BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(67), 2011, Pages 69–76
ISSN 1024–7696

On conjugate sets of quasigroups

Tatiana Popovich

Abstract. It is known that the set of conjugates (the conjugate set) of a binary quasigroup can contain 1, 2, 3 or 6 elements. We establish a connection between different pairs of conjugates and describe all six possible conjugate sets, with regard to the equality ("assembling") of conjugates. Four identities which correspond to the equality of a quasigroup to its conjugates are pointed out. Every conjugate set is characterized with the help of these identities. The conditions of the equality of a T-quasigroup to conjugates are established and some examples of T-quasigroups with distinct conjugate sets are given.

Mathematics subject classification: 20N05, 05B15.
Keywords and phrases: Quasigroup, T-quasigroup, conjugate, parastrophe, identity.

1 Introduction

A quasigroup is an ordered pair (Q, A) where Q is a set and A is a binary operation defined on Q such that each of the equations $A(a, y) = b$ and $A(x, a) = b$ is uniquely solvable for any pair of elements a, b in Q. It is known that the multiplication table of a finite quasigroup defines a Latin square and six (not necessarily distinct) conjugates (or parastrophes) are associated with each quasigroup (Latin square) [1, 3].

In [5] a connection between five identities of two variables and the equality of a quasigroup to some of the rest five its conjugates was established. It was also proved that the number of distinct conjugates in a finite quasigroup can be 1, 2, 3 or 6 and for any $m = 1, 2, 3, 6$ and any $n \geq 4$ there exists a quasigroup of order n with m distinct conjugates (see Theorem 6 of [5]).

We divide all pairs of conjugates of a quasigroup into four classes and consider six possible conjugate sets, with regard to the equality ("assembling") of conjugates. Four identities which correspond to these four classes (or to the equality of a quasigroup to its conjugates) are pointed out. It is proved that each of six conjugate sets can be described with the help of these identities and any two of these identities imply the rest two identities. The conditions of the equality of a T-quasigroup to its conjugates are established and some examples of T-quasigroups with distinct conjugate sets are given.

2 Preliminaries

Remind some necessary notions and results.

With any quasigroup (Q, A) the system $\Sigma(A)$ of six (not necessarily distinct) *conjugates (parastrophes)* is connected:

$$\Sigma(A) = (A, A^{-1}, {}^{-1}A, {}^{-1}\left(A^{-1}\right), ({}^{-1}A)^{-1}, A^*),$$

where $A(x, y) = z \Leftrightarrow A^{-1}(x, z) = y \Leftrightarrow {}^{-1}A(z, y) = x \Leftrightarrow A^*(y, x) = z$.

Using the suitable Belousov's designation of conjugates of a quasigroup (Q, A) of [2] we have the following conjugate system $\Sigma(A)$:

$$\Sigma(A) = (A,\ {}^{r}\!A,\ {}^{l}\!A,\ {}^{lr}\!A,\ {}^{rl}\!A,\ {}^{s}\!A),$$

where ${}^{r}\!A = A^{-1}$, ${}^{l}\!A = {}^{-1}A$, ${}^{lr}\!A = {}^{-1}(A^{-1})$, ${}^{rl}\!A = ({}^{-1}\!A)^{-1}$, ${}^{s}\!A = A^*$.

Note that

$$\left({}^{-1}(A^{-1})\right)^{-1} = {}^{rlr}\!A = {}^{-1}\left(({}^{-1}\!A)^{-1}\right) = {}^{lrl}\!A = {}^{s}\!A$$

and ${}^{rr}\!A = {}^{ll}\!A = A$, ${}^{\sigma\tau}\!A = {}^{\sigma}({}^{\tau}\!A)$.

Let $\overline{\Sigma}(A)$ be the set of conjugates (*the conjugate set*) of a quasigroup (Q, A).

It is known from [5] that $\mid \overline{\Sigma}(A) \mid = 1,2,3$ or 6.

A quasigroup is a totally-symmetric quasigroup (a TS-quasigroup) if $\mid \overline{\Sigma}(A) \mid = 1$.

3 Conjugates of quasigroups

We start with the following useful result concerning the (unordered) pairs of conjugates of a quasigroup.

Proposition 1. *All pairs of conjugates of the conjugate system* $\Sigma(A)$ *of a quasigroup* (Q, A) *can be divided into four disjoint classes:*

I. $(A, {}^{r}\!A)$, $({}^{l}\!A, {}^{lr}\!A)$, $({}^{rl}\!A, {}^{s}\!A)$;

II. $(A, {}^{l}\!A)$, $({}^{r}\!A, {}^{rl}\!A)$, $({}^{s}\!A, {}^{lr}\!A)$;

III. $(A, {}^{s}\!A)$, $({}^{r}\!A, {}^{lr}\!A)$, $({}^{l}\!A, {}^{rl}\!A)$;

IV. $({}^{l}\!A, {}^{r}\!A)$, $(A, {}^{lr}\!A)$, $({}^{r}\!A, {}^{s}\!A)$, $({}^{lr}\!A, {}^{rl}\!A)$, $(A, {}^{rl}\!A)$, $({}^{l}\!A, {}^{s}\!A)$

such that the equality (inequality) of components of one pair in a class implies the equality (inequality) of components of any pair in this class.

Proof. There are 15 unordered pairs of conjugates of a quasigroup. It is easy to check that if we take any conjugate of the operations in a pair of any class of I, II, III or IV , then we obtain some pair from the same class. For example, if we apply the conjugations r, l, rl, lr and s to the operations of the pair $({}^{l}\!A, {}^{lr}\!A)$ of class I, we obtain, respectively, the pairs of conjugates $({}^{rl}\!A, {}^{s}\!A)$, $(A, {}^{r}\!A)$, $({}^{r}\!A, A)$, $({}^{s}\!A, {}^{rl}\!A)$, $({}^{lr}\!A, {}^{l}\!A)$ of class I. Here we take into account that ${}^{rllr}\!A = A$, ${}^{lrl}\!A = {}^{s}\!A$, ${}^{lrlr}\!A = {}^{rlrr}\!A = {}^{rl}\!A$ and ${}^{slr}\!A = {}^{lrllr}\!A = {}^{l}\!A$. Analogously, the conjugations can be applied to the rest two pairs of class I and to the every pair of other classes.

Thus, any class pointed out in the proposition is closed with respect to taking the same conjugate of both operations in a pair from this class. □

Proposition 2. *If the components of pairs from any two classes of I, II, III, IV coincide for a quasigroup (Q, A), then the components of every pair of all classes coincide and (Q, A) is a TS-quasigroup.*

Proof. According to Proposition 1 for the proof we can take any pair of a class.

I, II: Let $A = {}^{r}A$ and $A = {}^{l}A$, then ${}^{l}A = {}^{r}A$ (it gives a pair of IV) and ${}^{s}A = {}^{rlr}A = {}^{r}A = A$ where $(A, {}^{s}A)$ is a pair of III.

I, III: If $A = {}^{r}A$ and $A = {}^{s}A$, then ${}^{r}A = {}^{s}A$ (it corresponds to a pair of IV); the last and the second equalities imply $A = {}^{lr}A = {}^{s}A$ (we obtain a pair $({}^{s}A, {}^{lr}A)$ of II).

I, IV: Let $A = {}^{r}A$ and ${}^{l}A = {}^{r}A$, then $A = {}^{l}A$ and we have a pair of II, so ${}^{r}A = {}^{rl}A$, and ${}^{l}A = {}^{rl}A$ (a pair of III).

III, IV: If $A = {}^{s}A$ and ${}^{l}A = {}^{s}A$, then $A = {}^{l}A$ (a pair of II). Let $A = {}^{s}A$ and ${}^{r}A = {}^{s}A$, then $A = {}^{r}A$ (a pair of I).

Analogously the rest cases can be considered. In every case all conjugates coincide, so (Q, A) is a TS-quasigroup. □

The following theorem describes all possible conjugate sets for quasigroups and points out the only possible variants of the equality ("assembling") of conjugates in every case.

Theorem 1. *The following conjugate sets of a quasigroup (Q, A) are only possible:*
$\overline{\Sigma}_1(A) = \{A\}$;
$\overline{\Sigma}_2(A) = \{A, {}^{s}A\} = \{A = {}^{lr}A = {}^{rl}A,\ {}^{l}A = {}^{r}A = {}^{s}A\}$;
$\overline{\Sigma}_6(A) = \{A,\ {}^{r}A,\ {}^{l}A,\ {}^{lr}A,\ {}^{rl}A,\ {}^{s}A\}$;
$\overline{\Sigma}_3(A) = \{A, {}^{lr}A, {}^{rl}A\}$ *and three cases are possible:*
$\overline{\Sigma}_3^1(A) = \{A = {}^{r}A,\ {}^{l}A = {}^{lr}A,\ {}^{rl}A = {}^{s}A\}$;
$\overline{\Sigma}_3^2(A) = \{A = {}^{l}A,\ {}^{r}A = {}^{rl}A,\ {}^{lr}A = {}^{s}A\}$;
$\overline{\Sigma}_3^3(A) = \{A = {}^{s}A,\ {}^{r}A = {}^{lr}A,\ {}^{l}A = {}^{rl}A\}$.

Proof. It follows from Proposition 1 that if the components of pairs of all classes I, II, III, IV (or by Proposition 2 at least any of two classes) coincide then all conjugates coincide and (Q, A) is a TS-quasigroup.

If the components of pairs from all classes do not coincide, then all conjugates of (Q, A) are different and $\overline{\Sigma}(A) = \overline{\Sigma}_6(A)$. In the rest cases by Proposition 2 we have exactly one of the groups of conjugate equalities:

I'. $A = {}^{r}A$, ${}^{l}A = {}^{lr}A$, ${}^{rl}A = {}^{s}A$;
II'. $A = {}^{l}A$, ${}^{r}A = {}^{rl}A$, ${}^{lr}A = {}^{s}A$;
III'. $A = {}^{s}A$, ${}^{r}A = {}^{lr}A$, ${}^{l}A = {}^{rl}A$;
IV'. $A = {}^{lr}A = {}^{rl}A$, ${}^{l}A = {}^{r}A = {}^{s}A$.

Moreover, different equalities in a group do not "assemble": if some conjugate of one equality from a group coincides with a conjugate from another equality of this group, then new equalities arise from the group of equalities corresponding to another class of pairs. So by Proposition 2 all six conjugates of the quasigroup coincide. Thus, in each of these cases there are exactly two (see equality group IV') or three (every of equality groups I', II' and III') distinct conjugates. Note that every equality group of I', II', III' contains conjugates A, ${}^{lr}A$ and ${}^{rl}A$, but there are distinct variants of their "assembling" with the rest conjugates which give the conjugate sets $\overline{\Sigma}_3^1(A)$, $\overline{\Sigma}_3^2(A)$ and $\overline{\Sigma}_3^3(A)$ respectively. □

From Proposition 1 and Theorem 1 follows immediately

Corollary 1. *Let $\overline{\Sigma}(A)$ be the conjugate set of a quasigroup (Q,A), then $\mid \overline{\Sigma}(A) \mid = 1$ or 3 in the case of the coincidence of the components of a pair in any of classes I, II, III and $\mid \overline{\Sigma}(A) \mid = 1$ or 2 by coincidence of the components of a pair in class IV. For a commutative quasigroup $\mid \overline{\Sigma}(A) \mid = 1$ or 3.*

Corollary 2. *If (Q,A) is a commutative quasigroup, then $\overline{\Sigma}(A) = \overline{\Sigma}_1(A)$ or $\overline{\Sigma}_3^3(A)$. For a noncommutative quasigroup $\overline{\Sigma}(A) = \overline{\Sigma}_2(A), \overline{\Sigma}_6(A), \overline{\Sigma}_3^1(A)$ or $\overline{\Sigma}_3^2(A)$.*

Proof. Indeed, for a commutative quasigroup we have $A =^s A$, it corresponds to the equality group III'. If it corresponds only to the equality group III', then $\overline{\Sigma}(A) = \overline{\Sigma}_3^3(A)$. If there are equalities of another group, then by Proposition 2 $\overline{\Sigma}(A) = \overline{\Sigma}_1(A)$. The rest conjugate sets are possible only for a noncommutative quasigroup. □

Let $\overline{\Sigma}(A) = \{A_1, A_2, ..., A_i\}$, $i = 1, 2, 3$ or 6, be the conjugate set of a quasigroup (Q,A) and ${}^\sigma\overline{\Sigma}(A) = \{{}^\sigma A_1, {}^\sigma A_2, ..., {}^\sigma A_i\}$ where σ is some conjugation of a quasigroup (Q,A).

Proposition 3. *Let σ be any conjugation of (Q,A). Then ${}^\sigma\overline{\Sigma}(A) = \overline{\Sigma}(A)$. If $\overline{\Sigma}(A) = \overline{\Sigma}_1, \overline{\Sigma}_2(A)$ or $\overline{\Sigma}_6(A)$, then $\overline{\Sigma}(A) = \overline{\Sigma}({}^\sigma A)$. If $\overline{\Sigma}(A) = \overline{\Sigma}_3(A)$, then $\mid \overline{\Sigma}(A) \mid = \mid \overline{\Sigma}({}^\sigma A) \mid$.*

Proof. The equality ${}^\sigma\overline{\Sigma}(A) = \overline{\Sigma}(A)$ follows from Proposition 1 as any class pointed out in this proposition is closed with respect to taking the same conjugate of both operations in a pair from this class.

If $\overline{\Sigma}(A) = \overline{\Sigma}_1(A) = \{A\}$, then $\overline{\Sigma}({}^\sigma A) = \overline{\Sigma}(A)$ since ${}^\sigma A = A$ for any σ. Let $\overline{\Sigma}(A) = \overline{\Sigma}_2(A) = \{A = {}^{lr}A = {}^{rl}A, {}^lA = {}^rA = {}^sA\} = \{A, {}^sA\}$, then these equalities can be written via the operation ${}^rA$ in the following way: $\overline{\Sigma}(A) = \{{}^r({}^rA) = {}^l({}^rA) = {}^s({}^rA), {}^{lr}({}^rA) = {}^rA = {}^{rl}({}^rA)\} = \overline{\Sigma}_2({}^rA)$. Analogously each of the rest conjugates can be used.

It is evident that if $\overline{\Sigma}(A) = \overline{\Sigma}_6(A)$, then analogous passage from A to ${}^\sigma A$ gives all six distinct conjugates.

In the case $\overline{\Sigma}(A) = \overline{\Sigma}_3(A) = \overline{\Sigma}_3^i(A)$ for some $i = 1, 2, 3$ writing corresponding equalities via ${}^\sigma A$ we obtain also three pairs of equal conjugates. But these pairs can correspond to $\overline{\Sigma}_3^j({}^\sigma A)$ where $i \neq j$. For example, let $\overline{\Sigma}(A) = \overline{\Sigma}_3^2(A) = \{A = {}^lA, {}^rA = {}^{rl}A, {}^{lr}A = {}^sA\}$ or using the conjugate ${}^rA$ we obtain $\overline{\Sigma}(A) = \{{}^r({}^rA) = {}^{lr}({}^rA), {}^rA = {}^s({}^rA), {}^l({}^rA) = {}^{rl}({}^rA)\} = \overline{\Sigma}({}^rA) = \{{}^rB = {}^{lr}B, B = {}^sB, {}^lB = {}^{rl}B\}$ where ${}^rA = B$. Thus, $\overline{\Sigma}(A) = \overline{\Sigma}_3^2(A) = \overline{\Sigma}_3^3({}^rA)$. □

Using Proposition 1 we obtain (see also Theorem 4 of [5]) the following

Proposition 4. *The components of any pair of a class of Proposition 1 coincide if and only if a quasigroup (Q,A) satisfies the identity*

$A(x, A(x,y)) = y$ *for class I;*

$A(A(y,x),x) = y$ *for class II;*
$A(x,y) = A(y,x)$ *for class III;*
$A(A(x,y),x) = y$ *for class IV.*

Proof. It is known that the identities $A(x, A(y,x)) = y$ and $A(A(x,y),x) = y$ are equivalent (see, for example, [3], p. 61). This fact follows also from Proposition 1 since the components of the pairs $({}^rA, {}^sA)$ and $({}^lA, {}^sA)$, giving equivalence of these identities, coincide simultaneously (see class IV).

I. By the definition of the conjugate ${}^rA(x,y)$ we have that $A(x,y) = {}^rA(x,y)$ if and only if $A(x, A(x,y)) = y$.

II. Analogously, $A(x,y) = {}^lA(x,y)$ if and only if $A(A(x,y),y) = x$ or $A(A(y,x),x) = y$.

III. $A = {}^sA$ means that $A(x,y) = A(y,x)$.

IV. ${}^rA = {}^sA$ (taking into account Proposition 1 we can take the last pair of class IV) if and only if $A(x, A(y,x)) = y$. But this identity is equivalent to the identity $A(A(x,y),x) = y$, as it was noted above. □

From Propositions 2 and 4 it follows immediately

Corollary 3. *Any two identities of four identities of Proposition 4 imply the rest two identities.*

In Theorem 4 of [5] it was shown that $\mid \overline{\Sigma}(A) \mid = 1$ if and only if in a quasigroup (Q, A) all five identities of the set $T = \{A(x, A(x,y)) = y, A(A(y,x),x) = y, A(x,y) = A(y,x), A(x, A(y,x)) = y, A(A(x,y),x) = y\}$ (corresponding to the equality of a quasigroup to one of its conjugates) are fulfilled,

it is 2 if and only if (Q, A) satisfies exactly 2 of the identities,

it is 3 if and only if (Q, A) satisfies exactly one of the identities,

it is 6 if and only if (Q, A) satisfies none of the identities.

In this case (and below) we assume that a quasigroup satisfies exactly k identities of a set of identities if it satisfies k identities and does not satisfy the rest identities of this set. Let $\overline{T} = \{A(x, A(x,y)) = y,\ A(A(y,x),x) = y,\ A(x,y) = A(y,x),\ A(A(x,y),x) = y\}$ be the set of identities of Proposition 4.

Taking into account the previous results we obtain the following result making more precise Theorem 4 of [5]:

Corollary 4. *Let (Q, A) be a quasigroup, then*
$\overline{\Sigma}(A) = \overline{\Sigma}_1(A)$ *if and only if any two identities of $\overline{T}$ are fulfilled;*
$\overline{\Sigma}(A) = \overline{\Sigma}_2(A)$ *if and only if exactly the identity $A(A(x,y),x) = y$ of $\overline{T}$ is fulfilled;*
$\overline{\Sigma}(A) = \overline{\Sigma}_3^1(A)$ *if and only if exactly the identity $A(x, A(x,y)) = y$ of $\overline{T}$ is fulfilled;*
$\overline{\Sigma}(A) = \overline{\Sigma}_3^2(A)$ *if and only if exactly the identity $A(A(y,x),x) = y$ of $\overline{T}$ is fulfilled;*
$\overline{\Sigma}(A) = \overline{\Sigma}_3^3(A)$ *if and only if exactly the identity $A(x,y) = A(y,x)$ of $\overline{T}$ is fulfilled;*
$\overline{\Sigma}(A) = \overline{\Sigma}_6(A)$ *if and only if (Q, A) satisfies none of four identities of $\overline{T}$.*

Proof. Let $\mid \overline{\Sigma}(A) \mid = m$. By Corollary 3 any two identities of $\overline{T}$ imply the rest ones, so by Proposition 2 the components of any pair of each class of Proposition 1 coincide. In this case all conjugates coincide, thus, $m = 1$.

Conversely, in a TS-quasigroup all conjugates coincide, so by Proposition 4 this quasigroup satisfies all identities of $\overline{T}$.

By Theorem 1 $m = 2$ can be only for class IV of pairs. The identity $A(A(x, y), x) = y$ corresponds to this class by Proposition 4.

The case $m = 3$ by Theorem 1 can be for the every of classes I,II and III. The identities $A(x, A(x, y)) = y$, $A(A(y, x), x) = y$, $A(x, y) = A(y, x)$ correspond to these classes, respectively, according to Proposition 4.

At last, $m = 6$ if components of any pair of all pairs in Proposition 1 do not coincide. That means that the quasigroup satisfies none of the four identities of Proposition 4. □

4 Conjugates of T-quasigroups

A quasigroup (Q, A) is *a T-quasigroup* if there exist an abelian group $(Q, +)$, its automorphisms φ, ψ and an element $c \in Q$ such that $A(x, y) = \varphi x + \psi y + c$ for any $x, y \in Q$ [4].

The conjugates of a T-quasigroup $A(x, y) = \varphi x + \psi y + c$ (which are also T-quasigroups) have the following form: ${}^{s}A(x, y) = \psi x + \varphi y + c$, ${}^{r}A(x, y) = \psi^{-1}(y - \varphi x - c)$, ${}^{l}A(x, y) = \varphi^{-1}(x - \psi y - c)$, ${}^{rl}A(x, y) = \psi^{-1}(x - \varphi y - c)$, ${}^{lr}A(x, y) = \varphi^{-1}(y - \psi x - c)$ where $Ix = -x$ (see, for example, [6]). Note that $I\varphi = \varphi I$ for any automorphism φ of a group.

An operation A of the form $A(x, y) = ax + by \pmod n$, $n \geq 2$, is a T-quasigroup if and only if the numbers a, b modulo n are relatively prime to n. In this case $\varphi = L_a$, $\psi = L_b$, where $L_a x = ax \pmod n$, $x \in Q = \{0, 1, 2, \ldots, n - 1\}$, are permutations (automorphisms of the additive group modulo n). For these quasigroups the conjugates have the following form:

${}^{s}A(x, y) = L_b x + L_a y \pmod n$, ${}^{r}A(x, y) = L_b^{-1}(y - L_a x) \pmod n$,
${}^{l}A(x, y) = L_a^{-1}(x - L_b y) \pmod n$, ${}^{rl}A(x, y) = L_b^{-1}(x - L_a y) \pmod n$,
${}^{lr}A(x, y) = L_a^{-1}(y - L_b x) \pmod n$.

Theorem 2. *The components of any pair of a class I, II, III or IV for a T-quasigroup (Q, A): $A(x, y) = \varphi x + \psi y$ coincide if and only if*

$\psi = I$ *for class I;*

$\varphi = I$ *for class II;*

$\varphi = \psi$ *for class III;*

$\varphi^2 = I\psi$ *and* $\psi^2 = I\varphi$ *(or $\varphi = \psi^{-1}$ and $\varphi^3 = I$) for class IV.*

Proof. I. Let $A = {}^{r}A$, then

$$\varphi x + \psi y = I\psi^{-1}\varphi x + \psi^{-1} y = \psi^{-1}(y - \varphi x). \tag{1}$$

For $y = 0$ (0 is the identity element of the group $(Q, +)$) we have $\varphi x = I\psi^{-1}\varphi x$ and $\psi = I$.

II. Let $A = {}^{l}\!A$, then

$$\varphi x + \psi y = \varphi^{-1}(x - \psi y), \tag{2}$$

whence for $x = 0$ it follows $\varphi = I$.

III. If $A = {}^{s}\!A$, then $\psi x + \varphi y = \varphi x + \phi y$, whence $\varphi = \psi$ for $x = 0$.

IV. Let ${}^{l}\!A = {}^{r}\!A$, then

$$\psi^{-1}(y - \varphi x) = \varphi^{-1}(x - \psi y). \tag{3}$$

Taking $x = 0$ we have $\psi^{-1}y = I\varphi^{-1}\psi y$, $\psi^2 = I\varphi$. If $y = 0$, then $\varphi^{-1}x = I\psi^{-1}\varphi x$ and so $\varphi^2 = I\psi$.

Note that the second pair of equalities in the theorem for the pairs of IV is equivalent to the first one: from $\varphi^2 = I\psi$ and $\psi^2 = I\varphi$ it follows that $\varphi^4 = \psi^2 = I\varphi$, whence $\varphi^3 = I$ and so $\psi^{-1} = I\varphi^{-2} = \varphi$. Conversely, if $\varphi = \psi^{-1}$ and $\varphi^3 = I$, then $\varphi^2 = I\varphi^{-1} = I\psi$ and $\psi^2 = \varphi^4 = I\varphi$.

Now check sufficiency of the conditions. Let $\psi = I$, then $\varphi x + Iy = Iy + \varphi x$, that is we obtain (1) and $A = {}^{r}\!A$.

If $\varphi = I$, then $Ix + \psi y = I(x - \psi y)$. It is (2), so $A = {}^{l}\!A$. It is evident that if $\varphi = \psi$, then $A = {}^{s}\!A$.

At last, let $\varphi^2 = I\psi$ and $\psi^2 = I\varphi$. Show that ${}^{l}\!A = {}^{r}\!A$, that is (3) holds. Indeed, $\psi^{-1}(y - \varphi x) = I\varphi^{-2}(y - \varphi x) = I\varphi^{-2}y + \varphi^{-1}x$. But $\varphi^{-1}(x - \psi y) = \varphi^{-1}x + \varphi y = \varphi^{-1}x + I\varphi^{-2}y$ as $\varphi^3 = I$ (it was shown above) and (3) is true. □

From Proposition 2 and Theorem 2 it follows

Corollary 5. *The conditions of Theorem 2 for any two classes of I, II, III, IV define a TS-T-quasigroup.*

Corollary 6. *If in Theorem 2 $A(x, y) = ax + by$ (mod n), then the conjugates of the T-quasigroup in a class of I, II, III or IV have the form:*

I. $A(x, y) = {}^{r}\!A(x, y) = ax + (n-1)y$ *(mod n)*, ${}^{l}\!A(x, y) = {}^{lr}\!A(x, y) = a^{-1}x + a^{-1}y$ *(mod n) and* ${}^{rl}\!A(x, y) = {}^{s}\!A(x, y) = (n-1)x + ay$ *(mod n)*;

II. $A(x, y) = {}^{l}\!A(x, y) = (n-1)x + by$ *(mod n)*, ${}^{r}\!A(x, y) = {}^{rl}\!A(x, y) = b^{-1}x + b^{-1}y$ *(mod n) and* ${}^{lr}\!A(x, y) = {}^{s}\!A(x, y) = bx + (n-1)y$ *(mod n)*;

III. $A(x, y) = {}^{s}\!A(x, y) = ax + ay$ *(mod n)*, ${}^{r}\!A(x, y) = {}^{lr}\!A(x, y) = (n-1)x + a^{-1}y$ *(mod n) and* ${}^{l}\!A(x, y) = {}^{rl}\!A(x, y) = a^{-1}x + (n-1)y$ *(mod n)*;

IV. $A(x, y) = {}^{lr}\!A(x, y) = {}^{rl}\!A(x, y) = ax + a^{-1}y$ *(mod n) and* ${}^{s}\!A(x, y) = {}^{l}\!A(x, y) = {}^{r}\!A(x, y) = a^{-1}x + ay$ *(mod n)*.

Proof. Follows from Proposition 1 and Theorem 2 if to take into account the form of a T-quasigroup, of its conjugates and that in this case $I = L_{n-1}$. For example, in class I: $A(x, y) = {}^{r}\!A(x, y) = ax + Iy = ax + (n-1)y$ (mod n), ${}^{l}\!A(x, y) = {}^{lr}\!A(x, y) = L_a^{-1}(y - Ix) = a^{-1}x + a^{-1}y$ (mod n). The rest cases are checked analogously. Note that in this case a, b modulo n are relatively prime to n, so they are invertible and belong to the multiplicative group of the residue-class ring (mod n). This multiplicative group consists of all numbers from 1 to $n - 1$ relatively prime to n. In this case $L_a^{-1}x = L_{a^{-1}}x$ (mod n). □

Examples. Using Corollary 6 we obtain that the operations $A_1(x,y) = 2x{+}4y$ (mod 5), $A_2(x,y) = 6x+4y$ (mod 7), $A_3(x,y) = 4x+4y$ (mod 9) define quasigroups with three different conjugates: $\overline{\Sigma}(A_1) = \overline{\Sigma}_3^1(A_1)$, $\overline{\Sigma}(A_2) = \overline{\Sigma}_3^2(A_2)$, $\overline{\Sigma}(A_3) = \overline{\Sigma}_3^3(A_3)$. The operation $A_4(x,y) = 2x+5y$ (mod 9) defines a quasigroup with two different conjugates: $\overline{\Sigma}(A_4) = \overline{\Sigma}_2(A_4)$.

For the operation A_1 these conjugates have the following form:

$A_1(x,y) = {}^{r}A_1(x,y) = 2x + 4y$ (mod 5), ${}^{l}A_1(x,y) = {}^{lr}A_1(x,y) = 3x + 3y$ (mod 5), ${}^{rl}A_1(x,y) = {}^{s}A_1(x,y) = 4x + 2y$ (mod 5) and are given by the following Cayley Tables:

A_1	0	1	2	3	4
0	0	4	3	2	1
1	2	1	0	4	3
2	4	3	2	1	0
3	1	0	4	3	2
4	3	2	1	0	4

Tab. 1

${}^{l}A_1$	0	1	2	3	4
0	0	2	4	1	3
1	4	1	3	0	2
2	3	0	2	4	1
3	2	4	1	3	0
4	1	3	0	2	4

Tab. 2

${}^{s}A_1$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

Tab. 3

References

[1] Belousov V. D. *Foundations of the quasigroup and loop theory*, Moscow, Nauka, 1967 (in Russian).

[2] Belousov V. D. *Parastrophic-orthogonal quasigroups*, Quasigroups and related systems, 2005, **13**, No. 1, 25–72.

[3] Dénes J., Keedwell A. D. *Latin squares and their applications*, Académiai Kiado, Budapest and Academic Press, New York, 1974.

[4] Kepka T., Nemec P. *T-quasigroups. I*, Acta Universitatis. Carolinae. Math. et Phys., 1971, **12**, No. 1, 39–49.

[5] Lindner C. C., Steedly D. *On the number of conjugates of a quasigroup*, Algebra Univ., 1975, **5**, 191–196.

[6] Mullen G., Shcherbacov V. *On orthogonality of binary operations and squares*, Buletinul Academiei de Ştiinţe a Republicii Moldova, Matematica, 2005, No. 2(48), 3–42.

Tatiana Popovich
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD-2028 Chişinău
Moldova
E-mail: *tanea-popovici@mail.ru*

Received March 30, 2011