Quasigroups and Related Systems **21** (2013), 117 − 130

On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts

Viacheslav A. Artamonov, Sucheta Chakrabarti,
Sugata Gangopadhyay and Saibal K. Pal

Abstract. We develop some methods and algorithms for checking the polynomial completeness property of some finite quasigroups by considering their corresponding Latin square representations. It is shown that polynomially complete quasigroups are simple and non-T-quasigroups. We study cyclic decompositions of permutations related to rows and columns of Latin squares of non-simple quasigroups and of T-quasigroups. Here we develop the criteria for the polynomial completeness of finite quasigroups based on this study.

1. Introduction

In this paper we develop some methods and algorithms for checking the polynomial completeness property of some finite quasigroups by considering their corresponding Latin square representations. Quasigroups in some applications are mainly given by their Latin squares. So we have to recognize algebraic properties basing on these squares.

In Section 2 we discuss the preliminaries of quasigroups and polynomial completeness. Section 3 deals with congruence simplicity of quasigroups.

A finite quasigroups is certainly polynomially complete if the combinations of lengths of cyclic decompositions for all rows and columns does not belong to the list of possible combinations for non-simple and for T-quasigroups. This ideas is realized in the case of quasigroups of order 4.

In Section 4, T-quasigroups are considered and criteria for non-T-quasigroups have been established from their corresponding Latin squares. Section 5 deals with quasigroups generated by left or right shifts with unit elements.

We also consider connections with quasigroups with one-sided unit element which are generated by shifts.

2010 Mathematics Subject Classification: 20N05, 08A40, 08B10
Keywords: Latin square, polynomial completeness, permutations.
Research of the first author was partially supported by grant RFFI 12-01-00070 and by grant COEC India.

2. Preliminaries

A *quasigroup* is a set Q with a binary operation of multiplication xy such that for all $a, b \in Q$ the equations $ax = b$, $ya = b$ have unique solutions $x = a\diagdown b$, $y = b\diagup a$. It can be checked that the following identities hold

$$(xy)\diagup y = x = (x\diagup y)y, \quad x\diagdown(xy) = y = x(x\diagdown y). \tag{1}$$

Basic facts concerning quasigroups can be found in [3] and in [8].

If Q is a quasigroup with elements $\{x_1, \dots, x_n\}$ then the multiplication table is given by a Latin square

$$\begin{array}{|c|ccc|}
\hline
 & x_1 & \dots & x_n \\
\hline
x_1 & a_{11} & \dots & a_{1n} \\
\vdots & \dots & \dots & \dots \\
x_n & a_{n1} & \dots & a_{nn} \\
\hline
\end{array} \tag{2}$$

of size n, where an entry a_{ij} stands for the product $x_i x_j$ in the quasigroup Q. Note that if we rearrange elements of Q using a permutation π then in the Latin square will have the form

$$\begin{array}{|c|ccc|}
\hline
 & x_{\pi(1)} & \dots & x_{\pi(n)} \\
\hline
x_{\pi(1)} & b_{11} & \dots & b_{1n} \\
\vdots & \dots & \dots & \dots \\
x_{\pi(n)} & b_{n1} & \dots & b_{nn} \\
\hline
\end{array}\,, \tag{3}$$

where $b_{ij} = a_{\pi(i),\pi(j)}$. Note that a rearrangement π gives an isomorphic quasigroup. Moreover the set of lengths of cyclic decompositions of its row and column permutations is stable under rearrangements.

It is useful to consider permutations of Q which are induced by operators L_y, R_y of left and right multiplications by an element y, namely $L_y x = yx$, $R_y x = xy$.

An operator L_{x_i} permutes element of Q and a result of this permutation is written in the ith row of the table (3). Similarly the map R_{x_i} is a permutation on Q whose results are written in the ith column.

Let $\varkappa_1 = R_{x_1}, \dots, \varkappa_n = R_{x_n}$ be column permutations and $\rho_1 = L_{x_1}, \dots,$ $\rho_n = L_{x_n}$ be row permutations. Then the jth row of the Latin square associated with $x\diagup y$ is equal to $k_i^{-1} x_j$, $i \in \{1, \dots, n\}$. Similarly the jth column in the Latin square associated with $x\diagdown y$ is equal to $\rho_i^{-1} x_j$ $i \in \{1, \dots, n\}$. These two new squares are again Latin squares.

Denote by $\mathcal{O}_n(A)$ the set of all n-ary algebraic operations on A and by $\mathcal{O}(A)$ the collection of all $\{\mathcal{O}_n(A) \mid n \geqslant 0\}$.

Let $F = \{F_n \mid n \geqslant 0\}$ be a family of sets called a *signature*. A non-empty set A is an *algebra of a signature* F or briefly an F*-algebra* if there is a map $\alpha : F \to \mathcal{O}(A)$ such that $\alpha(F_n) \subseteq \mathcal{O}_n(A)$. It means that each $f \in F_n$ is realized via α as an n-ary operation in A.

If $f \in \mathcal{O}_n(A)$ and $g_1, \ldots, g_n \in \mathcal{O}_m(A)$ then one can define a *Menger composition* (*superposition*) $f(g_1, \ldots, g_n) \in \mathcal{O}_m(A)$ by the rule

$$[f(g_1, \ldots, g_n)]\,(x_1, \ldots, x_m) = f\left(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m)\right), \qquad (4)$$

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

The composition satisfies the *super-associativity* law

$$[f(g_1, \ldots, g_n)]\,(h_1, \ldots, h_m) = f\left(g_1(h_1, \ldots, h_m), \ldots, g_n(h_1, \ldots, h_m)\right),$$

for all $f \in \mathcal{O}_n(A),\ g_1, \ldots, g_n \in \mathcal{O}_m(A),\ h_1, \ldots, h_m \in \mathcal{O}_r(A)$.

Observe that if the operations $g_1, \ldots g_n$ in (4) are nullary, that is $m = 0$ and $g_i(*) = a_i \in A$ then $[f(g_1, \ldots, g_n)]\,(*) = f(a_1, \ldots, a_n)$.

The family $\mathcal{O}(A)$ contains special operations of *projections*

$$p_{in}(x_1, \ldots, x_n) = x_i,$$

for all $n \geqslant 1$ and all $i = 1, \ldots, n$. Clearly, $f = f(p_{1n}, \ldots, p_{nn})$ for $f \in \mathcal{O}_n(A)$.

A family $\mathcal{C} = \{\mathcal{C}_n \subseteq \mathcal{O}_n(A) \mid n \geqslant 0\}$ is called a *clone of operations* on A if $\mathcal{C}$ contains all projections and it is closed under compositions. It means that if $f, g_1, \ldots, g_n \in \mathcal{C}$, then $f(g_1, \ldots, g_n) \in \mathcal{C}$.

Proposition 2.1. *Let $f \in \mathcal{C}_n$ and an operation g is obtained from f either by a permutation or by an identification of some of its arguments. Then $g \in \mathcal{C}$.* □

Let A be an F-algebra of a signature $F = \{F_n \mid n \geqslant 0\}$. Without loss of generality we can assume that $F_n \subseteq \mathcal{O}_n(A)$ for an any index $n \geqslant 0$.

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.

Definition 2.2. Let F be a signature. An operation $f \in \mathcal{O}_n(A)$ is *polynomial* if there exist a term operation $g \in \mathcal{O}_{n+m}(A)$ 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 $\mathrm{Pol}(F)$ of all polynomial operations is the least clone containing F and all nullary operations.

Definition 2.3. An algebra A of a signature F is *polynomially* (*functionally*) *complete* if $\mathcal{O}(A) = \mathrm{Pol}(F)$.

Definition 2.4. A Malcev operation on a set X is a ternary operations $m(x, y, z)$ satisfying the identities $m(x, x, y) = m(y, x, x) = y$.

Any quasigroup Q has at least two Malcev terms operations [7].

Definition 2.5. An algebra A is *affine* if A is equipped with a structure of an additive Abelian group such that each term operation f 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.

Note that if any term operation f has the above form then any polynomial operation in A can be presented in a similar form.

Definition 2.6. An algebra A is *simple* if it has only trivial congruences.

Proposition 2.7. *Let an affine algebra A has a polynomial Malcev operation. Then the addition in Definition* 2.5 *is a polynomial operation.*

Proof. Malcev polynomial operation $m(x, y, z)$ has a presentation

$$m(x, y, z) = \alpha x + \beta y + \gamma z + c.$$

Now for any $x, y \in A$ we get

$$y = m(x, x, y) = \alpha x + \beta x + \gamma y + c = m(y, x, x) = \alpha y + \beta x + \gamma x + c.$$

Hence $\alpha = -\beta = \gamma = 1$ and $c = 0$. So $m(x, y, z) = x - y + z$ for all $x, y, z \in A$. Now $x + y = m(x, 0, y)$ is a polynomial operation. □

Theorem 2.8. [9] *Let A be a finite F-algebra containing at least two elements. The following are equivalent:*

(i) *A is polynomially complete,*

(ii) *there exists a Malcev operation in* $\mathrm{Pol}(F)$ *on A and the algebra A is simple and non-affine.* □

3. Congruences on quasigroups and its simplicity

In the section we shall present some ideas of checking of a congruence-simplicity of a quasigroup. Some of the facts seem to be a folklore, but for the sake of completeness we include them into the text. For more details see [3], [13].

Let Q be a quasigroup with with a congruence $\wp$. It means that $\wp$ is a subquasigroup of Q^2, it contains a diagonal and it defines an equivalence in Q. The congruence class of $\wp$ containing x is denoted by $\wp(x)$.

It is easy to observe that for a congruence $\wp$

$$R_y\left(\wp(x)\right) = \wp(xy), \quad L_y\left(\wp(x)\right) = \wp(yx).$$

In particular the maps R_y, L_y permute congruence classes of $\wp$.

Suppose that $z, t \in Q$ and $t \in \wp(z)$. There exists a unique element $u \in Q$ such that $uz = x$. Since $\wp$ contains a diagonal in Q^2, we get $(u, u) \in \wp$ and therefore $(u, u)(z, t) = (uz, ut) = (x, ut) \in \wp$. Hence, $ut \in \wp(x)$. So L_u maps $\wp(z) \to \wp(x)$. Since Q is a quasigroup, the map L_u is a bijection. So we have

Proposition 3.1. ([4], Theorem 3.4) *Any two classes of a congruence $\wp$ in a quasigroup Q have the same cardinality. In particular, if Q is a finite quasigroup, then the order of each congruence class divides the order of Q.* □

Corollary 3.2. *A quasigroup of a prime order is congruence-simple. If a non-simple quasigroup has order p^2 where p is a prime, then congruence classes of a non-trivial congruence contain p elements.* □

Proposition 3.3. *Let a quasigroup Q have a left unit e and $\wp$ is a congruence in Q. Then the class $\wp(e)$ is a subquasigroup of Q. If $x, y \in Q$, then $(x, y) \in \wp$ if and only if $x \in \wp(e)y$. So the congruence classes consists of cosets $\wp(e)x,\ x \in Q$.*

Proof. If $y, z \in \wp(e)$, then the pairs $(y, e), (z, e) \in \wp$. Hence $(yz, e) \in \wp$ and therefore $yz \in \wp(e)$.

Now if $(u, v) \in \wp$, then $(u/v, v/v) \in \wp$. But $v/v = e$ because e is a left unit element. Hence if $(u, v) \in \wp$, then $u = (u/v)v \in \wp(e)v$ by (1).

Conversely if $u = av$, where $a \in \wp(e)$ then of course $(u, v) \in \wp$. □

The next statement is quite clear.

Proposition 3.4. *Let Q be a quasigroup of order n then $x_j/x_j = x_i$ are equal for all $j = 1, \dots, n$, if and only if x_i is a left unit element. Similarly $x_j \backslash x_j$ are equal to x_i for all j if and only if x_i is right unit element.* □

Proposition 3.5. *Let Q be a symmetric (commutative) quasigroup of order n. Then $x_i/x_j = x_j \backslash x_i$.* □

So we can say that, if the Latin square w.r.t. multiplication is symmetric, then the Latin squares w.r.t. the operations $/, \backslash$ are transpose to each other i.e. they are adjoint.

Proposition 3.6. *For a binary equivalence relation $\wp$ the following are equivalent:*

(i) *$\wp$ is a congruence,*

(ii) *if $(x_i, x_j) \in \wp$, then $(a_{it}, a_{jt}), (a_{ti}, a_{tj}) \in \wp$ for all t in the square (2).*

The property (ii) means that ith and jth rows and columns are coordinate-wise congruent modulo $\wp$. □

We can apply last two propositions to the case of a non-simple quasigroup Q of order 4. If $\wp$ is a non-trivial congruence, then by Corollary 3.2 there are two 2-element $\wp$-classes, say, $\{x_i, x_j\}, \{x_u, x_v\}$. Since the quotient $Q/\wp$ is a group of order 2, one of classes is a unit element in $Q/\wp$. Note that a class $\{x_i, x_j\}$ is a unit if and only if $x_i^2 \in \{x_i, x_j\}$. So

$$\{x_u, x_v\}\{x_i, x_j\} = \{x_i, x_j\}\{x_u, x_v\} = \{x_u, x_v\},$$
$$\{x_u, x_v\}\{x_u, x_v\} = \{x_i, x_j\}\{x_i, x_j\} = \{x_i, x_j\}.$$

So the class $\{x_i, x_j\}$ will be a two-element subquasigroup of order 2. So rearranging if necessary x_i, x_j we can always assume that $x_i^2 = x_i$. Then $x_i x_j = x_j x_i = x_j$ and $x_j^2 = x_i$. Then in the Latin square of Q we have

$$\begin{pmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{pmatrix} = \begin{pmatrix} x_i & x_j \\ x_j & x_i \end{pmatrix} . \tag{5}$$

Now we have

Theorem 3.7. *Let Q be a quasigroup of order 4 with a non-trivial congruence $\wp$. Then Q is partitioned into two blocks $\{x_i, x_j\}, \{x_u, x_v\}$ such that rearranging elements in the first block we can obtain* (5)*. Then the block*

$$\begin{pmatrix} a_{uu} & a_{uv} \\ a_{vu} & a_{vv} \end{pmatrix}$$

will either coincide with the block (5) *or will be equal to*

$$\begin{pmatrix} x_j & x_i \\ x_i & x_j \end{pmatrix}.$$

Each of the blocks

$$\begin{pmatrix} a_{iu} & a_{iv} \\ a_{ju} & a_{jv} \end{pmatrix}, \quad \begin{pmatrix} a_{ui} & a_{uj} \\ a_{vi} & a_{vj} \end{pmatrix}$$

has one of the forms

$$\begin{pmatrix} x_u & x_v \\ x_v & x_u \end{pmatrix}, \quad \begin{pmatrix} x_v & x_u \\ x_u & x_v \end{pmatrix} .$$

There are 12 *Latin squares of this form.* □

Corollary 3.8. *If Q is a quasigroup of order* 4 *and it is non-simple, then its Latin square* (2) *with $n = 4$ has the following property: there exists a row*

$$(a_{i1}\ a_{i2}\ a_{i3}\ a_{i4})$$

such that the permutation

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ a_{i1} & a_{i2} & a_{i3} & a_{i4} \end{pmatrix},$$

associated with the left multiplication L_{x_i}, is either a 2*-cycle or a product of two independent* 2*-cycles. Entries of non-trivial cycles and elements fixed by these non-trivial permutations are congruence classes.*

The remaining rows are either identical, 2*-cycles, products of two independent* 2*-cycles or* 4*-cycles.*

After a rearrangement according to these congruence classes as described we obtain a modified Latin square from Theorem 3.7. □

Example 3.9. Consider an example of an application of Theorem 3.7 and of Corollary 3.8. Take a Latin square

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

The first and the third lines are 4-cycles, the second is identical, the fourth one is a product of two 2-cycles $(1,3)(2,4)$. So congruence classes could be $\{1,3\},\{2,4\}$. Note that $2\cdot 2 = 2$. So we arrange the elements as $2,4,1,3$. Then the new Latin square will be

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

So it really defines a non-simple quasigroup.

Example 3.10. As another application of Theorem 3.7 and of Corollary 3.8, consider the quasigroup with the Latin square

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

(6)

The first row is a cycle of order 4, the second one has a decomposition $(1,3)(2,4)$, the third and the fourth rows are cycles of order 3. So Q is simple.

Example 3.11. Here we consider some more applications of Theorem 3.7 and of Corollary 3.8 to the Latin squares of the quasigroups which are given below.

	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	1	2	3
3	2	3	0	1

In the first Latin square the rows determine cycles of lengths 3, 4, 4, 3, respectively.

In the second Latin square the rows determine cycles of lengths 4, 0, 4, 2×2, respectively. The 2-cycles from the last row are $(0,3)(1,2)$. But $0\cdot 0 = 1$, $3\cdot 3 = 0$. So if $0 \sim 3$, then $1 = 0\cdot 0 \sim 3\cdot 3 = 0$ which is not the case.

In the third Latin square the rows determine cycles of lengths 2, 4, 3, 3, respectively.

In the last Latin square the rows determine cycles of lengths 2×2, 2×2, 0, 2×2, respectively. Congruence classes are element of 2-cycles. Suppose that according to the decomposition of the first row the classes are $(0,3),(1,2)$. Then $3 = 0 \cdot 0 \sim 3 \cdot 3 = 1$ which is impossible. Suppose that the congruence classes are $(0,1),(2,3)$ according to the second row cycle decomposition. Again $3 = 0 \cdot 0 \sim 1 \cdot 1 = 0$, a contradiction. Finally let congruence classes be $(0,2),(1,3)$ according to the last row. Then $3 = 0 \cdot 0 \sim 2 \cdot 2 = 2$, a contradiction. So all these squares also determine simple quasigroups.

We end the section with a sufficient condition of a simplicity of a finite quasigroups.

Suppose that L_x has a cycle $\left(a, L_x a, L_x^2 a, \ldots, L_x^{p-1} a\right)$, $L_x^p a = a$, of order p and $\wp$ is a congruence in Q. Choose the smallest positive integer d such that $L_x^d a \in \wp(a)$.

Proposition 3.12. *$d \mid p$.*

Proof. Let m be the greatest common divisor of p and d. Then $m = du + pv$ for some integeres u, v. Now $L_x^m a = \left(L_x^d\right)^u \left(L_x^p\right)^v a \in \wp(a)$. Hence $d \leqslant m \leqslant d$ and therefore $d = m$. So p is divisble by d. □

We can conclude that in the cycle of L_x the elements $\{a, L_x a, \ldots, L_x^{d-1} a\}$ belong to different classes of $\wp$, while $\{a, L_x^d a, \ldots, L_x^{d\left(\frac{p}{d}-1\right)}\}$ belong to $\wp(a)$.

Proposition 3.13. *Let p be a prime and $p > \frac{|Q|}{2}$. Then Q is simple.*

Proof. Consider the number d as above. Since p is a prime then either $d = 1$, or $d = p$. Suppose that $d = p$. Then different elements of the cycle belong to different classes of $\wp$. So p does not exceed the number of classes $\frac{|G|}{|\rho(a)|} \leqslant \frac{|G|}{2}$, a contradiction.

Suppose that $d = 1$. Then p does not exceed the number of elements in a class $\rho(a)$ and $|\rho(a)| \leqslant \frac{|G|}{2}$. Again we get a contradiction. □

Corollary 3.14. *Let Q be a quasigroup of order 4. Suppose that some of its row (column) permutations is a cycle of length 3. Then Q is simple.* □

4. Identification of T-quasigroups

We consider the problem of a identification of a T-quasigroups of order 4 based on corresponding Latin squares. The identification criteria are given in Proposition 4.4. It is used for a classification of simple non-T quasigroups of order 4. Note that simple T-quasigroups were characterized in [11, Theorem 2].

A quasigroup Q is a *T-quasigroup* if there exists a structure of an abelian group $(Q, +, 0, -)$ in Q such that

$$xy = \alpha(x) + \beta(y) + c \tag{7}$$

for some automorphisms α, β of the group $(Q, +, 0, -)$ and for some element $c \in Q$. Since any quasigroup has Malcev term operation, by Proposition 2.7 a quasigroup is affine if and only if it is a T-quasigroup. It follows that the class of affine quasigroups coincides with the class of T-quasigroups.

Proposition 4.1. [10] *For a quasigroup with multiplication* (7) *the following are equivalent:*

(i) *Q has a left* (*right*) *unit element e,*

(ii) $\beta = 1$ $(\alpha = 1)$ *and* $e = -\alpha^{-1}c$ $(e = -\beta^{-1}c)$. □

Suppose that T-quasigroup Q is defined on a cyclic group $(Q, +)$ of order n. Then each automorphisms has the form $x \mapsto ax$, where a is an invertible element of the ring $\mathbb{Z}/n$. Thus (7) has the form

$$xy = ax + by + c, \tag{8}$$

where a, b are invertible in $\mathbb{Z}/n$ and $c \in Q$.

Proposition 4.2. *Let Q be a T-quasigroup with multiplication form* (8). *Let $n = pq$. Then the relation $x \sim y \iff x \equiv y \pmod{q}$ is a congruence. In particular, if n is not a prime, then Q is not simple.*

Proof. Let $x, y, r, s \in \mathbb{Z}/n$. Then

$$(x + qr)(y + qs) = a(x + qr) + b(y + rs) + c = ax + by + c + q(ar + bs) \equiv xy.$$

Hence the relation $\sim$ is congruence relation. □

We are interested in the case of simple non T-quasigroups of order 4. So by Proposition 4.2 we can exclude the case when $Q = \mathbb{Z}/4$ and consider the case when $(Q, +) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

Then (7) holds for some $\alpha, \beta \in SL(2, \mathbb{Z}/2)$. The group $\mathrm{SL}(2, \mathbb{Z}/2)$ is isomorphic to the symmetric group S_3. Then α, β are one of 6 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{9}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \tag{10}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{11}$$

Here the matrix (9) is the unit, matrices from (10) have order 2, and matrices from (11) have order 3.

Proposition 4.3. *Let $(Q, +) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$. If xy has the from* (7), *then $x^2 = (\alpha + \beta)x + c$. Hence the following are equivalent:*

(i) $\alpha = \beta$,

(ii) *Q is commutative,*

(iii) *$x^2 = c$ for all x,*

(iv) *the diagonal entries of the Latin square are equal to c.* □

It is easy to check that for any positive integer m we have

$$L_x^m y = \beta^m(y) + \left(\beta^{m-1} + \beta^{m-2} + \cdots + 1\right)(\alpha x + c).$$

In particular,

$$L_x^3 y = \beta^3 y + (\beta^2 + \beta + 1)(\alpha x + c).$$

Hence if β has order 3, then $\beta^2 + \beta + 1 = 0$ and $\beta^3 = 1$. So $L_x^3 = 1$ and since L_x is not identical it determines 3-cycles in each row of the Latin square (2). Similarly if α has order 3, then the operator of right multiplication R_y determines 3-cycles in each column of the Latin square (2).

Suppose that β has order 2 and therefore β is one of the matrices (10).

Then

$$L_x^2 y = \beta^2 y + (\beta + 1)(\alpha x + c) = y + (\beta + 1)(\alpha x + c)$$

because $\beta^2 = 1$.

Suppose $L_x^2 y = y$ for some x. Then $\alpha x + c$ is annihilated by $\beta + 1$, where β is from (10). Thus $\beta + 1$ is one of the matrices

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

So $z = \alpha x + c$ is equal up to a scalar $0, 1$ to one of vectors

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Thus

$$x = \lambda\alpha^{-1} z + \alpha^{-1} c, \quad \lambda = 0, 1. \tag{12}$$

Moreover for each of x form (12) there exists an element y_0 such that $(1 + \beta)y_0 = z = \alpha x + c$. Then $L_x y_0 = \alpha x + \beta y_0 + c = y_0$. Thus taking different λ we obtain two rows which are 2-cycles having fixed elements y_0. If x is different from (12) then L_x is a cyclic of order 4 in the corresponding row because

$$L_x^4 y = \beta^4 y + \left(\beta^3 + \beta^2 + \beta + 1\right)(\alpha x + c) = y$$

for all $y \in Q$ since $\beta^4 = 1$ and $\beta^3 + \beta^2 + \beta + 1 = 0$.

Finally let $\beta = 1$. Then $L_x = 1$ if $\alpha x + c = 0$. Suppose that $L_x \neq 1$. Then $L_x^2 y = y$ for all y. So in this case L_x is of the type 2×2.

Hence we have

Proposition 4.4. *Let Q be a quasigroup of oder 4. Suppose that $(Q,+) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and xy is defined by (7). Then Q is a T-quasigroup if and only if either of the following conditions holds:*

1. *If β is from (11), then rows of the Latin square of Q are 3-cycles.*
2. *If β is from (10), then there exists two rows which are 2-cycles. Other two rows are 4-cycles.*
3. *If β is from (9), then one row is identical the other three rows are of type 2×2. In particular Q has a left unit element.*

Consider similar cases for α we obtain the same possible combinations for column cycle structure as for rows. □

For example the simple quasigroup Q with the Latin square (6) is not a T-quasigroup, since as it was already mentioned its row have cycles of lengths 4, 4, 2×2, 3. Hence it is polynomially complete.

Also cycle structures of rows of simple quasigroups from Example 3.11 are not included into Proposition 4.4. So we can conclude that all these quasigroups are polynomially complete.

5. Quasigroups generated by right and left shifts

A finite quasigroup $Q = \{x_1, \ldots, x_n\}$ is *generated by a right shift* [5] if the following property is satisfied: for all $1 \leqslant i, k, j \leqslant n$ we have

$$x_{i+k \,(\mathrm{mod}\ n)} x_j = x_i x_{j-k \,(\mathrm{mod}\ n)}. \tag{13}$$

It means that $a_{pq} = a_{rs}$, provided $p - r \equiv s - q \pmod{n}$. Similarly a quasigroup Q is *generated by a left shift* if

$$x_{i+k \,(\mathrm{mod}\ n)} x_j = x_i x_{j+k \,(\mathrm{mod}\ n)}$$

for any indices $1 \leqslant i, j, k \leqslant n$.

Proposition 5.1. *Let Q be a quasigroup of order $n = pq$ for some positive integers p, q. Assume that Q it generated by the right shift and it has a left unit element. Then the Latin square of Q has q cycles of length p.*

Proof. Let $Q = \{x_1, \ldots, x_n\}$ and x_i a left unit element of Q. Then $x_i x_j = x_j$ for all $j = 1, \ldots, n$. Since Q is generated by a right shift $x_k x_k = x_1 x_1 = x_i$ for all k. Also for all $k, j > 1$ we have

$$x_k x_1 = x_{k-1} x_n, \quad x_k x_j = x_{k-1} x_{j-1}.$$

Since x_i is the left unit element for all $1 \leqslant k \leqslant q$ we have

$$x_{i+q \,(\mathrm{mod}\ n)} x_k = x_{i+q-k \,(\mathrm{mod}\ n)} x_n = x_i x_{n-q+k \,(\mathrm{mod}\ n)} = x_{n-q+k \,(\mathrm{mod}\ n)},$$

$$
\begin{aligned}
&x_{i+q\,(\mathrm{mod}\ n)}x_{n-q+k\,(\mathrm{mod}\ n)} = x_i x_{n-q+k-q\,(\mathrm{mod}\ n)} = x_{n-2q+k\,(\mathrm{mod}\ n)},\\
&x_{i+q\,(\mathrm{mod}\ n)}x_{n-2q+k\,(\mathrm{mod}\ n)} = x_i x_{n-2q+k-q\,(\mathrm{mod}\ n)} = x_{n-3q+k\,(\mathrm{mod}\ n)},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&x_{i+q\,(\mathrm{mod}\ n)}x_{n-(p-1)q+k\,(\mathrm{mod}\ n)} = x_i x_{n-pq+k\,(\mathrm{mod}\ n)} = x_k.
\end{aligned}
$$

It means that the permutation of the $(i+q\,(\mathrm{mod}\ n))$th row of the Latin square has q disjoint p-cycles. Recall that here x_i is the left unit, i.e. ith row of the Latin square is the identity permutation. □

Proposition 5.2. *Let Q be a finite quasigroup generated by the left shift and with a left or a right unit element. Then Q is commutative. In particular left and right units coincide.*

Proof. Let x_i be a left unit. Then for any $x_r, x_s \in Q$ we have

$$x_r x_s = x_i x_{s+r-i} = x_{r+s-i} = x_i x_{s+r-i} = x_s x_r.$$

The proof for the right unit x_i is the same. □

Similarly one can prove

Proposition 5.3. *Let Q be a quasigroup of order $n = pq$ for some positive integers p, q. Assume that Q is generated by the left shift and it has a unit element. Then the Latin square of Q has q cycles of length p.* □

Proposition 5.4. *Let Q be generated by a right shift and Q has a left unit. Suppose that $|Q| = n = pq$. Then the relation $x_a \sim x_b \iff a \equiv b \pmod q$ is a congruence in Q. Any congruence relation on Q can be obtained in this way.*

Proof. Let x_i be a left unit element of Q. By (13) for any integers $k, s, u, v \pmod n$ we have

$$x_{k+qu}x_{s+qv} = x_i x_{s+qv-k-qu+i\,(\mathrm{mod}\ n)} = x_{s+q(v-u)-k+i\,(\mathrm{mod}\ n)}.$$

So if we take elements $x_{k+qu'}, x_{s+qv'}$ equivalent to x_{k+qu}, x_{s+qv} then their product

$$x_{k+qu'}x_{s+qv'} = x_{s+q(v'-u')-k+i\,(\mathrm{mod}\ n)}$$

is equivalent to $x_{s+q(v-u)-k+i\,(\mathrm{mod}\ n)}$, because

$$s + q(v-u) - k + i \equiv s + q(v' + u') - k + i\,(\mathrm{mod}\ q).$$

Now suppose that $\wp$ is a congruence relation in Q. By Proposition 3.3 the class $\wp(x_i)$ of a left unit element x_i is a subquasigroup in Q. Suppose that this class has order greater then 1. Take the smallest integer $q > 0$ such that $x_{i+q} \in \wp(x_i)$. If $x_j \in \wp(x_i)$, then $x_{i+q}x_j = x_i x_{j-q} = x_{j-q} \in \wp(x_i)$. Hence it is easy to deduce that $\wp(x_i)$ consists of all elements x_{i+lq} for all $l \in \mathbb{Z}/n$.

We claim that $(x_m, x_s) \in \wp$ if and only if $m \equiv s \pmod q$. In fact by Proposition 3.3 we have $x_m = x_v x_s$, where $x_v \in \wp(x_i)$. Hence $v = i + lq$ and therefore $x_v x_s = x_{i+lq} x_s = x_i x_{s-lq} = x_{s-lq}$. So $m = s - lq \equiv s \pmod q$. Conversely let $x_{m+lq} = x_i x_{m+lq} = x_{i-lq} x_m \in \wp(x_i) x_m$. Hence $(x_{m+lq}, x_m) \in \wp$. □

Corollary 5.5. *Each of cycles from Proposition* 5.1 *form a congruence class of* Q*. Thus* Q *is not simple.*

Proof. Each of p-cycles from Proposition 5.1 coincides with a class from Proposition 5.4. □

Corollary 5.6. *If the Latin square of the quasigroup* Q *of order* $n = 4 = 2^2$ *which are of the above type, then* Q *has* 2 *disjoint* 2*-cycles.*

Proposition 5.7. *Let* Q *be a quasigroup of order* n *and it is generated by the right shift then the operations* xy, x/y *are equal if and only if there exists a left identity.*

Proof. Let $Q = \{x_1, \dots, x_n\}$ and x_i a left unit element. It means that $x_i x_j = x_j$ for all $j = 1, \dots, n$. In particular we have $x_1 x_1 = x_1$.

We need to prove that $x_k x_j = x_k / x_j$. It suffices to show that

$$(x_k x_j)\, x_j = (x_k / x_j)\, x_j.$$

In fact by the right shift property

$$\begin{aligned}(x_k x_j)\, x_j &= \big(x_{k-(k-i)} x_{j-(k-i)\,(\text{mod } n)}\big)\, x_j = \big(x_i x_{j-(k-i)\,(\text{mod } n)}\big)\, x_j \\ &= x_{j-(k-i)\,(\text{mod } n)} x_j = x_{j-(k-i)+(k-i)\,(\text{mod } n)} x_{j+(k-i)\,(\text{mod } n)} \\ &= x_j x_{j+(k-i)\,(\text{mod } n)} = x_{i+(j-i)} x_{k+(j-i)\,(\text{mod } n)} = x_i x_k \\ &= x_k = (x_k / x_j)\, x_j.\end{aligned}$$

Conversely assume that $x_k x_j = x_k / x_j$ for all indices $k, j = 1, \dots, n$. Put $x_i = x_k^2$ for all $k = 1, \dots, n$ by the right shift property.

We claim that x_i is a left unit element in Q.

By the assumption $(x_i x_j)\, x_j = (x_i / x_j)\, x_j = x_i$ and therefore $x_i x_j = x_j$ for all $j = 1, \dots, n$. Hence x_i is the left unit element. □

Corollary 5.8. *Let* Q *be a quasigroup of order* n *and it is generated by the left shift. The operations* $xy, x\backslash y$ *are equal if and only if there exists a unit. In this case by Propsition* 3.5 *we have* $x/y = y\backslash x$ *for all* x, y *and* x/x *is the unit element for all* x. □

Acknowledgement. Our heartiest thanks to Prof. Bimal K. Roy, Director of ISI, and Prof. Subahamoy Maitra, ASU, ISI for their kind support to make this research collaboration possible and for their hospitality.

We are thankful to Dr. P. K. Saxena, Director SAG, DRDO and Dr. S. S. Bedi, Associate Director SAG DRDO for their support to carry out this collaborative research work at ISI, Kolkata.

References

[1] **V. A. Artamonov**, *Polynomially complete algebras*, Sci. Notes Orlov State Univ., ser. natural, techn and med. sci., **6** (2012), part 2, 23 – 29.

[2] **V. A. Artamonov, S. Chakrabarti**, *Properties of algebras of primary order with one ternary Mal'tsev operation*, Algebra and Logic **34** (1995), 132 – 144.

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

[4] **G. B. Belyavskaya**, *T-quasigroups and the center of a quasigroup*, (Russian), Math. Issled. **3** (1989), 24 – 43.

[5] **J. Dénes, A. D. Keedwell**, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[6] **V. Dimitrova, S. Markovski, D. Gligoroski**, *Classification of quasigroups as Boolean functions, their algebraic complexity and application of Gröbner bases in solving systems of quasigroup equations*, Gröbner, Coding and Cryptography, Springer, 2007.

[7] **R. Freese, R. McKenzie**, *Commutator theory for congruence modular varieties*, London Math. Soc. Lecture Note Series, Vol. 125, Cambridge Univ. Press, 1987.

[8] **M. M. Glukhov**, *On a system of orthogonal quasigroups,* Scie. Notes Orlov state univ. (sci. journal) series natural , techn and med. sci., **6** (2012), part 2, 11 – 22.

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

[10] **T. Kepka T., P. Nemec**, *T-quasigroups*, Acta Univ. Carol. Math. et Phys. **12** (1971), 39 – 49.

[11] **V. A. Shcherbakov**, *On linear quasigroups and their automorphism groups*, (Russian), Mat. Issled. **120** (1991), 104 – 114.

[12] **V. A. Shcherbakov**, *Elements of quasigroup theory and some its applications in code theory and cryptology,* 2003, www.karlin.mff.cuni.cz/drapal/speccurs.pdf

[13] **J. D. H. Smith**, *An introduction to quasigroups and their representations*, Studies in Adv. Math. Chapman & Hall/CRC, Boca Raton, 2007.

Received February 10, 2013
Revised September 11, 2013

V.A.Artamonov
Department of Algebra, Faculty of Mechanics and Mathematics, Moscow State University, Russia
E-mail: artamon@mech.math.msu.su

S.Chakrabarty
Scientific Analysis Group, DRDO, India

S.Gangopadhyay
Department of Mathematics, Indian Institute of Technology Roorkee, India

S.K.Pal
Scientific Analysis Group, DRDO, India