BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(59), 2009, Pages 22–30
ISSN 1024–7696

Conjugate-orthogonality and the complete multiplication group of a quasigroup

G. Belyavskaya, A. Diordiev *

Abstract. In this note we establish connections between the orthogonality of conjugates of a finite or infinite quasigroup and some strictly transitive subsets of the complete multiplication group of this quasigroup. These connections are used for the investigation of orthogonality of distinct pairs of conjugates for quasigroups (loops) from some classes. For finite quasigroups the quasi-identities corresponding to orthogonality of pairs of conjugates are given.

Mathematics subject classification: 20N05, 20N15.
Keywords and phrases: Quasigroup, loop, primitive quasigroup, quasi-identity, multiplication group, conjugate, parastrophe, conjugate-orthogonality.

1 Introduction

A quasigroup is an ordered pair $(Q, \cdot)$ (or (Q, A)) where Q is a set and $(\cdot)$ (or (A)) is a binary operation on Q such that each of the equations $ay = b$ and $xa = b$ 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, 12].

Two quasigroups (Q, A) and (Q, B) defined on a set Q are orthogonal if the system of equations $\{A(x, y) = a, B(x, y) = b\}$ is uniquely solvable for all $a, b \in Q$. The notion of orthogonality plays an important role in the theory of Latin squares, also in the quasigroup theory and in distinct applications.

There is significant interest in the investigation of quasigroups which are orthogonal to some their conjugates or two conjugates of which are orthogonal (so called conjugate-orthogonal or parastrophic-orthogonal quasigroups).

Many articles were devoted to the investigation of various aspects of conjugate-orthogonal quasigroups. Recall some of them. In [5, 7–9, 11, 16] the spectrum of conjugate-orthogonal quasigroups (Latin squares) was studied.

Different identities associated with the conjugate-orthogonality and related combinatorial designs were considered in [4, 6, 13]. In particular, F. E. Bennet in [6] investigated the spectrum of the varieties of quasigroups with every one of eight short conjugate-orthogonal identities (short two-variable identities).

*The first author was partially supported by the grant 08.820.08.08 RF.

F. E. Bennet and H. Zhang [10] considered a problem related to the spectrum of Latin squares where each conjugate is required to be orthogonal to precisely its transpose from among the other five conjugates.

In [5,15] some quasi-identities of finite parastrophic-orthogonal quasigroups were established.

In this paper we study properties of multiplication groups of conjugate-orthogonal quasigroups. In particular, we prove that some strictly transitive subset of the complete multiplicative group of a quasigroup corresponds to orthogonality of any two from six conjugates of this quasigroup. We also give some quasi-identities related to the orthogonality of two conjugates of a finite quasigroup (Q, A). The use of a criterion of conjugate-orthogonality in the strictly transitive subset language allows easily to obtain a number of useful statements with respect to the conjugate-orthogonality of quasigroups and loops from some classes.

2 Preliminaries

A quasigroup $(Q, \cdot)$ is finite of order n if the set Q is finite and $|Q| = n$.

A quasigroup with *the left (right) identity* f (e) is a quasigroup $(Q, \cdot)$ such that $fx = x$ $(xe = x)$ for every $x \in Q$. A *loop* is a quasigroup $(Q, \cdot)$ with the identity $e\colon xe = ex = x$ for each $x \in Q$ [1].

A loop $(Q, \cdot)$ is called *a Moufang loop* if it satisfies the identity $(zx \cdot y)x = z(x \cdot yx)$ [1].

A quasigroup is called *an IP-quasigroup* if there exist maps (permutations) I_r and I_l such that $(yx) \cdot I_r x = y$, $I_l x \cdot (xy) = y$ for any $x, y \in Q$ [1].

The permutations L_a, R_a and I_a defined by $L_a x = ax$, $R_a x = xa$ and $x \cdot I_a x = a$ for all $x \in Q$ are called the *left*, *right* and *middle translations* of a quasigroup $(Q, \cdot)$ respectively [1,3].

The multiplication group or the group associated with M or $M_{(\cdot)}$ of a quasigroup $(Q, \cdot)$ (or the group associated with a quasigroup $(Q, \cdot)$) is the group generated by all left and all right translations of $(Q, \cdot)$: $M =< L_a, R_a \,|\, a \in Q >$ [1].

The complete multiplication group $\overline{M}$ (or the complete group associated with a quasigroup $(Q, \cdot)$ [3]) is the group generated by all left, right and middle translations of this quasigroup: $\overline{M} =< L_a, R_a, I_a \,|\, a \in Q >$. It is evident that $M \subseteq \overline{M}$.

With any quasigroup $(Q, \cdot)$ the system Σ of six (not necessarily distinct) *conjugates (parastrophes)* is associated:

$$\Sigma = \left\{(\cdot), (\cdot)^{-1} = (\backslash), {}^{-1}(\cdot) = (/), {}^{-1}\left((\cdot)^{-1}\right), \left({}^{-1}(\cdot)\right)^{-1}, (*)\right\},$$

where $x \cdot y = z \Leftrightarrow x\backslash z = y \Leftrightarrow z/y = x \Leftrightarrow y * x = z$.

It is known [14] that the number of different conjugates in Σ can be 1,2,3 or 6.

If a quasigroup operation is denoted by A, then a quasigroup (Q, A) (or simply A) has the following system Σ of conjugates:

$$\Sigma = \left\{A, {}^{r}A, {}^{l}A, {}^{lr}A, {}^{rl}A, {}^{s}A\right\}.$$

Here we use very suitable designation of conjugates of V. D. Belousov from [4], where

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

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

Note that

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

and ${}^{rr}A = {}^{ll}A = A$.

In general $M_{(\cdot)} \neq M_{\sigma(\cdot)}$, where ${}^{\sigma}(\cdot)$ is some conjugate of $(\cdot)$. But V. D. Belousov proved that the complete multiplication group $\overline{M}_{(\cdot)}$ is always invariant with respect to conjugacy as according to [3]

$$ \overline{M}_{r(\cdot)} = < L_a^{-1}, I_a, R_a >, \quad \overline{M}_{l(\cdot)} = < I_a^{-1}, R_a^{-1}, L_a^{-1} >, $$

$$ \overline{M}_{lr(\cdot)} = < R_a^{-1}, I_a^{-1}, L_a >, \quad \overline{M}_{rl(\cdot)} = < I_a, L_a^{-1}, R_a^{-1} >, $$

$$ \overline{M}_{s(\cdot)} = < R_a, L_a, I_a^{-1} > \text{ for all } a \in Q. $$

A quasigroup operation $(\cdot)$ and its inverse operations $(\backslash)$ and $(/)$ are connected by the identities:

$$ x(x\backslash y) = y, \quad x\backslash xy = y, \quad (y/x)x = y, \quad yx/x = y. $$

The quasigroup $(Q, \cdot, \backslash, /)$ is called the *primitive quasigroup* corresponding to a quasigroup $(Q, \cdot)$ [1].

Let Q be a finite or infinite set, A, B be operations on Q, then the right, left multiplications $A \cdot B$, $A \circ B$ of Mann are defined in the following way [2]:

$$ (A \cdot B)(x,y) = A(x, B(x,y)), \quad (A \circ B)(x,y) = A(B(x,y), y). $$

If A and B are quasigroups, then $A \cdot B$ $(A \circ B)$ is always *invertible from the right (from the left)*, that is the equation $(A \cdot B)(a,y) = b$ $((A \circ B)(x,a) = b)$ has a unique solution.

According to *the criterion of Belousov* [2] two quasigroups (Q, A) and (Q, B) are orthogonal (shortly, $A \perp B$) if and only if the operation $A \cdot {}^{r}B$ $(A \circ {}^{l}B)$ is a quasigroup.

3 Orthogonality of a quasigroup to its conjugates and strictly transitive subsets of the multiplication group

Recall that the set S of maps on a set Q is called *strictly transitive* (more precisely, the set S acts on Q strictly transitively) if for any pair of elements $(a,b) \in Q^2$ there exists a unique map α of S such that $\alpha a = b$.

Let (Q, A) be a quasigroup and $(Q, {}^{\sigma}A)$ be its conjugate. It is evident that the sets $\{L_a \mid a \in Q\}$ and $\{R_a \mid a \in Q\}$, where L_a, R_a are translations of A $({}^{\sigma}A)$, form strictly transitive subsets in the multiplication group M_A of the respective quasigroup.

We shall show that some strictly transitive subset of the multiplicative group M_A corresponds to the orthogonality $A \perp^{\sigma} A$.

It is easy to see that if $A \perp B$, then ${}^{s}A \perp^{s} B$, so we have the following

Proposition 1. *Let (Q, A) be a quasigroup. Then*

$$A \perp^{r} A \Leftrightarrow {}^{s}A \perp^{rl} A, \qquad A \perp^{l} A \Leftrightarrow {}^{s}A \perp^{lr} A, \qquad A \perp^{rl} A \Leftrightarrow {}^{s}A \perp^{r} A,$$

$$A \perp^{lr} A \Leftrightarrow {}^{s}A \perp^{l} A, \qquad {}^{r}A \perp^{l} A \Leftrightarrow {}^{rl}A \perp^{lr} A, \qquad {}^{l}A \perp^{rl} A \Leftrightarrow {}^{lr}A \perp^{r} A.$$

Define the following collection of elements of the multiplication group M_A of a quasigroup (Q, A):

$$\mathcal{L}^2 = \{L_x^2 \,|\, x \in Q\}, \qquad \mathcal{R}^2 = \{R_x^2 \,|\, x \in Q\}, \qquad \mathcal{RL} = \{R_x L_x \,|\, x \in Q\},$$

$$\mathcal{LR} = \{L_x R_x \,|\, x \in Q\}, \qquad \mathcal{RL}^{-1} = \{R_x L_x^{-1} \,|\, x \in Q\},$$

where $L_x y = A(x, y)$, $R_x y = A(y, x)$ and the permutations in the products act from the right to the left.

Theorem 1. *Let (Q, A) be a quasigroup. Then*

$$A \perp^{r} A \ ({}^{s}A \perp^{rl} A) \Leftrightarrow \mathcal{L}^2 \quad \textit{is a strictly transitive subset (s.t.subset) of} \quad M_A;$$
$$A \perp^{l} A \ ({}^{s}A \perp^{lr} A) \Leftrightarrow \mathcal{R}^2 \quad \textit{is a s.t.subset of} \quad M_A;$$
$$A \perp^{rl} A \ ({}^{s}A \perp^{r} A) \Leftrightarrow \mathcal{RL} \quad \textit{is a s.t.subset of} \quad M_A;$$
$$A \perp^{lr} A \ ({}^{s}A \perp^{l} A) \Leftrightarrow \mathcal{LR} \quad \textit{is a s.t.subset of} \quad M_A;$$
$$A \perp^{s} A \Leftrightarrow \mathcal{RL}^{-1} \quad \textit{is a s.t.subset of} \quad M_A.$$

Proof. By the criterion of Belousov $A \perp^{r} A$ if and only if the operation $B(x, y) = A(x, A(x, y))$ is a quasigroup, that is the equation $A(x, A(x, a)) = b$ or $L_x^2 a = b$ has a unique solution x for any pair $(a, b) \in Q^2$ as the operation B is always invertible from the right. It means that $\mathcal{L}^2$ is a strictly transitive set.

$A \perp^{l} A$ if and only if the equation $A(A(a, y), y) = b$ or $R_y^2 a = b$ has a unique solution y for any pair $(a, b) \in Q^2$.

By Proposition 1, $A \perp^{rl} A$ $({}^{s}A \perp^{r} A)$ if and only if the equations ${}^{s}A(x, A(x, a)) = b$, $A(A(x, a), x) = b$, $R_x L_x a = b$ have a unique solution x for any $(a, b) \in Q^2$.

Analogously, $A \perp^{lr} A$ $({}^{s}A \perp^{l} A$) if and only if the equations $({}^{s}A \circ A)(a, y) = b$, ${}^{s}A(A(a, y), y) = A(y, A(a, y)) = b, L_y R_y a = b$ have a unique solution y for any $(a, b) \in Q^2$.

$A \perp^{s} A$ if and only if the equation $A(x, {}^{lr}A(x, a)) = L_x R_x^{-1} a = b$ has a unique solution since if ${}^{lr}A(x, a) = t$, then ${}^{r}A(t, a) = x$, $A(t, x) = a$, $t = R_x^{-1} a$.

For the orthogonality ${}^{s}A \perp^{rl} A$, ${}^{s}A \perp^{lr} A$ the statements follow from Proposition 1. $\square$

Note that an analog of Theorem 1 for finite quasigroups was proved in [15, Theorem 9].

If $(Q,\cdot)$ is a finite quasigroup then the conditions of conjugate-orthogonality from Theorem 1 are equivalent to some quasi-identities in the primitive quasigroup $(Q,\cdot,\backslash,/)$.

Corollary 1. *Let (Q,A) be a finite quasigroup. Then*

$$\begin{aligned}
(\cdot)\perp^r(\cdot) &\Leftrightarrow x\cdot xz = y\cdot yz \Rightarrow x=y;\\
(\cdot)\perp^l(\cdot) &\Leftrightarrow zx\cdot x = zy\cdot y \Rightarrow x=y;\\
(\cdot)\perp^{rl}(\cdot) &\Leftrightarrow xz\cdot x = yz\cdot y \Rightarrow x=y;\\
(\cdot)\perp^{lr}(\cdot) &\Leftrightarrow x\cdot zx = y\cdot zy \Rightarrow x=y;\\
(\cdot)\perp^s(\cdot) &\Leftrightarrow (x\backslash z)x = (y\backslash z)y \Rightarrow x=y;\\
&\text{or } x(z/x) = y(z/y) \Rightarrow x=y.
\end{aligned}$$

Proof follows from Theorem 1 if we take into account that

$$L_x^{-1}z = x\backslash z, \quad R_x^{-1}z = z/x \tag{1}$$

and that the strict transitivity of a set of maps $S=\{\alpha_1,\alpha_2,\dots,\alpha_n\}$ on a finite set Q means that $\alpha_i x = \alpha_j x \Rightarrow i=j$ for any $x\in Q$. □

These quasi-identities for the finite case were also established in [15, Theorem 10] and [5, Theorem 1].

From the conditions of conjugate-orthogonality of Theorem 1 some properties of quasigroups (loops) of distinct classes easy follow.

At first we remind (see, for example, [1,12]) that a quasigroup $(Q,\cdot)$ is *diagonal* if the map $x\to xx=x^2$ is a permutation; the *left (right) alternative law* is $x\cdot xy = xx\cdot y$ ($yx\cdot x = y\cdot xx$); the *elastic law* is $xy\cdot x = x\cdot yx$; *a diassociative loop* is a loop any two elements of which generate a subgroup.

Proposition 2. *1) If a commutative quasigroup (Q,A) is orthogonal to one of its conjugates different from ${}^sA$, then it is orthogonal to the rest ones (except ${}^sA$). If, in addition, (Q,A) is a loop then it is diagonal.*

2) If a quasigroup (Q,A) has the right (left) identity e (f) and $A\perp^r A$ or $A\perp^{rl}A$ ($A\perp^l A$ or $A\perp^{lr}A$), then it is diagonal.

3) If a quasigroup (Q,A) satisfies the left (right) alternative law and $A\perp^r A$ ($A\perp^l A$) then it is diagonal. Conversely, for any diagonal quasigroup with the left (right) alternative law $A\perp^r A$ ($A\perp^l A$). For any diagonal and diassociative loop $A\perp^r A$ and $A\perp^l A$.

4) If in a quasigroup (Q,A) the elastic law holds, then $A\perp^{rl}A \Leftrightarrow A\perp^{lr}A$. If (Q,A) is a loop with the elastic low and $A\perp^{rl}A$, then A is diagonal.

5) Any diagonal Moufang loop (in particular, a diagonal group) (Q,A) is orthogonal to each of its conjugates, except ${}^sA$.

Proof. 1) In a commutative quasigroup the equality $R_x = L_x$ holds for each $x \in Q$, so all collections $\mathcal{L}^2$, $\mathcal{R}^2$, $\mathcal{RL}$ and $\mathcal{LR}$ coincide. In a loop $(Q, \cdot)$ with the identity e the equations $L_x^2 e = b$, $x \cdot xe = b$, $x^2 = b$ have a unique solution x for any $b \in Q$ if $(\cdot) \perp^r (\cdot)$.

2) If $(\cdot) \perp^r (\cdot)$ ($(\cdot) \perp^{rl} (\cdot)$), then the equation $L_x^2 e = b$ or $x^2 = b$ ($R_x L_x e = b$ or $x^2 = b$) has a unique solution for any $b \in Q$. Analogously, if $(\cdot) \perp^l (\cdot)$ or $(\cdot) \perp^{lr} (\cdot)$.

3) If $(\cdot) \perp^r (\cdot)$ ($(\cdot) \perp^l (\cdot)$), then $L_x^2 a = x \cdot xa = x^2 \cdot a = b$, $x^2 = b/a$ ($R_x^2 a = ax \cdot x = a \cdot x^2 = b$, $x^2 = a \backslash b$). Conversely, if $(Q, \cdot)$ is diagonal and satisfies the left (right) alternative law then $x^2 = b \Rightarrow x^2 \cdot a = x \cdot xa = ba = c$ ($x^2 = b \Rightarrow a \cdot x^2 = ax \cdot x = ab = c$), where c is any element of Q. Thus, the equation $L_x^2 a = c$ ($R_x^2 a = c$) has a unique solution for any $a, c \in Q$. If a loop is diassociative, then it satisfies the left and right alternative lows, so the last statement is true as well.

4) In a quasigroup with the elastic law $\mathcal{RL}$ is a strictly transitive set if and only if $\mathcal{LR}$ is a strictly transitive set, since $R_x L_x a = L_x R_x a$. In a loop with elastic low $R_x L_x e = b \Rightarrow x^2 = b$.

5) Any Moufang loop (Q, A) is diassociative and satisfies the left and the right alternative laws and the elastic low, so $A \perp^r A$, $A \perp^l A$ and $A \perp^{rl} A$ by 3), and $A \perp^{lr} A$ by 4). It is known that any loop A can not be selforthogonal ($A \not\perp^s A$). Indeed, the equation $R_x L_x^{-1} a = a$, $a \neq e$ has two solutions $x = a$ and $x = e$. □

Note that item 5) of Proposition 2 was proved in [5] for finite Moufang loops. It is known that a Moufang loop (Q, A), just as a group, of odd order is diagonal, so by Proposition 2 it is orthogonal to each its conjugate, except A^* (see also [1, 5]).

4 Orthogonality of conjugates of a quasigroup and strictly transitive subsets of the complete multiplication group

Now we consider conditions for the orthogonality ${}^\sigma A \perp^\tau A$, where ${}^\sigma A$, ${}^\tau A \neq A$.

Denote ${}^r A = (\backslash)$, ${}^l A = (/)$, then

$$R_x^{\backslash} y = y \backslash x = L_y^{-1} x = I_x y, \quad L_x^{/} y = x / y = R_y^{-1} x = I_x^{-1} y, \tag{2}$$

and

$$L_x^{-1} R_x^{\backslash} = L_x^{-1} I_x, \quad L_x^{/} L_x = I_x^{-1} L_x, \quad R_x^{-1} R_x^{\backslash} = R_x^{-1} I_x, \tag{3}$$

where $y \cdot I_x y = x$ for any $y \in Q$.

Consider the following collections of permutations of the complete multiplication group $\overline{M}_A$ of a quasigroup (Q, A):

$$\begin{aligned} \mathcal{I}^{-1}\mathcal{L} &= \{L_x^{/} L_x \,|\, x \in Q\} = \{I_x^{-1} L_x \,|\, x \in Q\}, \\ \mathcal{I}^2 &= \{(R_x^{\backslash})^2 \,|\, x \in Q\} = \{I_x^2 \,|\, x \in Q\}, \\ \mathcal{IL} &= \{(L_x^{/})^{-1} L_x \,|\, x \in Q\} = \{I_x L_x \,|\, x \in Q\}, \\ \mathcal{R}^{-1}\mathcal{I} &= \{R_x^{-1} R_x^{\backslash} \,|\, x \in Q\} = \{R_x^{-1} I_x \,|\, x \in Q\}. \end{aligned}$$

Theorem 2. *Let (Q, A) be a quasigroup. Then*

$$
\begin{gathered}
{}^{r}A \perp^{l} A \ ({}^{rl}A \perp^{lr} A) \Leftrightarrow \mathcal{I}^{-1}\mathcal{L} \quad \textit{is a s.t.subset of} \quad \overline{M}_A, \\
{}^{r}A \perp^{lr} A \ ({}^{l}A \perp^{rl} A) \Leftrightarrow \mathcal{I}^{2} \quad \textit{is a s.t.subset of} \quad \overline{M}_A, \\
{}^{r}A \perp^{rl} A \Leftrightarrow \mathcal{I}\mathcal{L} \quad \textit{is a s.t.subset of} \quad \overline{M}_A, \\
{}^{l}A \perp^{lr} A \Leftrightarrow \mathcal{R}^{-1}\mathcal{I} \quad \textit{is a s.t.subset of} \quad \overline{M}_A.
\end{gathered}
$$

Proof. By the Belousov criterion and Proposition 1:

${}^{l}A \perp^{r} A$ (${}^{rl}A \perp^{lr} A$) if and only if the equations ${}^{l}A(x, A(x, a)) = b$, $L_x^{/} L_x a = I_x^{-1} L_x a = b$ have a unique solution x for any $(a, b) \in Q^2$. Thus, $\mathcal{I}^{-1}\mathcal{L}$ is a s.t.subset of $\overline{M}_A$.

${}^{r}A \perp^{lr} A$ (${}^{l}A \perp^{rl} A$) if and only if the equations ${}^{l}A(x, {}^{l}A(x, a)) = b$, $(L_x^{/})^2 a = b$, $I_x^2 b = a$ have a unique solution x for any $(a, b) \in Q^2$. Thus, $\mathcal{I}^2$ is a s.t.subset of $\overline{M}_A$.

${}^{r}A \perp^{rl} A$ if and only if the equations ${}^{r}A(x, {}^{l}A(x, a)) = b$, $A(x, b) = {}^{l}A(x, a)$, $L_x b = L_x^{/} a = I_x^{-1} a$, $I_x L_x b = a$ have a unique solution x for any $(a, b) \in Q^2$. Hence, $\mathcal{I}\mathcal{L}$ is a s.t.subset of $\overline{M}_A$.

And finally, ${}^{l}A \perp^{lr} A$ if and only if the equations ${}^{l}A(x, {}^{s}A(x, a)) = b$, $A(b, A(a, x)) = x$, ${}^{r}A(b, x) = A(a, x)$, $R_x^{\backslash} b = R_x a$, $R_x^{-1} I_x b = a$ have a unique solution, that is $\mathcal{R}^{-1}\mathcal{I}$ is a s.t.subset of $\overline{M}_A$.

The rest four cases of possible orthogonality of conjugates were considered in Theorem 1. □

Remark 1. The conditions of Theorem 2 can be also obtained from Theorem 1 if instead of a quasigroup A one takes the corresponding conjugate.

Remark 2. Note that there are quasigroups all subsets of Theorem 1 and Theorem 2 are strictly transitive. All conjugates of these quasigroups are distinct and pairwise orthogonal. An example of such quasigroup over the field of rational numbers: $xy = 2x + 3y$ is given by V.D. Belousov in [4, p. 66].

Corollary 2. *If $(Q, \cdot)$ is a finite quasigroup, then*

$$
\begin{gathered}
{}^{r}(\cdot) \perp^{l} (\cdot) \ ({}^{rl}(\cdot) \perp^{lr} (\cdot)) \Leftrightarrow x/(xz) = y/(yz) \Rightarrow x = y \text{ or } x\backslash(z\backslash x) = y\backslash(z\backslash y) \Rightarrow x = y, \\
{}^{r}(\cdot) \perp^{lr} (\cdot) \ ({}^{l}(\cdot) \perp^{rl} (\cdot)) \Leftrightarrow (z\backslash x)\backslash x = (z\backslash y)\backslash y \Rightarrow x = y \text{ or} \\
x/(x/z) = y/(y/z) \Rightarrow x = y, \\
{}^{r}(\cdot) \perp^{rl} (\cdot) \Leftrightarrow xz\backslash x = yz\backslash y \Rightarrow x = y \text{ or } x\backslash(x/z) = y\backslash(y/z) \Rightarrow x = y, \\
{}^{l}(\cdot) \perp^{lr} (\cdot) \Leftrightarrow (z\backslash x)/x = (z\backslash y)/y \Rightarrow x = y \text{ or } x/(zx) = y/(zy) \Rightarrow x = y.
\end{gathered}
$$

Proof. Prove the first quasi-identities in every pair of equivalent ones. The second quasi-identity can be obtained by change of the corresponding strictly transitive set by the set with inverse permutations and taking into account (2), (3).

$$
\begin{gathered}
\mathcal{I}^{-1}\mathcal{L}: \ L_x^{/} L_x z = L_y^{/} L_y z \Rightarrow x = y \text{ or } x/(xz) = y/(yz) \Rightarrow x = y, \\
\mathcal{I}^{2}: \ (R_x^{\backslash})^2 z = (R_y^{\backslash})^2 z \Rightarrow x = y \text{ or } (z\backslash x)\backslash x = (z\backslash y)\backslash y \Rightarrow x = y, \\
\mathcal{I}\mathcal{L}: \ R_x^{\backslash} L_x z = R_y^{\backslash} L_y z \Rightarrow x = y \text{ or } (xz)\backslash x = (yz)\backslash y \Rightarrow x = y, \\
\mathcal{R}^{-1}\mathcal{I}: \ R_x^{-1} R_x^{\backslash} z = R_y^{-1} R_y^{\backslash} z \Rightarrow x = y \text{ or } (z\backslash x)/x = (z\backslash y)/y \Rightarrow x = y.
\end{gathered}
$$

□

The following proposition eliminates the orthogonality of some conjugates (${}^{\sigma}A \not\perp^{\tau} A$) for quasigroups of some classes.

Proposition 3. *1) If (Q, A) is a commutative quasigroup, then ${}^{r}A \perp^{l} A \Leftrightarrow {}^{r}A \perp^{rl} A \Leftrightarrow {}^{l}A \perp^{lr} A \Leftrightarrow {}^{rl}A \perp^{lr} A$ and $A \not\perp^{s} A$, ${}^{l}A \not\perp^{rl} A$, ${}^{r}A \not\perp^{lr} A$.*

2) If a quasigroup (Q, A) has the right (left) identity e (f), then ${}^{r}A \not\perp^{rl} A$ (${}^{l}A \not\perp^{lr} A$).

3) If (Q, A) is an IP-quasigroup then ${}^{r}A \not\perp^{rl} A$ and ${}^{l}A \not\perp^{lr} A$.

4) For a loop (Q, A) $A \not\perp^{s} A$ and the orthogonality of conjugates from Theorem 2 is impossible.

Proof. 1) The first statements follows from Proposition 1 and Theorem 2 since in a commutative quasigroup $I_x = I_x^{-1}$, $R_x = L_x$, so $\mathcal{I}^{-1}\mathcal{L} = \mathcal{I}\mathcal{L}$ and $\mathcal{R}^{-1}\mathcal{I}$ is a s.t.subset of $\overline{M}_A$. if and only if $\mathcal{I}^{-1}\mathcal{R} = \mathcal{I}\mathcal{L}$ is a s.t.subset of $\overline{M}_A$. In a commutative quasigroup $R_a^{-1}x = L_a^{-1}x$, so $x/a = a\backslash x$, $(a\backslash x)a = x$, $(R_x^{\backslash})^2 a = (a\backslash x)\backslash x = a$ for any $x \in Q$. Hence, I^2 is not strictly transitive and so ${}^{r}A \not\perp^{lr} A$, ${}^{l}A \not\perp^{rl} A$ by Theorem 2. $A \not\perp^{s} A$ in view of Theorem 1 since in this case $\mathcal{R}^{-1}\mathcal{L} = \varepsilon$ (the identity permutation).

2) By Theorem 2 ${}^{r}(\cdot) \perp^{rl} (\cdot)$ if and only if the equations $R_x^{\backslash} L_x a = b$, $(xa)\backslash x = b$, $xa \cdot b = x$, $R_b R_a x = x$ have a unique solution x for any $(a, b) \in Q^2$, ${}^{l}(\cdot) \perp^{lr} (\cdot)$ if and only if the equations $R_x^{-1} R_x^{\backslash} a = b$, $a\backslash x = bx$, $L_a^{-1} x = L_b x$, $L_a L_b x = x$ have a unique solution for any $(a, b) \in Q^2$. But by $a = b = e$ ($a = b = f$) $R_e R_e x = x$ ($L_f L_f x = x$) for any $x \in Q$, so ${}^{r}(\cdot) \not\perp^{rl} (\cdot)$ and ${}^{l}(\cdot) \not\perp^{lr} (\cdot)$.

3) Let (Q, A) be an IP-quasigroup, then $R_a^{-1} = R_{I_r a}$, $L_a^{-1} = L_{I_l a}$ and $R_{I_r a} R_a x = R_a^{-1} R_a x = x$, $L_{I_l a} L_a x = L_a^{-1} L_a x = x$ for any $x \in Q$, so as above ${}^{r}A \not\perp^{rl} A$ and ${}^{l}A \not\perp^{lr} A$.

4) Let $(Q, \cdot)$ be a loop with the identity e. Then ${}^{r}(\cdot) \not\perp^{rl} (\cdot)$ and ${}^{l}(\cdot) \not\perp^{lr} (\cdot)$ by item 2).

${}^{r}(\cdot) \not\perp^{l} (\cdot)$ (${}^{rl}(\cdot) \not\perp^{lr} (\cdot)$) in view of Theorem 2 as $I_x^{-1} L_x e = L_x^{/} L_x e = x/(xe) = e$ for any $x \in Q$ and

${}^{r}(\cdot) \not\perp^{lr} (\cdot)$ (${}^{l}(\cdot) \not\perp^{rl} (\cdot)$) by Theorem 2 since $I_x^2 e = R_x^{\backslash} R_x^{\backslash} e = (e\backslash x)\backslash x = e$ for any $x \in Q$. □

References

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

[2] Belousov V. D. *Systems of orthogonal operations*. Mat. sbornik, 1968, **77(119):1**, 38–58 (in Russian).

[3] Belousov V. D. *On the group associated with a quasigroup*. Mat. Issled., 1969, **4**, No. 3, 21–39 (in Russian).

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

[5] Belyavskaya G. B., Diordiev A. D. *On some quasi-identities in finite quasigroups.* Buletinul Academiei de ştiinţe a Republicii Moldova, Matematica, 2005, No. 3(49), 19–32.

[6] Bennet F. E. *The spectra of a variety of quasigroups and related combinatorial designs.* Discrete Mathematics, 1989, **77**, 29–50.

[7] Bennet F. E. *Latin squares with pairwise orthogonal conjugates.* Discrete Mathematics, 1981, **36**, 117–137.

[8] Bennet F. E. *On conjugate orthogonal idempotent Latin squares.* Ars. Combinatorica, 1985, **19**, 37–50.

[9] Bennet F. E., Mendelsohn N. S. *Conjugate orthogonal Latin square graphs.* Congressus Numerantium, 1979, **23**, 179–192.

[10] Bennet F. E., Hantao Zhang. *Latin squares with self-orthogonal conjugates.* Discrete Mathematics, 2004, **284**, 45–55.

[11] Chaffer R. A., Lieberman D. J., Smith D. D. *The number of orthogonal conjugates of a quasigroup.* Congressus Numerantium, 1982, 169–180.

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

[13] Evans T. *Algebraic structures associated with Latin squares and orthogonal arrays.* Proc. Conf. Algebraic Aspects of Combinatorics, Congressus Numerantium, 1975, **13**, 31–52.

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

[15] 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.

[16] Phelps K. T. *Conjugate orthogonal quasigroups.* J. Combin. Theory (A), 1978, **25**, 117–127.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD-2028 Chisinau
Moldova

E-mail: *gbel@math.md, gbel1@rambler.ru*

Received July 17, 2008