BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 19–32
ISSN 1024–7696

# On some quasi-identities in finite quasigroups *

G. Belyavskaya, A. Diordiev

**Abstract.** In this article we consider some quasi-identities in quasigroups, in particular, quasi-identities connected with parastrophic orthogonality of a quasigroup. We also research some quasi-identities in quasigroups (in loops) with one parameter $\delta$ ($\delta$-quasi-identities) which arose by the study of detecting coding systems such as check character systems in [6] (see also [5, 7]), establish equivalence of such quasi-identities, connection of some of them with orthogonality of quasigroups and give a number of examples of finite quasigroups with such $\delta$-quasi-identities.

**Mathematics subject classification:** 20N05, 94B60.
**Keywords and phrases:** Quasigroup, loop, group, automorphism, quasi-identity, orthogonality, parastrophe.

## 1 Introduction

It is known that the concept of a quasi-identity (or a conditional identity [1, 11, 12]) in an algebraic system is a generalization of the concept of an identity and is used by the study of different algebraic systems, in particular, groups, semigroups.

A quasi-identity (or a conditional identity) is a formula of the form

$$(\forall x_1)\dots(\forall x_n)\ (u_1 = v_1 \,\&\dots\&\, u_m = v_m \Rightarrow u = v)$$

where $u, v, u_i, v_i$ $(i = 1, 2, \dots, m)$ are words in the alphabet $\{x_1, x_2, \dots, x_n\}$.

By writing of quasi-identities the quantor prefix usually is omitted. Each identity $u = v$ can be changed by the quasi-identity $x = x \Rightarrow u = v$.

Some classes of algebraic systems are given by means of quasi-identities. So, groupoids, in particular semigroups $(Q, \cdot)$ with the left (right) cancelation are defined by the quasi-identity $ca = cb \Rightarrow a = b$ $(ac = bc \Rightarrow a = b)$ in a groupoid (in a semigroup) $(Q, \cdot)$. The known class of separative semigroups is defined by the following quasi-identity: $a^2 = ab = b^2 \Rightarrow a = b$. The class of finite groups is simply the class of semigroups with left and right cancelation.

The concept of a quasi-identity lies in the base of definition of a quasi-variety of algebraic systems. So, the class of semigroups with the two-sided cancelation (the class of separative semigroups) forms a quasi-variety [1].



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

Different quasi-identities arise also in quasigroups and loops. So, a definition and some properties of finite quasigroups can be given by means of quasi-identities.

So, a finite quasigroup $(Q, \cdot)$ can be defined as a groupoid with the right and the left cancelations, that is with the quasi-identities:

$$xz = yz \Rightarrow x = y \text{ and } zx = zy \Rightarrow x = y.$$

For a finite qroupoid the right (left) cancelation is equivalent to left (right) invertibility.

A quasigroup $(Q, \cdot)$ is called diagonal [9] if the mapping $x \to x \cdot x = x^2$ is a permutation (bijection) on $Q$. In the case of a finite quasigroup this means that in such quasigroup the quasi-identity $x^2 = y^2 \Rightarrow x = y$ holds.

A quasigroup $(Q, \cdot)$ is called anti-commutative [3] if $xy \neq yx$ for $x \neq y$, that is the quasi-identity $xy = yx \Rightarrow x = y$ holds.

A quasigroup of Stein $(Q, \cdot)$ (that is a quasigroup with the identity $x \cdot xy = yx$) is an example of anti-commutative quasigroup: if $xy = yx$, then $x \cdot xy = xy$, $xy = y$, $x = y$, since a quasigroup of Stein is idempotent (that is $x^2 = x$ for each $x \in Q$). A quasigroup is called anti-abelian if $xy = zt$ and $yx = tz$ imply $x = z$ and $y = t$. Such a quasigroup is anti-commutative also [15].

In this article we consider some other quasi-identities in quasigroups, in particular, quasi-identities connected with parastrophic orthogonality of a quasigroup. We also research some quasi-identities in quasigroups (in loops) with one parameter $\delta$ ($\delta$-quasi-identities), which arose by the study of coding systems such as check character systems in [6] (see also [5, 7]), establish equivalence of such quasi-identities, connection of some of them with orthogonality of quasigroups and give a number of examples of finite quasigroups with these $\delta$-quasi-identities.

## 2 Some necessary notions and results

A binary quasigroup is a particular case of a groupoid.

*A groupoid* $(Q, \cdot)$ is a set $Q$ with some binary operation $(\cdot)$.

*A groupoid* $(Q, \cdot)$ *with the right (left) cancelation* is a groupoid such that in it the following quasi-identities hold: $xa = ya \Rightarrow x = y$ $(ax = ay \Rightarrow x = y)$.

*A quasigroup* $(Q, \cdot)$ is a groupoid in which every of the equations $ax = b$ and $xa = b$ has a unique solution for any $a, b \in Q$. In other words, a quasigroup is a groupoid which is invertible to the right and to the left.

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

*A quasigroup* $(Q, \cdot)$ *with a left identity* $f$ *(right identity* $e$*)* is a quasigroup such that $fx = x$ $(xe = x)$ for every $x \in Q$.

*A loop* $(Q, \cdot)$ is a quasigroup with the identity $e$: $xe = ex = x$ for each $x \in Q$.

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

*The primitive quasigroup* $(Q,\cdot,\backslash,/)$, where $x\cdot y \Leftrightarrow z/y = x,\ x\backslash z = y$, corresponds to every quasigroup $(Q,\cdot)$.

If for the designation of a quasigroup operation $(\cdot)$ the letter $A$ is used, then a primitive quasigroup $(Q, A, A^{-1}, {}^{-1}A)$, where $A(x,y) = z \Leftrightarrow A^{-1}(x,z) = y$, ${}^{-1}A(z,y) = x$ corresponds to a quasigroup $(Q,A)$. The operations $A^{-1}$, ${}^{-1}A$ (or $(\backslash)$, $(/)$) are also quasigroup operations which are called the right, left inverse operations for $A$ (for $(\cdot)$) respectively.

A quasigroup $(Q,B)$ is isotopic to a quasigroup $(Q,A)$ if there exists a tuple $T = (\alpha,\beta,\gamma)$ of permutations on $Q$ such that $B(x,y) = \gamma^{-1}A(\alpha x,\beta x)$ (shortly, $B = A^{(\alpha,\beta,\gamma)} = A^T$).

With any quasigroup operation $A$ five *parastrophes (or conjugate operations)* are connected

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

where $A^*(x,y) = A(y,x)$ [3].

**Definition 1 [2].** *Two operations $A$ and $B$, given on a set $Q$, are called orthogonal (shortly, $A\perp B$) if the system of equations $\{A(x,y)=a,\ B(x,y)=b\}$ has a unique solution for all $a,b\in Q$.*

Let $Q$ be a finite or infinite set, $A$ and $B$ be operations on $Q$, then the right (left) multiplication $A\cdot B$ $(A\circ B)$ of Mann is defined in the following way:

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

All invertible to the right (to the left) operations on a set $Q$ form a group with respect to the right (left) multiplication of Mann [13].

According to *the criterion of Belousov* [4] two quasigroups $(Q,A)$ and $(Q,B)$ are orthogonal if and only if the operation $A\cdot B^{-1}$ $(A\circ{}^{-1}B)$ is a quasigroup.

## 3 Parastrophic orthogonality of quasigroups and quasi-identities

A quasigroup $(Q,A)$ can be orthogonal with some its parastrophes. As it was proved by G. Mullen and V. Shcherbacov in [14], conditions for this orthogonality of finite quasigroups can be expressed by quasi-identities in the corresponding primitive quasigroup $(Q,A^{-1},{}^{-1}A)$. We shall give some his quasi-identities and other ones obtained with the help of the Belousov's criterion of orthogonality of two quasigroups.

**Proposition 1.** *Let $(Q,A)$ be a finite quasigroup, $(Q,\cdot,A^{-1},{}^{-1}A)$ be the corresponding primitive quasigroup. Then*

$$A\perp A^{-1} \Leftrightarrow A(x,A(x,z)) = A(y,A(y,z)) \Rightarrow x = y, \tag{1}$$

$$A \perp^{-1} A \Leftrightarrow A(A(z,x),x) = A((z,y),y) \Rightarrow x = y, \tag{2}$$
$$A \perp ({}^{-1}A)^{-1} \Leftrightarrow A(x, {}^{-1}A(x,z)) = A(y, {}^{-1}A(y,z)) \Rightarrow x = y, \tag{3}$$
$$A \perp^{-1} (A^{-1}) \Leftrightarrow A(A^{-1}(z,x),x) = A(A^{-1}(z,y),y) \Rightarrow x = y, \tag{4}$$
$$A \perp A^* \Leftrightarrow A(A^{-1}(x,z),x) = A(A^{-1}(y,z),y) \Rightarrow x = y. \tag{5}$$

**Proof.** By the criterion of Belousov $A \perp A^{-1}$ if and only if the operation $(A \cdot (A^{-1})^{-1}) = A \cdot A$ is a quasigroup. It is valid if and only if the quasi-identity (1) holds, since the operation $A \cdot A$ is always invertible from the right.

$A \perp^{-1} A$ if and only if $A \circ^{-1} ({}^{-1}A) = A \circ A$ is a quasigroup, that is the quasi-identity (2) is valid if we take into account that the operation $A \circ A$ is always invertible to the left.

By the criterion, $A \perp ({}^{-1}A)^{-1}$ if and only if the invertible from the right operation $A \cdot (({}^{-1}A)^{-1})^{-1} = A \cdot^{-1} A$ is a quasigroup, that is invertible from the left. It is valid if and only if the quasi-identity (3) holds.

Analogously, $A \perp^{-1} (A^{-1})$ if and only if the invertible from the left operation $A \circ^{-1} ({}^{-1}(A^{-1})) = A \circ A^{-1}$ is a quasigroup, that is the quasi-identity (4) holds.

At last, $A \perp A^*$ if and only if $A^* \cdot A^{-1}$ is a quasigroup, that is the quasi-identity (5) holds. □

**Proposition 2.** *Let $(Q, \cdot, \backslash, /)$ be a finite primitive quasigroup. Then the quasi-identity (1) is equivalent to the quasi-identity*

$$A({}^{-1}A(x,z),x) = A({}^{-1}A(y,z),y) \Rightarrow x = y, \tag{6}$$

*the quasi-identity (2) is equivalent to the quasi-identity*

$$A(x, A^{-1}(z,x)) = A(y, A^{-1}(z,y) \Rightarrow x = y, \tag{7}$$

*the quasi-identity (3) is equivalent to the quasi-identity*

$$A(A(x,z),x) = A(A(y,z),y) \Rightarrow x = y, \tag{8}$$

*the quasi-identity (4) is equivalent to the quasi-identity*

$$A(x, A(z,x)) = A(y, A(z,y)) \Rightarrow x = y, \tag{9}$$

*the quasi-identity (5) is equivalent to the quasi-identity*

$$A(x, {}^{-1}A(z,x)) = A(y, {}^{-1}A(z,y)) \Rightarrow x = y. \tag{10}$$

**Proof.** Indeed, $A \perp A^{-1}$ by the criterion of Belousov if and only if $A \circ^{-1} (A^{-1})$ is a quasigroup. But $(A \circ^{-1} (A^{-1}))(z,x) = A({}^{-1}(A^{-1})(z,x),x) = A({}^{-1}A(x,z),x)$, since ${}^{-1}(A^{-1})(z,x) = {}^{-1}A(x,z)$. So $A \circ^{-1} (A^{-1})$ is a quasigroup if and only if (6) holds.

$A \perp^{-1} A$ if and only if $A \cdot ({}^{-1}A)^{-1}$ is a quasigroup. Taking into account that $({}^{-1}A)^{-1}(x,z) = A^{-1}(z,x)$ we have $(A \cdot ({}^{-1}A)^{-1})(x,z) = A(x, ({}^{-1}A)^{-1}(x,z)) = A(x, A^{-1}(z,x))$. So $A \cdot ({}^{-1}A)^{-1}$ is a quasigroup if and only if (7) holds.

$A \perp ({}^{-1}A)^{-1}$ if and only if $A \circ^{-1} (({}^{-1}A)^{-1}) = A \circ A^*$ is a quasigroup, that is the quasi-identity $A(A^*(z,x),x) = A(A^*(z,y),y) \Rightarrow x = y$ or (8) holds.

$A \perp^{-1} (A^{-1})$ if and only if $A \cdot ({}^{-1}(A^{-1}))^{-1} = A \cdot A^*$ is a quasigroup. This condition is equivalent to the quasi-identity (9).

$A^* \perp A$ if and only if $A^* \circ^{-1} A$ is a quasigroup if and only if the quasi-identity $A^*({}^{-1}A(z,x),x) = A^*({}^{-1}A(z,y),y) \Rightarrow x = y$ or (10) holds. □

Using the designation $(\cdot)$ for an operation $A$ we can write the quasi-identities (1)-(10),respectively, in the following way (we use the same numeration for them) :

$$x \cdot xz = y \cdot yz \Rightarrow x = y, \tag{1}$$

$$zx \cdot x = zy \cdot y \Rightarrow x = y, \tag{2}$$

$$x \cdot (x/z) = y \cdot (y/z) \Rightarrow x = y, \tag{3}$$

$$(z\backslash x) \cdot x = (z\backslash y) \cdot y \Rightarrow x = y, \tag{4}$$

$$(x\backslash z) \cdot x = (y\backslash z) \cdot y \Rightarrow x = y, \tag{5}$$

$$(x/z) \cdot x = (y/z) \cdot y \Rightarrow x = y, \tag{6}$$

$$x \cdot (z\backslash x) = y \cdot (z\backslash y) \Rightarrow x = y, \tag{7}$$

$$xz \cdot x = yz \cdot y \Rightarrow x = y, \tag{8}$$

$$x \cdot zx = y \cdot zy \Rightarrow x = y, \tag{9}$$

$$x \cdot (z/x) = y \cdot (z/y) \Rightarrow x = y. \tag{10}$$

Note that the quasi-identities (1), (2), (8) and (9) were obtained in [14].

From Proposition 1 and 2 it follows at once

**Theorem 1.** *Let $(Q, \cdot)$ be a finite quasigroup. Then*

$$(\cdot) \perp (\cdot)^{-1} \Leftrightarrow x \cdot xz = y \cdot yz \Rightarrow x = y \Leftrightarrow (x/z) \cdot x = (y/z) \cdot y \Rightarrow x = y,$$

$$(\cdot) \perp^{-1} (\cdot) \Leftrightarrow zx \cdot x = zy \cdot y \Rightarrow x = y \Leftrightarrow x \cdot (z\backslash x) = y \cdot (z\backslash y) \Rightarrow x = y,$$

$$(\cdot) \perp ({}^{-1}(\cdot))^{-1} \Leftrightarrow x \cdot (x/z) = y \cdot (y/z) \Rightarrow x = y \Leftrightarrow xz \cdot x = yz \cdot y \Rightarrow x = y,$$

$$(\cdot) \perp^{-1} ((\cdot)^{-1}) \Leftrightarrow (z\backslash x) \cdot x = (z\backslash y) \cdot y \Rightarrow x = y \Leftrightarrow x \cdot zx = y \cdot zy \Rightarrow x = y,$$

$$(\cdot) \perp (\cdot)^* \Leftrightarrow (x\backslash z) \cdot x = (y\backslash z) \cdot y \Rightarrow x = y \Leftrightarrow x \cdot (z/x) = y \cdot (z/y) \Rightarrow x = y.$$

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

(i) *all quasi-identities (1)-(4),(6)-(9) are equivalent;*

(ii) *each one of the first four parastrophic orthogonalities of Theorem 1 implies the rest of these orthogonalities.*

**Proof.** In the case of a commutative quasigroup (that is $xy = yx$ for all $x, y \in Q$) it is easy to see that

$$(1) \Leftrightarrow (2) \Leftrightarrow (8) \Leftrightarrow (9).$$

Item (ii) follows from this fact and Theorem 1. □

In a finite commutative quasigroup the quasi-identities (5) and (10) do not hold, since $(\cdot)$ and $(\cdot)^* = (\cdot)$ are not orthogonal.

**Corollary 2.** *Let $(Q, \cdot)$ be a finite loop Moufang (in particular, a finite group). Then*

(i) *if in $(Q, \cdot)$ one of the quasi-identities (1)-(4), (6)-(9) holds, then $(Q, \cdot)$ is diagonal;*

(ii) *if $(Q, \cdot)$ is diagonal, then* (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (8) $\Leftrightarrow$ (9) *and $(Q, \cdot)$ is orthogonal to each of its parastrophes, except $(Q, (\cdot)^*)$;*

(iii) *$(Q, \cdot)$ is not orthogonal to $(Q, (\cdot)^*)$;*

(iv) *a loop Moufang $(Q, \cdot)$ of odd order is orthogonal to each of its parastrophes, except $(Q, (\cdot)^*)$.*

**Proof.** (i) Let (1) ((2), (8) or (9)) hold in a finite loop Moufang, then by $z = e$ ($e$ is the identity of the loop) we have that $x^2 = y^2 \Rightarrow x = y$. The rest quasi-identities, except (5) and (10), are equivalent to one of these quasi-identities by Theorem 1.

(ii) Let $(Q, \cdot)$ be diagonal, that is $x^2 = y^2 \Rightarrow x = y$, then (1) and (2) also hold, since a loop Moufang is diassociative (that is each two elements generate a subgroup) [3]. Show that from $x^2 = y^2 \Rightarrow x = y$ it follows (9):

$$x \cdot x = y \cdot y \Leftrightarrow z(x \cdot x) = z(y \cdot y) \Leftrightarrow zx \cdot x =$$

$$= zy \cdot y \Leftrightarrow x \cdot L_z^{-1}x = y \cdot L_z^{-1}y \Leftrightarrow x \cdot z_1 x = y \cdot z_1 y,$$

where $L_z x = zx$, $z_1 = z^{-1}$, since in a loop Moufang $L_z^{-1} = L_{z^{-1}}$ (see, for example,[3]). Thus, $x^2 = y^2 \Rightarrow x = y$ implies $x \cdot z_1 x = y \cdot z_1 y \Rightarrow L_z^{-1}x = L_z^{-1}y \Rightarrow x = y$. Analogously, have for (8):

$$x \cdot x = y \cdot y \Leftrightarrow x \cdot xz = y \cdot yz \Leftrightarrow R_z^{-1}x \cdot x = R_z^{-1}y \cdot y \Leftrightarrow xz_2 \cdot x = yz_2 \cdot x,$$

where $R_z x = xz$, $z_2 = z^{-1}$, since in a loop Moufang $R_z^{-1} = R_{z^{-1}}$. Hence, from $x^2 = y^2 \Rightarrow x = y$ it follows $xz_2 \cdot x = yz_2 \cdot y \Rightarrow R_z^{-1}x = R_z^{-1}y \Rightarrow x = y$.

(iii) If $(Q, \cdot)$ is a loop Moufang, then $x \backslash z = x^{-1}z$, $z/x = zx^{-1}$, so the quasi-identity (5) becomes $x^{-1}z \cdot x = y^{-1}z \cdot y \Rightarrow x = y$. But by $z = e$ this quasi-identity does not hold (we have $e = e$ by $x \neq y$).

(iv) Is a corollary of (ii) if to take into account that a loop Moufang (see, for example,[6]), as in the case of a group (see [3]), of odd order is diagonal. □

## 4 Some quasi-identities with one parameter

In different cases in a quasigroup $(Q, \cdot)$ quasi-identities ($\delta$-quasi-identities) in which one permutation $\delta$ of $Q$ presents, arise. For example, a quasigroup $(Q, \cdot)$ is called admissible if there exists a permutation $\delta$ (it is called *complete* for the quasigroup $(Q, \cdot)$) such that the mapping $x \to x \cdot \delta x$ is also a permutation of $Q$. If a quasigroup $(Q\cdot)$ is finite, then a permutation $\delta$ is complete if and only if in $(Q, \cdot)$ the $\delta$-quasi-identity $x \cdot \delta x = y \cdot \delta y \Rightarrow x = y$ with the permutation $\delta$ holds.

In some applications of the quasigroups and loops these quasi-identities also arise. So, by the study of such detecting coding systems as check character systems with one control symbol arose a number of quasi-identities with one parameter $\delta$.

A check character (or digit) system with one check character is an error detecting code over an alphabet $Q$ which arises by appending a check digit $a_n$ to every word $a_1 a_2 \dots a_{n-1} \in Q^{n-1}$:

$$a_1 a_2 \dots a_{n-1} \to a_1 a_2 \dots a_{n-1} a_n$$

(see surveys [7, 8, 10, 17]).

The control digit $a_n$ can be calculated by different check formulas, in particular, with the help of a quasigroup (a loop, a group) $(Q, \cdot)$. One of such formulas with a quasigroup $(Q, \cdot)$ is

$$(\dots(((a_1 \cdot \delta a_2) \cdot \delta^2 a_3) \cdot \dots) \cdot \delta^{n-2} a_{n-1}) \cdot \delta^{n-1} a_n = c, \tag{11}$$

where $\delta$ is a fixed permutation on $Q$, $c$ is a fixed element of $Q$.

This system can detect the most prevalent errors such as single errors ($a \to b$), adjacent errors ($ab \to ba$), jump transpositions ($acb \to bca$), twin errors ($aa \to bb$) and jump twin errors ($aca \to bcb$) if the parameter $\delta$ satisfies some conditions.

In [6] the following statement ([6, Theorem 1]) was proved.

**Theorem 2 [6].** *A check character system using a quasigroup $(Q, \cdot)$ and coding (11) for $n > 4$ is able to detect all*

I *single errors;*

II *transpositions if and only if for all $a, b, c, d \in Q$ with $b \neq c$ in the quasigroup $(Q, \cdot)$ the inequalities*

$$(\alpha_1) \qquad b \cdot \delta c \neq c \cdot \delta b \quad \text{and} \quad ab \cdot \delta c \neq ac \cdot \delta b \qquad (\alpha_2)$$

*hold;*

III *jump transpositions if and only if $(Q, \cdot)$ has the properties*

$$(\beta_1) \qquad bc \cdot \delta^2 d \neq dc \cdot \delta^2 b \quad \text{and} \quad (ab \cdot c) \cdot \delta^2 d \neq (ad \cdot c) \cdot \delta^2 b \qquad (\beta_2)$$

*for all $a, b, c, d \in Q$, $b \neq d$;*

IV *twin errors if and only if* $(Q,\cdot)$ *satisfies the inequalities*

$$(\gamma_1) \qquad b\cdot\delta b \neq c\cdot\delta c \quad \textit{and} \quad ab\cdot\delta b \neq ac\cdot\delta c \qquad (\gamma_2)$$

*for all* $a,,b,c,d\in Q,\ b\neq c$;

V *jump twin errors if and only if in* $(Q,\cdot)$ *the inequalities*

$$(\sigma_1) \qquad bc\cdot\delta^2 b \neq dc\cdot\delta^2 d \quad \textit{and} \quad (ab\cdot c)\cdot\delta^2 b \neq (ad\cdot c)\cdot\delta^2 d \qquad (\sigma_2)$$

*hold for all* $a,b,c,d\in Q,\ b\neq d$.

The following quasi-identities correspond to the inequalities of Theorem 2:

$$(a_1)\colon\ x\cdot\delta y = y\cdot\delta x \Rightarrow x=y, \qquad (a_2)\colon\ zx\cdot\delta y = zy\cdot\delta x \Rightarrow x=y,$$
$$(b_1)\colon\ xy\cdot\delta^2 z = zy\cdot\delta^2 x \Rightarrow x=z, \qquad (b_2)\colon\ (ux\cdot y)\cdot\delta^2 z = (uz\cdot y)\cdot\delta^2 x \Rightarrow x=z,$$
$$(c_1)\colon\ x\cdot\delta x = y\cdot\delta y \Rightarrow x=y, \qquad (c_2)\colon\ zx\cdot\delta x = zy\cdot\delta y \Rightarrow x=y,$$
$$(d_1)\colon\ xy\cdot\delta^2 x = zy\cdot\delta^2 z \Rightarrow x=z, \qquad (d_2)\colon\ (ux\cdot y)\cdot\delta^2 x = (uz\cdot y)\cdot\delta^2 z \Rightarrow x=z.$$

Below we shall assume that all these quasi-identities depend on a permutation $\delta$ and shall sometimes call them $\delta$-quasi-identities.

In a loop $(Q,\cdot)$ (in a quasigroup with the left identity) $(a_2)\Rightarrow(a_1)$, $(b_2)\Rightarrow(b_1)$, $(c_2)\Rightarrow(c_1)$, $(d_2)\Rightarrow(d_1)$. In a group these pairs of quasi-identities are equivalent (see Proposition 2 of [6]).

In [6] some properties of quasigroups with the pointed inequalities were established. In accordance with Proposition 3 and Corollaries 3 and 4 of [6] in a loop $(Q,\cdot)$ the following statements are valid if $\delta=\varepsilon$ ($\varepsilon$ is the identity permutation):

1) $\varepsilon$-quasi-identities $(a_2)$ and $(b_2)$ do not hold;

2) from $\varepsilon$-quasi-identity $(d_2)$ $\varepsilon$-quasi-identity $(c_2)$ follows;

3) in a loop Moufang (in particular, in a group) all $\varepsilon$-quasi-identities $(d_1)$, $(d_2)$, $(c_1)$ and $(c_2)$ are equivalent;

4) in a finite Moufang loop (in a finite group) $\varepsilon$-quasi-identity $(c_1)$ ($(c_2)$, $(d_1)$ ,$(d_2)$) holds if and only if $x^2=y^2\Rightarrow x=y$;

5) in a finite Moufang loop of odd order $\varepsilon$-quasi-identities $(c_1)$, $(c_2)$, $(d_1)$ and $(d_2)$ always hold.

From Corollary 2 and items 3) and 4) it follows

**Corollary 3.** *If in a finite Moufang loop (in a finite group)* $(Q,\cdot)$ $\varepsilon$*-quasi-identity* $(c_1)$ *(*$(c_2)$*,* $(d_1)$ *or* $(d_2)$*) holds, then this loop is orthogonal to every its parastrophes, except* $(Q,(\cdot)^*)$.

As it was said above, in a loop (a group) $\varepsilon$-quasi-identities $(a_2)$ and $(b_2)$ can not hold. But in a quasigroup with the left identity these $\varepsilon$-quasi-identities can hold.

All examples given below were checked by computer research.

**Example 1.** The quasigroup $(Q, \cdot)$ of order 4 on the set $Q = \{1, 2, 3, 4\}$ with the left identity 1 in Table 1 satisfies all $\varepsilon$-quasi-identities $(a_2)$, $(b_2)$, $(c_2)$, $(d_2)$ (and $(a_1)$, $(b_1)$, $(c_1)$, $(d_1)$ also).

Table 1:

| $(\cdot)$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 3 | 4 | 1 | 2 |
| 3 | 4 | 3 | 2 | 1 |
| 4 | 2 | 1 | 4 | 3 |

Table 2:

| $(\cdot)$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 3 | 4 | 2 | 5 | 1 |
| 3 | 4 | 1 | 5 | 3 | 2 |
| 4 | 5 | 3 | 1 | 2 | 4 |
| 5 | 2 | 5 | 4 | 1 | 3 |

Table 3:

| $(\cdot)$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 3 | 1 | 4 | 5 | 2 |
| 3 | 2 | 5 | 1 | 3 | 4 |
| 4 | 5 | 4 | 2 | 1 | 3 |
| 5 | 4 | 3 | 5 | 2 | 1 |

The quasigroup of order 5 with the left identity 1 given in Table 2 satisfies only $\varepsilon$-quasi-identities $(a_2)$, $(b_2)$, $(c_2)$ (and $(a_1)$, $(b_1)$, $(c_1)$ also).

In the quasigroup of order 5 with the left identity 1 in Table 3 $\delta$-quasi-identities $(a_2)$, $(b_2)$, $(c_2)$ (and $(a_1)$, $(b_1)$, $(c_1)$) hold with $\delta = (14532)$.

Note that here and below we do not write the first row of permutations in the natural order.

A loop (a group) can satisfy $\delta$-quasi-identities $(a_2)$, $(b_2)$ (and $(a_1)$, $(b_1)$) if $\delta \neq \varepsilon$ as the following example shows.

**Example 2.** The group of order 4 (of order 5) in Table 4 (in Table 5) satisfies $\delta$-quasi-identities $(a_1)$, $(a_2)$, $(b_1)$, $(b_2)$, $(c_1)$, $(c_2)$, $(d_1)$ and $(d_2)$ with $\delta = (1342)$ ($\delta$-quasi-identities $(a_1)$, $(a_2)$, $(b_1)$, $(b_2)$, $(c_1)$, $(c_2)$ with $\delta = (13524)$).

The loop of order 6 in Table 6 satisfies $\delta$-quasi-identities $(a_1)$, $(a_2)$ with $\delta = (213456)$.

Table 4:

| $(\cdot)$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 1 | 4 | 3 |
| 3 | 3 | 4 | 1 | 2 |
| 4 | 4 | 3 | 2 | 1 |

Table 5:

| $(\cdot)$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 5 | 1 |
| 3 | 3 | 4 | 5 | 1 | 2 |
| 4 | 4 | 5 | 1 | 2 | 3 |
| 5 | 5 | 1 | 2 | 3 | 4 |

Table 6:

| $(\cdot)$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 6 | 5 | 3 | 4 | 1 |
| 3 | 3 | 5 | 6 | 1 | 2 | 4 |
| 4 | 4 | 3 | 2 | 6 | 1 | 5 |
| 5 | 5 | 4 | 1 | 2 | 6 | 3 |
| 6 | 6 | 1 | 4 | 5 | 3 | 2 |

In [6, Corollary 1] it was also proved that if a finite quasigroup $(Q,\cdot)$ satisfies conditions $(\gamma_2)$ $((\sigma_1)$ or $(\sigma_2))$, then this quasigroup has orthogonal mate. This means that if in a finite quasigroup $(Q,\cdot)$ $\delta$-quasi-identity $(c_2)$ $((d_1)$ or $(d_2))$ holds, then it has orthogonal mate.

In addition now we shall establish some other orthogonalities which are connected with a quasigroup $(Q,A)$ with $\delta$-quasi-identity $(c_2)$ $((d_1)$ or $(d_2))$.

**Proposition 3.** *In a finite quasigroup $(Q,A)$*

(i) *$\delta$-quasi-identity $(c_2)$ holds if and only if $A^{(\varepsilon,\delta,\varepsilon)} \perp {}^{-1}A$;*

(ii) *$\delta$-quasi-identity $(d_1)$ holds if and only if $A^{(\varepsilon,\delta^2,\varepsilon)} \perp ({}^{-1}A)^{-1}$;*

(iii) *$\delta$-quasi-identity $(d_2)$ holds if and only if $A^{(\varepsilon,\delta^2 L_u^{-1},\varepsilon)} \perp ({}^{-1}A)^{-1}$ for any $u \in Q$.*

**Proof.** (i) Let $B = A^{(\varepsilon,\delta,\varepsilon)}$, that is $B(x,y) = A(x,\delta y)$ by the definition of isotopic quasigroups. By the criterion of Belousov $B \perp^{-1} A$ if and only if $B \circ A$ is a quasigroup. But $(B \circ A)(z,x) = B(A(z,x),x) = A(A(z,x),\delta x)$, so $B \circ A$ is a quasigroup if and only if $(B \circ A)(z,x) = (B \circ A)(z,y) \Rightarrow x = y$ or $A(A(z,x),\delta x) = A(A(z,y),\delta y) \Rightarrow x = y$. It is $\delta$-quasi-identity $(c_2)$.

(ii) Let $B(x,y) = A(x,\delta^2 y)$, then $B \perp ({}^{-1}A)^{-1}$ if and only if $B \circ A^*$ is a quasigroup, that is if and only if $B(A(x,y),x) = B(A(z,y),z) \Rightarrow x = z$ or $(d_1)$ holds.

(iii) Let $C = A^{(\varepsilon,\delta^2 L_u^{-1},\varepsilon)}$, that is $C(x,y) = A(x,\delta^2 L_u^{-1} y)$, then $C \perp ({}^{-1}A)^{-1}$ if and only if $C \circ^{-1} (({}^{-1}A)^{-1}) = C \circ A^*$ is a quasigroup. This is valid if and only if $(C \circ A^*)(y,x) = (C \circ A^*)(y,z) \Rightarrow x = z$ or $C(A(x,y),x) = C(A(z,y),z) \Rightarrow x = z$, that is $A(A(x,y),\delta^2 L_u^{-1} x) = A(A(z,y),\delta^2 L_u^{-1} z) \Rightarrow x = z$ or $A(A(L_u x,y),\delta^2 x) = A(A(L_u z,y),\delta^2 z) \Rightarrow L_u x = L_u z \Rightarrow x = z$. It is $\delta$-quasi-identity $(d_2)$. $\square$

From Proposition 3 it immediately follows (see also Theorem 1 concerning quasi-identities (2) and (8))

**Corollary 4.** *In a finite quasigroup $(Q,A)$*

(i) *$\varepsilon$-quasi-identity $(c_2)$ holds if and only if $A \perp^{-1} A$;*

(ii) *$\delta$-quasi-identity $(d_1)$ with $\delta^2 = \varepsilon$ holds if and only if $A \perp ({}^{-1}A)^{-1}$;*

(iii) *$\delta$-quasi-identity $(d_2)$ with $\delta^2 = \varepsilon$ holds if and only if $A^{(\varepsilon,L_u^{-1},\varepsilon)} \perp ({}^{-1}A)^{-1}$ for any $u \in Q$.*

As it was said above, in a loop from the $\varepsilon$-quasi-identity $(d_2)$ the quasi-identity $(c_2)$ follows, so from Corollary 4 it follows

**Corollary 5.** *If in a finite loop $(Q,A)$ $\varepsilon$-quasi-identity $(d_2)$ holds, then $A \perp^{-1} A$ and $A \perp ({}^{-1}A)^{-1}$.*

**Proposition 4.** *Let $(Q,\cdot)$ be a finite group. Then*

(i) *if* $\delta$ *is a complete permutation of* $(Q,\cdot)$ *then* ${}^{-1}(\cdot) \perp (\cdot)^{T_a}$ *for every* $a \in Q$, *where* $T_a = (\varepsilon, \delta L_a, \varepsilon)$;

(ii) *if in* $(Q,\cdot)$ $(d_1)$ *holds, then* ${}^{-1}(\cdot) \perp (\cdot)^{T_{a,b,c}}$ *for all* $a,b,c \in Q$, *where* $T_{a,b,c} = (\varepsilon, \delta^2 L_a R_b L_c, \varepsilon)$.

**Proof.** (i) By the condition of (i) in a group $(Q,\cdot)$ the $\delta$-quasi-identity $(c_1)$ holds, but then $(c_2)$ also holds for any $z = Ia$ $(I : x \to x^{-1})$, since in a group $\delta$-quasi-identity $(c_1)$ is equivalent to $(c_2)$, that is $L_{Ia}x\cdot\delta x = L_{Ia}y\cdot\delta y \Rightarrow x = y$ or $x\cdot\delta L_a x = y\cdot\delta L_a y \Rightarrow L_a x = L_a y$ (or $x = y$), since in a group $L_a^{-1} = L_{Ia}$. Thus, $x\cdot\delta_1 x = y\cdot\delta_1 y \Rightarrow x = y$, where $\delta_1 = \delta L_a$. By Proposition 3 ${}^{-1}(\cdot) \perp (\cdot)^{T_a}$, where $T_a = (\varepsilon, \delta_1, \varepsilon)$.

(ii) Let in $(Q,\cdot)$ $(d_1)$ hold, then $(d_2)$ is valid also, so for any $a,b \in Q$ we have $((Ia\cdot x)\cdot Ib)\cdot\delta^2 x = ((Ia\cdot z)\cdot Ib)\cdot\delta^2 z \Rightarrow x = z$ or $R_{Ib}L_{Ia}x\cdot\delta^2 x = R_{Ib}L_{Ia}z\cdot\delta^2 z \Rightarrow x = z$, whence it follows that $x\cdot\delta^2 L_a R_b x = z\cdot\delta^2 L_a R_b z \Rightarrow x = z$ or $x\cdot\overline{\delta}x = z\cdot\overline{\delta}z \to x = z$, where $\overline{\delta} = \delta^2 L_a R_b$. By item (i) of this Proposition ${}^{-1}(\cdot) \perp (\cdot)^{T_{a,b,c}}$ with $T_{a,b,c} = (\varepsilon, \delta^2 L_a R_b L_c, \varepsilon)$ for any $a,b,c \in Q$. □

## 5 Equivalence of some quasi-identities with one parameter

A quasigroup $(Q,\cdot)$ can satisfy some $\delta$-quasi-identities from $(a_1) - (d_2)$ with distinct permutations $\delta$. A part of such permutations can be obtained from the permutation $\delta$ of a $\delta$-quasi-identity with the help of the group of automorphisms of a quasigroup.

In [5] for quasigroups by analogy with groups (see [16]) the following transformation of $\delta$ with the help of an automorphism was introduced.

**Definition 1 [5].** *A permutation* $\delta_1$ *is called automorphism equivalent to a permutation* $\delta$ $(\delta_1 \sim \delta)$ *for a quasigroup* $(Q,\cdot)$ *if there exists an automorphism* $\alpha$ *of* $(Q,\cdot)$ *such that* $\delta_1 = \alpha\delta\alpha^{-1}$.

Proposition 1 of [5] can be reformulated for $\delta$-quasi-identities in the following way taking into account Theorem 1.

**Proposition 5.** (i) *Automorphism equivalence of permutations is an equivalence relation (that is reflexive, symmetric and transitive).*

(ii) *If a quasigroup* $(Q,\cdot)$ *satisfies the* $\delta$*-quasi-identity* $(a_1)$ $((a_2)$, $(b_1)$, $(b_2)$, $(c_1)$, $(c_2)$, $(d_1)$ *or* $(d_2))$ *and a permutation* $\delta_1$ *is an automorphism equivalent to* $\delta$, *then in* $(Q,\cdot)$ *the respective* $\delta_1$*-quasi-identity holds.*

More general transformation of permutations can be considered in a loop with a nonempty nucleus. So, in [5] for a loop a weak equivalence was introduced by analogy with a group (see [16]).

Recall that the nucleus $N$ of a loop is the intersection of the left, right and middle nuclei:

$$N = N_l \cap N_r \cap N_m,$$

where

$$N_l = \{a \in Q \mid ax \cdot y = a \cdot xy \text{ for all } x, y \in Q\},$$
$$N_r = \{a \in Q \mid x \cdot ya = xy \cdot a \text{ for all } x, y \in Q\},$$
$$N_m = \{a \in Q \mid xa \cdot y = x \cdot ay \text{ for all } x, y \in Q\}.$$

All these nuclei are subgroups in a loop [3]. In a group $(Q, \cdot)$ the nucleus $N$ coincides with $Q$.

**Definition 3.** *A permutation $\delta_1$ of a set $Q$ is called weakly equivalent to a permutation $\delta$ ($\delta_1 \overset{w}{\sim} \delta$) for a loop $(Q, \cdot)$ with the nucleus $N$ if there exist an automorphism $\alpha$ ($\alpha \in \mathrm{Aut}(Q, \cdot)$) of the loop and elements $p, q \in N$ such that $\delta_1 = R_p \alpha \delta \alpha^{-1} L_q$, where $R_p x = xp$, $L_q x = qx$*
*(the permutations act to the left from the right).*

Note that if $\delta$ is a complete permutation in a loop with nucleus $N$, then $\delta_1 = R_p \alpha \delta \alpha^{-1} L_q$ is also complete, where $\alpha \in \mathrm{Aut}(Q, \cdot)$, $p, q \in N$.

Proposition 2 of [5] can be reformulated for the $\delta$-quasi-identities in the following way.

**Proposition 6.** a) *Weak equivalence is an equivalence relation for a loop.*

b) *If in a loop $(Q, \cdot)$ the $\delta$-quasi-identity $(a_1)$ ($(a_2)$, $(c_1)$ or $(c_2)$) holds and the $\delta_1 \overset{w}{\sim} \delta$, then this loop satisfies the respective $\delta_1$-quasi-identities also.*

c) *If, in addition, $\delta$ is an automorphism of $(Q, \cdot)$ and $\delta$-quasi-identity $(a_1)$ ($(a_2)$, $(b_1)$, $(b_2)$, $(c_1)$, $(c_2)$, $(d_1)$ or $(d_2)$) holds, then the corresponding $\delta_1$-quasi-identity holds too.*

According to Corollary 2 of [5] in a Moufang loop of odd order with the nucleus $N$ the $\delta$-quasi-identities $(c_1)$, $(c_2)$, $(d_1)$, $(d_2)$ by $\delta = R_p L_q$, $p, q \in N$, always hold (the respective $\varepsilon$-quasi-identities hold too).

In [5] an example of a loop of order 8 with the nucleus of four elements and with the group of automorphisms of order 4, some permutations and weak equivalent permutations to these permutations which satisfy the quasi-identities $(c_2)$ were given. Here we give a loop of order 9 with the nucleus of three elements and with the group of automorphisms of order 6.

**Example 3.** The loop $(Q, \cdot)$ of order 9 on the set $Q = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ with the identity 1 is given in Table 7.

Table 7:

| $(\cdot)$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2 | 2 | 3 | 1 | 5 | 6 | 4 | 8 | 9 | 7 |
| 3 | 3 | 1 | 2 | 6 | 4 | 5 | 9 | 7 | 8 |
| 4 | 4 | 5 | 6 | 8 | 9 | 7 | 2 | 3 | 1 |
| 5 | 5 | 6 | 4 | 9 | 7 | 8 | 3 | 1 | 2 |
| 6 | 6 | 4 | 5 | 7 | 8 | 9 | 1 | 2 | 3 |
| 7 | 7 | 8 | 9 | 2 | 3 | 1 | 5 | 6 | 4 |
| 8 | 8 | 9 | 7 | 3 | 1 | 2 | 6 | 4 | 5 |
| 9 | 9 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 |

A computer research has shown that this loop has the following group of automorphisms of order 6:

$$\operatorname{Aut} Q = \{(123456789), (123789456), (123645897), (123897645),$$

$$(123564978), (123978564)\}$$

and the nucleus $N = N_r = \{1, 2, 3\}$.

This loop satisfies the quasi-identities $(c_2)$ and $(d_2)$ with the permutation $\delta_0 = (123456897)$ and with the following permutations which are weakly equivalent to $\delta_0$ (that is have the form $R_p \alpha \delta_0 \alpha^{-1} L_q$, where $\alpha \in \operatorname{Aut}(Q, \cdot)$, $p, q \in N$): (123456897), (231564978), (312645789), (123564789), (231645897), (312456978).

## References


[1] Artamonov A., Salii V.N., Skornyakov L.A. *General algebra. Vol. 2.* Moscow, 1991 (in Russian).

[2] Belousov V.D. *On properties of binary operations.* Uchenie zapiski of Bel'skogo pedinstituta, 1960, vyp. 5, p. 9–28 (in Russian).

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

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

[5] Belyavskaya G.B. *On check character systems over quasigroups and loops.* Algebra and discrete mathematics, 2003, N 2, p. 1–13.

[6] Belyavskaya G.B., Izbash V.I., Mullen G.L. *Check character systems using quasigroups: I.* Designs, Codes and Cryptography, 2005, **37**, p. 215–227.

[7] Belyavskaya G.B., Izbash V.I., Shcherbacov V.A. *Check character systems over quasigroups and loops.* Quasigroups and related systems, 2003, **10**, p. 1–28.

[8] Damm M. *Pruefziffersysteme ueber Quasigruppen.* Diplomarbeit Universitaet Marburg, Maerz, 1998.

[9] Deneš J., Keedwell A.D. *Latin squares and their applications.* Budapest, Academiai Kiado, 1974.

[10] Ecker A., Poch G. *Check character systems.* Computing, 1986, N 37(4), p. 277–301.

[11] Gorbunov V.A. *Algebraic theory of quasi-varieties*. Novosibirsk, 1998 (in Russian).

[12] Mal'cev A.I. *Algebraic systems*. Moscow, Nauka, 1970 (in Russian).

[13] Mann H.B. *On orthogonal latin squares*. Bull. Amer. Math. Soc., 1944, **50**, p. 249–257.

[14] Mullen G.L., Shcherbacov V.A. *On orthogonality of binary operations and squares*. Buletinul A. Ş. M., Matematica, 2005, N 2(48), p. 3–42.

[15] Sade A. *Produit direct-singular di quasigroups orthogonaux et anti-abelians*. Ann. Soc. Sci., Bruxelles, Ser. I, 1960, **74**, p. 91–99.

[16] Schulz R.-H. *On check digit systems using anti-symmetric mappings*. In J. Althofer. et al. editors. Number, Information and Complexity, Kluwer Acad. Publ. Boston, 2000, p. 295–310.

[17] Verhoeff I. *Error Detecting Decimal Codes*. Math. Center Tracts 29, Amsterdam, 1969.

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

*Received December 12, 2005*