BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(48), 2005, Pages 3–42
ISSN 1024–7696

On orthogonality of binary operations and squares

Gary L. Mullen, Victor A. Shcherbacov

Abstract. Orthogonality of a pair of binary groupoids, left quasigroups and quasigroups from some points of view is studied. Necessary and sufficient conditions of orthogonality of a finite quasigroup and any its parastrophe (conjugate quasigroup in other terminology), including ones in language of quasi-identities, are given. New concept of gisotopy, which generalizes the concept of isotopy, is defined. There is information on quasigroups with self-orthogonal conjugates.

Mathematics subject classification: 20N05, 05B15, 20N02, 08C15.
Keywords and phrases: Groupoid, left quasigroup, quasigroup, Latin square, row-Latin square, Latin square with self-orthogonal conjugates, orthogonality, parastrophy, isotopy, isostrophy, gisotopy.

1 Introduction

Results presented in this article were received after reading the works [5, 10–12, 19, 30]. With orthogonality of quasigroup parastrophes the authors met by the study of codes with one check symbol [31, 32].

Taking into consideration the rule that articles are written for readers in some places of this paper we recall in details some known facts, many of which can be found in [4, 8, 9, 27, 35], maybe, in an other form, or, more or less easy, can be proved independently. Some results of this article were announced in [41].

It is not very difficult to see that the majority of results on orthogonality, especially, on orthogonality of quasigroups, which are included in this paper, are true also in the infinite case.

1.1 Groupoids, quasigroups and loops

Definition 1. A binary operation A defined on a nonempty set Q is a map $A : Q \times Q \to Q$ such that A is defined for every pair of elements in Q and uniquely associates each pair of elements in Q to some element of Q, i.e. $D(A) = Q^2$, $ImA \subseteq Q$ ([21]).

Definition 2. A binary groupoid (G, A) is understood to be a non-empty set G together with a binary operation A.

Any finite binary groupoid (Q, A) can be defined as the set $\mathfrak{T}(A)$ of ordered triplets $(a_1, a_2, A(a_1, a_2))$, where $a_1, a_2 \in Q$. Binary groupoids (Q, A) and (Q, B)

are equal if and only if $\mathfrak{T}(A) = \mathfrak{T}(B)$, where $\mathfrak{T}(B)$ is the set of triplets of the groupoid (Q, B).

If we need to show what groupoid operation was used by obtaining the third component of a groupoid triplet, then we denote an element from the set $\mathfrak{T}(Q, A)$ as $A(x_1, x_2, x_3)$.

Definition 3. A groupoid $(Q, \circ)$ is called a *right quasigroup* if, for all $a, b \in Q$, there exists a unique solution $x \in Q$ of the equation $x \circ a = b$.

Definition 4. A groupoid $(Q, \circ)$ is called a *left quasigroup* if, for all $a, b \in Q$, there exists unique solution $y \in Q$ of the equation $a \circ y = b$.

Definition 5. A left and right quasigroup $(Q, \circ)$ is called a *quasigroup*.

Definition 6. A binary groupoid (Q, A) with operation A such that in the equality $A(x_1, x_2) = x_3$ the knowledge of any two elements of x_1, x_2, x_3 uniquely specifies the remaining one is called a *binary quasigroup* [8].

It is easy to see that Definitions 5 and 6 are equivalent.

Definition 7. An element 1 of a groupoid $(Q, \cdot)$ is called an *identity element* of the groupoid $(Q, \cdot)$ if $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$.

Definition 8. A quasigroup with an identity element is called a *loop*.

We shall use definition of a quasigroup as an algebra with three binary operations [4].

Definition 9. A groupoid $(Q, \cdot)$ is called a quasigroup, if on the set Q there exist operations "$\backslash$" and "$/$" such that in the algebra $(Q, \cdot, \backslash, /)$ the following identities are fulfilled:

$$x \cdot (x\backslash y) = y,\ (y/x) \cdot x = y,\ x\backslash(x \cdot y) = y,\ (y \cdot x)/x = y. \tag{1}$$

As usual, $\overline{1, n}$ denotes the set $\{1, 2, \ldots, n\}$.

Remark 1. We shall use the following order of multiplication (of composition) of maps: $(\alpha\beta)(x) = \alpha(\beta(x))$, where α, β are the maps.

1.2 Isotopy of groupoids, isostrophy and parastrophy of quasigroups

We denote by S_Q the group of all permutations (bijections in infinite case) of a set Q.

A groupoid (Q, A) is an *isotope of a groupoid* (Q, B) if there exist permutations μ_1, μ_2, μ_3 of the set Q such that $A(x_1, x_2) = \mu_3^{-1} B(\mu_1 x_1, \mu_2 x_2)$ for all $x_1, x_2 \in Q$.

We also can write this fact in the form $(Q, A) = (Q, B)T$, where $T = (\mu_1, \mu_2, \mu_3)$ [4, 9, 35]. As usual, if $\mu_1 = \mu_2 = \mu_3$, then a groupoid (Q, A) is *isomorphic to a groupoid* (Q, B).

With any quasigroup $(Q, \circ)$ it is possible to associate five further quasigroups called *parastrophes* of $(Q, \circ)$. This follows, for instance, from Definition 6.

If we denote a quasigroup operation by the letter A, then with this quasigroup operation A we can associate the following quasigroup operations (see [4,7,8,29,35]): $A(x_1, x_2) = x_3 \Leftrightarrow A^{(12)}(x_2, x_1) = x_3 \Leftrightarrow A^{(13)}(x_3, x_2) = x_1 \Leftrightarrow A^{(23)}(x_1, x_3) = x_2 \Leftrightarrow A^{(123)}(x_2, x_3) = x_1 \Leftrightarrow A^{(132)}(x_3, x_1) = x_2$. In other words $A^{\sigma}(x_{\sigma 1}, x_{\sigma 2}) = x_{\sigma 3} \Leftrightarrow A(x_1, x_2) = x_3$ where $\sigma \in S_3$.

For example, $A^{(132)}(x_3, x_1) = x_2 \Leftrightarrow A(x_1, x_2) = x_3$: that is, $A^{(132)}(x_{(132)1}, x_{(132)2}) = x_{(132)3} \Leftrightarrow A(x_1, x_2) = x_3$.

The concept of parastrophy has a well-known geometrical motivation. See, for example, [7, 35].

In some articles, especially in combinatorics, see, for example [36], parastrophic quasigroups are called *conjugate quasigroups*.

We can see on a classical definition of parastrophe of a quasigroup (Q, A) as on a bijective map of a set of quasigroup triplets $\mathfrak{T}(Q, A)$ in the set $\mathfrak{T}(Q, A)$ such that $\sigma : A(x_1, x_2, x_3) \mapsto (A(x_1, x_2, x_3))^{\sigma} = A^{\sigma}(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3})$ where $\sigma \in S_3$.

To be able to restore a quasigroup (Q, A) from the set of quasigroup triplets $\mathfrak{T}(Q, A)$ we need to require that the set Q is a fully ordered set.

In this case, for example, triplet $(3, 4, 5)$ shows that in Cayley table of quasigroup (Q, A) the element 5 of this quasigroup is situated in the third row and in the fourth column.

From "triplets" point of view we can consider an isotopy $T = (\alpha_1, \alpha_2, \alpha_3)$ as a bijective map of a set of quasigroup triplets $\mathfrak{T}(Q, A)$ in the set $\mathfrak{T}(Q, B)$ of the form: $T : A(x_1, x_2, x_3) \mapsto B(\alpha_1 x_1, \alpha_2 x_2, \alpha_3 x_3)$.

We recall, as usual, if $T = (\alpha_1, \alpha_2, \alpha_3)$ is an isotopy, σ is a parastrophy, then $T^{\sigma} = (\alpha_{\sigma 1}, \alpha_{\sigma 2}, \alpha_{\sigma 3})$.

Lemma 1. $(AT)^{\sigma} = A^{\sigma} T^{\sigma}$, $(T_1 T_2)^{\sigma} = T_1^{\sigma} T_2^{\sigma}$ *[4, 8].*

Definition 10. A quasigroup (Q, B) is an isostrophic image of a quasigroup (Q, A) if there exists a collection of permutations $(\sigma, (\alpha_1, \alpha_2, \alpha_3)) = (\sigma, T)$, where $\sigma \in S_3$, $T = (\alpha_1, \alpha_2, \alpha_3)$ and $\alpha_1, \alpha_2, \alpha_3$ are permutations of the set Q such that $B(x_1, x_2) = A(\sigma, T)(x_1, x_2) = \alpha_3^{-1} A^{\sigma}(\alpha_1 x_1, \alpha_2 x_2)$ for all $x_1, x_2 \in Q$ [8].

A collection of permutations $(\sigma, (\alpha_1, \alpha_2, \alpha_3)) = (\sigma, T)$ will be called an *isostrophy* of a quasigroup (Q, A).

Often an isostrophy (σ, T) is called σ-isostrophy T or isostrophy of type σ. We can re-write the equality from Definition 10 in the form $A^{\sigma} T = B$, where $T = (\alpha_1, \alpha_2, \alpha_3)$.

From the quasigroup triplets point of view we can write the definition of isostrophy in the form: $A(\sigma, T) = (A^{\sigma})T = (x_1, x_2, x_3)^{\sigma}(\lambda, \mu, \nu) = (x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3})(\lambda, \mu, \nu) = (\lambda x_{\sigma 1}, \mu x_{\sigma 2}, \nu x_{\sigma 3}) = B$ for all triplets of the quasigroup (Q, A).

Lemma 2. *([8]). An isostrophic image of a quasigroup is a quasigroup.*

Proof. The proof follows from the fact that any parastrophic image of a quasigroup is a quasigroup and any isotopic image of a quasigroup is a quasigroup. □

From Lemma 2 it follows that it is possible to define the multiplication of isostrophies of a quasigroup operation defined on a set Q.

Definition 11. If (σ, S) and (τ, T) are isostrophies of a quasigroup (Q, A), then

$$(\sigma, S)(\tau, T) = (\sigma\tau, S^\tau T),$$

where $A^{\sigma\tau} = (A^\sigma)^\tau$ and $(x_1, x_2, x_3)(S^\tau T) = ((x_1, x_2, x_3)\ S^\tau)T$ for any quasigroup triplet (x_1, x_2, x_3).

Slightly different operation on the set of all isostrophies (multiplication of quasigroup isostrophies) is defined in [8]. The definition from [28] is very close to Definition 11. See, also, [24].

Proposition 1. *The set of all isostrophies of a quasigroup (Q, A) forms the group of isostrophies $ISOS(Q, A)$ with respect to the operation of multiplication, moreover $ISOS(Q, A) \cong (S_Q \times S_Q \times S_Q) \leftthreetimes S_3$.*

Proof. If A is a quasigroup operation and (σ, S) is an isostrophy, then $A(\sigma, S)$ is a quasigroup.

Further we have $(A(\sigma, S))(\tau, T) = (A^\sigma S)(\tau, T) = (A^\sigma S)^\tau T =$ (we use Lemma 1) $= A^{\sigma\tau} S^\tau T = A(\sigma\tau, S^\tau T)$, i.e. if $(\sigma, S), (\tau, T) \in ISOS(Q)$, then $(\sigma, S)(\tau, T) \in ISOS(Q, A)$.

The associativity of this operation follows from the associativity of multiplication of permutations.

Let $S = (\alpha_1, \alpha_2, \alpha_3)$ be an isotopy of a quasigroup A, $S^{-1} = (\alpha_1^{-1}, \alpha_2^{-1}, \alpha_3^{-1})$, $S^\sigma = (\alpha_{\sigma 1}, \alpha_{\sigma 2}, \alpha_{\sigma 3})$. Then $(\sigma^{-1}, S)^{-1} = (\sigma, (S^{-1})^\sigma)$. Indeed,

$$(\sigma^{-1}, S)(\sigma, (S^{-1})^\sigma) = (\varepsilon, S^\sigma (S^{-1})^\sigma) = (\varepsilon, (SS^{-1})^\sigma) = (\varepsilon, \varepsilon).$$

The proof of the fact that $ISOS(Q, A) \cong (S_Q \times S_Q \times S_Q) \leftthreetimes S_3$ is standard [23] and we omit it. □

Remark 2. It is clear that for any pair of quasigroups (Q, A) and (Q, B) we have $ISOS(Q, A) = ISOS(Q, B)$ and it is possible to speak about the set (about the group) of isostrophies of a set Q.

Lemma 3. *A (12)-isostrophic image of a groupoid is a groupoid.*

Proof. An isotopic image of a groupoid is a groupoid, (12)-parastrophic image of a groupoid is a groupoid, therefore (12)-isostrophic image of a groupoid is a groupoid. □

Proposition 2. *The set of all ε-isostrophies and (12)-isostrophies of a groupoid (Q, A) forms the group $ISOS_{(12)}(Q)$ of isostrophies with respect to the operation of multiplication, moreover $ISOS_{(12)}(Q) \cong (S_Q \times S_Q \times S_Q) \leftthreetimes Z_2$. If $|Q| = m$, then $|ISOS_{(12)}(Q)| = 2(m!)^3$.*

Proof. It is possible to use standard facts from Group Theory [23]. □

Proposition 3. *The set of all ε-isostrophies, (123)-isostrophies and (132)-isostrophies of a quasigroup (Q, A) forms the group $ISOS_{(123)}(Q)$ of isostrophies with respect to the operation of multiplication, moreover $ISOS_{(123)}(Q) \cong (S_Q \times S_Q \times S_Q) \leftthreetimes Z_3$.*

Proof. It is possible to use standard facts from Group Theory [23]. □

1.3 Translations of groupoids and quasigroups

Let $(Q, \cdot)$ be a groupoid. As usual, the map $L_a : L_a x = a \cdot x$ for all $x \in Q$ is a left translation of the groupoid $(Q, \cdot)$ relatively to a fixed element $a \in Q$, the map $R_a : R_a x = x \cdot a$ is a right translation.

For some groupoids we can define the notion of a middle translation. A map $P_a : x \cdot P_a x = a$, where $x \in Q$, is called a middle translation of a groupoid $(Q, \cdot)$ relatively to a fixed element $a \in Q$ [4,6,9,35]. Usually middle translations are defined for quasigroups.

In a right (left) quasigroup $(Q, \circ)$ any right (left) translation is a permutation of the set Q [35].

Lemma 4. *Any isotope of a groupoid $(Q, \circ)$ is a groupoid [35]. Any isotope of a left (right) quasigroup $(Q, \circ)$ is a left (right) quasigroup.*

Proof. If $(Q, \circ)$ is a (θ, ϕ, ψ)-isotope of a left quasigroup $(Q, \cdot)$, then $x \circ y = \psi^{-1}(\theta x \cdot \phi y)$ for all $x, y \in Q$. Hence, $L_x^{(\circ)} y = \psi^{-1} L_{\theta x}^{(\cdot)} \phi y$ and the map $L_x^{(\circ)}$ is a permutation since the map $L_{\theta x}^{(\cdot)}$ is a permutation. □

In a quasigroup $(Q, \cdot)$ all left, right and middle translations are permutations of the set Q [35].

Lemma 5. *There exist the following connections between different kinds of translations in the parastrophes of a quasigroup $(Q, \cdot)$ [20, 40].*

Table 1

	ε	(12)	(13)	(23)	(123)	(132)
R	R	L	R^{-1}	P	P^{-1}	L^{-1}
L	L	R	P^{-1}	L^{-1}	R^{-1}	P
P	P	P^{-1}	L^{-1}	R	L	R^{-1}
R^{-1}	R^{-1}	L^{-1}	R	P^{-1}	P	L
L^{-1}	L^{-1}	R^{-1}	P	L	R	P^{-1}
P^{-1}	P^{-1}	P	L	R^{-1}	L^{-1}	R

Proof. In Table 1, for example, $R^{(23)} = P^{(\cdot)}$. Indeed, if $R_a^{(23)} x = x \backslash a = b$, then $x \cdot b = a$, $P_a^{(\cdot)} x = b$, i.e. $R^{(23)} = P^{(\cdot)}$. □

The sets of all left, right and middle translations of a quasigroup $(Q,\cdot)$ will be denoted $\mathbf{L}(Q,\cdot)$, $\mathbf{R}(Q,\cdot)$, $\mathbf{P}(Q,\cdot)$, respectively. Further, let

$$\begin{array}{ll}\mathbf{L}^2(Q,\cdot)=\{L_aL_a \mid a\in Q\}; & \mathbf{L}^{-1}(Q,\cdot)=\{L_a^{-1} \mid a\in Q\};\\ \mathbf{R}^2(Q,\cdot)=\{R_aR_a \mid a\in Q\}; & \mathbf{R}^{-1}(Q,\cdot)=\{R_a^{-1} \mid a\in Q\};\\ \mathbf{LR}(Q,\cdot)=\{L_aR_a \mid a\in Q\}; & \mathbf{P}^{-1}(Q,\cdot)=\{P_a^{-1} \mid a\in Q\};\\ \mathbf{RL}(Q,\cdot)=\{R_aL_a \mid a\in Q\}; & \mathbf{RL}^{-1}(Q,\cdot)=\{R_aL_a^{-1} \mid a\in Q\}.\end{array}$$

1.4 Squares and Latin squares

We give some definitions of squares and Latin squares.

Definition 12. An $m\times m$ square $S(Q)$ is an arrangement of k variables $x_1,x_2,\ldots,$ x_k, $k\le m$, into m rows and m columns [30].

We shall say that the square $S(Q)$ is defined on the set Q, where $Q=\{x_1,x_2,\ldots,x_k\}$. Sometimes we also shall write this fact in the form $D(S)=Q$.

We shall write the fact that in a square $S(Q)$ in a cell with co-ordinates (i,j) an element $a\in Q$, where $i,j\in\{1,\ldots,m\}$, is arranged as $(i,j,a)\in S$.

The squares $S_1(Q)$ and $S_2(Q)$ are equal if and only if $(i,j,a)=(i,j,b)$ for all $(i,j,a)\in S_1$ and $(i,j,b)\in S_2$.

Definition 13. A *permutation square of order* m is an arrangement of m variables $x_1,x_2,\ldots,x_m$ into m rows and m columns such that no row or no column contains any of variables twice.

It is well known ([27, 34]), that a permutation square in which no row contains any of variables twice is called a *row-Latin square*. Permutation square in which no column contains any of variables twice, is called a *column-Latin square*. In this article we prefer the term permutation square.

Definition 14. A *Latin square* is an arrangement of m variables $x_1,x_2,\ldots,x_m$ into m rows and m columns such that no row and no column contains any of variables twice [30].

In [17] there is such definition of a Latin square.

Definition 15. For a positive integer n, Latin square L of order n is a $n\times n$ matrix whose entries (or values) belong to a set X of n elements and such that every element of X has exactly one occurrence in each row and each column.

It is easy to see that the body of Cayley table (i.e. a Cayley table without the bordering row and the bordering column) of a groupoid (G,A) is a *square* $S(G)$ and any square $S(G)$ can be a body of Cayley table of a groupoid (G,A).

The body of Cayley table of a left quasigroup (Q,A) is a *permutation square* $L(Q,A)$ in which no row contains any of variables twice, the body of Cayley table of a right quasigroup (Q,A) is a *permutation square* $R(Q,A)$ in which no column contains any of variables twice.

Any permutation square in which no row contains any of variables twice can be a body of Cayley table of a left quasigroup (Q, A). Any permutation square in which no column contains any of variables twice can be a body of Cayley table of a right quasigroup (Q, A).

The body of Cayley table of a quasigroup (Q, A) is a *Latin square* $L(Q, A)$ and any Latin square can be a body of Cayley table of a quasigroup (Q, A).

Proposition 4. *An unbordered square S corresponds to a groupoid $(G, \cdot)$ and to all isotopes of $(G, \cdot)$, which arise from an isotopy T of the form $T = (\alpha, \beta, \varepsilon)$, where $\alpha, \beta \in S_Q$.*

Proof. Any isotopic image of a groupoid $(G, \cdot)$ under the isotopy T can be obtained by changing the bordering row and the bordering column of the Cayley table of the groupoid $(G, \cdot)$ without any changing the body of this Cayley table.

Let $(G, \circ) = (G, \cdot)T$, i.e. $x \circ y = \alpha x \cdot \beta y$ for all $x, y \in Q$. Then the permutation α changes elements in the bordering column of the groupoid $(G, \cdot)$ in the following way: an element b in the bordering column of the groupoid $(G, \cdot)T$ is equal to the element $\alpha^{-1}a$, where the element a takes the same position in the bordering column of the groupoid $(G, \cdot)$ as the element b in the bordering column of the groupoid $(G, \cdot)T$.

The permutation β changes the elements in the bordering row of the groupoid $(G, \cdot)$ in the similar way as the permutation α changes the elements in its bordering column.

Indeed, if $x \cdot y = z$, i.e. the element x is the first co-ordinate of the element z, the element y is the second co-ordinate of the element z in the Cayley table of the groupoid $(G, \cdot)$, then $\alpha^{-1}x \circ \beta^{-1}y = \alpha(\alpha^{-1}x) \cdot \beta(\beta^{-1}y) = x \cdot y = z$, i.e. the element $\alpha^{-1}x$ is the first co-ordinate of the element z, the element $\beta^{-1}y$ is the second co-ordinate of the element z in the Cayley table of the groupoid $(G, \circ)$. □

Remark 3. A fixation of any order in the bordering row and any order in the bordering column of all groupoids which are defined on a non-empty set Q gives us a bijection between the class of all groupoids, defined on the set Q, and the class of all squares defined on Q.

Remark 4. Below in this article we suppose that the set Q is a well ordered set. We shall fix an order of any bordering row and bordering column of any groupoid, moreover, we shall suppose that orders in bordering row and bordering column of any groupoid coincide with the order of the set Q.

Remark 5. It is possible do define an infinite square as the body of Cayley table of an infinite groupoid.

1.5 m-Tuples of maps and its product

In [30] Mann defined so-called set of permutations of a Latin square S. Mann wrote: "The rows of a Latin square are permutations of the row $x_1, x_2, \ldots, x_m$. Let

p_i be the permutation which transforms $x_1, x_2, \ldots, x_m$ into the i-th row of the Latin square. Then $p_i p_j^{-1}$ leaves no variables unchanged for $i \neq j$. For otherwise one column would contain a variable twice. On the other hand each set of m permutations $(p_1, p_2, \ldots, p_m)$ such that $p_i p_j^{-1}$ $(i \neq j)$ leaves no variable unchanged generates a Latin square. We may therefore identify every Latin square with a set of m permutations $(p_1, p_2, \ldots, p_m)$ such that $p_i p_j^{-1}$ $(i \neq j)$ leaves no variable unchanged".

Therefore Mann obtained a new presentation of a Latin square $S(Q)$, $|Q| = m$, as a set of m permutations of the set Q. As Denes and Keedwell wrote [17], the similar presentation of a Latin square as a set of permutations can be found in the earlier article of Schöngardt [39].

From the article [30] it follows that by permutations in a permutation square H.B. Mann understood rows of this square, i.e. left translations in terminology of this article. Moreover, by the set of permutations $(s_1, s_2, \ldots, s_m)$ he, in fact, understood an ordered set of permutations, i.e. m-tuple of permutations of a set Q. Later many authors used this presentation in their articles [12, 27, 34].

Definition 16. Let Q be a non-empty well ordered finite set of order m. By *m-tuple M of maps defined on the set Q* we shall understand any well ordered m-element set of maps of Q indexed by elements of the set Q, i.e. $M = (\mu_{a_1}, \mu_{a_2}, \ldots, \mu_{a_m})$, where $a_i \in Q$, μ_{a_i} is a map of the set Q into the set Q, $a_i < a_j$ if and only if $i < j$ for all $i, j \in \overline{1, m}$ such that $i \neq j$.

Below we shall often consider a non-empty set Q of order m as the set of natural numbers $Q = \{1, 2, \ldots, m\}$ with their natural order, i.e. $1 < 2 < 3 < \cdots < m$. We do not lose the generality since there exists a bijective map between the set Q and any other set of a finite order m.

Definition 17. An m-tuple of maps $T = (\mu_1, \mu_2, \ldots, \mu_m)$ of a set Q such that any map μ_i is a permutation of the set Q will be called an *m-tuple of permutations of the set Q*.

In other words, the tuple M is a vector whose co-ordinates are m fixed maps of the set Q, the permutation tuple T consists of m permutations of the group S_Q.

Example 1. *Let $Q = \{1, 2, 3\}$. The following ordered sets of permutations are 3-tuples of permutations: $T_1 = (\varepsilon, (123), (132))$, $T_2 = ((12), (13), (132))$.*

Definition 18. If $M_1 = (\mu_{a_1}, \mu_{a_2}, \ldots, \mu_{a_m})$ and $M_2 = (\nu_{a_1}, \nu_{a_2}, \ldots, \nu_{a_m})$ are m-tuples of maps defined on a set Q, $Q = \{a_1, a_2, \ldots, a_m\}$, then the product $M_1 * M_2$ is an m-tuple of the form $(\mu_{a_1}\nu_{a_1}, \mu_{a_2}\nu_{a_2}, \ldots, \mu_{a_m}\nu_{a_m})$.

Below we shall omit usually a symbol of an operation of the product of m-tuples.

Proposition 5. *The set $\mathcal{M}$ of all m-tuples of maps, defined on a non-empty set Q of order m, forms a semigroup $(\mathcal{M}, *)$ relative to the operation $*$. The semigroup $(\mathcal{M}, *)$ is isomorphic to the direct product of m copies of the symmetric semigroup $\mathfrak{S}_Q$, i.e. $(\mathcal{M}, *) \simeq \mathfrak{S}_Q \times \mathfrak{S}_Q \times \cdots \times \mathfrak{S}_Q = \bigotimes_{i=1}^{m} (\mathfrak{S}_Q)_i$, $|(\mathcal{M}, *)| = (m^m)^m$.*

Proof. We omit the proof, since it is easy and standard. □

Corollary 1. *([34]) The set $\mathcal{P}$ of all m-tuples of permutations, defined on a non-empty set Q of order m, forms a group $(\mathcal{P}, *)$ relative to the operation $*$. The group $(\mathcal{P}, *)$ is isomorphic to the direct product of m copies of the symmetric group S_Q, i.e. $(\mathcal{P}, *) \simeq S_Q \times S_Q \times \cdots \times S_Q = \bigotimes_{i=1}^{m} (S_Q)_i$, $|(\mathcal{P}, *)| = (m!)^m$.*

Proof. We also omit the proof, since it is easy and standard. □

1.6 Connections between groupoids and m-tuples of maps, kinds of tuples

Let (Q, A) be a finite groupoid of order m which is defined on the well-ordered set $Q = \{1, 2, \ldots, m\}$. This groupoid defines two sets of translations, namely the set of all left translations and the set of all right translations. It is clear, that the last statement is true for any groupoid, not only for a finite groupoid (Q, A).

Moreover, the groupoid (Q, A) defines uniquely two m-tuples of maps, namely $T_1 = (L_1, L_2, \ldots, L_m)$ and $T_2 = (R_1, R_2, \ldots, R_m)$.

Any of the m-tuples T_1 and T_2 specifies the groupoid (Q, A) uniquely if we indicate a method (rows or columns) of filling Cayley table of groupoid (Q, A).

It is easy to see that any m-tuple of maps $T = \{\mu_1, \mu_2, \ldots, \mu_m\}$ of a well-ordered set Q, $|Q| = m$, defines uniquely the following two groupoids: groupoid (Q, A), in which the maps μ_i are left translations and groupoid (Q, B), in which the maps μ_i are right translations.

We shall denote an m-tuple T of maps that consists of all left (respectively, right, middle, inverse of left, inverse of right, inverse of middle) translations of a groupoid (Q, A) by T^l (respectively, by T^r, T^p, T^{Il}, T^{Ir}, T^{Ip}). In this case we shall say that the tuple T^l has the *kind* l, or we shall say that the tuple T^l is of the *kind* l.

Remark 6. A kind of maps (of permutations) defines the way of writing the maps (the permutations) in a square (in a permutation square) S. The left translations correspond to rows of the square S, the right translations correspond to columns of the square S and the middle translations correspond to cells of the square S (see Example 3).

We denote by $\mathcal{T}^l(Q)$ the class of all m-tuples of maps of the kind l, which are defined on a well ordered set Q, $|Q| = m$, and denote by $\mathcal{G}(Q)$ the class of all groupoids defined on the set Q.

By the analogy with m-tuples of maps, we shall denote a square S that consists of all left (respectively, right, middle, inverse to the left, inverse to the right, inverse to the middle) translations of a groupoid (Q, A) by S^l (respectively, by S^r, S^p, S^{Il}, S^{Ir}, S^{Ip}).

We denote by $\mathbb{S}^l(Q)$ the class of all squares of the kind l that are defined on a set Q. In conditions of Remark 3 and Remark 4 we can formulate the following

Proposition 6. *There exist bijections between the classes $\mathcal{T}^l(Q)$, $\mathbb{S}^l(Q)$, $\mathbb{S}^r(Q)$ and $\mathcal{G}(Q)$.*

It is well known that a Latin square L defines m-tuples of permutations of all six kinds. If $\mathcal{Q}(Q)$ denotes the class of all quasigroups that are defined on a well ordered set Q, then Proposition 6 is also true for classes of tuples and classes of squares of the kinds $\{Il, Ir, p, Ip\}$.

Proposition 7. *Any permutation square defines m-tuples of at least of three kinds.*

Proof. From the definition of a permutation square it follows that a permutation square defines at least one m-tuple of permutations T. Since the tuple T is a permutation tuple, then T^{-1} is a permutation tuple, too. □

Example 2. *The permutation square*

$$S = \begin{array}{cc} 1 & 2 \\ 1 & 2 \end{array}$$

defines the following 2-tuples: $T_1 = (L_1, L_2) = (\varepsilon, \varepsilon)$ of the kind l, $T_2 = (L_1^{-1}, L_2^{-1}) = (\varepsilon, \varepsilon)$ of the kind Il and $T_3 = (R_1, R_2)$ of the kind r, where $R_1(1) = R_1(2) = 1$, $R_2(1) = R_2(2) = 2$.

Proposition 8. *If a square $S(Q)$ defines m-tuples of permutations of the kind l and r, then this square is a Latin square.*

Proof. Let $Q = \{a_1, \ldots, a_m\}$. We denote by T_1 the m-tuple of permutations of kind l and by T_2 the m-tuple of permutations of the kind r which generate the square $S(Q)$.

If we suppose that there exist permutations p_1 and p_2 of the m-tuple T_1 such that $p_1(a_i) = p_2(a_i) = a_j$, then the column number a_i contains twice the element a_j, therefore the square $S(Q)$ does not define an m-tuple of the kind r.

If we suppose that there exist permutations p_1 and p_2 of the m-tuple T_2 such that $p_1(a_i) = p_2(a_i) = a_j$, then the row number a_i contains twice the element a_j, therefore the square $S(Q)$ does not define an m-tuple of the kind l.

Therefore, if a permutation square $S(Q)$ defines m-tuples of the kind l and r, then this square is a Latin square. □

Proposition 9. *A square $S(Q)$ defines an m-tuple of permutations of the kind p if and only if this square is a Latin square.*

Proof. Let $Q = \{a_1, \ldots, a_m\}$. We suppose that the square $S(Q)$ defines the m-tuple T of permutations of the kind p. We recall $p_x(y) = z$, where p_x is a middle translation of the groupoid (Q, A) which corresponds to the square $S(Q)$, means that in the square $S(Q)$ in the position (y, z) the element x is situated.

If we suppose that there exist permutations p_{a_x} and p_{a_y} $(a_x \neq a_y)$ of the m-tuple T such that $p_{a_x}(a_i) = p_{a_y}(a_i) = a_j$, then we have that in the position (a_i, a_j) the elements a_x and a_y are situated simultaneously.

Therefore we can conclude that the m-tuple T contains pairwise different permutations of the set Q such that "$p_i p_j^{-1}$ leaves no variables unchanged for $i \neq j$ ", i.e. the square $S(Q)$ is a Latin square.

It is easy to see that any Latin square defines an m-tuple of the kind p. □

Corollary 2. *Any permutation square S defines one or three m-tuples of permutations from the following set of the kinds of m-tuples of permutations $\{l, r, p\}$.*

Proof. The proof follows from Example 2, Propositions 8 and 9. □

We notice it is possible to define tuples of maps of an infinite groupoid.

1.7 The τ-property of m-tuples of permutations

We denote the property of a set of permutations $\{p_1, p_2, \ldots, p_m\}$ of an m-element set Q "$p_i p_j^{-1}$ $(i \neq j)$ leaves no variable unchanged" [30] as the τ-property. An m-tuple of permutations T can also have the τ-property. We shall call the m-tuple T as a τ-m-tuple.

In [30], in fact, Mann proves the following

Theorem 1. *A set $T = \{p_1, p_2, \ldots, p_m\}$ of m permutations of a finite set Q of order m of a kind α, where $\alpha \in \{l, Il, r, Ir\}$, defines Cayley table of a quasigroup if and only if T has the τ-property.*

A permutation α of a finite non-empty set Q which leaves no elements of the set Q unchanged will be called a *fixed point free permutation.*

Definition 19. Let Q be a non-empty finite set of an order m. A set $M = \{\mu_1, \mu_2, \ldots, \mu_m\}$ of m maps of the set Q is called *strictly transitive* (more precise, the set M acts on the set Q strictly transitively) if for any pair of elements x, y of the set Q there exists a unique map μ_j of the set Q such that $\mu_j(x) = y$.

Theorem 2. *A set $M = \{\mu_1, \mu_2, \ldots, \mu_m\}$ of maps of a finite set Q of order m is a strictly transitive set if and only if M is a set of permutations of the set Q.*

Proof. Let $Q = \{1, 2, \ldots, m\}$. We construct the map θ_M of the set Q^2 in the following way $\theta_M : (j; x) \mapsto (j; \mu_j(x))$, i.e.

$$\begin{array}{lcl}
(1;1) & \longrightarrow & (1;\mu_1(1)) \\
(1;2) & \longrightarrow & (1;\mu_1(2)) \\
\ldots & \ldots & \ldots \\
(1;m) & \longrightarrow & (1;\mu_1(m)) \\
(2;1) & \longrightarrow & (2;\mu_2(1)) \\
(2;2) & \longrightarrow & (2;\mu_2(2)) \\
\ldots & \ldots & \ldots \\
(m;m) & \longrightarrow & (m;\mu_m(m)).
\end{array}$$

The set M is a strictly transitive set of maps if and only if the map θ_M is a permutation of the set Q.

If θ_M is a permutation of the set Q^2, then $|Im\,\mu_i| = m$ for any map μ_i. Indeed, if we suppose that there exists a map μ_j such that $|Im\,\mu_i| < m$, then we obtain that θ_M is not a permutation of the set Q^2. □

An m-tuple of permutations also can have the property of strictly transitivity.

Theorem 3. *A set $T = \{p_1, p_2, \ldots, p_m\}$ of m permutations of a finite set Q of order m is strictly transitive if and only the set T has the τ-property.*

Proof. Mann (Theorem 1) proved that the set T of m permutations of an m-element set Q defines a Latin square if and only if the set T has the τ-property. He also proved ([30]) that the set T has the property of strict transitivity if and only if the set T defines a Latin square.

Therefore we can conclude that for the set T the τ-property and the property of strict transitivity are equivalent. □

Proposition 10. *An m-tuple of permutations T is a tuple of the kind p or of the kind Ip if and only if the tuple T is a τ-m-tuple of permutations.*

Proof. The proof follows from Proposition 9. □

Any m-tuple $T = (p_1, p_2, \ldots, p_m)$ defines m-tuple T^{-1} such that $T^{-1} = (p_1^{-1}, p_2^{-1}, \ldots, p_m^{-1})$.

Proposition 11. *An m-tuple $T = (p_1, p_2, \ldots, p_m)$ has the τ-property if and only if the m-tuple T^{-1} has the τ-property.*

Proof. From Theorem 3 it follows that this proposition will be proved if we prove the following equivalence: an m-tuple $T = (p_1, p_2, \ldots, p_m)$ is strictly transitive m-tuple if and only if the m-tuple T^{-1} is strictly transitive.

But it is easy to see the the following statements are equivalent: $(\forall\ a, b \in Q)\ (\exists!\ p_i \in T)\ p_i(a) = b$ and $(\forall\ a, b \in Q)\ (\exists!\ p_i^{-1} \in T^{-1})\ p_i^{-1}(b) = a$. □

Proposition 12. *An m-tuple of permutations $T = (p_1, p_2, \ldots, p_m)$ has the τ-property if and only if the m-tuple $pTq = (pp_1q, pp_2q, \ldots, pp_mq)$, where p, q are some fixed permutations of the set Q, has the τ-property.*

Proof. It is easy to see that the following statements are equivalent: "for any fixed elements $a, b \in Q$ there exists an unique permutation $p_i \in T$ such that $p_i(a) = b$" and "for any fixed elements $a, b \in Q$ there exists a unique permutation $p_iq \in Tq$ such that $p_iq(a) = q(b)$".

Since elements a, b are arbitrary fixed elements of the set Q, we can denote the element $q(b)$ by b_1. Therefore, we can re-write the last statement in the following equivalent form "for any fixed elements $a, b_1 \in Q$ there exists a unique permutation $p_iq \in Tq$ such that $p_iq(a) = b_1$".

The last statement is equivalent to the following "for any fixed elements $a, b_1 \in Q$ there exists a unique permutation $pp_iq \in pTq$ such that $pp_iq(a) = p(b_1)$".

Similarly, as it was pointed above, further we can re-write the last statement in the following equivalent form "for any fixed elements $a, b_2 \in Q$ there exists a unique permutation $pp_iq \in pTq$ such that $pp_iq(a) = b_2$", where $b_2 = p(b_1)$. □

Remark 7. In fact, Proposition 12 in an other form can be found in article of Mann [30].

Corollary 3. *An m-tuple of permutations $pT = (pp_1, pp_2, \dots, pp_m)$ has the τ-property if and only if the m-tuple $Tp = (p_1p, p_2p, \dots, p_mp)$, where p is a permutation of the set Q, has the τ-property.*

Proof. By Proposition 11 we have that an m-tuple pT has the τ-property if and only if the m-tuple $p^{-1}pTp = Tp$ has the τ-property. □

Corollary 4. *An m-tuple of permutations $T = (p_1, p_2, \dots, p_m)$ has the τ-property if and only if the m-tuple $p^{-1}Tp = (p^{-1}p_1p, p^{-1}p_2p, \dots, p^{-1}p_mp)$, where p is a permutation of a set Q, has the τ-property.*

Proof. It is easy to see. □

Lemma 6. *In a quasigroup $(Q, \cdot)$ any of the sets $\mathbf{L}(Q, \cdot)$, $\mathbf{R}(Q, \cdot)$, $\mathbf{P}(Q, \cdot)$, $\mathbf{L}^{-1}(Q, \cdot)$, $\mathbf{R}^{-1}(Q, \cdot)$ and $\mathbf{P}^{-1}(Q, \cdot)$ has the τ-property.*

Proof. Let us suppose the contrary that there exist translations L_a, L_b, $a \neq b$, of a quasigroup $(Q, \cdot)$ and an element $x \in Q$ such that $L_aL_b^{-1}x = x$. If in the last equality we change the element x by the element L_bx, then we obtain $L_ax = L_bx$, $a \cdot x = b \cdot x$, $a = b$. We received a contradiction. Therefore the set $\mathbf{L}(Q, \cdot)$ has the τ-property.

Similarly it can be proved the remaining cases. □

Remark 8. Any of the sets $\mathbf{L}$, $\mathbf{R}$, $\mathbf{P}$, $\mathbf{L}^{-1}$, $\mathbf{R}^{-1}$ and $\mathbf{P}^{-1}$ of a quasigroup $(Q, \cdot)$ defines this quasigroup in the unique way. Indeed, we can take into consideration the agreements of Remark 4 and the fact that all these quasigroup translations are indexed by the elements of set Q.

Example 3. *If $P_1^{-1} = (23)$, $P_2^{-1} = (13)$, $P_3^{-1} = (12)$ are inverse permutations for middle translations of a quasigroup $(Q, \circ)$, then we can construct $(Q, \circ)$ in the following way:*

	1	2	3
1	1		
2			1
3		1	

	1	2	3
1	1		2
2		2	1
3	2	1	

$\circ$	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

We can supplement Proposition 6 in the following way. Let Q be a finite well ordered set.

We denote:

- by $\mathcal{LQ}(Q)$ the class of all left quasigroups, which are defined on the set Q;

- by $\mathcal{Q}(Q)$ the class of all quasigroups, which are defined on the set Q;

- by $\mathbb{PS}(\mathcal{LQ})$ ($\mathbb{PS}(\mathcal{Q})$) the class of all permutation squares, which are bodies of Cayley tables of left quasigroups (quasigroups) from $\mathcal{LQ}(Q)$ ($\mathcal{Q}(Q)$);

- by $\mathfrak{T}^{\alpha}(Q)$ we denote the class of m-tuples of permutations of a kind α, $\alpha \in \{l, Il, r, Ir, p.Ip\}$ that are defined on the set Q.

In conditions of Remark 3 and Remark 4 is true the following

Proposition 13. *(i) There exist bijections between the classes $\mathcal{LQ}(Q)$, $\mathbb{PS}(\mathcal{LQ})$ and $\mathfrak{T}^{\alpha}(Q)$, $\alpha \in \{l, Il\}$;*

(ii) there exist bijections between the classes $\mathcal{Q}(Q)$, $\mathbb{PS}(\mathcal{Q})$ and $\mathfrak{T}^{\alpha}(Q)$, $\alpha \in \{l, Il, r, Ir, p.Ip\}$.

Proof. The proof follows from results of Subsection 1.6 and this subsection. □

Proposition 14. *A τ-m-tuple T of a finite set Q of order m "defines" six Latin squares, namely: L^l, L^r, L^p, L^{Il}, L^{Ir}, L^{Ip}, which correspond to six quasigroups (Q, A), $(Q, A^{(12)})$, $(Q, A^{(132)})$, $(Q, A^{(23)})$, $(Q, A^{(123)})$ and $(Q, A^{(13)})$, respectively.*

Proof. The tuple T can have the following kinds $\{l, r, p, Il, Ir, Ip\}$. Thus this tuple defines six Latin squares. If we denote the Latin square, that corresponds to the tuple T^l by L^l, then we can denote other Latin squares by L^r, L^p, L^{Il}, L^{Ir}, L^{Ip}. If we denote the quasigroup that corresponds to the square L^l by (Q, A), then other five quasigroups are $(Q, A^{(12)})$, $(Q, A^{(132)})$, $(Q, A^{(23)})$, $(Q, A^{(123)})$ and $(Q, A^{(13)})$, respectively. □

Corollary 5. *Latin squares L^l, L^r, L^p, L^{Il}, L^{Ir} and L^{Ip} which are constructed from a τ-m-tuple T define at most six τ-m-tuples, namely six tuples that are left, right, middle translations and their inverse one's of the quasigroup (Q, A) which corresponds to the square L^l.*

Proof. Any of Latin squares L^l, L^r, L^p, L^{Il}, L^{Ir} and L^{Ip} from Proposition 14 defines six, in general various, τ-m-tuples of permutations. But, as it follows from Table 1, any of this 36 τ-m-tuples of permutations coincides with the τ-m-tuples which are left (=T), right, middle translations and their inverse one's of the quasigroup (Q, A). □

It is not very difficult to understand that the number n of various τ-m-tuples which can be constructed from a τ-m-tuple T, using the way of Proposition 14, is equal to 1, 2, 3 or 6.

For example, it is easy to see, if the tuple T defines a TS-quasigroup, then $n = 1$, since in any TS-quasigroup $(Q, \cdot)$ all its parastrophes coincide with $(Q, \cdot)$ [4]. We notice TS-quasigroup of order 3 is given in Example 3.

1.8 Definitions of orthogonality of groupoids, squares and m-tuples

One of the most frequently applied and historically one of the first studied properties of Latin squares is the property of orthogonality. Orthogonality of quasigroups and Latin squares is used by application of quasigroups in Coding Theory and Cryptology [17]. The famous Euler problem on Latin squares is devoted to the question of the existence of a pair of orthogonal Latin squares of order $4k + 2$, $k \in N$ [17,27].

Definition 20. ([30]). Two $m \times m$ squares S_1 and S_2, defined on the sets Q_1 and Q_2 respectively, $|Q_1| = |Q_2| = m$, are called orthogonal if when one is superimposed upon the other every ordered pair of variables occurs once in the resulting square, i.e. the resulting square S_{12} is defined on the set $Q_1 \times Q_2$.

Example 4. *Let a square S_1 be defined on the set $Q_1 = \{1, 2, 3, 4\}$, a square S_2 be defined on the set $Q_2 = \{a, b, c, d\}$. Let*

$$S_1 = \begin{array}{cccc} 1 & 2 & 3 & 3 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 3 & 3 \\ 4 & 4 & 4 & 4, \end{array} \quad S_2 = \begin{array}{cccc} a & a & a & b \\ b & c & b & c \\ d & d & c & d \\ a & b & c & d. \end{array} \quad \textit{Then } S_{12} = \begin{array}{cccc} 1a & 2a & 3a & 3b \\ 1b & 1c & 2b & 2c \\ 2d & 1d & 3c & 3d \\ 4a & 4b & 4c & 4d. \end{array}$$

Proof. The squares S_1 and S_2 are orthogonal since the square S_{12} is defined on the set $Q_1 \times Q_2$. □

We can give the following definition.

Definition 21. We suppose that $m \times m$ squares S_1 and S_2 are defined on the sets Q_1 and Q_2, respectively. We define the operation $\oplus$ of *superimposition of the squares* S_1 and S_2 in the following way: $S_1 \oplus S_2 = S_{12}$ is an $m \times m$ square such that in any position (i, j), $i, j \in \{1, 2, \ldots, m\}$, in S_{12} is arranged an ordered pair of elements (a, b), where the element a is arranged in position (i, j) in the square S_1 and the element b is arranged in position (i, j) in the square S_2.

It is easy to see that the square S_{12} is defined on the set Q_{12} such that $Q_{12} \subseteq Q_1 \times Q_2$.

In language of notions of Definition 21 we can re-write Definition 20 in the following form.

Definition 22. Two $m \times m$ squares S_1 and S_2, defined on the sets Q_1 and Q_2 respectively, $|Q_1| = |Q_2| = m$, are called orthogonal if and only if $D(S_1 \oplus S_2) = Q_1 \times Q_2$.

Definition 23. If a square $S_2(Q_2)$ is Cayley table of a groupoid (Q_2, B) and a square $S_1(Q_1)$ is Cayley table of a groupoid (Q_1, A), then the square $S_2(Q_2)$ is an isotopic image of the square $S_1(Q_1)$ with an isotopy T if and only if $(Q_2, B) = (Q_1, A)T$.

We formulate well known lemma which is a mathematical folklore.

Lemma 7. *Squares $S_1(Q_1)$ and $S_2(Q_2)$ are orthogonal if and only if their isotopic images are orthogonal with the isotopies of the form $T_1 = (\varepsilon, \varepsilon, \varphi)$ and $T_2 = (\varepsilon, \varepsilon, \psi)$, respectively.*

Proof. We recall the isotopy T_1 changes an element $b \in S_1(Q_1)$ with co-ordinates (i, j) by the element $\varphi b \in S_1(Q_1)T_1$ with co-ordinates (i, j).

If $S_1(Q_1)T_1$ is an isotopic image of a square $S_1(Q_1)$, $S_2(Q_2)T_2$ is an isotopic image of a square $S_2(Q_2)$ and $D(S_1(Q_1) \oplus S_2(Q_2)) = Q_1 \times Q_2$, then $D(S_1(Q_1)T_1 \oplus S_2(Q_2)T_2) = \varphi(Q_1) \times \psi(Q_2)$. □

Corollary 6. *Squares $S_1(Q_1)$ and $S_2(Q_2)$ are orthogonal if and only if are orthogonal the squares $S_1(Q_1)$ and $S_2'(Q_1) = S_2(Q_2)T_2$, where ψ is a third component of isotopy T_2 such that $\psi(Q_2) = Q_1$.*

Proof. In conditions of Lemma 7 it is sufficient to suppose that $\varphi = \varepsilon$ and to choose the component ψ of the isotopy T_2 such that $\psi(Q_2) = Q_1$. □

Remark 9. Below in this article we shall study only orthogonality of squares, which are defined on the same set Q.

Definition 24. ([17]). Two groupoids $(Q, \cdot)$ and $(Q, *)$ defined on the same set Q are said to be *orthogonal* if the system of equations $x \cdot y = a$ and $x * y = b$ (where a and b are any two given elements of Q) has a unique soluion.

We shall denote a fact that groupoids $(Q, \cdot)$ and $(Q, *)$ are orthogonal by $(Q, \cdot) \perp (Q, *)$. There exist various generalizations of Definitions 20 and 24 on n-ary case, i.e. on hypercubes and n-ary groupoids [2, 26].

1.9 Numerical estimations for the property of orthogonality of squares

It is well known that on a finite set G of an order m there exist $(m)^{m^2}$ binary groupoids and $(m)^{m^2}$ squares.

Following [17] we shall call any square S_2 which is orthogonal to a square S_1 *orthogonal mate of a square* S_1. Similarly, we shall call any groupoid (G, B) which is orthogonal to a groupoid (G, A) orthogonal mate, too.

In [17] (on page 155) there are necessary and sufficient conditions for a Latin square in order to have an orthogonal mate.

We give the similar condition for a square to have an orthogonal mate.

Lemma 8. *An $m \times m$ square S defined on the set $Q = \{1, 2, \ldots, m\}$ has an orthogonal mate if and only if in this square there are m entries of any element of the set Q.*

Proof. This proof is a version of the proof of Theorem 5.1.1 from [17]. Let $S(Q)$ be an $m \times m$ square with m entries of any element of the set Q. We will be able to construct an orthogonal mate to the square S if and only if we will be able to change all entries of the element 1 in the square S by all elements of the set Q in any order, all entries of the element 2 in the square S by all elements of the set Q in any order and so on. □

The proof of Lemma 8 provides, probably, one of the most universal and the most simple methods of construction of an orthogonal mate to any binary groupoid which has such a mate. In [3] V.D. Belousov called operations with the property that is similar to the property of squares from Lemma 8 *full operations*.

Corollary 7. *There exist $(n^2)!$ squares defined on a set Q of the order n that have an orthogonal mate.*

Proof. In the square S there exist n^2 cells. To obtain a square with an orthogonal mate we must fill n cells by the element 1. We have $n^2(n^2-1)(n^2-2)\ldots(n^2-n+1)$

different variants to do this. Further we have $(n^2-n)\dots(n^2-2n+1)$ variants to fill remaining cells by the element 2. Therefore we have $n^2(n^2-1)(n^2-2)\dots(n^2-n)(n^2-n-1)\dots(n^2-2n+1)$ variants to write the elements 1 and 2 in the cells of the square S. Further we have $n^2\dots(n^2-3n+1)$ variants to fill the cells of the square S by the elements $1,2,3$ and so on.

Finally, we obtain that we have $(n^2)!$ variants to construct a groupoid with an orthogonal mate. □

Corollary 8. *If a square S which is defined on n-element set Q, $Q=\{1,2,\dots,n\}$, has an orthogonal mate, then there exist at least $(n!)^n$ squares which are orthogonal to the square S.*

Proof. The proof follows from Lemma 8. We can fill all entries of the element 1 by all elements of the square Q in any order, we can fill all entries of the element 2 by all elements of the square Q in any order and so on. □

1.10 Orthogonality in works of V.D. Belousov

In a series of articles, see, for example, [3,5,7,10,11], V.D. Belousov studied the property of orthogonality of binary and n-ary operations and systems of operations from algebraic and geometric point of view. Later his researches were continued by his pupils and by many others mathematicians.

In this subsection we suppose that all binary operation are defined on the same non-empty set $Q=\{1,2,\dots,m\}$.

V.D. Belousov by his study of the property of orthogonality used the idea, that a pair of binary operations $A(x,y)$ and $B(x,y)$ defines a map θ of the set Q^2 such that $\theta(x,y)=(A(x,y),B(x,y))$. It is easy to see that the operations A and B are orthogonal if and only if θ is a permutation of the set $Q\times Q$.

Following [3,5], the binary operation $F(x,y)=x$ for all $x,y\in Q$ will be called *the left identity operation*, the operation $E(x,y)=y$ will be called *the right identity operation*. It is easy to see that the squares F and E that correspond to the groupoids (Q,F) and (Q,E), respectively, have the forms

$$F=\begin{array}{cccc} 1 & 1 & \dots & 1 \\ 2 & 2 & \dots & 2 \\ \dots & \dots & \dots & \dots \\ m & m & \dots & m, \end{array} \qquad E=\begin{array}{cccc} 1 & 2 & \dots & m \\ 1 & 2 & \dots & m \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & m. \end{array}$$

It is easy to see that to the square F corresponds to the m-tuple $T^r_\varepsilon=(\varepsilon,\varepsilon,\dots,\varepsilon)$ of the kind r and the square E corresponds to the m-tuple $T^l_\varepsilon=(\varepsilon,\varepsilon,\dots,\varepsilon)$ of the kind l.

We re-formulate the well known [34], [5], [17], [27] results on orthogonality of left quasigroups, right quasigroups and quasigroups with the identity permutation squares of the kind l and r in the following manner:

Lemma 9. *(i) A square S is a permutation square of the kind l or the kind Il if and only if $S \perp F$;*

(ii) a square S is a permutation square of the kind r or the kind Ir if and only if $S \perp E$;

(iii) a permutation square S of the kind l is a Latin square if and only if $S \perp E$;

(iv) a permutation square S of the kind r is a Latin square if and only if $S \perp F$;

(v) a square S is a Latin square if and only if $S \perp F$ and $S \perp E$.

We denote by F_p^r the square, which is determined by the following tuple of permutations $T^r = (p, p, \ldots, p)$, and we denote by E_g^l the square, which is determined by the following tuple of permutations $T^l = (g, g, \ldots, g)$, where p and g are permutations of the set $Q = \{1, 2, \ldots, m\}$.

We can re-write Lemma 9 in the following form:

Lemma 10. *(i) A square S is a permutation square of the kind l or the kind Il if and only if $S \perp F_p^r$;*

(ii) a square S is a permutation square of the kind r or the kind Ir if and only if $S \perp E_g^l$;

(iii) a permutation square S of the kind l is a Latin square if and only if $S \perp E_g^l$;

(iv) a permutation square S of the kind r is a Latin square if and only if $S \perp F_p^r$;

(v) a square S is a Latin square if and only if $S \perp F_p^r$ and $S \perp E_g^l$.

1.11 Mann's product of permutation squares and product of squares

In [30] H.B. Mann defined the product of two permutation squares in such a way: "Denote now by an m sided square S any set of m permutations $(s_1, s_2, \ldots, s_m)$ and by the product SS' of two squares S and S' the square $(s_1 s'_1, s_2 s'_2, \ldots, s_m s'_m)$".

Using Definition 17 we can give Mann's definition of product of squares and corresponding groupoids in the following form.

Definition 25. If $(p_1, p_2, \ldots, p_m)$ and $(q_1, q_2, \ldots, q_m)$ are m-tuples of the kind l of the permutation squares L_1 and L_2 respectively, then the product $L_1 L_2$ is the permutation square $(p_1 q_1, p_2 q_2, \ldots, p_m q_m)$ of the same kind.

Using Definition 25 of the product of squares it is possible to define the concept of the power of a square and, in particular, the concept of the power of a Latin square.

We can give the following generalization of Definition 25.

Definition 26. If $(p_1, p_2, \ldots, p_m)$ and $(q_1, q_2, \ldots, q_m)$ are m-tuples of maps of some fixed kinds of squares L_1 and L_2, respectively, then the product $L_1 L_2$ is the square $(p_1 q_1, p_2 q_2, \ldots, p_m q_m)$ of an admissible kind.

We notice, in general, $L_1^l L_2^l \neq L_1^r L_2^r$.

In conditions of Definition 26 the multiplication of a pair of Latin squares L_1 and L_2 defines at least $6^2 \cdot 4 = 144$ squares. Indeed, $L_1^\alpha L_2^\beta = L^\gamma$, where $\alpha, \beta \in$

$\{l, r, p, Il, Ir, Ip\}$, $\gamma \in \{l, r, Il, Ir\}$. The multiplication of a pair of Latin squares of equal kinds defines at least 24 squares.

Example 5. *If T_1 and T_2 are some m-tuples of maps, then m-tuple $T = T_1T_2$ defines a square of kind α, where $\alpha \in \{l, r\}$.*

If T_1 and T_2 are some m-tuples of permutations, then m-tuple $T = T_1T_2$ defines a permutation square of kind α, where $\alpha \in \{l, r, Il, Ir\}$.

If, in addition, the m-tuple T has the τ-property, then T defines six Latin squares of any kind from the set of kinds $\{l, r, p, Il, Ir, Ip\}$.

Remark 10. Below in this article we shall suppose that we multiply squares only of equal kinds α and that resulting square also has the kind α.

2 Orthogonality and parastroph orthogonality

We give necessary and sufficient conditions of orthogonality of permutation squares, Latin squares, quasigroups and their parastrophes.

2.1 Orthogonality of quasigroups and left quasigroups

In this subsection we give necessary and sufficient conditions of orthogonality of permutation squares, Latin squares, quasigroups and left (right) quasigroups.

Below in this article we shall suppose that we multiply squares only of equal kinds α and that resulting square also has the kind α.

For Latin squares H.B. Mann proved the following basic theorem [30], which we give in a bit more general form. See, also, [17, 27, 34].

Theorem 4. *Permutation squares L_1 and L_2 of kind α, $\alpha \in \{l, Il, r, Ir\}$, are orthogonal if and only if there exists a Latin square L_3 such that $L_3L_1 = L_2$.*

Proof. Let $L_1 \perp L_2$, $\alpha = l$. We suppose that m-tuple $T_1 = (p_1, p_2, \ldots, p_m)$ corresponds to the permutation square L_1, m-tuple $T_2 = (q_1, q_2, \ldots, q_m)$ corresponds to the permutation square L_2.

If we superimpose the square L_1 on the square L_2, then in any cell (i, j) of the square of pairs P we shall have the pair $(p_i(j), q_i(j))$. The fact that the squares L_1 and L_2 are orthogonal means that in the square P any pair of elements $(x, y) \in Q \times Q$ appears exactly one time.

In other words for any pair of elements (a, b), where a, b are some fixed elements of the set Q, there exists unique pair of elements $i, j \in Q$ such that $p_i(j) = a$ and $q_i(j) = b$.

Since $p_i^{-1}(a) = j$, further we have $q_i p_i^{-1}(a) = b$. The last equality means that the tuple $T_2T_1^{-1} = (q_1p_1^{-1}, q_2p_2^{-1}, \ldots, q_mp_m^{-1})$ is a strictly transitive set of permutations that acts on the set Q.

From Theorem 3 it follows that the tuple $T_2T_1^{-1}$ has the τ-property. Then the tuple $T_2T_1^{-1}$ defines a Latin square. It is easy to see that if the $T_2T_1^{-1}$ defines the Latin square L_3 of the kind l, then $L_3 = L_2L_1^{-1}$.

Converse. Let τ-m-tuple $T_1 = (p_1, p_2, \dots, p_m)$ (respectively, $T_2 = (q_1, q_2, \dots, q_m)$, $T_3 = (s_1, s_2, \dots, s_m)$) of the kind l correspond to the permutation square L_1 (L_2, L_3, respectively).

The equality $L_3 L_1 = L_2$ means that $s_i(p_i(j)) = q_i(j)$ for any fixed element $p_i(j) \in Q$. Since the squares L_1 and L_2 are permutations squares, then in every row of the square of pairs P the set of the first components of pairs is equal to the set Q and the set of the second components of any row of the square P coincides with the set Q, too.

Since the tuple T_3 is a strictly transitive set of permutations that acts on the set Q, we obtain that for any pair of elements $(a, b) \in Q^2$ there exists a unique element $s_i \in T_3$ such that $s_i(a) = b$, i.e. $s_i(p_i(j)) = q_i(j)$, for an element j of the set Q.

Therefore, in the square P any ordered pair (a, b) appears exactly one time, i.e. $L_1 \perp L_2$.

For permutation squares of the kind Il, r, Ir the proof is similar. □

Remark 11. Theorem 4 describes all orthogonal mates of a permutation square L_1 which are permutation squares, but, in general, there exist orthogonal mates of the square L_1 which are not permutation squares. For example, $L_1 \perp L_2$, but L_2 is not a permutation square:

$$L_1 = \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 3, \end{array} \qquad L_2 = \begin{array}{ccc} 1 & 1 & 1 \\ 3 & 3 & 2 \\ 2 & 3 & 2. \end{array}$$

We denote the number of all Latin squares that are defined on a set Q of an order m by $\mathfrak{L}(m)$.

Corollary 9. *The number of permutation squares of the kind l that are defined on a set Q of order m and that are orthogonal to a fixed permutation square $S(Q)$ of the kind l is equal to the number $\mathfrak{L}(m)$.*

Proof. This is a direct consequence of Theorem 4. □

Corollary 10. *Latin squares L_1 and L_2 of a kind α are orthogonal if and only if the square $L_2 L_1^{-1}$ is a Latin square of the kind α, where $\alpha \in \{l, r, Il, Ir\}$.*

Proof. In is easy to see. □

The problem of construction of a Latin square L_j which is orthogonal to a fixed Latin square L is reduced to the problem when Mann's product of two Latin squares (of a square L_j and the square L^{-1}) is a Latin square. We think, it is possible to use computer by the check if Mann's product of Latin squares is a Latin square.

Corollary 11. *Latin squares L_1 and L_2 are orthogonal if and only if $L_1 L_2^{-1}$ is a Latin square.*

Proof. The proof follows from Corollary 10 and the following notice: $L_1 \perp L_2$ if and only if $L_2 \perp L_1$. Then $L_1 \perp L_2$ if and only if $L_1 L_2^{-1}$ is a Latin square. □

Theorem 4 allows us to give the following definition of orthogonality of m-tuples of permutations.

Definition 27. m-Tuples of permutations T_1 and T_2 are called *orthogonal* if $T_1T_2^{-1}$ has the τ-property.

Since the product of squares (Definition 25) is defined with the help of the notion of the product of permutation tuples, we can re-formulate Theorem 4 in the language of m-tuples of permutations.

Theorem 5. *Permutation squares L_1 and L_2 of a kind α, $\alpha \in \{l, Il, r, Ir\}$, are orthogonal if and only if $T_1T_2^{-1}$ is a τ-m-tuple, where T_1, T_2 are m-tuples of permutations of the kind α that correspond to the squares L_1 and L_2, respectively.*

Taking into consideration bijections which we formulated in Proposition 13 we can formulate Theorem 4 for finite right quasigroups, left quasigroups and for quasigroups.

Theorem 6. *Left (right) quasigroups (Q, A) and (Q, B) are orthogonal if and only if there exists a τ-m-tuple T_3 such that $T_3T_A = T_B$, where T_A is an m-tuple of the kind α that corresponds to left (right) quasigroup (Q, A), T_B is an m-tuple of the kind α that corresponds to left (right) quasigroup (Q, B), $\alpha \in \{l, Il\}$ ($\alpha \in \{r, Ir\}$).*

Theorem 7. *Quasigroups (Q, A) and (Q, B) are orthogonal if and only if $T_3 = T_A^{\alpha}(T_B^{\alpha})^{-1}$ is a τ-m-tuple, where T_A^{α} is a τ-m-tuple of the kind α that corresponds to the quasigroup (Q, A), T_B^{α} is a τ-m-tuple of the kind α that corresponds to the quasigroup (Q, B) and $\alpha \in \{l, r, Il, Ir\}$.*

We notice it is possible to formulate conditions of orthogonality of quasigroups on the language of the τ-m-tuples of the kind p. But these conditions differ sufficiently sharply from conditions of orthogonality of quasigroups given in language of the τ-m-tuples of the kinds l and r.

2.2 Orthogonality of quasigroups and its parastrophes

In this subsection we give some conditions of orthogonality of a quasigroup and its parastrophes.

We suppose that $Q = \{1, 2, \ldots, m\}$. For convenience we denote a finite quasigroup (Q, A) by the letter A. We denote m-tuples of translations of the quasigroup A in the following way $\overline{L} = (L_1, L_2, \ldots, L_m)$, $\overline{L^{-1}} = (L_1^{-1}, L_2^{-1}, \ldots, L_m^{-1})$, $\overline{R} = (R_1, R_2, \ldots, R_m)$, $\overline{R^{-1}} = (R_1^{-1}, R_2^{-1}, \ldots, R_m^{-1})$.

Theorem 8. *For a finite quasigroup A the following equivalences are fulfilled:*

(i) $A \perp A^{(12)} \Longleftrightarrow \overline{R}\,\overline{L^{-1}}$ *is a τ-m-tuple;*
(ii) $A \perp A^{(13)} \Longleftrightarrow \overline{R}\,\overline{R}$ *is a τ-m-tuple;*
(iii) $A \perp A^{(23)} \Longleftrightarrow \overline{L}\,\overline{L}$ *is a τ-m-tuple;*
(iv) $A \perp A^{(123)} \Longleftrightarrow \overline{L}\,\overline{R}$ *is a τ-m-tuple;*
(v) $A \perp A^{(132)} \Longleftrightarrow \overline{R}\,\overline{L}$ *is a τ-m-tuple.*

Proof. *(i)* We can identify Cayley table of a quasigroup A with a τ-m-tuple T_1 of the kind r, i.e. T_1 is a vector whose components are all right translations R_a, $a \in Q$, of the quasigroup A.

It is possible to identify Cayley table of the quasigroup $A^{(12)}$ with τ-m-tuple T_2 of the kind r, too, where T_2 is composed of the permutations $R_a^{(12)}$, $a \in Q$. From Table 1 it follows, that $R_a^{(12)} = L_a$.

In order to obtain a criterion of orthogonality of the quasigroups A and $A^{(12)}$ we can apply Theorem 7, since the τ-tuples T_1 and T_2 are of the same kind. Therefore we have that $A \perp A^{(12)}$ if and only if $T_1 T_2^{-1} = (R_1 L_1^{-1}, R_2 L_2^{-1}, \dots, R_m L_m^{-1}) = \overline{R}\,\overline{L^{-1}}$ is a τ-tuple.

(ii) In this case we identify Cayley tables of quasigroups A and $A^{(13)}$ with the τ-m-tuples T_1 and T_2 of the kind r, too. From Table 1 it follows that $R_a^{(13)} = R_a^{-1}$, i. e. $T_2 = (R_1^{-1}, \dots, R_m^{-1})$, where R_a is a right translation of the quasigroup A, $a \in Q$. Application of Theorem 7 gives us that $A \perp A^{(13)}$ if and only if $T_1 T_2^{-1} = (R_1 R_1, R_2 R_2, \dots, R_m R_m) = \overline{R}\,\overline{R} = \overline{R^2}$ is a τ-tuple.

(iii) We identify Cayley tables of quasigroups A and $A^{(23)}$ with the τ-tuples T_1 and T_2 of the kind l. From Table 1 it follows that $L_a^{(23)} = L_a^{-1}$, i. e. $T_2 = (L_1^{-1}, \dots, L_m^{-1})$. Then $T_1 (T_2)^{-1} = \overline{L}\ \overline{L} = \overline{L^2}$. From Theorem 7 it follows that $A \perp A^{(23)}$ if and only if the tuple $\overline{L^2}$ is a τ-m-tuple.

(iv) In this case we identify Cayley tables of quasigroups A and $A^{(123)}$ with the τ-tuples T_1 and T_2 of the kind l. From Table 1 it follows that $L_a^{(123)} = R_a^{-1}$, i. e. $T_2 = (R_1^{-1}, \dots, R_m^{-1})$. Then $T_1 (T_2)^{-1} = \overline{L}\,\overline{R}$. From Theorem 7 it follows that $A \perp A^{(123)}$ if and only if the tuple $\overline{L}\,\overline{R}$ is a τ-m-tuple.

(v) In this case we identify Cayley tables of quasigroups A and $A^{(132)}$ with the τ-tuples T_1 and T_2 of the kind r. From Table 1 it follows that $R_a^{(132)} = L_a^{-1}$, i. e. $T_2 = (L_1^{-1}, \dots, L_m^{-1})$ in this case. Then $T_1 (T_2)^{-1} = \overline{R}\,\overline{L}$. From Theorem 7 it follows that $A \perp A^{(132)}$ if and only if the tuple $\overline{R}\,\overline{L}$ is a τ-m-tuple. □

Since by proving Theorem 8 we do not use the property, that the sets of permutations of a quasigroup $(Q, \cdot)$ are well ordered sets, then it is possible to re-formulate Theorem 8 in the following form.

Theorem 9. *For a finite quasigroup A the following equivalences are fulfilled:*

(i) $A \perp A^{(12)} \Longleftrightarrow \mathbf{RL}^{-1}$ *has the τ-property;*
(ii) $A \perp A^{(13)} \Longleftrightarrow \mathbf{R}^2$ *has the τ-property;*
(iii) $A \perp A^{(23)} \Longleftrightarrow \mathbf{L}^2$ *has a τ-property;*
(iv) $A \perp A^{(123)} \Longleftrightarrow \mathbf{LR}$ *has the τ-property;*
(v) $A \perp A^{(132)} \Longleftrightarrow \mathbf{RL}$ *has the τ-property.*

We recall if the set of permutations $\mathbf{RL}^{-1}$ ($\mathbf{R}^2$, $\mathbf{L}^2$, $\mathbf{LR}$, $\mathbf{RL}$) has the τ-property, then this set defines a Latin square of a kind α, where $\alpha \in \{l, r, p, Il, Ir, Ip\}$.

Corollary 12. *If L is a Latin square that coincides with Cayley table of a quasigroup (Q, A), then:*

(i) the square $L^r L^{Il}$ is a Latin square if and only if $A \perp A^{(12)}$;
(ii) the square $L^r L^r$ is a Latin square if and only if $A \perp A^{(13)}$;
(iii) the square $L^l L^l$ is a Latin square if and only if $A \perp A^{(23)}$;
(iv) the square $L^l L^r$ is a Latin square if and only if $A \perp A^{(123)}$;
(v) the square $L^r L^l$ is a Latin square if and only if $A \perp A^{(132)}$.

Proof. The proof follows from Theorem 8. □

2.3 Orthogonality of quasigroups with its parastrophes in the language of identities and quasi-identities

Conditions of orthogonality of a quasigroup and its parastrophe in language of identities have long and rich history [10, 17, 18, 42]. Very deep and, unfortunately, not finished results in this direction belong to T. Evans ([18], Chapter 7; [14], Chapter 3).

In this subsection we suppose that any quasigroup is defined as an algebra with three binary operations, see Definition 9.

We re-formulate Theorem 8 in language of quasi-identities and prove that it is possible to characterize orthogonality of quasigroups and its σ-conjugates quasigroups in language of identities.

Theorem 10. *For a finite quasigroup $(Q, \cdot)$ the following equivalences are fulfilled:*

(i) $(Q,\cdot)\perp(Q,\cdot)^{(12)} \iff ((x\backslash yz)x = zy \implies x = y) \iff (P_{zy}P_{yz}x = x \implies x = y)$;
(ii) $(Q,\cdot)\perp(Q,\cdot)^{(13)} \iff (zx\cdot x = zy\cdot y \implies x = y) \iff (R_x^2 z = R_y^2 z \implies x = y)$;
(iii) $(Q,\cdot)\perp(Q,\cdot)^{(23)} \iff (x\cdot xz = y\cdot yz \implies x = y) \iff (L_x^2 z = L_y^2 z \implies x = y)$;
(iv) $(Q,\cdot)\perp(Q,\cdot)^{(123)} \iff (x \cdot zx = y \cdot zy \implies x = y) \iff (L_x R_x z = L_y R_y z \implies x = y)$;
(v) $(Q,\cdot)\perp(Q,\cdot)^{(132)} \iff (xz \cdot x = yz \cdot y \implies x = y) \iff (R_x L_x z = R_y L_y z \implies x = y)$.

Proof. *(i)* From Theorem 8 it follows that the tuple $\overline{R}\ \overline{L^{-1}}$ has τ-property. The τ-property means: if $x, y, z \in Q$, $x \neq y$, then the following inequality is fulfilled $(R_x L_x^{-1})(R_y L_y^{-1})^{-1} z \neq z$ for all $x, y, z \in Q$.

Further proof is only a simplification of the last inequality. We can write the last implication in an equivalent form: if $(R_x L_x^{-1})(R_y L_y^{-1})^{-1} z = z$, then $x = y$. We simplify equality $(R_x L_x^{-1})(R_y L_y^{-1})^{-1} z = z$ in the following way: $R_x L_x^{-1} L_y R_y^{-1} z = z$, $(z \to R_y z)$, $R_x L_x^{-1} L_y z = R_y z$, $R_x L_x^{-1}(yz) = zy$, $(x\backslash yz)x = zy$, $(x\backslash yz)\backslash zy = x$, $R_{zy}^{\backslash} R_{yz}^{\backslash} x = x$, (Table 1), $P_{zy}P_{yz}x = x$.

(ii) From Theorem 8 it follows that the tuple $\overline{R}\ \overline{R}$ has τ-property. Then we have: if $x, y, z \in Q$, $x \neq y$, then the following inequality is fulfilled $(R_x R_x)(R_y R_y)^{-1} z \neq z$ for all $x, y, z \in Q$.

We can write the last implication in an equivalent form: if $(R_xR_x)(R_yR_y)^{-1}z = z$, then $x = y$. We simplify equality $(R_xR_x)(R_yR_y)^{-1}z = z$ in the following way: $R_xR_xR_y^{-1}R_y^{-1}z = z$, $(z \to R_yR_yz)$, $R_xR_xz = R_yR_yz$, $zx \cdot x = zy \cdot y$.

Cases *(iii), (iv)* and *(v)* are proved similarly to Case *(i)* and we omit the proofs of these cases. □

We notice it is possible to deduce Theorem 10 from the following Belousov criteria ([5], Lemma 2) of orthogonality of two binary quasigroups.

Theorem 11. *([5]). Quasigroups (Q, A) and (Q, B) are orthogonal if and only if the following binary operation $C(x, y) = A(x, B^{(23)}(x, y))$ is a quasigroup.*

Proof. From Definition 24 it follows that $A \perp B$ if and only if the system

$$\begin{cases} A(x, y) = a \\ B(x, y) = b \end{cases}$$

has a unique solution $(x, y) \in Q^2$ for any fixed elements $a, b \in Q$. The last system is equivalent to the following

$$\begin{cases} A(x, y) = a \\ B^{(23)}(x, b) = y \end{cases} \iff \begin{cases} A(x, B^{(23)}(x, b)) = a \\ B^{(23)}(x, b) = y. \end{cases}$$

We denote the binary operation $A(x, B^{(23)}(x, y))$ by $C(x, y)$. It is easy to see that the operation C is a left quasigroup. Therefore, quasigroups (Q, A) and (Q, B) are orthogonal if and only if the operation C is a right quasigroup. Thus $A \perp B$ if and only if the operation C is a quasigroup. □

We shall denote a quasigroup class: with the quasiidentity $x\backslash yz)x = zy \Longrightarrow x = y$ by $\mathfrak{C}^{(12)}$; with the quasiidentity $zx \cdot x = zy \cdot y \Longrightarrow x = y$ by $\mathfrak{C}^{(13)}$; with the quasiidentity $x \cdot xz = y \cdot yz \Longrightarrow x = y$ by $\mathfrak{C}^{(23)}$; with the quasiidentity $x \cdot zx = y \cdot zy \Longrightarrow x = y$ by $\mathfrak{C}^{(123)}$; with the quasiidentity $xz \cdot x = yz \cdot y \Longrightarrow x = y$ by $\mathfrak{C}^{(132)}$.

Proposition 15. *Any of classes $\mathfrak{C}^{\sigma}$, where $\sigma \in S_3\backslash\{\varepsilon\}$, forms a quasi-variety and this class is closed under the formation of subalgebras, products, ultraproducts, isomorphic algebras and it contains a trivial algebra.*

Proof. This follows from definition of the classes $\mathfrak{C}^{\sigma}$ and standard information on quasivarieties [15, 22]. □

A quasivariety $\mathfrak{Q}$ is a variety if and only if it is closed under the formation of homomorphic (more precisely, epimorphic) images [15, 22].

Lemma 11. *If a quasi-identity of the form $f(x, y, \ldots, z) = g(x, y, \ldots, z) \Longrightarrow x = y$ is true in a quasigroup $(Q, \cdot, \backslash, /)$, where $f(x, y, \ldots, z)$, $g(x, y, \ldots, z)$ are some (generally speaking non-reduced) quasigroup words which are constructed from free variables $x, y, \ldots, z$ and the binary operations $\cdot, \backslash, /$, then this quasi-identity is true in any homomoorphic image of the quasigroup $(Q, \cdot, \backslash, /)$.*

Proof. Let h be a homomorphism of a quasigroup $(Q,\cdot,\backslash,/)$ onto a quasigroup $(hQ,\circ,\backslash\backslash,//)$, i.e. $h(x\cdot y)=hx\circ hy$, $h(x\backslash y)=hx\backslash\backslash hy$, $h(x/y)=hx//hy$ for all $x,y\in Q$.

Let us suppose that in a quasigroup $(Q,\cdot,\backslash,/)$ a quasi-identity of the form $(f(x,y,\dots,z)=g(x,y,\dots,z)\Longrightarrow x=y)$ is true and that in the quasigroup $(hQ,\circ,\backslash\backslash,//)$ this quasi-identity is not fulfilled. Thus there exist elements $\bar a,\bar b,\bar c\in hQ$ such that $(f(\bar a,\bar b,\dots,\bar c)=g(\bar a,\bar b,\dots,\bar c)\Longrightarrow \bar a\neq\bar b)$. Then, turning back to the quasigroup $(Q,\cdot)$, we obtain that there exist elements $a,b,c\in Q$, $a\in\bar a$, $b\in\bar b$, $c\in\bar c$ such that $(f(a,b,\dots,c)=g(a,b,\dots,c)\Longrightarrow a\neq b)$. We received a contradiction that demonstrates that our supposition is not true.

Thus, if in a quasigroup $(Q,\cdot,\backslash,/)$ a quasi-identity of the form $f(x,y,\dots,z)=g(x,y,\dots,z)\Longrightarrow x=y$ is true, then this quasi-identity is true in any homomorphic image of the quasigroup $(Q,\cdot,\backslash,/)$. □

Corollary 13. *Any of classes $\mathfrak{C}^\sigma$, where $\sigma\in S_3\backslash\{\varepsilon\}$, is closed under the formation of epimorphic images.*

Proof. Any of quasi-identities from Theorem 10 fulfils the conditions of Lemma 11. □

Theorem 12. *Any of classes $\mathfrak{C}^\sigma$, where $\sigma\in S_3\backslash\{\varepsilon\}$, forms a variety and it can be defined by a set of identities.*

Proof. The fact, that any of classes $\mathfrak{C}^\sigma$, $\sigma\in S_3\backslash\{\varepsilon\}$, forms a variety, follows from definition of classes $\mathfrak{C}^\sigma$, Proposition 15 and Corollary 13.

From Theorem of G. Birkhoff ([15, 22]) it follows that there exists a set of identities which define any of the classes $\mathfrak{C}^\sigma$. □

From Theorem12 it follows that there exists a set of identities such that fulfillment in a finite quasigroup $(Q,\cdot)$ of these identities is a sufficient and necessary condition of orthogonality of $(Q,\cdot)$ and its conjugate quasigroup.

In [10] all identities of the form $A^\alpha(x,A^\beta(x,A^\gamma(x,y)))=y$, where $A^\alpha,A^\beta,A^\gamma$ are some parastrophes of a quasigroup operation A which provide orthogonality of operation A and some its parastrophe are classified up to parastrophical equivalence. V.D. Belousov proved that these identities are minimal, i.e. these identities have minimal number of variables (2), and minimal number of occurrences of these variables in both sides of an identity (5).

He also proved that there exist 7 types of such identities and found a model (a quasigroup) for some representatives (for some identities) of any from these 7 types of identities.

Theorem 8 allows us to give some sufficient conditions of orthogonality of a quasigroup and its parastroph on language of identities. In the following theorem we list some identities which provide orthogonality of a quasigroup $(Q,\cdot)$ and its concrete parastrophe.

Theorem 13. *1. Fulfilment in a finite quasigroup $(Q,\cdot)$ of any of the identities*

$x\cdot xy=yx$ *(I),* $xy\cdot y=yx$ *(II),* $xy\cdot yx=x$ *(III),* $yx\cdot xy=x$ *(IV)*

is a sufficient condition for orthogonality of $(Q,\cdot)$ and $(Q,\cdot)^{(12)}$;

2. Fulfilment in a quasigroup $(Q,\cdot)$ of any of the identities

$(yx\cdot x)x=y$ *(V),* $yx\cdot x=xy$ *(VI),* $(xy\cdot x)x=y$ *(VII),* $y(yx\cdot x)=x$ *(VIII),* $(yx\cdot x)y=x$ *(IX)*

is a sufficient condition for orthogonality of $(Q,\cdot)$ and $(Q,\cdot)^{(13)}$;

3. Fulfilment in a quasigroup $(Q,\cdot)$ of any of the identities

$x(x\cdot xy)=y$ *(X),* $x\cdot xy=yx$ *(XI),* $x(x\cdot yx)=y$ *(XII),* $y(x\cdot xy)=x$ *(XIII),* $(x\cdot xy)y=x$ *(XIV)*

is a sufficient condition for orthogonality of $(Q,\cdot)$ and $(Q,\cdot)^{(23)}$;

4. Fulfilment in a quasigroup $(Q,\cdot)$ of any of the identities

$x(x\cdot yx)=y$ *(XV),* $x(yx\cdot x)=y$ *(XVI),* $y(x\cdot yx)=x$ *(XVII),* $(x\cdot yx)y=x$ *(XVIII)*

is a sufficient condition for orthogonality of $(Q,\cdot)$ and $(Q,\cdot)^{(123)}$;

5. Fulfilment in a quasigroup $(Q,\cdot)$ of any of the identities

$(xy\cdot x)x=y$ *(XIX),* $(x\cdot xy)x=y$ *(XX),* $y(xy\cdot x)=x$ *(XXI),* $(xy\cdot x)y=x$ *(XXII)*

is a sufficient condition for orthogonality of $(Q,\cdot)$ and $(Q,\cdot)^{(132)}$.

Proof. The truth of case 1 follows easy from Belousov's results [5]. Also we can apply Theorem 8. From this theorem it follows that, if we will be able to find a τ-tuple T of permutations such that $\overline{R}\ \overline{L^{-1}}=T$, then $(Q,\cdot)\perp(Q,\cdot)^{(12)}$. The first candidates on the role of tuple T can be tuples of the left, right, middle translations of the quasigroup $(Q,\cdot)$ or their inverse tuples.

It is easy to see that for our purpose equalities $R_xL_x^{-1}y=R_xy$ and $R_xL_x^{-1}y=L_x^{-1}y$ for all $x,y\in Q$ do not suit, since in these cases we obtain $L_x^{-1}y=y$ and $R_xz=z$ for all $x,y,z\in Q$. The fulfillment of any from last two equalities in a quasigroup $(Q,\cdot)$ means that $|Q|=1$.

Other 4 possibilities give us the first 4 identities. Namely,

$R_xL_x^{-1}y=L_xy$, $y\to L_xy$, $R_xy=L_x^2y$, $x\cdot xy=yx$ (I);

$R_xL_x^{-1}y=R_x^{-1}y$, $R_x^2L_x^{-1}y=y$, $R_x^2y=L_xy$, $yx\cdot x=xy$, $x\leftrightarrow y$, $xy\cdot y=yx$ (II);

$R_xL_x^{-1}y=P_xy$, $R_xy=P_xL_xy$, $yx=P_x(xy)$, $xy\cdot yx=x$ (III);

$R_xL_x^{-1}y=P_x^{-1}y$, $R_xy=P_x^{-1}L_xy$, $yx=P_x^{-1}(xy)$, $yx\cdot xy=x$ (IV).

Identities (V)-(XXII) are obtained similarly. □

Corollary 14. *If in a finite quasigroup* $(Q,\cdot)$ *the identity* $x\cdot xy = yx$ *(I) holds, then* $(Q,\cdot)\perp(Q,\cdot)^{(12)}$, $(Q,\cdot)\perp(Q,\cdot)^{(23)}$;

if in a quasigroup $(Q,\cdot)$ *the identity* $xy\cdot y = yx$ *(II) holds, then* $(Q,\cdot)\perp(Q,\cdot)^{(12)}$, $(Q,\cdot)\perp(Q,\cdot)^{(13)}$;

if in a quasigroup $(Q,\cdot)$ *the identity* $x(x\cdot yx) = y$ *(XII) holds, then* $(Q,\cdot)\perp(Q,\cdot)^{(23)}$, $(Q,\cdot)\perp(Q,\cdot)^{(123)}$;

if in a quasigroup $(Q,\cdot)$ *the identity* $(xy\cdot x)x = y$ *(VII) holds, then* $(Q,\cdot)\perp(Q,\cdot)^{(13)}$, $(Q,\cdot)\perp(Q,\cdot)^{(132)}$.

Proof. In Theorem 13 there are the following equalities or equivalences of identities: (XI)=(I), (VI)$\leftrightarrow$ (II) ($x\leftrightarrow y$), (XV)=(XII), (XIX) = (VII). □

Remark 12. It is easy to see that identities from Theorem 13 have two variables and five occurrences of these variables in any identity. In fact all these identities or their parastrophically equivalent forms can be found in the preprint of V.D. Belousov [10]. Identity (I) is called in [10] the first Stein identity, identity (IV) is called the third Stein identity. (III) $\leftrightarrow$ $yx\cdot xy = y$ ($x\leftrightarrow y$), the last identity is called the second Schreder identity.

2.4 Some transformations of groupoids and quasigroups which preserve the property of orthogonality

From definitions of orthogonality of squares, groupoids and m-tuples of permutations and properties of these objects it follows that the property of orthogonality is symmetric, i.e. $A\perp B$ if and only if $B\perp A$, where A and B are squares, groupoids or m-tuples of permutations.

Let (Q,A) be a groupoid and $S_1(Q)$ be a square that coincides with the body of the Cayley table of this groupoid, let (Q,B) be a groupoid and $S_2(Q)$ be a square that coincides with the body of the Cayley table of this groupoid. Then $(Q,A)\perp(Q,B)$ if and only if $S_1(Q)\perp S_2(Q)$.

Proposition 16. *Groupoids* (Q,A) *and* (Q,B) *are orthogonal if and only if* $(Q,A)T\perp(Q,B)T$, *where* T *is an isotopy.*

Proof. Let $T=(\alpha,\beta,\gamma)$. We can decompose this isotopy in the product of isotopies $T_1T_2T_3$, where $T_1=(\alpha,\varepsilon,\varepsilon)$, $T_2=(\varepsilon,\beta,\varepsilon)$ and $T_3=(\varepsilon,\varepsilon,\gamma)$ [4].

It is well known that the isotopy T_1 changes the order of rows in Cayley tables of the groupoids (Q,A) and (Q,B), the isotopy T_2 changes the order of columns in these Cayley tables, the isotopy T_3 changes elements in these Cayley tables.

It is easy to see, if $(Q,A)\perp(Q,B)$, then

$$(Q,A)T_1\perp(Q,B)T_1,$$
$$(Q,A)T_1T_2\perp(Q,B)T_1T_2,$$
$$(Q,A)T_1T_2T_3\perp(Q,B)T_1T_2T_3.$$

Therefore, if $(Q,A)\perp(Q,B)$, then $(Q,A)T\perp(Q,B)T$.

It is clear that the implication $(Q,A)T \perp (Q,B)T \Rightarrow (Q,A) \perp (Q,B)$ is fulfilled, too. □

We notice in [11] Proposition 16 is proved for quasigroups. See, also, Lemma 7.

Proposition 17. *Groupoids (Q,A) and (Q,B) are orthogonal if and only if $(Q,A^{(12)})\perp(Q,B^{(12)})$.*

Proof. From the properties of (12)-parastrophy of groupoids it follows that the i-th row of the body of Cayley table of groupoid $(Q,A^{(12)})$ coincides with the i-th column of the body of Cayley table of groupoid (Q,A). Similar situation is with groupoids (Q,B) and $(Q,B^{(12)})$.

We denote by S_1 and S_2 the bodies of Cayley tables of groupoids (Q,A) and (Q,B) respectively. By Definition 22 if $S_1 \perp S_2$, then $D(S_1 \oplus S_2) = Q \times Q$. Since i-th rows in the square $S_1^{(12)} \oplus S_2^{(12)}$ coincide with the i-th columns of the square $S_1 \oplus S_2$, we conclude that $D(S_1^{(12)} \oplus S_2^{(12)}) = Q \times Q$, i.e. $S_1^{(12)} \perp S_2^{(12)}$.

Therefore, if $(Q,A)\perp(Q,B)$, then $(Q,A^{(12)})\perp(Q,B^{(12)})$. Using the same arguments we can prove that, if $(Q,A^{(12)})\perp(Q,B^{(12)})$, then $(Q,A)\perp(Q,B)$. □

In [10] Proposition 17 is proved for quasigroups.

Corollary 15. *Groupoids (Q,A) and (Q,B) are orthogonal if and only if $(Q,A)\beta \perp (Q,B)\beta$, where $\beta \in ISOS_{(12)}(Q)$.*

Proof. The proof follows from Propositions 16 and 17. □

Unfortunately, in general, it is impossible to extend result of Proposition 17 on other types of parastrophy of quasigroups.

Example 6. *There exists a pair of orthogonal quasigroups (Q,A) and (Q,B) such that quasigroups $(Q,A^{(23)})$ and $(Q,B^{(23)})$ are not orthogonal.*

A,B	0	1	2	3	4
0	00	23	41	14	32
1	11	34	02	20	43
2	22	40	13	31	04
3	33	01	24	42	10
4	44	12	30	03	21

$A^{(23)},B^{(23)}$	0	1	2	3	4
0	00	32	14	41	23
1	23	00	32	14	41
2	41	23	00	32	14
3	14	41	23	00	32
4	32	14	41	23	00

Corollary 16. *Suppose that quasigroups (Q,A) and (Q,B) are orthogonal. Then $(Q,A^{\sigma})\perp(Q,B^{\sigma})$ for any $\sigma \in S_3$ if and only if $(Q,A^{\delta})\perp(Q,B^{\delta})$, where $\delta \in \{(13),(23),(123),(132)\}$.*

Proof. The elements (12) and δ generate the group S_3. □

Proposition 18. *([34]). The permutation squares S_1 and S_2 of a kind α, $\alpha \in \{l, Il, r, Ir\}$ are orthogonal if and only if $S_1S_3 \perp S_2S_3$, where S_3 is a permutation square of the kind α.*

Proof. From Theorem 4 it follows that the permutation squares S_1 and S_2 are orthogonal if and only if the tuple $T_2T_1^{-1}$ of a kind α, $\alpha \in \{l, Il, r, Ir\}$ is strictly transitive, where T_1 and T_2 are m-tuples of a kind α of the squares S_1 and S_2 respectively.

The permutation squares S_1S_3 and S_2S_3 are orthogonal if and only if the tuple $T_2T_3T_3^{-1}T_1^{-1}$ of the kind α is a strictly transitive set of permutations. But $T_2T_3T_3^{-1}T_1^{-1} = T_2T_1^{-1}$. □

Proposition 18 leads us to the following generalization of the concept of isotopy.

2.5 On generalized isotopy of squares and permutation squares

It is possible give a concept which is a generalization of the concept of isotopy in many cases. As we saw, the concept of isotopy has sense for any square and any groupoid. The concept of generalized isotopy (probably, gisotopy for convenience) also has sense for squares and groupoids. As we shall see, for permutation squares and left (right) quasigroups the concept of generalized isotopy is more general than the concept of "usual" isotopy.

Definition 28. Any m-tuple of permutations P of a kind α, $\alpha \in \{l, Il, r, Ir, p, Ip\}$, will be called a *generalized isotopy of the kind* α or *gisotopy of the kind* α.

Definition 29. A groupoid (Q, A) is a *gisotope of a kind* α *of a groupoid* (Q, B), where $\alpha \in \{l, r\}$, if there exists an m-tuple of permutations P of the set Q of the kind α such that $T_A^\alpha = T_B^\alpha P$, i.e. $(t_A^\alpha)_i = (t_B^\alpha)_i\, p_i$ for all suitable values of the index i, where T_A^α, T_B^α are m-tuples of maps of the kind α that correspond to the groupoids (Q, A), (Q, B), respectively.

Remark 13. We follow the agreements of Remark 1 in the order of multiplication of maps and we write a gisotopy P from the right from a groupoid (Q, A), as we write an isotopy T from the right from a groupoid (Q, A).

It is easy to see that the concept of gisotopy has sense for m-tuples of maps and for squares, since gisotopy is defined using concept of multiplication of m-tuples.

For left (right) quasigroups the kind α from Definition 29 can be any element of the set $\{l, Il, r, Ir\}$. Using Mann's product of permutation squares, we can give the following

Definition 30. A permutation square S_1 of a kind α, $\alpha \in \{l, Il, r, Ir\}$, is a *gisotopic image of a permutation square* S_2 of the kind α if and only if $S_1 = S_2P$, where P is a gisotopy of the kind α.

Example 7. *As it follows from Albert theorem ([4]), the groups* $Z_2 \oplus Z_2$ *and* Z_4

$Z_2 \oplus Z_2$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Z_4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

are non-isotopic, but these groups are gisotopic with the left gisotopy $P = (\varepsilon, (02), \varepsilon, (02))$.

Example 8. *Groupoids* (Q, A) *and* (Q, B) *are isotopic:* $B(x, y) = \gamma^{-1}A(x, y)$*, where* $\gamma = (01)$*, but these groupoids are not gisotopic.*

A	0	1
0	0	0
1	0	0

B	0	1
0	1	1
1	1	1

Proposition 19. *For the class of groupoids* $\mathfrak{G}$ *the class of isotopies* $\mathcal{I}(\mathfrak{G})$ *and the class of gisotopies* $\mathcal{GI}(\mathfrak{G})$ *are intersected, but* $\mathcal{I} \nsubseteq \mathcal{GI}$ *and* $\mathcal{GI} \nsubseteq \mathcal{I}$.

Proof. The proof follows from Examples 7 and 8. □

Theorem 14. *If* (Q, A) *is a left quasigroup,* T *is an isotopy, then there exists a gisotopy* GT *of the kind* l *such that* $(Q, A)T = (Q, A)GT$*, i.e. any isotopy of a left quasigroup is a gisotopy.*

Proof. If (Q, A) is a left quasigroup, T is an isotopy, then by Lemma 4 $(Q, A)T$ is a left quasigroup.

If S_1 is a permutation square of the kind l which corresponds to the left quasigroup (Q, A), S_2 is a permutation square of the kind l which corresponds to the left quasigroup $(Q, A)T$, then $S_2 = S_1(S_1^{-1}S_2)$. Thus m-tuple of permutation GT of the kind l that corresponds to the square $S_1^{-1}S_2$ is a gisotopy such that $(Q, A)T = (Q, A)GT$.

Therefore any isotopy of a left quasigroup is a gisotopy. □

Remark 14. It is easy to see that the similar theorem is true for right quasigroups.

Corollary 17. *Any isotopy of a quasigroup is a generalized isotopy.*

Proof. The proof is a direct consequence of Theorem 14 and Remark 14. □

It is easy to see that, generally speaking, gisotopic image of a square is a square, gisotopic image of a permutation square is a permutation square, gisotopic image of a Latin square is a permutation square.

Proposition 20. *The action of gisotopy* $P = (p_1, p_2, \dots, p_n, \dots)$ *of the kind* l *on a groupoid* $(Q, \cdot)$ *coincides with the action of the tuple* T *of isotopies of the form* $T = ((\varepsilon, p_1, \varepsilon), (\varepsilon, p_2, \varepsilon), \dots, (\varepsilon, p_i, \varepsilon), \dots)$*, where the isotopy* $(\varepsilon, p_i, \varepsilon)$ *acts only on the* i*-th row of Cayley table of the groupoid* $(Q, \cdot)$.

Proof. If L_{a_i} is the i-th left translation of the groupoid $(Q, \cdot)$, then in groupoid $(Q, \cdot)P$ the i-th row has the form $L_{a_i}^{\cdot}p_i(x) = a_i \cdot (p_i(x))$.

If we apply the isotopy $(\varepsilon, p_i, \varepsilon)$ to the groupoid $(Q, \cdot)$, then we have $x \circ y = x \cdot p_i(y)$. The i-th left translation of the groupoid $(Q, \circ)$ has the form $L_{a_i}^{\circ}y = L_{a_i}^{\cdot}p_i(y)$. □

Proposition 21. *The action of gisotopy $P = (p_1, p_2, \dots, p_n, \dots)$ of the kind r on a groupoid $(Q, \cdot)$ coincides with the action of the tuple T of isotopies of the form $T = ((p_1, \varepsilon, \varepsilon), (p_2, \varepsilon, \varepsilon), \dots, (p_i, \varepsilon, \varepsilon), \dots)$, where the isotopy $(p_i, \varepsilon, \varepsilon)$ acts only on the i-th column of Cayley table of the groupoid $(Q, \cdot)$.*

Proof. If R_{a_i} is the i-th right translation of the groupoid $(Q, \cdot)$, then in groupoid $(Q, \cdot)P$ the i-th column has the form $R^{\cdot}_{a_i} p_i(x) = (p_i(x)) \cdot a_i$.

If we apply the isotopy $(p_i, \varepsilon, \varepsilon)$ to the groupoid $(Q, \cdot)$, then we have $x \circ y = p_i(x) \cdot y$. The i-th right translation of the groupoid $(Q, \circ)$ has the form $R^{\circ}_{a_i} x = R^{\cdot}_{a_i} p_i(x)$. □

Corollary 18. *If a gisotopy T has the form $T = (p, \dots, p)$ and the kind l or r, where $p \in S_Q$, then a gisotopic image LT of a Latin square L, which is defined on the set Q, is a Latin square.*

Proof. This follows from Propositions 20 and 21 and from well known fact that isotopic image of a Latin square is a Latin square. □

The class of all permutation squares defined on a set Q will be denoted by $\mathfrak{S}(Q)$.

Proposition 22. $\mathfrak{S}(Q)P \subseteq \mathfrak{S}(Q)$ *for any* $P \in \mathfrak{S}(Q)$, *i.e. in other words* $\mathfrak{S}(Q)\mathfrak{S}(Q) \subseteq \mathfrak{S}(Q)$.

Proof. Product of two m-tuples of permutations is an m-tuple of permutations. □

Proposition 23. *If S_1, S_2 are permutation squares of a kind α, $\alpha \in \{l, Il, r, Ir\}$, then there exists a generalized isotopy P of the kind α such that $S_1 P = S_2$.*

Proof. Indeed, $P = S_1^{-1} S_2$. □

Corollary 19. *If S_1, S_2 are Latin squares of a kind α, $\alpha \in \{l, Il, r, Ir, p, Ip\}$, then there exists a generalized isotopy P of the kind α such that $S_1 P = S_2$.*

Proof. Indeed, $P = S_1^{-1} S_2$. □

We notice that Proposition 23 and Corollary 19 are true for a pair of left (right) quasigroups, for a pair of quasigroups, respectively.

Proposition 24. *If L_1 is a Latin square of a kind α, $\alpha \in \{l, Il, r, Ir\}$, P is a permutation square of the kind α and $P = L_1^{-1} L_2$, where L_2 is a Latin square, then $L_1 P$ is a Latin square.*

Proof. It is easy to see that $L_1 P = L_1 L_1^{-1} L_2 = L_2$. □

2.6 Gisotopy and orthogonality

Gisotopy is a transformation which preserves the property of orthogonality of squares, groupoids and m-tuples of maps. We formulate the following proposition for squares.

Proposition 25. *Squares S_1 and S_2, both of a kind α, $\alpha \in \{l, r\}$, are orthogonal if and only if any its gisotopic images S_1P and S_2P are orthogonal, where P is a gisotopy of the kind α.*

Proof. We denote by T_1 m-tuple of the kind l that corresponds to the square S_1, i.e. $T_1 = (L_1, L_2, \ldots, L_m)$, and $T_2 = (L'_1, L'_2, \ldots, L'_m)$ is m-tuple of the kind l which corresponds to the square S_2. Thus in the square of pairs E in the position (i, j) the pair $(L_i j, L'_i j)$ is situated.

If $P = (p_1, p_2, \ldots, p_m)$ is a left gisotopy, then in the square of pairs EP, in cell (i, j) the pair $(L_i p_i(j), L'_i p_i(j))$ will be situated, the pair $(L_i j, L'_i j)$ will be situated in the cell $(i, p_i^{-1}(j))$.

Thus, any gisotopy P of kind l changes the order of pairs in any row of the square of pairs E.

Similarly, any gisotopy P of kind r changes the order of pairs in any column of the square E.

Therefore, if $S_1 \perp S_2$, then $S_1P \perp S_2P$ for any gisotopy P of kind l or kind r. □

In article [30] H.B. Mann, in fact, proved the following

Theorem 15. *If Latin squares L_1 and L_2 are orthogonal, then the Latin squares L_1P_1 and L_2P_2 are also orthogonal, where P_1 and P_2 are gisotopies of the form $P_1 = (p_1, p_1, \ldots, p_1)$ and $P_2 = (p_2, p_2, \ldots, p_2)$, respectively.*

Proof. We suppose that Latin squares L_1 and L_2 have the kind l. If $L_1 \perp L_2$, then by Theorem 4 $L_3 = L_2 L_1^{-1}$ is a Latin square.

This theorem will be proved if we prove that the permutation square $L_4 = L_2 P_2 P_1^{-1} L_1^{-1}$ is a Latin square.

From Corollary 3 it follows that $(P_2 P_1^{-1}) L_1^{-1}$ is a Latin square if and only if $L_1^{-1}(P_2 P_1^{-1})$ is a Latin square.

Therefore L_4 is a Latin square if and only if $L_2 L_1^{-1}(P_2 P_1^{-1})$ is a Latin square.

It is easy to see that $L_2 L_1^{-1}(P_2 P_1^{-1})$ is a Latin square. This follows from the forms of gisotopies P_1, P_2 and Corollary 18. □

A theorem that is a generalization of Theorem 15 can be found in [17].

Corollary 20. *If Latin squares L_1 and L_2 are orthogonal, then the Latin squares L_1 and L_2P are also orthogonal, where P is a gisotopy of the form $P = (p, p, \ldots, p)$.*

Proof. It is easy to see. □

3 On orthogonality of T-quasigroups

In this section we give the conditions of orthogonality of a pair of T-quasigroups defined on the same abelian group $(Q, +)$ (not necessary a finite), also we study parastrophe orthogonality of T-quasigroups.

3.1 On parastrophe orthogonality of a pair of T-quasigroups

Definition 31. ([33]). A quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y+a$, where $(Q,+)$ is an abelian group, φ,ψ are automorphisms of the group $(Q,+)$, and the element a is some fixed element of the set Q, is called a *T-quasigroup*.

Definition 32. ([4]). A quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y+a$, where $(Q,+)$ is an abelian group, φ,ψ are commuting automorphisms of the group $(Q,+)$, and the element a is some fixed element of the set Q, is called a *medial quasigroup*.

Theorem 16. *T-quasigroup $(Q,\cdot)$ of the form $x\cdot y=\alpha x+\beta y+c$ and T-quasigroup $(Q,\circ)$ of the form $x\circ y=\gamma x+\delta y+d$, both over a commutative group $(Q,+)$ are orthogonal if and only if the map $\alpha^{-1}\beta-\gamma^{-1}\delta$ is an automorphism of the group $(Q,+)$.*

Proof. Quasigroups $(Q,\cdot)$ and $(Q,\circ)$ are orthogonal if and only if the system of equations

$$\begin{cases}\alpha x+\beta y+c=a\\ \gamma x+\delta y+d=b\end{cases}$$

has a unique solution for any fixed elements $a,b\in Q$.

We solve this system of equations in the usual way.

$$\begin{cases}\alpha x+\beta y=a-c\\ \gamma x+\delta y=b-d\end{cases}\iff\begin{cases}x+\alpha^{-1}\beta y=\alpha^{-1}(a-c)\\ -x-\gamma^{-1}\delta y=-\gamma^{-1}(b-d).\end{cases}$$

Therefore, $y=(\alpha^{-1}\beta-\gamma^{-1}\delta)^{-1}(\alpha^{-1}(a-c)-\gamma^{-1}(b-d))$. Similarly, $x=(\beta^{-1}\alpha-\delta^{-1}\gamma)^{-1}(\beta^{-1}(a-c)-\delta^{-1}(b-d))$.

It is clear that quasigroups $(Q,\cdot)$ and $(Q,\circ)$ are orthogonal if and only if the endomorphisms $(\alpha^{-1}\beta-\gamma^{-1}\delta)$ and $(\beta^{-1}\alpha-\delta^{-1}\gamma)$ are automorphisms of the group $(Q,+)$.

The map $(\alpha^{-1}\beta-\gamma^{-1}\delta)$ is a permutation of the set Q if and only if the map $\varepsilon-\alpha\gamma^{-1}\delta\beta^{-1}$ is a permutation of the set Q. Indeed, $\alpha(\alpha^{-1}\beta-\gamma^{-1}\delta)\beta=\varepsilon-\alpha\gamma^{-1}\delta\beta^{-1}$.

Similarly, $(\beta^{-1}\alpha-\delta^{-1}\gamma)$ is a permutation of set Q if and only if the map $\varepsilon-\beta\delta^{-1}\gamma\alpha^{-1}$ is a permutation of the set Q. If we denote the map $\alpha\gamma^{-1}\delta\beta^{-1}$ by ψ, then $\beta\delta^{-1}\gamma\alpha^{-1}=\psi^{-1}$.

Further we have the following equivalence: the map $\varepsilon-\psi$ is a permutation if and only if the map $\varepsilon-\psi^{-1}$ is a permutation of the set Q. Indeed, $\varepsilon-\psi$ is a permutation if and only if the map $\psi-\varepsilon$ is a permutation, $\psi-\varepsilon$ is a permutation if and only if $\psi^{-1}(\psi-\varepsilon)=\varepsilon-\psi^{-1}$ is a permutation. □

Corollary 21. *([32]). T-quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y+c$ over a commutative group $(Q,+)$ and its (12)-parastroph $(Q,\star)$ of the form $x\star y=\psi x+\varphi y+c$ are orthogonal if and only if the map $\varphi^{-1}\psi-\psi^{-1}\varphi$ is an automorphism of the group $(Q,+)$.*

Corollary 22. *T-quasigroup $(Q,\cdot)$ of the form $x\cdot y=\alpha x+\beta y+c$ and medial quasigroup $(Q,\circ)$ of the form $x\circ y=\gamma x+\delta y+d$, both over a commutative group $(Q,+)$, are orthogonal if and only if the map $\alpha\delta-\gamma\beta$ is an automorphism of the group $(Q,+)$.*

Proof. From the proof of Theorem 16 it follows, that the quasigroups $(Q,\cdot)$ and $(Q,\circ)$ are orthogonal if and only if the map $\varepsilon-\beta\delta^{-1}\gamma\alpha^{-1}$ is a permutation of the set Q. Further, since $\delta\gamma=\gamma\delta$, we have $\beta\delta^{-1}\gamma\alpha^{-1}=\beta\gamma\delta^{-1}\alpha^{-1}$ and the map $\varepsilon-\beta\delta^{-1}\gamma\alpha^{-1}$ is a permutation of the set Q if and only if the map $(\varepsilon-\beta\gamma\delta^{-1}\alpha^{-1})\alpha\delta=\alpha\delta-\beta\gamma$ is a permutation of the set Q. □

Theorem 17. *For a T-quasigroup (Q,A) of the form $x\cdot y=\varphi x+\psi y+a$ over an abelian group $(Q,+)$ the following equivalences are fulfilled:*

(i) $A\perp A^{12}\iff(\varphi-\psi),(\varphi+\psi)$ *are permutations of the set Q;*
(ii) $A\perp A^{13}\iff(\varepsilon+\varphi)$ *is a permutation of the set Q;*
(iii) $A\perp A^{23}\iff(\varepsilon+\psi)$ *is a permutation of the set Q;*
(iv) $A\perp A^{123}\iff(\varphi+\psi^2)$ *is a permutation of the set Q;*
(v) $A\perp A^{132}\iff(\varphi^2+\psi)$ *is a permutation of the set Q.*

Proof. *(i)* From Theorem 16 it follows that the T-quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y+c$ over a commutative group $(Q,+)$ and its (12)-parastroph $(Q,\star)$ of the form $x\cdot y=\psi x+\varphi y+c$ are orthogonal if and only if the map $\varphi^{-1}\psi-\psi^{-1}\varphi$ is a permutation of the set Q (i.e. this map is an automorphism of the group $(Q,+)$).

Below we repeat a part of the proof of Theorem 15 from [32]. We demonstrate an equivalence of the following conditions:

(the maps $\varphi-\psi$ and $\varphi+\psi$ are permutations of the set Q) and
(the map $\varphi^{-1}\psi-\psi^{-1}\varphi$ is a permutation of the set Q).

We notice that the map $\varphi-\psi$ is a permutation if and only if the map $\varphi^{-1}-\psi^{-1}$ is a permutation of the set Q. Indeed, we have $\psi^{-1}(\varphi-\psi)\varphi^{-1}=\psi^{-1}-\varphi^{-1}$. It is clear that the map $\psi^{-1}-\varphi^{-1}$ is a permutation if and only if the map $\varphi^{-1}-\psi^{-1}$ is a permutation.

Then we have the following equivalence

(the maps $\varphi-\psi$ and $\varphi+\psi$ are permutations of the set Q) $\iff$
(the maps $\varphi^{-1}-\psi^{-1}$ and $\varphi+\psi$ are permutations of the set Q).

Since $(\varphi^{-1}-\psi^{-1})(\varphi+\psi)=\varepsilon+\varphi^{-1}\psi-\psi^{-1}\varphi-\varepsilon=\varphi^{-1}\psi-\psi^{-1}\varphi$, we can say that the following conditions

(the maps $\varphi-\psi$ and $\varphi+\psi$ are permutations of the set Q) and
(the map $\varphi^{-1}\psi-\psi^{-1}\varphi$ is a permutation of the set Q)

are equivalent, too.

(ii) We recall, $x\cdot y=z$ if and only if $z/y=x$. Then we have $\varphi x=z-\psi y-a$, $x=\varphi^{-1}z-\varphi^{-1}\psi y-\varphi^{-1}a=z/y$, i.e. $x/y=\varphi^{-1}x-\varphi^{-1}\psi y-\varphi^{-1}a$.

From Theorem 16 it follows that $A\perp A^{(13)}$ if and only if $\varphi^{-1}\psi-\varphi(-\varphi^{-1}\psi)$ is a permutation of the set Q. The last condition is equivalent to the following: $A\perp A^{(13)}$ if and only if $\varepsilon+\varphi$ is a permutation of the set Q.

(iii) It is easy to see that $x\backslash y = -\psi^{-1}\varphi x+\psi^{-1}y-\psi^{-1}a$. Application of Theorem 16 gives us that $A\perp A^{(23)}$ if and only if $\varphi^{-1}(\psi+\varepsilon)$ is a permutation of the set Q. The last condition is equivalent to the following: $A\perp A^{(23)}$ if and only if $\varepsilon+\psi$ is a permutation of the set Q.

(iv) We have $A^{(123)}(x,y) = -\varphi^{-1}\psi x+\varphi^{-1}y-\varphi^{-1}a$. From Theorem 16 it follows that $A\perp A^{(123)}$ if only if $\varphi^{-1}\psi+\psi^{-1}$ is a permutation of the set Q. The last condition is equivalent to the condition: $\varphi+\psi^2$ is a permutation of the set Q.

(v) We have $A^{(132)}(x,y) = \psi^{-1}x-\psi^{-1}\varphi y-\psi^{-1}a$. From Theorem 16 it follows that $A\perp A^{(132)}$ if only if $\varphi^{-1}\psi-(\psi(-\psi^{-1}\varphi)) = \varphi^{-1}\psi+\varphi$ is a permutation of the set Q. The last condition is equivalent to the condition: $\psi+\varphi^2$ is a permutation of the set Q. □

Remark 15. It is possible to use Theorem 8 by proving Theorem 17 at least for finite quasigroups.

From the form of quasigroup $(Q,\cdot)$ it follows that $L_x^{\cdot}y = L_{\varphi x+a}\psi y$, $R_y^{\cdot}x = L_{\psi y+a}\varphi y$. For instance, using Theorem 8 we can prove Case *(ii)* in the following way.

Any map $R_y^{\cdot}R_y^{\cdot}x$ has the following form :

$$R_y^{\cdot}R_y^{\cdot}x = L_{\psi y+a}\varphi L_{\psi y+a}\varphi x =$$
$$\psi y+a+\varphi(\psi y+a+\varphi x) = \varphi^2 x+(\varphi+\varepsilon)\psi y+\varphi a+a =$$
$$L_{(\varphi+\varepsilon)\psi y+\varphi a+a}\varphi^2 x.$$

It is easy to see that the m-tuple $(R_y^{\cdot}R_y^{\cdot})$, where variable y runs over all the set Q, will have the τ-property if and only if the map $\varphi+\varepsilon$ is a permutation of the set Q.

Corollary 23. *If L is a Latin square that is Cayley table of a finite T-quasigroup $(Q,\cdot)$ of the form $x\cdot y = \varphi x+\psi y+a$, then:*

(i) the square L^rL^{Il} is a Latin square if and only if $(\varphi-\psi),(\varphi+\psi)$;
(ii) the square L^rL^r is a Latin square if and only if $(\varepsilon+\varphi)$;
(iii) the square L^lL^l is a Latin square if and only if $(\varepsilon+\psi)$;
(iv) the square L^lL^r is a Latin square if and only if $(\varphi+\psi^2)$;
(v) the square L^rL^l is a Latin square if and only if $(\varphi^2+\psi)$.

Proof. The proof follows from Corollary 12 and Theorem 17. □

Example 9. *The quasigroup $(Z_p,\circ)$ of the form $x\circ y = 1\cdot x+2\cdot y$, where $(Z_p,+)$ is the additive group of residues modulo p, p is a prime number, $p\geq 7$, is orthogonal to any of its parastrophes.*

Example 10. *The quasigroup $(Z_{11},\circ)$ of the form $x\circ y = 3\cdot x+9\cdot y$, where $(Z_{11},+)$ is the additive group of residues modulo 11, is an idempotent quasigroup, which is orthogonal to any of its parastrophes.*

3.2 Orthogonality of a quasigroup and its conjugate

Orthogonality of a quasigroup and its (12)-parastrophe is more clear from the intuitive point of view and this orthogonality was studied in many articles ([5, 13, 17, 38]), see, also, Theorem 10 and Lemma 11 of this article.

A. Sade ([17, 38]) has called a quasigroup $(Q, \cdot)$ *anti-abelian* if it is orthogonal to its (12)-parastrophe $(Q, \star)$: that is, if $x \cdot y = z \cdot t$ and $y \cdot x = t \cdot z$ ($x \star y = z \star t$) imply $x = z$ and $y = t$.

We recall ([31]), a quasigroup $(Q, \cdot)$ with the quasi-identities $x \cdot y = y \cdot x \Rightarrow x = y$ and $x \cdot x = y \cdot y \Rightarrow x = y$ is called a *totally anti-commutative quasigroup*. M. Damm ([16]) proved that any anti-abelian quasigroup is a totally anti-commutative quasigroup.

The following two theorems were proved in [32].

Theorem 18. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ is a totally anti-commutative quasigroup if and only if it is an anti-abelian quasigroup .*

Theorem 19. *For a T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ over a commutative group $(Q, +)$ the following conditions are equivalent:*

- *$(x \cdot y = y \cdot x) \Rightarrow (x = y)$, $(x \cdot x = y \cdot y) \Rightarrow (x = y)$ for all $x, y \in Q$;*
- *$(x \cdot y = z \cdot t$ and $y \cdot x = t \cdot z) \Rightarrow (x = z$ and $y = t)$ for all $x, y, z, t \in Q$;*
- *the maps $\varphi - \psi$ and $\varphi + \psi$ are permutations of the set Q;*
- *the maps $\varphi^{-1} - \psi^{-1}$ and $\varphi + \psi$ are permutations of the set Q;*
- *the map $\varphi^{-1}\psi - \psi^{-1}\varphi$ is a permutation of the set Q;*
- *the T-quasigroup $(Q, \cdot)$ and its (12)-parastroph $(Q, \star)$ are orthogonal.*

Corollary 24. *([32]). For a medial quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ over a commutative group $(Q, +)$ the following conditions are equivalent:*

(the maps $\varphi - \psi$ and $\varphi + \psi$ are permutations of the set Q) and
(the map $\varphi^2 - \psi^2$ is a permutation of the set Q).

Proof. From the definition of a medial quasigroup we have that $\varphi\psi = \psi\varphi$. Then $(\varphi - \psi)(\varphi + \psi) = \varphi^2 + \varphi\psi - \psi\varphi - \psi^2 = \varphi^2 - \psi^2$. □

In [13] Bennet and Zhang study Latin squares with self-orthogonal conjugates. In language of this paper Latin squares with self-orthogonal conjugates correspond to quasigroups with the property: $(Q, A^\sigma) \perp (Q, A^\sigma)^{(12)}$ for any $\sigma \in S_3$. For short we shall call quasigroups with such property SOC-quasigroups.

For *SOC-T*-quasigroups we can prove the following

Theorem 20. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ over a group $(Q, +)$ is a SOC-quasigroup if and only if the maps $\varphi - \psi$, $\varphi + \psi$, $\varepsilon - \psi$, $\varepsilon + \psi$, $\varepsilon - \varphi$ and $\varepsilon + \varphi$ are permutations of the set Q.*

Proof. If $(Q,\cdot)$ is a T-quasigroup of the form $x\cdot y=\varphi x+\psi y+c$, then its parastrophes have the following forms, respectively:

$$\begin{aligned} x \overset{(12)}{\cdot} y &= \psi x+\varphi y+c,\\ x \overset{(13)}{\cdot} y &= \varphi^{-1}x-\varphi^{-1}\psi y-\varphi^{-1}c,\\ x \overset{(23)}{\cdot} y &= -\psi^{-1}\varphi x+\psi^{-1}y-\psi^{-1}c,\\ x \overset{(123)}{\cdot} y &= -\varphi^{-1}\psi x+\varphi^{-1}y-\varphi^{-1}c,\\ x \overset{(132)}{\cdot} y &= \psi^{-1}x-\psi^{-1}\varphi y-\psi^{-1}c. \end{aligned}$$

From Theorem 17 Case (i) (see, also, Theorem 19) it follows that $(Q,\cdot)\perp(Q,\overset{(12)}{\cdot})$ if and only $\varphi-\psi$, $\varphi+\psi$ are permutations of the set Q.

By Theorem 17 quasigroup $(Q,\overset{(13)}{\cdot})$ is orthogonal to its (12)-parastrophe if and only if $\varphi^{-1}-\varphi^{-1}\psi=\varphi^{-1}(\varepsilon-\psi)$ and $\varphi^{-1}+\varphi^{-1}\psi=\varphi^{-1}(\varepsilon+\psi)$ are permutations of the set Q. The last two statements are equivalent to the following: the maps $(\varepsilon-\psi)$ and $(\varepsilon+\psi)$ are permutations of the set Q.

Similarly, by Theorem 17, quasigroup $(Q,\overset{(23)}{\cdot})$ is orthogonal to its (12)-parastroph if and only if $-\psi^{-1}\varphi+\psi^{-1}=\psi^{-1}(-\varphi+\varepsilon)$ and $-\psi^{-1}\varphi-\psi^{-1}=\psi^{-1}(-\varphi-\varepsilon)$ are permutations of the set Q. The last two equality are equivalent to the following: $(\varepsilon-\varphi)$ and $(\varepsilon+\varphi)$ are permutations of the set Q. □

Example 11. *The quasigroup $(Z_7,\circ)$ of the form $x\circ y=3\cdot x+5\cdot y$, where $(Z_7,+)$ is the additive group of residues modulo 7, is SOC-quasigroup of order 7.*

Proof. The proof follows from Theorem 20, since $3+5\equiv 1 \pmod 7$, $3-5\equiv 5 \pmod 7$, $1-3\equiv 5 \pmod 7$, $1+3\equiv 4 \pmod 7$, $1-5\equiv 3 \pmod 7$, $1+5\equiv 6 \pmod 7$. □

Example 12. *The quasigroup $(Z_{11},\circ)$ of the form $x\circ y=3\cdot x+9\cdot y$, where $(Z_{11},+)$ is the additive group of residues modulo 11, is a SOC-quasigroup of order 11.*

Proof. The proof follows from Theorem 20, since $3+9\equiv 1 \pmod{11}$, $3-9\equiv 5 \pmod{11}$, $1-3\equiv 9 \pmod{11}$, $1+3\equiv 4 \pmod{11}$, $1-9\equiv 3 \pmod{11}$, $1+9\equiv 10 \pmod{11}$. □

Therefore, from Examples 11 and 12 it follows that there exist Latin squares with self-orthogonal conjugates of order 7 and 11. These examples supplement results of Bennet and Zhang [13].

Proposition 26. *A quasigroup $(\mathbb{Q},\circ)$ of the form $x\circ y=a\cdot x+b\cdot y+c$, where $(\mathbb{Q},+)$ is the additive group of rational numbers, $a\neq b$, $a\neq 1$, $a\neq 0$, $b\neq 1$,$b\neq 0$, is an infinite SOC-quasigroup.*

Proof. The proof follows from Theorem 20. □

Remark 16. It is easy to see that classes of SOC-quasigroups and quasigroups which are orthogonal to all its parastrophes, intersect (Example 12 = Example 10), but any of these two classes is not included in the other.

Constructed in Example 9 quasigroups are orthogonal to all its parastrophes and are not SOC-quasigroups ($1 - 1 \equiv 0 \pmod{p}$).

In Example 11 a SOC-quasigroup is constructed which is not orthogonal to all its parastrophes ($3^2 + 5 \equiv 0 \pmod{7}$).

Acknowledgments. The authors thank very much Prof. G.B. Belyavskaya and Prof. E.A. Zamorzaeva that carefully re-read this paper and proposed many improvements.

The research described in this publication was made possible in part by Award No. MM1-3040-CH-02 of the Moldovan Research and Development Association (MRDA) and U.S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

References

[1] Barlotti A., Strambach K. *The geometry of binary systems*. Adv. in Math., 1983, **49**, p. 1–105.

[2] Bektenov A.S., Yakubov T. *Systems of orthogonal n-ary operations*. Izvestiya AN MSSR, Ser. fiz.-tekh. i mat. nauk, 1974, N 3, p. 7–14 (in Russian).

[3] Belousov V.D. *On properties of binary operations*. Uchenye zapiski Beltskogo ped. instituta, 1960, vyp. 5, p. 9–28 (in Russian).

[4] Belousov V.D. *Foundations of the Theory of Quasigroups and Loops*. Moscow, Nauka, 1967 (in Russian).

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

[6] Belousov V.D. *On group associated with a quasigroup*. Mat. issled., Kishinev, RIO AN MSSR, 1969, **4**, N 3, p. 21–39 (in Russian).

[7] Belousov V.D. *Algebraic nets and quasigroups*. Kishinev, Shtiintsa, 1971 (in Russian).

[8] Belousov V.D., *n-Ary Quasigroups*. Kishinev, Shtiintsa, 1972 (in Russian).

[9] Belousov V.D. *Elements of the Quasigroup Theory, A Special Course*. Kishinev, 1981 (in Russian).

[10] Belousov V.D. *Parastrophically orthogonal quasigroups*. Kishinev, Shtiintsa, 1983 (in Russian).

[11] Belousov V.D., Belyavskaya G.B. *Latin squares, quasigroups and their applications*. Kishinev, Shtiintsa, 1989 (in Russian).

[12] Belyavskaya G.B. *Quasigroup power sets*. Quasigroups and Related Systems, 2002, **9**, p. 1–19.

[13] Bennett F., Hantao Zhang. *Latin Squares with Self-Orthogonal Conjugates*. Discrete Mathematics, 1004, **284**, Issues 1–3, p. 45–55.

[14] Burris S., Sankappanavar H.P. *A Course in Universal Algebra*. Springer-Verlag, New York, 1981.

[15] Cohn P.M. *Universal Algebra*. Harper & Row, Publishers, New York, 1965.

[16] Damm M. *Prüfziffersysteme über Quasigruppen*. Diplomarbeit, Philipps-Universität Marburg, 1998.

[17] Dénes J., Keedwell A.D.: *Latin Squares and their Applications*. Académiai Kiadó, Budapest, 1974.

[18] Dénes J., Keedwell A.D.: *Latin Squares. New Development in the Theory and Applications*. Annals of Discrete Mathematics, 1991, **46**, North-Holland.

[19] Dulmage A.L., Johnson D.M., Mendelsohn N.S. *Orthomorphisms of groups and orthogonal latin squares, I*. Canad. J. Math., 1961, **13**, p. 356–372.

[20] Duplak J. *A parastrophic equivalence in quasigroups*. Quasigroups and Related Systems, 2000, **7**, p. 7–14.

[21] Fraleigh J.B. *A First Course in Abstract Algebra*. Addison-Wesley, Reading, Massachusetts, 1982.

[22] *General algebra*. Editor L.A. Skornyakov. Moscow, Nauka, 1991 (in Russian).

[23] Kargapolov M.I., Merzlyakov Yu.I. *Foundations of Group Theory*. Moscow, Nauka, 1977 (in Russian).

[24] Keedwell A.D., Shcherbacov V.A. *Construction and properties of* (r, s, t)*-inverse quasigroups, II*. Discrete Math., 2004, **288**, p. 61–71.

[25] Kepka T., Němec P. *T-quasigroups, Part II*. Acta Universitatis, Carolinae Math. et Physica, 1971, **12**, N 2, p. 31–49.

[26] Kishen K. *On the construction of latin and hyper-graceo-latin cubes and hypercubes*. J. Ind. Soc. Agric. Statist., 1950, **2**, p. 20–48.

[27] Laywine Ch.F., Mullen G.L. *Discrete Mathematics Using Latin Squares*. New York, John Wiley & Sons, Inc., 1998.

[28] Leakh I.V. *On transformations of orthogonal systems of operations and algebraic nets*. Ph. D. Dissertation, Kishinev, Institute of Mathematics, 1986, p. 108 pages (in Russian).

[29] LindnerC.C. *Quasigroup identities and orthogonal arrays*. London Math. Soc., Lect. Note Ser., 1983, **82**, p. 77–105.

[30] Mann H.B. *The construction of orthogonal latin squares*. Ann. Math. Statist., 1942, **13**, p. 418–423.

[31] Mullen G.L., Shcherbacov V. *Properties of codes with one check symbol from a quasigroup point of view*. Buletinul Academiei de Ştiinţe a Republicii Moldova, Matematica, 2002, N 3(40), p. 71–86.

[32] Mullen G.L., Shcherbacov V. *n-T-quasigroup codes with one check symbol and their error detection capabilities*. Comment. Math. Univ. Carolinae, 2004, **45**, N 2, p. 321–340.

[33] Němec P., Kepka T. *T-quasigroups, Part I*. Acta Universitatis, Carolinae Math. et Physica, 1971, **12**, N 1, p. 39–49.

[34] Norton D.A. *Group of orthogonal row-latin squares*. Pacific J. Math., 1952, **2**, p. 335–341.

[35] Pflugfelder H.O. *Quasigroups and loops: Introduction*. Berlin, Heldermann Verlag, 1990.

[36] Phelps K.T. *Conjugate orthogonal quasigroups*. J. Comb. Theory, 1978, **A25**, N 2, p. 117–127.

[37] Rybnikov K.A. *Introduction in combinatorial analysis*. Moscow, Publishing House of Moscow State University, 1985 (in Russian).

[38] Sade A. *Produit direct-singulier de quasigroupes othogonaux et anti-abeliens*. Ann. Soc. Sci. Bruxelles, Ser. I, 1960, **74**, p. 91–99.

[39] Schöngardt E. *Über lateinische Quadrate und Unionen*. J. Reine Angew. Math., 1930, **163**, p. 183–229.

[40] Shcherbacov V.A. *On automorphism groups and congruences of quasigroups*. IM AN MSSR. Thesis of Ph. D., Kishinev, 1991, p. 88 (in Russian).

[41] Shcherbacov V.A. *About orthogonality of a quasigroup and its parastrophes*. International Conference on Radicals (ICOR-2003), August 11–16, 2003, Chisinau, Moldova, p. 47–48.

[42] Stein Sh.K. *On the foundations of quasigroups*. Trans. Amer. Math. Soc., 1957, **85**, N 1, p. 228–256.

Received June 16, 2005

Gary L. Mullen
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
USA
E-mail: *mullen@math.psu.edu*

Victor A. Shcherbacov
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
str. Academiei 5, MD-2028 Chisinau
Moldova
E-mail: *scerb@math.md*