each congruence classes of $\wp$ are equal and therefore the order q of $Q/\wp$ is a divisor of the order of Q. By assumption $\pi(G) = 1$ which means that G acts identically on $Q/\wp$. It means that each class of the congruence $\wp$ is stable under the action of G.

Let $x \in Q$ and C the class of $\wp$ containing x. The order of C is equal to $\frac{n}{q} < n$. Since C is stable under action of G there exists a group homomorphism $\xi : G \to \mathbf{S}_{\frac{n}{q}}$. By assumption $\xi(G) = 1$. It means that $g(x) = x$ for any $g \in G$, a contradiction. Hence Q is simple. □

Corollary 4.3. *Let Q be a quasigroup of order n and G a simple non-identical subgroup of* $\mathrm{Mult}(Q)$. *Suppose that the order of G does not divide $q!$ for any proper factor q of n. Then any homomorphisms of G into any symmetric group $\mathbf{S}_q$ is identical provided $q < n$ and $q \mid n$. In particular Q is simple.*

Proof. Let $\pi : G \to \mathbf{S}_q$ be a homomorphism where $q < n$ and $q \mid n$. Then the order of the image $\pi(G)$ divides $q!$. If π is not identical then by simplicity of G the order of $\pi(G)$ is equal to the order of G, a contradiction. □

Theorem 4.4. *Let Q be a finite quasigroup of order n and* $\mathrm{Mult}(Q)$ *contain a subgroup isomorphic the alternative subgroup $\mathbf{A}_m$, where*

$$m \geqslant \max\left(\left[\frac{n}{2}\right] + 1, 5\right). \tag{11}$$

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

Proof. To prove the theorem we need the following two lemmas.

Lemma 4.5. *The group G, isomorphic to $\mathbf{A}_m$ yields the assumption of Proposition* 4.2.

Proof. Let π be a non-identical homomorphism of $G = \mathbf{A}_m$ into $\mathbf{S}_r$ where $r \mid n$ and $r < n$. Since $\mathbf{A}_m$ is simple the map π is injective and therefore $\frac{m!}{2}$, the order of $\mathbf{A}_m$ divides $r!$, the order of $\mathbf{S}_r$. Thus $m! \mid 2 \cdot r!$. It is required to mention that

$$r \leqslant \left[\frac{n}{2}\right]$$

and

$$m \geqslant \left[\frac{n}{2}\right] + 1.$$

Hence

$$\left(\left[\frac{n}{2}\right] + 1\right)! \mid 2 \cdot \left[\frac{n}{2}\right]!.$$

It follows that $\left[\frac{n}{2}\right] + 1 \mid 2$ and $\left[\frac{n}{2}\right] = 1$. In this case $r = 1$ and

$$\frac{5!}{2} \mid \frac{m!}{2} \mid r! = 1,$$

a contradiction. □

Lemma 4.6. *Let p be an odd prime. Then $p+1 \leqslant \left[\frac{p^2}{2}\right]$.*

Proof. Since $p \geqslant 3$ we have

$$p^2 - 2p - 2 = (p-1)^2 - 3 \geqslant 2^2 - 3 = 1 > 0.$$

Hence $p^2 > 2p+2$ and the proof follows. □

Now it follows from Lemma 4.5 and Propositions 4.2, 3.2 Q is a vector space over the field $\mathbb{F}_p$ for some prime p of dimension d.

The maps L_x, R_y are affine transformations of the vector space Q by (10). Therefore $\mathrm{Mult}(Q)$ consists of affine transformations of $(Q,+)$.

Recall some basic facts related to the group $\mathrm{Aff}(Q)$ of affine transformations of $(Q,+)$. Let $f \in \mathrm{Aff}(Q)$ and $f(x) = \alpha(x) + c$ where $\alpha \in \mathrm{GL}(d, \mathbb{F}_p)$ and $c \in Q$. Put $\zeta(f) = \alpha$. Then $\zeta : \mathrm{Aff}(q) \to \mathrm{GL}(d, \mathbb{F}_p)$ is a surjective group homomorphism with abelian kernel consisting of translations $f(x) = x + c,\ c \in Q$. Since $\mathbf{A}_m$ is a nonabelian simple group the homomorphism ζ maps $\mathbf{A}_m$ injectively into $\mathrm{GL}(d, \mathbb{F}_p)$. Moreover there is a surjective group homomorphism $\det : \mathrm{GL}(d, \mathbb{F}_p) \to \mathbb{F}_p^*$ with kernel $\mathrm{SL}(d, \mathbb{F}_p)$. The group $\mathbb{F}_p^*$ of nonzero elements of the field $\mathbb{F}_p$ is abelian. Again by simplicity of $\mathbf{A}_m$ we have $\det(\zeta(\mathbf{A}_m)) = 1$. It means that ζ embeds $\mathbf{A}_m$ into $\mathrm{SL}(d, \mathbb{F}_p)$ and by Lagrange's theorem $\frac{m!}{2}$ divides the order of $\mathrm{SL}(d, \mathbb{F}_p)$ which is equal to

$$\frac{(p^d-1)(p^d-p)\cdots(p^d-p^{d-1})}{p-1} = p^{\frac{d(d-1)}{2}}(p^d-1)(p^{d-1}-1)\cdots(p^2-1).$$

Since $m \geqslant \left[\frac{p^d}{2}\right] + 1$ we can conclude that

$$\left(\left[\frac{p^d}{2}\right] + 1\right)! \mid 2p^{\frac{d(d-1)}{2}}(p^d-1)(p^{d-1}-1)\cdots(p^2-1). \tag{12}$$

Note that by definition $p^{d-1} \leqslant \frac{p^d}{2}$. Hence the product $(p^{d-1}-1)\cdots(p^2-1)$ occurs in $\left(\left[\frac{p^d}{2}\right]+1\right)!$. After cancellation in (12) we obtain

$$p^{d-1}\left(p^{d-1}+1\right) \mid 2p^{\frac{d(d-1)}{2}}(p^d-1)$$

and therefore $\left(p^{d-1}+1\right) \mid 2(p^d-1)$. Note that

$$2p + 2 = -2\left(p^d - 1\right) + 2p\left(p^{d-1}+1\right).$$

Hence

$$\left(p^{d-1}+1\right) \mid 2(p+1). \tag{13}$$

Let $p = 2$. Then $d \geqslant 3$, because $n = 2^d \geqslant 5$. So in (13) we have $\left(2^{d-1}+1\right) \mid 6$. Then $d = 1$, 2, a contradiction.

Now let p be an odd prime and (13) holds. If $d \geqslant 3$, then

$$p^{d-1} + 1 \geqslant p^2 + 1 > 2(p+1),$$

a contradiction.

Let $d = 2$. Then in (12) we have

$$\left(\left[\frac{p^d}{2}\right] + 1\right)! \mid 2p(p^2-1) = 2p(p-1)(p+1). \tag{14}$$

Cancel (14) by $(p-1)p(p+1)$. Then by Lemma 4.6, $1 \cdot \ldots \cdot (p-2) \cdot (p+2) \cdots \mid 2$, and therefore $p+2$ divides 2, a contradiction, since p is an odd prime.

So (12) is impossible and Q is not affine. Therefore Q is polynomially complete.

In particular, if $\operatorname{Mult}(Q)$ is highly non-associative, then $\operatorname{Mult}(Q)$ contains $\mathbf{S}_n$ and $\mathbf{A}_m$, where m is from (11). □

Proposition 4.7. *Let Q be a quasigroup of order $n \geqslant 5$. Suppose that there exists an element of* $\operatorname{Mult}(Q)$ *with a cycle decomposition containing a cycle of prime length $p > \frac{n}{2}$ and $n - p \neq 0, 1$. Then* $\operatorname{Mult} Q$ *is simple and* $\operatorname{Mult} Q$ *contains $\mathbf{A}_n$ if one of the following conditions is satisfied:*

(i) $n \geqslant p + 3$

(ii) $n = p + 2$ *and* $n - 1 \neq 2^t$, $t \in \mathbb{N}$.

Proof. Let $\sigma \in \operatorname{Mult}(Q)$ and $\sigma = \sigma_1 \cdots \sigma_m$ a decomposition into a product of independent cycles and the length of σ_1 is equal to p. Then the lengths of other cycles σ_j, $j > 1$ is less than p. Let d be the least common multiple of orders of cycles σ_j, $j > 1$. Then d is coprime with p. Therefore $\sigma^d = \sigma_1^d \in \operatorname{Mult}(Q)$ is a cycle of prime length p fixing $n - p$ elements of Q. Hence $\sigma_1 \in \operatorname{Mult}(Q)$ and therefore

$$\sigma_2 \cdots \sigma_m = \sigma_1^{-1}\sigma \in \operatorname{Mult}(Q).$$

The group $G = \langle \sigma_1 \rangle$ has a prime order. Hence it is a simple subgroup in $\operatorname{Mult}(Q)$. Suppose there exists a homomorphism $f : G \to \mathbf{S}_q$ where $q < n$ and $q \mid n$. So $q \leqslant \frac{n}{2}$, $p > \frac{n}{2}$ so $\frac{n}{2} < p$ and therefore $q < p$.

The image $f(G)$ has order p so $p \mid q!$ where $(q, p) = 1$. It follows that p can't divide $q!$, a contradiction. Hence $f(G) = 1$.

By Proposition 4.2 we obtain that Q is simple and therefore $\operatorname{Mult} Q$ is primitive group of permutations.

Now since $n - p \neq 0, 1$, so either

(i) $n - p \geqslant 3$, then, by [14, Theorem 1.2, Corollary 1.3], $\mathbf{A}_n \subseteq \operatorname{Mult}(Q)$, or

(ii) $n-p=2$ then by [14, Theorem 1.2, Corollary 1.3] we obtain $\mathbf{A}_n \subseteq \mathrm{Mult}(Q)$, if $n-1=p+1$ is not a prime power. Suppose that $p+1=q^t$ for some prime q. Then $q^t-1=p$ and $(q-1) \mid p$ which means that $q=2$. So in this case if $n-1 \neq 2^t$ then the proposition holds. □

By using Proposition 4.7 in a restricted domain and Theorem 4.4 we develop an algorithm (Figure 1) to identify polynomially complete quasigroups of order $n>5$ based on their Latin square representations. Compute $\mathrm{Mult}(Q)$ from Q is computationally expensive. Hence in this algorithm we choose the element from Q of $\mathrm{Mult}(Q)$ and it able to identify a subclass of polynomially complete quasigroup using lesser computation. The algorithm is given below:

Algorithm

Input : $n \times n$ Latin square of the quasigroup Q of order n
Output : Decision - quasigroup is polynomially complete / unidentified
Steps :

```
1. flag=0
2. for $i = 1 : n$
       • Decompose row permutation $\sigma_i$ of $Q$ into disjoint cycles
       • Check whether there exists a sub-cycle of $\sigma_i$ of prime length $p \in \left[\left[\frac{n}{2}\right]+1, n-2\right]$
           – if yes, then check whether
                 $(n-p \geqslant 3)$ or $(n-p=2 \& n \neq 2^t$ for $t \in \mathbb{N})$
           – if yes then flag=1; break; endif
       endif
       endfor
3. if flag=0 then repeat step2 for column permutation $\tau_j, 1 \leqslant j \leqslant n$, of $Q$
   endif
4. if flag=1 print : Polynomially Complete
   else print : unidentified
   endif
```

Figure 1: Algorithm for identifying polynomially complete quasigroup of order > 5.

The following example shows the application of the algorithm to identify the polynomially complete quasigroup Q from the given corresponding Latin square by testing the cycle structures of row / column permutations of $Q \subseteq \mathrm{Mult}(Q)$.

Let Q be a finite quasigroup Q of order $n=7$. The corresponding 7×7 Latin square is given below

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

Following the steps of the algorithm described in Figure 1, for $i = 4$, σ_4 has a sub-cycle of length $p = 5$. Now $n - p = 2\,\&n - 1 = 6 \neq 2^t$ for $t \in \mathbb{N}$. So by the algorithm it is identified as polynomially complete.

Recall that the *Klein* subgroup V_4 of $\mathbf{S}_4$ consists of an identity permutation and of all three 2×2-cycles. The order of V_4 is equal to 4 and it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proposition 4.8. *Let Q be a quasigroup of order 4. Suppose that* $\mathrm{Mult}(Q)$ *does not contain a cycle of length 3. Then* $\mathrm{Mult}(Q)$ *is contained in a Sylow 2-group* Syl_2 *of* $\mathbf{S}_4$ *which is a semi-direct product of the Klein group V_4 and a subgroup of order 2 generated by 2-cycle.*

Proof. By assumption each non-identical element from $\mathrm{Mult}(Q) \subseteq \mathbf{S}_4$ is either a 4-cycle or a product of independent 2-cycles. It means that each element of $\mathrm{Mult}(Q)$ has order 1, 2, 4. So it is contained in Sylow 2-subgroup of $\mathbf{S}_4$. □

Proposition 4.9. *Let Q be a quasigroup of order 4 in which* $\mathrm{Mult}(Q)$ *has a 3-cycle. Then the group* $\mathrm{Mult}(Q)$ *contains* $\mathbf{A}_4$*. Hence if there is also an odd permutation among its row or column permutations then Q is highly non-associative and therefore polynomially complete.*

Proof. Let a 3-cycle σ exist. By [1, Proposition 3.13] the quasigroup Q is simple.

Let $G = \mathrm{Mult}(Q)$ and H a subgroup in G fixing the same element as σ. Then σ belongs to H. Hence the order of H is divisible by 3 and also $|G| = 4|H|$ because G acts transitively on Q. Hence the order of G is divisible by 12.

Since G is a subgroup of $\mathbf{S}_4$ we can conclude that the order of G is either 12 or 24. So either $G = \mathbf{A}_4$ or $G = \mathbf{S}_4$.

If in addition there exists an odd permutation from $\mathrm{Mult}(Q) \supset \mathbf{A}_4$, then $\mathrm{Mult}(Q) = \mathbf{S}_4$. By [1, Proposition 4.4] Q is not a affine quasigroup. □

Proposition 4.10. *Let Q be a non-simple quasigroup of order 4. Then* $\mathrm{Mult}(Q)$ *is contained in Sylow 2-subgroup* Syl_2 *of* $\mathbf{S}_4$*. Note that the commutator of* Syl_2 *is contained in V_4 and it has order 2.*

Proof. If Q is non-simple then $\mathrm{Mult}(Q)$ does not contain 3-cycles by Proposition 4.9. Apply Proposition 4.8. □

Proposition 4.11. *Let $|Q| = p^d$ for some prime p and* $\mathrm{Mult}(Q)$ *is embedded into the group of all affine transformations of a vector space V of dimension d over the field $\mathbb{F}_p$ with p elements. Then Q can be identified with V and*

$$xy = x * y + \alpha(x) + \beta(y) + c, \quad c \in Q,$$

where $x * y$ is a bilinear multiplication in Q such that α, β and the maps

$$x \mapsto x * y + \alpha(x), \quad y \mapsto x * y + \beta(y) \tag{15}$$

are invertible linear operators in Q.

Proof. By assumption on the order of Q and on action of $\mathrm{Mult}(Q)$ we can identify Q with the vector space V of dimension d over the field $\mathbb{F}_p$ such that the maps of left and right multiplication became affine transformations on Q. More precisely, for any $x, y \in Q$ we have

$$\begin{aligned} xy = L_x y = \beta_x(y) + \gamma(x), &\quad \gamma(x) \in Q; \\ xy = R_y x = \alpha_y(x) + \delta(y), &\quad \delta(y) \in Q, \end{aligned}$$

where β_x, α_y are invertible linear operators in Q for any $x, y \in Q$.

Setting $\beta = \beta_0, \alpha = \alpha_0$ we get

$$\begin{aligned} 0y = \beta(y) + \gamma(0) = \delta(y); \\ x0 = \alpha(x) + \delta(0) = \gamma(x). \end{aligned}$$

Hence

$$xy = \beta_x(y) + \alpha(x) + \delta(0) = \alpha_y(x) + \beta(y) + \gamma(0).$$

Setting $x = y = 0$ we obtain $\delta(0) = \gamma(0)$ and therefore

$$\beta_x(y) - \beta(y) = \alpha_y(x) - \alpha(x)$$

is a bilinear multiplication $x * y$ in Q. Finally, $\alpha_y(x) = x * y + \alpha(x)$ and it follows that xy has the required form.

As we have noticed above α, β are invertible linear operators. Since Q is a quasigroup the maps (15) are also invertible linear operators for any $x, y \in Q$. □

Consider a quasigroup

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

.

In this example the fist row is the cycle $(1, 2)$, the second row is the cycle $(2, 3, 4)$. It also contains a cycle $(1, 3, 2, 4)$ and by Theorem 4.9 it is highly non-associative. Therefore by Proposition 4.1 it is simple.

Consider another quasigroup

$$\begin{array}{|c|cccc|}\hline & 1 & 2 & 3 & 4 \\ \hline 1 & 3 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 2 \\ 3 & 1 & 4 & 2 & 3 \\ 4 & 2 & 3 & 1 & 4 \\ \hline \end{array}\ . \tag{16}$$

In this example row permutations are

$$(1,3,4),\ (1,4,2),\ (2,4,3),\ (1,2,3). \tag{17}$$

Column permutations are

$$(1,3)(2,4), \quad (1,2)(3,4), \quad (1,4)(2,3), \quad \varepsilon, \tag{18}$$

where ε is the identity permutation. So by Proposition 4.9 this is a simple quasigroups whose $\mathrm{Mult}(Q) = \mathbf{A}_4$. So simplicity does no imply highly-nonassociativity.

Now we shall characterize invariant class of polynomially complete highly non associative quasigroup under isotopy.

Proposition 4.12. *Let Q be a finite quasigroup of order $n \geqslant 5$. Suppose that the group $G(Q)$ from § 2 contains a subgroup isomorphic to $\mathbf{A}_m$, $m \geqslant \max(\frac{|Q|}{2}+1, 5)$. The class of quasigroups Q with given property is stable under isotopies. All of them are polynomially complete.*

Apply Theorems 2.2 and 4.4.

5. Method for derivation of associative triples

In this section we present a method for deriving associative triples of quasigroups of order n. It is based on commutators of row and column permutations of its Latin squares. Here we also give an algorithm for this scheme.

Recall that a triple (x, a, y) of elements of a quasigroup Q is *associative* if $x(ay) = (xa)y$. In other words $L_x R_y a = R_y L_x a$, where L_x, R_y are maps of left multiplication by x and right multiplication by y.

Suppose that a finite quasigroup Q of order n is given by its Latin square (2) with row and column permutations $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_n$. Let $x = x_i$, $y = x_j$. So $L_x = \sigma_i$, $R_y = \tau_j$. Then $L_x R_y a = \sigma_i \tau_j a$, $\quad R_y L_x a = \tau_j \sigma_i a$. Hence a triple (x_i, a, x_j) is associative if and only if $\sigma_i \tau_j a = \tau_j \sigma_i a$. It can be written in equivalent form $\sigma_i^{-1} \tau_j^{-1} \sigma_i \tau_j a = a$. If we use group commutator $[\sigma_i^{-1}, \tau_j^{-1}] = \sigma_i^{-1} \tau_j^{-1} \sigma_i \tau_j$ then we can write $[\sigma_i^{-1}, \tau_j^{-1}] a = a$.

So we have

Proposition 5.1. *A triple (x_i, a, x_j) is associative if and only if a is a fixed element of the permutation $[\sigma_i^{-1}, \tau_j^{-1}]$.*

So the number of associative triples is equal to a sum of numbers of all fixed elements under commutators $[\sigma_i^{-1}, \tau_j^{-1}]$ for all $i, j = 1, \dots, n$.

The algorithm for associative triples of a quasigroup Q of order n is developed based on commutators of column and row permutations of its Latin square by using Proposition 5.1. The algorithm is given below.

Algorithm

Input : $n \times n$ Latin square of the quasigroup Q of order n
Output : Associative triples of Q and total number
Steps :

1. Write all row $(\sigma_1, \dots, \sigma_n)$ & $(\tau_1, \dots, \tau_n)$ permutations of Latin square
2. Write all $\sigma_1^{-1}, \dots, \sigma_n^{-1} \& \tau_1^{-1}, \dots, \tau_n^{-1}$
3. Calculate $[\sigma_i^{-1}, \tau_j^{-1}] = \sigma_i^{-1} \tau_j^{-1} \sigma_i \tau_j$
4. Represent each $[\sigma_i^{-1}, \tau_j^{-1}]$ is cycle form
5. Write all elements $x_k \in Q$ such that x_k does not belong to any nontrivial cycle of $[\sigma_i^{-1}, \tau_j^{-1}]$ and denote by $\overline{x_k}$
6. Associative triples for each $[\sigma_i^{-1}, \tau_j^{-1}]$ are $(x_i, \overline{x_k}, x_j)\, \forall \overline{x_k}$
7. Total number of associative triples $= \sum \# \overline{x_k}$ for each i, j where $1 \leqslant i, j \leqslant n$

Figure 2: Algorithm for associative triples.

This algorithm first calculates n^2 number of commutators and directly calculate associative triples directly instead of calculations of $2n^3$ triplets of the form $(xy)z$, $x(yz)$ and comparing them to derive associative triplets.

The following example shows application of the algorithm for a quasigroup of order 5. Consider a quasigroup Q of order 5 with the Latin square

	1	2	3	4	5
1	4	2	3	5	1
2	5	1	4	2	3
3	2	3	5	1	4
4	3	5	1	4	2
5	1	4	2	3	5

.

Then the row and column permutations are

$$\begin{aligned}
&\sigma_1 = (1,4,5),\ \sigma_2 = (1,5,3,4,2),\ \sigma_3 = (1,2,3,5,4),\\
&\sigma_4 = (1,3)(,2,5),\ \sigma_5 = (2,4,3),\\
&\tau_1 = (1,4,3,2.5),\ \tau_2 = (1,2)(4,5),\ \tau_3 = (1,3,5,2,4),\\
&\tau_4 = (1,5,3),\ \tau_5 = (2,3,4).
\end{aligned}$$

A calculations by algorithm given in Figure 2 shows that the following commutators have fixed elements:

commutators	fixed elements	associative triples	number of associative triples
$[\sigma_1^{-1}, \tau_1^{-1}] = (1,2,4)$	x_3, x_5	$(x_1, x_3, x_1), (x_1, x_5, x_1)$	2
$[\sigma_1^{-1}, \tau_2^{-1}] = (1,5)(2,4)$	x_3	(x_1, x_3, x_2)	1
$[\sigma_1^{-1}, \tau_4^{-1}] = (1,3)(4,5)$	x_2	(x_1, x_2, x_4)	1
$[\sigma_1^{-1}, \tau_5^{-1}] = (1,3,4)$	x_2, x_5	$(x_1, x_2, x_5), (x_1, x_5, x_5)$	2
$[\sigma_2^{-1}, \tau_4^{-1}] = (2,5,3)$	x_1, x_4	$(x_2, x_1, x_4), (x_2, x_4, x_4)$	2
$[\sigma_2^{-1}, \tau_5^{-1}] = (2,5,4))$	x_1, x_3	$(x_2, x_1, x_5), (x_2, x_3, x_5)$	2
$[\sigma_4^{-1}, \tau_4^{-1}] = (1,5)(2,3)$	x_4	(x_4, x_4, x_4)	1
$[\sigma_5^{-1}, \tau_1^{-1}] = (1,2,3)$	x_4, x_5	$(x_5, x_4, x_1), (x_5, x_5, x_1)$	2
$[\sigma_5^{-1}, \tau_4^{-1}] = (3,4,5)$	x_1, x_2	$(x_5, x_1, x_4), (x_5, x_2, x_4)$	2
$[\sigma_5^{-1}\tau_5^{-1}] = \varepsilon$	$x_i,\ \forall i$	$(x_5, x_i, x_5)\ \forall i$	5

The total number of associative triples is equal to 20. This algorithm can explicitly able to compute the associative triples of any finite order quasigroups and hence total number of associative triples. In our experiment we find the lowest number of associative triples for quasigroup of order 5 is 20.

In the following section we present experimental results of number of associative triples for all quasigroups of order 4 of different algebraic classes considered in [2].

6. Experimental results

The algorithm for derivation of associative triples of quasigroups of finite order is implemented. It has been succesfully applied on different order of quasigroups. From algebraic point of view we classify the the quasigroups of order 4 in four different classes [2] which are viz. (i) Simple and affine quasigroups (ii) Simple and non-affine quasigroups (Polynomially complete), (iii) Non-simple and affine quasigroups and (iv) Non-simple and non-affine quasigroups. Experiments are carried out on the set of all quasigroups of order 4 to find out the number of associative triples of different classes. Experimental results show that number of associative triples are either 16 or 24 for simple cases and 32 or 64 for non-simple cases. So, 16 is the minimum number of associative triples of quasigroups of order 4 [9].

The table given below shows the number of quasigroups and corresponding associative triples of each class.

Classes	Number of quasigroups	Number of associative triples
Simple and affine	104	16
Simple and non-affine (polynomially complete)	240	16
	144	24
Non-simple and affine	48	32
	8	64
Non-simple and non-affine	24	32
	8	64

Figure 3: Associative triples of different classes of quasigroups of order 4

From algebraic point of view we know that cryptographic suitable quasigroups are polynomially complete [1]. Minimum number of associative triples is also an important algebraic property for good choice of cryptographic quasigroups. Experimental results show that cryptographic suitable quasigroups of order 4 are 240 beloging to the polynomially complete class. It is also observed that number of associative triples of non-simple quasigroups are always greater than simple quasigroups of order 4. Therefore, quasigroups belonging to the non-simple class are unsuitable for cryptographic purpose.

7. Acknowledgement

We are thankful to Dr. G.Athithan, DG (MED & CoS), DRDO and Ms. Anu Khosla, Director SAG, DRDO for their support and encouragements to carry out the collaborative research work.

Our heartiest thanks to Professor Bimal K. Roy, ASU, ISI Kolkata for his support and hospitality.

Authors are also thankful to all professors of Indo-Russian joint project team for their technical support and cooperation.

References

[1] **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.

[2] **V.A. Artamonov, S. Chakrabarti, S.K. Pal**, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200** (2016), 5 – 17.

[3] **V.D. Belousov**, *Foundations of the theory of quasigroups and loops*, (Russian), Izdat. Nauka, Moscow, 1967.

[4] **P.J. Cameron**, *Almost all quasigroups have rank* 2, Discrete Math. **106/107** (1992), 111 – 115.

[5] **J. Dénes, T. Dénes**, *Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack*, Quasigroups and Related Topics, **8** (2001), 7 – 14.

[6] **J. Dénes, A.D. Keedwell**, *A new authentication scheme based on Latin squares.* Discrete Math. **106/107** (1992), 57 – 161.

[7] **A. Drápal**, *On quasigroups rich in associative triples.* Discrete Math. **44** (1983), 251 – 265.

[8] **A. Drápal, T. Kepka**, *A note on the number of associative triples in quasigroups isotopic to groups.* Comment. Math. Univ. Carol. **22** (1981), 735 – 743.

[9] **O. Grošek, P. Horák**, *On quasigroups with few associative triples.* Des. Codes Cryptogr. **64** (2012), 221 – 227.

[10] **M.M. Glukhov**, *On application of quasigroups in cryptology*, Applied Discrete Math. **2** (2008), 28 – 32.

[11] **D. Gligoroski, S. Markovski, S.J. Knapskof**, *The stream cipher Edon-80*, Lecture Notes Computer Sci. **4986** (2008), 152 – 169.

[12] **J. Hagemann, C. Herrmann**, *Arithmetically locally equational classes and representation of partial functions.* Universal Algebra, Estergom (Hungary) **29**, Colloq. Math. Soc. J. Bolyai, 1982, 345 – 360.

[13] **T. Ihringer**, *On multiplication groups of quasigroups*, European J. Combin. **5** (1984), 137 – 141.

[14] **G.A. Jones**, *Primitive permutation groups containing a cycle*, Bull. Aust. Math. Soc. **89** (2014), 159 – 165.

[15] **L. Guohao, Y. Xu**, *Cryptographic classification of quasigroups of order* 4, Intern. Workshop on Cloud Computing and Information Security (2013), 278 – 281.

[16] **V.A. Shcherbacov**, *Quasigroups in cryptology*, Computer Sci. J. Moldova **17** (2009), 193 – 227.

[17] **K.K. Schukin**, *Simplicity of a quasigroup and primitivity of its of its multiplication group,* Izv. Akad. Nauk. Mold. SSR. Mat. **3** (1990), 66 – 68.

[18] **J.D. Smith**, *Multiplication groups of quasigroups*, Preprint No. **603**, Technische Hochschule Darmstadt, 1981.

Received November 10, 2016

V.A. Artamonov
Faculty of Mchanics and Mathematics, Moscow Satate University, Leninsky Gory 1,
119992 Moscow, Russia
e-mail: artamon@mech.math.msu.su

S. Chakrabarti, S.K. Pal
Scientific Analysis Group, DRDO, India,
e-mail: suchetadrdo@hotmail.com, skptech@yahoo.com