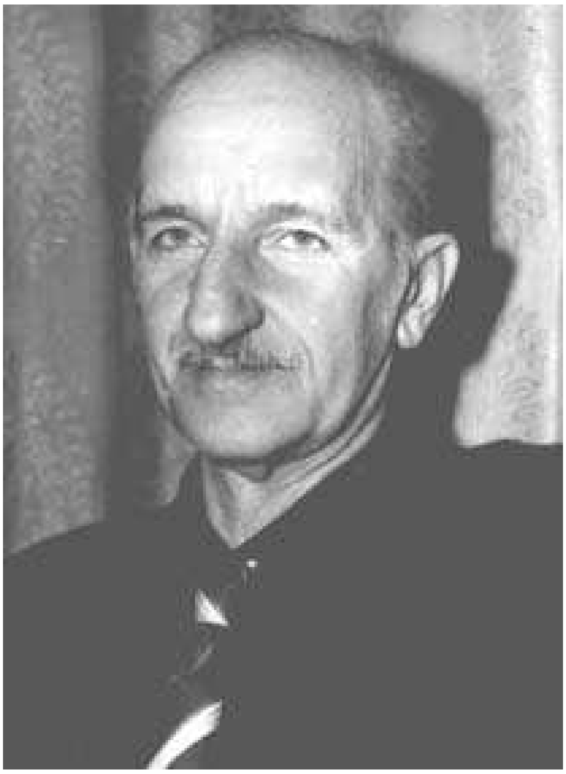
Valentin Danilovich Belousov
(1925 – 1988)

This issue is a tribute in honor of his 80th birthday



This year it has been 80 years since V. D. Belousov's birth. He was a famous scientist which made a great contribution to the theory of binary and n-ary quasigroups and loops, theory of algebraic nets and theory of functional equations on quasigroups. In the opinion of many famous mathematicians he was the leading specialist in theory of quasigroups during the sixties and the seventies of the previous century. A. D. Keedwell wrote about him: "*V. D. Belousov, prolific as a researcher, who, like Albert, Bruck and Artzy, engaged in work which was ahead of its time.*"

V.D. Belousov studied many general questions on quasigroups and loops: derivative operations of loops; groups of regular mappings; nuclei of quasigroups; autotopies and antiautotopies, characterized groups of inner permutations, normal subquasigroups, isotopy and crossed isotopy and different groups associated with quasigroups.

In many papers special classes of quasigroups and loops are investigated: IP-quasigroups, F-quasigroups, TS-quasigroups, CI-quasigroups, Stein quasigroups, I-quasigroups, Bol loops, G-loops etc. Belousov's articles contain definitions of new classes of quasigroups and loops, for example, PI-quasigroups, P-quasigroups, S-loops, M-loops, linear quasigroups over groups.

Very important Belousov's results are connected with distributive quasigroups. He proved that every distributive quasigroup is isotopic to a commutative Moufang loop.

In a series of papers transitive distributive quasigroups are described. Simultaneously he found a class of left-distributive quasigroups non-isotopic to groups and characterized connections between some of such quasigroups, Moufang and Bol loops. Loops isotopic to left-distributive quasigroups are studied too. The series of papers is devoted to different systems of binary operations defined on the same set. In particular, Belousov studied systems of quasigroup operations satisfying some laws of distributivity, associativity, mediality and transitivity. Positional algebras of partial quasigroup operations investigated by him are called now *Belousov algebras*.

A large cycle of Belousov's articles is connected with different types of functional equations on quasigroups, such as the functional equations of generalized associativity, distributivity, mediality and Moufang. Belousov had published a number of works devoted to study of n-ary quasigroups. Now these works form the foundation of the theory of n-ary quasigroups.

Quasigroups have many applications in discrete mathematics, especially in the theory of Latin squares. A similar connection between n-ary quasigroups and n-dimensional cubes holds. In connection with this fact V. D. Belousov studied the problem of extensions of quasigroups and systems of orthogonal binary and n-ary operations. He established the connection between orthogonal systems of operations and orthogonal systems of quasigroups (OSQ) and studied the parastrophy transformation of these OSQ.

The first description of minimal identities connected with the orthogonality of parastrophes of binary quasigroups is given too. Some interrelations between the orthogonality of quasigroups and closure operations in k-nets are proved.

All ideas mentioned above are now in elaboration by numerous Belousov's pupils and many other mathematicians. He was a supervisor about of 30 of Ph. D. thesis. Now these pupils work in many countries.

He was not only a famous scientist. He was a very good lecturer. As a Corresponding Member of the Academy of the Pedagogical Sciences of the USSR (section Mathematics) he was an organizer of the scientific life in Moldova.

As a person, V. D. Belousov was full of generosity and warmth. Contact with him was very pleasant. Belousov wrote epigrams, liked music, especially Moldavian folk music and music of V. A. Mozart. He had a large library of science (in many languages) and also a fiction literature.

Valentin Danilovich Belousov devoted his life to science, a life that will always be an example and inspiration to his followers.

Galina B. Belyavskaya
Wieslaw A. Dudek
Victor A. Shcherbacov

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 5–18
ISSN 1024–7696

Pairwise orthogonality of n-ary operations *

G. Belyavskaya

Abstract. The notions of hypercube and of the orthogonality of two hypercubes were arised in combinatorial analysis. In [11] a connection between n-dimensional hypercubes and algebraic n-ary operations was established. In this article we use an algebraic approach to the study of orthogonality of two hypercubes (pairwise orthogonality). We give a criterion of orthogonality of two finite k-invertible n-ary operations, which is used by the research of orthogonality and parastrophe-orthogonality of two n-ary T-quasigroups. Some examples are given and connection between admissibility and pairwise orthogonality of n-ary operations is established.

Mathematics subject classification: 20N05, 20N15.
Keywords and phrases: Hypercube, orthogonal hypercubes, n-ary operation, n-ary quasigroup, n-ary T-quasigroup, parastrophe, transversal, orthogonal n-ary operations .

1 Introduction

It is known that two binary operations A and B, given on a set Q, are called orthogonal if the system of equations $\{A(x,y) = a, B(x,y) = b\}$ has exactly one solution for any $a, b \in Q$ (see [1], where such operations are called compatible). Orthogonal binary operations, in particular, orthogonal quasigroups were considered in different works (see, for example, [1–7]).

In [6] H.B. Mann proved that if A, B, C are quasigroups, given on a set Q and satisfying the equality

$$C(x, B(x,y)) = A(x,y)$$

for all $x, y \in Q$, then the quasigroups A and B are orthogonal.

V.D. Belousov in [3, Lemma 2] gave the following criterion of orthogonality of two binary quasigroups. Let A, B be binary quasigroups on a set Q. Then A and B are orthogonal if and only if the operation $A \cdot B^{-1}$ is a quasigroup, where $(A \cdot B^{-1})(x,y) = A(x, B^{-1}(x,y))$ and B^{-1} is the right inverse quasigroup for B ($B^{-1}(x,z) = y$ if and only if $B(x,y) = z$).

In the case of n-ary operations there exist distinct versions of orthogonality (they are reflected in [11]) which correspond to different types of orthogonality of n-dimensional hypercubes.

*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).

In this article we consider the weakest (for $n > 2$) case of orthogonality of n-ary operations, namely, pairwise orthogonality (see Definition 1). At first orthogonality of two finite k-invertible n-ary operations (pairwise orthogonality) is considered. Then, using the obtained criterion of orthogonality of finite n-ary operations, we give a definition of pairwise orthogonality for arbitrary k-invertible n-operations, in particular, for finite or infinite n-quasigroups. A connection between admissibility and pairwise orthogonality of k-invertible n-ary operations is established. In the last part of the article pairwise orthogonality of n-ary T-quasigroups ($n-T$-quasigroups), in particular, $n-T$-quasigroups which are orthogonal to some their parastrophes are studied. Some examples of such quasigroups are given.

2 Necessary notions and results

We recall some notations, concepts and results which are used in the article. At first remember the following designations and notes from [10]. By x_i^j we will denote the sequence $x_i, x_{i+1}, \dots, x_j$, $i \le j$. If $j < i$, then x_i^j is the empty sequence, $\overline{1,n} = \{1, 2, \dots, n\}$. Let Q be a finite or an infinite set, $n \ge 1$ be a positive integer and let Q^n denote the Cartesian power of the set Q.

A n-ary operation A (briefly, an n-operation) on a set Q is a mapping $A : Q^n \to Q$ defined by $A(x_1^n) \to x_{n+1}$, and in this case we write $A(x_1^n) = x_{n+1}$.

A finite n-groupoid (Q, A) *of order m* is a set Q with one n-ary operation A defined on Q, where $|Q| = m$.

A *n-ary quasigroup* is an n-groupoid such that in the equality

$$A(x_1^n) = x_{n+1}$$

each of n elements from x_1^{n+1} uniquely defines the $(n+1)$-th element. Usually itself quasigroup n-operation A is considered as a n-quasigroup.

The n-operation E_i, $1 \le i \le n$, on Q with $E_i(x_1^n) = x_i$ is called *the i-th identity operation (or the i-th selector) of arity n.*

An n-operation A on Q is called *i-invertible* for some $i \in \overline{1,n}$ if the equation

$$A(a_1^{i-1}, x_i, a_{i+1}^n) = a_{n+1}$$

has a unique solution for each fixed n-tuple $(a_1^{i-1}, a_{i+1}^n, a_{n+1}) \in Q^n$.

For an i-invertible n-operation there exists *the i-inverse n-operation* ${}^{(i)}A$ defined in the following way:

$${}^{(i)}A(x_1^{i-1}, x_{n+1}, x_{i+1}^n) = x_i \Leftrightarrow A(x_1^n) = x_{n+1}$$

for all $x_1^{n+1} \in Q^{n+1}$.

It is evident that

$$A(x_1^{i-1}, {}^{(i)}A(x_1^n), x_{i+1}^n) = {}^{(i)}A(x_1^{i-1}, A(x_1^n), x_{i+1}^n) = x_i$$

and ${}^{(i)}[{}^{(i)}A] = A$ for $i \in \overline{1,n}$.

Let Ω_n be the set of all n-ary operations on a finite or an infinite set Q. On Ω_n define a binary operation $\underset{i}{\oplus}$ (the i-multiplication) in the following way:

$$(A \underset{i}{\oplus} B)(x_1^n) = A(x_1^{i-1}, B(x_1^n), x_{i+1}^n),$$

$A, B \in \Omega_n, x_1^n \in Q^n$. Shortly this equality can be written as

$$A \underset{i}{\oplus} B = A(E_1^{i-1}, B, E_{i+1}^n)$$

where E_i is the i-th selector.

In [9] it was proved that $(\Omega_n; \underset{i}{\oplus})$ is a semigroup with the identity E_i. If Λ_i is the set of all i-invertible n-operations from Ω_n for some $i \in \overline{1,n}$, then $(\Lambda_i; \underset{i}{\oplus})$ is a group. In this group E_i is the identity, the inverse element of A is the operation ${}^{(i)}A \in \Lambda_i$, since $A \underset{i}{\oplus} E_i = E_i \underset{i}{\oplus} A$, $A \underset{i}{\oplus} {}^{(i)}A = {}^{(i)}A \underset{i}{\oplus} A = E_i$.

A n-ary quasigroup (Q, A) (or simply A), is an n-groupoid with an i-invertible n-operation for each $i \in \overline{1,n}$ [10].

Let A be an n-quasigroup and $\sigma \in S_{n+1}$, then the n-quasigroup ${}^{\sigma}A$ defined by

$${}^{\sigma}A(x_{\sigma 1}^{\sigma n}) = x_{\sigma(n+1)} \Leftrightarrow A(x_1^n) = x_{n+1}$$

is called the σ-parastrophe (or simple, parastrophe) of A [10].

For any n-operation A there exist the σ-parastrophes ${}^{\sigma}A$, where $\sigma(n+1) = n+1$ (the principal parastrophes). The i-inverse operation ${}^{(i)}A$ for A, $i \in \overline{1,n}$, is the σ-parastrophe defined by the cycle $(i, n+1)$.

Let $(x_1^n)_k$ denote the $(n-1)$-tuple $(x_1^{k-1}, x_{k+1}^n) \in Q^{n-1}$ and let A be an n-operation, then the $(n-1)$-operation A_a:

$$A_a(x_1^n)_k = A(x_1^{k-1}, a, x_{k+1}^n)$$

is called *the* $(n-1)$-*retract* of A, defined by position k, $k \in \overline{1,n}$, with the element a in this position (with $x_k = a$) [10].

An n-ary operation A on Q is called *complete* if there exists a permutation $\overline{\varphi}$ on Q^n such that $A = E_1\overline{\varphi}$ (that is $A(x_1^n) = E_1\overline{\varphi}(x_1^n)$). If a complete n-operation A is finite and has order m, then the equation $A(x_1^n) = a$ has exactly m^{n-1} solutions for any $a \in Q$ [9].

Any i-invertible n-operation A, $i \in \overline{1,n}$, is complete, but there exist complete n-operations, which are not i-invertible for each $i \in \overline{1,n}$ [9].

3 Orthogonality of two n-ary operations

In the case of n-ary operations for $n > 2$ it is possible to consider different versions of orthogonality. The weakest is the notion of the pairwise orthogonality.

Definition 1 [11]. *Two n-ary operations ($n \geq 2$) A and B given on a set Q of order m are called orthogonal (shortly, $A \perp B$) if the system $\{A(x_1^n) = a, B(x_1^n) = b\}$ has exactly m^{n-2} solutions for any $a, b \in Q$.*

This concept corresponds to two orthogonal n-dimensional hypercubes [11, 13]. The following type of orthogonality is strongest.

Definition 2 [8]. *An n-tuple $< A_1, A_2, \ldots, A_n >$ of n-operations on a set Q is called orthogonal if the system $\{A_i(x_1^n) = a_i\}_{i=1}^n$ has a unique solution for any $a_1^n \in Q^n$. A set $\Sigma = \{A_1^t\}$, $t \geq n$, of n-operations is called orthogonal if any n-tuple of distinct n-operations from Σ is orthogonal.*

This concept corresponds to an orthogonal n-tuple of n-dimensional hypercubes [11–13]. Orthogonal n-operations and their sets in the sense of Definition 2 were considered in many articles (see, for example, [8, 11–17, 19, 20, 22]).

In [11] intermediate types of orthogonality of n-operations and their sets were studied.

Definition 3 [11]. *A k-tuple $< A_1^k >, 2 \leq k \leq n$, of distinct n-operations on a set Q of order m is called orthogonal if the system $\{A_i(x_1^n) = a_i\}_{i=1}^k$ has exactly m^{n-k} solutions for any $a_1^k \in Q^k$. A set $\Sigma = \{A_1^t\}$, $t \geq k$, of n-operations is called k-wise orthogonal if any k-tuple of distinct n-operations from Σ is orthogonal.*

The following connection exists between different considered types of orthogonality.

Theorem 1 [11]. *If a set $\Sigma = \{A_1^t\}$, $t \geq k$, of finite n-operations is k-wise orthogonal, then Σ is l-wise orthogonal for any l, $2 \leq l \leq k$.*

Thus, every pair of different n-ary operations from an orthogonal n-tuple is orthogonal.

Let $A_1, A_2, \ldots, A_n$ be n-operations given on a set Q. In [14] it is proved that a n-tuple $< A_1^n >$ of n-operations is orthogonal if and only if the mapping $\bar{\theta} : x_1^n \to (A_1(x_1^n), A_2(x_1^n), \ldots, A_n(x_1^n)) = (A_1, A_2, \ldots, A_n)(x_1^n)$ is a permutation on Q^n.

In [1] V.D. Belousov proved that a binary operation A has an operation which is orthogonal to A (an orthogonal mate) if and only if A is a complete operation. This is valid and for finite n-operations.

Proposition 1. *A finite n-operation A has an orthogonal mate if and only if A is complete.*

Proof. By Proposition 5 of [11] A is a complete n-operation if and only if it is a component of some permutation $\overline{\theta} = (A, B_1^{n-1})$ on Q^n, where $< A, B_1^{n-1} >$ is an orthogonal n-tuple. By Theorem 1 $A \perp B_i$ for any $i \in \overline{1, n-1}$.

Conversely, if B is an orthogonal mate for A , that is $A \perp B$, then by Corollary 4 of [11] the pair A, B can be embedded in an orthogonal n-tuple of n-operations and by Proposition 5 of [11] A is a complete n-operation. $\square$

Now we shall consider orthogonality of k-invertible n-operations for some fixed k, $1 \leq k \leq n$. For them the following criterion is valid.

Theorem 2. *Let k be a fixed number from $\overline{1,n}$. Two finite k-invertible n-operations A and B on a set Q are orthogonal if and only if the $(n-1)$-retract C_a of the n-operation $C = B \underset{k}{\oplus} {}^{(k)}A$, defined by $x_k = a$, is complete for every $a \in Q$.*

Proof. We shall prove this statement when $k = n$ for the sake of simplicity. For the rest $k \in \overline{1, n-1}$ the proof is similar.

Let a be an arbitrary element of Q, $|Q| = m$ and the $(n-1)$-retract C_a by $x_n = a$ of n-operation $C = B \underset{n}{\oplus} {}^{(n)}A$ is complete for any $a \in Q$. Then the equation

$$C_a(x_1^{n-1}) = C(x_1^{n-1}, a) = (B \underset{n}{\oplus} {}^{(n)}A)(x_1^{n-1}, a) = B(x_1^{n-1}, {}^{(n)}A(x_1^{n-1}, a)) = b$$

has $m^{(n-1)-1}$ solutions for any $a, b \in Q$. From the last equation we have ${}^{(n)}B(x_1^{n-1}, b) = {}^{(n)}A(x_1^{n-1}, a) = z$, whence it follows that the system $\{A(x_1^{n-1}, z) = a, B(x_1^{n-1}, z) = b\}$ has m^{n-2} solutions. Thus, $A \perp B$.

Conversely, let $A \perp B$, that is the system $\{A(x_1^n) = a, B(x_1^n) = b\}$ has m^{n-2} solutions for any $a, b \in Q$. From the first equality we have $x_n = {}^{(n)}A(x_1^{n-1}, a)$ and then the equation $B(x_1^{n-1}, {}^{(n)}A(x_1^{n-1}, a)) = b$ or $C_a(x_1^{n-1}) = (B \underset{n}{\oplus} {}^{(n)}A)(x_1^{n-1}, a) = b$ has m^{n-2} solutions for any $a, b \in Q$. Therefore, the $(n-1)$-retract of $B \underset{n}{\oplus} {}^{(n)}A$, defined by any $a \in Q$, is complete. $\square$

For the binary case from Theorem 2 we have the following

Corollary 1. *Two finite invertible from the right (that is 2-invertible) binary operations A, B on Q are orthogonal if and only if the operation $C(x, y) = (A \cdot B^{-1})(x, y) = A(x, B^{-1}(x, y))$ is a quasigroup.*

Proof. The operation $C = B \cdot A^{-1} (= B \underset{2}{\oplus} {}^{(2)}A)$ is always invertible from the right. If the operation $C_a x = C(x, a)$ is complete for any $a \in Q$, that is the equation $C(x, a) = b$ has exactly $m^{2-2} = 1$ solutions for any $a, b \in Q$, then the operation C is invertible from the left (that is 1-invertible). Thus, C is a quasigroup.

Conversely, if C is a quasigroup, then any its (unary) retract is complete (that is a permutation). $\square$

From this corollary the criterion of V.D.Belousov [3, Lemma 2] for finite binary quasigroups follows.

Proposition 2. *If A and B are k-invertible n-operations on a set Q for some $k \in \overline{1,n}$, then the following equalities are equivalent: $C = B \underset{k}{\oplus} {}^{(k)}A$, $C \underset{k}{\oplus} A = B$,*

$A = {}^{(k)}C \underset{k}{\oplus} B$, $C \underset{k}{\oplus} A \underset{k}{\oplus} {}^{(k)}B = E_k$, ${}^{(k)}A \underset{k}{\oplus} {}^{(k)}C \underset{k}{\oplus} B = E_k$, $A \underset{k}{\oplus} {}^{(k)}B \underset{k}{\oplus} C = E_k$, ${}^{(k)}C \underset{k}{\oplus} B \underset{k}{\oplus} {}^{(k)}A = E_k$.

Proof. It is easy to see taking into account that all k-invertible n-operations on Q form a group with the identity E_k with the respect to the k-multiplication of n-operations. □

Remark 1. If A and B are n-quasigroups, then they are k-invertible for any $k \in \overline{1,n}$, so $A \perp B$ if and only if for some $k \in \overline{1,n}$ the $(n-1)$-retract C_a of $C = B \underset{k}{\oplus} {}^{(k)}A$, defined by $x_k = a$, is complete for any $a \in Q$. If that holds for some fixed $k \in \overline{1,n}$, then the $(n-1)$-retract of $C_1 = B \underset{l}{\oplus} {}^{(l)}A$, defined by $x_l = a$, is also complete for any $l \in \overline{1,n}$ and any $a \in Q$.

From Proposition 2 and Theorem 2 we have the following

Corollary 2. *If A and B are finite n-quasigroups on Q, $C = B \underset{k}{\oplus} {}^{(k)}A$ and $A \perp B$, then $C \perp {}^{(k)}A$, ${}^{(k)}C \perp {}^{(k)}B$ for any $k \in \overline{1,n}$.*

Proof. $C \perp {}^{(k)}A$ $({}^{(k)}C \perp {}^{(k)}B)$ follows from the second (from the third) equality of Proposition 2 and Theorem 2, since A and B are n-quasigroups and so any $(n-1)$-retract of B (A) is an $(n-1)$-quasigroup which is always complete. Further use Remark 1. □

Using the criterion of orthogonality of two finite n-operations from Theorem 2 we can define a pairwise orthogonality of arbitrary k-invertible n-operations (finite or infinite).

Definition 4. *Two k-invertible n-operations A and B , given on an arbitrary set Q, are called orthogonal if the $(n-1)$-retract of the n-operation $B \underset{k}{\oplus} {}^{(k)}A$,defined by $x_k = a$, is complete for each $a \in Q$.*

As it was noted above, an n-operation A on Q is called complete if there exists a permutation (a bijection) $\overline{\varphi}$ on Q^n such that $A = E_1\overline{\varphi}$. In the case of Definition 4 each $(n-1)$-retract

$$C_a(x_1^n)_k = C(x_1^{k-1}, a, x_{k+1}^n) = B(x_1^{k-1}, {}^{(k)}A(x_1^{k-1}, a, x_{k+1}^n), x_{k+1}^n)$$

is complete, that is $C_a = E_1\overline{\psi}$ for some permutation $\overline{\psi}$ of Q^{n-1}.

Remark 2. Note that for binary case (n=2) Definition 4 is equivalent to the usual definition of orthogonality of two 1- or 2-invertible operations.

Indeed, let A, B be 2-invertible binary operations on a set Q and $A \perp B$, that is the system $\{A(x,y) = a, B(x,y) = b\}$ has a unique solution for any $a, b \in Q$. Then $A^{-1}(x,a) = y$ and the equation $B(x, A^{-1}(x,a)) = b$ has a unique solution x for any

$a, b \in Q$, that is $C_a(x) = B(x, R_a x) = E\varphi_a x = \varphi_a x$ where $R_a x = A^{-1}(x, a)$, E is the selector in the 1-ary case ($Ex = \varepsilon x = x$) and so φ_a is a bijection Q on Q. Thus, $C_a = \varphi_a$ is a complete 1-ary (unary) operation for any $a \in Q$.

Conversely, if $C_a = \varphi_a$ is a bijection for any $a \in Q$, then the equation $B(x, A^{-1}(x, a)) = b$ has a unique solution for any $a, b \in Q$ and the system $\{A(x, y) = a, B(x, y) = b\}$ has a unique solution.

For 1-invertible binary operations the proof is similar.

Now we consider a connection between orthogonality of two n-operations and their admissibility.

It is known that a binary quasigroup $(Q, \cdot)$ is called admissible if it has a complete permutation (a bijection) (or a transversal).

A permutation θ on Q is called *complete* for a quasigroup $(Q, \cdot)$ if the mapping θ': $\theta' x = x \cdot \theta x$ is a permutation on Q. All elements $\theta' x$, $x \in Q$, are different and form *a transversal* which is defined by the permutation θ [5].

A binary quasigroup of order m has an orthogonal mate if and only if it has m disjoint transversals $\theta'_1, \theta'_2, \ldots, \theta'_m$ (or m disjoint complete permutations $\theta_1, \theta_2, \ldots, \theta_m$), that is $\theta'_i x \neq \theta'_j x, i \neq j$, for any $x \in Q$ [5].

Using the criterion of Corollary 4 of orthogonality of binary 2-invertible (or 1-invertible) operations A and B on Q of order m, it is easy to find in this case m disjoint transversals.

Indeed, if $A \perp B$, then the operation $A \cdot B^{-1}$ $((A \cdot B^{-1})(x, y) = A(x, B^{-1}(x, y)))$ is a quasigroup. By $y = a$ we have $A(x, B^{-1}(x, a)) = A(x, R_a x) = C_a x$ and C_a is a permutation where $R_a : R_a x = B^{-1}(x, a)$ is also permutation. Thus, in A there exist m disjoint complete permutations $\{R_a, a \in Q\}$ which define m disjoint transversals $\{C_a, a \in Q\}$.

In [20, 22] the admissibility of n-quasigroups and their connection with orthogonality were considered. By analogue with n-quasigroups (see [21]) the following definition of admissible n-operations was given.

Definition 5. *An n-operation B given on a set Q is called admissible if for some k, $1 \leq k \leq n$, on Q there exists an $(n-1)$-operation A such that the $(n-1)$-operation C:*

$$C(x_1^n)_k = B(x_1^{k-1}, A(x_1^n)_k, x_{k+1}^n)$$

is complete. In this case the $(n-1)$-operation C is called a k-transversal of the n-operation B, defined by the $(n-1)$-operation A.

The n-tuples $(x_1^{k-1}, A(x_1^n)_k, x_{k+1}^n)$ are positions of elements of a k-transversal C. The values $C(x_1^n)_k$, when $(n-1)$-tuples $(x_1^n)_k$ run through Q^{n-1}, are the elements of the k-transversal C.

Two k-transversals of an n-operation B defined by $(n-1)$-operations A_1 and A_2 are called disjoint if $A_1(x_1^n)_k \neq A_2(x_1^n)_k$ for all $(x_1^n)_k \in Q^{n-1}$.

From Theorem 2 it follows

Proposition 3. *Let A, B be finite k-invertible n-operations given on a set Q of order m, $A \perp B$. Then the $(n-1)$-operations ${}^{(k)}A_a(x_1^n)_k = {}^{(k)}A(x_1^{k-1}, a, x_{k+1}^n)$, $a \in Q$, define m pairwise disjoint k-transversals in B.*

Proof. By Theorem 2 $A \perp B$ if and only if the $(n-1)$-operation

$$C_a(x_1^n)_k = B(x_1^{k-1}, {}^{(k)}A(x_1^{k-1}, a, x_{k+1}^n), x_{k+1}^n) = B(x_1^{k-1}, {}^{(k)}A_a(x_1^n)_k, x_{k+1}^n)$$

is complete for any $a \in Q$. Thus, by Definition 5 the operations ${}^{(k)}A_a$, $a \in Q$, define m transversals C_a, $a \in Q$. It is evident that ${}^{(k)}A_a(x_1^n)_k \neq {}^{(k)}A_b(x_1^n)_k$, if $a \neq b$, since A is a k-invertible n-operation. Moreover, in this case we have $C_a(x_1^n)_k \neq C_b(x_1^n)_k$ by virtue of k-invertibility of the n-operation B. $\square$

Let A, B be two n-operations on a set Q. Recall that an n-operation B is called isotopic to an n-operation A if there exists an $(n+1)$-tuple $T = (\alpha_1, \alpha_2, \ldots, \alpha_n, \gamma)$ of permutations (bijections) of Q such that $B(x_1^n) = \gamma^{-1}A(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n)$ for all $x_1^n \in Q^n$ (shortly, $B = A^T$)[10].

It is easy to prove that the following statement is valid.

Proposition 4. *Any n-operation B which is isotopic to a complete finite or infinite n-operation A is also complete.*

Proof. Let A be a complete n-operation on a set Q, $B = A^T$, $T = (\alpha_1, \alpha_2, \ldots, \alpha_n, \gamma)$, then $A = E_1\overline{\varphi}$ for some permutation $\overline{\varphi} = (C_1, C_2, \ldots, C_n)$ (where the n-tuple $< C_1, C_2, \ldots, C_n >$ of n-operations is orthogonal) and

$$B(x_1^n) = \gamma^{-1}A(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n) =$$

$$\gamma^{-1}E_1\overline{\varphi}(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n) = \gamma^{-1}E_1(C_1, C_2, \ldots, C_n)(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n) =$$

$$E_1(\gamma^{-1}\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_n)(x_1^n)$$

where $\overline{C}_i(x_1^n) = C_i(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n)$. It is easy to see that the n-tuple $< \gamma^{-1}\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_n >$ is also orthogonal. Thus, $B = E_1\overline{\psi}$, where

$$\overline{\psi} = (\gamma^{-1}\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_n). \qquad \square$$

From Proposition 1 and Proposition 3 we obtain the following

Corollary 3. *If a finite n-operation A has an orthogonal mate and $B = A^T, T = (\alpha_1, \alpha_2, \ldots, \alpha_n, \gamma)$, then B has an orthogonal mate too.*

4 Pairwise orthogonal n − T-quasigroups

Below we shall consider in more detail orthogonality of two n-ary T-quasigroups (briefly, $n-T$-quasigroups) which are closely connected with finite or infinite abelian groups and generalize the known binary T-quasigroups.

Definition 6 [18]. *An n-quasigroup (Q,A) is called an $n-T$-quasigroup if there exist a binary abelian group $(Q,+)$, its automorphisms $\alpha_1,\alpha_2,\dots,\alpha_n$ and an element $a\in Q$ such that*

$$A(x_1^n)=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n+a \tag{1}$$

for all $x_1^n\in Q^n$.

Let $k\in\overline{1,n}$, then the k-inverse n-operation ${}^{(k)}A$ for an $n-T$-quasigroup A of (1) has the form

$${}^{(k)}A(x_1^n)=\alpha_k^{-1}(-\alpha_1x_1-\alpha_2x_2-\cdots-\alpha_{k-1}x_{k-1}+x_k-\alpha_{k+1}x_{k+1}-\cdots-\alpha_nx_n-a) \tag{2}$$

and is also $n-T$-quasigroup, since the mapping $I: Ix=-x$ is an automorphism in an abelian group.

Proposition 5. *Let (Q,A) and (Q,B) be two finite $n-T$-quasigroups over a group $(Q,+)$ of odd order,*

$$A(x_1^n)=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_{k-1}x_{k-1}+x_k+\alpha_{k+1}x_{k+1}+\cdots+\alpha_nx_n,$$

$$B(x_1^n)=\beta_1x_1+\beta_2x_2+\cdots+\beta_{k-1}x_{k-1}+x_k+\beta_{k+1}x_{k+1}+\cdots+\beta_nx_n,$$

where $\beta_i=2\alpha_i$ for each $i\in\overline{1,n}$, $i\neq k$, then $C=B\underset{k}{\oplus}{}^{(k)}A=A$, $B=A\underset{k}{\oplus}A$ and $A\perp(A\underset{k}{\oplus}A)$, $A\perp^{(k)}A$, ${}^{(k)}(A\underset{k}{\oplus}A)\perp^{(k)}A$.

Proof. In this case $\beta_i=2\alpha_i$ is an automorphism for any $i\in\overline{1,n}$, $i\neq k$, since in a group $(Q,+)$ of odd order the mapping $x\to 2x$ is a permutation. Find the form of the n-operation C using (2): $C(x_1^n)=(B\underset{k}{\oplus}{}^{(k)}A)(x_1^n)=B(x_1^{k-1},{}^{(k)}A(x_1^n),x_{k+1}^n)=$ $2\alpha_1x_1+2\alpha_2x_2+\cdots+2\alpha_{k-1}x_{k-1}-\alpha_1x_1-\alpha_2x_2-\cdots-\alpha_{k-1}x_{k-1}+x_k-\alpha_{k+1}x_{k+1}-$ $\cdots-\alpha_nx_n+2\alpha_{k+1}x_{k+1}+\cdots+2\alpha_nx_n=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_{k-1}x_{k-1}+x_k+$ $\cdots+\alpha_{k+1}x_{k+1}+\cdots+\alpha_nx_n=A(x_1^n)$. Any $(n-1)$-retract of $C=A$ is a $(n-1)$-quasigroup, so is complete and $A\perp B$ by Definition 4 (or by Theorem 2). Since $C=B\underset{k}{\oplus}{}^{(k)}A=A$, then $B=A\underset{k}{\oplus}A$. Orthogonality of the rest n-operations pointed in the proposition follows from Corollary 2. □

The following useful criterion of orthogonality of two $n-T$-quasigroups is valid.

Theorem 3. *Two $n-T$-quasigroups (Q,A) and (Q,B) where*

$$A(x_1^n)=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n+a,B(x_1^n)=\beta_1x_1+\beta_2x_2+\cdots+\beta_nx_n+b$$

are orthogonal if and only if the $(n-1)$*-operation* $\overline{C}$*:*

$$\overline{C}(x_1^n)_k = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_{k-1}x_{k-1} + \gamma_{k+1}x_{k+1} + \cdots + \gamma_n x_n \tag{3}$$

is complete, where

$$\gamma_i x_i = \beta_i x_i - \beta_k \alpha_k^{-1}\alpha_i x_i = (\beta_i - \beta_k\alpha_k^{-1}\alpha_i)x_i, \quad i \in \overline{1,n}, i \neq k.$$

Proof. By Remark 1 and Definition 4 we need to prove that $\overline{C}$ is complete if and only if the $(n-1)$-retract C_c of $C = B \underset{k}{\oplus} {}^{(k)}A$ defined by $x_k = c$, for some $k \in \overline{1,n}$ and $c \in Q$, is complete. Using (2) we have $C(x_1^n) = (B \underset{k}{\oplus} {}^{(k)}A)(x_1^n) = B(x_1^{k-1}, {}^{(k)}A(x_1^n), x_{k+1}^n) = \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{k-1}x_{k-1} + \beta_k\alpha_k^{-1}(-\alpha_1 x_1 - \alpha_2 x_2 - \cdots - \alpha_{k-1}x_{k-1} + x_k - \alpha_{k+1}x_{k+1} - \cdots - \alpha_n x_n - a) + \beta_{k+1}x_{k+1} + \cdots + \beta_n x_n + b = (\beta_1 - \beta_k\alpha_k^{-1}\alpha_1)x_1 + (\beta_2 - \beta_k\alpha_k^{-1}\alpha_2)x_2 + \cdots + (\beta_{k-1} - \beta_k\alpha_k^{-1}\alpha_{k-1})x_{k-1} + \beta_k\alpha_k^{-1}x_k + (\beta_{k+1} - \beta_k\alpha_k^{-1}\alpha_{k+1})x_{k+1} + .. + (\beta_n - \beta_k\alpha_k^{-1}\alpha_n)x_n - \beta_k\alpha_k^{-1}a + b = \overline{C}(x_1^n)_k + \beta_k\alpha_k^{-1}x_k - \beta_k\alpha_k^{-1}a + b$ (see (3)).

Let $x_k = c$ be an arbitrary element of Q, then we have

$$C(x_1^{k-1}, c, x_{k+1}^n) = C_c(x_1^n)_k = \overline{C}(x_1^n)_k + d = R_d\overline{C}(x_1^n)_k,$$

where $d = \beta_k\alpha_k^{-1}c - \beta_k\alpha_k^{-1}a + b$, $R_d x = x + d$. Thus, the $(n-1)$-retract $C_c(x_1^n)_k$ of C, defined by $x_k = c$, is isotopic to the $(n-1)$-ary operation $\overline{C}$: $C_c = \overline{C}^T$, $T = (\varepsilon, \varepsilon, \ldots, \varepsilon, R_d^{-1})$ (ε denotes the identity permutation on Q) and by Proposition 4 C_c is complete if and only if $\overline{C}$ is complete. □

Remark 3. Note that if the conditions of Theorem 3 hold for some $k \in \overline{1,n}$, then they hold for any $k \in \overline{1,n}$ (see Remark 1 for n-quasigroups).

Corollary 4. *If in Theorem 3* $\gamma_{i_0} = \beta_{i_0} - \beta_k\alpha_k^{-1}\alpha_{i_0}$ *is a permutation for some* $i_0 \in \overline{1,n}$*,* $i_0 \neq k$*, then* $A \perp B$*.*

Proof. In this case the $(n-1)$-operation $\overline{C}$ of (3) is i_0-invertible, so it is complete. □

From Theorem 3 and Corollary 4 a number of useful statements follow.

Corollary 5. *Let in Theorem 3* $\alpha_k = \beta_k$ *for some* $k \in \overline{1,n}$*. Then*

(i) if $\beta_{i_0} - \alpha_{i_0}$ *is a permutation for some* $i_0 \in \overline{1,n}$*,* $i_0 \neq k$*, then* $A \perp B$*;*

(ii) if $(Q,+)$ *is an (abelian) group of odd order and* $\beta_{i_0} = 2\alpha_{i_0}$ *for some* $i_0 \in \overline{1,n}$*,* $i \neq k$*, then* $A \perp B$*.*

Proof. By $\alpha_k = \beta_k$ we have $\beta_k\alpha_k^{-1} = \varepsilon$ and $\gamma_i = \beta_i - \alpha_i$ for all $i \in \overline{1,n}$, $i \neq k$. In (i) use Corollary 4. Item (ii) is a particular case of (i), since $\beta_{i_0} = 2\alpha_{i_0}$ is a permutation (and so an automorphism) in a group of odd order. □

Corollary 6. *Let $\Sigma = \{A_1^t\}$ be a set of $n-T$-quasigroups on a set Q over the same group $(Q,+)$:*

$$A_i(x_1^n) = \alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n, i \in \overline{1,t}, \tag{4}$$

where $\alpha_{1k} = \alpha_{2k} = \cdots = \alpha_{tk}$ for some $k \in \overline{1,n}$. If for all $i,j \in \overline{1,t}$, $i \neq j$ there exists one number $s \in \overline{1,n}$, $s \neq k$ such that $\alpha_{is} - \alpha_{js}$ is a permutation, then the set Σ is pairwise orthogonal.

Proof. In this case $A_i \perp A_j$ for each $i,j \in \overline{1,t}$, $i \neq j$ by virtue of item (i) of Corollary 5 since $\alpha_{ik} = \alpha_{jk}$ for all $i,j \in \overline{1,t}$, $i \neq j$. □

Example 1. Let $\Sigma = \{A_1^{p-1}\}$ be a set of $n-T$-quasigroups over a group $(Q,+)$ (with the identity 0) of a prime order p, where $n-T$-quasigroups of (4) have the form

$$A_1(x_1^n) = a_1x_1 + a_{12}x_2 + \cdots + a_{1,n-1}x_{n-1} + ax_n,$$

$$A_2(x_1^n) = a_2x_1 + a_{22}x_2 + \cdots + a_{2,n-1}x_{n-1} + ax_n,$$

$$\cdots$$

$$A_{p-1}(x_1^n) = a_{p-1}x_1 + a_{p-1,2}x_2 + \cdots + a_{p-1,n-1}x_{n-1} + ax_n,$$

$\alpha_{i1}x = a_ix$, $a_i \neq a_j$, if $i \neq j$, $i,j \in \overline{1,p-1}$, $\alpha_{ik}x = a_{ik}x$, if $k \neq 1$ and $k \neq n$,$a_{in} = a$, $i \in \overline{1,p-1}$, $a, a_i, a_{ik} \in Q \setminus 0$ for all $i \in \overline{1,p-1}$.

By Corollary 6 the set Σ is pairwise orthogonal by $s = 1$ since $a_{i1} - a_{j1} = a_i - a_j \neq 0$, so the mapping $x \to (a_i - a_j)x$ is a permutation by $i \neq j$ and by $\alpha_{1n}x = \alpha_{2n}x = \cdots = \alpha_{p-1,n}x = ax$ (here $k = n$).

Further we shall establish some conditions for orthogonality of an $n-T$-quasigroup to some its parastrophes, using Theorem 3. Parastrophe-orthogonality of binary quasigroups and minimal identities connected with such orthogonality were in detail studied by V.D.Belousov in [4].

At first we recall that an automorphism α of a group $(Q,+)$ is called complete if the mapping $x \to x + \alpha x$ is a permutation of Q, that is if α is a complete permutation [5].

Proposition 6. *If an $n-T$-quasigroup (Q,A), $A(x_1^n) = \alpha_1x_1 + \alpha_2x_2 + \cdots + \alpha_nx_n + a$ where α_l is a complete automorphism of the group $(Q,+)$ for some $l \in \overline{1,n}$, then $A \perp {}^{(l)}A$.*

Proof. Using expression (2) for ${}^{(l)}A$ and taking in Theorem 3 $k \neq l$, $B = {}^{(l)}A$ we obtain $\beta_l = \alpha_l^{-1}$ and $\beta_k = -\alpha_l^{-1}\alpha_k$. Then $\gamma_l = \beta_l - \beta_k\alpha_k^{-1}\alpha_l = \alpha_l^{-1} + \alpha_l^{-1}\alpha_k\alpha_k^{-1}\alpha_l = \alpha_l^{-1}(\varepsilon + \alpha_l)$ is a permutation and so $A \perp {}^{(l)}A$ by Corollary 4. □

Corollary 7. *An $n-T$-quasigroup (Q,A) over a group $(Q,+)$ with $A(x_1^n) = \alpha x_1 + \alpha x_2 + \cdots + \alpha x_n + a$, where α is a complete automorphism of $(Q,+)$, is orthogonal to ${}^{(l)}A$ for each $l \in \overline{1,n}$. Moreover, if, in addition, $n \geq 3$, then the set $\Sigma = \{A, {}^{(1)}A, \ldots, {}^{(n)}A\}$ is pairwise orthogonal.*

Proof. The first statement follows immediately from Proposition 6. Prove that ${}^{(i)}A \perp {}^{(j)}A$ for each $i,j \in \overline{1,n}$, $i \neq j$. By (2) we have

$$^{(i)}A(x_1^n) = \alpha^{-1}(-\alpha x_1 - \alpha x_2 - \cdots - \alpha x_{i-1} + x_i - \alpha x_{i+1} - \cdots - \alpha x_n - a) =$$

$$-x_1 - x_2 - \cdots - x_{i-1} + \alpha^{-1} x_i - x_{i+1} - \cdots - x_n - \alpha^{-1} a =$$

$$Ix_1 + Ix_2 + \cdots + Ix_{i-1} + \alpha^{-1} x_i + Ix_{i+1} + \cdots + Ix_n + b =$$

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + b, b = -\alpha^{-1} a,$$

$$^{(j)}A(x_1^n) = Ix_1 + Ix_2 + \cdots + Ix_{j-1} + \alpha^{-1} x_j + Ix_{j+1} + \cdots + Ix_n + b =$$

$$\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + b.$$

Since $i \neq j$ and $n \geq 3$ then there exists $k \in \overline{1,n}$ such that $\alpha_k = \beta_k$ $(k \neq i,j)$. In this case we have $\alpha^{-1} x_j - (Ix_j) = (\alpha^{-1} + \varepsilon) x_j$, so the map $\beta_j - \alpha_j = \alpha^{-1} + \varepsilon$ is a permutation since α is a complete automorphism. By item (i) of Corollary 5 (if $i_0 = j$)) ${}^{(i)}A \perp {}^{(j)}A$. Taking into account that $A \perp {}^{(l)}A$ for any $l \in \overline{1,n}$, we obtain that Σ is a pairwise orthogonal set. □

From Corollary 7, in particular, it follows that if A is an $n-T$-quasigroup $(n \geq 3)$ (Q,A): $A(x_1^n) = x_1 + x_2 + \cdots + x_n + a$ over a group of odd order, then $\Sigma = \{A, {}^{(1)}A, \ldots, {}^{(n)}A\}$ is pairwise orthogonal set, since the identity automorphism ε in such group is complete.

A direct corollary of Theorem 3 for an $n-T$-quasigroup which is orthogonal to some its principal σ-parastrophe is the following

Proposition 7. *Let (Q,A) be an $n-T$-quasigroup over a group $(Q,+)$: $A(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a$, $\sigma(n+1) = n+1$. Then $A \perp {}^{\sigma}A$ if and only if for some $k \in \overline{1,n}$ the $(n-1)$-operation $\overline{C}$:*

$$\overline{C}(x_1^n)_k = (\alpha_{\sigma 1} - \alpha_{\sigma k}\alpha_k^{-1}\alpha_1)x_1 + (\alpha_{\sigma 2} - \alpha_{\sigma k}\alpha_k^{-1}\alpha_2)x_2 + \cdots + (\alpha_{\sigma(k-1)} - \alpha_{\sigma k}\alpha_k^{-1}\alpha_{k-1})x_{k-1} +$$

$$(\alpha_{\sigma(k+1)} - \alpha_{\sigma k}\alpha_k^{-1}\alpha_{k+1})x_{k+1} + \cdots + (\alpha_{\sigma n} - \alpha_{\sigma k}\alpha_k^{-1}\alpha_n)x_n$$

is complete.

Proof. By the definition of a principal parastrophe ${}^{\sigma}A$ $(\sigma(n+1) = n+1)$ of A

$$^{\sigma}A(x_1^n) = A(x_{\sigma^{-1}1}^{\sigma^{-1}n}) = \alpha_1 x_{\sigma^{-1}1} + \alpha_2 x_{\sigma^{-1}2} + \cdots + \alpha_n x_{\sigma^{-1}n} + a =$$

$$\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + a,$$

where $\beta_i x_i = \alpha_{\sigma i} x_i$, $i \in \overline{1,n}$. Further use Theorem 3 with $\gamma_i = \beta_i - \beta_k \alpha_k^{-1} \alpha_i = \alpha_{\sigma i} - \alpha_{\sigma k}\alpha_k^{-1}\alpha_i$. □

Corollary 8. *If (Q,A) is an $n-T$-quasigroup, $n \geq 3$, $A(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a$, $\sigma(n+1) = n+1$, $\sigma k = k$ for some $k \in \overline{1,n}$ and $\alpha_{\sigma i_0} - \alpha_{i_0}$ is a* *permutation for some* $i_0 \in \overline{1,n}$*,* $i_0 \neq k$*, then* $A \perp {}^{\sigma}A$*. If, in addition,* $(Q,+)$ *has odd order and* $\alpha_{\sigma i_0} = 2\alpha_{i_0}$ *, then* $A \perp {}^{\sigma}A$*.*

Proof. We have ${}^{\sigma}A(x_1^n) = \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{k-1}x_{k-1} + \alpha_k x_k + \beta_{k+1}x_{k+1} + \cdots + \beta_n x_n + a$, where $\beta_i = \alpha_{\sigma i}$, so $\beta_k = \alpha_k$, as $\sigma k = k$ and we can use items (i) and (ii) of Corollary 5, respectively. □

Note that for $n = 2$ we have $\sigma = \varepsilon$ (that is ${}^{\sigma}A = A$) by the conditions of this corollary (if $\sigma 3 = 3$, $\sigma 1 = 1$, then $\sigma = (1, \sigma 2, 3) \Rightarrow \sigma 2 = 2$).

Example 2. Let (Q, A) be an $n-T$-quasigroup, $n \geq 3$, over a group of odd order with $A(x_1^n) = \alpha_1 x_1 + 2\alpha_1 x_2 + \cdots + \alpha_n x_n + a$, $i_0 = 1$, $\sigma(n+1) = n+1, \sigma 1 = 2$ and $\sigma k = k$ for some $k \in \overline{1,n}$, $k \neq 1$. Then $\alpha_{\sigma 1} - \alpha_1 = \alpha_2 - \alpha_1 = 2\alpha_1 - \alpha_1 = \alpha_1$. By Corollary 8 $A \perp {}^{\sigma}A$ for any $\alpha_i \neq 0$, $i \in \overline{1,n}$, $i \neq 2$.

Corollary 9. *If* (Q, A) *is an* $n-T$*-quasigroup ,* $n \geq 3$*, over a group of a prime order,* $A(x_1^n) = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n + a$*,* $a_i \neq 0$*,* $a_i \neq a_j$*, if* $i \neq j$*,* $\sigma(n+1) = n+1$*,* $\sigma k = k$ *for some* $k \in \overline{1,n}$ *and* $\sigma i_0 \neq i_0$ *for some* $i_0 \neq k$*, then* $A \perp {}^{\sigma}A$*.*

Proof. In a group of a prime order all mappings $x \to ax$, where $a \neq 0$ are automorphisms. If $\sigma i_0 \neq i_0$, then the mapping $x \to (a_{\sigma i_0} - a_{i_0})x$ is a permutation (an automorphism), so by Corollary 8 $A \perp {}^{\sigma}A$. □

Example 3. Let $(Q,+) = (Z_p,+)$ be a group of a prime order $p \geq 7$, $Q = \{0, 1, 2, \ldots, p-1\}$, $A(x_1^5) = 3x_1 + 5x_2 + 4x_3 + 2x_4 + x_5$ and $\sigma = (2,3)$, then $\sigma 3 = 2 \neq 3$, $\sigma 4 = 4$ $(k = 4, i_0 = 3)$, ${}^{\sigma}A(x_1^5) = A(x_{\sigma^{-1}1}^{\sigma^{-1}5}) = 3x_1 + 5x_3 + 4x_2 + 2x_4 + x_5 = 3x_1 + 4x_2 + 5x_3 + 2x_4 + x_5$. By Corollary 9 $A \perp {}^{\sigma}A$.

References

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

[2] Belousov V.D. *Systems of quasigroups with generalized identities.* Uspehi mat. nauk, 1965, **XX**, N 1(121), p. 75–146 (in Russian).

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

[4] Belousov V.D. *Parastrophe-orthogonal quasigroups.* Preprint, Kishinev, Shtiintsa, 1983 (in Russian); see also Quasigroups and related systems, vol. 13,2005,25-72.

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

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

[7] Sade A. *Groupoides orthogonaux.* Publ. Math. Debrecen, 1958, **5**, p. 229–240.

[8] Belousov V.D., Yacubov T. *On orthogonal n-ary operations.* Combinatornaya matematica. Moscow, 1974, p. 3–17 (in Russian).

[9] Yacubov T. *On $(2, n)$-semigroup of n-ary operations.* Izvestiya AN MSSR., Ser. fiz.-teh. i mat. nauk, 1974, N 1, p. 29–46 (in Russian).

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

[11] Belyavskaya G., Mullen Gary L. *Orthogonal hypercubes and n-ary operations.* Quasigroups and related systems, vol. 13, 2005, 73-86.

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

[13] Laywine C.F., Mullen G.L., Whittle G. *D-Dimensional hypercubes and the Euler and MacNeish conjectures.* Monatsh. Math., 1995, **111**, p. 223–238.

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

[15] Evans T. *Latin cubes orthogonal to their transposes – a ternary analogue of Stein quasigroups.* Aequat. Math., 1973, **9**, N 2/3, p. 296–297.

[16] Evans T. *The construction of orthogonal k-skeins and Latin k-cubes.* Aequat. Math., 1976, **14**, N 3, p.485–491.

[17] Stojacović Z. *Medial cyclic n-quasigroups.* Novi Sad J. Math., 1998, **28**, N 1, p. 47-54.

[18] Syrbu P.N. *On congruences of n-ary T-quasigroups.* Quasigroups and related systems, 1999, **6**, p. 71–80.

[19] Syrbu P.N. *On orthogonality and self-orthogonality of n-ary operations.* Mat. Issled., vyp. 95. Kishinev, Shtiintsa, 1987, p. 121–130 (in Russian).

[20] Belyavskaya G., Murathudjaev S. *About admissibility of n-ary quasigroups.* Colloquia Mathematica Societatis Janos Bolyai. Combinatorics, Keszthely (Hungary), 1976, p. 101–119.

[21] Belyavskaya G., Murathudjaev S. *Admissibility and orthogonality of many-placed operations.* Abstracts of the Second Conf. of Math. Soc. of Republic of Moldova. Chishinau, 2004, p. 40–41.

[22] Murathudjaev S. *Admissible n-quasigroups.* Connection of admissibility with orthogonality. Mat. Issled., vyp. 83, Kishinev, Shtiintsa, 1985, p. 77–86 (in Russian).

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

Received November 9, 2005

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 δ (δ-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 δ-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 δ (δ-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 δ-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*

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

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

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. $\square$

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

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

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

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

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

$$A(A(x,z),x) = A(A(y,z),y) \Rightarrow x = y, \quad (8)$$

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

$$A(x, A(z,x)) = A(y, A(z,y)) \Rightarrow x = y, \quad (9)$$

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

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

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. $\square$

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. $\square$

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 $x \backslash z = x^{-1} z$, $z / x = z x^{-1}$, 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. $\square$

4 Some quasi-identities with one parameter

In different cases in a quasigroup $(Q, \cdot)$ quasi-identities (δ-quasi-identities) in which one permutation δ of Q presents, arise. For example, a quasigroup $(Q, \cdot)$ is called admissible if there exists a permutation δ (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 δ is complete if and only if in $(Q, \cdot)$ the δ-quasi-identity $x \cdot \delta x = y \cdot \delta y \Rightarrow x = y$ with the permutation δ 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 δ.

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 $a_1a_2 \ldots a_{n-1} \in Q^{n-1}$:

$$a_1a_2 \ldots a_{n-1} \to a_1a_2 \ldots a_{n-1}a_n$$

(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

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

where δ 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 δ 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*

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

hold;

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

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

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 δ and shall sometimes call them δ-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 $\delta = \varepsilon$ (ε is the identity permutation):

1) ε-quasi-identities (a_2) and (b_2) do not hold;

2) from ε-quasi-identity (d_2) ε-quasi-identity (c_2) follows;

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

4) in a finite Moufang loop (in a finite group) ε-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 ε-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)* $(Q, \cdot)$ ε*-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) ε-quasi-identities (a_2) and (b_2) can not hold. But in a quasigroup with the left identity these ε-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 ε-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 ε-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 δ-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 δ-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 δ-quasi-identities (a_1), (a_2), (b_1), (b_2), (c_1), (c_2), (d_1) and (d_2) with $\delta = (1342)$ (δ-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 δ-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 (γ_2) $((\sigma_1)$ or $(\sigma_2))$, then this quasigroup has orthogonal mate. This means that if in a finite quasigroup $(Q,\cdot)$ δ-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 δ-quasi-identity (c_2) $((d_1)$ or $(d_2))$.

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

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

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

(iii) *δ-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 δ-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 δ-quasi-identity (d_2). □

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

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

(iii) *δ-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 ε-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) ε-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 δ 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 δ-quasi-identity (c_1) holds, but then (c_2) also holds for any $z = Ia$ $(I : x \to x^{-1})$, since in a group δ-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 δ-quasi-identities from $(a_1) - (d_2)$ with distinct permutations δ. A part of such permutations can be obtained from the permutation δ of a δ-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 δ with the help of an automorphism was introduced.

Definition 1 [5]. *A permutation δ_1 is called automorphism equivalent to a permutation δ $(\delta_1 \sim \delta)$ for a quasigroup $(Q,\cdot)$ if there exists an automorphism α of $(Q,\cdot)$ such that $\delta_1 = \alpha\delta\alpha^{-1}$.*

Proposition 1 of [5] can be reformulated for δ-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 δ-quasi-identity (a_1) ((a_2), (b_1), (b_2), (c_1), (c_2), (d_1) or (d_2)) and a permutation δ_1 is an automorphism equivalent to δ, then in $(Q,\cdot)$ the respective δ_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 δ_1 of a set Q is called weakly equivalent to a permutation δ ($\delta_1 \overset{w}{\sim} \delta$) for a loop $(Q, \cdot)$ with the nucleus N if there exist an automorphism α ($\alpha \in \mathrm{Aut}(Q, \cdot)$) of the loop and elements $p, q \in N$ such that $\delta_1 = R_p\alpha\delta\alpha^{-1}L_q$, where $R_px = xp$, $L_qx = qx$*
(the permutations act to the left from the right).

Note that if δ 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 δ-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 δ-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 δ_1-quasi-identities also.*

c) *If, in addition, δ is an automorphism of $(Q, \cdot)$ and δ-quasi-identity (a_1) ((a_2), (b_1), (b_2), (c_1), (c_2), (d_1) or (d_2)) holds, then the corresponding δ_1-quasi-identity holds too.*

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

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

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

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 δ_0 (that is have the form $R_p \alpha \delta_0 \alpha^{-1} L_q$, where $\alpha \in \mathrm{Aut}(Q, \cdot)$, $p, q \in N$): (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

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 33–42
ISSN 1024–7696

On a small quasi-compactness

Laurenţiu Calmuţchi

Abstract. The notion of small quasi-compactness is introduced and studied. Let P be a small quasi-compactness. We prove that the classes of equivalence of P-compactifications of a given space X form a lattice with maximal and minimal elements. Some properties of maximal elements are studied.

Mathematics subject classification: 54D30, 54D40.
Keywords and phrases: Quasi-compactness, small quasi-compactness, lattice, compactifications.

1 Introduction

Compactness is one of the most important notions.

A quasi-compactness is a class of spaces which is multiplicative, hereditary with respect to closed subspaces and contains an infinite T_0-space.

A g-extension of a space X is a pair (Y, f), where Y is a T_0-space, $f : X \to Y$ is a continuous mapping and the set $f(X)$ is dense in Y. If f is an embedding of X into Y, then (Y, f) is an extension of the space X.

Denote by $E(X)$ the class of all extensions of a space X and by $GE(X)$ the class of all g-extensions of the space X. If $e_X(x) = x$ for every $x \in X$, then $(X, e_X) \in E(X)$. Thus $\Phi \neq E(X) \subseteq GE(X)$.

In the family $GE(X)$ there exists a binary relation $\leq$: $(Y_1, f_1) \leq (Y_2, f_2)$ if there exists a continuous mapping $\varphi : Y_2 \to Y_1$ such that $f_1 = \varphi \circ f_2$, i. e. $f_1(x) = \varphi(f_2(x))$ for each $x \in X$.

If $(Y_1, f_1) \leq (Y_2, f_2)$ and $(Y_2, f_2) \leq (Y_1, f_1)$ then we say that the g-extensions (Y_1, f_1) and (Y_2, f_2) are equivalent and we denote $(Y_1, f_1) \approx (Y_2, f_2)$.

We say that (Y,f) is a g-extension with a T_1-remainder if for every point $x \in Y \setminus f(X)$ the set $\{x\}$ is closed in Y.

1.1. Example. Let X be an infinite T_0-space, A and B be two non-empty sets, $Y_1 = X \cup A$, $Y_2 = X \cup B$, $f_1(x) = f_2(x) = x$ for every $x \in X$, X is an open subspace of Y_1 and Y_2, the neighborhoods of the point $x \in A$ are of the form $Y_1 \setminus (F \cup \Phi)$, where F is a closed compact subset of X and Φ is a finite subset of A, the neighborhoods of the points $x \in B$ are of the form $Y_2 \setminus (F \cup \Phi)$, where F is a closed compact subset of X and Φ is a finite subset of B. The pairs (Y_1, f_1) and (Y_2, f_2) are equivalent compactifications of the space X. Let (Y, f) be a g-compactification of the space X with a T_1-remainder and $Y \setminus f(X) \neq \emptyset$. Fix a non-empty set A. We put $Z = Y \cup A$. Consider some mapping $\varphi : A \to Y \setminus f(X)$. On Z we consider the topology with the base $\{U \subseteq Y : U$ is open in $Y\} \cup \{\varphi^{-1}(U) \backslash F) \cup (U \backslash \Phi) : U$ is an open subset of Y, F is a finite subset of A and Φ is a finite subset of $Y \backslash f(X)\}$. Then (Z, f) is a g-compactification of the space X with a T_1-remainder and the g-compactifications (Y, f) and (Z, f) are equivalent. Thus the class of equivalence of some g-compactification of X is not a set.

For every g-extension (Y, f) of a space X by $e(Y, f, X)$ we denote the class of all g-extensions of X equivalent to the g-extension (Y, f) .

1.2. Definition. *A class L of g-extensions of a space X is a lattice of g-extensions if the following conditions are fulfilled:*

– *there exists a set $e(L) \subseteq L$ such that $L \subseteq \cup\{e(Y, f, X) : (Y, f) \in e(L)\}$;*

– *there exists a g-extension $(m_L X, m_L) \in L$ such that $(m_L X, m_L) \leq (Y, f)$ for every $(Y, f) \in L$;*

– *for every non-empty set $A \subseteq L$ there exists a g-extension $(Z, g) \in L$ such that $(Z, g) = \vee A$ and $(Y, f) \leq (Z, g)$ for every $(Y, f) \in L$.*

If L is a lattice of g-extensions of a space X, then by $(\beta_L X, \beta_L)$ we denote some maximal element of the class L.

1.3. Example. M. Hušec [6, 7] constructed an infinite non-compact T_1- space X such that the class of all $T_1 - g$-compactifications of X is not a lattice.

Let P be a quasi-compactness.

A g-extension (Y, f) of a space X is called a $g - P$-extension of X if $Y \in P$. Let $PGE(X) = \{(Y, f) \in GE(X) : Y \in P\}$ be the class of all $g - P$-extensions and $PE(X) = E(X) \cap PGE(X)$ be the class of all P-extensions of the space X.

If $PGE(X)$ is a lattice of g-extensions of the space X, then $(\beta_P X, \beta_P)$ is one of the maximal elements of the class $PGE(X)$.

First General Problem. To find the methods of construction and of study of the P-extensions and of special P-extensions of a given space X.

Second General Problem. Under which conditions the class $PGE(X)$ is a lattice?

Third General Problem. Let P be a compactness and K be a class of spaces. Under which conditions there exists a set valued functor $F : K \to P$ such that:

– $F(X)$ is a non-empty lattice of $g - P$-extensions of the space X for every space X;

– $F(X) \cap PE(X) \neq \emptyset$ for every $X \in K_B$ and the maximal element $(\beta_F X, \beta_F)$ of the lattice $F(X)$ is an extension of X;

– for every closed continuous mapping $f : X \to Y$ of a space $X \in K$ onto a space $Y \in K$ there exists a continuous extension $g = \beta f : \beta_F X \to \beta_F Y$ such that $f = g|X$?

The functor F with these properties is called a functor of the Wallman type.

Fourth General Problem. Let P be a compactness and K be a class of spaces. Under which conditions there exists a set-valued functor $F : K \to P$ such that:

– $F(X) \cap PE(X) \neq \emptyset$ and $F(X)$ is a lattice of $g - P$-extensions of the space X for every space $X \in K$;

– for every continuous mapping $f : X \to Y$ of a space $X \in K$ into a space $Y \in K$ there exists a continuous extension $g = \beta f : \beta_F X \to \beta_F Y$ of the mapping f onto the maximal extensions?

A functor with these properties is called a functor of the Stone-Čech type. Every functor of the Stone-Čech type is a functor of the Wallman type.

1.4. Example. If P is a compactness, i.e. P is a quasi-compactness and every space $X \in P$ is a Hausdorff space, then for every space X the class $PGE(X)$ is a set.

If $K = \{X : E(X) \cap PGE(X) \neq \emptyset\}$, then $F : K \to PGE(X)$, where $F(X) = PG(X)$, is a functor of the Stone-Čech type.

1.5. Example. Let K be the class of all T_0-spaces, ωX be the Wallman extension of the T_0-space X (see [1]). A g-compactification (Y, f) of a space X is called a regular g-compactification of X if $\{cl_Y A : A \subseteq f(X)\}$ is a closed base of Y and there exists a continuous mapping $g : \omega X \to Y$ such that $g(x) = f(x)$ for every $x \in X$. If the mapping g is closed, then the g-compactification (Y, f) is called a $g - \omega\alpha$-compactification of X (see [9]). Let $F(X) = \{(Y, f) : (Y, f)$ is a regular g-compactification of X $\}$ and $\Phi(X) = \{(Y, f) : (Y, f)$ is a $g - \omega\alpha$-compactification of X $\}$. Then F and Φ are functors of the Wallman type.

1.6. Example. Let K be the class of all T_0-spaces and $PGE(X)$ be the set of all spectral g-compactifications of the T_0-space X. Then the correspondence $X \to PGE(X)$ is a functor of the Stone-Čech type (see [1]).

1.7. Example. Let K be the class of all completely regular spaces and $PGE(X)$ be the set of all Hausdorff g-compactifications of the space X. Then the correspondence $X \to PGE(X)$ is a functor of the Stone-Čech type.

The purpose of the present paper is to investigate the class of P-extensions of topological spaces.

In this article we shall use the following notations:

– we denote by $cl_X A$ or clA the closure of a set A in a space X;
– we denote by $|A|$ the cardinality of a set A;
– we denote by $w(X)$ the weight of a space X.
– R is the space of reals, $N = \{1, 2, ...\}$, $\quad I = [0, 1]$;
– every space is considered to be a T_0-space.

We use the terminology from [3, 1].

2 Small quasi-compactness

Let K be a class of T_0-spaces and $2 \leq |X|$ for some $X \in K$. Then there exists a minimal quasi-compactness $P(K)$ such that $K \subseteq P(K)$. We put $KGE(X) = P(K)GE(X)$ for every non-empty T_0-space X.

2.1. Definition. *A quasi-compactness P is called a small quasi-compactness if there exists a set K of spaces such that $P = P(K)$.*

2.2. Proposition. *Let P be a small quasi-compactness and for every space $X \in P$ there exists a point $b_X \in X$ such that the set $\{a_X\}$is closed in X. Then $P = P(\{E\})$ for some space $E \in P$.*

Proof. There exists a non-empty set $K \subseteq P$ of spaces such that $P = P(K)$. Suppose that $K = \{X_\alpha : \alpha \in A\}$. For every $\alpha \in A$ there exists a point $b_\alpha \in X_\alpha$ such that the set $\{b_\alpha\}$ is closed in X_α. We put $E = \Pi\{X_\alpha : \alpha \in A\}$ and $E_\beta = \{(x_\alpha : \alpha \in A) \in E : x_\alpha = b_\alpha$ for every $\alpha \in A\backslash\{\beta\}$ and $x_\beta \in X_\beta\}$. Then E_β is a closed subspace of the space E. For every $\beta \in A$ the spaces E_α and X_α are homeomorphic. Thus $P(K) = P(\{E\})$.

2.3. Lemma. *Let F be a non-empty compact subset of T_0-space X. Then there exists a point $b \in F$ such that the set $\{b\}$ is closed in X.*

Proof. Let ξ be a maximal family of closed subsets of the space X such that:

1. $\emptyset \notin \xi$ and $H \subseteq F$ for every $H \in \xi$;
2. If $H, M \in \xi$, then $H \cap M \in \xi$.

We put $\Phi = \cap\xi$. The set Φ is non-empty and closed in X. There exists a unique point $b \in F$ such that $\Phi = \{b\}$. Really, if $x_1, x_2 \in \Phi$ and $x_1 \neq x_2$, then there exists an open subset U of X such that $U \cap \{x_1, x_2\}$ is a singleton set. Then $\Phi\backslash U \in \xi$ and $\{x_1, x_2\}\backslash\Phi \neq \emptyset$, a contradiction. The proof is complete.

2.4. Corollary. *Let P be a small quasi-compactness and every space $X \in P$ be a compact T_0-space. Then $P = (\{E\})$ for some space $E \in P$.*

Fix a quasi-compactness P and a non-empty space X. For every $Y \in P$ denote by $C(X,Y)$ the set of all continuous mappings of the space X into the space Y. Let $\Phi = \{f_\alpha : X \to Y_\alpha : \alpha \in A\} \subseteq \cup\{C(X,Y) : Y \in P\}$ be a set of mappings. We put $f_\Phi(x) = \{f_\alpha(x) : \alpha \in A\} \in \Pi\{Y_\alpha : \alpha \in A\}$ for every $x \in X$. Denote by $e_\Phi X$ the closure of the set $f_\Phi(X)$ in the space $\Pi\,\{Y_\alpha : \alpha \in A\}$. Then $(e_\Phi X, f_\Phi) \in PGE(X)$.

2.5. Theorem. *Let K be a class of T_0-spaces and $P = P(K)$. For every T_0-space X and every $g - P$-extension $(Y, f) \in PGE(X)$ there exists a set $\Phi = \{f_\alpha : X \to Y_\alpha : \alpha \in A\} \subseteq \cup\{C(X,Z) : Z \in K\}$ such that the $g - P$-extensions (Y, f) and $(e_\Phi X, f_\Phi)$ are equivalent. Moreover, $f_\alpha \neq f_\beta$ for every $\alpha, \beta \in A$ and $\alpha \neq \beta$.*

Proof. There exists a set $\{E_\beta : \beta \in B\} \subseteq K$ such that Y is homeomorphic to a closed subset of the space $E = \Pi\{E_\beta : \beta \in B\}$. We assume that Y is a closed subspace of the space E. Let $p_\beta : E \to E_\beta$ be the continuous projections of E onto $E_\beta : p_\beta((x_\mu : \mu \in B)) = x_\beta$ for every point $(x_\mu \in E_\mu : \mu \in B) \in E$. For every $\beta \in B$ we put $g_\beta = p_\beta \circ f$. Then $g_\beta : X \to E_\beta$ is a continuous mapping. There exists a minimal set of mappings $\Phi = \{f_\alpha : X \to Y_\alpha : \alpha \in A\}$ such that:

1. For every $\alpha \in A$ there exists a $\beta \in B$ such that $f_\alpha = g_\beta$.
2. For every $\beta \in B$ there exists a unique $\alpha = i(\beta) \in A$ such that $f_\alpha = g_\beta$.

Thus there exists a mapping $i : B \to A$ of B onto A such that $f_\alpha = g_\beta$ for all $\alpha \in A$ and $\beta \in i^{-1}(\alpha)$. If $\alpha, \lambda \in A$ and $\alpha \neq \lambda$, then $f_\alpha \neq f_\lambda$.

We put $B_\alpha = i^{-1}(\alpha)$ for each $\alpha \in A$. By construction, $E_\beta = E_\mu$ for all $\alpha \in A$ and $\beta, \mu \in B_\alpha$. We may consider that $E_\beta = X_\alpha$ for all $\alpha \in A$ and $\beta \in B_\alpha$. For every $\beta \in B_\alpha$ we consider the mapping $\delta_{\alpha\beta} : X_\alpha \to E_\beta$ such that $\delta_{\alpha\beta}(x) = x$ for every $x \in X_\alpha$. We put $\delta_\alpha(x) = (\delta_{\alpha\beta}(x) : \beta \in B_\alpha) \in \Pi\{E_\beta : \beta \in B_\alpha\}$ for every $\alpha \in A$ and every $x \in X_\alpha$. Then $\delta_\alpha : X_\alpha \to \Pi\{E_\beta : \beta \in B_\alpha\}$ is an embedding. The set $\Delta_\alpha(X_\alpha) = \delta_\alpha(X_\alpha)$ is the diagonal of the space X_α in $\Pi\{E_\beta : \beta \in B_\alpha\}$. Fix $\beta(\alpha) \in B_\alpha$. Let $h_\alpha : \Pi\{E_\beta : \beta \in B_\alpha\} \to X_\alpha$ be the projection $h_\alpha(x_\beta : \beta \in B_\alpha) = x_{\beta(\alpha)}$ for every point $(x_\beta : \beta \in B_\alpha) \in \Pi\{E_\beta : \beta \in B_\alpha\}$.

Now we consider the continuous mapping $h : \Pi\{E_\beta : \beta \in B\} = \Pi\{\Pi\{E_\beta : \beta \in B_\alpha\} : \alpha \in A\} \to \Pi\{X_\alpha : \alpha \in A\}$, where $h(x_\beta : \beta \in B) = (h_\alpha(x_\beta : \beta \in B_\alpha) : \alpha \in A)$ for every point $(x_\beta : \beta \in B) \in \Pi\{E_\beta : \beta \in B\}$. The mapping $\delta : \Pi\{X_\alpha : \alpha \in A\} \to \Pi\{\Delta_\alpha(X_\alpha) : \alpha \in A\}$, where $\delta(x_\alpha : \alpha \in A) = (\delta_\alpha(x_\alpha) : \alpha \in A)$ for every $(x_\alpha : \alpha \in A) \in \Pi\{X_\alpha : \alpha \in A\}$, is a homeomorphism of the space $\Pi\{X_\alpha : \alpha \in A\}$ onto the subspace $\Pi\{\Delta_\alpha(X_\alpha) : \alpha \in A\}$ of the space $\Pi\{E_\beta : \beta \in B\}$.

Let $f_\Phi(x) = (f_\alpha(x) : \alpha \in A)$ for every $x \in X$ and $e_\Phi X$ be the closure of the subspace $f_\Phi(X)$ in $\Pi\{X_\alpha : \alpha \in A\}$. Let $\varphi = \delta | e_\Phi X : e_\Phi X \to \Pi\{E_\beta : \beta \in B\}$. Then $\varphi(f_\Phi(x)) = (g_\beta(x) : \beta \in B) = f(x)$ for every $x \in X$. Thus $(Y, f) \leq (e_\Phi X, f_\Phi)$. Let $\Psi = h\,|\,Y$. Then $\Psi(f(x)) = f_\Phi(x)$ for every $x \in X$. Thus $(e_\Phi X, f_\Phi) \leq (Y, f)$. The proof is complete.

2.6. Remark. *By construction, $\varphi : e_\Phi X \to Y$ is an embedding and $\Psi : Y \to e_\Phi X$ is a retract, i.e. $\varphi(\Psi(y)) = y$ for every $y \in \varphi(e_\Phi X)$.*

2.7. Theorem. *Let $\Phi = \{f_\alpha : X \to Y_\alpha : \alpha \in A\} \subseteq \cup\{C(X,Y) : Y \in P\}$ and $G = \{g_\beta : X \to Z_\beta : \beta \in B\} \subseteq \cup\{C(X,Y) : Y \in P\}$ be two sets of mappings, $A \subseteq B$ and $Y_\alpha = Z_\alpha$, $\quad f_\alpha = g_\alpha$ for each $\alpha \in A$. Then $(e_\Phi X, f_\Phi) \leq (e_G X, f_G)$.*

Proof. Consider the projection $p : \Pi\{Z_\beta : \beta \in B\} \to \Pi\{Y_\alpha : \alpha \in A\} = \Pi\{Z_\alpha : \alpha \in A\}$, where $p(z_\beta : \beta \in B) = (z_\beta : \beta \in A)$. Then $p(f_G(x)) = f_\Phi(x)$ for every $x \in X$. Thus $p(e_G X) \subseteq e_\Phi X$ and $(e_\Phi X, f_\Phi) \leq (e_G X, f_G)$. The proof is complete.

2.8. Corollary. *Let A be a set, $\Phi_\alpha = \{g_\beta : X \to Z_\beta : \beta \in B_\alpha\} \subseteq \cup\{C(X,Y) : Y \in P\}$ be a set of continuous mappings for every $\alpha \in A$, $\quad B = \cup\{B_\alpha : \alpha \in A\}$ and $\Phi = \{g_\beta : X \to Z_\beta : \beta \in B\}$. Then $(e_\Phi X, f_\Phi) = \vee\{(e_{\Phi_\alpha} X, f_{\Phi_\alpha}) : \alpha \in A\}$.*

2.9. Corollary. *Let P be a small quasi-compactness. Then there exists a set $K \subseteq P$ of spaces such that:*

1. For every $(Y, f) \in PGE(X)$ there exist a set $\Phi \subseteq \cup\{C(X,Y) : Y \in K\}$, an embedding $\varphi : e_\Phi X \to Y$ and a retraction $\Psi : Y \to e_\Phi X$ such that $\varphi(\Psi(y)) = y$ for every $y \in \varphi(e_\Phi X)$ and $(Y, f) \sim (e_\Phi X, f_\Phi)$.

2. The class $PGE(X)$ is a lattice provided $PE(X) \neq \emptyset$.

3. For every space X there exists a maximal element $(\beta_p X, \beta_p)$, where $(\beta_p X, \beta_p) = (e_\Phi X, f_\Phi)$ for $\Phi = \cup\{C(X,Y) : Y \in K\}$.

2.10. Definition. *A quasi-compactness P is called a virtual small quasi-compactness if for every space X the class $PGE(X)$ is a lattice.*

Every small quasi-compactness is a virtual small quasi-compactness

2.11. Corollary. *Let P be a virtual small quasi-compactness. Then:*

1. For every space X there exists some maximal element $(\beta_P X, \beta_P)$ in $PGE(X)$.

2. For every continuous mapping $f : X \to Y$ there exists a continuous mapping $\beta f : \beta_P X \to \beta_P Y$ such that $\beta f(\beta_P(x)) = \beta_P(f(x))$ for every $x \in X$.

3. For every continuous mapping $f : X \to Y$ into a space there exists a continuous mapping $\beta f : \beta_P X \to Y$ such that $\beta f(\beta_P(x)) \to f(x)$ for every $x \in X$.

2.12. Remark. *If $Y \in P$ and $i_\varphi : Y \to Y$ is the identical mapping, then $(Y, i_\varphi) = (\beta_P Y, \beta_P)$ is one of the maximal elements from $PGE(X)$ and $PE(X) \neq \emptyset$.*

3 On E-compact spaces

Let E be a space and $|E| \geq 2$. Consider the small compactness $P = P(E) = P(\{E\})$. We put $EGE(X) = P(E)GE(X)$ and $EE(X) = P(E)E(X)$. If $(Y, f) \in EGE(X)$, then (Y, f) is called a $g - E$-compactification of the space X. If $(Y, f) \in EE(X)$, then (Y, f) or Y is called a E-compactification of the space.

The notion of E-compactification was introduced by S. Mrovka [7,4]. From Theorems 2.5, 2.7, 2.10 and Corollary 2.9 follow the next assertions.

3.1. Corollary. *For every space X the class $EGE(X)$ is a lattice with the maximal element $(\beta_E X, \beta_E) = (e_{C(X,E)} X, f_{C(X,E)})$.*

3.2. Corollary. *For every $(Y, f) \in EGE(X)$ there exists a set $\Phi \subseteq C(X, E)$ such that:*

1. $(e_\Phi X, f_\Phi) \approx (Y, f)$.

2. There exist a continuous mapping $\varphi : Y \to e_\Phi X$ and an embedding $\Psi : e_\Phi X \to Y$ such that $\Psi(f_\Phi(x)) = \varphi(f(x))$ and $\varphi(\Psi(y)) = y$ for all $x \in X$ and $y \in e_\Phi X$.

3.3. Corollary. *For every continuous mapping $\varphi : X \to Y$ there exists a continuous mapping $\beta\varphi : \beta_E X \to \beta_E Y$ such that the diagram*

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ {\scriptstyle \beta_E}\downarrow & & \downarrow{\scriptstyle \beta_E} \\ \beta_E X & \xrightarrow{\beta_\varphi} & \beta_E Y \end{array}$$

is commutative.

3.4. Corollary. *If Ind X=0, then $EE(X) \neq \emptyset$ and $(\beta_E X, \beta_E) \in EE(X)$.*

3.5. Corollary. *If E is a T_1-space, then there exists a regular space X such that $EE(X) = \emptyset$.*

3.6. Corollary. *If E is a T_0-space and E is not a T_1-space, then $EE(X) \neq \emptyset$ and $(\beta_E X, \beta_E) \subseteq EE(X)$ for every T_0-space X.*

4 Examples

4.1. Example. Let $F = \{0, 1\}$ with the topology $\{\emptyset, \{0\}, \{0, 1\}\}$. Then F is a T_0-space and F is not a T_1-space. In this case $FE(X) \neq \emptyset$ for every T_0-space X. The class $FE(X)$ is not a set and the class $FGE(X)$ is a lattice.The assertions of the preceding section are true for $FGE(X)$.

The space F^m is called the Alexandroff cube (see [3]).

Denote by (maX, m_X) the maximal element of the lattice $FGE(X)$ of a space X. We may suppose that $maX = e_{C(X,F)}X$. We identify $x \in X$ and $m_X(x) \in maX$. In this case X is a dense subspace of the T_0-compact space maX. If $\varphi : X \to Y$ is a continuous mapping, then there exists a continuous mapping $m\varphi : maX \to maY$ such that $\varphi = m\varphi|X$.

4.2. Example. Let D=$\{0, 1\}$ with the discrete topology $\{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. In this case:

– $EGE(X)$ is a set for every space X;
– $EGE(X)$ is a lattice for every space X;
– $EE(X) \neq \emptyset$ if and only if ind X=0.

4.3. Example. Let $I = [0, 1]$ be a subspace of reals. In this case:

– $EGE(X)$ is a set for every space X;
– $EGE(X)$ is a lattice for every space X;
– $EE(X) \neq \emptyset$ if and only if X is a completely regular space;
– for every completely regular space the compactification $\beta_E \in X$ is the Stone-Čech compactification βE of the space X.

4.4. Example. Let τ be an infinite cardinal and E be a space of cardinality τ with the topology $\{\emptyset, E\} \cup \{E \backslash F : F \text{ is a finite subset}\}$. The space E is a compact T_1-space and E is not a Hausdorff space. In this case:

– $EGE(X)$ is not a set for some T_1-space;
– $EGE(X)$ is a lattice for every space X;
– If X is a T_1-space and $|X| \leq \tau$, then $EE(X) \neq \emptyset$;
– If $c \leq \tau$, then $EE(X) \neq \emptyset$ for every completely regular space X.

4.5. Example. A class P of topological T_0-spaces is called a double compactness if the following conditions are fulfilled:

1. There exists a space $X \in D$ such that $|X| \geq 2$.

2. If Γ is the topology of the space $X \in P$, then there is determined the Hausdorff topology $d\Gamma$ on X such that $(X, d\Gamma) \in P$, $\quad \Gamma \subseteq d\Gamma$ and $dd\Gamma = d\Gamma$. We say that $d\Gamma$ is the strong topology and Γ is the weak topology on X.

3. If $\{(X_\alpha, \Gamma_\alpha) \in P : \alpha \in A\}$ is a non-empty set of spaces, $X = \Pi\{X_\alpha : \alpha \in A\}$, Γ is the product of topologies Γ_α on X and Γ' is the product of topologies $d\Gamma_\alpha$ on X, then $\Gamma' \subseteq d\Gamma$.

4. If $(X, \quad \Gamma) \in P$, $Y \subseteq X$ and Y is a closed subset of the space $(X, d\Gamma)$, then $(Y, \Gamma) \in P$ and $d\Gamma|Y \subseteq d(\Gamma|Y)$, where $\Gamma|Y = \{U \cap Y : U \in \Gamma\}$ for the topology Γ on X.

Every double compactness is a quasi-compactness.

Let P be a double compactness. Then $PGE(X)$ is a set for every space X. Moreover, for every non-empty subset $L \subseteq PGE(X)$ there exists the supremum $\vee L \in PGE(X)$. In particular, there exists the maximal element $(\beta_p X, \beta_P)$.

A mapping $f : X \to Y$ of a space $(X, \Gamma) \in P$ into a space $(Y, \Gamma') \in P$ is double continuous if $f^{-1}\Gamma' \subseteq \Gamma$ and $f^{-1}d\Gamma' \subseteq d\Gamma$. For every continuous mapping $f : X \to Y$ of a space X into a space $Y \in P$ there exists a unique double continuous mapping $\beta f : \beta_p X \to P$ such that $f(x) = \beta f(\beta_P(x))$ for every point $x \in X$. In particular, for every continuous mapping $f : X \to Y$ there exists a unique double continuous mapping $\beta f : \beta_p X \to \beta_p Y$ such that $\beta_p(f(x)) = \beta f(\beta_P(x))$ for every $x \in X$.

4.6. Example. Let K be a class of triples $(X,\, T_X, T'_X)$, where X is a non-empty set, T_X and T'_X are topologies on X, $T_X \subseteq T'_X$ and T'_X is a Hausdorff topology. Then there exists a minimal double compactness P such that $(X,\, T_X) \in P$ and $T'_X = dT_X$ for every triple $(X,\, T_X, T'_X) \in K$. We say that the double compactness is generated by the class K. If P' is the quasi-compactness generated by the class $\{(X,\, T_X), (X, T'_X) : (X,\, T_X, T'_X) \in K\}$, then $P' \subseteq P$.

4.7. Example. Let $X_0 = \{0, 1\}, T_{X_0} = \{\emptyset, \{0\}, \{0, 1\}\}$, $T'_{X_0} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$, then there exists the minimal double compactness S such that $(X_0, T_{X_0}) \in S$ and $dT_{X_0} = T'_{X_0}$. The class S is the class of all spectral spaces (see [1]).

The class S satisfies the following properties:

1. For every T_0-space X the class $SGE(X)$ is a set, is a lattice, $SE(X) \neq \emptyset$ and the maximal element $(\beta_S X, \beta_S)$ is a compactification of X. We may consider that X is a subspace of $\beta_S X$ and X is dense in $\beta_S X$ in the strong topology on $\beta_S X$.
2. The class S is a virtual small quasi-compactness.
3. The class S is not a small quasi-compactness.

5 Non-existence of universal compactification

5.1. Definition. *A compactification $(bX,\, \varphi)$ of a space X is called a universal compactification of a space X if $(Y, f) \leq (bX,\, \varphi)$ for every compactification (Y, f) of X.*

5.2. Definition. *Let $i \in \{0, 1, 2\}$ and X be a T_i-space. A compactification (bX, φ) of the space X is called a universal T_i-compactification of X if bX is a T_i-space and $(Y, f) \leq (bX, \varphi)$ for every $T_i - g$-compactification (Y, f) of the space X.*

If X is a completely regular space, then the Stone-Čech compactification βX of X is a universal T_2-compactification of the space X.

5.3.Theorem. *Let X be a T_1-space. The following assertions are equivalent:*

1. For a space X there exists a universal compactification.

2. For a space X there exists a universal T_0-compactification.

3. For a space X there exists a universal T_1-compactification.

Proof. Part 1. Let Z be a space with the topology T. Denote by nT the topology on Z generated by the open base $\{U \backslash H : U \in T, H \text{ is finite subset of } Z\}$. The topology nT is called the T_1-modification of the topology T. Denote by nZ the set Z with the topology nT. The space Z is compact if and only if the space nZ is compact.

Part 2. Let (Y, f) be a compactification of the T_1-space X. Then $f : X \to Y$ is an embedding. It is obvious that the mapping $f : X \to nY$ is an embedding too. Thus (nY, f) is a T_1-compactification of the space X. By construction, $(Y, f) \leq (nY, f)$.

Part 3. For every g-compactification (Y, f) of the space X there exists a T_1-compactification (Z, g) of X such that $(Y, f) \leq (Z, g)$.

Let (Y_1, f_1) be some compactification of X. Consider the mapping $g : X \to Y \times Y_1$, where $g(x) = (f(x), f_1(x))$ for every $x \in X$. Then g is an embedding. Denote by Y_2 the closure of the set $g(X)$ in the space $Y \times Y_1$. Then (Y_2, g) is a compactification of X. We put $Z = nY_2$. Then (Z, g) is a T_1-compactification of X and $(Y, f) \leq (Y_2, g) \leq (Z, g)$.

Part 4. Let (Z, φ) be a universal compactification of the space X. Then (mZ, φ) is a universal compactification, a universal T_0-compactification and a universal T_1-compactification. The implications $1 \to 2$ and $1 \to 3$ are proved.

Part 5. Let (Z, φ) be a universal T_0-compactification. Then $(Z, g) \leq (Z, \varphi) \leq (nZ, \varphi)$ for every $T_1 - g$-compactification of X. Thus (nZ, φ) is a universal T_0-compactification, universal T_1-compactification. From Part 3 it follows that (nZ, φ) is a universal compactification. The implications $2 \to 1$ and $2 \to 3$ are proved.

Part 6. Let (Z, φ) be a universal T_1-compactification. From Part 3 it follows that (Z, φ) is a universal compactifiction and a universal T_0-compactification, too. The implications $3 \to 1$ and $3 \to 2$ and the theorem are proved.

5.4. Corollary. There exists a T_1-space X such that:

1. For X a universal T_1-compactification does not exist.
2. For X a universal T_0-compactification does not exist.
3. For X a universal compactification does not exist.

Proof. The existence of T_1-space X without universal T_1-compactification was proved by M. Hušec [5, 6]. Theorem 5.2. completes the proof.

6 The minimality of the compactification maX

Fix a T_0-space X. Let F be the space from Example 4.1.

6.1. Theorem. *Let P be a quasi-compactness and F be a subspace of some space from P. Then:*

1. There exists a compactification $(Y, f) \in PE(X)$ such that $(maX, m_X) \leq (Y, f)$.

2. If P is a small quasi-compactness then $(maX, m_X) \leq (\beta_p X, \beta_p)$.

Proof. Let $E \in P$ and F be a subspace of the space E. There exists an open subset U of E such that $0 \in U$ and $1 \notin U$. Consider the mapping $r : E \to F$, where $r^{-1}(0) = U$ and $r^{-1}(1) = E \backslash U$. The mapping r is a continuous retraction. By construction, $C(X, F) \subseteq C(X, E)$. We put $\Phi = C(X, F)$. Consider the mapping

$f_\Phi : X \to F^\Phi \subseteq E^\Phi$. By construction, maX is the closure of the set $f_\Phi(X)$ in the space F^Φ. Let Y be the closure of the set $f_\Phi(X)$ in the space E^Φ. Then $(Y, f_\Phi) \in P(E)E(P) \subseteq PE(X)$. Consider the continuous mapping $h : E^\Phi \to F^\Phi$, where $h(x_f : f \in \Phi) = (r(x_f) : f \in \Phi)$ for every point $x = (x_f : f \in \Phi) \in E^\Phi$. The mapping h is a retraction and $maX \subseteq h(Y)$. Thus maX is a subspace of the space Y and $(maX, m_X) = (maX, f_\Phi) \leq (Y, f_\Phi)$. The assertion 1 is proved. If P is a small quasi-compactness, then we may consider that $P = P(E)$. In this case $(Y, f_\Phi) \leq (\beta_p X, \beta_p)$. The proof is complete.

References

[1] Calmuţchi L.I., Choban M.M. *Extensions and mappings of topological spaces.* Buletin Ştiinţific. Universitatea din Piteşti, Matematica şi Informatica, 2005, **11**, 2005, p. 50.

[2] Choban M.M., Calmuţchi L.I. *On universal properties.* Analele Univer. din Oradea, Fascicole Matematica, 1999–2000, **VII**, p. 67–72.

[3] Engelking R. *General Topology.* Warsawa, PWN, 1997.

[4] Engelking R., Mrowka S. *On E-compact spaces.* Bulletin Acad. Polon. Sci., Mathematica, 1958, **6**, p. 429–436.

[5] Herrlich H. *Compact T_0-spaces and T_0-compactifications.* Applied Categorial Structures 1, 1993, p. 111–132.

[6] Hušec M. *Čech-Stone-like compactifications for general topological spaces.* Coment. Math. Univ. Carolinae, 1992, **33:1**, p. 159–163.

[7] Mrowka S. *Compactness and product spaces.* Colloq. Math., 1959–1960, **7**, p. 19–22.

[8] Kovar M.M. *Which topological spaces have a weak reflection in compact spaces.* Comment. Math. Univ. Carolinae, 1995, **36:3**, p. 529–536.

[9] Osmotescu T.C. *"$\omega\alpha$-extensions".* Vestnic Moscow. Univ., Matematica, 1963, **6**, p. 45–54.

Department of Mathematics
Tiraspol State University
5 Gh. Iablocichin str.
Chişinău, MD-2069, Moldova

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 43–62
ISSN 1024–7696

On the Riemann extension of the Gödel space-time metric

Valery Dryuma

Abstract. Some properties of the Gödel space-metric and its Riemann extension are studied. The spectrum of de Rham operator acting on 1-forms is studied. The examples of translation surfaces of the Gödel space-metric are constructed.

Mathematics subject classification: 53Bxx, 58xxx, 53xxx.
Keywords and phrases: Gödel space-time, translation surfaces, Riemann extensions, geodesics.

SATOR AREPO TENET OPERA ROTAS

1 Introduction

The notion of the Riemann extension of nonriemannian spaces was introduced first in [1]. Main idea of this theory is application of the methods of Riemann geometry for studying properties of nonriemaniann spaces.

For example the system of differential equations of the form

$$\frac{d^2x^k}{ds^2} + \Pi^k_{ij}\frac{dx^i}{ds}\frac{dx^j}{ds} = 0 \tag{1}$$

with arbitrary coefficients $\Pi^k_{ij}(x^l)$ can be considered as a system of geodesic equations of affinely connected space with local coordinates x^k.

For n-dimensional Riemannian spaces with the metrics

$${}^{n}ds^2 = g_{ij}dx^i dx^j$$

the system of geodesic equations looks similarly but the coefficients $\Pi^k_{ij}(x^l)$ now have very special form and depend on the choice of the metric g_{ij};

$$\Pi^i_{kl} = \Gamma^i_{kl} = \frac{1}{2}g^{im}(g_{mk,l} + g_{ml,k} - g_{kl,m})$$

In order that methods of Riemann geometry can be applied for studying properties of spaces with equations (1) the construction of $2n$-dimensional extension of the space with local coordinates x^i was introduced .

The metric of extended space is constructed with the help of coefficients of equation (1) and looks as follows

$${}^{2n}ds^2 = -2\Pi^k_{ij}(x^l)\Psi_k dx^i dx^j + 2d\Psi_k dx^k \tag{2}$$

where Ψ_k are the coordinates of additional space.

An important property of such type metric is that the geodesic equations of metric (2) decompos into two parts

$$\ddot{x}^k + \Gamma^k_{ij}\dot{x}^i\dot{x}^j = 0, \tag{3}$$

and

$$\frac{\delta^2\Psi_k}{ds^2} + R^l_{kji}\dot{x}^j\dot{x}^i\Psi_l = 0, \tag{4}$$

where

$$\frac{\delta\Psi_k}{ds} = \frac{d\Psi_k}{ds} - \Gamma^l_{jk}\Psi_l\frac{dx^j}{ds}.$$

The first part (3) of the full system is the system of equations for geodesics of basic space with local coordinates x^i and it does not contain coordinates Ψ_k.

The second part (4) of system of geodesic equations has the form of linear 4×4 matrix system of second order ODE's for coordinates Ψ_k

$$\frac{d^2\vec{\Psi}}{ds^2} + A(s)\frac{d\vec{\Psi}}{ds} + B(s)\vec{\Psi} = 0 \tag{5}$$

with the matrix

$$A = A(x^i(s), \dot{x}^i(s)), \quad B = B(x^i(s), \dot{x}^i(s)).$$

From this point of view we have the case of geodesic extension of the basic space (x^i). It is important to note that the geometry of extended space is connected with geometry of basic space.

For example the property of the space to be a Ricci-flat

$$R_{ij} = 0, \quad R_{ij;k} + R_{ki;j} + R_{jk;i} = 0,$$

or symmetrical

$$R_{ijkl;m} = 0$$

keeps also for the extended space.

This fact givs us the possibility to use the linear system of equation (5) for studying properties of basic space.

In particular the invariants of 4×4 matrix-function

$$E = B - \frac{1}{2}\frac{dA}{ds} - \frac{1}{4}A^2$$

under change of coordinates Ψ_k can be used for that.

For example the condition

$$E = B - \frac{1}{2}\frac{dA}{ds} - \frac{1}{4}A^2 = 0$$

for a given system means that it is equivalent to the simplest system

$$\frac{d^2\vec{\Phi}}{ds^2} = 0$$

and corresponding extended space is a flat space.

Other cases of integrability of the system (5) are connected with non-flat spaces having special form of the curvature tensor.

Remark that for extended spaces all scalar invariants constructed with the help of curvature tensor and its covariant derivatives are vanishing.

The first applications of the notion of extended spaces to the studying of non-linear second order differential equations and the Einstein spaces were done in the works of author [2–11]

Here we consider properties of the Gödel space-time and its Riemann extension.

2 The Gödel space-time metric

The line element of the metric of the Gödel space-time in coordinates x, y, z, t has the form

$$ds^2 = -dt^2 + dx^2 - 2\,e^{\frac{x}{a}} dtdy - 1/2\,e^{2\,\frac{x}{a}} dy^2 + dz^2. \tag{6}$$

Here the parameter a is the velocity of rotation [12].

The geodesic equations of the metric (6) are given by

$$2\left(\frac{d^2}{ds^2}x(s)\right)a + \left(e^{\frac{x(s)}{a}}\right)^2\left(\frac{d}{ds}y(s)\right)^2 + 2\,e^{\frac{x(s)}{a}}\left(\frac{d}{ds}t(s)\right)\frac{d}{ds}y(s) = 0, \tag{7}$$

$$\left(\frac{d^2}{ds^2}y(s)\right)e^{\frac{x(s)}{a}}a - 2\left(\frac{d}{ds}t(s)\right)\frac{d}{ds}x(s) = 0, \tag{8}$$

$$\frac{d^2}{ds^2}z(s) = 0, \tag{9}$$

$$\left(\frac{d^2}{ds^2}t(s)\right)a + e^{\frac{x(s)}{a}}\left(\frac{d}{ds}y(s)\right)\frac{d}{ds}x(s) + 2\left(\frac{d}{ds}t(s)\right)\frac{d}{ds}x(s) = 0. \tag{10}$$

The first integral of geodesics satisfies the condition

$$-\left(\frac{d}{ds}t(s)\right)^2 + \left(\frac{d}{ds}x(s)\right)^2 - 2\,e^{\frac{x(s)}{a}}\left(\frac{d}{ds}t(s)\right)\frac{d}{ds}y(s) - 1/2\,e^{2\,\frac{x(s)}{a}}\left(\frac{d}{ds}y(s)\right)^2 +$$

$$+\left(\frac{d}{ds}z(s)\right)^2 - \mu = 0.$$

The symbols of Christoffel of the metric (6) are

$$\Gamma^4_{12} = \frac{\exp(x/a)}{2a}, \quad \Gamma^2_{14} = -\frac{\exp(-x/a)}{a}, \quad \Gamma^4_{14} = \frac{1}{a}, \quad \Gamma^1_{22} = \frac{\exp(2x/a)}{2a},$$

$$\Gamma^1_{24} = \frac{\exp(x/a)}{2a}.$$

To find solutions of the equations of geodesics (7)–(10) we present the metric (6) in equivalent form [13]

$$ds^2 = -(dt + \frac{a\sqrt{2}}{y}dx)^2 + \frac{a^2}{y^2}(dx^2 + dy^2) + dz^2. \tag{11}$$

The correspondence between the both forms of the metrics is given by the relations

$$y = a\sqrt{2}\exp(-x/a), \quad x = y.$$

The equations of geodesics of the metric (11) are defined by

$$\left(\frac{d^2}{ds^2}x(s)\right)a + \sqrt{2}\left(\frac{d}{ds}t(s)\right)\frac{d}{ds}y(s) = 0, \tag{12}$$

$$\left(\frac{d^2}{ds^2}y(s)\right)y(s)a - \left(\frac{d}{ds}x(s)\right)^2 a - \sqrt{2}\left(\frac{d}{ds}t(s)\right)\left(\frac{d}{ds}x(s)\right)y(s) - \left(\frac{d}{ds}y(s)\right)^2 a = 0, \tag{13}$$

$$\left(\frac{d^2}{ds^2}t(s)\right)(y(s))^2 - \sqrt{2}a\left(\frac{d}{ds}y(s)\right)\frac{d}{ds}x(s) - 2\left(\frac{d}{ds}t(s)\right)\left(\frac{d}{ds}y(s)\right)y(s) = 0, \tag{14}$$

$$\frac{d^2}{ds^2}z(s) = 0. \tag{15}$$

The geodesic equations admit the first integral

$$\frac{dt}{ds} = \frac{(-c_2/\sqrt{2} + \sqrt{2}y)}{c_0}, \qquad \frac{dx}{ds} = \frac{y(c_2 - y)}{ac_0},$$

$$\frac{dy}{ds} = \frac{y(x - c_1)}{ac_0}, \qquad \frac{dz}{ds} = \frac{c_3}{c_0}, \tag{16}$$

where c_i, a_0 are parameters.

Remark 1. In the theory of varieties the Chern-Simons characteristic class is constructed from a matrix gauge connection A^i_{jk} as

$$W(A) = \frac{1}{4\pi^2}\int d^3x\epsilon^{ijk}tr\left(\frac{1}{2}A_i\partial_j A_k + \frac{1}{3}A_iA_jA_k\right).$$

This term can be translated into a three-dimensional geometric quantity by replacing the matrix connection A^i_{jk} with the Christoffel connection Γ^i_{jk}.

For the density of Chern-Simons invariant the expression can be obtained [14]

$$CS(\Gamma) = \epsilon^{ijk}(\Gamma^p_{iq}\Gamma^q_{kp;j} + \frac{2}{3}\Gamma^p_{iq}\Gamma^q_{jr}\Gamma^r_{kp}).$$

For the metric (11) by the condition $z = const$

$$ds^2 = -a^2/y^2dx^2 - 2\sqrt{2}a/ydxdt + a^2/y^2dy^2 - dt^2$$

we find the quantity

$$CS(\Gamma) = -\frac{\sqrt{2}}{ay^2}.$$

For the spatial metric

$$^3ds^2 = -g_{\alpha\beta} + \frac{g_{0\alpha}g_{0\beta}}{g_{00}}$$

of the metric (11)

$$-ds^2 = \frac{a^2}{y^2}(dx^2 + dy^2) + dz^2$$

the quantity $CS(\Gamma) = 0$.

3 The Riemann extension of the Gödel metric

The Christofell symbols of the metric (11) are

$$\Gamma^2_{11} = -\frac{1}{y}, \quad \Gamma^2_{22} = -\frac{1}{y}, \quad \Gamma^2_{14} = -\frac{\sqrt{2}}{2a}, \quad \Gamma^1_{24} = \frac{\sqrt{2}}{2a}, \quad \Gamma^4_{12} = -\frac{a\sqrt{2}}{2y^2}, \quad \Gamma^4_{14} = -\frac{1}{y}.$$

Now with the help of the formulae (2) we construct eight-dimensional extension of the metric (11).

It has the form

$$^8ds^2 = \frac{2}{y}Qdx^2 + \frac{2a\sqrt{2}}{y^2}Vdxdy + \frac{2\sqrt{2}}{a}Qdxdt + \frac{2}{y}Qdy^2 + (\frac{4}{y}V - 2\frac{\sqrt{2}}{a}P)dydt+$$
$$+2dxdP + 2dydQ + 2dzdU + 2dtdV. \tag{17}$$

where (P, Q, U, V) are additional coordinates.

The Ricci tensor of the four-dimensional Gödel space with the metric (11) or (6) satisfies the condition

$$^4R_{ik;l} + {}^4R_{li;k} + {}^4R_{kl;i} = 0.$$

This property is valid for the eight-dimensional space in local coordinates (x, y, z, t, P, Q, U, V) with the metric (11)

$$^8R_{ik;l} + {}^8R_{li;k} + {}^8R_{kl;i} = 0.$$

The full system of geodesic equations for the metric (7) decomposes into two parts.

The first part coincides with the equations (12)–(15) on the coordinates (x, y, z, t) and second part forms the linear system of equations for coordinates P, Q, U, V.

They are defined as

$$\frac{d^2}{ds^2}P(s) = -\frac{\left(\sqrt{2}a^2\left(\frac{d}{ds}x\right)^2 + 2\left(\frac{d}{ds}t\right)\left(\frac{d}{ds}x\right)ya - \sqrt{2}a^2\left(\frac{d}{ds}y\right)^2\right)V(s)}{(y)^3\,a} -$$

-

$$\frac{\left(2\,\left(\frac{d}{ds}x\right)(y)^2 a+\sqrt{2}\left(\frac{d}{ds}t\right)(y)^3\right)\frac{d}{ds}Q(s)}{(y)^3 a}-\frac{\sqrt{2}a\left(\frac{d}{ds}V(s)\right)\frac{d}{ds}y}{(y)^2}, \tag{18}$$

$$\begin{aligned}\frac{d^2}{ds^2}Q(s)=&\frac{\left(-3\,\left(\frac{d}{ds}x\right)^2 ya-2\sqrt{2}\left(\frac{d}{ds}t\right)\left(\frac{d}{ds}x\right)(y)^2-\left(\frac{d}{ds}y\right)^2 ya\right)Q(s)}{(y)^3 a}+\\&+\frac{\left(2\,a\left(\frac{d}{ds}y\right)\left(\frac{d}{ds}x\right)y+2\,\left(\frac{d}{ds}t\right)\left(\frac{d}{ds}y\right)(y)^2\sqrt{2}\right)P(s)}{(y)^3 a}+\\&+\frac{\left(-2\,\left(\frac{d}{ds}t\right)\left(\frac{d}{ds}y\right)ya-2\sqrt{2}a^2\left(\frac{d}{ds}y\right)\frac{d}{ds}x\right)V(s)}{(y)^3 a}+\frac{\sqrt{2}\left(\frac{d}{ds}t\right)\frac{d}{ds}P(s)}{a}-\\&-2\,\frac{\left(\frac{d}{ds}y\right)\frac{d}{ds}Q(s)}{y}+\frac{\left(-\sqrt{2}a^2\left(\frac{d}{ds}x\right)y-2\,\left(\frac{d}{ds}t\right)(y)^2 a\right)\frac{d}{ds}V(s)}{(y)^3 a},\end{aligned} \tag{19}$$

$$\frac{d^2}{ds^2}U(s)=0, \tag{20}$$

$$\begin{aligned}\frac{d^2}{ds^2}V(s)=&\frac{\left(\left(\frac{d}{ds}x\right)^2 a\sqrt{2}y+2\,\left(\frac{d}{ds}t\right)\left(\frac{d}{ds}x\right)(y)^2+\sqrt{2}\left(\frac{d}{ds}y\right)^2 ay\right)P(s)}{a^2(y)^2}+\\&+\frac{\left(-2\sqrt{2}\left(\frac{d}{ds}t\right)\left(\frac{d}{ds}x\right)y(s)a-2\,a^2\left(\frac{d}{ds}x\right)^2\right)V(s)}{a^2(y)^2}+\frac{\sqrt{2}\left(\frac{d}{ds}y\right)\frac{d}{ds}P(s)}{a}-\\&-\frac{\sqrt{2}\left(\frac{d}{ds}x\right)\frac{d}{ds}Q(s)}{a}-2\,\frac{\left(\frac{d}{ds}y\right)\frac{d}{ds}V(s)}{y}+2\,\frac{Q(s)\left(\frac{d}{ds}t\right)\frac{d}{ds}y}{a^2}.\end{aligned} \tag{21}$$

In result we have got a linear matrix-second order ODE for the coordinates U,V,P,Q

$$\frac{d^2\Psi}{ds^2}=A(x,\phi,z,t)\frac{d\Psi}{ds}+B(x,\phi,z,t)\Psi, \tag{22}$$

where

$$\Psi(s)=\begin{pmatrix}P(s)\\Q(s)\\U(s)\\V(s)\end{pmatrix}$$

and A,B are some 4×4 matrix-functions depending on the coordinates $x(s)$, $y(s)$, $z(s)$, $t(s)$ and their derivatives.

Now we shall investigate properties of the matrix system of equations (18)–(21).

To integrate this system we use the relation

$$\dot{x}(s)P(s)+\dot{y}(s)Q(s)+\dot{z}(s)U(s)+\dot{t}(s)V(s)-\frac{s}{2}-\mu=0, \tag{23}$$

which is valid for every Riemann extensions of affinely connected space and which is a consequence of the well known first integral of geodesic equations $g_{ik}\dot{x}^i\dot{x}^k=\nu$ of arbitrary Riemann space.

Using the expressions for the first integrals of geodesic (16) and $U(s)=\alpha s+\beta$ from the equation (20) the system of equations (18)–(21) may be simplified.

In result we get the system of equations for additional coordinates

$$\frac{d^2}{ds^2}P(s)=\frac{\left(\sqrt{2}c_0\,ac_1-\sqrt{2}c_0\,ax\right)\frac{d}{ds}V(s)}{yc_0{}^2a}+$$

$$+\frac{\left(-\sqrt{2}c_2\,y-2\sqrt{2}xc1+\sqrt{2}c_1{}^2+\sqrt{2}(y)^2+\sqrt{2}(x)^2\right)V(s)}{yc_0{}^2a}-\frac{\left(\frac{d}{ds}Q(s)\right)c_2}{c_0\,a}, \tag{24}$$

$$\frac{d^2}{ds^2}Q(s)=-\frac{\left(2\,(y)^2c_1-2\,(y)^2x\right)P(s)}{ya^2c_0{}^2}-$$

$$-\frac{\left(y\,(x)^2-(y)^3+yc_1{}^2+yc_2{}^2-2\,yxc_1\right)Q(s)}{ya^2c_0{}^2}-$$

$$-\frac{\left(2\,ac_0\,yx-2\,ac_0\,yc_1\right)\frac{d}{ds}Q(s)}{ya^2c_0{}^2}-\frac{\left(ac_0\,yc_2-2\,ac_0\,(y)^2\right)\frac{d}{ds}P(s)}{ya^2c_0{}^2}-\frac{\sqrt{2}\frac{d}{ds}V(s)}{c_0}-$$

$$-\frac{\left(\sqrt{2}c_2\,ax-\sqrt{2}c_2\,ac_1\right)V(s)}{ya^2c_0{}^2}, \tag{25}$$

$$\frac{d^2}{ds^2}V(s)=\frac{\left((y)^2\sqrt{2}c_2-(y)^3\sqrt{2}+y\sqrt{2}(x)^2-2\,y\sqrt{2}xc_1+y\sqrt{2}c_1{}^2\right)P(s)}{c_0{}^2a^3}+$$

$$+\frac{\left(-\sqrt{2}yxc_2+\sqrt{2}yc_1\,c_2+2\sqrt{2}(y)^2x-2\sqrt{2}(y)^2\,c_1\right)Q(s)}{c_0{}^2a^3}+$$

$$+\frac{\left(-\sqrt{2}yac_0\,c_2+\sqrt{2}(y)^2ac_0\right)\frac{d}{ds}Q(s)}{c_0{}^2a^3}+\frac{\left(\sqrt{2}yac_0\,x-\sqrt{2}yac_0\,c_1\right)\frac{d}{ds}P(s)}{c_0{}^2a^3}+$$

$$+\frac{\left(-2\,a^2c_0\,x+2\,a^2c_0\,c_1\right)\frac{d}{ds}V(s)}{c_0{}^2a^3}+\frac{\left(-2\,ac_2\,y+2\,a\,(y)^2\right)V(s)}{c_0{}^2a^3}. \tag{26}$$

The relation (23) in this case takes the form

$$-1/2\,\frac{(-2\,\alpha\,c3\,a+c_0\,a)\,s}{c_0\,a}-1/2\,\frac{\left(c_2\,\sqrt{2}a-2\,y\sqrt{2}a\right)V\,(s)}{c_0\,a}-$$

$$-1/2\,\frac{(2\,c_1\,y-2\,xy)\,Q\,(s)}{c_0\,a}-1/2\,\frac{\left(2\,(y)^2-2\,c_2\,y\right)P\,(s)}{c_0\,a}-\nu=0 \qquad (27)$$

and the system from three equations (24)–(26) can be reduced to the system of two coupled equations.

As example the substitution of the expression

$$Q\,(s)=1/2\,\frac{(-2\,\alpha\,c_3\,a+c_0\,a)\,s}{y\,(x-c_1)}+1/2\,\frac{\left(c_2\,\sqrt{2}a-2\,y\sqrt{2}a\right)V\,(s)}{y\,(x-c_1)}+$$

$$+1/2\,\frac{\left(2\,(y)^2-2\,c_2\,y\right)P\,(s)}{y\,(x\,(s)-c_1)}+\frac{\nu\,c_0\,a}{y\,(x-c_1)}$$

into the equation for $Q(s)$ give us the identity and in result our system takes the form

$$\frac{d^2}{ds^2}P\,(s)=-\frac{(-c_2+y)\,c_2\,\frac{d}{ds}P\,(s)}{c_0\,a\,(x-c_1)}-$$

$$-1/2\,\frac{\left(2\,(x)^2-4\,xc_1-2\,c_2\,y+c_2{}^2+2\,c_1{}^2\right)\sqrt{2}\frac{d}{ds}V\,(s)}{c_0\,(x-c_1)\,y}-$$

$$-\frac{c_2\,y\left((y)^2+c_2{}^2-2\,c_2\,y+c_1{}^2-2\,xc_1+(x)^2\right)P\,(s)}{a^2c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}+L(s)V\,(s)-$$

$$-1/2\,\frac{(-2\,\alpha\,c_3\,ac_2+c_0\,ac_2)\,sy\,(s)}{a^2c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}-1/2\,\frac{\left(-c_0\,ac_2{}^2+2\,\alpha\,c_3\,ac_2{}^2\right)s}{a^2c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}-$$

$$-1/2\,\frac{\left((2\,\alpha\,c_3\,ac_2-c_0\,ac_2)\,(x)^2+(2\,c_1\,c_0\,ac_2-4\,\alpha\,c_3\,c_1\,ac_2)\,x\right)s}{a^2c_0{}^2y\left((x)^2-2\,xc_1+c_1{}^2\right)}-$$

$$-1/2\,\frac{\left(2\,\alpha\,c_3\,c_1{}^2ac_2-c_1{}^2c_0\,ac_2\right)s}{a^2c_0{}^2y\left((x)^2-2\,xc_1+c_1{}^2\right)}, \qquad (28)$$

where

$$L\,(s)=\frac{(y)^2\,\sqrt{2}c_2}{ac_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}+1/2\,\frac{\sqrt{2}\left(2\,(x)^2-3\,c_2{}^2-4\,xc_1+2\,c_1{}^2\right)y}{ac_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}+$$

$$+1/2\,\frac{\sqrt{2}\left(-2\,c_2\,(x)^2-2\,c_1{}^2c_2+c_2{}^3+4\,c_2\,c_1\,x\right)}{ac_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}+$$

$$+1/2\,\frac{\sqrt{2}\left(2\,(x)^4-8\,(x)^3\,c_1+\left(c_2{}^2+12\,c_1{}^2\right)(x)^2+\left(-2\,c_2{}^2c_1-8\,c_1{}^3\right)x\right)}{ac_0{}^2y\left((x\,(s))^2-2\,xc_1+c_1{}^2\right)}+$$

$$+1/2\,\frac{\sqrt{2}\left(c_1{}^2c_2{}^2+2\,c_1{}^4\right)}{ac_0{}^2y\left((x\,(s))^2-2\,xc_1+c_1{}^2\right)},$$

and

$$\frac{d^2}{ds^2}V\,(s)=-\frac{\left(2\,(x)^2-4\,xc_1-3\,c_2\,y+2\,(y)^2+2\,c_1{}^2+c_2{}^2\right)\frac{d}{ds}V\,(s)}{ac_0\,\left(x-c_1\right)}+$$

$$+\frac{\left((y)^2+c_2{}^2-2\,c_2\,y+c_1{}^2-2\,xc_1+(x)^2\right)\sqrt{2}y\frac{d}{ds}P\,(s)}{c_0\,a^2\,(x-c_1)}+$$

$$+M(s)V\,(s)+N(s)P\,(s)+1/2\,\frac{\sqrt{2}\,(c_0-2\,\alpha\,c_3)\,s\,(y)^3}{a^2\,c_0{}^2\,(x-c_1{}^2)}+$$

$$+1/2\,\frac{\sqrt{2}\,(-2\,c_0\,c_2+4\,\alpha\,c_3\,c_2)\,s\,(y)^2}{a^2\,c_0{}^2\,(x-c_1{}^2)}+$$

$$+1/2\,\frac{\sqrt{2}\left(-2\,\alpha\,c_3\,c_2{}^2+c_2{}^2c_0+c_1{}^2c_0+x^2(c_0-2\,\alpha\,c_3)-2\,\alpha\,c_3\,c_1{}^2\right)sy}{a^2\,c_0{}^2\,(x-c_1{}^2)}+$$

$$+1/2\,\frac{\sqrt{2}\,((4\,\alpha\,c_3c_1-2c_0\,c_1)\,x)\,sy}{a^2\,c_0{}^2\,(x-c_1{}^2)},\tag{29}$$

where

$$M\,(s)=-2\,\frac{(y)^4}{a^2c_0{}^2\left((x)^2-2\,x\,(s)\,c_1+c_1{}^2\right)}+5\,\frac{(y)^3\,c_2}{a^2c_0{}^2\left((x)^2-2\,x\,(s)\,c_1+c_1{}^2\right)}-$$

$$-\frac{\left(-4\,xc_1+2\,(x)^2+4\,c_2{}^2+2\,c_1{}^2\right)(y)^2}{a^2c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}-\frac{\left(-c_2\,(x)^2-c_1{}^2c_2+2\,c_2\,c_1\,x-c_2{}^3\right)y}{a^2c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)},$$

$$N\,(s)=\frac{\sqrt{2}\,(y)^5}{a^3c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}-3\,\frac{\sqrt{2}\,(y)^4\,c_2}{a^3c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}+$$

$$+\frac{\sqrt{2}\left(2\,(x)^2+3\,c_2{}^2+2\,c_1{}^2-4\,xc_1\right)(y)^3}{a^3c_0{}^2\left((x)^2-2\,xc_1+c_1{}^2\right)}+$$

$$+\frac{\sqrt{2}\left(-3\,c_2\,\left(x\right)^2-{c_2}^3-3\,{c_1}^2c_2+6\,c_2\,c_1\,x\right)\left(y\right)^2}{a^3{c_0}^2\left(\left(x\right)^2-2\,x\,c_1+{c_1}^2\right)}+$$

$$+\frac{\sqrt{2}\left(\left(x\right)^4-4\,\left(x\right)^3\mathit{c1}+\left(6\,\mathit{c1}^2+\mathit{c2}^2\right)\left(x\right)^2+\left(-2\,\mathit{c2}^2\mathit{c1}-4\,\mathit{c1}^3\right)x\right)}{a^3\mathit{c0}^2\left(\left(x\right)^2-2\,x\,\mathit{c1}+\mathit{c1}^2\right)}+$$

$$+\frac{\sqrt{2}\left(\mathit{c1}^4+\mathit{c1}^2\mathit{c2}^2\right)y}{a^3\mathit{c0}^2\left(\left(x\right)^2-2\,x\,\mathit{c1}+\mathit{c1}^2\right)}.$$

The expressions for functions $x(s)$ and $y(s)$ are dependent on the choice of parameters and can be defined from the equations (16).

The integration of the equations (28)–(29) for the additional coordinates $P(s)$, $Q(s)$ is reduced to investigation of a 2×2 system of second order ODE's with variable coefficients.

Remark that the matrix E and its properties play important role in the analysis of such type of system of equations.

In result we get the correspondence between the geodesic in the x, y, x, t-space and the geodesic in the space with local coordinates P, Q, U, V (partner space).

The studying of such type of correspondence may be useful from various points of view.

4 Translation surfaces of the Gödel spaces

Now we discuss some properties of translation surfaces of the Gödel spaces.

According with definition ([15]) translation surfaces in arbitrary Riemannian space are defined by the systems of equations for local coordinates $x^i(u, v)$ of the space

$$\frac{\partial x^i(u,v)}{\partial u \partial v}+\Gamma^i_{jk}(x^m)\frac{\partial x^j(u,v)}{\partial u}\frac{\partial x^k(u,v)}{\partial v}=0, \tag{30}$$

where Γ^i_{jk} are the Christoffel coefficients.

In the case of the Gödel metric (6) we get the equations

$$\frac{\partial^2}{\partial u \partial v}x\left(u,v\right)+\frac{\sqrt{2}}{2a}\frac{\partial y(u,v)}{\partial u}\frac{\partial t(u,v)}{\partial v}+\frac{\sqrt{2}}{2a}\frac{\partial t(u,v)}{\partial u}\frac{\partial y(u,v)}{\partial v}=0, \tag{31}$$

$$\begin{aligned}&\frac{\partial^2}{\partial u \partial v}y\left(u,v\right)-\frac{\sqrt{2}}{2a}\frac{\partial x(u,v)}{\partial v}\frac{\partial t(u,v)}{\partial u}-\frac{\sqrt{2}}{2a}\frac{\partial t(u,v)}{\partial v}\frac{\partial x(u,v)}{\partial u}-\\&-\frac{1}{y(u,v)}\frac{\partial x(u,v)}{\partial u}\frac{\partial x(u,v)}{\partial v}-\frac{1}{y(u,v)}\frac{\partial y(u,v)}{\partial u}\frac{\partial y(u,v)}{\partial v}=0,\end{aligned} \tag{32}$$

$$\frac{\partial^2}{\partial u \partial v} t\,(u,v) - \frac{1}{y(u,v)} \frac{\partial y(u,v)}{\partial u} \frac{\partial t(u,v)}{\partial v} - \frac{1}{y(u,v)} \frac{\partial t(u,v)}{\partial u} \frac{\partial y(u,v)}{\partial v} -$$
$$- \frac{\sqrt{2a}}{2y(u,v)^2} \frac{\partial x(u,v)}{\partial u} \frac{\partial y(u,v)}{\partial v} - \frac{\sqrt{2a}}{2y(u,v)^2} \frac{\partial x(u,v)}{\partial v} \frac{\partial y(u,v)}{\partial u} = 0, \tag{33}$$

$$\frac{\partial^2}{\partial u \partial v} z\,(u,v) = 0. \tag{34}$$

Full integration of this nonlinear system of equations is a difficult problem. Give one example.

With this aim we present our system of equations in new coordinates $u = r + s, v = r - s$.

It takes the form

$$2 \left(1/4 \frac{\partial^2}{\partial r^2} x(r,s) - 1/4 \frac{\partial^2}{\partial s^2} x(r,s)\right) a +$$
$$+\sqrt{2} \left(1/2 \frac{\partial}{\partial r} y(r,s) + 1/2 \frac{\partial}{\partial s} y(r,s)\right) \left(1/2 \frac{\partial}{\partial r} t(r,s) - 1/2 \frac{\partial}{\partial s} t(r,s)\right) +$$
$$+\sqrt{2} \left(1/2 \frac{\partial}{\partial r} t(r,s) + 1/2 \frac{\partial}{\partial s} t(r,s)\right) \left(1/2 \frac{\partial}{\partial r} y(r,s) - 1/2 \frac{\partial}{\partial s} y(r,s)\right) = 0,$$

$$-2 \left(1/4 \frac{\partial^2}{\partial r^2} y(r,s) - 1/4 \frac{\partial^2}{\partial s^2} y(r,s)\right) y(r,s) a +$$
$$+2 \left(1/2 \frac{\partial}{\partial r} x(r,s) + 1/2 \frac{\partial}{\partial s} x(r,s)\right) \left(1/2 \frac{\partial}{\partial r} x(r,s) - 1/2 \frac{\partial}{\partial s} x(r,s)\right) a +$$
$$+\sqrt{2} \left(1/2 \frac{\partial}{\partial r} x(r,s) + 1/2 \frac{\partial}{\partial s} x(r,s)\right) \left(1/2 \frac{\partial}{\partial r} t(r,s) - 1/2 \frac{\partial}{\partial s} t(r,s)\right) y(r,s) +$$
$$+2 \left(1/2 \frac{\partial}{\partial r} y(r,s) + 1/2 \frac{\partial}{\partial s} y(r,s)\right) \left(1/2 \frac{\partial}{\partial r} y(r,s) - 1/2 \frac{\partial}{\partial s} y(r,s)\right) a +$$
$$+\sqrt{2} \left(1/2 \frac{\partial}{\partial r} t(r,s) + 1/2 \frac{\partial}{\partial s} t(r,s)\right) \left(1/2 \frac{\partial}{\partial r} x(r,s) - 1/2 \frac{\partial}{\partial s} x(r,s)\right) y(r,s) = 0,$$

$$-2 \left(1/4 \frac{\partial^2}{\partial r^2} t(r,s) - 1/4 \frac{\partial^2}{\partial s^2} t(r,s)\right) (y(r,s))^2 +$$
$$+\sqrt{2} a \left(1/2 \frac{\partial}{\partial r} x(r,s) + 1/2 \frac{\partial}{\partial s} x(r,s)\right) \left(1/2 \frac{\partial}{\partial r} y(r,s) - 1/2 \frac{\partial}{\partial s} y(r,s)\right) +$$
$$+\sqrt{2} a \left(1/2 \frac{\partial}{\partial r} y(r,s) + 1/2 \frac{\partial}{\partial s} y(r,s)\right) \left(1/2 \frac{\partial}{\partial r} x(r,s) - 1/2 \frac{\partial}{\partial s} x(r,s)\right) +$$

$$+2\left(1/2\,\frac{\partial}{\partial r}y(r,s)+1/2\,\frac{\partial}{\partial s}y(r,s)\right)\left(1/2\,\frac{\partial}{\partial r}t(r,s)-1/2\,\frac{\partial}{\partial s}t(r,s)\right)y(r,s)+$$

$$+2\left(1/2\,\frac{\partial}{\partial r}t(r,s)+1/2\,\frac{\partial}{\partial s}t(r,s)\right)\left(1/2\,\frac{\partial}{\partial r}y(r,s)-1/2\,\frac{\partial}{\partial s}y(r,s)\right)y(r,s)=0.$$

A solution of this system of equations we shall seek in the form

$$y(r,s)=B(r),\quad t(r,s)=C(r)-s,\quad x(r,s)=s+A(r),$$

where $B(r),C(r),A(r)$ are some unknown functions.

In result our system takes the form

$$\left(\frac{d^2}{dr^2}C(r)\right)(B(r))^2-\sqrt{2}a\left(\frac{d}{dr}B(r)\right)\frac{d}{dr}A(r)-2\left(\frac{d}{dr}B(r)\right)B(r)\frac{d}{dr}C(r)=0,$$

$$\left(\frac{d^2}{dr^2}B(r)\right)B(r)a-a\left(\frac{d}{dr}A(r)\right)^2+a-\sqrt{2}B(r)\left(\frac{d}{dr}A(r)\right)\frac{d}{dr}C(r)-\sqrt{2}B(r)-$$

$$-\left(\frac{d}{dr}B(r)\right)^2a=0,$$

$$\left(\frac{d^2}{dr^2}A(r)\right)a+\sqrt{2}\left(\frac{d}{dr}B(r)\right)\frac{d}{dr}C(r)=0.$$

Using the first integral

$$\frac{d}{dr}C(r)=-\frac{\sqrt{2}a\frac{d}{dr}A(r)}{B(r)}+\alpha,$$

the system can be written in the form

$$\left(\frac{d^2}{dr^2}B(r)\right)B(r)a+a\left(\frac{d}{dr}A(r)\right)^2+a-\sqrt{2}\left(\frac{d}{dr}A(r)\right)\alpha\,B(r)-\sqrt{2}B(r)-$$

$$-\left(\frac{d}{dr}B(r)\right)^2a=0,$$

$$\left(\frac{d^2}{dr^2}A(r)\right)aB(r)-2\left(\frac{d}{dr}B(r)\right)a\frac{d}{dr}A(r)+\sqrt{2}\left(\frac{d}{dr}B(r)\right)\alpha\,B(r)=0.$$

Integration of the last equation gives us the expression for the function $A(r)$

$$A(r)=\int\frac{B(r)\left(\sqrt{2}\alpha+B(r)C_1\,a\right)}{a}dr+C_2$$

with parameters C_1,C_2 and α.

After substitution of the expression for $A(r)$ in the first equation we get the equation

$$\left(\frac{d^2}{dr^2}B(r)\right)B(r)a+(B(r))^3\sqrt{2}\alpha\,C_1+(B(r))^4\,{C_1}^2a+a-\sqrt{2}B(r)-$$

$$-\left(\frac{d}{dr}B(r)\right)^2 a = 0$$

for the function $B(r)$.

Remark that this equation can be written in the form

$$\frac{d^2}{dr^2}E(r) = \frac{\sqrt{2}e^{-E(r)}}{a} - {C_1}^2 e^{2E(r)} - \frac{\sqrt{2}\alpha\, C_1\, e^{E(r)}}{a} - e^{-2E(r)}$$

after the change of variable $B(r) = \exp(E(r))$.

With the help of its solutions the examples of the translation surfaces of the Gödel space (6) can be constructed.

They can be presented in form

$$t + x = A(r) + C(r), \quad y = B(r),$$

or $t(x, y) = x + \phi(y)$ with some function $\phi(y)$.

Detailed consideration of properties of this type of translation surfaces, their intrinsic geometry and characteristic lines will be done in following publications of author.

Remark that with the help of the translation surfaces the properties of closed trajectories of the Gödel space can be investigated.

Let us consider the eight-dimensional extension of the Gödel space with the metric (17).

Translation surfaces in this case are determined by the equations (28)–(31) for coordinates x, y, z, t and by the linear system of equations in coordinates P, Q, U, V

$$\frac{\partial^2}{\partial u \partial v}P(u, v) -$$
$$-\frac{1}{2ay^3}\left(-2a^2\sqrt{2}\frac{\partial x}{\partial u}\frac{\partial x}{\partial v} - 2ay\frac{\partial x}{\partial u}\frac{\partial t}{\partial v} + 2a^2\sqrt{2}\frac{\partial y}{\partial u}\frac{\partial y}{\partial v} - 2ay\frac{\partial t}{\partial u}\frac{\partial x}{\partial v}\right)V(u, v) +$$
$$+\frac{1}{2ay^3}\left(2a^2\frac{\partial x}{\partial u} + \sqrt{2}y^3\frac{\partial t}{\partial u}\right)\frac{\partial Q(u, v)}{\partial v} + \frac{1}{2ay^3}\left(2a^2\frac{\partial x}{\partial v} + \sqrt{2}y^3\frac{\partial t}{\partial v}\right)\frac{\partial Q(u, v)}{\partial u} +$$
$$+\frac{a\sqrt{2}}{2y^2}\frac{\partial y}{\partial u}\frac{\partial V(u, v)}{\partial v} + \frac{a\sqrt{2}}{2y^2}\frac{\partial y}{\partial v}\frac{\partial V(u, v)}{\partial u} = 0, \tag{35}$$

$$\frac{\partial^2}{\partial u \partial v}Q(u, v) +$$
$$+\frac{1}{2ay^3}\left(6ay\frac{\partial x}{\partial u}\frac{\partial x}{\partial v} + 2\sqrt{2}y^2\frac{\partial x}{\partial u}\frac{\partial t}{\partial v} + 2\sqrt{2}y^2\frac{\partial x}{\partial v}\frac{\partial t}{\partial u} + 2ay\frac{\partial y}{\partial u}\frac{\partial y}{\partial v}\right)Q(u, v) +$$
$$+\frac{1}{2ay^3}\left(-2ay\frac{\partial x}{\partial u}\frac{\partial y}{\partial v} - 2\sqrt{2}y^2\frac{\partial y}{\partial u}\frac{\partial t}{\partial v} - 2\sqrt{2}y^2\frac{\partial y}{\partial v}\frac{\partial t}{\partial u} - 2ay\frac{\partial y}{\partial u}\frac{\partial x}{\partial v}\right)P(u, v) +$$

$$+\frac{1}{2ay^3}\left(2ay\frac{\partial y}{\partial u}\frac{\partial t}{\partial v}+2\sqrt{2}y^2\frac{\partial y}{\partial v}\frac{\partial x}{\partial u}+2\sqrt{2}y^2\frac{\partial y}{\partial u}\frac{\partial x}{\partial v}+2ay\frac{\partial y}{\partial v}\frac{\partial t}{\partial u}\right)V(u,v)+$$
$$+\frac{1}{y}\frac{\partial y}{\partial u}\frac{\partial Q(u,v)}{\partial v}+\frac{1}{y}\frac{\partial y}{\partial v}\frac{\partial Q(u,v)}{\partial u}-\frac{\sqrt{2}}{2a}\frac{\partial t}{\partial u}\frac{\partial P(u,v)}{\partial v}-\frac{\sqrt{2}}{2a}\frac{\partial t}{\partial v}\frac{\partial P(u,v)}{\partial u}+$$
$$+\frac{1}{2ay^3}\left(2ay^2\frac{\partial t}{\partial u}+\sqrt{2}a^2y\frac{\partial x}{\partial u}\right)\frac{\partial V(u,v)}{\partial v}+$$
$$+\frac{1}{2ay^3}\left(2ay^2\frac{\partial t}{\partial v}+\sqrt{2}a^2y\frac{\partial x}{\partial v}\right)\frac{\partial V(u,v)}{\partial u}=0, \tag{36}$$

$$\frac{\partial^2}{\partial u\partial v}V(u,v)+\ -\frac{1}{a^2}\left(\frac{\partial y}{\partial u}\frac{\partial t}{\partial v}+\frac{\partial y}{\partial v}\frac{\partial t}{\partial u}\right)Q(u,v)-$$
$$-\frac{1}{a^2y}\left(y\frac{\partial x}{\partial u}\frac{\partial t}{\partial v}+a\sqrt{2}\frac{\partial x}{\partial u}\frac{\partial x}{\partial v}+a\sqrt{2}\frac{\partial y}{\partial u}\frac{\partial y}{\partial v}+y\frac{\partial t}{\partial u}\frac{\partial x}{\partial v}\right)P(u,v)+$$
$$+\frac{1}{ay^2}\left(2a\frac{\partial x}{\partial u}\frac{\partial x}{\partial v}+y\sqrt{2}\frac{\partial x}{\partial u}\frac{\partial t}{\partial v}+y\sqrt{2}\frac{\partial t}{\partial u}\frac{\partial x}{\partial v}\right)V(u,v)+$$
$$+\frac{\sqrt{2}}{2a}\frac{\partial x}{\partial u}\frac{\partial Q}{\partial v}+\frac{\sqrt{2}}{2a}\frac{\partial x}{\partial v}\frac{\partial Q}{\partial u}+\frac{1}{y}\frac{\partial y}{\partial u}\frac{\partial V}{\partial v}+\frac{1}{y}\frac{\partial y}{\partial v}\frac{\partial V}{\partial u}-$$
$$-\frac{\sqrt{2}}{2a}\frac{\partial y}{\partial v}\frac{\partial P}{\partial u}-\frac{\sqrt{2}}{2a}\frac{\partial y}{\partial u}\frac{\partial P}{\partial v}=0, \tag{37}$$

$$\frac{\partial^2}{\partial u\partial v}U(u,v)=0. \tag{38}$$

The system of linear equations (32)–(35) is the matrix analog of the Laplace equation

$$\frac{\partial^2\Psi(u,v)}{\partial u\partial v}+A(u,v)\frac{\partial\Psi(u,v)}{\partial u}+B(u,v)\frac{\partial\Psi(u,v)}{\partial v}+C(u,v)\Psi(u,v)=0, \tag{39}$$

where

$$\Psi(u,v)=\begin{pmatrix}P(u,v)\\Q(u,v)\\U(u,v)\\V(u,v)\end{pmatrix}$$

is a vector-function, and $A(u,v),B(u,v),C(u,v)$ are matrices depending on the variables (u,v).

For integration of such type of equation the matrix generalization of the Darboux Invariants [16] can be used.

Remark 2. We remind basic facts on the integration of the matrix Laplace-equation.

The system (39) can be presented in the form

$$(\partial_u + B)(\partial_v + A)\Psi - H\Psi = 0,$$

or

$$(\partial_v + A)(\partial_u + B)\Psi - K\Psi = 0,$$

where

$$H = \frac{\partial A}{\partial u} + BA - C, \quad K = \frac{\partial B}{\partial v} + AB - C,$$

are the Darboux invariants of the system.

In the case $K = 0$ or $H = 0$ the system can be integrated.

If $K \neq 0$ and $H \neq 0$ the system may be presented in a similar form for the functions

$$\Psi_1 = \frac{\partial \Psi}{\partial y} + A\Psi.$$

or

$$\Psi_{-1} = \frac{\partial \Psi}{\partial x} + B\Psi.$$

In the first case one gets

$$\frac{\partial^2 \Psi_1(u,v)}{\partial u \partial v} + A_1(u,v)\frac{\partial \Psi_1(u,v)}{\partial u} + B_1(u,v)\frac{\partial \Psi_1(u,v)}{\partial v} + C_1(u,v)\Psi_1(u,v) = 0,$$

where

$$A_1 = HAH^{-1} - H_v H^{-1}, \quad B_1 = B, \quad C_1 = B_v - H + (HAH^{-1} - H_v H^{-1})B.$$

The invariants H_1 and K_1 for this equation are

$$H_1 = H - B_v + (HAH^{-1} - H_y H^{-1})_u + B(HAH^{-1} - H_v H^{-1}) - (HAH^{-1} - H_v H^{-1})B,$$

$$K_1 = H.$$

In the case $H_1 = 0$ the system can be integrated.

In the second case we get the equation for the function Ψ_{-1}

$$\frac{\partial^2 \Psi_{-1}(u,v)}{\partial u \partial v} + A_{-1}(u,v)\frac{\partial \Psi_{-1}(u,v)}{\partial u} + B_{-1}(u,v)\frac{\partial \Psi_{-1}(u,v)}{\partial v} + C_{-1}(u,v)\Psi_{-1}(u,v) = 0,$$

where

$$B_{-1} = KBK^{-1} - K_u K^{-1}, \quad A_{-1} = A, \quad C_{-1} = A_u - K + (KBK^{-1} - K_u K^{-1})A.$$

The invariants H_{-1} and K_{-1} for this equation are

$$K_{-1} = K - A_u + (KBK^{-1} - K_u K^{-1})_v + A(KBK^{-1} - K_u K^{-1}) - (KBK^{-1} - K_u K^{-1})A,$$

$$H_{-1} = K$$

and by the condition $K_{-1} = 0$ the system is also integrable.

To integrate the system of equations (39) in explicit form it is necessary to use the expressions for coordinates $x(u,v), y(u,v), z(u,v), t(u,v)$ of translation surfaces of the basic space.

The properties of the invariants H and K also may be important for classifications of translation surfaces of the basic and extended Gödel space.

5 On the spectrum of the Gödel space-time metric

In this section the spectrum λ of de Rham operator

$$\Delta = g^{ij}\nabla_i\nabla_j - Ricci,$$

defined on a four-dimensional Riemannian manifold and acting on 1-forms

$$\omega = A_i(x,y,z)dx^i = u(x,y,z,t)dx + v(x,y,z,t)dy + p(x,y,z,t)dz + q(x,y,z,t)dt$$

will be calculated.

The problem is reduced to the solution of the system of equations

$$g^{ij}\nabla_i\nabla_j A_k - R^l_k A_l - \mu^2 A_k = 0, \tag{40}$$

where ∇_k is a symbol of covariant derivative and R^i_j is the Ricci tensor of the metric g^{ij} of the Gödel space-time.

We use the Gödel space-time metric in form (11) and for simplicity sake the components of the 1-form ω will be presented as

$$A_k = [0, v(y,t), 0, q(y,t)].$$

As this takes place the system (40) looks as

$$-\frac{\partial}{\partial t}v(y,t) + \frac{\partial}{\partial y}q(y,t) = 0,$$

$$2\left(\frac{\partial}{\partial y}v(y,t)\right)y + \left(\frac{\partial^2}{\partial y^2}v(y,t)\right)y^2 + a^2\frac{\partial^2}{\partial t^2}v(y,t) - \mu^2 v(y,t)a^2 = 0,$$

$$2\left(\frac{\partial}{\partial y}q(y,t)\right)y - 2\left(\frac{\partial}{\partial t}v(y,t)\right)y + \left(\frac{\partial^2}{\partial y^2}q(y,t)\right)y^2 + \left(\frac{\partial^2}{\partial t^2}q(y,t)\right)a^2 -$$
$$-\mu^2 q(y,t)a^2 = 0.$$

It is equivalent to the following non-homogeneous equation

$$-\left(\frac{\partial^2}{\partial y^2}\Phi(y,t)\right)y^2 - \left(\frac{\partial^2}{\partial t^2}\Phi(y,t)\right)a^2 + \mu^2\Phi(y,t)a^2 + \epsilon = 0, \tag{41}$$

where

$$q(y,t) = \frac{\partial\Phi(y,t)}{\partial t}, v(y,t) = \frac{\partial\Phi(y,t)}{\partial y}$$

and ϵ is a parameter.

The simplest solution of homogeneous equation can be presented in the form

$$\Phi(y,t) = F_1(y)F_2(t), \tag{42}$$

where

$$\frac{d^2}{dt^2}F_2(t) = -\frac{c_1 F_2(t)}{a^2} + \mu^2 F_2(t),$$
$$\frac{d^2}{dy^2}F_1(y) = \frac{c_1 F_1(y)}{y^2}, \tag{43}$$

and c_1 is a parameter.

The second equation from (43) has the form

$$\frac{d^2}{dy^2}F_1(y) - \frac{c_1 F_1(y)}{y^2} = 0$$

and its solutions are defined by the relations

$$\frac{F_1}{\sqrt{y}} = C_1\cos(b\ln(y)) + C_2\sin(b\ln(y)), \quad b^2 = -c_1 - \frac{1}{4} > 0,$$

$$\frac{F_1}{\sqrt{y}} = C_1 x^b + C_2 x^{-b}, \quad b^2 = \frac{1}{4} + c_1 > 0,$$
$$\frac{F_1}{\sqrt{y}} = C_1 + C_2\ln(y), \quad c_1 = -\frac{1}{4},$$

which depend on the parameter c_1.

The solutions of the first equation of the system (43) are

$$F_2(t) = C_3\,\sin(1/4\,\frac{\sqrt{2}\sqrt{c_1 - 8\,\mu^2 a^2}t}{a}) + C_4\,\cos(1/4\,\frac{\sqrt{2}\sqrt{c_1 - 8\,\mu^2 a^2}t}{a}).$$

In result the general solution of the equation (41) can be constructed with the help of solutions $F_1(y)$ and $F_2(t)$.

So in dependence depend upon the choice of c_1 the spectrum of manifold and the solutions of the equation (41) will be various.

The problem of solutions of the system (40) in more general case of the 1-form $\omega = A_i(x,y,z)dx^i$ requires more detailed consideration.

Remark 3. For determination of the spectrum λ of Laplace operator

$$\Delta = g^{ij}\nabla_i\nabla_j$$

acting on the $0-form$- function $\psi(x,y,z,t)$ defined on the manifold with the metric g_{ij}, it is necessary to solve the equation

$$g^{ij}\nabla_i\nabla_j\psi = \lambda\psi.$$

In the case of Gödel space-time metric (6) we get

$$a\left(\frac{\partial^2}{\partial x^2}\psi(x,y,z,t)\right)e^{\frac{2x}{a}} + 2a\left(\frac{\partial^2}{\partial y^2}\psi(x,y,z,t)\right) + \left(\frac{\partial}{\partial x}\psi(x,y,z,t)\right)e^{\frac{2x}{a}} -$$

$$-4a\,e^{\frac{x}{a}}\left(\frac{\partial^2}{\partial t\partial y}\psi(x,y,z,t)\right)+a\left(\frac{\partial^2}{\partial z^2}\psi(x,y,z,t)\right)e^{\frac{2x}{a}}+a\left(\frac{\partial^2}{\partial t^2}\psi(x,y,z,t)\right)e^{\frac{2x}{a}}-$$

$$-a\lambda\,\psi(x,y,z,t)e^{\frac{2x}{a}}=0.$$

The substitution here the function $\psi(x,y,z,t)$ in form

$$\psi(x,y,z,t)=V(x)\exp(-x/(2a))\exp(my+nz+kt),$$

where m,n,k are the parameters lead to the equation

$$\frac{d^2}{dx^2}V(x)-\left(-2m^2\,e^{-\frac{2x}{a}}+4km\,e^{-\frac{x}{a}}-n^2-k^2+1/4\,a^{-2}+\lambda\right)V(x)=0.$$

having the form of one dimensional Schrödinger equation for the spectrum of the particle in the field with the Morse potential.

In such type of potential a finite number of stationary states λ_n at the some relations between the parameters m,n,k,a may be existed.

This fact is important for understanding of the properties of the Gödel space-time metric.

6 Spatial metric of the four-dimensional Gödel space-time

The spatial metric of any four-dimensional metric

$${}^4ds^2=g_{\alpha\beta}dx^\alpha dx^\beta+2g_{0\alpha}dx^0dx^\alpha+g_{00}dx^0dx^0$$

has the form

$${}^3dl^2=\gamma_{\alpha\beta}dx^\alpha dx^\beta,$$

where

$$\gamma_{\alpha\beta}=-g_{\alpha\beta}+\frac{g_{0\alpha}g_{0\beta}}{g_{00}}$$

is a three-dimensional tensor determining the properties of the space.

In the case of the Gödel space-time the spatial three-dimensional metric has the form

$$-{}^3dl^2=\frac{a^2}{y^2}(dx^2+dy^2)+dz^2. \tag{44}$$

Three-dimensional space with the metric (44) belongs to one of the eight types of W.Thurston geometries and has diverse global properties.

In particular it admits the surfaces bundle.

As example we consider the translation surfaces of the space (44).

They defined by the system of equations for coordinates $x(u,v),y(u,v)$ and $z(u,v)$

$$\left(\frac{\partial^2}{\partial u\partial v}x(u,v)\right)y(u,v)-\left(\frac{\partial}{\partial u}x(u,v)\right)\frac{\partial}{\partial v}y(u,v)-\left(\frac{\partial}{\partial u}y(u,v)\right)\frac{\partial}{\partial v}x(u,v)=0,$$

$$\left(\frac{\partial^2}{\partial u \partial v} y(u,v)\right) y(u,v) + \left(\frac{\partial}{\partial u} x(u,v)\right) \frac{\partial}{\partial v} x(u,v) - \left(\frac{\partial}{\partial u} y(u,v)\right) \frac{\partial}{\partial v} y(u,v) = 0, \tag{45}$$

$$\frac{\partial^2}{\partial u \partial v} z(u,v) = 0.$$

The simplest solutions of these equations are of the form

$$y(u,v) = 1/2 \left(1 + \left(\left(\frac{u}{v}\right)^{C_1}\right)^2 \left(e^{C_2\, C_1}\right)^{-2}\right) e^{C_2\, C_1} \left(\left(\frac{u}{v}\right)^{C_1}\right)^{-1} C_1{}^{-1},$$

$$x(u,v) = \ln(u) + \ln(v),$$

and

$$z(u,v) = A(u) + B(v),$$

where $A(v)$ and $B(v)$ are arbitrary functions and C_1, C_2 are parameters.

In particular case $C_1 = 1$, $C_2 = 0$ one get

$$y(u,v) = 1/2\, \frac{u^2 + v^2}{uv}, \qquad x(u,v) = \ln(uv).$$

From here we find

$$v = \sqrt{ye^x + e^x\sqrt{y^2 - 1}}, \qquad u = \frac{e^x}{\sqrt{ye^x + e^x\sqrt{y^2 - 1}}}$$

and

$$z(x,y) = A(\sqrt{ye^x + e^x\sqrt{y^2 - 1}}) + B(\frac{e^x}{\sqrt{ye^x + e^x\sqrt{y^2 - 1}}})$$

with arbitrary functions $A(u), B(v)$.

The properties of surfaces are dependent on the choice of the functions A and B.

Remark 4. From the system (45) we find the relations

$$\left(\frac{\partial}{\partial v} x(u,v)\right)^2 - \frac{e^{2\,z(u,v)}}{v^2} + \left(\frac{\partial}{\partial v} z(u,v)\right)^2 e^{2\,z(u,v)} = 0,$$

$$\left(\frac{\partial}{\partial u} x(u,v)\right)^2 - \frac{e^{2\,z(u,v)}}{u^2} + \left(\frac{\partial}{\partial u} z(u,v)\right)^2 e^{2\,z(u,v)} = 0,$$

where $z(u,v) = \ln(y(u,v))$.

This fact allows us to get one equation in variable $y(u,v)$ only.

$$\left(-\sqrt{(y)^2 - \left(\frac{\partial}{\partial v} y\right)^2 v^2}\, v \left(\frac{\partial}{\partial u} y\right) u^2 + \sqrt{(y)^2 - \left(\frac{\partial}{\partial u} y\right)^2 u^2}\, u \left(\frac{\partial}{\partial v} y\right) v^2\right) \frac{\partial^2}{\partial u \partial v} y +$$

$$+\sqrt{(y(u,v))^2 - \left(\frac{\partial}{\partial v} y\right)^2 v^2}\, v \left(\frac{\partial}{\partial v} y\right) y - \sqrt{(y)^2 - \left(\frac{\partial}{\partial u} y\right)^2 u^2}\, u \left(\frac{\partial}{\partial u} y\right) y = 0.$$

References

[1] Paterson E.M., Walker A.G. *Riemann extensions.* Quart. J. Math. Oxford, 1952, **3**, p. 19–28.

[2] Dryuma V. *Applications of Riemannian and Einstein-Weyl Geometry in the theory of second order ordinary differential equations.* Theoretical and Mathematical Physics, 2001, **128**, N 1, p. 845–855.

[3] Dryuma V. *The Riemann Extension in theory of differential equations and their applications.* Matematicheskaya fizika, analiz, geometriya, 2003, **10**, N 3, p. 1–19.

[4] Dryuma V. *The Invariants,the Riemann and Einstein-Weyl geometry in theory of ODE's and all tha.* New Trends in Integrability and Partial Solvability / Eds. A.B. Shabat et al., 2004, p. 115–156; Kluwer Academic Publishers. ArXiv: nlin: SI/0303023, 11 March , 2003, p. 1–37.

[5] Dryuma V. *The Riemann Extension of the Schwarzschild space-time.* Buletinul A. Ş. M., Matematica, 2003, N 3(43), p. 92–103.

[6] Dryuma V. *On geodesical extension of the Schwarzshild space-time.* Proceedings of Institute of Mathematics of NAS of Ukraine, 2004, **50**, p. 1294–1300.

[7] Dryuma V. *On the Riemann extension of the space-time with vanishing curvature invariants.* http://www.math.kth.se/4ecm/abstract/14.27.pdf, Sweden, Stockholm, June 27–July 2, ECM'2004.

[8] Dryuma V. *The Riemann Extension of the Minkowsky space-time in rotating coordinate system.* ArXiv: gr-qc/0505122, vol. 1, 24 May 2005, p. 1–10.

[9] Dryuma V. *On theory of the spaces of constant curvature.* ArXiv: math.DG/0505376, 18 May 2005, p. 1–12.

[10] Dryuma V. *Riemann extensions in theory of the first order systems of differential equations.* ArXiv:math.DG/0510526, 25 October 2005, p. 1–21.

[11] Dryuma V. *From the Number theory to the Riemann geometry.* Scientific Papers International Conference "Differential Equations and Computer Algebra Systems (DE and CAS'2005)", Part 1, Minsk, BGPU, 2005, p. 14–15.

[12] Hawking S.W., Ellis G. *The Large Scale Structure of Space-Time.* Moskow, 1977 (in Russian).

[13] Dautcourt G. *Abdel-Megied M.,Revisiting the Light Cone of the Gödel Universe.* ArXiv:gr-qc/0511015, 3 Nov 2005, p. 1–23.

[14] Jackiw R. *A Pure Cotton Kink in a Funny Place.* ArXiv: math-ph/0403044, vol. 2, 21 July 2004.

[15] Eisenhart L.P. *Riemannian geometry.* Moskow, 1948 (in Russian).

[16] Elianu I.P. *Cercetari asupra sistemelor de ecuatii lineare cu derivate partiale de tip Laplace.* Studii si cercetari matematice, 1953, **IV**, N 1–2, p. 155–196.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
str. Academiei 5, MD-2028 Chişinău
Moldova
E-mails: *valery@dryuma.com; cainar@mail.md*

Received November 11, 2005

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 63–70
ISSN 1024–7696

Some n-ary analogs of the notion of a normalizer of an n-ary subgroup in a group

A.M. Gal'mak

Abstract. In this article n-ary analogs of the concept of normalizer of a subgroup of a group are constructed. It is proved that in an n-ary group the role of these n-ary analogs play the concepts of a normalizer and seminormalizer of n-ary subgroup in n-ary group. A connection of these analogs with its binary prototypes is established.

Mathematics subject classification: 20N15.
Keywords and phrases: n-ary group, normalizer, seminormalizer.

In this article for any n-ary group $< A, [\ ] >$ we denote by θ_A the introduced by Post [1] equivalence which is defined on a free semigroup F_A by the rule: $(\alpha, \beta) \in \theta_A$ if and only if there exist sequences γ and δ such that $[\gamma\alpha\delta] = [\gamma\beta\delta]$.

For any n-ary group $< A, [\ ] >$ Post defined also the universal enveloping group $A^* = F_A/\theta_A$. In this enveloping group he selected a normal subgroup

$$A_o = \{\theta_A(a_1 \dots a_{n-1}) | a_1, \dots, a_{n-1} \in A\},$$

which is called a corresponding group for the group $< A, [\ ] >$ and he proved that

$$A^*/A_o = \{\theta_A(a)A_o, \theta_A^2(a)A_o, \dots, \theta_A^{n-1}(a)A_o = A_o\}$$

for any $a \in A$, moreover A^*/A_o is a cyclic group of order $n-1$, but generating coset of this cyclic group is an n-ary group that is isomorphic to the n-ary group $< A, [\ ] >$.

We use standard notations. We remark only that one can find definition of n-ary group in the book of V.D. Belousov [2]. In this book the existence of the group A^* is proved and properties of a solution of the equation $[x \underbrace{a \dots a}_{n-1}] = a$ are given. This solution is denoted by the symbol $\bar{a}$ and is called a skew element for the element a.

We recall the normalizer of a subset B in an n-ary group $< A, [\ ] >$ ([3]) is the set

$$N_A(B) = \{x \in A | [x \overset{n-1}{B}] = [\overset{i}{B} x \overset{n-1-i}{B}], \forall i = 1, \dots, n-1\},$$

and a seminormalizer of a subset B in n-ary group $< A, [\ ] >$ ([3]) is the set

$$HN_A(B) = \{x \in A | [x \overset{n-1}{B}] = [\overset{n-1}{B} x]\}.$$

In [3] it is proved that if $< B, [\ ] >$ is an n-ary subgroup of an n-ary group $< A, [\ ] >$, then $< N_A(B), [\ ] >$ and $< HN_A(B), [\ ] >$ are n-ary subgroups in $< A, [\ ] >$ and $N_A(B) \subseteq HN_A(B)$.

For any subset B of an n-ary group $< A, [\ ] >$ it is supposed [4]:

$$B_o(A) = \{\theta_A(\alpha) \in A_o \mid \exists b_1, \ldots, b_{n-1} \in B,\ \alpha\theta_A b_1 \ldots b_{n-1}\};$$

$$B^*(A) = \{\theta_A(\alpha) \in A^* \mid \exists b_1, \ldots, b_i \in B (i \geq 1),\ \alpha\theta_A b_1 \ldots b_i\}.$$

It is clear that $B^*(A) \subseteq A^*$, $B_o(A) \subseteq A_o$. In particular, $A^*(A) = A^*$, $A_o(A) = A_o$.

If $< B, [\ ] >$ is an n-ary subgroup of an n-ary group $< A, [\ ] >$, then $B^*(A)$ is a subgroup of the group A^* that is isomorphic to the group B^*, and $B_o(A)$ is a subgroup of the group A_o, which is isomorphic to the group B_o [4].

Lemma 1. *Let $< B, [\ ] >$ be an n-ary subgroup of an n-ary group $< A, [\ ] >$, $b \in B$, $u = \theta_A(x\underbrace{b \ldots b}_{n-2}) \in N_{A_o}(B_o(A))$. Then $x \in HN_A(B)$.*

Proof. By condition $u^{-1}vu \in B_o(A)$ for any

$$v = \theta_A(b_o\underbrace{b \ldots b}_{n-2}) \in B_o(A), b_o \in B,$$

i.e.

$$\theta_A(\bar{b}\bar{x}\underbrace{x \ldots x}_{n-3})\theta_A(b_o\underbrace{b \ldots b}_{n-2})\theta_A(x\underbrace{b \ldots b}_{n-2}) \in B_o(A),$$

whence

$$\bar{b}\bar{x}\underbrace{x \ldots x}_{n-3}b_o\underbrace{b \ldots b}_{n-2}x\underbrace{b \ldots b}_{n-2}\theta_A b_1 \ldots b_{n-1}$$

for some $b_1, \ldots, b_{n-1} \in B$. Then

$$[b_o\underbrace{b \ldots b}_{n-2}x] = [x\underbrace{b \ldots b}_{n-2}b_1 \ldots b_{n-1}\bar{b}] \in [x\underbrace{B \ldots B}_{n-1}].$$

Since b_o is an arbitrary element of B, then the inclusion is proved

$$[\underbrace{B \ldots B}_{n-1}x] \subseteq [x\underbrace{B \ldots B}_{n-1}]. \tag{1}$$

If we again apply the condition, then we obtain $uvu^{-1} \in B_o(A)$, i.e.

$$\theta_A(x\underbrace{b \ldots b}_{n-2})\theta_A(b_o\underbrace{b \ldots b}_{n-2})\theta_A(\bar{b}\bar{x}\underbrace{x \ldots x}_{n-3}) \in B_o(A),$$

whence

$$x\underbrace{b \ldots b}_{n-2}b_o\underbrace{b \ldots b}_{n-2}\bar{b}\bar{x}\underbrace{x \ldots x}_{n-3}\theta_A c_1 \ldots c_{n-1}$$

for some $c_1, \ldots, c_{n-1} \in B$. Then

$$[x\underbrace{b\ldots b}_{n-2}b_o] = [c_1 \ldots c_{n-1}x] \in [\underbrace{B\ldots B}_{n-1}x],$$

whence

$$[x\underbrace{B\ldots B}_{n-1}] \subseteq [\underbrace{B\ldots B}_{n-1}x]. \tag{2}$$

From (1) and (2) it follows

$$[x\underbrace{B\ldots B}_{n-1}] = [\underbrace{B\ldots B}_{n-1}x].$$

Therefore, $x \in HN_A(B)$. The lemma is proved.

Theorem 1. *If $< B, [\ ] >$ is an n-ary subgroup in an n-ary group $< A, [\ ] >$, then*

$$(HN_A(B))_o(A) = N_{A_o}(B_o(A)).$$

Proof. We fix $h \in HN_A(B)$ and choose an arbitrary

$$u = \theta_A(h_o\underbrace{h\ldots h}_{n-2}) \in (HN_A(B))_o(A), h_o \in HN_A(B).$$

If b_o is an arbitrary element, b is a fixed element of the set B, then

$$v = \theta_A(b_o\underbrace{b\ldots b}_{n-2})$$

is an arbitrary element of $B_o(A)$. Since h_o, $\bar{h} \in HN_A(B)$, then

$$u^{-1}vu = \theta_A(\bar{h}\bar{h}_o\underbrace{h_o\ldots h_o}_{n-3})\theta_A(b_o\underbrace{b\ldots b}_{n-2})\theta_A(h_o\underbrace{h\ldots h}_{n-2}) =$$

$$= \theta_A(\bar{h}\bar{h}_o\underbrace{h_o\ldots h_o}_{n-3}b_o\underbrace{b\ldots b}_{n-2}h_o\underbrace{h\ldots h}_{n-2}) = \theta_A(\bar{h}\bar{h}_o\underbrace{h_o\ldots h_o}_{n-3}[b_o\underbrace{b\ldots b}_{n-2}h_o]\underbrace{h\ldots h}_{n-2}) =$$

$$= \theta_A(\bar{h}\bar{h}_o\underbrace{h_o\ldots h_o}_{n-3}[h_ob_1\ldots b_{n-1}]\underbrace{h\ldots h}_{n-2}) = \theta_A([\bar{h}b_1\ldots b_{n-1}]\underbrace{h\ldots h}_{n-2}) =$$

$$= \theta_A([b'_1\ldots b'_{n-1}\bar{h}]\underbrace{h\ldots h}_{n-2}) = \theta_A(b'_1\ldots b'_{n-1}),$$

where $b_1, \ldots, b_{n-1}, b'_1, \ldots, b'_{n-1} \in B$. Then, $u^{-1}vu \in B_o(A)$, whence $u \in N_{A_o}(B_o(A))$ and the inclusion is proved

$$(HN_A(B))_o(A) \subseteq N_{A_o}(B_o(A)). \tag{3}$$

Since any element $u \in N_{A_o}(B_o(A))$ can be presented in the form

$$u = \theta_A(x\underbrace{b\ldots b}_{n-2}), b \in B,$$

then by Lemma 1 $x \in HN_A(B)$, whence, taking into consideration $B \subseteq HN_A(B)$, we have

$$u = \theta_A(x\underbrace{b\ldots b}_{n-2}) \in (HN_A(B))_o(A).$$

Therefore,

$$N_{A_o}(B_o(A)) \subseteq (HN_A(B))_o(A). \tag{4}$$

From (3) and (4) it follows the needed equality. The theorem is proved.

By remark 2.2.20 [4], corresponding group N_o of n-ary subgroup $< N, [\ ] >$ of n-ary group $< A, [\ ] >$ is isomorphic to subgroup $N_o(A)$ of corresponding group A_o. Therefore from Theorem 1 follows

Corollary 1. *The corresponding Post group of semi-normalizer $< HN_A(B), [\ ] >$ of n-ary subgroup $< B, [\ ] >$ in n-ary group $< A, [\ ] >$ is isomorphic to normalizer of subgroup $B_o(A)$ in corresponding group A_o:*

$$(HN_A(B))_o \simeq N_{A_o}(B_o(A)).$$

Thus Theorem 1 and Corollary 1 establish a correspondence between a semi-normalizer of n-ary subgroup in an n-ary group and its binary prototype in the corresponding Post group.

We notice in [5] a correspondence between a semi-normalizer of an n-ary subgroup in an n-ary group and its binary prototype in the group to which the n-ary group is reducible by Gluskin-Hossu theorem. Namely, the following propositions are proved.

Theorem 2 [5]. *A semi-normalizer of n-ary subgroup $< B, [\ ] >$ in n-ary group $< A, [\ ] >$ coincides with the normalizer of the subgroup $< B_a, ⓐ >$ in the group $< A, ⓐ >$ for any $a \in HN_A(B)$, where $B_a = [\underbrace{B\ldots B}_{n-1}a]$, and the operation ⓐ is defined in the following way*

$$x ⓐ y = [x\bar{a}\underbrace{a\ldots a}_{n-3}y].$$

Corollary 2 [5]. *A semi-normalizer of n-ary subgroup $< B, [\,] >$ in n-ary group $< A, [\,] >$ coincides with the normalizer of the subgroup $< B, ⓐ >$ in group $< A, ⓐ >$ for any $a \in B$.*

We establish now a connection between normalizer of an n-ary subgroup in n-ary group and its binary prototype in enveloping Post group.

Lemma 2 [3]. *If $< B, [\,] >$ is an n-ary subgroup of an n-ary group $< A, [\,] >$, then*

$$N_A(B) = \{x \in A | [xB\underbrace{x \dots x}_{n-3}\bar{x}] = B\} = \{x \in A | [\bar{x}\underbrace{x \dots x}_{n-3}Bx] = B\}.$$

Lemma 3. *If $< B, [\,] >$ is an n-ary subgroup of an n-ary group $< A, [\,] >$, $x \in N_A(B)$, then*

$$[\underbrace{x \dots x}_{i-1}B\underbrace{x \dots x}_{n-i-1}\bar{x}] = B, \quad [\bar{x}\underbrace{x \dots x}_{n-i-1}B\underbrace{x \dots x}_{i-1}] = B$$

for any $i = 1, \dots, n-1$.

Proof. We prove the second equality. If $i = 1$, then $B = B$. If $i = 2$, then by Lemma 2

$$[\bar{x}\underbrace{x \dots x}_{n-3}Bx] = B.$$

From the last equality we have

$$[\bar{x}\underbrace{x \dots x}_{n-3}[\bar{x}\underbrace{x \dots x}_{n-3}Bx]x] = [\bar{x}\underbrace{x \dots x}_{n-3}Bx], \quad [\bar{x}\underbrace{x \dots x}_{n-4}Bxx] = B,$$

whence

$$[\bar{x}\underbrace{x \dots x}_{n-3}[\bar{x}\underbrace{x \dots x}_{n-4}Bxx]x] = [\bar{x}\underbrace{x \dots x}_{n-3}Bx], \quad [\bar{x}\underbrace{x \dots x}_{n-5}Bxxx] = B.$$

Further we have

$$[\bar{x}xB\underbrace{x \dots x}_{n-3}] = B, \quad [\bar{x}B\underbrace{x \dots x}_{n-2}] = B.$$

Therefore, the second equality is true for any $i = 1, \dots, n-1$.

The first equality is proved similarly. The lemma is proved.

Theorem 3. *If $< B, [\,] >$ is an n-ary subgroup of an n-ary group $< A, [\,] >$, then*

$$(N_A(B))^*(A) = N_{A_*}(B^*(A)).$$

Proof. We fix an element $h \in N_A(B)$ and take any element

$$u = \theta_A(h_o \underbrace{h \ldots h}_{i-1}) \in (N_A(B))^*(A),\ h_o \in N_A(B).$$

If b_o is any element and b is a fixed element from B, then

$$v = \theta_A(b_o \underbrace{b \ldots b}_{j-1})$$

is any element from $B^*(A)$. Since $h_o, h \in N_A(B)$, then, if we apply Lemma 2, after that Lemma 3, then we obtain

$$u^{-1}vu = \theta_A(\bar{h} \underbrace{h \ldots h}_{n-i-1} \bar{h}_o \underbrace{h_o \ldots h_o}_{n-3})\theta_A(b_o \underbrace{b \ldots b}_{j-1})\theta_A(h_o \underbrace{h \ldots h}_{i-1}) =$$

$$= \theta_A(\bar{h} \underbrace{h \ldots h}_{n-i-1} \bar{h}_o \underbrace{h_o \ldots h_o}_{n-3} b_o \underbrace{b \ldots b}_{j-1} h_o \underbrace{h \ldots h}_{i-1}) =$$

$$= \theta_A(\bar{h} \underbrace{h \ldots h}_{n-i-1}[\bar{h}_o \underbrace{h_o \ldots h_o}_{n-3} b_o h_o] \underbrace{[\bar{h}_o \underbrace{h_o \ldots h_o}_{n-3} b h_o] \ldots [\bar{h}_o \underbrace{h_o \ldots h_o}_{n-3} b h_o]}_{j-1} \underbrace{h \ldots h}_{i-1}) =$$

$$= \theta_A(\bar{h} \underbrace{h \ldots h}_{n-i-1} b'_o \underbrace{b' \ldots b'}_{j-1} \underbrace{h \ldots h}_{i-1}) =$$

$$= \theta_A([\bar{h} \underbrace{h \ldots h}_{n-i-1} b'_o \underbrace{h \ldots h}_{i-1}] \underbrace{[\bar{h} \underbrace{h \ldots h}_{n-i-1} b' \underbrace{h \ldots h}_{i-1}] \ldots [\bar{h} \underbrace{h \ldots h}_{n-i-1} b' \underbrace{h \ldots h}_{i-1}]}_{j-1}) = \theta_A(b''_o \underbrace{b'' \ldots b''}_{j-1}),$$

where $b'_o, b', b''_o, b'' \in B$. Therefore, $u^{-1}vu \in B^*(A)$, $u \in N_{A^*}(B^*(A))$ and the following inclusion is proved

$$(N_A(B))^*(A) \subseteq N_{A^*}(B^*(A)). \qquad (5)$$

Let $c \in B$ and

$$u = \theta_A(x \underbrace{c \ldots c}_{i-1}) = \theta_A(x)\theta_A(\underbrace{c \ldots c}_{i-1})$$

be an element of $N_{A^*}(B^*(A))$. Since

$$\theta_A(\underbrace{c \ldots c}_{i-1}) \in B^*(A) \subseteq N_{A^*}(B^*(A)),$$

then from the last equality it follows

$$\theta_A(x) \in N_{A^*}(B^*(A)). \tag{6}$$

Thus $\theta_A^{-1}(x)\theta_A(b)\theta_A(x) \in B^*(A)$ for any $b \in B$, whence

$$\theta_A(\bar{x}\underbrace{x\ldots x}_{n-3}bx) \in B^*(A),$$

i.e.

$$[\bar{x}\underbrace{x\ldots x}_{n-3}bx] = b'$$

for some $b' \in B$. Since the element b was an arbitrary element of B, then

$$[\bar{x}\underbrace{x\ldots x}_{n-3}Bx] \subseteq B. \tag{7}$$

From (6) it follows also that $\theta_A(x)\theta_A(b)\theta_A^{-1}(x) \in B^*(A)$ for any $b \in B$, whence

$$[xB\underbrace{x\ldots x}_{n-3}\bar{x}] \subseteq B.$$

From the last inclusion it follows that

$$B \subseteq [\bar{x}\underbrace{x\ldots x}_{n-3}Bx]. \tag{8}$$

Then from (7) and (8) it follows

$$[\bar{x}\underbrace{x\ldots x}_{n-3}Bx] = B,$$

whence, taking in consideration Lemma 2, $x \in N_A(B)$. Then

$$u = \theta_A(x\underbrace{c\ldots c}_{i-1}) \in (N_A(B))^*(A),$$

whence

$$N_{A^*}(B^*(A)) \subseteq (N_A(B))^*(A). \tag{9}$$

From (5) and (9) the required equality follows. The theorem is proved.

By Theorem 2.2.19 [4] universal enveloping Post group N^* of an n-ary subgroup $< N, [\ ] >$ of an n-ary group $< A, [\ ] >$ is isomorphic to a subgroup $N^*(A)$ of universal enveloping Post group A^*. Therefore from Theorem 3 it follows

Corollary 3. *An universal enveloping Post group of a normalizer $< N_A(B), [\ ] >$ of n-ary subgroup $< B, [\ ] >$ in n-ary group $< A, [\ ] >$ is isomorphic to the normalizer of subgroup $B^*(A)$ in universal enveloping Post group A^*:*

$$(N_A(B))^* \simeq N_{A^*}(B^*(A)).$$

References

[1] Post E.L. *Polyadic groups.* Trans. Amer. Math. Soc., 1940, **48**, N 2, p. 208–350.

[2] Belousov V.D. *n-ary quasigroup.* Kishinev, Stiinta, 1972.

[3] Rusakov S.A. *Algebraic n-ary systems.* Minsk, Navuka i Tehnika, 1992.

[4] Gal'mak A.M. *n-ary groups.* Gomel', F. Skorina Gomel' State University, 2003.

[5] Gal'mak A.M. *Congruences of poliadic groups.* MInsk, Belarusskaya navuka, 1999.

Mogilev State University of Foodstuffs
Shmidt av. 3, 212027 Mogilev
Belarus
E-mail: *mti@mogilev.by*

Received April 18, 2005

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 71–87
ISSN 1024–7696

Loops of Bol-Moufang type with a subgroup of index two

M. K. Kinyon, J. D. Phillips, P. Vojtěchovský

Abstract. We describe all constructions for loops of Bol-Moufang type analogous to the Chein construction $M(G,*,g_0)$ for Moufang loops.

Mathematics subject classification: 20N05.
Keywords and phrases: Bol loop, Moufang loop, C-loop, loop $M(G,*,g_0)$, loops of Bol-Moufang type, loops with subgroup of index 2.

1 Introduction

Due to the specialized nature of this paper we assume that the reader is already familiar with the theory of quasigroups and loops. We therefore omit basic definitions and results (see [1],[6]).

In a sense, a nonassociative loop is closest to a group when it contains a subgroup of index two. Such loops proved useful in the study of Moufang loops, and it is our opinion that they will also prove useful in the study of other varieties of loops.

Here is the well-known construction of Moufang loops with a subgroup of index two:

Theorem 1.1 (Chein [3])**.** *Let G be a group, $g_0 \in Z(G)$, and $*$ an involutory antiautomorphism of G such that $g_0^* = g_0$, $gg^* \in Z(G)$ for every $g \in G$. For an indeterminate u, define multiplication $\circ$ on $G \cup Gu$ by*

$$g \circ h = gh, \quad g \circ (hu) = (hg)u, \quad gu \circ h = (gh^*)u, \quad gu \circ hu = g_0 h^* g, \tag{1}$$

where $g, h \in G$. Then $L = (G \cup Gu, \circ)$ is a Moufang loop. Moreover, L is associative if and only if G is commutative.

It has been shown in [9] that (1) is the only construction of its kind for Moufang loops. (This statement will be clarified later.) In [10], all constructions similar to (1) were determined for Bol loops.

The purpose of this paper is to give a complete list of all constructions similar to (1) for all loops of Bol-Moufang type. A groupoid identity is of *Bol-Moufang type* if it has three distinct variables, two of the variables occur once on each side, the third variable occurs twice on each side, and the variables occur in the same order on both sides. A loop is of *Bol-Moufang type* if it belongs to a variety of loops defined by

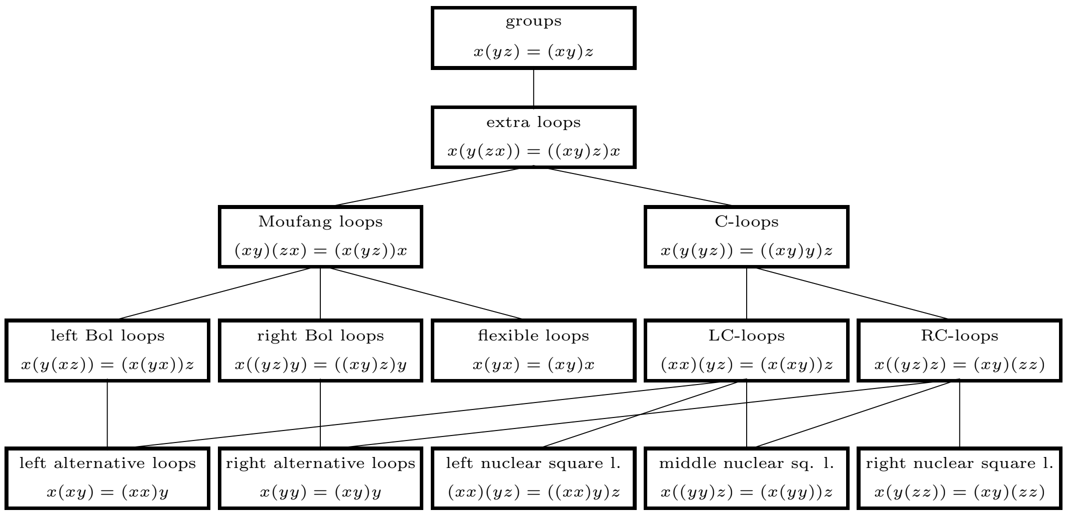


Figure 1. The varieties of loops of Bol-Moufang type.

a single identity of Bol-Moufang type. Figure 1 shows all varieties of loops of Bol-Moufang type and all inclusions among them (cf.[4],[8]). Some varieties of Figure 1 can be defined equivalently by other identities of Bol-Moufang type. For instance, Moufang loops are equivalently defined by the identity $x(y(xz)) = ((xy)x)z$. See [8] for all such equivalences. Furthermore, although some defining identities of Figure 1 do not appear to be of Bol-Moufang type, they are in fact equivalent to some Bol-Moufang identity. For instance, the flexible law $x(yx) = (xy)x$ is equivalent to the Bol-Moufang identity $(x(yx))z = ((xy)x)z$ in any variety of loops.

As we shall see, the computational complexity of our programme is overwhelming (for humans). We therefore first carefully define what we mean by a construction similar to (1) (see Section 2), and then identify situations in which two given constructions are "the same" (see Sections 3, 4, 5). Upon showing which constructions yield loops, we work out one construction by hand (see Section 6), and then switch to a computer search, described in Section 7. The results of the computer search are summarized in Section 8.

2 Similar Constructions

Throughout the paper, we assume that G is a finite group, $g_0 \in Z(G)$, and $*$ is an involutory automorphism of G such that $g_0^* = g_0$ and $gg^* \in Z(G)$ for every $g \in G$.

The following property of $*$ will be used without reference:

Lemma 2.1. *Let G be a group and $* : G \to G$ an involutory map such that $gg^* \in Z(G)$ for every $g \in G$. Then $g^*g = gg^* \in Z(G)$ for every $g \in G$.*

Proof. For $g \in G$, we have $g^*g = g^*(g^*)^* \in Z(G)$. Then $(g^*g)g^* = g^*(g^*g)$, and $gg^* = g^*g$ follows upon canceling g^* on the left. □

Consider the following eight bijections of $G \times G$:

$$\begin{array}{ll} \theta_{xy}(g,h) = (g,h), & \theta_{xy^*}(g,h) = (g,h^*), \\ \theta_{x^*y}(g,h) = (g^*,h), & \theta_{x^*y^*}(g,h) = (g^*,h^*), \\ \theta_{yx}(g,h) = (h,g), & \theta_{yx^*}(g,h) = (h,g^*), \\ \theta_{y^*x}(g,h) = (h^*,g), & \theta_{y^*x^*}(g,h) = (h^*,g^*). \end{array}$$

They form a group Θ under composition, isomorphic to the dihedral group D_8 (unless G or $*$ are trivial). It is generated by $\{\theta_{yx}, \theta_{xy^*}\}$, say. Let Θ_0 be the group generated by Θ and θ_{g_0}, where $\theta_{g_0}(g,h) = (g_0g,h)$.

Let $\Delta : G \times G \to G$ be the map $\Delta(g,h) = gh$, and u an indeterminate. Given α, β, γ, $\delta \in \Theta_0$, define multiplication $\circ$ on $G \cup Gu$ by

$$g \circ h = \Delta\alpha(g,h), \quad g \circ hu = (\Delta\beta(g,h))u, \quad gu \circ h = (\Delta\gamma(g,h))u, \quad gu \circ hu = \Delta\delta(g,h),$$

where g, $h \in G$. The resulting groupoid $(G \cup Gu, \circ)$ will be denoted by

$$Q(G, *, g_0, \alpha, \beta, \gamma, \delta),$$

or by $Q(G, \alpha, \beta, \gamma, \delta)$, when g_0, $*$ are known from the context or if they are not important. It is easy to check that $Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ is a quasigroup.

We also define

$$\mathcal{Q}(G, *, g_0) = \{Q(G, *, g_0, \alpha, \beta, \gamma, \delta) \mid \alpha,\ \beta,\ \gamma,\ \delta \in \Theta_0\},$$

and

$$\mathcal{Q}(G) = \bigcup_{*, g_0} \mathcal{Q}(G, *, g_0),$$

where the union is taken over all involutory antiautomorphisms $*$ satisfying $gg^* \in Z(G)$ for every $g \in G$, and over all elements g_0 such that $g_0^* = g_0 \in Z(G)$. By definition, we call elements of $\mathcal{Q}(G)$ *quasigroups obtained from* G *by a construction similar to* (1).

3 Reductions

The goal of this section is to show that one does not have to take all elements of Θ_0 into consideration in order to determine $\mathcal{Q}(G, *, g_0)$.

Note that $g_0^n = (g_0^n)^* \in Z(G)$ for every integer n. Therefore

$$g_0^n \Delta\theta_0(g,h) = \Delta\theta_{g_0}^n \theta_0(g,h) = \Delta\theta_0\theta_{g_0}^n(g,h) \tag{2}$$

for every $\theta_0 \in \Theta_0$ and every g, $h \in G$.

Lemma 3.1. *For every integer* n*, the quasigroup* $Q(G, \theta_{g_0}^n\alpha, \theta_{g_0}^n\beta, \theta_{g_0}^n\gamma, \theta_{g_0}^n\delta)$ *is isomorphic to* $Q(G, \alpha, \beta, \gamma, \delta)$.

Proof. We use (2) freely in this proof. Let $t = g_0^n$. Denote by $\circ$ the multiplication in $Q(G, \alpha, \beta, \gamma, \delta)$, and by $\bullet$ the multiplication in $Q(G, \theta_{g_0}^n\alpha,\ \theta_{g_0}^n\beta,\ \theta_{g_0}^n\gamma,\ \theta_{g_0}^n\delta)$. Let f be the bijection of $G \cup Gu$ defined by $g \mapsto t^{-1}g$, $gu \mapsto (t^{-1}g)u$, for $g \in G$. Then for g, $h \in G$, we have

$$f(g \circ h) = t^{-1}\Delta\alpha(g,h) = t\Delta\alpha(t^{-1}g, t^{-1}h) = t^{-1}g \bullet t^{-1}h = f(g) \bullet f(h),$$
$$f(g \circ hu) = t^{-1}\Delta\beta(g,h)u = t\Delta\beta(t^{-1}g, t^{-1}h)u = t^{-1}g \bullet (t^{-1}h)u = f(g) \bullet f(hu),$$

and similarly for γ, δ. Hence f is the desired isomorphism. □

Therefore, if we only count the quasigroups in $\mathcal{Q}(G, *, g_0)$ up to isomorphism, we can assume that $\mathcal{Q}(G, *, g_0) = \{Q(G, *, g_0, \alpha, \beta, \gamma, \delta) \mid \alpha \in \Theta$, and β, γ, δ are of the form $\theta\theta_{g_0}^n$ for some $n \in \mathbb{Z}$ and $\theta \in \Theta\}$.

Given a groupoid $(A, \cdot)$, the *opposite groupoid* $(A, \cdot^{\mathrm{op}})$ is defined by $x \cdot^{\mathrm{op}} y = y \cdot x$.

Lemma 3.2. *The quasigroups $Q(G, \alpha, \beta, \gamma, \delta)$ and $Q(G, \theta_{yx}\alpha,\ \theta_{yx}\gamma,\ \theta_{yx}\beta,\ \theta_{yx}\delta)$ are opposite to each other.*

Proof. Let $\circ$ denote the multiplication in $Q(G, \alpha, \beta, \gamma, \delta)$, and $\bullet$ the multiplication in $Q(G, \theta_{yx}\alpha,\ \theta_{yx}\gamma,\ \theta_{yx}\beta,\ \theta_{yx}\delta\}$. For g, $h \in G$ we have

$$\begin{aligned}
g \circ h &= \Delta\alpha(g,h) = \Delta\theta_{yx}\alpha(h,g) = h \bullet g,\\
g \circ hu &= \Delta\beta(g,h)u = \Delta\theta_{yx}\beta(h,g)u = hu \bullet g,\\
gu \circ h &= \Delta\gamma(g,h)u = \Delta\theta_{yx}\gamma(h,g)u = h \bullet gu,\\
gu \circ hu &= \Delta\delta(g,h) = \Delta\theta_{yx}\delta(h,g) = hu \bullet gu.
\end{aligned}$$

□

Therefore, if we only count the quasigroups in $\mathcal{Q}(G, *, g_0)$ up to isomorphism and opposites, we can assume that $\mathcal{Q}(G, *, g_0) = \{Q(G, *, g_0, \alpha, \beta, \gamma, \delta) \mid \alpha \in \{\theta_{xy},\ \theta_{xy^*},\ \theta_{x^*y},\ \theta_{x^*y^*}\}$, and β, γ, δ are of the form $\theta\theta_{g_0}^n$ for some $n \in \mathbb{Z}$ and $\theta \in \Theta\}$.

Assumption 3.3. From now on we assume that $\alpha \in \{\theta_{xy},\ \theta_{xy^*},\ \theta_{x^*y},\ \theta_{x^*y^*}\}$, and that β, γ, δ are of the form $\theta\theta_{g_0}^n$ for some $n \in \mathbb{Z}$ and $\theta \in \Theta$.

4 When $*$ is identical on G

Assume for a while that $g = g^*$ for every $g \in G$. Then $gh = (gh)^* = h^*g^* = hg$ shows that G is commutative. In particular, $\Theta = \{\theta_{xy}\}$, and $\Theta_0 = \bigcup_n \theta_{g_0}^n$. We show in this section that loops $Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ obtained with identical $*$ are not interesting.

Let ψ be a groupoid identity, and let $\operatorname{var}\psi$ be all the variables appearing in ψ. Assume that for every $x \in \operatorname{var}\psi$ a decision has been made whether x is to be taken from G or from Gu. Then, while evaluating each side of the identity ψ in $G \cup Gu$, we have to use the multiplications α, β, γ and δ a certain number of times.

Example 4.1. Consider the left alternative law $x(xy) = (xx)y$. With $x \in G$, $y \in Gu$, we see that we need β twice to evaluate $x \circ (x \circ y)$, while we need α once and β once to evaluate $(x \circ x) \circ y$.

A groupoid identity is said to be *strictly balanced* if the same variables appear on both sides of the identity the same number of times and in the same order. For instance $(x(y(xz)))(yx) = ((xy)x)(z(yx))$ is strictly balanced.

The above example shows that the same multiplications do not have to be used the same number of times even while evaluating a strictly balanced identity. However:

Lemma 4.2. *Let ψ be a strictly balanced identity. Assume that for $x \in \operatorname{var}\psi$ a decision has been made whether $x \in G$ or $x \in Gu$. Then, while evaluating ψ in $Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$, δ is used the same number of times on both sides of ψ.*

Proof. Let k be the number of variables on each side of ψ, with repetitions, whose value is assigned to be in Gu. The number k is well-defined since ψ is strictly balanced.

While evaluating the identity ψ, each multiplication reduces the number of factors by 1. However, only δ reduces the number of factors from Gu (by two). Since the coset multiplication in $G \cup Gu$ modulo G is associative, and since ψ is strictly balanced, either both evaluated sides of ψ will end up in G (in which case δ is applied $k/2$ times on each side), or both evaluated sides of ψ will end up in Gu (in which case δ is applied $(k-1)/2$ times on each side). $\square$

Lemma 4.3. *If $\alpha \in \Theta$ and $L = Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ is a loop, then the neutral element of Q coincides with the neutral element of G.*

Proof. Let e be the neutral element of L and 1 the neutral element of G. Since $1 = 1^*$, we have $1 \circ 1 = \Delta\alpha(1, 1) = 1 = 1 \circ e$, and the result follows from the fact that L is a quasigroup. $\square$

Proposition 4.4. *Assume that $g^* = g$ for every $g \in G$, and let α, β, γ, $\delta \in \Theta_0$. If $L = Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ happens to be a loop, then every strictly balanced identity holds in L. In particular, L is an abelian group.*

Proof. Since $*$ is identical on G, we have $\Theta_0 = \{\theta_{g_0}^n \mid n \in \mathbb{Z}\}$. By Assumption 3.3, we have $\alpha = \theta_{xy}$. Then by Lemma 4.3, L has neutral element 1. Assume that $\beta = \theta_{g_0}^n$ for some n. Then $gu = 1 \circ gu = (\Delta\beta(1, g))u = (g_0^n g)u$, which means that $n = 0$. Similarly, if $\gamma = \theta_{g_0}^m$ then $m = 0$.

Let $\delta = \theta_{g_0}^k$. Let ψ be a strictly balanced identity. For every $x \in \operatorname{var}\psi$, decide if $x \in G$ or $x \in Gu$. By Lemma 4.2, while evaluating ψ in L, the multiplication δ is used the same number of times on the left and on the right, say t times. Since $\alpha = \beta = \gamma = \theta_{xy}$, we conclude that ψ reduces to $g_0^{kt} z = g_0^{kt} z$, for some $z \in G \cup Gu$.

Since the associative law is strictly balanced, L is associative. We have already noticed that identical $*$ forces G to be abelian. Then L is abelian too, as $gu \circ h = (gh)u = (hg)u = h \circ gu$ and $gu \circ hu = g_0^k gh = g_0^k hg = hu \circ gu$ for every g, $h \in G$. $\square$

We have just seen that if $g = g^*$ for every $g \in G$ then our constructions do not yield nonassociative loops. Therefore:

Assumption 4.5. From now on, we assume that there exists $g \in G$ such that $g^* \neq g$.

5 Loops

In this section we further narrow the choices of α, β, γ, δ when $Q(G,\alpha,\beta,\gamma,\delta)$ is supposed to be a loop.

Proposition 5.1. *Let $L = Q(G,*,g_0,\alpha,\beta,\gamma,\delta)$. Then L is a loop if and only if $\alpha = \theta_{xy}$, $\beta \in \{\theta_{xy},\, \theta_{x^*y},\, \theta_{yx},\, \theta_{yx^*}\}$, $\gamma \in \{\theta_{xy},\, \theta_{xy^*},\, \theta_{yx},\, \theta_{y^*x}\}$, and δ is of the form $\theta\theta_{g_0}^n$ for some integer n and $g_0 \in G$.*

Proof. If L is a loop then $\alpha \in \{\theta_{xy},\, \theta_{xy^*},\, \theta_{x^*y},\, \theta_{x^*y^*}\}$ and Lemma 4.3 imply that 1 is the neutral element of L.

The equation $g = 1 \circ g$ holds for every $g \in G$ if and only if $\Delta\alpha(1,g) = g$ for every $g \in G$, which happens if and only if $\alpha \in \{\theta_{xy},\, \theta_{x^*y}\}$. (Note that we use Assumption 4.5 here.) Similarly, $g = g \circ 1$ holds for every $g \in G$ if and only if $\Delta\alpha(g,1) = g$ for every $g \in G$, which happens if and only if $\alpha \in \{\theta_{xy},\, \theta_{xy^*}\}$. Therefore $g = 1 \circ g = g \circ 1$ holds for every $g \in G$ if and only if $\alpha = \theta_{xy}$.

Now, $gu = 1 \circ gu$ holds for every $g \in G$ if and only if $\Delta\beta(1,g) = g$ for every $g \in G$, which happens if and only if $\beta \in \{\theta_{xy},\, \theta_{x^*y},\, \theta_{yx},\, \theta_{yx^*}\}$. Similarly, $gu = gu \circ 1$ holds for every $g \in G$ if and only if $\Delta\gamma(g,1) = g$ for every $g \in G$, which happens if and only if $\gamma \in \{\theta_{xy},\, \theta_{xy^*},\, \theta_{yx},\, \theta_{y^*x}\}$. $\square$

We are only interested in loops, and we have already noted that $(g_0^n)^* = g_0^n \in Z(G)$. Since we allow $g_0 = 1$, we can agree on:

Assumption 5.2. From now on, we assume that $\alpha = \theta_{xy}$, $\beta \in \{\theta_{xy},\, \theta_{x^*y},\, \theta_{yx},\, \theta_{yx^*}\}$, $\gamma \in \{\theta_{xy},\, \theta_{xy^*},\, \theta_{yx},\, \theta_{y^*x}\}$, and $\delta \in \theta_{g_0}\Theta$.

Our last reduction concerns the maps β and γ.

Lemma 5.3. *We have $\Delta\theta_{x^*y^*}\theta_0 = \Delta\theta_0\theta_{x^*y^*}$ for every $\theta_0 \in \Theta_0$.*

Proof. The group Θ_0 is generated by θ_{yx}, θ_{xy^*} and θ_{g_0}. It therefore suffices to check that $\Delta\theta_{x^*y^*}\theta_0 = \Delta\theta_0\theta_{x^*y^*}$ holds for $\theta_0 \in \{\theta_{yx},\, \theta_{xy^*},\, \theta_{g_0}\}$, which follows by straightforward calculation. $\square$

Lemma 5.4. *The quasigroups $Q(G,*,g_0,\alpha,\beta,\gamma,\delta)$, $Q(G,*,g_0,\alpha,\beta',\gamma',\theta_{x^*y^*}\delta)$ are isomorphic if*

$$\begin{aligned} \{\beta,\beta'\} &\in \{\{\theta_{xy},\theta_{yx^*}\},\, \{\theta_{yx},\theta_{x^*y}\}\},\\ \{\gamma,\gamma'\} &\in \{\{\theta_{xy},\theta_{y^*x}\},\, \{\theta_{yx},\theta_{xy^*}\}\}. \end{aligned}$$

Proof. Let $\circ$ denote the multiplication in $Q(G,*,g_0,\alpha,\beta,\gamma,\delta)$, and $\bullet$ the multiplication in $Q(G,*,g_0,\alpha,\beta',\gamma',\theta_{x^*y^*}\delta)$. Consider the permutation f of G defined by $f(g) = g$, $f(gu) = g^*u$, for $g \in G$.

We show that f is an isomorphism of $(G \cup Gu, \circ)$ onto $(G \cup Gu, \bullet)$ if and only if

$$(\Delta\beta(g,h))^* = \Delta\beta'(g,h^*), \quad (\Delta\gamma(g,h))^* = \Delta\gamma'(g^*,h). \tag{3}$$

Once we establish this fact, the proof is finished by checking that the pairs (β, β'), (γ, γ') in the statement of the Lemma satisfy (3).

Let g, $h \in G$. Then

$$\begin{aligned} f(g \circ h) &= f(\Delta\alpha(g,h)) = \Delta\alpha(g,h), \\ f(g \circ hu) &= f(\Delta\beta(g,h)u) = (\Delta\beta(g,h))^* u, \\ f(gu \circ h) &= f(\Delta\gamma(g,h)u) = (\Delta\gamma(g,h))^* u, \\ f(gu \circ hu) &= f(\Delta\delta(g,h)) = \Delta\delta(g,h), \end{aligned}$$

while

$$\begin{aligned} f(g) \bullet f(h) &= g \bullet h = \Delta\alpha(g,h), \\ f(g) \bullet f(hu) &= g \bullet h^* u = \Delta\beta'(g,h^*)u, \\ f(gu) \bullet f(h) &= g^* u \bullet h = \Delta\gamma'(g^*,h)u, \\ f(gu) \bullet f(hu) &= g^* u \bullet h^* u = \Delta\theta_{g^* h^*}\delta(g^*,h^*). \end{aligned}$$

We see that $f(g \circ h) = f(g) \bullet f(h)$ always holds. By Lemma 5.3, $f(gu \circ hu) = f(gu) \bullet f(hu)$ always holds. Finally, $f(g \circ hu) = f(g) \bullet f(hu)$, $f(gu \circ h) = f(gu) \bullet f(h)$ hold if and only if (β, β'), (γ, γ') satisfy (3). □

Assume that $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is a loop (satisfying Assumption 5.2). Then Lemma 5.4 provides an isomorphism of $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ onto some loop $Q(G, *, g_0, \theta_{xy}, \beta', \gamma', \delta')$ such that if $\gamma = \theta_{xy^*}$ then $\gamma' = \theta_{yx}$, and if $\gamma = \theta_{y^*x}$ then $\gamma' = \theta_{xy}$. We can therefore assume:

Assumption 5.5. From now on, we assume that $\alpha = \theta_{xy}$, $\beta \in \{\theta_{xy}, \theta_{x^*y}, \theta_{yx}, \theta_{yx^*}\}$, $\gamma \in \{\theta_{xy}, \theta_{yx}\}$, and $\delta \in \theta_{g_0}\Theta$.

In order to find all loops $Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ that satisfy a given groupoid identity ψ, we only have to consider $1 \cdot 4 \cdot 2 \cdot 8 = 64$ choices for $(\alpha, \beta, \gamma, \delta)$. (To appreciate the reductions, compare this with the unrestricted case α, β, γ, $\delta \in \Theta_0$.) Once $(\alpha, \beta, \gamma, \delta)$ is chosen, we must verify 2^k equations in G, where k is the number of variables in ψ (since each variable can be assigned value in G or in Gu).

We work out the calculation for one identity ψ and one choice of multiplication $(\alpha, \beta, \gamma, \delta)$. After seing the routine nature of the calculations, we gladly switch to a computer search.

6 C-loops arising from the construction of de Barros and Juriaans

C-loops are loops satisfying the identity $((xy)y)z = x(y(yz))$. In [2], de Barros and Juriaans used a construction similar to (1) to obtain loops whose loop algebras are flexible. In our systematic notation, their construction is

$$Q(G, *, g_0, \theta_{xy}, \theta_{xy}, \theta_{y^*x}, \theta_{g_0}\theta_{xy^*}), \tag{4}$$

with the usual conventions on g_0 and $*$. The construction (4) violates Assumption 5.5 but, by Lemma 5.4, it is isomorphic to

$$Q(G, *, g_0, \theta_{xy}, \theta_{yx^*}, \theta_{xy}, \theta_{g_0}\theta_{x^*y}),$$

which complies with all assumptions we have made.

Theorem 6.1. *Let G be a group and let L be the loop defined by (4). Then L is a flexible loop, and the following conditions are equivalent:*

(i) L is associative,

(ii) L is Moufang,

(iii) G is commutative.

Furthermore, L is a C-loop if and only if $G/Z(G)$ is an elementary abelian 2-group. When L is a C-loop, it is diassociative.

Proof. Throughout the proof, we use $g_0 = g_0^* \in Z(G)$, $gg^* = g^*g \in Z(G)$, $(g^*)^* = g$ and $(gh)^* = h^*g^*$ without warning.

By Proposition 5.1, L is a loop.

Flexibility. For x, $y \in G$ we have:

$$\begin{aligned}
&(x \circ y) \circ x = (xy)x = x(yx) = x \circ (y \circ x),\\
&(x \circ yu) \circ x = (xy)u \circ x = x^*xyu = xx^*yu = x \circ x^*yu = x \circ (yu \circ x),\\
&(xu \circ y) \circ xu = y^*xu \circ xu = g_0y^*xx^* = g_0xx^*y^* = xu \circ (yx)u = xu \circ (y \circ xu),\\
&(xu \circ yu) \circ xu = g_0xy^* \circ xu = g_0xy^*xu = xu \circ g_0yx^* = xu \circ (yu \circ xu).
\end{aligned}$$

Thus L is flexible.

Associativity. For x, y, $z \in G$ we have:

$$\begin{aligned}
&x \circ (y \circ z) = x(yz) = (xy)z = (x \circ y) \circ z,\\
&x \circ (y \circ zu) = x(yz)u = (xy)zu = (x \circ y) \circ zu,\\
&xu \circ (y \circ z) = xu \circ yz = z^*y^*xu = y^*xu \circ z = (xu \circ y) \circ z,\\
&x \circ (yu \circ zu) = x \circ g_0yz^* = g_0xyz^* = xyu \circ zu = (x \circ yu) \circ zu,\\
&xu \circ (yu \circ z) = xu \circ z^*yu = g_0xy^*z = g_0xy^* \circ z = (xu \circ yu) \circ z.
\end{aligned}$$

Furthermore,

$$\begin{aligned}
&x \circ (yu \circ z) = x \circ z^*yu = xz^*yu, \qquad (x \circ yu) \circ z = xyu \circ z = z^*xyu,\\
&xu \circ (y \circ zu) = xu \circ yzu = g_0xz^*y^*, \qquad (xu \circ y) \circ zu = y^*xu \circ zu = g_0y^*xz^*,\\
&xu \circ (yu \circ zu) = xu \circ g_0yz^* = g_0zy^*xu, \qquad (xu \circ yu) \circ zu = g_0xy^* \circ zu = g_0xy^*zu.
\end{aligned}$$

Thus L is associative if and only if G is commutative. (Sufficiency is obvious. For necessity, note that $*$ is onto, and substitute 1 for one of x, y, z if needed.)

Moufang property. Let x, y, $z \in G$. Then

$$x \circ (yu \circ (x \circ z)) = x \circ (yu \circ xz) = x \circ z^*x^*yu = xz^*x^*yu,$$
$$((x \circ yu) \circ x) \circ z = (xyu \circ x) \circ z = x^*xyu \circ z = z^*x^*xyu.$$

Therefore, this particular form of the Moufang identity holds if and only if $xz^*x^* = z^*x^*x$. Now, given x, $y \in G$, there is $z \in G$ such that $z^*x^* = y$. Therefore $xz^*x^* = z^*x^*x$ holds in G if and only if G is commutative. However, when G is commutative, then L is associative, and we have proved the equivalence of (i), (ii), (iii).

C property. Let x, y, $z \in G$. Then

$$\begin{aligned}
&x \circ (y \circ (y \circ z)) = x(y(yz)) = ((xy)y)z = ((x \circ y) \circ y) \circ z,\\
&x \circ (y \circ (y \circ zu)) = (x(y(yz))u = ((xy)y)z)u = ((x \circ y) \circ y) \circ zu,\\
&x \circ (yu \circ (yu \circ z)) = x \circ (yu \circ z^*yu) = x \circ g_0yy^*z = g_0xyy^*z = g_0xyy^* \circ z\\
&\qquad = (xyu \circ yu) \circ z = ((x \circ yu) \circ yu) \circ z,\\
&xu \circ (y \circ (y \circ z)) = xu \circ yyz = z^*y^*y^*xu = y^*y^*xu \circ z = (y^*xu \circ y) \circ z\\
&\qquad = ((xu \circ y) \circ y) \circ z,\\
&x \circ (yu \circ (yu \circ zu)) = x \circ (yu \circ g_0yz^*) = x \circ g_0zy^*yu = g_0xzy^*yu\\
&\qquad = g_0xyy^*zu = g_0xyy^* \circ zu = (xyu \circ yu) \circ zu = ((x \circ yu) \circ yu) \circ zu,\\
&xu \circ (yu \circ (yu \circ z)) = xu \circ (yu \circ z^*yu) = xu \circ g_0yy^*z = g_0z^*yy^*xu = g_0z^*xy^*yu\\
&\qquad = g_0xy^*yu \circ z = (g_0xy^* \circ yu) \circ z = ((xu \circ yu) \circ yu) \circ z,\\
&xu \circ (yu \circ (yu \circ zu)) = xu \circ (yu \circ g_0yz^*) = xu \circ g_0zy^*yu = g_0^2xy^*yz^*\\
&\qquad = g_0xy^*yu \circ zu = (g_0xy^* \circ yu) \circ zu = ((xu \circ yu) \circ yu) \circ zu.
\end{aligned}$$

While verifying the remaining form of the C identity, we obtain

$$xu \circ (y \circ (y \circ zu)) = xu \circ yyzu = g_0xz^*y^*y^*,$$
$$((xu \circ y) \circ y) \circ zu = (y^*xu \circ y) \circ zu = y^*y^*xu \circ zu = g_0y^*y^*xz^*.$$

The identity therefore holds if and only if y^*y^* commutes with all elements of G, which happens if and only if $G/Z(G)$ is an elementary abelian 2-group.

Finally, by Lemma 4.4 of [7], flexible C-loops are diassociative. □

7 The Algorithm

7.1 Collecting Identities

Let G be a group, ψ a groupoid identity and $(\alpha, \beta, \gamma, \delta)$ a multiplication. Then the following algorithm will output a set Ψ of group identities such that $Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ satisfies ψ if and only if G satisfies all identities of Ψ:

(i) Let $f : \operatorname{var}\psi \to \{0, 1\}$ be a function that decides whether $x \in \operatorname{var}\psi$ is to be taken from G or from Gu.

(ii) Upon assigning the variables of ψ according to f, let $\psi_f = (u, v)$ be the identity ψ evaluated in $Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$.

(iii) Let $\Psi = \{\psi_f \mid f : \operatorname{var}\psi \to \{0, 1\}\}$.

This algorithm is straightforward but not very useful, since it typically outputs a large number of complicated group identities.

7.2 Understanding the identities in the Bol-Moufang case

We managed to decipher the meaning of Ψ for all multiplications $(\alpha, \beta, \gamma, \delta)$ and for all identities of Bol-Moufang type by another algotihm. First, we reduced the identity $\psi_f = (u, v)$ to a canonical form as follows:

(a) replace g_0^* by g_0,

(b) move all g_0 to the very left,

(c) replace x^*x by xx^*,

(d) move all substrings xx^* immediately to the right of the power g_0^m, and order the substrings xx^*, yy^*, ... lexicographically,

(e) cancel as much as possible on the left and on the right of the resulting identity.

Then we used Lemmas 7.1–7.5 to understand what the canonical identities collected in Ψ say about the group G:

Lemma 7.1. *If an identity of Ψ reduces to $x^* = x$ then it does not hold in any group.*

Proof. This follows since we assume that $*$ is not identical on G. □

Lemma 7.2. *The following conditions are equivalent:*

(i) $G/Z(G)$ is an elementary abelian 2-group,

(ii) $xxy = yxx$,

(iii) $xyx^* = x^*yx$.

Proof. We have $xyx^* = x^*yx$ if and only if $x^*xyx^*x = x^*x^*yxx$. Since $x^*x \in Z(G)$, the latter identity is equivalent to $x^*xx^*xy = x^*x^*yxx$. Since $xx^* = x^*x$, we can rewrite it equivalently as $x^*x^*xxy = x^*x^*yxx$, which is by cancellation equivalent to $xxy = yxx$. □

Lemma 7.3. *The following conditions are equivalent:*

(i) G is commutative,

(ii) $xx^*y = x^*yx$.

Proof. If $xx^*y = x^*yx$ then $x^*xy = x^*yx$ and so $xy = yx$. □

Lemma 7.4. *If ψ is a strictly balanced identity that reduces to $xy = yx$ upon substituting 1 for some of the variables of ψ, then ψ is equivalent to commutativity.*

Proof. ψ implies commutativity. Once commutativity holds, we can rearrange the variables of ψ so that both sides of ψ are the same, because ψ is strictly balanced. □

Lemma 7.5. *The following conditions are equivalent:*

(i) $xxy = yx^*x^*$ *holds in* G,

(ii) $(xx)^* = xx$ *and* $G/Z(G)$ *is an elementary abelian* 2*-group.*

Proof. Condition (ii) clearly implies (i). If (i) holds, we have $xx = x^*x^*$ (with $y = 1$) and so $(xx)^* = xx$. Also $xxy = yx^*x^* = yxx$. □

7.3 What the identities mean in the Bol-Moufang case

Lemmas 7.1–7.5 are carefully tailored to loops of Bol-Moufang type, and we discovered them upon studying the canonical identities Ψ obtained by the computer search.

It just so happens that every identity ψ_f of Ψ is equivalent to a combination of the following properties of G:

(PN) No group satisfies ψ_f.

(PA) All groups satisfy ψ_f.

(PC) G is commutative.

(PB) $G/Z(G)$ is an elementary abelian 2-group.

(PS) $(gg)^* = gg$ for every $g \in G$.

A prominent example of $*$ is the inverse operation $^{-1}$ in G. Then (PB) says that G is of exponent 4, and it is therefore not difficult to obtain examples of groups satisfying any possible combination of (PN), (PA), (PC), (PB) and (PS).

We have implemented the algorithm in GAP [5], and made it available online at

`http://www.math.du.edu/~petr`

in section Research. The algorithm is not safe for identities that are not strictly balanced.

8 Results

We now present the results of the computer search. In order to organize the results, observe that if $L = Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ is associative, it satisfies all identities of Bol-Moufang type. Since we do not want to list the multiplications and properties of G repeatedly, we first describe all cases when L is associative, then all cases when L is an extra loop, then all cases when L is a Moufang loop, etc., guided by the inclusions of Figure 1.

All results of this section are computer generated. To avoid errors in transcribing, the TEX source of the statements of the results is also computer generated. In the statements, we write xy instead of θ_{xy}, g_0yx^* instead of $\theta_{g_0}\theta_{yx^*}$, etc., in order to save space and improve legibility. Some results are mirror versions of others (cf. Theorem 8.5 versus Theorem 8.6), but we decided to include them anyway for quicker future reference. Finally, when G is commutative, $\Delta(\Theta \cup \theta_{g_0}\Theta)$ coincides with $\Delta(S \cup \theta_{g_0}S)$, where $S = \{\theta_{xy},\ \theta_{xy^*},\ \theta_{x^*y},\ \theta_{x^*y^*}\}$. We therefore report only maps α, β, γ, δ from $S \cup \theta_{g_0}S$ in the commutative case.

In Theorems 8.1 – 8.14, G is a group, $*$ is a nonidentical involutory antiautomorphism of G satisfying $gg^* \in Z(G)$ for every $g \in G$, the element $g_0 \in Z(G)$ satisfies $g_0^* = g_0$, and the maps α, β, γ, δ are as in Assumption 5.5.

Theorem 8.1. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is associative iff the following conditions are satisfied:*

(β, γ, δ) is equal to
(xy, xy, g_0xy), or

G is commutative and (β, γ, δ) is equal to (x^*y, xy, g_0x^*y).

Theorem 8.2. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is extra iff it is associative or if the following conditions are satisfied:*

$G/Z(G)$ is an elementary abelian 2-group and (β, γ, δ) is equal to
(x^*y, yx, g_0yx^*).

Theorem 8.3. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is Moufang iff it is extra or if the following conditions are satisfied:*

(β, γ, δ) is equal to
(x^*y, yx, g_0yx^*).

Theorem 8.4. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is a C-loop iff it is extra or if the following conditions are satisfied:*

$G/Z(G)$ is an elementary abelian 2-group and (β, γ, δ) is among
(yx, yx, g_0yx), (yx^*, xy, g_0x^*y).

Theorem 8.5. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is left Bol iff it is Moufang or if the following conditions are satisfied:*

$G/Z(G)$ is an elementary abelian 2-group and (β,γ,δ) is among
(xy, yx, g_0yx), (x^*y, xy, g_0x^*y), or

G is commutative, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0x^*y), (x^*y, xy, g_0xy), or

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0x^*y), (xy, yx, g_0yx^*), (x^*y, xy, g_0xy), (x^*y, yx, g_0yx).

Theorem 8.6. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is right Bol iff it is Moufang or if the following conditions are satisfied:*

$G/Z(G)$ is an elementary abelian 2-group and (β,γ,δ) is among
(yx, xy, g_0yx), (yx^*, yx, g_0x^*y), or

G is commutative, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0xy^*), $(x^*y, xy, g_0x^*y^*)$, or

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0xy^*), $(x^*y, yx, g_0y^*x^*)$, (yx, xy, g_0y^*x), $(yx^*, yx, g_0x^*y^*)$.

Theorem 8.7. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is an LC-loop iff it is a C-loop or if the following conditions are satisfied:*

$G/Z(G)$ is an elementary abelian 2-group and (β,γ,δ) is among
(xy, yx, g_0yx), (x^*y, xy, g_0x^*y), (yx, xy, g_0xy), (yx^*, yx, g_0yx^*), or

G is commutative, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0x^*y), (x^*y, xy, g_0xy), or

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0x^*y), (xy, yx, g_0yx^*), (x^*y, xy, g_0xy), (x^*y, yx, g_0yx),
(yx, xy, g_0x^*y), (yx, yx, g_0yx^*), (yx^*, xy, g_0xy), (yx^*, yx, g_0yx).

Theorem 8.8. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is an RC-loop iff it is a C-loop or if the following conditions are satisfied:*

$G/Z(G)$ is an elementary abelian 2-group and (β,γ,δ) is among
(xy, yx, g_0xy), (x^*y, xy, g_0yx^*), (yx, xy, g_0yx), (yx^*, yx, g_0x^*y), or

G is commutative, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0xy^*), $(x^*y, xy, g_0x^*y^*)$, or

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^* = xx$ for every $x \in G$ and (β,γ,δ) is among
(xy, xy, g_0xy^*), (xy, yx, g_0xy^*), $(x^*y, xy, g_0y^*x^*)$, $(x^*y, yx, g_0y^*x^*)$,
(yx, xy, g_0y^*x), (yx, yx, g_0y^*x), $(yx^*, xy, g_0x^*y^*)$, $(yx^*, yx, g_0x^*y^*)$.

Theorem 8.9. *The loop $Q(G,*,g_0,\theta_{xy},\beta,\gamma,\delta)$ is flexible iff it is Moufang or if the following conditions are satisfied:*

(β,γ,δ) is among
$(xy,xy,g_0y^*x^*)$, (x^*y,yx,g_0xy^*), (x^*y,yx,g_0x^*y), (x^*y,yx,g_0y^*x),
$(yx,yx,g_0x^*y^*)$, (yx,yx,g_0yx), (yx^*,xy,g_0xy^*), (yx^*,xy,g_0x^*y),
(yx^*,xy,g_0yx^*), (yx^*,xy,g_0y^*x), *or*

$G/Z(G)$ is an elementary abelian 2-group and (β,γ,δ) is among
$(xy,xy,g_0x^*y^*)$, (xy,xy,g_0yx), (yx,yx,g_0xy), $(yx,yx,g_0y^*x^*)$.

Theorem 8.10. *The loop $Q(G,*,g_0,\theta_{xy},\beta,\gamma,\delta)$ is left alternative iff it is left Bol or an LC-loop or if the following conditions are satisfied:*

(β,γ,δ) is among
(xy,xy,g_0x^*y), (xy,yx,g_0yx^*), (x^*y,xy,g_0x^*y), (yx,xy,g_0x^*y),
(yx,yx,g_0yx^*), (yx^*,xy,g_0x^*y), (yx^*,yx,g_0yx^*), *or*

$(xx)^*=xx$ for every $x\in G$ and (β,γ,δ) is equal to
(x^*y,xy,g_0xy).

Theorem 8.11. *The loop $Q(G,*,g_0,\theta_{xy},\beta,\gamma,\delta)$ is right alternative iff it is right Bol or an RC-loop or if the following conditions are satisfied:*

(β,γ,δ) is among
(xy,xy,g_0xy^*), (xy,yx,g_0xy^*), (x^*y,xy,g_0yx^*), (yx,xy,g_0y^*x),
(yx,yx,g_0y^*x), (yx^*,xy,g_0x^*y), (yx^*,yx,g_0x^*y), *or*

$(xx)^*=xx$ for every $x\in G$ and (β,γ,δ) is equal to
$(yx^*,yx,g_0x^*y^*)$.

Theorem 8.12. *The loop $Q(G,*,g_0,\theta_{xy},\beta,\gamma,\delta)$ is a left nuclear square loop iff it is an LC-loop or if the following conditions are satisfied:*

(β,γ,δ) is among
(xy,xy,g_0xy^*), (yx^*,yx,g_0x^*y), $(yx^*,yx,g_0x^*y^*)$, *or*

$G/Z(G)$ is an elementary abelian 2-group and (β,γ,δ) is among
(xy,xy,g_0yx), (xy,xy,g_0y^*x), (xy,yx,g_0xy), (xy,yx,g_0xy^*),
(xy,yx,g_0y^*x), $(x^*y,xy,g_0x^*y^*)$, (x^*y,xy,g_0yx^*), $(x^*y,xy,g_0y^*x^*)$,
(x^*y,yx,g_0x^*y), $(x^*y,yx,g_0x^*y^*)$, $(x^*y,yx,g_0y^*x^*)$, (yx,xy,g_0xy^*),
(yx,xy,g_0yx), (yx,xy,g_0y^*x), (yx,yx,g_0xy), (yx,yx,g_0xy^*),
(yx,yx,g_0y^*x), $(yx^*,xy,g_0x^*y^*)$, (yx^*,xy,g_0yx^*), $(yx^*,xy,g_0y^*x^*)$,
$(yx^*,yx,g_0y^*x^*)$, *or*

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^*=xx$ for every $x\in G$ and (β,γ,δ) is among
$(xy,xy,g_0x^*y^*)$, (xy,xy,g_0yx^*), $(xy,xy,g_0y^*x^*)$, (xy,yx,g_0x^*y),
$(xy,yx,g_0x^*y^*)$, $(xy,yx,g_0y^*x^*)$, (x^*y,xy,g_0xy^*), (x^*y,xy,g_0yx),
(x^*y,xy,g_0y^*x), (x^*y,yx,g_0xy), (x^*y,yx,g_0xy^*), (x^*y,yx,g_0y^*x),

$(yx, xy, g_0x^*y^*)$, (yx, xy, g_0yx^*), $(yx, xy, g_0y^*x^*)$, (yx, yx, g_0x^*y), $(yx, yx, g_0x^*y^*)$, $(yx, yx, g_0y^*x^*)$, (yx^*, xy, g_0xy^*), (yx^*, xy, g_0yx), (yx^*, xy, g_0y^*x), (yx^*, yx, g_0xy), (yx^*, yx, g_0xy^*), (yx^*, yx, g_0y^*x).

Theorem 8.13. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is a middle nuclear square loop iff it is an LC-loop or an RC-loop or if the following conditions are satisfied:*

(β, γ, δ) is among
$(xy, xy, g_0y^*x^*)$, (yx^*, xy, g_0xy^*), (yx^*, xy, g_0yx^*), *or*

$G/Z(G)$ is an elementary abelian 2-group and (β, γ, δ) is among
$(xy, xy, g_0x^*y^*)$, (xy, xy, g_0yx), $(xy, yx, g_0x^*y^*)$, $(xy, yx, g_0y^*x^*)$, (x^*y, xy, g_0xy^*), (x^*y, xy, g_0y^*x), (x^*y, yx, g_0xy^*), (x^*y, yx, g_0x^*y), (x^*y, yx, g_0y^*x), $(yx, xy, g_0x^*y^*)$, $(yx, xy, g_0y^*x^*)$, (yx, yx, g_0xy), $(yx, yx, g_0x^*y^*)$, $(yx, yx, g_0y^*x^*)$, (yx^*, xy, g_0y^*x), (yx^*, yx, g_0xy^*), (yx^*, yx, g_0y^*x), *or*

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^* = xx$ for every $x \in G$ and (β, γ, δ) is among
(xy, xy, g_0yx^*), (xy, xy, g_0y^*x), (xy, yx, g_0x^*y), (xy, yx, g_0y^*x), $(x^*y, xy, g_0x^*y^*)$, (x^*y, xy, g_0yx), (x^*y, yx, g_0xy), $(x^*y, yx, g_0x^*y^*)$, (yx, xy, g_0xy^*), (yx, xy, g_0yx^*), (yx, yx, g_0xy^*), (yx, yx, g_0x^*y), (yx^*, xy, g_0yx), $(yx^*, xy, g_0y^*x^*)$, (yx^*, yx, g_0xy), $(yx^*, yx, g_0y^*x^*)$.

Theorem 8.14. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is a right nuclear square loop iff it is an RC-loop or if the following conditions are satisfied:*

(β, γ, δ) is among
(xy, xy, g_0x^*y), (x^*y, xy, g_0xy), (x^*y, xy, g_0x^*y), *or*

$G/Z(G)$ is an elementary abelian 2-group and (β, γ, δ) is among
(xy, xy, g_0yx), (xy, xy, g_0yx^*), (xy, yx, g_0x^*y), (xy, yx, g_0yx), (xy, yx, g_0yx^*), (x^*y, xy, g_0yx), (x^*y, yx, g_0xy), (x^*y, yx, g_0x^*y), (x^*y, yx, g_0yx), (yx, xy, g_0xy), (yx, xy, g_0x^*y), (yx, xy, g_0yx^*), (yx, yx, g_0xy), (yx, yx, g_0x^*y), (yx, yx, g_0yx^*), (yx^*, xy, g_0xy), (yx^*, xy, g_0yx), (yx^*, xy, g_0yx^*), (yx^*, yx, g_0xy), (yx^*, yx, g_0yx), (yx^*, yx, g_0yx^*), *or*

$G/Z(G)$ is an elementary abelian 2-group, $(xx)^* = xx$ for every $x \in G$ and (β, γ, δ) is among
$(xy, xy, g_0x^*y^*)$, (xy, xy, g_0y^*x), $(xy, xy, g_0y^*x^*)$, $(xy, yx, g_0x^*y^*)$, (xy, yx, g_0y^*x), $(xy, yx, g_0y^*x^*)$, (x^*y, xy, g_0xy^*), $(x^*y, xy, g_0x^*y^*)$, (x^*y, xy, g_0y^*x), (x^*y, yx, g_0xy^*), $(x^*y, yx, g_0x^*y^*)$, (x^*y, yx, g_0y^*x), (yx, xy, g_0xy^*), $(yx, xy, g_0x^*y^*)$, $(yx, xy, g_0y^*x^*)$, (yx, yx, g_0xy^*), $(yx, yx, g_0x^*y^*)$, $(yx, yx, g_0y^*x^*)$, (yx^*, xy, g_0xy^*), (yx^*, xy, g_0y^*x), $(yx^*, xy, g_0y^*x^*)$, (yx^*, yx, g_0xy^*), (yx^*, yx, g_0y^*x), $(yx^*, yx, g_0y^*x^*)$.

9 Concluding remarks

(I) Figure 1 and Theorems 8.1–8.14 taken together tell us more than if we consider them separately. For instance, Theorem 8.1 and Theorem 8.3 plus the fact that every group is a Moufang loop imply that the construction of Theorem 8.3 yields a nonassociative loop if and only if the group G is not commutative. In other words, the two theorems encompass Theorem 1.1, and, in addition, show that Chein's construction is unique for Moufang loops.

(II) Note that we have also recovered (an isomorphic copy of) the construction (4) of de Barros and Juriaans. Our results on Bol loops agree with those of [10], obtained by hand.

(III) To illustrate how the algorithm works for loops that are not of Bol-Moufang type, we show the output for nonassociative RIF loops. A loop is an *RIF loop* if it satisfies $(xy)(z(xy)) = ((x(yz))x)y$.

Theorem 9.1. *The loop $Q(G, *, g_0, \theta_{xy}, \beta, \gamma, \delta)$ is RIF iff it is associative or if the following conditions are satisfied:*

(β, γ, δ) is among
(x^*y, yx, g_0yx^*), (yx^*, xy, g_0x^*y), or

(β, γ, δ) and G are as in the following list:
(yx, yx, g_0yx) and $xyzxy = yxzyx$.

Note that the algorithm did not manage to decipher the meaning of the group identity $xyzxy = yxzyx$, so it simply listed it.

(IV) We conclude the paper with the following observation:

Lemma 9.2. *Let $L = Q(G, *, g_0, \alpha, \beta, \gamma, \delta)$ be a loop. Then L has two-sided inverses.*

Proof. Let $g \in G$. Since $g^*(g^{-1})^* = (g^{-1}g)^* = 1^* = 1$, we have $(g^*)^{-1} = (g^{-1})^*$, and the antiautomorphisms $^{-1}$ and $*$ commute. Let us denote $(g^{-1})^* = (g^*)^{-1}$ by g^{-*}.

We show that for every $\alpha \in \Theta_0$ and $g \in G$, there is $h \in G$ such that $\Delta\alpha(g, h) = g \circ h = 1 = h \circ g = \Delta\alpha(h, g)$. The proof for $gu \in Gu$ is similar.

Assume that $\alpha \in \{\theta_{xy}, \theta_{xy^*}, \theta_{x^*y}, \theta_{x^*y^*}\}$. Then

$$\begin{aligned}
\Delta\theta_{xy}(g, g^{-1}) &= gg^{-1} = 1 = g^{-1}g = \Delta\theta_{xy}(g^{-1}, g),\\
\Delta\theta_{xy^*}(g, g^{-*}) &= g(g^{-*})^* = 1 = g^{-*}g^* = \Delta\theta_{xy^*}(g^{-*}, g),\\
\Delta\theta_{x^*y}(g, g^{-*}) &= g^*g^{-*} = 1 = (g^{-*})^*g = \Delta\theta_{x^*y}(g^{-*}, g),\\
\Delta\theta_{x^*y^*}(g, g^{-1}) &= g^*g^{-*} = 1 = g^{-*}g^* = \Delta\theta_{x^*y^*}(g^{-1}, g)
\end{aligned}$$

show that the two-sided inverse h exists. The case $\alpha \in \{\theta_{yx}, \theta_{y^*x}, \theta_{yx^*}, \theta_{y^*x^*}\}$ is similar. The general case $\alpha \in \Theta_0$ then follows thanks to $g_0 = g_0^* \in Z(G)$. $\square$

References

[1] Bruck R.H. *A Survey of Binary Systems, third printing, corrected*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge **20**, Springer-Verlag, 1971.

[2] De Barros L.G.X., Juriaans S.O. *Some loops whose loop algebras are flexible II.* International Journal of Mathematics, Game Theory and Algebra **8**, N 1, p. 73–80.

[3] Chein O. *Moufang loops of small order*. Mem. Amer. Math. Soc., 1978, **13**, N 197.

[4] Fenyves F. *Extra loops II, On loops with identities of Bol-Moufang type*. Publ. Math. Debrecen, 1969, **16**, p. 187–192.

[5] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews (1999). (Visit http://www-gap.dcs.st-and.ac.uk/~gap).

[6] Pflugfelder H.O. *Quasigroups and Loops: Introduction*. Sigma series in pure mathematics, **7**, Heldermann Verlag Berlin, 1990.

[7] Phillips J.D., Vojtěchovský P. *On C-loops* (to appear in Publ. Math. Debrecen).

[8] Phillips J.D., Vojtěchovský P. *The varieties of loops of Bol-Moufang type* (to appear in Algebra Universalis).

[9] Vojtěchovský P. *On the uniqueness of loops $M(G,2)$*. Comment. Math. Univ. Carolin., 2003, **44**, N 4, p. 629–635.

[10] Vojtěchovský P. *A class of Bol loops with a subgroup of index two*. Comment. Math. Univ. Carolin., 2004, **45**, N 2, p. 371–381.

Received June 7, 2005

M. K. Kinyon
Department of Mathematical Sciences
Indiana University South Bend
South Bend, Indiana 46634
U.S.A.
E-mail: *mkinyon@iusb.edu*

J. D. Phillips
Department of Mathematics & Computer Science
Wabash College
Crawfordsville, Indiana 47933
U.S.A.
E-mail: *phillipj@wabash.edu*

P. Vojtěchovský
Department of Mathematics
University of Denver
2360 S Gaylord St
Denver, Colorado 80208
U.S.A.
E-mail: *petr@math.du.edu*

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 88–100
ISSN 1024–7696

On identities of Bol-Moufang type *

A. Pavlů, A. Vanžurová

Abstract. (Left) Bol loops are usually introduced as loops in which (left) Bol condition is satisfied, and the existence of the two-sided inverse of any element as well as the left inverse property are deduced. It appears that some of the assumptions on the structure are superflous and can be omitted, or modified. Also, Bol loops can be presented in various settings as far as the family of operation symbols is concerned. First we give a short survey on main known results on identities of Bol-Moufang type in quasigroups, written in a unified notation, and try to employ only multiplication and left division for the equational theory of left Bol loops. Then we propose a rather non-traditional concept of the variety of left Bol loops in type $(2,1,0)$, with operation symbols $(\cdot, {}^{-1}, e)$ and with five-element defining set of identities, namely $xe = ex = x$, $(x^{-1})^{-1} = x$, $x^{-1}(xy) = y$, $x(y(xz)) = (x(yx))z$.

Mathematics subject classification: 20N05.
Keywords and phrases: Groupoid, variety of algebras, quasigroup, loop, Bol identity, Moufang identity.

1 Preliminaries

The set of all terms over an alphabet X is denoted $T_{(\tau)}(X)$. If $\mathcal{A} = (A; F)$ is an algebra with the carrier set A and the sequence $F = (f_i)_{i\in I}$ of operation symbols, and $\tilde{F} = (f_i)_{i\in\tilde{I}}$, $\tilde{I} \subset I$, a subsequence of the sequence F of operation symbols then $\tilde{\mathcal{A}} = (A; \tilde{F})$ is called a *reduct* of $\mathcal{A}$. $\underline{V}$ denotes a class of algebras defined by identities, i.e. a variety of algebras, and we write $\underline{V} = Mod(\Sigma)$ if Σ is the defining set of identities for $\underline{V}$. We will distinguish graphically between identities in a variety and equalities between elements in a particular algebra.

An algebra with one binary operation (of type $\tau = (1)$) is called a *groupoid* here, [4]. (The terminology varies in this respect. In [11] and in [10, p. 23] *magma* is used, and 1970' edition of N. Bourbaki's *Algebra* is mentioned as the first source. In [19], magma means a groupoid with two-sided neutral element.)

Convention. We use a common convention of nonassociative algebra that the symbol of binary operation can be omitted (to save space and brackets in formulas); if $\cdot$ is used it plays the role of parentheses, i.e. indicates priority of the "non-dotted" multiplication, or other operation.

Given a groupoid $(A; \cdot)$ and $a \in A$ then $L_a : A \to A$, $x \mapsto ax$ denotes the left translation by an element a, similarly $R_a : x \mapsto ax$ denotes the right translation by a. An element e of a groupoid $\mathcal{A} = (\mathcal{A}; \cdot)$ is called a *right* (respectively *left*, respectively

*Supported by grant No201/05/2707 of The Grant Agency of Czech Republic.

two-sided) *neutral element* of $\mathcal{A}$ if for all elements $a \in A$, $ae = a$ (respectively $ea = a$, respectively both equalities) hold(s). The following easy observation is useful:

If e' is a left and e a right neutral element of $\mathcal{A}$ they coincide, $e' = e'e = e$.

If "$\circ$" is a binary operation on the carrier set A then so is its *dual* (opposite) operation $\tilde{\circ} : A \to A$, $(a, b) \mapsto a\tilde{\circ}b := b \circ a$. The groupoid $\tilde{\mathcal{A}} = (A, \tilde{\circ})$ is *dual* (opposite)[1] to $\mathcal{A} = (A, \circ)$, and left (right) translations of $\tilde{\mathcal{A}}$ ($\mathcal{A}$). If an identity is satisfied in $(A, \circ)$ then its *dual* ("mirror") is this same identity in $\tilde{\mathcal{A}} = (A, \tilde{\circ})$ (that is, "$\tilde{\circ}$" replaces "$\circ$" in each occurance), rewritten into an identity in $(A, \circ)$ [10, p. 2]. A groupoid $\mathcal{B}$ is *antiisomorphic* to $\mathcal{A}$ if it is isomorphic to $\tilde{\mathcal{A}}$. The advantage of dualisation is obvious: it saves space and time. If something is proven for an algebraic structure (which is not "self-dual"), the dual ("mirror") proof must clearly work for the dual structure, and it is sufficient to study one of both theories.

1.1 Quasigroups, one-sided and two-sided equasigroups. Quasigroups (in the "usual" sense) form a historically important class of groupoids in which groups can be considered as a subclass. A (two-sided) quasigroup is often characterized as a groupoid $\mathcal{A} = (A; \cdot)$ such that the following "quasigroup property" (Q) is satisfied, [16]:

(Q) the maps $L_a : A \to A$ and $R_a : A \to A$ are bijections for all $a \in A$.

Equivalently, for each of the equations $a \cdot x = b$, $y \cdot a = b$ with $a, b \in A$, there exists a uniquely determined solution in A, $x \in A$ or $y \in A$, respectively [4, 14]. Another speaking, for any triple of elements a, b, c from A such that $a \cdot b = c$, each couple of them determines the third one in A uniquely. Such a characterization might be sufficient in many aspects, but makes troubles in the infinite case as far as congruence relations, quotient algebras and homomorphisms are concerned. If a homomorphic image $\mathcal{A}'$ of a quasigroup $\mathcal{A}$ (in the above sense) is finite, or associative, then $\mathcal{A}'$ is a quasigroup. But there are infinite examples of groupoids (even loops) with the above "quasigroup property" (Q) admitting homomorphic maps onto (neither finite nor associative) groupoids in which (Q) fails, i.e. the image is no quasigroup [1, p. 1182–1183]. That is why the so called equasigroups were introduced (see [6]) defined via identities, i.e. forming a variety (see [7]) (primitive quasigroups in the sense of [2]). We prefer to keep the outline of an equational theory here.

Under a *left quasigroup* we will understand an algebra $(A; \cdot, \backslash)$ of type $(2, 2)$ in which the following identities hold (that guarantee existence and unicity of the solution):

$$(Q1_l): \quad x(x\backslash y) \approx y, \qquad (Q2_l): \quad x\backslash(xy) \approx y.$$

Left quasigroups form the variety $\underline{LQ} = Mod(\{(Q1_l), (Q2_l)\})$ in type $(2, 2)$, and an algebra $(A; \cdot, \backslash)$ belongs to $\underline{LQ}$ if and only if in the groupoid $(A; \cdot)$, the equations of the form $a \cdot u = b$ are uniquely solvable in A for any $a, b \in A$, with $u = a\backslash b$.

[1] sometimes also denoted by $\mathcal{A}^{\mathrm{op}}$

Similarly, we can introduce mirrors of $(Q1_l)$, $(Q2_l)$

$$(Q1_r): \quad (y/x)x \approx y, \qquad (Q2_r): \quad (yx)/x \approx y,$$

the variety of right quasigroups in type $(2,2)$ with operation symbols $(\cdot, /)$, $\underline{RQ} = Mod(\{(Q1_r),(Q2_r)\})$, and to give a dual characterization. Each left (right) quasigroup is left (right) cancellative, that is satisfies the following quasi-identity:

$(C_l) \qquad xz = xz' \Longrightarrow z = z' \qquad (left\ cancellation)$

respectively

$(C_r) \qquad zx = z'x \Longrightarrow z = z' \qquad (right\ cancellation).$

In fact, if $\mathcal{Q} = (Q; \cdot, \backslash) \in \underline{LQ}$ and $ab = ab'$ for $a, b, b' \in Q$ then $a\backslash ab = a\backslash ab'$. Applying $(Q2_l)$ we obtain $b = b'$ (and the dual proof works for right quasigroups).

We prefer "left" structures here.

If in a left quasigroup $\mathcal{Q} \in \underline{LQ}$, $q\backslash q = p\backslash p$ holds for any $p, q \in Q$, then the common value $e = q\backslash q$ is a right neutral element of $\mathcal{Q}$.

A *quasigroup* ("equasigroup") is an algebra $\mathcal{A} = (\mathcal{A}; \cdot, \backslash, /)$ of type $(2,2,2)$ satisfying all of $(Q1_l)$, $(Q2_l)$, $(Q1_r)$, $(Q2_r)$ (and $\mathcal{A} \in \underline{Q}$ iff equations of both types are solved uniquely in A), [7, 24], i.e. the reduct $(A; \cdot, \backslash)$ is a left quasigroup, and the reduct $(A; \cdot, /)$ is a right one). Obviously, quasigroups are left and right cancellative (equivalently, all left and right translations are bijections on A).

In the variety of quasigroups $\underline{Q} = Mod(\{(Q1_l), (Q2_l), (Q1_r), (Q2_r)\})$, the following identities are consequences of the defining ones:

$$(Q3): \qquad y/(x\backslash y) \approx x, \qquad\qquad (Q4): \qquad (y/x)\backslash y \approx x.$$

If a quasigroup possesses a neutral element we speak about a *loop*. If this is the case, we can identify e with a new nullary operation $e : \{\emptyset\} \to A$, $\emptyset \mapsto e$. Let us consider the following identities:

$$(U_r): \qquad xe \approx x, \qquad\qquad (U_l): \qquad ex \approx x,$$

$(AS) \qquad x(yz) \approx (xy)z \qquad$ (associativity),

$(CO) \qquad xy \approx yx \qquad$ (commutativity).

Associative groupoids are called *semigroups*. Commutative associative quasigroups are also called *abelian*.

1.2 Groups as quasigroups. It is well known that a *group* can be regarded as a quasigroup $\mathcal{G} = (\mathcal{G}; \cdot, \backslash, /)$ for which the reduct $(G; \cdot)$ is a semigroup (satisfies (AS)), [14, Chap. II], [4, p. 28], and that in the variety of "groups" in type $(2,2,2)$, $\underline{G'} = Mod(\{(Q1_l),(Q2_l),(Q1_r),(Q2_r),(AS)\})$, the following identities hold:

$$x/x \approx y/y, \qquad x\backslash x \approx y\backslash y, \qquad x/x \approx x\backslash x,$$

i.e. a uniquely determined neutral element is present in any $\mathcal{G} \in \underline{\mathcal{G}'}$, and $\mathcal{G}$ can be regarded as an associative loop.

1.3 Loops. A *loop* is often considered as "usual" quasigroup $(Q,\cdot)$, i.e. satisfying (Q), endowed with an identity element. For our purpose, let us consider a *variety of loops* $\underline{L}$ of type $(2,2,2,0)$ with the sequence of operation symbols $(\cdot,\backslash,/,e)$ as

$$\underline{L} = Mod(\{(Q1_l),(Q2_l),(Q1_r),(Q2_r),(U_r),(U_l)\});$$

now a *loop* $\mathcal{L} = (\mathcal{Q};\cdot,\backslash,/,\rceil)$ will be an algebra belonging to the variety $\underline{L}$. Obviously, a reduct $(Q;\cdot,\backslash,/)$ of $\mathcal{L}$ is in $\underline{Q}$. Denote by $\underline{Gr}$ the subvariety of $\underline{L}$ determined by the additional identity (AS).

It is also reasonable to consider *left loops* with two-sided neutral element in type $(2,2,0)$ with operation symbols $(\cdot,\backslash,e)$ as elements from the variety

$$\underline{LL} = Mod(\{(Q1_l),(Q2_l),(U_r),(U_l)\})$$

and similarly *right loops* with two-sided neutral element and operation symbols $(\cdot,/,e)$ as elements from

$$\underline{RL} = Mod(\{(Q1_r),(Q2_r),(U_r),(U_l)\}).$$

Associativity is rather a strong property. Many kinds of "weak" associativity are studied in quasigroups, e.g. [8, 9, 12, 13, 17, 21, 22], as well as in the varieties $\underline{L}$, $\underline{LL}$ or $\underline{RL}$, respectively.

2 Identities of Bol-Moufang type in quasigroups

2.1 Identities of Bol-Moufang type. An identity $s \approx t$ where $s,t \in T_{(2)}(X)$ are binary terms, is said to be *of Bol-Moufang type* if the number of distinct variables occuring in s as well as in t is three, the total number of variables appearing in s is four, the same for t, and the order in which the variables appear in s is exactly the same as the order of these variables in the term t [17]. Historically, some of these identities have been discovered in connection with geometric closure conditions in webs.

2.2 Left Bol quasigroups. A (two-sided) quasigroup satisfying the so-called left Bol identity

(B_l) $\quad x(y(xz)) \approx (x(yx))z$

is called a *left Bol quasigroup* (after Geritt Bol [3]). Similarly, *right Bol quasigroups* satisfy its dual, the so called right Bol identity

(B_r) $\quad ((zx)y)x \approx z((xy)x).$

Both theories are "mirror-symmetric" to each other, we prefer here the variety of left Bol quasigroups in type $(2,2,2)$

$$\underline{LBQ} = Mod(\{(Q1_l),(Q2_l),(Q1_r),(Q2_r),(B_l)\}).$$

Note that the mirror variety $\underline{RBQ}$ of right Bol quasigroups was investigated in [22].

Lemma 2.1 [22]. *Let $(A;\cdot,\backslash,/)$ be a left (right) Bol quasigroup. Then $(A;\cdot)$ has a unique right (respectively left) neutral element satisfying (U_r) (respectively (U_l)).*

Proof. Let $a \in A$ be a fixed element of a left Bol quasigroup. For any $b \in A$, $b(a\backslash a) \underset{(Q1_l)}{=} (a \cdot (a\backslash b)) \cdot (a\backslash a) \underset{(Q1_r)}{=} (a \cdot [((a\backslash b)/a) \cdot a]) \cdot (a\backslash a) \underset{(B_l)}{=} a((a\backslash b)/a) \cdot (a \cdot (a\backslash a))) \underset{(Q1_l)}{=} a(((a\backslash b)/a) \cdot a) \underset{(Q1_r)}{=} a(a\backslash b) \underset{(Q1_l)}{=} b$. So, indeed, $a\backslash a$ is right neutral, and (U_r) holds. Unicity follows from $b(a\backslash a) = b = b(c\backslash c)$, $c \in A$ by (C_l). Similarly for right Bol quasigroups. □

In any algebra $\mathcal{A} \in \underline{\mathcal{LBQ}}$, a new nullary operation $e^{\mathcal{A}}$ satisfying (U_r) can be introduced by $e^{\mathcal{A}} : \{\emptyset\} \to A$, $e^{\mathcal{A}}(\emptyset) = e \in A$, and a Bol quasigroup $\mathcal{A}$ can be regarded as a reduct of the algebra $\mathcal{A}' = (A;\cdot,\backslash,/,e)$ of type $(2,2,2,0)$ from the variety $\underline{LBQ'} = Mod(\{(Q1_l),(Q2_l),(Q1_r),(Q2_r),(U_r),(B_l)\})$ (of left Bol quasigroups with right neutral element). Consequently, in the variety $\underline{LBQ}$ (as well as in $\underline{LBQ'}$), the identity $x\backslash x \approx y\backslash y$ holds. (Analogously for the varieties of right Bol quasigroups $\underline{RBQ}$ and $\underline{RBQ'}$.)

Corollary 2.2. *Each Bol quasigroup (belonging to $\underline{LBQ}$, $\underline{LBQ'}$, $\underline{RBQ}$, or to $\underline{RBQ'}$) satisfies*

(H) $(xx)x \approx x(xx)$ *(monoassociativity).*

Proof. In the left Bol case, we use (B_l) with $y = x$, $z = e$, and (U_r). □

If the right neutral element of a left Bol quasigroup is two-sided, i.e. satisfies $xe = ex = x$ for all x, the quasigroup is left alternative: setting $y = e$ in (B_l) we get $x(xz) = (xx)z$.

Note that a groupoid $\mathcal{A}$ is said to have the *left inverse property*, or is a LIP-groupoid, if for each $a \in A$ there is at least one $a' \in A$ such that $a'(ac) = c$ for every $c \in A$ [4, p. 111]. The right case is mirror again.

In a Bol quasigroup, each element has a (unique) two-sided inverse, and left (right) Bol quasigroups have left (right) inverse property:

Lemma 2.3 [22]. *In $\underline{LBQ'}$ the following identities hold:*

lip $(e/x) \cdot (xy) \approx y$ *(left inverse property),*
lip‴ $x \cdot ((x\backslash e)y) \approx y$,
bi $e/x \approx x\backslash e$ *(two-sided inverse),*
lip″ $(x\backslash e) \cdot (xy) \approx y$,
lip′ $x \cdot ((e/x)y) \approx y$,

Proof. Let us evaluate $x((e/x) \cdot (xy)) \underset{(B_l)}{\approx} [x((e/x) \cdot x)]\, y \underset{(Q1_r)}{\approx} (xe)y \underset{(U_r)}{\approx} xy$. By left cancellation we obtain (lip). Similarly, $(x\backslash e) \cdot (x \cdot ((x\backslash e)y)) \underset{(B_l)}{\approx} [(x\backslash e)(x \cdot (x\backslash e))]\, y \underset{(Q1_l)}{\approx} ((x\backslash e) \cdot e)y \underset{(U_r)}{\approx} (x\backslash e)y$, and (C_l) gives (lip'''). Let $\mathcal{A} \in \underline{\mathcal{LBQ}'}$ have the right neutral element e. For $a \in A$, $((e/a)(a \cdot e/a))a = (e/a) \cdot (a(e/a \cdot a)) = e/a \cdot (ae) = e/a \cdot a$. According to (C_r), $(e/a) \cdot (a(e/a)) = e/a = (e/a)e$, and we obtain $a(e/a) = e$ by (C_l). Since also $a(a\backslash e) = e$ holds it must be $e/a = a\backslash e$ again by (C_l). The rest is a consequence. □

Hence for every (left) Bol quasigroup $\mathcal{B} \in \underline{\mathcal{LBQ}'}$, it is natural to introduce for any $b \in B$ an element $b^{-1} =: e/b = b\backslash e$, a both-sided inverse. In this way, a new unary operation $b \mapsto b^{-1}$ of "inverting" arises (on the carrier set B) satisfying $b^{-1}(bc) = c$ and $b(b^{-1}c) = c$ for all $b, c \in B$ ($\mathcal{B}$ has the left inverse property, is a LIP-quasigroup). Analogously, the same construction works for right Bol quasigroups, and $(cb)b^{-1} = (cb^{-1})b = c$ holds for all $b, c \in B$ (right Bol quasigroups have the right inverse property).

2.3 Moufang quasigroups (are loops). A bit stronger "weak associativity" conditions are conditions of Moufang type (after Ruth Moufang). Consider the following pairs of identities:

$$(M1): \quad (xy)(zx) \approx (x(yz))x, \qquad (N1): \quad ((zx)y)x \approx z(x(yx)),$$

$$(M2): \quad x((yz)x) \approx (xy)(zx), \qquad (N2): \quad ((xy)x)z \approx x(y(xz)).$$

Each of the identities is a mirror of the other one on the same row. By results of Bol and Bruck [3], [4, p. 115] all four identities are equivalent in the variety of loops. By results of [12], they are in fact equivalent even in the variety $\underline{Q}$ of quasigroups.

Call a quasigroup *Moufang* if it satisfies $(M1)$, and denote by $\underline{MQ}$ the variety of all Moufang quasigroups. If $\mathcal{Q}$ is a Moufang quasigroup let us choose a fixed $a \in Q$. Then $e =: a\backslash a$ is a left neutral element. In fact, for every $b \in Q$, $(ba)b = (b(a \cdot a\backslash a))b = (ba)(a\backslash a \cdot b)$, and $a\backslash a \cdot b = b$ follows by left cancellation. Similarly, $f =: (a\backslash a)/(a\backslash a)$ is a right neutral element since $[b((a\backslash a)/(a\backslash a)] \cdot (a\backslash a) = (a\backslash a)[[b((a\backslash a)/(a\backslash a)] \cdot (a\backslash a)] = [(a\backslash a)b][(a\backslash a)/(a\backslash a) \cdot (a\backslash a)] = b \cdot (a\backslash a)$. Now using (C_r) we conclude

Lemma 2.4 [12]. *Every Moufang quasigroup has an identity element e (and therefore can be regarded as a reduct of a Moufang loop).*

For quasigroups satisfying $(M2)$, a mirror proof of the same statement can be easily given. To prove that every quasigroup satisfying $(N1)$ (or $(N2)$, respectively) has a two-sided neutral element is rather more complicated, [12, p. 233].

Lemma 2.5. *Moufang quasigroups are left and right alternative and elastic, that is satisfy*

(ALT_l)	$(xx)y \approx x(xy)$	*(left alternativity),*
(ALT_r)	$(yx)x \approx y(xx)$	*(right alternativity),*
$(FLEX)$	$(xy)x \approx x(yx)$	*(flexibility, elasticity).*

Proof. From $(N2)$ with $y = e$ and (U_r), $(xx)z = x(xz)$. From $(N1)$ with $y = e$, (U_l) and (U_r), $(zx)x = z(xx)$. From $(N1)$ with $z = e$ and (U_l) (or from $(N2)$ with $z = e$ and (U_r)), $(xy)x = x(yx)$. □

Note that if a groupoid satisfies a left Bol identity and possesses a two-sided neutral element then it is left alternative.

Every Moufang quasigroup is at the same time left and right Bol quasigroup:

Lemma 2.6. *The variety $\underline{MQ}$ is a subvariety in $\underline{LBQ}$ as well as in $\underline{RBQ}$.*

Proof. In $\underline{MQ}$, the identity (B_l) is a consequence of $(N2)$ and $(FLEX)$ since

$$(x(yx))z \underset{(FLEX)}{\approx} ((xy)x)z \underset{(N2)}{\approx} x(y(xz)),$$

and (B_r) is a consequence of (N_1) and $(FLEX)$,

$$z((xy)x) \underset{(FLEX)}{\approx} z(x(yx)) \underset{(N1)}{\approx} ((zx)y)x. \qquad \square$$

Hence in every Moufang quasigroup each element has a (unique) both-sided inverse, and both left and right inverse properties are satisfied.

Due to (AS), $\underline{G'}$ is a subvariety in $\underline{MQ}$. Now it is apparent that in each $\mathcal{G} \in \underline{G'}$ there is a (unique) identity element e satisfying (U_r), (U_l), and each $g \in G$ has a (unique) both-sided inverse $g^{-1} := e/g = g\backslash e$. More often, we take $(\cdot, ^{-1}, e)$ as fundamental operations for groups.

3 Bol and Moufang loops

3.1 Left Bol loops. Left Bol loops are usually considered as a subvariety

$$\underline{LBL} = Mod(\{(Q1)_l, (Q2)_l, (Q1)_r, (Q2)_r, (U_r), (U_l), (B_l)\})$$

determined in $\underline{L}$ by the identity (B_l) (and belonging also to Bol quasigroups with right unit). Similarly, the subvariety $\underline{RBL}$ of right Bol loops is distinguished by the additional condition (B_r), and has mirror properties [20].

Lemma 3.1 [20]. *In the variety $\underline{LBL}$ of (left) Bol loops the following identities hold: (H), (lip), (lip'), (bi), (ALT_l),*

(inv) $\quad e/(e/x) \approx x, \qquad (x\backslash e)\backslash e \approx x,$

(sa) $\quad (x(yx))\backslash e \approx (x\backslash e) \cdot (y\backslash e \cdot x\backslash e)$ $\quad$ *(semiautomorphic inverse).*

Proof. The first part was already proven. Left alternativity is an immediate consequence of (B_l) and (U_l) if we set $y = e$ and $z = y$, $x(xy) \approx x(e(xy)) \approx (x(ex))y \approx (xx)y$ (and monoassociativity follows for $y = x$). From (bi), $e/(e/x) \approx e/(x\backslash e) \underset{(Q3)}{\approx} x$. Now $(x(yx)) \cdot [(x\backslash e) \cdot (y\backslash e \cdot x\backslash e)] \underset{(Q3)}{\approx} x(y(x(x\backslash e(y\backslash e \cdot x\backslash e))) \underset{(lip')}{\approx} x(y(y\backslash e \cdot x\backslash e)) \underset{(lip')}{\approx} x(x\backslash e) \underset{(Q1_l)}{\approx} e$ which is equivalent to (sa). $\square$

In the more usual notation, $x^{-1}(xy) = y$, $x(x^{-1}y) = y$, $(x^{-1})^{-1} = x$, and $(x(yx))^{-1} = x^{-1}(y^{-1}x^{-1})$. Further, $x^{-1}x = xx^{-1} = e$ due to $(Q1_l)$, $(Q1_r)$.

3.2 Moufang loops. The variety of Moufang loops $\underline{ML}$ is introduced as the subvariety of $\underline{L}$ satisfying the identity of Moufang $(N2)$ (or equivalently, any one of the identities $(M1)$, $(M2)$, $(N1)$ [4, 12]), and $\underline{ML}$ is exactly a common part of $\underline{LBL}$

and $\underline{RBL}$. It can be easily checked that a left Bol loop is Moufang if and only if it is elastic, or equivalently, if and only if is right alternative:

Lemma 3.2 [2, p. 105, 1]. *In $\underline{L}$, a pair of identities (B_l), $(FLEX)$ is equivalent to $(N2)$, and a pair of identities (B_r), $(FLEX)$ is equivalent to $(N1)$.*

Lemma 3.3 [2, p. 105, 5]. *In the variety $\underline{L}$ of loops, a couple of identities (B_l), (ALT_r) is equivalent to $(N2)$, and a couple (B_r), (ALT_l) of identities is equivalent to $(N1)$.*

Proof. Let $\mathcal{B}$ be a Bol loop satisfying (ALT_r). Let us show that $\mathcal{B}$ is also elastic. Let $a, c \in B$. Then (B_l) with $x = z =: a$ and $y =: c$ and (ALT_r) give $(a(ca))a = a(c(aa)) = a((ca)a)$. Now let a, $b \in B$ be arbitrary elements. Then $(ab)a = (a((b/a) \cdot a))a = a(((b/a) \cdot a)a) = a(ba)$, that is, $(FLEX)$ holds in $\mathcal{B}$. Hence $\mathcal{B}$ is Moufang. The converse is obvious. □

Corollary 3.4. *A left (right) Bol loop is a Moufang loop if and only if it is right (left) alternative.*

Lemma 3.5. *For Bol loops (particularly for Moufang loops), $(a^{-1})^2 = (a^2)^{-1}$.*

Proof. In a left Bol loop, $(a^{-1}a^{-1})(aa) \underset{(ALT)_l}{=} a^{-1}(a^{-1}(aa)) \underset{(lip)}{=} a^{-1}a \approx e$. In the case of a right Bol loop, a mirror proof works. □

The common value can be denoted by $a^{-2} := (a^{-1})^2 = (a^2)^{-1}$. Similarly, $(a^n)^{-1} = (a^{-1})^n$ for any natural number n.

More generally, in a left Bol loop $\mathcal{B}$, a power a^n can be introduced for any element $a \in B$ and any integer: $a^0 = e$, $a^n = a \cdot a^{n-1}$, $a^{-n} = (a^{-1})^n$ for any natural $n \in \mathbb{N}$. In a left Bol loop, $b^n(b^m a) = b^{n+m}a$, in particular, $b^n b^m = b^{n+m}$ (Bol and Moufang loops are power-associative) [20].

The variety $\underline{CML}$ of commutative Moufang loops can be characterized as a subvariety of $\underline{L}$, which is characterized by the additional identity $x^2(yz) \approx (xy)(xz)$, a modification of $(M1)$.

The fact that most of the varieties of loops of Bol-Moufang type can be defined in several equivalent ways was a motivation for [17–19].

3.3 Left Bol left loops. We can investigate Bol conditions even in weaker structures, and await reasonable results.

Let us start with a left loop (with a two-sided neutral element e) which satisfies left Bol identity (B_l), and can be called a *left Bol left loop*. More formally, let $\mathcal{Q} = (Q; \cdot, \backslash, e)$ belong to

$$\underline{LBLL} = Mod(\{(Q1_l), (Q2_l), (U_l), (U_r), (B_l)\}).$$

Our aim is to show that on Q, a suitable binary operation / can be introduced in such a way that our algebra $\mathcal{Q}$ is in fact a reduct of some left Bol loop from $\underline{LBL}$. Note that both concepts are different from the theoretical view-point of universal algebra, but as far as more practical purposes are concerned: their classes of examples are in a bijective correspondence, that is, essentially the same.

Lemma 3.6. *In any $\mathcal{Q} \in \underline{LBLL}$, the following identities are satisfied:*

(lip'): $x(x\backslash e \cdot y) \approx y$,
(lip''): $x\backslash e(xy) \approx y$,
$(*)$: $x\backslash e \cdot x \approx e$.

Proof. Let us start from the chain of identities

$$x\backslash e \cdot (x(x\backslash e \cdot y)) \underset{(B_l)}{\approx} [x\backslash e \cdot (x \cdot x\backslash e)]y \underset{(Q1_l),(U_r)}{\approx} x\backslash e \cdot y.$$

Due to left cancellation, (lip') is obtained. To prove (lip'') we proceed similarly, $x(x\backslash e(xy)) \underset{(B_l)}{\approx} x(x\backslash e \cdot x))y \underset{(lip')}{\approx} xy$, and we use (C_l) again. Setting $y = e$ in (lip') we get the rest. $\square$

Given $\mathcal{Q} \in \underline{\mathcal{LBLL}}$ let us introduce a new binary operation "\" on Q by

$$a/b := b\backslash e(ba \cdot b\backslash e) \quad \text{for any} \quad a, b \in Q.$$

Let us check that $(Q1_r)$ and $(Q2_r)$ are satisfied:

$$xy/y = y\backslash e(y(xy)\cdot)y\backslash e \underset{(B_l)}{=} y\backslash e(y(x(y\cdot y\backslash e))) \underset{(Q1_l)}{=} y\backslash e(y(x\cdot e)) \underset{(U_r)}{=} y\backslash e(yx)x \underset{(lip')}{=} x,$$

$$x/y \cdot y = [y\backslash e(yx \cdot y\backslash e)]y \underset{(B_l)}{=} y\backslash e(yx \cdot (y\backslash e \cdot y)) \underset{(*)}{=} y\backslash e(yx \cdot e) \underset{(U_r)}{=} y\backslash e(yx) \underset{(lip')}{=} x.$$

4 Bol loops in signature $(\cdot, {}^{-1}, e)$

As we have already seen, varieties of loops of Bol-Moufang type (including groups) can be introduced in various types. The fact that they belong to the class of the so called IP-loops is of considerable importance.

(Left) Bol loops are frequently introduced as loops in which (left) Bol condition is satisfied, and consequences of the axioms (some of which might be redundant) are derived: particularly the existence of two-sided inverse elements and the left inverse property, (LIP), are remarkable. We propose here a rather non-traditional way how to minimalize the axiomatic system.

Let us introduce a variety of left Bol loops $\underline{B}$ in type $(2, 1, 0)$ with operation symbols $(\cdot, {}^{-1}, e)$. Considering the fact that Bol loops belong to the class of left inverse property loops we can choose

$$xe \approx x, \quad ex \approx x, \quad (x^{-1})^{-1} \approx x, \; x^{-1}(xy) \approx y, \quad x(y(xz)) \approx (x(yx))z$$

as a basis of identities. For some purposes, this definition in type $(2, 1, 0)$ seems to be quite convenient, and the fact that groups (in the usual setting) form a subvariety in $\underline{B}$ is transparent enough.

Let K denote a class of algebras in type $(2, 1, 0)$, with a sequence of operation symbols $(\cdot, {}^{-1}, e)$. Let us consider the following set of identities:

$(IN_r):\quad x\cdot x^{-1}\approx e,\qquad (IN_l):\quad x^{-1}\cdot x\approx e,$
$(LIP):\quad x^{-1}(xy)\approx y,\qquad (LIP)':\quad x(x^{-1}y)\approx y,$
$(INV):\quad (x^{-1})^{-1}\approx x,\qquad (Lu):\quad (x^{-1}((xx)x^{-1})\cdot x\approx x.$

The following can be easily checked.

Lemma 4.1. *In an algebra $\mathcal{B}=(Q;\cdot,{}^{-1},e)\in K$ the following implications are satisfied:*

(i) *(U_r) and (LIP) imply (IN_l),*
(ii) *(U_r), (INV) and (LIP) imply (IN_r),*
(iii) *if (U_r), (INV) and (LIP) are satisfied then also $(LIP)'$ holds,*
(iv) *if (U_r) and $(N2)$ hold then $(FLEX)$ is also satisfied,*
(v) *(U_r), (INV), (LIP) and $(N2)$ imply (U_l),*
(vi) *(U_r) and $(N2)$ imply (B_l),*
(vii) *if (U_r), (INV), (LIP) and $(N2)$ hold then (ALT_l) is satisfied.*

Proof. Under the respective assumptions, we get the following chains of identities:

$$x^{-1}x \underset{(U_r)}{\approx} x^{-1}(xe) \underset{(LIP)}{\approx} e,$$

$$xx^{-1} \underset{(INV)}{\approx} (x^{-1})^{-1}x^{-1} \underset{(U_r)}{\approx} (x^{-1})^{-1}(x^{-1}e) \underset{(LIP)}{\approx} e,$$

$$x(x^{-1}y) \underset{(INV)}{\approx} (x^{-1})^{-1}(x^{-1}y)x \underset{(LIP)}{\approx} e,$$

$$(x^{-1}((xx)x^{-1}))\cdot x \underset{(B_l)}{\approx} x^{-1}\cdot[(xx)(x^{-1}x)] \underset{(IN_l)}{\approx} x^{-1}\cdot[(xx)e] \underset{(U_r)}{\approx} x^{-1}\cdot(xx) \underset{(LIP)}{\approx} x,$$

$$x(yx) \underset{(U_r)}{\approx} x(y(xe)) \underset{(N2)}{\approx} (x(yx))e \underset{(U_r)}{\approx} (xy)x,$$

$$ex \underset{(IN_r)}{\approx} (xx^{-1})x \underset{(FLEX)}{\approx} x(x^{-1}x) \underset{(IN_l)}{\approx} xe \underset{(U_r)}{\approx} x,$$

$$x(y(xz)) \underset{(N2)}{\approx} ((xy)x)z \underset{(FLEX)}{\approx} (x(yx))z,$$

$$x(xz) \underset{(U_l)}{\approx} x(e(xz)) \underset{(N2)}{\approx} ((xe)x)z \underset{(U_r)}{\approx} (xx)z. \qquad \square$$

The condition (Lu) tells that the "left neutral" element e^l_b of $b\in B$, determined by the equation $e^l_b\cdot b=b$, is of the form $b^{-1}[(bb)b^{-1}]$. In general, left neutral elements e^l_a, e^l_b corresponding to different elements $a\neq b$ might be different.

Lemma 4.2. *Let $\mathcal{B}\in K$ be an algebra satisfying (LIP). Then $\mathcal{B}$ satisfies the left cancellation law (C_l).*

Proof. Let a, c, $c'\in B$ and suppose $ac=ac'$. Then we evaluate $c \underset{(LIP)}{=} a^{-1}(ac)= a^{-1}(ac') \underset{(LIP)}{=} c'$. $\square$

Lemma 4.3. *Let $\mathcal{B}\in K$ satisfy (U_r), (IN_r), (C_l) and (B_l). Then $\mathcal{B}$ satisfies also the right cancellation law (C_r).*

Proof. Let the assumptions hold in $\mathcal{B}$. Suppose $ca = c'a$. Then also $a(ca) = a(c'a)$. Calculate

$$ac \underset{(U_r)}{=} a(ce) \underset{(IN_r)}{=} a(c(aa^{-1})) \underset{(B_l)}{=} (a(ca)) \cdot a^{-1} =$$

$$= (a(c'a)) \cdot a^{-1} \underset{(B_l)}{\approx} a(c'(aa^{-1})) \underset{(IN_r)}{\approx} a(c'e) = ac'.$$

Hence $ac = ac'$, and by (C_l), also $c = c'$. □

In the class K, distinguish the variety

$$\underline{B} = Mod(\{(U_r), (U_l), (INV), (LIP), (B_l)\}),$$

and call its algebras again left Bol loops.

Corollary 4.4. *Algebras from $\underline{B}$ satisfy (IN_r), (IN_l), and are both left and right cancellative.*

Let us consider also the varieties

$$\underline{M} = Mod(\{(U_r), (INV), (LIP), (N2)\}), \quad \underline{G} = Mod(\{(U_r), (IN_r), (AS).$$

In $\underline{G}$, the identities (U_l), (IN_l), (IN_r), (INV) are satisfied (now we have "usual" groups). Obviously, we obtain the chain of subvarieties $\underline{G} \subset \underline{M} \subset \underline{B}$.

Proposition 4.5. *Given an algebra $\mathcal{B} = (Q; \cdot, ^{-1}, e) \in \underline{B}$ of type $(2, 1, 0)$ let us introduce a couple of binary operations $\backslash$, $/$ by $a\backslash b := a^{-1}b$, $b/a := a^{-1}((ab)a^{-1})$, $a, b \in Q$ [15]. Then $\mathcal{B}' = (Q; \cdot, \backslash, /, e)$ is a Bol loop belonging to the variety $\underline{BL}$.*

Proof. Let us verify that in $\mathcal{B}'$, $(Q1_l)$, $(Q2_l)$, $(Q1_r)$ and $(Q2_r)$ hold. Given $a, b \in Q$ let us evaluate

$$a(a\backslash b) = a(a^{-1}b) \underset{(LIP)'}{=} b, \qquad a\backslash(ab) = a^{-1}(ab) \underset{(LIP)}{=} b,$$

$$(b/a)a = (a^{-1}((ab)a^{-1})a \underset{(B_l)}{=} a^{-1}((ab)(a^{-1}a)) \underset{(IN_l)}{=} a^{-1}((ab)e) \underset{(U_r)}{=} a^{-1}(ab) \underset{(LIP)}{=} b,$$

$$(ba)/a = a^{-1}((a(ba))a^{-1}) \underset{(B_l)}{=} a^{-1}(a(b(aa^{-1}))) \underset{(LIP)}{=} b(aa^{-1}) \underset{(IN_r)}{=} be \underset{(U_r)}{=} b.$$

Since (U_r), (U_l) and (B_l) are among the defining identities of $\underline{B}$ the rest follows. □

The varieties $\underline{B}$ and $\underline{BL}$ are term equivalent, the same for the varieties of groups $\underline{G}$ and $\underline{Gr}$, or for Moufang loops.

For any $\mathcal{B} \in \underline{B}$ the map $J : Q \to Q$, $x \mapsto x^{-1}$ is an involutive permutation of the underlying set Q, and moreover a semiautomorphism of the loop $\mathcal{B}$ ([20, p. 344]), that is, $J(x(yx)) = J(x)(J(y)J(x))$ holds.

Lemma 4.6. *In the variety $\underline{B}$ the following identities are satisfied:*

$$(SA)': \quad [x(y^{-1}x)]^{-1} \approx x^{-1}(yx^{-1}), \qquad (SA): \quad [x(yx)]^{-1} \approx x^{-1}(y^{-1}x^{-1}).$$

Proof. The first assertion $(SA)'$ follows by right cancellation (C_r) from

$$x^{-1}(yx^{-1})\cdot x(y^{-1}x) \underset{(B_l)}{\approx} x^{-1}(y(x^{-1}[x(y^{-1}x)])) \underset{(LIP)}{\approx} x^{-1}(y(y^{-1}x)) \underset{(LIP)'}{\approx}$$

$$\underset{(LIP)'}{\approx} x^{-1}x \underset{(IN_l)}{\approx} \approx [x(y^{-1}x)]^{-1}\cdot x(y^{-1}x),$$

and the second is a consequence. □

Lemma 4.7. *In the variety $\underline{B}$, the following identities hold for $n \geq 2$:*

(i) $$x_n(x_{n-1}(\dots(x_3(x_2(x_1(x_2(x_3(\dots(x_{n-1}(x_nz))\dots)\approx$$

$$\approx x_n(x_{n-1}(\dots[x_3([x_2(x_1x_2)]x_3)]\dots)x_{n-1}))x_n)\cdot z,$$

(ii) $$x_n(x_{n-1}(\dots(x_2(x_1(x_2(\dots(x_{n-1}x_n)\dots)\approx$$

$$\approx x_n((x_{n-1}(\dots[\dots[x_2(x_1x_2)]\dots]x_{n-1})x_n),$$

(iii) $$[x_n(x_{n-1}(\dots(x_2(x_1(x_2(\dots(x_{n-1}x_n)\dots)]^{-1}\approx$$

$$\approx x_n^{-1}(x_{n-1}^{-1}(\dots(x_2^{-1}(x_1^{-1}(x_2^{-1}(\dots(x_{n-1}^{-1}x_n^{-1})\dots).$$

Proof. We use the idenity (B_l) $(n-1)$-times to prove the first identity,

$$[x_n((x_{n-1}([\dots[x_3([x_2(x_1x_2)]x_3)]\dots]x_{n-1}))x_n)]\cdot z \underset{(B_l)}{\approx}$$

$$\underset{(B_l)}{\approx} x_n((x_{n-1}([\dots[x_3([x_2(x_1x_2)]x_3)]\dots]x_{n-1}))(x_nz)) \underset{(B_l)}{\approx}\dots$$

$$\dots\underset{(B_l)}{\approx} x_n(x_{n-1}(\dots(x_3(x_2(x_1(x_2(x_3(\dots(x_{n-1}(x_nz))\dots).$$

For $z=e$, the second identity is obtained, and (iii) is a consequence of (SA). □

References

[1] Bates G., Kiokemeister F. *A note on homomorphic mappings of quasigroups into multiplicative systems.* Bull. Amer. Math. Soc., 1948, **54**, p. 1180–1185.

[2] Belousov V.D. *Foundations of the theory of quasigroups and loops.* Moscow, Nauka, 1967.

[3] Bol G. *Gewebe und Gruppen.* Math. Ann., 1937, **114**, p. 411–431.

[4] Bruck R.H. *A Survey of Binary Systems.* berlin, Springer, 1958.

[5] *Quasigroups and Loops: Theory and Applications / Eds. Chein O., Pflugfelder H.O., Smith J.D.H.* Berlin, Heldermann Verlag, 1990.

[6] Evans T. *Homomorphisms of non-associative systems.* J. London Math. Soc., 1949, **24**, p. 254–260.

[7] Evans T. *Varieties of loops and quasigroups.* Quasigroups and Loops: Theory and Applications / Eds. Chein, O., Pflugfelder, H.O., Smith, J.D.H. Berlin, Heldermann Verlag, 1990, p. 1–160.

[8] Fenyves F. *Extra loops I.* Publ. Math., 1968, **15**, p. 235–238.

[9] Fenyves F. *Extra loops II.* Publ. Math., 1969, **16**, p. 187–192.

[10] Kiechle H. *Theory of K-Loops.* Berlin-Heidelberg-New York, Springer, 2002.

[11] Kinyon M.K. *Global left loop structures on spheres.* Comment. Math. Univ. Carolinae, 2000, **41**, N 2, p. 325–346.

[12] Kunen K. *Moufang quasigroups.* Jour. of Algebra, 1996, **183**, p. 231–234.

[13] Kunen K. *Quasigroups, loops and associative laws.* Jour. of Algebra, 1996, **185**, p. 194–204.

[14] Kurosh A.G. *Lekcii po obshchei algebre.* Moskva, Fizmatgiz, 1962 (in Russian).

[15] Mikheev P.O., Sabinin L.V. *The Theory of Smooth Bol Loops.* Friendship of Nations University, Moscow, 1985.

[16] Pflugfelder H.O. *Quasigroups and Loops, Introduction.* Berlin, Heldermann Verlag, 1990.

[17] Phillips J.D., Vojtěchovský P. *The varieties of loops of Bol-Moufang type.* Preprint series M03/03, 2003.

[18] Phillips J.D., Vojtěchovský P. *The varieties of quasigroups of Bol-Moufang type: An equational reasoning approach.* Preprint series M03/12, 2003.

[19] Phillips J.D., Vojtěchovský P. *A scoop from groups: New equational foundations for loops.* Preprint series M04/05, 2004.

[20] Robinson D.A. *Bol loops.* Trans. Amer. Math. Soc., 1966, **123**, p. 341–354.

[21] Robinson D.A. *Holomorphy theory of extraloops.* Publ. Math. Debrecen, 1972, **18**, p. 59–64.

[22] Robinson D.A. *Bol quasigroups.* Publ. Math. Debrecen, 1972, **19**, p. 151–153.

[23] Sabinin L.V. *Smooth Quasigroups and Loops.* Kluwer Acad. Publ., Dordrecht-Boston-London, 1999.

[24] Smith J.D.H. *Homotopy and semisymmetry of quasigroups.* Algebra Univ., Birkhäuser, Basel, 1997, **38**, p. 175–184.

Faculty Sciences
Department Algebra and Geometry
Palacký University
Tomkova 40, 779 00 Olomouc
Czech Republic
E-mail: *vanzurov@inf.upol.cz*

Received August 11, 2005

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 101–114
ISSN 1024–7696

A loop transversal in a sharply 2-transitive permutation loop

Eugene Kuznetsov

Abstract. The well-known theorem of M.Hall about the description of a finite sharply 2-transitive permutation group is generalized for the case of permutation loops. It is shown that the identity permutation with the set of all fixed-point-free permutations in a finite sharply 2-transitive permutation loop forms a loop transversal by its proper subloop – a stabilizator of one symbol.

Mathematics subject classification: 20N05.
Keywords and phrases: Quasigroup, loop, transversal, projective plane.

1 Introduction

In the theory of finite multiply transitive permutation groups the following M. Hall's theorem is well-known.

Theorem 1. *Let G be a sharply 2-transitive permutation group on a finite set of symbols E, i.e.*

1. *G is a 2-transitive permutation group on E;*
2. *only the identity permutation id fixes two symbols from the set E.*

Then

1. *the identity permutation id together with the set of all fixed-point-free permutations from the group G forms a transitive invariant subgroup A in the group G;*
2. *the group G is isomorphic to the group of linear transformations*

$$G_K = \{\alpha \,|\, \alpha(x) = x \cdot a + b, \quad a, b \in E, \quad a \neq 0\}$$

of some near-field $K = \langle E, +, \cdot, 0, 1\rangle$.

In the articles [11,12,14] the notion of a permutation loop on some set of symbols E is defined. Both for permutation groups, and for permutation loops the notions of transitivity, multiple transitivity and sharply multiple transitivity can be defined

[11,12,14]. The studying of a sharply 2-transitive permutation loop of permutations is the most interesting, because (see [6]) there exists a 1-1 correspondence between every finite projective plane and some sharply 2-transitive permutation loop.

Using the notion of a transversal in a loop to its subloop (see [11, 13]), the author of the present article proves a generalization of Hall's Theorem for the case of a sharply 2-transitive permutation loop.

Theorem 2. *Let L be a sharply 2-transitive permutation loop on a finite set of symbols E, i.e.*

1. *L is a 2-transitive set of permutations on the finite set of symbols E;*
2. *permutations from the set L form a loop by some operation "$\cdot$";*
3. *only the identity permutation id fixes two symbols from the set E.*

Then

1. *the identity permutation id together with the set of all fixed-point-free permutations from the loop L forms a transitive loop transversal A in the loop L to its proper subloop R_a, where R_a is a loop of all permutations from the loop L which fix some symbol $a \in E$;*
2. *this loop transversal A is a unique loop transversal in the loop L to its proper subloop R_a, i.e. any other loop transversal T in the loop L to its proper subloop R_a coincide with the transversal T.*

Let us give some necessary notations and prove some basic statements.

2 Necessary definitions and notations

Definition 1. *A system $\langle E, \cdot\rangle$ is called [2, 5] a **right (left) quasigroup** if for arbitrary $a, b \in E$ the equation $x \cdot a = b$ ($a \cdot y = b$) has a unique solution in the set E. If a system $\langle E, \cdot\rangle$ is both a right and left quasigroup, then it is called a **quasigroup**. If in a right (left) quasigroup $\langle E, \cdot\rangle$ there exists an element $e \in E$ such that*

$$x \cdot e = e \cdot x = e,$$

*for any $x \in E$, then the system $\langle E, \cdot\rangle$ is called a **right (left) loop** (the element e is called a **unit** or **identity element**). If a system $\langle E, \cdot\rangle$ is both a right and left loop, then it is called a **loop**.*

Definition 2. *Let G be a group and H be a subgroup in G. A complete system $T = \{t_i\}_{i\in E}$ of representatives of the left (right) cosets of H in G ($e = t_1 \in H$) is called [1] a **left (right) transversal in** G **to** H.*

Let $T = \{t_x\}_{x \in E}$ be a left transversal in G to H. We can define correctly (see [1, 6]) the following operation (**transversal operation**) on the set E (E is an index set; left cosets of H in G are numbered by indexes from E):

$$x \overset{(T)}{\cdot} y = z \quad \overset{def}{\Longleftrightarrow} \quad t_x t_y = t_z h, \quad h \in H. \tag{1}$$

In [5] it was proved that the system $\langle E, \overset{(T)}{\cdot}, 1\rangle$ is a left loop with the unit 1.

Definition 3. *Let T be a left transversal in G to H. If the system $\langle E, \overset{(T)}{\cdot}, 1\rangle$ is a loop, then T is called a **left loop** (or simply "**loop**") **transversal** in G to H.*

3 A transversal in a loop to its subloop

The author of the present article generalized in [10, 11] the well-known (in group theory) notion of a transversal in a group to its proper subgroup. Also the analogous generalization is studied in [3].

At the beginning let us define a partition of a loop by left (right) cosets to its proper subloop.

Definition 4. *Let $\langle L, \cdot\rangle$ be a loop and $\langle R, \cdot\rangle$ be its proper subloop. Then [13] a **left coset** of R is a set of the form*

$$xR = \{xr \,|\, r \in R\},$$

*and a **right coset** has the form*

$$Rx = \{rx \,|\, r \in R\}.$$

The cosets of a subloop do not necessarily form a partition of the loop. This leads to the following definition.

Definition 5. *A loop L has a **left (right) coset decomposition by its proper subloop** R [13], if the left (right) cosets form a partition of the loop L, i.e. for some set of indexes E*

1. $\underset{i \in E}{\cup} (a_i R) = L$;
2. *for every $i, j \in E$, $i \neq j$*

$$(a_i R) \cap (a_j R) = \varnothing.$$

Lemma 1. *The following conditions are equivalent:*

1. *a loop L has a left coset decomposition by its proper subloop R;*

2. *the following condition take place (it can be named a* ***weak left Condition A****, see below): for every $a \in L$*

$$(aR)R = aR. \tag{2}$$

Proof. See in [13], Theorem I.2.12.

In order to define correctly the notion of a left (right) transversal in a loop to its proper subloop, it is necessary that the following condition be fulfilled.

Definition 6. *(**Left Condition A**) The multiplication to the left of an arbitrary element a of the loop L by an arbitrary left coset in the loop L to its proper subloop R is a left coset in the loop L to its proper subloop R too, i.e. for every $a, b \in L$ there exists an element $c \in L$ such that*

$$a(bR) = cR. \tag{3}$$

The **right Condition A** is defined analogously.

Lemma 2. *The following conditions are equivalent:*

1. *a left Condition A is fulfilled in the loop L to its proper subloop R;*

2. *for every $a, b \in L$*

$$a(bR) = (ab)R. \tag{4}$$

Proof. See in [11].

Remark 1. The condition (4) is called in [3] a **strong left coset decomposition of the loop L by its proper subloop R**. Also we can say that the subloop R is a **left invariant** subloop in the loop L.

Definition 7. *(See also [3]) Let $\langle L, \cdot, e\rangle$ be a loop and $\langle R, \cdot, e\rangle$ be its proper subloop. Let a left Condition A be fulfilled in the loop L to its proper subloop R. Then the loop L has a left coset decomposition by its proper subloop R. A* ***left transversal*** *$T = \{t_x\}_{x\in E}$ in the loop L to its proper subloop R is a set of representatives, one from each left coset; moreover, $t_1 = e \in R$.*

A right transversal $T = \{t_x\}_{x\in E}$ in the loop L to its proper subloop R is defined analogously.

Remark 2. If in the last definition we eliminate the condition $t_1 = e \in R$, then we obtain a definition of a **non-reduced left transversal** $T = \{t_x\}_{x\in E}$ in the loop L to its proper subloop R.

Let $T = \{t_x\}_{x \in E}$ be a left transversal in a loop L to its proper subloop R. We can define correctly the following operation (**transversal operation**) on the set E:

$$x \overset{(T)}{\cdot} y = z \quad \overset{def}{\Longleftrightarrow} \quad t_x \cdot t_y = t_z \cdot r, \quad r \in R, \tag{5}$$

where $t_x, t_y, t_z \in T,\ r \in R$. In [11] it is proved that the system $\langle E, \overset{(T)}{\cdot}, 1\rangle$ is a left loop with the unit 1.

Definition 8. *Let T be a left transversal in a loop L to its proper subloop R. If the system $\langle E, \overset{(T)}{\cdot}, 1\rangle$ is a loop, then T is called a **left loop** (or simply "**loop**") **transversal** in the loop L to its proper subloop R.*

4 Finite projective planes, DK-ternars and loop transversals in the group S_n to $St_{a,b}(S_n)$

Let us remember the basic facts from the theory of finite projective planes and their coordinatization (see [7]).

Definition 9. *The **projective plane** of order n is the incidence structure $\langle P, L, I\rangle$ which satisfies the following axioms:*

1. *Given any two distinct points from P there exists just one line from L incident with both of them;*
2. *Given any two distinct lines from L there exists just one point from P incident with both of them;*
3. *There exist four points such that a line incident with any two of them is not incident with either of the remaining two.*
4. *There exists a line in L which consists of exactly $n+1$ points.*

Definition 10. *A system $\langle E, (x,t,y), 0, 1\rangle$ is called [7] a **DK-ternar** (i.e. a set E with ternary operation (x,t,y) and distinguished elements $0, 1 \in E$) if the following conditions hold:*

1. $(x, 0, y) = x,$
2. $(x, 1, y) = y,$
3. $(x, t, x) = x,$
4. $(0, t, 1) = t,$

5. *if a, b, c, d are arbitrary elements from E and $a \neq b$, then the system*

$$\begin{cases} (x, a, y) = c \\ (x, b, y) = d \end{cases}$$

has an unique solution in $E \times E$.

Definition 11. *A set M of permutations on a set X is called [4]* ***sharply 2-transitive*** *if for any two pairs (a, b) and (c, d) of different elements from X there exists an unique permutation $\alpha \in M$ satisfying the following conditions:*

$$\alpha(a) = c, \qquad \alpha(b) = d.$$

Lemma 3. *Let π be an arbitrary finite projective plane. We can introduce on the plane π the coordinates $(a, b), (m), (\infty)$ for points and $[a, b], [m], [\infty]$ for lines (where the set E is a finite set with the distinguished elements $0, 1$ and $a, b, m \in E$) such that if we define a ternary operation (x, t, y) on the set E by the formula*

$$(x, t, y) = z \quad \overset{def}{\Longleftrightarrow} \quad (x, y) \in [t, z],$$

then the system $\langle E, (x, t, y), 0, 1\rangle$ be a DK-ternar.

Proof. See Lemma 1 in [7].

Now let a system $\langle E, (x, t, y), 0, 1\rangle$ be a DK-ternar. Let us define the following binary operation (x, ∞, y) on the set E:

$$(x, \infty, 0) \overset{def}{=} x,$$
$$\begin{cases} (x, \infty, y) = u \\ (x, y) \neq (u, 0) \end{cases} \quad \overset{def}{\Longleftrightarrow} \quad \begin{matrix} (x, t, y) \neq (u, t, 0) \\ \forall t \in E. \end{matrix}$$

Lemma 4. *Operation (x, ∞, y) satisfies the following conditions:*

1. $\begin{cases} (x, \infty, y) = (u, \infty, v) \\ (x, y) \neq (u, v) \end{cases} \quad \Longleftrightarrow \quad \begin{matrix} (x, t, y) \neq (u, t, v) \\ \forall t \in E. \end{matrix}$

2. $(x, \infty, x) = 0.$

3. *if a, b, c are arbitrary elements from E, then the system*

$$\begin{cases} (x, a, y) = b \\ (x, \infty, y) = c \end{cases}$$

has a unique solution in $E \times E$.

Proof. See Lemma 4 in [7].

Let $\langle E,(x,t,y),0,1\rangle$ be a finite DK-ternar. Let us introduce points $(a,b),(m),(\infty)$ and lines $[a,b],[m],[\infty]$ (where $a,b,m\in E$) and define the following incidence relation I between points and lines:

$$\begin{array}{l}(a,b)\ I\ [c,d] \quad\Longleftrightarrow\quad (a,c,b)=d,\\ (a,b)\ I\ [d] \quad\Longleftrightarrow\quad (a,\infty,b)=d,\\ (a)\ I\ [c,d] \quad\Longleftrightarrow\quad a=c,\\ (a)\ I\ [\infty], \qquad (\infty)\ I\ [d], \qquad (\infty)\ I\ [\infty],\\ (a,b)\ I\ [\infty] \Longleftrightarrow (a)\ I\ [d] \Longleftrightarrow\\ \ (\infty)\ I\ [c,d] \Longleftrightarrow false.\end{array} \tag{6}$$

Lemma 5. *The incidence system $\langle X,L,I\rangle$, where*

$$X=\{(a,b),(m),(\infty)\mid a,b,m\in E\},$$
$$L=\{[a,b],[m],[\infty]\mid a,b,m\in E\},$$
I is the incidence relation, defined above in (6),

is a projective plane.

Proof. See Lemma 5 in [7].

Lemma 6. ***(Cell permutations)*** *Let the system $\langle E,(x,t,y),0,1\rangle$ be a finite DK-ternar. Let a,b be arbitrary elements from E and $a\neq b$. Then every unary operation $\alpha_{a,b}(t)=(a,t,b)$ is a permutation on the set E.*

Proof. See Lemma 6 in [7].

Lemma 7. *Cell permutations $\{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ of the finite DK-ternar $\langle E,(x,t,y),0,1\rangle$ satisfy the following conditions:*

1. *All cell permutations are distinct;*
2. *The set M of all cell permutations is sharply 2-transitive on the set E;*
3. *A permutation $\alpha_{a,b}$ is a fixed-point-free cell permutation on the set E iff the following condition holds*

$$(a,\infty,b)=(0,\infty,1).$$

4. *There exists the fixed-point-free permutation ν_0 on the set E such that we can represent the set A of all fixed-point-free cell permutations together with the identity cell permutation $\alpha_{0,1}$ in the following form:*

$$A=\{\alpha_{a,b}\,|\,b=\nu_0(a),\quad a\in E\}=\{\alpha_{a,\nu_0(a)}\}_{a\in E}.$$

Proof. See Lemma 7 in [7].

Lemma 8. *Let $M = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ be a set of permutations on the set E (E is a finite set with distinguished elements 0 and 1), and the following conditions hold:*

1. $\alpha_{0,1} = id$.
2. $\alpha_{a,b}(0) = a,\ \alpha_{a,b}(1) = b$.
3. *The set M is a sharply 2-transitive set of permutations on E.*

   Let us suppose by definition:

$$(x,t,y) \stackrel{def}{=} \alpha_{x,y}(t) \quad if \quad x \neq y,$$
$$(x,t,x) \stackrel{def}{=} x.$$

Then the system $\langle E, (x,t,y), 0, 1\rangle$ is a finite DK-ternar.

Proof. See Lemma 8 in [7].

Next theorem shows a connection between finite sharply 2-transitive sets of permutations and loop transversals in the symmetric group S_n.

Theorem 3. *Let E be a finite set and $\operatorname{card} M = n$. Then the following conditions are equivalent:*

1. *A set T of permutations of degree n is a sharply 2-transitive set of permutations on the set E and $id \in T$.*
2. *A set T of permutations of degree n is a loop transversal in S_n to $St_{a,b}(S_n)$ (where a, b are arbitrary fixed elements from E and $a \neq b$).*
3. *A system $\langle E\times E - \{\triangle\}, \stackrel{(T)}{\cdot}, \langle a,b\rangle\rangle$ is a sharply 2-transitive permutation loop of degree n (a definition of permutation loop see in [11, 12, 14]).*

Proof. See Theorem 1 in [6].

Lemma 9. *Let $T_{a,b} = \{\alpha_{x,y}\}_{x,y\in E,\ x\neq y}$ be a loop transversal in S_n to $St_{a,b}(S_n)$ (where a, b are arbitrary fixed elements from E and $a \neq b$). Let a system $\langle E\times E - \{\triangle\}, \stackrel{(T_{a,b})}{\cdot}, \langle a,b\rangle\rangle$ be a loop transversal operation corresponding to the transversal $T_{a,b}$. Then*

$$\langle x,y\rangle \stackrel{(T_{a,b})}{\cdot} \langle u,v\rangle = \langle \alpha_{x,y}(u), \alpha_{x,y}(v)\rangle. \tag{7}$$

Proof. See Lemma 10 in [7].

5 A loop transversal in a sharply 2-transitive permutation loop

As it is shown above, there exist a 1-1 correspondences between

- a finite projective plane π of order n;
- a finite DK-ternar $\langle E,(x,t,y),0,1\rangle$ which gives a coordinatization of the projective plane π;
- a sharply 2-transitive permutation loop $L=\{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ of cell permutations of the DK-ternar $\langle E,(x,t,y),0,1\rangle$;
- a loop transversal $T_{a,b}=\{\alpha_{x,y}\}_{x,y\in E,\ x\neq y}$ in the symmetric group S_n to $St_{a,b}(S_n)$ (where a,b are arbitrary fixed elements from E and $a\neq b$);
- a loop transversal operation $\langle E\times E-\{\triangle\},\overset{(T_{a,b})}{\cdot},\langle a,b\rangle\rangle$ corresponding to the transversal $T_{a,b}$ (in [7] this loop is called a **loop of pairs** of the DK-ternar $\langle E,(x,t,y),0,1\rangle$).

Below for simplicity we shall consider that $\langle a,b\rangle=\langle 0,1\rangle$.

Lemma 10. *The set*

$$H_0^*=\{\langle 0,a\rangle\,|\,a\in E-\{0\}\}$$

forms a subloop in the loop of pairs $L^*=\langle E\times E-\{\triangle\},\overset{(T_{0,1})}{\cdot},\langle a,b\rangle\rangle$.

Proof. See Lemma 11 in [7].

Lemma 11. *A left Condition A is fulfilled for the loop of pairs L^* to its proper subloop H_0^*.*

Proof. Let us have

$$\begin{aligned} a_0 &= \langle a,b\rangle\in L, \qquad b_0=\langle c,d\rangle\in L,\\ x &= \langle 0,u\rangle\in H_0^*, \quad y=\langle 0,v\rangle\in H_0^*, \end{aligned}$$

where $a,b,c,d\in E,\quad a\neq b,\quad c\neq d,\quad u,v\in E-\{0\}$. According to (7), we obtain

$$\begin{aligned} a_0\overset{(T_{0,1})}{\cdot}(b_0\overset{(T_{0,1})}{\cdot}x) &= \langle a,b\rangle\overset{(T_{0,1})}{\cdot}(\langle c,d\rangle\overset{(T_{0,1})}{\cdot}\langle 0,u\rangle)=\langle a,b\rangle\overset{(T_{0,1})}{\cdot}\langle\alpha_{c,d}(0),\alpha_{c,d}(u)\rangle=\\ &= \langle a,b\rangle\overset{(T_{0,1})}{\cdot}\langle c,\alpha_{c,d}(u)\rangle=\langle\alpha_{a,b}(c),\alpha_{a,b}\alpha_{c,d}(u)\rangle, \end{aligned}$$

since $\alpha_{x,y}(0)=x$ (see Lemma 8). By the analogous way we obtain

$$\begin{aligned} (a_0\overset{(T_{0,1})}{\cdot}b_0)\overset{(T_{0,1})}{\cdot}y &= (\langle a,b\rangle\overset{(T_{0,1})}{\cdot}\langle c,d\rangle)\overset{(T_{0,1})}{\cdot}\langle 0,v\rangle=\langle\alpha_{a,b}(c),\alpha_{a,b}(d)\rangle\overset{(T_{0,1})}{\cdot}\langle 0,v\rangle=\\ &= \langle\alpha_{a,b}(c),\alpha_{\alpha_{a,b}(c),\alpha_{a,b}(d)}(v)\rangle. \end{aligned}$$

Because the function $\alpha_{a,b}(t)$ is a permutation on the set E, then for every $u \in E-\{0\}$ there exists $u \in E-\{0\}$ such that

$$\alpha_{a,b}\alpha_{c,d}(u) = \alpha_{\alpha_{a,b}(c),\alpha_{a,b}(d)}(v);$$

really

$$v = \alpha^{-1}_{\alpha_{a,b}(c),\alpha_{a,b}(d)}\alpha_{a,b}\alpha_{c,d}(u).$$

Let us note that

$$\alpha_{a,b}\alpha_{c,d}(0) = \alpha_{a,b}(c) = \alpha_{\alpha_{a,b}(c),\alpha_{a,b}(d)}(0).$$

Finally we obtain that for every $x \in H_0^*$ there exists $y \in H_0^*$ such that

$$a_0 \overset{(T_{0,1})}{\cdot} (b_0 \overset{(T_{0,1})}{\cdot} x) = (a_0 \overset{(T_{0,1})}{\cdot} b_0) \overset{(T_{0,1})}{\cdot} y$$

for every $a_0, b_0 \in L$. A left Condition A is fulfilled for the loop of pairs L^* to its proper subloop H_0^*. $\square$

According to the last Lemma we obtain that the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ of cell permutations has a strong left coset decomposition by its proper subloop $H_0 = \{\alpha_{0,a} \,|\, a \in E-\{0\}\}$. So it is possible to define and investigate a left or right transversals in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its proper subloop H_0.

Let us study the set $A = \{\alpha_{a,\nu(a)}\}_{a\in E} \subset L$ of all fixed-point-free permutations and the identity permutation (see Lemma 8).

Lemma 12. *The set $A = \{\alpha_{a,\nu(a)}\}_{a\in E}$ is a loop transversal in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its proper subloop H_0.*

Proof. Let us study left cosets $(\alpha_{a,b} \overset{(T_{0,1})}{\cdot} H_0)$ in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0. We have

$$\begin{array}{rcl} \alpha_{c,d} & \in & \alpha_{a,b} \overset{(T_{0,1})}{\cdot} H_0, \\ \alpha_{c,d} & = & \alpha_{a,b} \overset{(T_{0,1})}{\cdot} \alpha_{0,u} \end{array}$$

for some $u \in E-\{0\}$. Then we obtain

$$\begin{cases} c = \alpha_{a,b}(0) = a, \\ d = \alpha_{a,b}(u) \neq a, \end{cases}$$

i.e.

$$\alpha_{a,b} \overset{(T_{0,1})}{\cdot} H_0 = \{\alpha_{a,v} \,|\, v \in E-\{a\}\}.$$

So for every $a \in E$ a left coset $H_a = (\alpha_{a,b} \overset{(T_{0,1})}{\cdot} H_0)$ in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0 is a set of all permutations φ from L such that $\varphi(0) = a$.

Let us study the set $A = \{\alpha_{a,\nu(a)}\}_{a\in E}$ from the Lemma's condition. If $a = 0$ then

$$\alpha_{0,\nu(0)} = \alpha_{0,1} = id \in A \cap H_0,$$

i.e. the unit id of the loop L belongs to the set A. Further,

$$\alpha_{a,\nu(a)}(0) = a \quad \Rightarrow \quad \alpha_{a,\nu(a)} \in H_a,$$

i.e. for every $a \in E$ it is true that

$$A \cap H_a = \{\alpha_{a,\nu(a)}\}.$$

Then the set $A = \{\alpha_{a,\nu(a)}\}_{a \in E}$ is a left transversal in the loop $L = \{\alpha_{a,b}\}_{a,b \in E,\ a \neq b}$ to its proper subloop H_0.

Finally, let us consider a transversal operation $\langle E, \overset{(A)}{\cdot}, 1\rangle$ corresponding to the transversal A:

$$x \overset{(A)}{\cdot} y = z \quad \Leftrightarrow \quad \alpha_{x,\nu(x)} \overset{(T_{0,1})}{\cdot} \alpha_{y,\nu(y)} = \alpha_{z,\nu(z)} \overset{(T_{0,1})}{\cdot} \alpha_{0,u}, \tag{8}$$

where $\alpha_{0,u} \in H_0$. According to [11], the system $\langle E, \overset{(A)}{\cdot}, 1\rangle$ is a left loop with the unit 1. It is sufficient to prove that the system $\langle E, \overset{(A)}{\cdot}, 1\rangle$ is a right loop with the same unit 1 too. So let us study for every $a, b \in E$ the equation $x \overset{(A)}{\cdot} a = b$. According (8), we have

$$\begin{aligned} x \overset{(A)}{\cdot} a &= b, \\ \alpha_{x,\nu(x)} \overset{(T_{0,1})}{\cdot} \alpha_{a,\nu(a)} &= \alpha_{b,\nu(b)} \overset{(T_{0,1})}{\cdot} \alpha_{0,u}, \end{aligned}$$

where $u \in E - \{0\}$. It is equivalent to the following system

$$\begin{cases} \alpha_{x,\nu(x)}(a) = \alpha_{b,\nu(b)}(0) = b, \\ \alpha_{x,\nu(x)}(\nu(a)) = \alpha_{b,\nu(b)}(u). \end{cases}$$

It is easy to see that it is sufficient to show, that for every $a, b \in E$ there exists a unique permutation $\gamma \in A$ such that $\gamma(a) = b$. If $a = b$, then $\gamma = id = \alpha_{0,1}$. Let $a \neq b$; then according to Lemma 4 we obtain:

$$\begin{cases} \alpha_{x,\nu(x)}(a) = b, \\ \alpha_{x,\nu(x)} \text{ is a fixed-point-free permutation on the set } E, \end{cases}$$
$$\begin{cases} (x, a, \nu(x)) = b, \\ (x, t, \nu(x)) \neq t \quad \forall t \in E, \end{cases}$$
$$\begin{cases} (x, a, \nu(x)) = b, \\ (x, \infty, \nu(x)) = (0, \infty, 1). \end{cases}$$

According to Lemma 4 the last system has a unique solution in $E \times E$, i.e. there exists a unique such $\gamma = \alpha_{x,\nu(x)}$. $\square$

Lemma 13. *There exists a unique left loop transversal in the loop $L = \{\alpha_{a,b}\}_{a,b \in E,\ a \neq b}$ to its subloop H_0.*

Proof. According to the last Lemma there exists a such left loop transversal: the transversal $A = \{\alpha_{a,\nu(a)}\}_{a\in E}$ of all fixed-point-free permutations and the identity permutation. Let us prove that the transversal $A = \{\alpha_{a,\nu(a)}\}_{a\in E}$ is a unique left loop transversal in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0.

Let $T = \{t_x\}_{x\in E}$ be a left loop transversal in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0. Because the set T is a left transversal in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0, then

$$T = \{\alpha_{x,\delta(x)}\}_{x\in E},$$

where δ is some function on the set E; $\delta(x) \neq x$ for every $x \in E$. Moreover,

$$t_1 = \alpha_{0,\delta(0)} = id = \alpha_{0,1} \in H_0,$$

i.e. $\delta(0) = 1$.

Let us study a transversal operation $\langle E, \overset{(T)}{\cdot}, 1\rangle$, corresponding to the transversal T in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0. According to the definition of transversal operation, we have:

$$x \overset{(T)}{\cdot} y = z \quad \Leftrightarrow \quad \alpha_{x,\delta(x)} \overset{(T_{0,1})}{\cdot} \alpha_{y,\delta(y)} = \alpha_{z,\delta(z)} \overset{(T_{0,1})}{\cdot} \alpha_{0,u},$$

where $\alpha_{0,u} \in H_0$. So we obtain the following system

$$\begin{cases} \alpha_{x,\delta(x)}(y) = \alpha_{z,\delta(z)}(0) = z, \\ \alpha_{x,\delta(x)}(\delta(y)) = \alpha_{z,\delta(z)}(u). \end{cases}$$

Since the transversal $T = \{t_x\}_{x\in E}$ is a left loop transversal in the loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ to its subloop H_0, then for every $a, b \in E$ the equation $x \overset{(T)}{\cdot} a = b$ has a unique solution in the set E; i.e. for every $a, b \in E$ the equation

$$\alpha_{x,\delta(x)}(a) = b$$

has a unique solution in the set E. It means that if $x_1, x_2 \in E$ and $x_1 \neq x_2$, then must be

$$\alpha_{x_1,\delta(x_1)}(a) \neq \alpha_{x_2,\delta(x_2)}(a).$$

It is true for every $a \in E$, so we obtain for every $a \in E$ and $x_1, x_2 \in E$, $x_1 \neq x_2$:

$$\alpha_{x_1,\delta(x_1)}(a) \neq \alpha_{x_2,\delta(x_2)}(a),$$

i.e. for every $a \in E$ and $x_1, x_2 \in E$, $x_1 \neq x_2$:

$$(x_1, a, \delta(x_1)) \neq (x_2, a, \delta(x_2)).$$

According to Lemma 4, we obtain

$$(x_1, \infty, \delta(x_1)) = (x_2, \infty, \delta(x_2)). \tag{9}$$

It means that for any different elements $\alpha_{x_1,\delta(x_1)}$ and $\alpha_{x_2,\delta(x_2)}$ of the left loop transversal $T = \{\alpha_{x,\delta(x)}\}_{x\in E}$ the formula (9) holds. Moreover,

$$t_1 = \alpha_{0,\delta(0)} = \alpha_{0,1} \in T,$$

since for every $x \in E - \{0\}$ we have

$$(x, \infty, \delta(x)) = (0, \infty, \delta(0)) = (0, \infty, 1).$$

According to Lemma 8 (statements 2 and 3), we obtain that $\delta(x) = \nu(x)$ for every $x \in E$, i.e.

$$T = \{\alpha_{x,\delta(x)}\}_{x\in E} = \{\alpha_{x,\nu(x)}\}_{x\in E} = A.$$

$\square$

Corollary 1. *There exist exactly $n-2$ different non-reduced left loop transversals in the loop L to its subloop H_0.*

Proof. The proof is analogous to the proof of the last Lemma till the moment, when we obtain the following identity for the non-reduced left loop transversal $T = \{\alpha_{x,\delta(x)}\}_{x\in E}$ in the loop L to its subloop H_0:

$$(x_1, \infty, \delta(x_1)) = (x_2, \infty, \delta(x_2)) \tag{10}$$

for every $x_1, x_2 \in E, \quad x_1 \neq x_2$. Since $T = \{\alpha_{x,\delta(x)}\}_{x\in E}$ is a *non-reduced* left loop transversal in the loop L to its subloop H_0, then $T \cap H_0 = \{\alpha_{0,u_0}\}$ for some $u_0 \in E - \{0, 1\}$. So we obtain from (10) for every $x \in E$

$$(x, \infty, \delta(x)) = (0, \infty, \delta(0)) = (0, \infty, u_0).$$

Since $u_0 \neq 0, 1$, then there exist exactly $n-2$ such elements u_0 in the set E. So there exist exactly $n-2$ different non-reduced left loop transversals in the loop L to its subloop H_0. $\square$

Remark 3. We can note a correlation between the left loop transversal A in the loop L to its subloop H_0 and points of the line $[(0, \infty, 1)]$ in the projective plane π:

$$\alpha_{x,\nu(x)} \in A \quad \Leftrightarrow \quad (x, \nu(x)) \in [(0, \infty, 1)].$$

There exists an analogous correlation between non-reduced left loop transversals in the loop L to its subloop H_0 and points of the lines $[d]$ $(d \neq 0)$ in the projective plane π:

$$\alpha_{x,\delta(x)} \in T_c \quad \Leftrightarrow \quad (x, \delta(x)) \in [(0, \infty, c)], \quad c \neq 0, 1.$$

Corollary 2. *The following condition is fulfilled for the loop $\langle E, \overset{(A)}{\cdot}, 0\rangle$ and permutation ν: for every $x \in E$*

$$\nu(x) = x \overset{(A)}{\cdot} 1.$$

Proof. According to formula (8) we have for the transversal operation $\langle E, \overset{(A)}{\cdot}, 0\rangle$:

$$x \overset{(A)}{\cdot} y = z \quad \Leftrightarrow \quad \alpha_{x,\nu(x)}(y) = z.$$

If $y = 1$ then we obtain

$$x \overset{(A)}{\cdot} 1 = z \quad \Leftrightarrow \quad \alpha_{x,\nu(x)}(1) = z \quad \Leftrightarrow \quad \nu(x) = z,$$

i.e.

$$\nu(x) = z = x \overset{(A)}{\cdot} 1.$$

□

References

[1] Baer R. *Nets and groups. 1.* Trans. Amer. Math. Soc., 1939, **46**, p. 110–141.

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

[3] Foguel T., Kappe L.C. *On loops covered by subloops.* Expositiones Mathematicae, 2005, **23**, p. 255–270.

[4] Hall M. *Group theory.* Moscow, IL, 1962 (in Russian).

[5] Kuznetsov E.A *Transversals in groups. 1. Elementary properties.* Quasigroups and related systems, 1994, **1**, N 1, p. 22–42.

[6] Kuznetsov E.A. *Sharply k-transitive sets of permutations and loop transversals in S_n.* Quasigroups and related systems, 1994, **1**, N 1, p. 43–50.

[7] Kuznetsov E.A. *About some algebraic systems related with projective planes.* Quasigroups and related systems, 1995, **2**, p. 6–33.

[8] Kuznetsov E.A. *Sharply 2-transitive permutation groups. 1.* Quasigroups and related systems, 1995, **2**, p. 83–100.

[9] Kuznetsov E.A. *Loop transversals in S_n by $St_{a,b}(S_n)$ and coordinatizations of projective planes.* Bulletin of AS of RM, Mathematics, 2001, N 2(36), p. 125–135.

[10] Kuznetsov E.A. *Transversals in loops: Abstracts of International Conference "Loops'03".* Prague, August 10-17, 2003, p. 18–20.

[11] Kuznetsov E.A. *Transversals in loops. 1. Elementary properties and structural theorems* (to appear).

[12] Kuznetsov E.A *Permutation loops* (to appear).

[13] Pflugfelder H. *Quasigroups and Loops: Introduction.* Sigma Series in Pure Math., 7, Helderman Verlag, New York, 1972.

[14] Bonetti F., Lunardon G., Strambach K. *Cappi di permutazionni.* Rend. Math., 1979, **12**, N 3-4, p. 383–395.

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

Received August 22, 2005

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 115–122
ISSN 1024–7696

Multiobjective Games and Determining Pareto-Nash Equilibria

D. Lozovanu, D. Solomon, A. Zelikovsky

Abstract. We consider the multiobjective noncooperative games with vector payoff functions of players. Pareto-Nash equilibria conditions for such class of games are formulated and algorithms for determining Pareto-Nash equilibria are proposed.

Mathematics subject classification: 90B10, 90C35, 90C27.
Keywords and phrases: Multicriterion problem, Pareto optimum, noncooperative games, Nash equilibria, Pareto-Nash equilibria, multiobjective games.

1 Introduction and Problem Formulation

In this paper we consider multiobjective games, which generalize noncooperative ones [1–3] and Pareto multicriterion problems [4, 5]. The payoff functions of players in such games are presented as vector functions, where players intend to optimize them in the sense of Pareto on their sets of strategies. At the same time in our game model it is assumed that players are interested to preserve Nash optimality principle when they interact between them on the set of situations. Such statement of the game leads to a new equilibria notion which we call Pareto-Nash equilibria.

The multiobjective game with p players is denoted by $\overline{G} = (X_1, X_2, \dots, X_p, \overline{F}_1, \overline{F}_2, \dots, \overline{F}_p)$, where X_i is the set of strategies of player i, $i = \overline{1,p}$, and $\overline{F}_i = (F_i^1, F_i^2, \dots, F_i^{r_i})$ is the vector payoff function of player i, defined on set of situations $X = X_1 \times X_2 \times \cdots \times X_p$:

$$\overline{F}_i \ : \ X_1 \times X_2 \times \cdots \times X_p \to R^{r_i}, \ i = \overline{1,p}.$$

Each component F_i^k of $\overline{F}_i$ corresponds to a partial criterion of player i and represents a real function defined on set of situations $X = X_1 \times X_2 \times \cdots \times X_p$:

$$F_i^k \ : \ X_1 \times X_2 \times \cdots \times X_p \to R^1, \ k = \overline{1,r_i}, \ i = \overline{1,p}.$$

We call the solution of the multiobjective game $\overline{G} = (X_1, X_2, \dots, X_p, \overline{F}_1, \overline{F}_2, \dots, \overline{F}_p)$ Pareto-Nash equilibrium and define it in the following way.

Definition 1. The situation $x^* = (x_1^*, x_2^*, \dots, x_p^*) \in X$ is called Pareto-Nash equilibrium for the multiobjective game $\overline{G} = (X_1, X_2, \dots, X_p, \overline{F}_1, \overline{F}_2, \dots, \overline{F}_p)$ if for every

$i \in \{1, 2, \ldots, p\}$ the strategy x_i^* represents Pareto solution for the following multicriterion problem:

$$\max_{x_i \in X_i} \to \overline{f}^i_{x^*}(x_i) = (f^{i1}_{x^*}(x_i), f^{i2}_{x^*}(x_i), \ldots, f^{ir_i}_{x^*}(x_i)),$$

where

$$f^{ik}_{x^*}(x_i) = F^k_i(x_1^*, x_2^*, \ldots, x_{i-1}^*, x_i, x_{i+1}^*, \ldots, x_p^*),\ k = \overline{1, r_i},\ i = \overline{1, p}.$$

This definition generalizes well-known Nash equilibria notion for classical noncooperative games (single objective games) and Pareto optimum for multicriterion problems. If $r_i = 1$, $i = \overline{1, p}$, then $\overline{G}$ becomes classical noncooperative game, where x^* represents Nash equilibria solution; in the case $p = 1$ the game $\overline{G}$ becomes Pareto multicriterion problem, where x^* is Pareto solution.

An important special class of multiobjective games represents zero-sum games of two players. This class is obtained from general case of the multiobjective game $\overline{G} = (X_1, X_2, \ldots, X_p, \overline{F}_1, \overline{F}_2, \ldots, \overline{F}_p)$ when $p = 2$, $r_1 = r_2 = r$ and $\overline{F}_2(x_1, x_2) = -\overline{F}_1(x_1, x_2)$.

Zero-sum multiobjective game is denoted $\overline{G} = (X_1, X_2, \overline{F})$, where $\overline{F}(x_1, x_2) = \overline{F}_2(x_1, x_2) = -\overline{F}_1(x_1, x_2)$. Pareto-Nash equilibrium for this game corresponds to saddle point $x^* = (x_1^*, x_2^*) \in X_1 \times X_2$ for the following max-min multiobjective problem:

$$\max_{x_1 \in X_1} \min_{x_2 \in X_2} \to \overline{F}(x_1, x_2) = (F^1(x_1, x_2), F^2(x_1, x_2), \ldots, F^r(x_1, x_2)). \quad (1)$$

Strictly we define the saddle point $x^* = (x_1^*, x_2^*) \in X_1 \times X_2$ for zero-sum multiobjective problem (1) in the following way.

Definition 2. The situation $(x_1^*, x_2^*) \in X_1 \times X_2$ is called the saddle point for max-min multiobjective problem (1) (i.e. for zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$) if x_1^* is Pareto solution for multicriterion problem:

$$\max_{x_1 \in X_1} \to \overline{F}(x_1, x_2^*) = (F^1(x_1, x_2^*), F^2(x_1, x_2^*), \ldots, F^r(x_1, x_2^*)),$$

and x_2^* is Pareto solution for multicriterion problem:

$$\min_{x_2 \in X_2} \to \overline{F}(x_1^*, x_2) = (F^1(x_1^*, x_2), F^2(x_1^*, x_2), \ldots, F^r(x_1^*, x_2)).$$

If $r = 1$ this notion corresponds to classical saddle point notion for min-max problems, i.e. we obtain saddle point notion for classical zero-sum games of two players.

In this paper we show that theorems of J. Nash [2] and J. Neumann [1] related to classical noncooperative games can be extended for our multiobjective case of games. Moreover, we show that all results related to discrete multiobjective games, especially matrix games can be developed in analogous way as for classical ones. Algorithms for determining the optimal strategies of players in considered games will be developed.

2 The main results

First we formulate the main theorem which represents an extension of the Nash theorem for our multiobjective version of the game.

Theorem 1. *Let $\overline{G} = (X_1, X_2, \ldots, X_p, \overline{F}_1, \overline{F}_2, \ldots, \overline{F}_p)$ be a multiobjective game, where $X_1, X_2, \ldots, X_p$ are convex compact sets and $\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_p$ represent continuous vector payoff functions. Moreover, let us assume that for every $i \in \{1, 2, \ldots, p\}$ each component $F_i^k(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_p)$, $k \in \{1, 2, \ldots, r_i\}$, of the vector function $\overline{F}_i(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_p)$ represents a concave function with respect to x_i on X_i for fixed $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_p$. Then for multiobjective game $\overline{G} = (X_1, X_2, \ldots, X_p, \overline{F}_1, \overline{F}_2, \ldots, \overline{F}_p)$ there exists Pareto-Nash equilibria situation $x^* = (x_1^*, x_2^*, \ldots, x_p^*) \in X_1 \times X_2 \times \cdots \times X_p$.*

Proof. Let $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1}, \alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2}, \ldots, \alpha_{p1}, \alpha_{p2}, \ldots, \alpha_{pr_p}$ be an arbitrary set of real numbers which satisfy the following condition

$$\begin{cases} \sum_{k=1}^{r_i} \alpha_{ik} = 1, & i = \overline{1,p}; \\ \alpha_{ik} > 0, & k = \overline{1,r_i},\ i = \overline{1,p}. \end{cases} \tag{2}$$

We consider an auxiliary noncooperative game (single objective game) $G = (X_1, X_2, \ldots, X_p, f_1, f_2, \ldots, f_p)$, where

$$f_i(x_1, x_2, \ldots, x_p) = \sum_{k=1}^{r_i} \alpha_{ik} F_i^k(x_1, x_2, \ldots, x_p),\ i = \overline{1,p}.$$

It is evident that $f_i(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_p)$ for every $i \in \{1, 2, \ldots, p\}$ represents a continuous and concave function with respect to x_i on X_i for fixed $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_p$ because $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1}, \alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2}, \ldots, \alpha_{p1}, \alpha_{p2}, \ldots, \alpha_{pr_p}$ satisfy condition (2) and $F_i^k(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_p)$ is a continuous and concave function with respect to x_i on X_i for fixed $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_p$, $k = \overline{1,r_i}$, $i = \overline{1,p}$.

According to Nash theorem [2] for the noncooperative game $G = (X_1, X_2, \ldots, X_p, f_1, f_2, \ldots, f_p)$ there exists Nash equilibria situation $x^* = (x_1^*, x_2^*, \ldots, x_p^*)$, i.e.

$$f_i(x_1^*, x_2^*, \ldots, x_{i-1}^*, x_i, x_{i+1}^*, \ldots, x_p^*) \leq$$
$$\leq f_i(x_1^*, x_2^*, \ldots, x_{i-1}^*, x_i^*, x_{i+1}^*, \ldots, x_p^*)$$
$$\forall x_i \in X_i,\ i = \overline{1,p}.$$

Let us show that $x^* = (x_1^*, x_2^*, \ldots, x_p^*)$ is Pareto-Nash equilibria solution for multiobjective game $\overline{G} = (X_1, X_2, \ldots, X_p, \overline{F}_1, \overline{F}_2, \ldots, \overline{F}_p)$. Indeed, for every $x_i \in X_i$ we have

$$\sum_{k=1}^{r_i} \alpha_{ik} F_i^k(x_1^*, x_2^*, \ldots, x_{i-1}^*, x_i, x_{i+1}^*, \ldots, x_p^*) =$$

$$= f_i(x_1^*, x_2^*, \dots, x_{i-1}^*, x_i, x_{i+1}^*, \dots, x_p^*) \leq$$
$$\leq f_i(x_1^*, x_2^*, \dots, x_{i-1}^*, x_i^*, x_{i+1}^*, \dots, x_p^*) =$$
$$= \sum_{k=1}^{r_i} \alpha_{ik} F_i^k(x_1^*, x_2^*, \dots, x_{i-1}^*, x_i^*, x_{i+1}^*, \dots, x_p^*)$$
$$\forall x_i \in X_i, \ i = \overline{1,p}.$$

So,

$$\sum_{k=1}^{r_i} \alpha_{ik} F_i^k(x_1^*, x_2^*, \dots, x_{i-1}^*, x_i, x_{i+1}^*, \dots, x_p^*) \leq$$
$$\leq \sum_{k=1}^{r_i} \alpha_{ik} F_i^k(x_1^*, x_2^*, \dots, x_{i-1}^*, x_i^*, x_{i+1}^*, \dots, x_p^*), \tag{3}$$
$$\forall x_i \in X_i, \ i = \overline{1,p},$$

for given $\alpha_{11}, \alpha_{12}, \dots, \alpha_{1r_1}, \alpha_{21}, \alpha_{22}, \dots, \alpha_{2r_2}, \dots, \alpha_{p1}, \alpha_{p2}, \dots, \alpha_{pr_p}$, which satisfy (2).

Taking in account that the functions $f_{x^*}^{i_k} = F_i^k(x_1^*, x_2^*, \dots, x_{i-1}^*, x_i, x_{i+1}^*, \dots, x_p^*)$, $k = \overline{1, r_i}$, are concave functions with respect to x_i on convex set X_i and $\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ik}$ satisfy the condition $\sum_{k=1}^{r_i} \alpha_{ik} = 1$, $\alpha_{ik} > 0$, $k = \overline{1, r_i}$, then according to Theorem 1 from [6] (see also [7–9]) the condition (3) implies that x_i^* is Pareto solution for the following multicriterion problem:

$$\max_{x_i \in X_i} \to \overline{f}_{x^*}^i(x_i) = (f_{x^*}^{i1}(x_i), f_{x^*}^{i2}(x_i), \dots, f_{x^*}^{ir_i}(x_i)), \ i \in \{1, 2, \dots, p\}.$$

This means that $x^* = (x_1^*, x_2^*, \dots, x_p^*)$ is Pareto-Nash equilibria solution for multiobjective game $\overline{G} = (X_1, X_2, \dots, X_p, \overline{F}_1, \overline{F}_2, \dots, \overline{F}_p)$. □

So, if conditions of Theorem 1 are satisfied then Pareto-Nash equilibria solution for multiobjective game can be found by using the following algorithm.

Algorithm 1

1. Fix an arbitrary set of real numbers $\alpha_{11}, \alpha_{12}, \dots, \alpha_{1r_1}, \alpha_{21}, \alpha_{22}, \dots, \alpha_{2r_2}, \dots, \alpha_{p1}, \alpha_{p2}, \dots, \alpha_{pr_p}$, which satisfy condition (2);
2. Form the single objective game $G = (X_1, X_2, \dots, X_p, f_1, f_2, \dots, f_p)$, where

$$f_i(x_1, x_2, \dots, x_p) = \sum_{k=1}^{r_i} \alpha_{ik} F_i^k(x_1, x_2, \dots, x_p), \ i = \overline{1,p};$$

3. Find Nash equilibria $x^* = (x_1^*, x_2^*, \dots, x_p^*)$ for noncooperative game $G = (X_1, X_2, \dots, X_p, f_1, f_2, \dots, f_p)$ and fix x^* as a Pareto-Nash equilibria solution for multiobjective game $\overline{G} = (X_1, X_2, \dots, X_p, \overline{F}_1, \overline{F}_2, \dots, \overline{F}_p)$.

Remark 1. Algorithm 1 finds only one of the solutions for multiobjective game $\overline{G} = (X_1, X_2, \ldots, X_p, \overline{F}_1, \overline{F}_2, \ldots, \overline{F}_p)$. In order to find all solutions in Pareto-Nash sense it is necessary to apply algorithm 1 for every $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1}, \alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2}, \ldots, \alpha_{p1}, \alpha_{p2}, \ldots, \alpha_{pr_p}$ which satisfy (2) and then to form the union of all obtained solutions.

Note that the proof of Theorem 1 is based on reduction the multiobjective game $\overline{G} = (X_1, X_2, \ldots, X_p, \overline{F_1}, \overline{F_2}, \ldots, \overline{F_p})$ to the auxiliary one $G = (X_1, X_2, \ldots, X_p, f_1, f_2, \ldots, f_p)$ for which Nash theorem from [2] can be applied. In order to reduce multiobjective game $\overline{G}$ to auxiliary one G linear convolution criteria for vector payoff functions in the proof of Theorem 1 have been used. Perhaps similar reduction of the multiobjective game to classical one can be used also applying other convolution procedures for vector payoff functions of players, as example the standard procedure for multicriterion problem from [6–9].

For zero-sum multiobjective game of two players the following theorem holds.

Theorem 2. *Let $\overline{G} = (X_1, X_2, \overline{F})$ be a zero-sum multiobjective game of two players, where X_1, X_2 are convex compact sets and $\overline{F}(x_1, x_2)$ is a continuous vector function on $X_1 \times X_2$. Moreover, let us assume that each component $F^k(x_1, x_2)$, $k \in \{1, 2, \ldots, r\}$, of $\overline{F}(x_1, x_2)$ for fixed $x_1 \in X_1$ represents a convex function with respect to x_2 on X_2 and for every fixed $x_2 \in X_2$ it is a concave function with respect to x_1 on X_1. Then for zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$ there exists saddle point $x^* = (x_1^*, x_2^*) \in X_1 \times X_2$, i.e. x_1^* is Pareto solution for multicriterion problem:*

$$\max_{x_1 \in X_1} \to \overline{F}(x_1, x_2^*) = (F^1(x_1, x_2^*), F^2(x_1, x_2^*), \ldots, F^r(x_1, x_2^*))$$

and x_2^* is Pareto solution for multicriterion problem:

$$\min_{x_2 \in X_2} \to \overline{F}(x_1^*, x_2) = (F^1(x_1^*, x_2), F^2(x_1^*, x_2), \ldots, F^r(x_1^*, x_2)).$$

Proof. The proof of Theorem 2 can be obtained as a corollary from Theorem 1 if we will regard our zero-sum game as a game of two players of the form $\overline{G} = (X_1, X_2, \overline{F}_1(x_1, x_2), \overline{F}_2(x_1, x_2)$, where $\overline{F}_2(x_1, x_2) = -\overline{F}_1(x_1, x_2) = \overline{F}(x_1, x_2)$.

The proof of Theorem 2 can be obtained also by reducing our zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$ to classical single objective case $G = (X_1, X_2, f)$ and applying J. Neumann theorem from [1], where

$$f(x_1, x_2) = \sum_{k=1}^{r} \alpha_k F^k(x_1, x_2)$$

and $\alpha_1, \alpha_2, \ldots, \alpha_r$ are arbitrary real numbers such that

$$\sum_{k=1}^{r} \alpha_k = 1; \ \alpha_k > 0, \ k = \overline{1, r}.$$

It is easy to show that if $x^* = (x_1^*, x_2^*)$ is a saddle point for zero-sum game $G = (X_1, X_2, f)$ then $x^* = (x_1^*, x_2^*)$ represents a saddle point for zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$. □

So, if conditions of Theorem 2 are satisfied then a solution of zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$ can be found by using the following algorithm.

Algorithm 2

1. Fix an arbitrary set of real numbers $\alpha_1, \alpha_2, \dots, \alpha_r$ such that $\sum\limits_{k=1}^{r} \alpha_k = 1$; $\alpha_k > 0$, $k = \overline{1, r}$;

2. Form the zero-sum game $G = (X_1, X_2, f)$, where $f(x_1, x_2) = \sum\limits_{k=1}^{r} \alpha_k F^k(x_1, x_2)$.

3. Find a saddle point $x^* = (x_1^*, x_2^*)$ for single zero-sum game $G = (X_1, X_2, f)$. Then fix $x^* = (x_1^*, x_2^*)$ as a saddle point for zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$.

Remark 2. Algorithm 2 finds only a solution for given zero-sum multiobjective game $\overline{G} = (X_1, X_2, \overline{F})$. In order to find all saddle points it is necessary to apply algorithm 2 for every $\alpha_1, \alpha_2, \dots, \alpha_r$ satisfying conditions $\sum\limits_{k=1}^{r} \alpha_k = 1$; $\alpha_k > 0$, $k = \overline{1, r}$, and then to form the union of obtained solutions.

Note that for reducing the zero-sum multiobjective games to classical ones also can be used other convolution criteria for vector payoff functions, i.e. the standard procedure from [7–9].

3 Discrete and matrix multiobjective games

Discrete multiobjective games are determined by the discrete structure of sets of strategies $X_1, X_2, \dots, X_p$. If $X_1, X_2, \dots, X_p$ are finite sets then we may consider $X_i = J_i$, $J_i = \{1, 2, \dots, q_i\}$, $i = \overline{1, p}$. In this case the multiobjective game is determined by vectors

$$\overline{F}_i = (F_i^1, F_i^2, \dots, F_i^{r_i}),\ i = \overline{1, p},$$

where each component F_i^k, $k = \overline{1, r_i}$, represents p-dimensional matrix of size $q_1 \times q_2 \times \dots \times q_p$.

If $p = 2$ then we have bimatrix multiobjective game and if $F_2 = -F_1$ then we obtain matrix multiobjective one. In analogous way as for single objective matrix games here we can interpret the strategies $j_i \in J_i$, $i = \overline{1, p}$, of players as pure strategies.

It is evident that for such matrix multiobjective games Pareto-Nash equilibria may not exist because Nash equilibria may not exist for bimatrix and matrix games in pure strategies. But to each finite discrete multiobjective game we can associate a continuous multiobjective game $\overline{\overline{G}} = (Y_1, Y_2, \dots, Y_p, \overline{f}_1, \overline{f}_2, \dots, \overline{f}_p)$ by introducing mixed strategies $y_i = (y_{i1}, y_{i2}, \dots, y_{ir_i}) \in Y_i$ of player i and vector payoff functions $\overline{f}_1, \overline{f}_2, \dots, \overline{f}_p$, which we define in the following way:

$$Y_i = \{y_i = (y_{i1}, y_{i2}, \dots, y_{ir_i}) \in R^{r_i} \Big| \sum_{j=1}^{r_i} y_{ij} = 1, y_{ij} \geq 0, j = \overline{1, r_i}\};$$

$$\overline{f}_i = (f_i^1, f_i^2, \dots, f_i^{r_i}),$$

where

$$f_i^k(y_{11}, y_{12}, \dots, y_{1r_1}, y_{21}, y_{22}, \dots, y_{2r_2}, \dots, y_{p1}, y_{p2}, \dots, y_{pr_p}) =$$
$$= \sum_{j_1=1}^{r_1} \sum_{j_2=1}^{r_2} \cdots \sum_{j_p=1}^{r_p} F^k(j_1, j_2, \dots, j_p) y_{ij_1} y_{ij_2} \dots y_{ij_p}; \quad k = \overline{1, r_i}, \ i = \overline{1, p}.$$

It is easy to observe that for auxiliary multiobjective game $\overline{\overline{G}} = (Y_1, Y_2, \dots, Y_p, \overline{f}_1, \overline{f}_2, \dots, \overline{f}_p)$ conditions of theorem 1 are satisfied and therefore Pareto-Nash equilibria $y^* = (y_{11}^*, y_{12}^*, \dots, y_{1r_1}^*, y_{21}^*, y_{22}^*, \dots, y_{2r_2}^*, \dots, y_{p1}^*, y_{p2}^*, \dots, y_{pr_p}^*)$ exist.

In the case of matrix games the auxiliary zero-sum multiobjective game of two players is defined as follows: $\overline{\overline{G}} = (Y_1, Y_2, \overline{f})$;

$$Y_1 = \{y_1 = (y_{11}, y_{12}, \dots, y_{1r}) \in R^r \Big| \sum_{j=1}^{r} y_{1j} = 1, y_{1j} \geq 0, j = \overline{1, r}\};$$
$$Y_2 = \{y_2 = (y_{21}, y_{22}, \dots, y_{2r}) \in R^r \Big| \sum_{j=1}^{r} y_{2j} = 1, y_{2j} \geq 0, j = \overline{1, r}\};$$

$$\overline{f} = (f^1, f^2, \dots, f^r),$$
$$f^k(y_{11}, y_{12}, \dots, y_{1r}, y_{21}, y_{22}, \dots, y_{2r}) = \sum_{j_1=1}^{r} \sum_{j_2=1}^{r} F^k(j_1, j_2) y_{1j_1} y_{2j_2};$$
$$k = \overline{1, r}.$$

The game $\overline{\overline{G}} = (Y_1, Y_2, \overline{f})$ satisfies conditions of theorem 2 and therefore a saddle point $y^* = (y_1^*, y_2^*) \in Y_1 \times Y_2$ exists.

So, the results related to discrete and matrix game can be extended for multiobjective case of the game and can be interpreted in analogous way as for single objective games. In order to solve these associated multiobjective games algorithms 1 and 2 can be applied.

4 Conclusion

The considered multiobjective games extend classical ones and represent a combination of cooperative and noncooperative games. Indeed, the player i in multiobjective game $\overline{G} = (X_1, X_2, \dots, X_p, \overline{F}_1, \overline{F}_2, \dots, \overline{F}_p)$ can be regarded as a union of r_i subplayers with payoff functions $F_i^1, F_i^2, \ldots, F_i^{r_i}$ respectively. So, the game $\overline{G}$ represents a game with p coalitions $1, 2, \ldots, p$ which interact between them on the set of situations $X_1 \times X_2 \times \cdots \times X_p$.

The introduced Pareto-Nash equilibria notion uses the concept of cooperative games because according to this notion subplayers of the same coalitions should optimize in the sense of Pareto their vector functions F_i on set of strategies X_i. On the other hand Pareto-Nash equilibria notion takes into account also the concept of noncooperative games because coalitions interact between them on the set of situations $X_1 \times X_2 \times \cdots \times X_p$ and are interested to preserve Nash equilibria between coalitions.

The obtained results allow us to describe a class of multiobjective games for which Pareto-Nash equilibria exists. Moreover, a suitable algorithm for finding Pareto-Nash equilibria is proposed.

References

[1] Neumann J., Morgenstern O. *Theory of games and economic behaviour.* Princeton, Princeton Univ. Press., 1953.

[2] Nash j. *Non-cooperative games.* Ann. Math., 1951, **54**, p. 286–295.

[3] Moulin H. *Theorie des Jeux pour l'economie et la politique.* Paris, 1981.

[4] Pareto V. *Manuel d'economie politique.* Giard, Paris, 1904.

[5] Podinovsky V,, Noghin V. *Pareto optimal solution for multicriterion problem.* Moscow, Nauka, 1982.

[6] Emelichev V., Perepelitsa V. *The complexity of discrete multicriterion problems.* Discrete mathematics and applications, 1994, N 6(1), p. 5–33.

[7] Brucher P. *Discrete parameter optimization problem and essential efficient points.* Operat. Res., 1972, N 16(5), p. 189–197.

[8] Burkard R., Krarup J., Pruzan P. *Efficiency and optimality in minisum, minimax* $0-1$ *progrmming problems.* J. Oper. Res. Soc., 1982, N 33(2), p. 137–151.

[9] Burkard R., Krarup J., Pruzan P. *A relationship between optimality and efficiency in multicriteria* $0-1$ *programming problems.* Comp. Oper. Res., 1981, N 8(2), p. 241–247.

D. Lozovanu, D. Solomon
Institute of Mathematics and Computer Science
5 Academiei Str.
Chişinău MD−2028, Moldova
E-mails:*lozovanu@math.md, cipti@softhome.net*

Received November 23, 2005

A. Zelikovsky
Georgia State University
34 Peachtree Str., Suite 1450
Atlanta, GA 30303, USA
E-mail:*alexz@cs.gsu.edu*

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 123–140
ISSN 1024–7696

On Bruck-Belousov Problem

Victor Shcherbacov

Abstract. In this paper on the language of subgroups of the multiplication group of a quasigroup (of the associated group of a quasigroup) necessary and sufficient conditions of normality of congruences of a left (right) loop are given. These conditions can be considered as a partial answer to the problem posed in books of R. H. Bruck and V.D. Belousov about conditions of normality of all congruences of quasigroups. Results on the regularity of congruences of quasigroups and the behavior of quasigroup congruences by isotopy are given.

Mathematics subject classification: 20N05.
Keywords and phrases: Quasigroup, congruence, normal congruence.

1 Introduction

The main purpose of this paper is an attempt to promote in solving the following Bruck-Belousov problem: *What loops G have the property that every image of G under a multiplicative homomorphism is also a loop [9, p. 92]? What quasigroups or loops in which all congruences are normal [5, Problem 20, p. 221]?*

We notice it is well known (see [3]), if homomorphic image of a multiplicative homomorphism φ of a loop is also a loop then congruence θ which corresponds to φ, is a normal congruence.

This article is an extended variant of the paper [27]. See also [28]. We shall use standard quasigroup notations and definitions from [5,6,11,23]. Information on lattices and universal algebras can be found in [10,20,30], on groups in [14,19], on semigroups in [12].

For convenience of readers we recall some well known definitions.

A groupoid $(Q,\cdot)$ in which for any fixed elements a,b from the set Q the equations $a\cdot x=b$ and $y\cdot a=b$ have unique solutions is called a *quasigroup*.

A quasigroup $(Q,\cdot)$ that has an element f such that $f\cdot x=x$ for all $x\in Q$ is called a *left loop*.

A quasigroup $(Q,\cdot)$ that has an element e such that $x\cdot e=x$ for all $x\in Q$ is called a *right loop*.

A quasigroup with the identity of associativity ($x\cdot yz=xy\cdot z$) is a group [19].

It is known (see [5]) that in a quasigroup left ($L_a: x\to a\cdot x$), right ($R_a: x\to x\cdot a$) translations, as well as its inverse, are permutations. Let $\mathbb{L}=\{L_a\,|\,a\in Q\}$, $\mathbb{R}=\{R_b\,|\,b\in Q\}$, $\mathbb{T}=\{L_a,R_b\,|\,a,b\in Q\}$.

By $\Pi(Q)$ or by Π for the short we shall designate a semigroup generated by the left and right translations of a quasigroup Q, i.e. elements of a semigroup $\Pi(Q)$ are words of the form $T_1^{\alpha_1}T_2^{\alpha_2}\dots T_n^{\alpha_n}$, where $T_i \in \mathbb{T}$, $\alpha_i \in \mathbb{N}$.

The group generated by all left and right translations of a quasigroup Q will be denoted by $M(Q)$, or by M for the short. Elements of the group M are words of the form $T_1^{\alpha_1}T_2^{\alpha_2}\dots T_n^{\alpha_n}$, where $T_i \in \mathbb{T}$, $\alpha_i \in \mathbb{Z}$.

A binary relation φ on a set Q is a subset of the cartesian product $Q \times Q$ [10,22].

As it is known ([10,12,20,30]), a binary relation q is an equivalence if and only if $\varepsilon \subseteq q$, $q^{-1} = q$, $q^2 = q$, where $\varepsilon = \{(x,x) \mid x \in Q\}$. We shall use both definitions: this definition and definition of equivalence as reflexive, symmetric and transitive relation on the language of pairs of elements.

A class of an equivalence θ that contains an element a will be denoted by $\theta(a)$.

An equivalence θ of a quasigroup $(Q,\cdot)$ such that from $a\theta b$ follows $(c\cdot a)\theta(c\cdot b)$ for all $a,b,c \in Q$ is called a *left congruence* of a quasigroup $(Q,\cdot)$.

An equivalence θ of a quasigroup $(Q,\cdot)$ such that from $a\theta b$ follows $(a\cdot c)\theta(b\cdot c)$ for all $a,b,c \in Q$ is called a *right congruence* of a quasigroup $(Q,\cdot)$.

A left and right congruence θ of a quasigroup $(Q,\cdot)$ is called a *congruence* of a quasigroup $(Q,\cdot)$ [5,6].

A congruence θ of a quasigroup $(Q,\cdot)$ is called *normal,* if from $(a\cdot c)\theta(b\cdot c)$ follows $a\theta b$, from $(c\cdot a)\theta(c\cdot b)$ follows $a\theta b$ for all $a,b,c \in Q$.

We shall call a binary relation θ of a groupoid $(Q,\cdot)$ *stable from the left* (accordingly from the right) if from $x\theta y$ it follows $(a\cdot x)\theta(a\cdot y)$, (accordingly $(x\cdot a)\theta(y\cdot a)$) for all $a \in Q$.

It is easy to see that a stable from the left (from the right) equivalence of a quasigroup $(Q,\cdot)$ is called a *left (right) congruence.* A congruence is an equivalence relation which is stable from the left and from the right.

Definition 1. *If θ is a binary relation on a set Q, α is a permutation of the set Q and from $x\theta y$ it follows $\alpha x\theta\alpha y$ for all $(x,y) \in \theta$, then we shall say that the permutation α is* ***semi-admissible relative to the relation*** *θ.*

Remark 1. We notice in [13] a permutation with such property is called an admissible permutation.

Definition 2. *If θ is a binary relation on a set Q, α is a permutation of the set Q and from $x\theta y$ it follows $\alpha x\theta\alpha y$ and $\alpha^{-1}x\theta\alpha^{-1}y$ for all $(x,y) \in \theta$, then we shall say that the permutation α is an* ***admissible permutation relative to the binary relation*** *θ [5].*

We recall any element of the group $M(Q)$ of a quasigroup Q is admissible relative to any normal congruence of the quasigroup Q; any element the semigroup $\Pi(Q)$ of a quasigroup Q is semi-admissible relative to any congruence of the quasigroup Q [5,6].

As it is known (see [5, 6]) to each homomorphism φ of a quasigroups Q it is possible to associate a congruence θ by the rule: $a\theta b$ if and only if $\varphi a = \varphi b$. In this case $\varphi Q \cong Q/\theta$.

As is was proved in [3], see also [5,11], homomorphic image of a quasigroups Q can be a quasigroup or a groupoid with division. If homomorphic image of a quasigroup is a quasigroup, then the congruence θ which corresponds to this homomorphism is normal, if φQ is a proper division groupoid, then congruence θ is not normal [6].

If φ and ψ are binary relations on Q, then their product is defined in the following way: $(a, b) \in \varphi \circ \psi$ if there is an element $c \in Q$ such that $(a, c) \in \varphi$ and $(c, b) \in \psi$ [12, 30]. The operation of product of binary relations is associative [12, 22, 24].

Below we shall designate product of binary relations and quasigroup operation by a point, by the letter Q we shall designate a quasigroup $(Q, \cdot)$ and a set on which this quasigroup is defined.

Lemma 1. *For all binary relations $\varphi, \psi, \theta \subseteq Q^2$ from $\varphi \subseteq \psi$ follows $\varphi\theta \subseteq \psi\theta$, $\theta\varphi \subseteq \theta\psi$, i.e. it is possible to say that a binary relation of set-theoretic inclusion of binary relations is stable from the left and from the right relative to the multiplication of binary relations.*

Proof. If $(x, z) \in \varphi\theta$, then there exists an element $y \in Q$, such that $(x, y) \in \varphi$ and $(y, z) \in \theta$. Since $\varphi \subseteq \psi$, then we have $(x, y) \in \psi$, $(x, z) \in \psi\theta$. $\square$

Remark 2. Translations of a quasigroup can be considered as binary relations: $(x, y) \in L_a$, if and only if $y = a \cdot x$, $(x, y) \in R_b$, if and only if $y = x \cdot b$.

Remark 3. To coordinate the multiplication of translations with their multiplication as binary relations, we use the following multiplication of translations: if α, β are translations, x is an element of the set Q, then $(\alpha\beta)(x) = \beta(\alpha(x))$, i.e. $(\alpha\beta)x = \beta\alpha\, x$.

A partially ordered set $(L, \subseteq)$ is called a lower (an upper) semilattice if any its two-element subset has exact lower (upper) bound, i.e. in a set L exists $\inf(a, b)$ ($\sup(a, b)$) for all $a, b \in L$ [10, 20].

If a partially ordered set is simultaneously the lower and upper semilattice, then it is called a *lattice*.

We can define a lattice as algebra $(L, \vee, \wedge)$ satisfying the following axioms ([10]):

$$\begin{array}{ll} (a \vee b) \vee c = a \vee (b \vee c); & a \vee b = b \vee a; \\ a \vee a = a; & (a \vee b) \wedge a = a; \\ (a \wedge b) \wedge c = a \wedge (b \wedge c); & a \wedge b = b \wedge a; \\ a \wedge a = a; & (a \wedge b) \vee a = a. \end{array}$$

We notice similarly as for quasigroups, which are defined in a signature with one and three binary operations, for the lattices which are defined in a signature with one binary operation $\leq$ and with two binary operations $\vee$ and $\wedge$, the concepts of a sublattice do not coincide. Namely, the sublattice of a lattice $(L, \vee, \wedge)$ always is a sublattice of a lattice $(L, \leq)$, but an inverse is not always correct [20].

2 Congruences of a quasigroup and its associated group

Connections between normal subloops of a loop Q and normal subgroups of the group $M(Q)$ were studied by A. Albert [1, 2]. Generalizations of Albert results on some classes of quasigroups can be found in works of V.A. Beglaryan [4] and K.K. Shchukin [29]. In these works also questions of the lattice embedding of lattices of some normal congruences of a quasigroup Q into the lattice of normal subgroups of the group $M(Q)$ are studied.

Proposition 1. *An equivalence θ is a congruence of a quasigroup Q if and only if $\theta\omega \subseteq \omega\theta$ for all $\omega \in \mathbb{T}$.*

Proof. Let θ be an equivalence, $\omega = L_a$. It is clear that $(x, z) \in \theta L_a$ is equivalent to that there exists an element $y \in Q$ such that $(x, y) \in \theta$ and $(y, z) \in L_a$. But if $(y, z) \in L_a$, $z = ay$, then $y = L_a^{-1}z$. Therefore, from the relation $(x, z) \in \theta L_a$ it follows that $(x, L_a^{-1}z) \in \theta$.

Let us prove that from $(x, L_a^{-1}z) \in \theta$ it follows $(x, z) \in \theta L_a$. We have $(x, L_a^{-1}z) \in \theta$ and $(L_a^{-1}z, z) \in L_a$, $(x, z) \in \theta L_a$. Thus $(x, z) \in \theta L_a$ is equivalent to $(x, L_a^{-1}z) \in \theta$.

Similarly, $(x, z) \in L_a\theta$ is equivalent to $(ax, z) \in \theta$. Now we can say that the inclusion $\theta\omega \subseteq \omega\theta$ by $\omega = L_a$ is equivalent to the following implication:

$$(x, L_a^{-1}z) \in \theta \Longrightarrow (ax, z) \in \theta$$

for all suitable $a, x, z \in Q$.

If we replace in the last implication z with $L_a z$, we shall obtain the following implication:

$$(x, z) \in \theta \Longrightarrow (ax, az) \in \theta$$

for all $a \in Q$.

Thus, the inclusion $\theta L_a \subseteq L_a\theta$ is equivalent to the stability of the relation θ from the left relative to an element a. Since the element a is an arbitrary element of the set Q, we have that the inclusion $\theta\omega \subseteq \omega\theta$ by $\omega \in \mathbb{L}$ is equivalent to the stability of the relation θ from the left.

Similarly, the inclusion $\theta\omega \subseteq \omega\theta$ for any $\omega \in \mathbb{R}$ is equivalent to the stability from the right of relation θ. Uniting the last two statements, we obtain required equivalence. □

Let us remark Proposition 1 can be deduced from results of the article of Thurston [26].

The following proposition is almost obvious corollary of Theorem 5 from [21].

Proposition 2. *An equivalence θ is a congruence of a quasigroup Q if and only if $\omega\theta(x) \subseteq \theta(\omega x)$ for all $x \in Q$, $\omega \in \mathbb{T}$.*

Proof. Let θ be an equivalence relation and for all $\omega \in \mathbb{T}$, $\omega\theta(x) \subseteq \theta(\omega x)$. We shall prove that from $a\theta b$ follows $ca\theta cb$, $ac\theta bc$ for all $c \in Q$.

By definition of the equivalence θ, $a\theta b$ is equivalent to $a \in \theta(b)$. Then $ca \in c\theta(b) \subseteq \theta(cb)$, $ca\theta cb$. Similarly, from $a\theta b$ follows $ac\theta bc$.

Converse. Let θ be a congruence. We shall prove that $c\,\theta(a) \subseteq \theta(ca)$ for all $c, a \in Q$. Let $x \in c\,\theta(a)$. Then $x = cy$, where $y \in \theta(a)$, that is $y\theta a$. Then, since θ is a congruence, we obtain $cy\theta ca$. Therefore $x = cy \in \theta(ca)$. Thus, $L_c\theta \subseteq \theta(ca)$. It is similarly proved that $R_c\theta(a) \subseteq \theta(ac)$. □

Corollary 1. *An equivalence θ of a quasigroup $(Q, \cdot)$ is a congruence if and only if $\theta\omega \subseteq \omega\theta$ for all $\omega \in \Pi$.*

Proof. The multiplication of binary relations is associative, therefore, if $\theta\omega_1 \subseteq \omega_1\theta$, $\theta\omega_2 \subseteq \omega_2\theta$, where $\omega_1, \omega_2 \in \Pi$, then $\theta(\omega_1\omega_2) = (\theta\omega_1)\omega_2 \subseteq (\omega_1\theta)\omega_2 = \omega_1(\theta\omega_2) \subseteq \omega_1(\omega_2\theta) = (\omega_1\omega_2)\theta$. □

Corollary 2. *An equivalence θ is a congruence of a quasigroup Q if and only if $\omega\theta(x) \subseteq \theta(\omega x)$ for all $x \in Q$, $\omega \in \Pi$.*

Proof. The proof is similar with the previous one. □

Corollary 3. *A congruence θ of a quasigroup Q is normal if and only if at least one of the following conditions is fulfilled:*
(i) $\omega\theta \subseteq \theta\omega$ *for all* $\omega \in \mathbb{T}$;
(ii) $\omega\theta = \theta\omega$ *for all* $\omega \in \mathbb{T}$;
(iii) $\theta(\omega x) \subseteq \omega\theta(x)$ *for all* $\omega \in \mathbb{T}$, $x \in Q$;
(vi) $\theta(\omega x) = \omega\theta(x)$ *for all* $\omega \in \mathbb{T}$, $x \in Q$.

Proof. As it is proved in Proposition 1, the inclusion $\theta L_a \subseteq L_a\theta$ is equivalent to the implication $x\theta y \Longrightarrow ax\theta ay$.

Let us check up that the inclusion $L_a\theta \subseteq \theta L_a$ is equivalent to the implication

$$ax\theta ay \Rightarrow x\theta y.$$

Indeed, as it is proved in Proposition 1, $(x, z) \in \theta L_a$ is equivalent with $(x, L_a^{-1}z) \in \theta$. Similarly, $(x, z) \in L_a\theta$ is equivalent with $(ax, z) \in \theta$. The inclusion $\omega\theta \subseteq \theta\omega$ by $\omega = L_a$ has the form $L_a\theta \subseteq \theta L_a$ and it is equivalent to the following implication:

$$(ax, z) \in \theta \Longrightarrow (x, L_a^{-1}z) \in \theta$$

for all $a, x, z \in Q$. If we change in the last implication the element z by the element L_az, we shall obtain that the inclusion $\theta L_a \supseteq L_a\theta$ is equivalent to the implication $ax\theta ay \Rightarrow x\theta y$. Therefore, the equivalence θ is cancellative from the left.

Similarly, the inclusion $R_b\theta \subseteq \theta R_b$ is equivalent to the implication:

$$(xa, za) \in \theta \Longrightarrow (x, z) \in \theta.$$

If a congruence θ is cancellative from the left and from the right, then, by definition, θ is a normal congruence.

Cases *(ii), (iii), (iv)* are proved similarly. □

Corollary 4. *A congruence θ of a quasigroup Q is normal if and only if $\omega\theta = \theta\omega$ for all $\omega \in \Pi$.*

A congruence θ of a quasigroup Q is normal if and only if $\omega\theta = \theta\omega$ for all $\omega \in M$.

Proof. The proof is obvious. □

It is easy to see that an equivalence q of a set M is a congruence of the group M if and only if q is admissible relative to all elements of the set $\mathbb{T} \cup \mathbb{T}^{-1}$, where $\mathbb{T}^{-1} = \{L_x^{-1}, R_x^{-1} \,|\, \forall\, x \in Q\}$.

Theorem 1. *The lattice of congruences $(L(Q), \leq_1)$ of one-sided loop (in particular, of a loop) Q is isomorphically embedded in the lattice $(L(M(Q)), \leq_2)$ of the left congruences of group M, which are semi-admissible from the right relative to all permutations of the semigroup Π.*

Proof. The proof of this theorem in some parts repeats the proof of the theorem on an isomorphic embedding of normal congruences of a quasigroup Q in the lattice of congruences of the group $M(Q)$ [26].

By a quasigroup Q during the proof of this theorem we shall understand a quasigroup with the right unit, i.e. right loop.

Let q be a congruence of a quasigroup Q. We shall define the relation $q^{\top}$ in group M as follows: $\theta q^{\top} \varphi \Longleftrightarrow \theta^{-1}\varphi \subseteq q$ for all $\theta, \varphi \in M$.

We prove that $q^{\top}$ is a left congruence of the group M which is admissible from the right relative to all permutations α, $\alpha \in \Pi$.

Reflexivity of $q^{\top}$. Since $\varepsilon \subseteq q$, $\alpha q^{\top} \alpha$ for all $\alpha \in M$.

Symmetry of $q^{\top}$. The equivalence $\theta q^{\top} \varphi \leftrightarrow \varphi q^{\top} \theta$ is equivalent to the equivalence $\theta^{-1}\varphi \subseteq q \leftrightarrow \varphi^{-1}\theta \subseteq q$. The last equivalence is true since, if $\theta^{-1}\varphi \subseteq q$, then $(\theta^{-1}\varphi)^{-1} \subseteq q^{-1}$, $\varphi^{-1}\theta \subseteq q^{-1} = q$. It is clear that in the same way it is possible to receive also an inverse implication: $(\varphi^{-1}\theta \subseteq q) \rightarrow (\theta^{-1}\varphi \subseteq q)$.

Transitivity of $q^{\top}$. An implication $\theta q^{\top} \varphi \wedge \varphi q^{\top} \psi \rightarrow \theta q^{\top} \psi$ is equivalent with the implications $\theta^{-1}\varphi \subseteq q \wedge \varphi^{-1}\psi \subseteq q \rightarrow \theta^{-1}\psi \subseteq q$. We shall show that the last implication is fulfilled. Indeed, if $\theta^{-1}\varphi \subseteq q \wedge \varphi^{-1}\psi \subseteq q$, $\theta^{-1}\varphi\varphi^{-1}\psi = \theta^{-1}\psi \subseteq q^2 = q$.

Let us show that $q^{\top}$ is semi-admissible from the left relative to any permutation $\alpha \in M$. Indeed, the condition "if $\theta q^{\top} \varphi$, then $\alpha\theta q^{\top} \alpha\varphi$" is equivalent with the following condition: if $\theta^{-1}\varphi \subseteq q$, then $\theta^{-1}\alpha^{-1}\alpha\varphi = \theta^{-1}\varphi \subseteq q$.

Let us show that the binary relation $q^{\top}$ (we have already proved that $q^{\top}$ is a left congruence of M) is semi-admissible from the right relative to any permutation $\alpha \in \Pi$. For this purpose we shall show that $\theta\alpha q^{\top} \varphi\alpha$ for all $\alpha \in \Pi$. We shall pass, using Proposition 1, to the needed inclusions.

Then we have $\theta q^{\top} \varphi \leftrightarrow \theta^{-1}\varphi \subseteq q$, $\theta\alpha q^{\top} \varphi\alpha \leftrightarrow \alpha^{-1}\theta^{-1}\varphi\alpha \subseteq q$. Since q is a congruence, then by Corollary 1 we have $\alpha^{-1} q \alpha \subseteq q$ for all $\alpha \in \Pi$. Therefore, if $\theta^{-1}\varphi \subseteq q$, then $\alpha^{-1}\theta^{-1}\varphi\alpha \subseteq \alpha^{-1} q \alpha \subseteq q$.

Thus, we have proved that an arbitrary congruence of a quasigroup Q corresponds the left congruence $q^{\top}$ of the group M which is semi-admissible from the right relative to all permutations of the semigroup Π.

Let p be a left congruence of the group M, that is semi-admissible from the right relative to all $\alpha \in \Pi$. We shall define a binary relation on a quasigroup Q in the following way: $p^{\perp} = \cup\, \theta^{-1}\varphi$ for all $\theta, \varphi \in M$, such that $\theta\, p\, \varphi$.

We demonstrate that $p^{\perp}$ is a congruence of a quasigroup Q.

Reflexivity of $p^{\perp}$. Since $\theta\, p\, \theta$ for all $\theta \in M$, then $\theta^{-1}\theta = \varepsilon \subseteq p^{\perp}$.

Symmetry of $p^{\perp}$. $(p^{\perp})^{-1} = p^{\perp}$, since $p^{-1} = p$ and $p^{\perp} = \cup\, \theta^{-1}\varphi$ for all $\theta, \varphi \in M$, such that $\theta\, p\, \varphi$.

Transitivity of $p^{\perp}$. Let $(a, b) \in (p^{\perp})^2$, i.e. there exists element c such that $ap^{\perp}c$ and $cp^{\perp}b$. Hence, there exist $\theta, \varphi, \psi, \xi \in M$, $\theta p \varphi$, $\psi p \xi$, such that $a\theta^{-1}\varphi c$ and $c\psi^{-1}\xi b$. Then $c = (\theta^{-1}\varphi)\, a, b = (\psi^{-1}\xi)\, c$, and $b = (\theta^{-1}\varphi\psi^{-1}\xi)\, a$, i. e. $(a, b) \in (\varphi^{-1}\theta)^{-1}\psi^{-1}\xi$.

We need to prove that $\varphi^{-1}\theta\, p\, \psi^{-1}\xi$. If $\theta\, p\, \varphi$, then taking into account that the binary relation p is stable from the left relative to any permutation $\alpha \in M$, we obtain, $\varphi^{-1}\theta\, p\, \varphi^{-1}\varphi$, $\varphi^{-1}\theta\, p\, \varepsilon$.

Similarly, $\varepsilon\, p \psi^{-1}\xi$, and by transitivity of the relation p we have: $\varphi^{-1}\theta\, p\, \psi^{-1}\xi$. Thus, we have proved that p is an equivalence on Q.

Let us show that $p^{\perp}$ is a congruence of a quasigroup Q. For this purpose it is sufficient, taking into account Corollary 1, to prove that for all $\omega \in \Pi$, $\omega^{-1}\, p^{\perp}\, \omega \subseteq p^{\perp}$.

Let $(a, b) \in \omega^{-1}p^{\perp}\omega$. Then there exist $\varphi, \theta \in M$, $\theta p \varphi$ such that $(a, b) \in \omega^{-1}\theta^{-1}\varphi\omega = (\theta\omega)^{-1}\varphi\omega$.

Since $\theta\, p\, \varphi$ then for all $\omega \in \Pi$, $\theta\omega\, p\, \varphi\omega$, and then $(\theta\omega)^{-1}\varphi\omega \subseteq p^{\perp}$.

Thus $(a, b) \in p^{\perp}$, $\omega^{-1}\, p^{\perp}\, \omega \subseteq p^{\perp}$ for all $\omega \in \Pi$, i.e. $p^{\perp}$ is a congruence of a quasigroup Q.

We prove if q is a congruence of a quasigroup Q, then $q^{\top\perp} = q$, i.e. we establish that the map $\top$ is a bijective map and that $(\top)^{-1} = \perp$.

It is easy to understand that $q^{\top\perp} \subseteq q$. Indeed, if $(a, b) \in (q^{\perp})^{\top}$ there is a pair of permutations $\varphi, \theta \in M$ such that $\theta q^{\top} \varphi$, $(a, b) \in \theta^{-1}\varphi$.

By definition of the relation $q^{\top}$, $\varphi q^{\top} \theta$ if and only if $\varphi^{-1}\theta \subseteq q$, and then $(a, b) \in q$.

Let us prove a converse inclusion. Now we use property that the quasigroup Q has the right unit.

Let $(a, b) \in q$. Then for all x from Q the relation $ax\, q\, bx$ is equivalent with $L_a x\, q\, L_b x$. Having replaced x by $L_a^{-1}x$, we obtain $x\, q\, (L_a^{-1}L_b)x$, i.e. $L_a^{-1}L_b \subseteq q$, and then $L_a q^{\top} L_b$, $L_a^{-1}L_b \subseteq (q^{\top})^{\perp}$. From the last relation we have $(a, (L_a^{-1}L_b)a) = (a, L_b e_a) = (a, b) \in (q^{\top})^{\perp}$, since $e_a = e_b$. Therefore $q \subseteq (q^{\top})^{\perp}$.

If we have quasigroup with the left unit, then instead of translations L_a, L_b we take translations R_a, R_b. Thus $(q^{\top})^{\perp} \supseteq q$, the map $\top$ is a bijective map, $(\top)^{-1} = \perp$.

Let us recall lattices $\mathcal{L}_1 = (L_1, \leq_1)$ and $\mathcal{L}_2 = (L_2, \leq_2)$ are called isomorphic if there is a bijective map σ such that $a \leq_1 b$ in $\mathcal{L}_1$ if and only if $\sigma(a) \leq_1 \sigma(b)$ in $\mathcal{L}_2$ [10].

In order to prove that $\top$ is a lattice isomorphism, we need to prove: if $q_1 \subseteq q_2$, then $q_1^\top \subseteq q_2^\top$, if $p_1 \subseteq p_2$, then $p_1^\perp \subseteq p_2^\perp$, where q_1, q_2 are congruences of a quasigroup Q, p_1, p_2 are the left congruences of group M that are semi-admissible relative to multiplication from the right on permutations α from the semigroup Π. These two implications, taking into account the definition of maps $\perp, \top$, are obvious. $\square$

Proposition 3. *If the lattice of congruences is considered as an algebra of the form $(L, \vee, \wedge)$, i.e. in a signature with two binary operations, then $(q_1 \wedge q_2)^\top = q_1^\top \wedge q_2^\top$.*

Proof. Indeed, the operation $\wedge$ both in a lattice of congruences of a quasigroup and in a lattice of the left congruences of group M coincides with the set-theoretic intersection of congruences. Therefore, if $(\alpha, \beta) \in (q_1 \wedge q_2)^\top$, then $\alpha^{-1}\beta \subseteq q_1 \wedge q_2$, $\alpha^{-1}\beta \subseteq q_1 \cap q_2$, $\alpha^{-1}\beta \subseteq q_1$, $\alpha^{-1}\beta \subseteq q_2$, $(\alpha, \beta) \in q_1^\top$, $(\alpha, \beta) \in q_2^\top$, $(\alpha, \beta) \in q_1^\top \cap q_2^\top = q_1^\top \wedge q_2^\top$.

Conversely, let $(\alpha, \beta) \in q_1^\top \wedge q_2^\top$. Then $\alpha^{-1}\beta \subseteq q_1$, $\alpha^{-1}\beta \subseteq q_2$, $\alpha^{-1}\beta \subseteq q_1 \cap q_2 = q_1 \wedge q_2$, $(\alpha, \beta) \in (q_1 \wedge q_2)^\top$. Thus, $(q_1 \wedge q_2)^\top = q_1^\top \wedge q_2^\top$. $\square$

Remark 4. It is easy to see that $q_1^\top \vee q_2^\top \subseteq (q_1 \vee q_2)^\top$. Indeed, $q_1^\top \subseteq (q_1 \vee q_2)^\top$, $q_2^\top \subseteq (q_1 \vee q_2)^\top$, $q_1^\top \vee q_2^\top \subseteq (q_1 \vee q_2)^\top \vee (q_1 \vee q_2)^\top = (q_1 \vee q_2)^\top$.

Probably, in general, there exist examples such that $q_1^\top \vee q_2^\top \subsetneqq (q_1 \vee q_2)^\top$. Results from [1, 2, 4, 29] strengthen our guess.

Since in Theorem 1 it is proved that the map $\top$ is bijective, we can formulate the following theorem.

Theorem 2. *The lower semilattice of congruences of an one-sided loop Q is isomorphically embedded in the lower semilattice of the left congruences of the group $M(Q)$ that are semi-admissible relative to all elements of the semigroup $\Pi(Q)$.*

Corollary 5. *The lower semilattice of congruences of an one-sided loop Q is isomorphically embedded in the lower semilattices of congruences: of the semigroup $L\Pi$, of the semigroup Π and of the left congruences of the group LM.*

Proof. By the intersection of the left congruences of group M with the set $L\Pi \times L\Pi$, for example, we obtain some binary relations of semigroup $L\Pi$.

It is easy to understand that these binary relations are equivalences which are semi-admissible relative to multiplication from the left and from the right by elements of the semigroup $L\Pi$, i.e. these equivalences are congruences of semigroup $L\Pi$.

Now we should prove: if $p_1 \subset p_2$ and $p_1^\perp \subset p_2^\perp$, then p_1, p_2 are elements of lattice of the left congruences of the group M, $p_1 \cap (L\Pi)^2 \subset p_2 \cap (L\Pi)^2$.

If $p_1 \subset p_2$ and $p_1^\perp \subset p_2^\perp$, then there is a pair (a, b), such that $(a, b) \in p_2^\perp$ and $(a, b) \notin p_1^\perp$. Then $(L_a, L_b) \in p_2 = ((p_2)^\perp)^\top$ and $(L_a, L_b) \notin p_1$.

If we suppose that $(L_a, L_b) \in p_1$, then $L_a^{-1}L_b \subseteq p_1^{\perp}$, $(a, L_a^{-1}L_b a) = (a, b) \in p_1^{\perp}$. We have received a contradiction. Thus $p_1 \cap (L\Pi)^2 \subset p_2 \cap (L\Pi)^2$.

The remaining inclusion maps are proved similarly. □

Corollary 6. *A lower semilattice of congruences of a loop is isomorphically embedded in the lower semilattices of congruences of semigroups $L\Pi$, $R\Pi$, Π, the left congruences of groups LM, RM.*

Theorem 3. *In an one-sided loop Q all congruences are normal if and only if in the group M all left congruences, which are semi-admissible from the right relative to all elements of the semigroup Π, are congruences.*

Proof. We suppose that in the group M all left congruences, which are semi-admissible from the right relative to permutations from the semigroup Π, are congruences. We shall show that then they induce in Q only normal congruences. Indeed, let p be a congruence of the group M. We demonstrate that then $p^{\perp}$ is a normal congruence of a quasigroup Q.

For this purpose it is enough to prove, taking into account Theorem 1, Corollary 1, that $\omega p^{\perp}\omega^{-1} \subseteq p^{\perp}$ for all $\omega \in \Pi$.

Let $(a, b) \in \omega p^{\perp}\omega^{-1}$. Then there exist $\theta, \varphi \in M$, $\theta\, p\, \varphi$ such that $(a, b) \in \omega\theta^{-1}\varphi\omega^{-1} = (\theta\omega^{-1})^{-1}\varphi\omega^{-1}$. Since p is a congruence of the group M, then from $\theta\, p\, \varphi$ follows $\theta\omega^{-1}\, p\, \varphi\omega^{-1}$ for all $\omega \in M$. Thus, $(a, b) \in p^{\perp}$, $\omega p^{\perp}\omega^{-1} \subseteq p^{\perp}$.

Converse. Let in an one-sided loop Q all congruences be normal. We shall prove that then in the group M all left congruences, which are semi-admissible from the right relatively to permutations from Π, are congruences.

We suppose converse, that in the group M there exists a left congruence p which is not semi-admissible relative to multiplication on the right by at least one element from the set $\mathbb{T}^{-1}$. We denote such element by R_c^{-1}. In other words there exist elements α, β such that $\alpha\, p\, \beta$, but αR_c^{-1} is not congruent with the element βR_c^{-1}.

Passing to the congruence $p^{\perp}$, we obtain $\alpha^{-1}\beta \subseteq p^{\perp}$, but $R_c\alpha^{-1}\beta R_c^{-1} \nsubseteq p^{\perp}$, i.e. there is an element $x \in Q$ such that $(x, (R_c\alpha^{-1}\beta R_c^{-1})x) \notin p^{\perp}$.

Since $p^{\perp}$ is a normal congruence of an one-sided loop Q, then: if $(a, b) \notin p^{\perp}$, then for all $x \in Q$ we obtain $(a\, x, b\, x) \notin p^{\perp}$.

Thus, if $(x, (R_c\alpha^{-1}\beta R_c^{-1})x) \notin p^{\perp}$, $(R_c x, (R_c\alpha^{-1}\beta)x) \notin p^{\perp}$ or $(xc, (\alpha^{-1}\beta)xc) \notin p^{\perp}$, i.e. $\alpha^{-1}\beta \nsubseteq p^{\perp}$. We have a contradiction.

Therefore left but not right congruence θ of the group M, which is semi-admissible from the right relative to permutations of the semigroup Π defines a non-normal congruence of an one-sided loop. □

Definition 3. *A subgroup H of a group M will be called A-invariant relative to a set A of elements of the group M, if $a^{-1}Ha \subseteq H$ for all $a \in A$.*

In the language of Definition 3 any normal subgroup H of a group G is G-invariant subgroup of the group G [14].

We reformulate Theorems 2 and 3 as follows.

Theorem 4. *The lower semilattice of congruences of an one-sided loop is isomorphically embedded in the lower semilattice of* Π*-invariant subgroups of the group* M.

Proof. We shall show that the kernel of a left congruence θ of the group M is some its subgroup H, but the left congruence θ is a partition of the group M in left coset classes by this subgroup. Indeed, if $\alpha\,\theta\,\varepsilon$ and $\beta\,\theta\,\varepsilon$, then $\alpha\beta\,\theta\,\alpha$, whence, $\alpha\beta\,\theta\,\varepsilon$.

If $\alpha\,\theta\,\varepsilon$, then $\alpha^{-1}\alpha\,\theta\,\alpha^{-1}\varepsilon$, $\alpha^{-1}\,\theta\,\varepsilon$. Thus, the kernel of left congruence θ is a subgroup of a group M.

We notice that various left congruences of the group M define various kernels. Indeed, if we suppose converse, that $\alpha\,\theta_1\,\beta$ and it is not true that $\alpha\,\theta_2\,\beta$, but $\beta^{-1}\alpha\,\theta_1\,\varepsilon$ and $\beta^{-1}\alpha\,\theta_2\,\varepsilon$, then $\beta(\beta^{-1}\alpha)\,\theta_2\,\beta\varepsilon$, $\alpha\,\theta_2\,\beta$. We have received a contradiction.

Since any subgroup H of a group M defines the left congruence ($\alpha \sim \beta \iff \alpha H = \beta H$), we proved that there is a bijection between the left congruences of the group M and its subgroups.

We shall show, that the left congruence θ of the group M is semi-admissible from the right relatively all permutations of the semigroup Π if and only if its kernel H fulfill the relation $H\gamma \subseteq \gamma H$ for all elements $\gamma \in \Pi$, or, equivalently, $\gamma^{-1}H\gamma \subseteq H$.

Indeed, if the left congruence θ of the group M is semi-admissible from the right relatively permutations of the semigroup Π, then for the kernel H of the congruence θ we have: let $\alpha \in H$, i.e. $\alpha\,\theta\,\varepsilon$.

Then, taking into consideration the semi-admissibility from the right of the congruence θ, we obtain $\alpha\gamma\,\theta\,\gamma$ for all $\gamma \in \Pi$. Since θ is a left congruence, then $\gamma^{-1}\alpha\gamma\,\theta\,\gamma^{-1}\gamma$, $\gamma^{-1}\alpha\gamma\,\theta\,\varepsilon$. Therefore, for all $\gamma \in \Pi$ we have $\gamma^{-1}H\gamma \subseteq H$.

Converse. Let kernel the H of a congruence θ satisfy the relation $\gamma^{-1}H\gamma \subseteq H$ for all $\gamma \in \Pi$. If $\alpha\,\theta\,\beta$, then $\beta^{-1}\alpha\,\theta\,\varepsilon$, whence $\gamma^{-1}\beta^{-1}\alpha\gamma\,\theta\,\varepsilon$, $\alpha\gamma\,\theta\,\beta\gamma$ for all $\gamma \in \Pi$. $\square$

Theorem 5. *Congruences of an one-sided loop are normal if and only if* Π*-invariant subgroups of the group* M *are normal in* M.

We can give sufficient conditions of normality of all congruences of a quasigroup.

Proposition 4. *If a quasigroup* Q *satisfies the condition* $\mathbb{T}^{-1} \subseteq \Pi$*, then in* Q *all congruences are normal.*

Proof. If θ is a congruence of a quasigroup Q, then, obviously, from $a\theta b$ follows $\alpha a\,\theta\,\alpha b$ for all $\alpha \in \Pi$.

Since $\mathbb{T}^{-1} \subseteq \Pi$, then from $ab\,\theta\,ac$ follows $L_a^{-1}(ab)\theta L_a^{-1}(ac)$, $b\theta c$, from $ca\,\theta\,ba$ follows $R_a^{-1}(ca)\theta R_a^{-1}(ba)$, $c\theta b$. $\square$

Corollary 7. *If in a quasigroup* Q *the condition* $M = \Pi$ *is fulfilled, then in the quasigroup* Q *all congruences are normal.*

Proof. It is easy to see that conditions $\mathbb{T}^{-1} \subseteq \Pi$ and $M = \Pi$ are equivalent. $\square$

Conditions of Proposition 4 and Corollary 7 can be used for concrete classes of quasigroups. See some examples below.

But, in general, these conditions are only sufficient, since there exists an example of a quasigroup, in which all congruences are normal, but $\mathbb{T} \subsetneqq \Pi$, or, that is equivalent, $M \neq \Pi$.

Example 1. Let $A = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$, where $\mathbb{Z}$ is the set of integers, and $\mathbb{N}$ is the set of natural numbers.

The set A forms a torsion-free abelian group of rank 1 relative to the operation of addition of elements of the set A [19].

Using the group $(A, +)$ we define on the set A a new quasigroup operation $\circ$. Let φ be a map of the set A into itself such that $\varphi x = \frac{1}{2}x$ for all $x \in A$.

It is easy to check that φ is an automorphism of the group $(A, +)$. Then $(A, \cdot)$ with the form $x \cdot y = \varphi x + y$ for all $x, y \in A$ is a left loop with the left identity 0. Indeed, $0 \cdot x = \varphi 0 + x = x$.

We prove that in the quasigroup $(A, \cdot)$ $M(A, \cdot) \neq \Pi(A, \cdot)$, and all congruences are normal.

For this purpose in the beginning we calculate the form of translations of a quasigroup $(A, \cdot)$. We have $R^{\cdot}_a x = x \cdot a = \varphi x + a = (\varphi R^+_a)x$, $L^{\cdot}_a x = a \cdot x = \varphi a + x = L^+_{\varphi a} x$. Using results from [14, 29] further it is possible to deduce the following relations

$$
\begin{aligned}
&LM(A, \cdot) = LM(A, +) \cong (A, +),\\
&RM(A, \cdot) \cong RM(A, +) \leftthreetimes \langle \varphi \rangle \cong (A, +) \leftthreetimes (\mathbb{Z}, +),\\
&L\Pi(A, \cdot) = L\Pi(A, +),\\
&R\Pi(A, \cdot) = \{(\varphi^n R^+_a) \mid a \in A, n \in \mathbb{N}\}
\end{aligned}
$$

It is easy to see that $M(A, \cdot) = RM(A, \cdot) = \{(\varphi^n R^+_a) \mid a \in A, n \in \mathbb{Z}\}$, $\Pi(A, \cdot) = \{(\varphi^n R^+_a) \mid a \in A, n \in \mathbb{N} \cup \{0\}\}$. Thus, $\Pi(A, \cdot) \subsetneqq M(A, \cdot)$. Moreover, if we denote by $\Pi^{-1}(A)$ the set $\{(\varphi^n R^+_a) \mid a \in A, n \in -\mathbb{N}\}$, then $M(A) = \Pi(A) \cup \Pi^{-1}(A)$.

Since $(A, \cdot)$ is a left loop, we can use Theorem 4. As it follows from Theorem 4, the subgroups of the group $M(A, \cdot)$ that are invariant relative to all permutations of the semigroup $\Pi(A, \cdot)$ correspond to congruences of the quasigroup $(A, \cdot)$.

We demonstrate that any Π-invariant subgroup of the group $M(A, \cdot)$ is a normal subgroup of the group $M(A, \cdot)$.

We notice that following our agreements we have $(R^+_a \varphi)(x) = \varphi(x + a) = \varphi x + \varphi a = (\varphi R^+_{\varphi a})(x)$. Below in this example we shall write R_x instead of R^+_x. We have $(\varphi^k R_a)(\varphi^l R_b) = \varphi^{k+l} R_{\varphi^l a + b}$, $(\varphi^n R_a)^{-1} = \varphi^{-n} R_{-\varphi^{-n} a}$.

It is clear that any element of a subgroup H of the group M has the form $\varphi^k R_b$. If H is a Π-invariant subgroup of the group M, then we have: if $\varphi^k R_b \in H$, then $\varphi^{-n} R_{-\varphi^{-n} a} \varphi^k R_b \varphi^n R_a = \varphi^k R_c \in H$ for all $\varphi^k R_b \in H$, $\varphi^n R_a \in \Pi$, where $c = -\varphi^k a + \varphi^n b + a$.

In other words, If H is a Π-invariant subgroup of the group M, then: if $\varphi^k R_b \in H$, then $\varphi^k R_{\varphi^n b} R_{-\varphi^k a + a} \in H$ for all $\varphi^k R_b \in H$, $n \in \mathbb{N} \cup \{0\}$, $a \in A$.

If we change in the last implication a by $-a$, then we obtain the following implication:

if $\varphi^k R_b \in H$, then $\varphi^k R_{\varphi^n b} R_{\varphi^k a - a} \in H$ for all $\varphi^k R_b \in H$, $n \in \mathbb{N} \cup \{0\}$, $a \in A$. $(*)$

From the implication $(*)$ by $a = 0$ it follows:

if $\varphi^k R_b \in H$, then $\varphi^k R_{\varphi^n b} \in H$ for all $\varphi^k R_b \in H$, $n \in \mathbb{N} \cup \{0\}$. $(**)$

We can write the condition that the Π-invariant subgroup H of group M is a normal subgroup of group M, in the form: if $\varphi^k R_b \in H$, then $\varphi^n R_a \varphi^k R_b \varphi^{-n} R_{-\varphi^{-n} a} = \varphi^k R_d \in H$, where $d = -\varphi^{-n}(-\varphi^k a - b + a)$, for all $\varphi^k R_b \in H$, $\varphi^n R_a \in \Pi$.

Applying to the last implication condition $(**)$, we obtain the following equivalent condition of normality of Π-invariant group H: if $\varphi^k R_b \in H$, then $\varphi^k R_h \in H$, where $h = \varphi^k a + b - a$ for all $\varphi^k R_b \in H$, $a \in A$.

The last implication we can re-write in the form:
if $\varphi^k R_b \in H$, then $\varphi^k R_b R_{\varphi^k a - a} \in H$ for all $\varphi^k R_b \in H$, $a \in A$.

It is easy to see that the last implication follows from the implication $(*)$ by $n = 0$.

Example 2. Using the group $(A, +)$ from Example 1 we define on the set A a binary operation $*$ in the following way $x * y = 2 \cdot x + y$ for all $x, y \in A$. The operation $*$ is a quasigroup operation, since the map $2 : x \mapsto 2 \cdot x$ for all $x \in A$ is an automorphism of the group $(A, +)$, moreover, a left loop operation, see Example 1.

We denote by H the following subgroup of the group $M(A, *)$: $H = \langle R_1^+ \mid 1 \in A \rangle = \{\dots R_{-2}^+, R_{-1}^+, R_0^+, R_1^+, R_2^+, \dots\}$. It is easy to see that $H \cong (\mathbb{Z}, +)$.

We check that the group H is a Π-invariant non-normal subgroup of the group M.

We use results of Example 1 by $\varphi = 2$. Thus, if H is a Π-invariant subgroup of the group M, then we have: $2^{-n} R_{-2^{-n} a} R_1 2^n R_a = R_{2^n} \in H$ for all $2^n R_a \in \Pi$.

We prove that the group H is a non-normal subgroup of the group M. We have $2^n R_a R_1 2^{-n} R_{-2^{-n} a} = R_{2^{-n}} \notin H$ for all $2^n R_a \in M$ such that $n > 1$.

As it follows from Theorems 2 and 4, the subgroup H of the group $M(A, *)$ induces a non-normal congruence of the quasigroup $(A, *)$.

Remark 5. The fact that the group H induces a congruence of the quasigroup $(A, *)$ can be deduced from results of the article of T. Kepka and P. Nemec [16, Theorem 42], since the quasigroup $(A, *)$ is a T-quasigroup, moreover, it is a medial quasigroup.

3 On normality of congruences of some inverse quasigroups

Definition 4. *A quasigroup Q is called rst-inverse quasigroup, if there exist a permutation J of the set Q, some fixed integers r, s, t such that in the quasigroup Q for all $x, y \in Q$ the relation $J^r(x \circ y) \circ J^s x = J^t y$ is fulfilled [16].*

A $(0,1,0)$-inverse quasigroup is called a CI-quasigroup. A $(-1,0,-1)$-inverse quasigroup is called an WIP-quasigroup [5]. An $(m,m+1,m)$-inverse quasigroup is called an m-inverse quasigroup [15].

Proposition 5. *In rst-quasigroup $(Q,\cdot)$ all congruences are normal if permutations J^r and J^{-t} are semi-admissible relative to any congruence of $(Q,\cdot)$.*

Proof. In the language of translations we can re-write Definition 4 in the form $L_x J^r R_{J^s x} = J^t$. Then $L_x^{-1} = J^r R_{J^s x} J^{-t}$, $R_{J^s x}^{-1} = J^{-t} L_x J^r$.

Using Proposition 4 we obtain the required. □

Corollary 8. *In CI-quasigroup all congruences are normal.*

Corollary 9. *In WIP-quasigroup $(Q,\cdot)$ all congruences are normal if the permutation J is admissible relative to any congruence of $(Q,\cdot)$.*

Corollary 10. *In m-inverse quasigroup $(Q,\cdot)$ all congruences are normal if the permutation J^m is admissible relative to any congruence of $(Q,\cdot)$.*

In [17] Definition 4 is generalized in the following way.

Definition 5. *A quasigroup $Q,\circ)$ is called an (α,β,γ)-inverse quasigroup if there exist permutations α,β,γ of the set Q such that $\alpha(x\circ y)\circ \beta x = \gamma y$ for all $x,y\in Q$.*

Proposition 6. *In (α,β,γ)-quasigroup $(Q,\cdot)$ all congruences are normal if permutations α and γ^{-1} are semi-admissible relative to any congruence of $(Q,\cdot)$.*

Proof. The proof repeats the proof of Proposition 5. □

Definition 6. *A quasigroup $(Q,\circ)$ has the **λ-inverse-property** if there exist permutations $\lambda_1,\lambda_2,\lambda_3$ of the set Q such that $\lambda_1 x\circ \lambda_2(x\circ y) = \lambda_3 y$ for all $x,y\in Q$ [8].*

Definition 7. *A quasigroup $(Q,\circ)$ has the **ρ-inverse-property** if there exist permutations ρ_1,ρ_2,ρ_3 of the set Q such that $\rho_1(x\circ y)\circ \rho_2 y = \rho_3 x$ for all $x,y\in Q$ [8].*

Definition 8. *A quasigroup $(Q,\circ)$ that has λ-inverse-property and ρ-inverse-property is called I-inverse quasigroup [8].*

Proposition 7. *In an I-inverse quasigroup $(Q,\cdot)$ all congruences are normal if permutations λ_2, λ_3^{-1}, ρ_1 and ρ_3^{-1} are semi-admissible relative to any congruence of $(Q,\cdot)$.*

Proof. From Definition 6 we have $L_x\lambda_2 L_{\lambda_1 x} = \lambda_3$. Then $L_x^{-1} = \lambda_2 L_{\lambda_1 x}\lambda_3^{-1}$. From Definition 7 we have $R_y\rho_1 R_{\rho_2 y} = \rho_3$. Therefore $R_y^{-1} = \rho_1 R_{\rho_2 y}\rho_3^{-1}$. Further we can apply Proposition 4. □

If in I-inverse quasigroup $(Q,\circ)$ $\lambda_2=\lambda_3=\rho_1=\rho_3=\varepsilon$, then $(Q,\circ)$ is called an IP-quasigroup.

Corollary 11. *In IP-quasigroup all congruences are normal [5].*

Proof. The proof follows from the definition of IP-quasigroup and Proposition 7. □

4 On regularity of congruences of quasigroups

Definition 9. *A congruence is called regular if it is uniquely defined by any its coset, the coset of a congruence is called regular if it is a coset of only one congruence.*

In [21] A.I. Mal'tsev has given necessary and sufficient conditions that a normal complex K of an algebraic systems A is a coset of only one congruence, i.e. K is a coset of only one congruence of a system A.

For this purpose for any set $S \subseteq A$ the congruence $\mathrm{mod}\, \mathrm{S}$ is constructed. Elements a, b are equivalent $a \sim b \,(\mathrm{mod}\, \mathrm{S})$ if either $a = b$, or $a, b \in S$, or $a = \alpha u$, $b = \alpha v$, where $u, v \in S$, α is a translation of the algebraic system A.

A.I. Mal'tsev names elements a and b *comparable* if there exists a sequence $x_1, \dots, x_n$ of elements from A such that: $a \sim x_1, x_1 \sim x_2, \dots, x_n \sim b \,(\mathrm{mod}\, \mathrm{S})$.

The binary relation $(\mathrm{mod}\, \mathrm{S})$ is a congruence on an algebraic system A, and the congruence $(\mathrm{mod}\, \mathrm{S})$ is minimal among all congruences for which elements of the set S are comparable with each other [21].

Theorem 6. *The normal complex K is a coset of only one congruence of an algebraic system A if and only if elements $a, b \in A$, for which by any translation α the statements $\alpha a \in K$ and $\alpha b \in K$ are equivalent, are comparable* $(\mathrm{mod}\, \mathrm{K})$ *[21].*

We notice if in Theorem 6 A is a binary quasigroup, then α is an element of $\Pi(A)$.

If in Mal'tsev theorem we pass from a quasigroup A to its homomorphic image $\bar{A} = A/\mathrm{mod}\, \mathrm{K}$, then we shall have the following conditions of regularity of a normal complex K of a quasigroup A.

Proposition 8. *The normal complex K is a coset of only one congruence of a quasigroup A if and only if for each pair of elements $\bar{a}, \bar{b} \in \bar{A}$ for which by any translation $\bar{\alpha} \in \bar{A}$ the statements $\bar{\alpha}\bar{a} = \bar{k}$ and $\bar{\alpha}\bar{b} = \bar{k}$ are equivalent the equality $\bar{a} = \bar{b}$ is fulfilled.*

Remark 6. Let's remark if $\bar{A}$ is a binary quasigroup, then conditions of Proposition 8 are fulfilled. Indeed, if we take translation $\bar{\alpha}$ such that $\bar{\alpha} = \bar{L_c}$ and $\bar{c} \cdot \bar{a} = \bar{k}$, then we have $\bar{c} \cdot \bar{b} = \bar{k}$ by conditions of the proposition. Then $\bar{a} = \bar{c} \backslash \bar{k} = \bar{b}$.

Example 3. It is possible to construct division groupoid in which the conditions of Proposition 8 are satisfied. We denote by $(\mathbb{Q}, +)$ the group of rational numbers relative to the operation of addition, and by $(\mathbb{Z}, +)$ the group of integers relative to the operation of addition. On the factor group $\bar{A} = (\mathbb{Q}/\mathbb{Z}, +)$ we define operation $x \circ y = 2x + y$ for all $x, y \in \bar{A}$.

It is easy to check up that $(\bar{A}, \circ)$ is a division groupoid. We shall show that this groupoid satisfies conditions of Proposition 8. Since $(\bar{A}, \circ)$ is a division groupoid, then for any $\bar{k} \in \bar{A}$ there exists $\bar{c} \in \bar{A}$ such that $\bar{c} \circ \bar{a} = \bar{k}$, and then by conditions of this proposition also $\bar{c} \circ \bar{b} = \bar{k}$. Therefore $2\bar{c} + \bar{a} = \bar{k}$, $2\bar{c} + \bar{b} = \bar{k}$, $\bar{a} = \bar{b} = \bar{k} - 2\bar{c}$.

Proposition 9. *There exist a quasigroup Q and its subset K such that K is a coset of more than one congruence.*

Proof. It is known (see [9. p. 10]) that any division groupoid is a homomorphic image of some quasigroups.

From Mal'tsev theorem it follows that to give an example of a quasigroup in which not all congruences are regular it is necessary to find a pair of elements $a, b \in Q$ such that $a \nsim b\,(\mathrm{mod\,K})$, where K is a coset of some congruence, but for which by any translation α statements $\alpha a \in K$ and $\alpha b \in K$ are equivalent.

We pass to homomorphic image $P = Q/\mathrm{modK}$ of quasigroups Q. Then conditions that the coset K is not regular are the following: $\bar{a} \neq \bar{b}$, but for any $c \in Q$ the equality $\bar{c} \cdot \bar{a} = \bar{k}$ is equivalent with the equality $\bar{c} \cdot \bar{b} = \bar{k}$, the equality $\bar{a} \cdot \bar{c} = \bar{k}$ is equivalent to the equality $\bar{b} \cdot \bar{c} = \bar{k}$ where $\bar{k}$ is an image of the set K in the groupoid P.

We construct the following division groupoid. Let $\mathbb{C}$ be a set of complex numbers, $x \circ y = (xy)^2$ for all $x, y \in \mathbb{C}$. It is easy to check that $(\mathbb{C}, \circ)$ is a commutative division groupoid.

Let $\bar{k} = 4$. Then the equation $a \circ y = 4 \Longleftrightarrow (ay)^2 = 4$, $ay = \pm 2$, $y = \pm\frac{2}{a}$ has two solutions. And, if one of radicals is a solution of the equations $a \circ y = 4$, so is the other, for any $a \in \mathbb{C}$. If we take in a quasigroup Q pre-images of elements of 2 and -2, then we find the necessary pair. $\square$

5 On behavior of congruences by an isotopy

A quasigroup $(Q, \circ)$ is an isotope of a quasigroup $(Q, \cdot)$ if there exist permutations α, β, γ of the set Q such that $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$ for all $x, y \in Q$. We can also write this fact in the form $(Q, \circ) = (Q, \cdot)T$, where $T = (\alpha, \beta, \gamma)$ [5,6,23]. An isotopy $T = (\alpha, \beta, \gamma)$ is admissible relative to a binary relation θ, if the permutations α, β, γ are admissible relative to θ.

If $(Q, \cdot)$ is a quasigroup, then an isotopy of the form $(R_a^{-1}, L_b^{-1}, \varepsilon)$, where R_a, L_b are some fixed translations of the quasigroup $(Q, \cdot)$ is called LP-isotopy. Any LP-isotopic image of a quasigroup is a loop [5,6].

In [5], p. 59 the following lemma is proved.

Lemma 2. *Let θ be a normal congruence of a quasigroup $(Q, \cdot)$. If a quasigroup $(Q, \circ)$ is isotopic to $(Q, \cdot)$ and the isotopy (α, β, γ) is admissible relative to θ, then θ is a normal congruence also in $(Q, \circ)$.*

Corollary 12. *If $(Q, \cdot)$ is a quasigroup, $(Q, +)$ is a loop of the form $x + y = R_a^{-1}x \cdot L_b^{-1}y$ for all $x, y \in Q$, then $nCon(Q, \cdot) \subseteq nCon(Q, +)$, where $nCon(Q, \cdot)$ is the set of normal congruences of the quasigroup $(Q, \cdot)$, and $nCon(Q, +)$ is the set of normal congruences of the loop $(Q, +)$.*

Proof. If θ is a normal congruence of a quasigroup $(Q, \cdot)$, then, since θ is admissible relative to the isotopy $T = (R_a^{-1}, L_b^{-1}, \varepsilon)$, θ is also a normal congruence of a loop $(Q, +)$. $\square$

Remark 7. It is easy to see, if $x + y = R_a^{-1}x \cdot L_b^{-1}y$, then $x \cdot y = R_a x + L_b y$. If in conditions of Corollary 12 we shall in addition suppose, that the isotopy $T^{-1} = (R_a, L_b, \varepsilon)$ is admissible relative to any normal congruence of the loop $(Q, +)$, then we obtain the following equality $nCon(Q, \cdot) = nCon(Q, +)$.

Proposition 10. *The lattice $(L, \vee, \wedge)$ of normal congruences of a quasigroup $(Q, \cdot)$ is isomorphic to a sublattice of the lattice $(L_1, \vee, \wedge)$ of normal congruences of isotope loop $(Q, \circ)$ [9].*

Proof. By an LP-isotopy T ($T = (R_a^{-1}, L_b^{-1}, \varepsilon)$) a normal congruence θ of quasigroup $(Q, \cdot)$ is also a normal congruence of a loop $(Q, \star)$, $(Q, \star) = (Q, \cdot)T$ (Corollary 12).

Since the operation $\wedge$ in sets of congruences of a quasigroup $(Q, \cdot)$ and loops $(Q, \star)$ coincides with the set-theoretic intersection, and the operation $\vee$ coincides, in view of the permutability of normal congruences, with their product as binary relations ([30]), we can state that the lattice of normal congruences of a quasigroup $(Q, \cdot)$ is a sublattice of the lattice of normal congruences of the loop $(Q, \star)$. This corollary is proved, since any isotopy between a loop and a quasigroup has the form $(R_a^{-1}, L_b^{-1}, \varepsilon)(\varphi, \varphi, \varphi)$. $\square$

Obviously, any permutation of the semigroup $\Pi(Q, \cdot)$ is semi-admissible relative to any congruence of a quasigroup $(Q, \cdot)$. An isotopy is semi-admissible, if all permutations included in it are semi-admissible.

Proposition 11. *Let θ be a congruence of a quasigroup $(Q, \cdot)$. If a quasigroup $(Q, \circ)$ is isotopic to $(Q, \cdot)$, and the isotopy T is semi-admissible relative to θ, then θ is a congruence also in $(Q, \circ)$.*

Proof. We suppose that the isotopy T has the form $T = (\alpha, \beta, \gamma)$. If $a\theta b$, then $\beta a \theta \beta b$, $\alpha c \cdot \beta a \theta \alpha c \cdot \beta b$, $\gamma^{-1}(\alpha c \cdot \beta a)\theta\gamma^{-1}(\alpha c \cdot \beta b)$.

Finally, we obtain $(c \circ a)\theta(c \circ b)$. Similarly, if $a\theta b$, then $a \circ c\theta b \circ c$. $\square$

Proposition 12. *If in a quasigroup $(Q, \cdot)$ there exist elements a, b such that R_a^{-1}, $L_b^{-1} \in \Pi$, then the lower semilattice $(L_1, \wedge)$ of congruences of a quasigroup $(Q, \cdot)$ is a subsemilattice of the semilattice $(L_2, \wedge)$ of congruences of the loop $(Q, \circ)$ which is an isotope of a quasigroup $(Q, \cdot)$ of the form $(R_a^{-1}, L_b^{-1}, \varepsilon)$.*

Proof. If $R_a^{-1}, L_b^{-1} \in \Pi$, then the isotopy $(R_a^{-1}, L_b^{-1}, \varepsilon)$ is admissible relative to any congruence of quasigroup $(Q, \cdot)$. The corollary is true, since the operations $\wedge$ in $(L_1, \wedge)$ and $(L_2, \wedge)$ coincide with the set-theoretic intersection of congruences. $\square$

In any IP-loop $(Q, \circ)$ with the identity 1 the map $J : a \mapsto a^{-1}$ for all $a \in Q$, where $a \circ a^{-1} = 1$, is a permutation of the set Q, $J^2 = \varepsilon$ ([11]).

Example 4. If $(Q, \circ)$ is an IP-loop, $(Q, \cdot)$ is its isotope of the form $(\alpha J^{\tau}, \beta J^{\kappa}, \varepsilon)$, where $\alpha, \beta \in M(Q, \circ)$, $\tau, \kappa \in \{0, 1\}$, i.e. $x \cdot y = \alpha J^{\tau} x \circ \beta J^{\kappa} y$ for all $x, y \in Q$, then $Con(Q, \circ) = nCon(Q, \cdot)$.

Proof. The permutation J is an antiautomorphism in $(Q,\circ)$ and any normal congruence in $(Q,\circ)$ is admissible relative to this permutation. Indeed, if $x\theta y$, then $1\theta x^{-1}\circ y$, $y^{-1}\theta(x^{-1}\circ y)\circ y^{-1}$, $y^{-1}\theta x^{-1}$, $x^{-1}\theta y^{-1}$ and in the similar way $x\theta y$ follows from $x^{-1}\theta y^{-1}$.

By Corollary 11 in an IP-loop all congruences are normal, i.e. $Con(Q,\circ) = nCon(Q,\circ)$. Then permutations α,β and J are admissible relative to any congruence of the loop $(Q,\circ)$, by Lemma 2 $Con(Q,\circ) \subseteq nCon(Q,\cdot)$.

Since $(Q,\cdot) = (Q,\circ)(\alpha J^{\tau},\beta J^{\kappa},\varepsilon)$, then $(Q,\circ) = (Q,\cdot)((\alpha J^{\tau})^{-1},(\beta J^{\kappa})^{-1},\varepsilon)$. It is known ([5,6]) that every principal isotopy (the third component of such isotopy is an identity mapping) of a quasigroup $(Q,\cdot)$ to a loop $(Q,\circ)$ has the form $(R_a^{-1},L_b^{-1},\varepsilon)$, where $R_a x = x\cdot a$, $L_b x = b\cdot x$.

Thus, taking into consideration Corollary 12, we have: $nCon(Q,\cdot) \subseteq Con(Q,\circ)$. Therefore $nCon(Q,\cdot) = Con(Q,\circ)$. □

Example 5. If $(Q,\circ)$ is a CI-loop, $(Q,\cdot)$ is its isotope of the form $x\cdot y = \alpha J^{\tau}x\circ\beta J^{\kappa}y$ for all $x,y\in Q$, where $\alpha,\beta\in M(Q,\circ)$, $\tau,\kappa\in\{0,1\}$, then $Con(Q,\circ) = nCon(Q,\cdot)$.

Proof. The permutation J is an automorphism in $(Q,\circ)$ ([5]) and any normal congruence in $(Q,\circ)$ is admissible relative to this permutation. Indeed, if $x\theta y$, then $1\theta y\circ Jx$, $Jy\theta(y\circ Jx)\circ Jy$, $Jy\theta Jx$, $Jx\theta Jy$.

In any CI-quasigroup $(Q,\circ)$ the following equality is true $x\circ(y\circ Jx) = y$ for all $x,y\in Q$ [16]. If $Jx\theta Jy$, then $y\circ Jx\,\theta\, y\circ Jy$, $y\circ Jx\,\theta\,1$, $x\circ(y\circ Jx)\,\theta\,x$, $y\theta x$.

By Corollary 8 in the loop $(Q,\circ)$ all congruences are normal. Therefore, permutations α,β are admissible relative to any congruence of the loop $(Q,\circ)$. □

Acknowledgement. The author thanks Prof. G.B. Belyavskaya and Prof. E.A. Zamorzaeva for their helpful comments.

References

[1] Albert A.A. *Quasigroups, I.* Trans. Amer. Math. Soc., 1943, **54**, p. 507–519.

[2] AlbertA.A. *Quasigroups, II.* Trans. Amer. Math. Soc., 1944, **55**, p. 401–419.

[3] Bates G.E., Kiokemeister F. *A note on homomorphic mappings of quasigroups into multiplicative systems.* Bull. Amer. Math. Soc., 1948, **54**, p. 1180–1185.

[4] Beglaryan V.A. *To theory of homomorphisms in quasigroups.* Thesis of Ph. Degree. Kishinev, 1981 (in Russian).

[5] Belousov V.D. *Foundation of the theory of quasigroups and loops.* Moscow, Nauka, 1967.

[6] Belousov V.D. *Elements of the Quasigroup Theory: A special course.* Kishinev, Kishinev State University Press, 1981 (in Russian).

[7] Belousov V.D. *Inverse loops.* Mat. Issled., vyp. 95. Kishinev, Shtiintsa, 1987, p. 3–22 (in Russian).

[8] Belousov V.D. *Inverse loops.* Mat. Issled., vyp. 95. Kishinev, Shtiintsa, 1987, p. 3–22 (in Russian).

[9] Belyavskaya G.B. *Direct decompositions of quasigroups.* Mat. Issled., vyp. 95. Kishinev, Shtiintsa, 1987, p. 23–38 (in Russian).

[10] Birkhoff G. *Lattice theory.* Moscow, Nauka, 1984, (in Russian).

[11] Bruck R.H. *A Survey of Binary Systems.* Berlin, Springer Verlag, 1958.

[12] Clifford A.H., Preston G.B. *The algebraic thery of semigroups, V. 1.* Moscow, Mir, 1972 (in Russian).

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

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

[15] Karklin´š B.B., Karklin´V.B. *Inverse loops.* Nets and groups, Mat. Issled., vyp. 39. Kishinev, Shtiintsa, 1976, p. 87–101 (in Russian).

[16] Keedwell A.D., Shcherbacov V.A. *Construction and properties of (r, s, t)-inverse quasigroups, I.* Discrete Math., 2003, **266**, N 1-3, p. 275–291.

[17] Keedwell A.D., Shcherbacov V.A. *Quasigroups with an inverse property and generalized parastrophic identities.* Quasigroups and related systems, 2005, **13**, p. 109-124.

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

[19] Kurosh A.G. *The Group Theory.* Moscow, Nauka, 1967 (in Russian).

[20] Kurosh A.G. *Lectures on General Algebra.* Moscow, Gos. Izd. Fiz.-mat. Lit., 1962 (in Russian).

[21] Mal'tsev A.I. *To general theory of algebraic systems.* Mat. sbornik, 1954, **35**, p. 3–20 (in Russian).

[22] Parovichenko I.I. *The Theory of Operations over Sets.* Kishinev, Shtiintsa, 1981.

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

[24] Riguet J. *Relations binares, fermetures, correspondances de Galois.* Bull. Soc. Math. France, 1948, **76**, p. 114–155.

[25] Thurston H.A. *Equivivalences and mappings.* Proc. London Math. Soc., 1952, **3**, N 2, p. 175–182.

[26] Thurston H.A. *Certain congruences on quasigroups.* Proc. Amer. Math. Soc., 1952, **3**, p. 10–12.

[27] Shcherbacov V.A. *On congruences of quasigroups.* Reg. in VINITI 01.08.90, N 4413-B90. Moscow, 1990 (in Russian).

[28] Shcherbacov V.A. *On automorphism groups and congruences of quasigroups.* Thesis of Ph. Degree. Kishinev, 1991 (in Russian).

[29] Shchukin K.K. *Action of a group on a quasigroup.* Kishinev, Kishinev State University Press, 1985 (in Russian).

[30] Smith J.D.H. *Mal'cev Varieties.* Lecture Notes in Mathematics, 1976, **554**.

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

Received August 19, 2005

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 141–152
ISSN 1024–7696

On Commutativity and Mediality of Polyagroup Cross Isomorphs

F.M. Sokhatsky, O.V. Yurevych

Abstract. The notion of *cross isotopy* (*cross isomorphism*) of n-ary operations can be got from the well-known notion of *isotopy* (*isomorphism*) by replacing one of its components with a k-ary m-invertible operation [1, 2]. The idea of consideration of cross isotopy belongs to V.D. Belousov [3], who defined it for binary quasigroups.
In the paper necessary and sufficient conditions for commutativity and mediality of a polyagroup cross isomorph (when $n > 2k$) are determined. A neutrality criterion of an arbitrary element is stated.

Mathematics subject classification: 20N15.
Keywords and phrases: n-ary quasigroup, cross isomorphism, cross isotopy, (i, j)-associative operation.

1 Introduction

V.D. Belousov [3] introduced left and right cross isotopy notions for binary quasigroups by replacing the left (right) component of the common isotopy with a left (right) invertible binary operation.

For the first time the corresponding notion for multiary operations was proposed in [1] and was based on the same idea. Namely, the notion of *i-cross isotopy of an $(n+1)$-ary operation* can be received from the well-known notion of isotopy by replacing its i-th nonprincipal component with an m-invertible operation depending on variables having indices in $\vec{\imath} := (i_0, \dots, i_k)$, where $0 \leqslant i_0 < \dots < i_k \leqslant n$ and $i_m = i$. The pair $(m; \vec{\imath})$ is called a *type* of the cross isotopy. If all its components coincide, except the i-th one, then the cross isotopy is called a *cross isomorphism*.

General properties of cross isotopy were studied in [1]. The set of all cross isotopies of fixed type of a set Q forms a group acting on the set of all operations of Q. It follows that the set of all cross autotopies of an operation is its subgroup; cross autotopy groups of cross isotopic operations are isomorphic; cross isotopy is an equivalence relation and so on. The same results were proved for cross isomorphism. Some other results were observed in the mentioned work too. For example, every two quasigroup operations defined on the same set are cross isomorphic if its type is maximal, i.e. if $n = k$, but there exists a pair of quasigroup operations (irreducible and completely reducible) which is not cross isotopic for every nonmaximal type.

In [2] the study of cross isotopy and cross isomorphism was continued: the structure of polyagroup nonmaximal type cross isotopism was found if the type is a segment of integers or the polyagroup is medial (i.e. a decomposition group of the polyagroup is commutative); an associate being i-cross isotopic to a quasigroup is a polyagroup if i is one of the integers $1, \ldots, n-1$; the notions of strong cross isomorphism and the well-known notion of isomorphism coincide if its type does not contain 1 or $n-1$ or the polyagroup is medial and the integers from the set $\{1, \ldots, n-1\}$, which is not in the cross isotomorphism type are relatively prime.

E.A.Kuznetsov [4] used the notion of cross isotopy for describing some classes of loops. It is proposed a description of all cross isotopies between the given class of loops and well-studied class of loops, for example, the class of groups.

The same problem exists for multiary operations. Now the most developed operations are polyadic groups. So, the problem is *to describe the structure of cross isotopies assuring a polyagroup cross isotope belongs to the given class* $\mathfrak{A}$.

Here, we consider the problem in the case if the cross isotopy is a cross isomorphism and if the class $\mathfrak{A}$ is a class of commutative or medial operations. We also determine the neutrality criterion for an element of polyagroup cross isomorph.

2 General notion

All the operations below are defined on the same fixed set Q. We recall that $(n+1)$-ary operation f is called

- (i,j)-*associative* if for arbitrary $x_0, \ldots, x_n \in Q$ the identity

$$f(x_0, \ldots, x_{i-1}, f(x_i, \ldots, x_{i+n}), x_{i+n+1}, \ldots, x_{2n}) =$$

$$= f(x_0, \ldots, x_{j-1}, f(x_j, \ldots, x_{j+n}), x_{j+n+1}, \ldots, x_{2n})$$

  is true;

- i-*invertible* if for any $a_0, \ldots, a_n$ of Q the equation

$$f(a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) = a_i \tag{1}$$

  has a unique solution;

- *invertible* or a *quasigroup operation* if it is i-invertible for all i=0, 1, ..., n.

A groupoid $(Q; f)$ is called (see [5]) an *associate of the kind* (s, n), where $s|n$, if the operation f is (i,j)-associative for all pairs (i,j) such that $i \equiv j \pmod s$; a *quasigroup* if f is invertible; a *polyagroup of the kind* (s, n) if it is an associate of the kind (s, n) and a quasigroup; an $(n+1)$-*group* if it is a polyagroup and $s = 1$.

Theorem 1 [6]. *If a groupoid $(Q; f)$ is a polyagroup of the kind (s, n), then for arbitrary element $0 \in Q$ there exists a unique triple of operations $(+, \varphi, a)$ of the arities 2, 1, 0 respectively such that the following conditions are true:*

1) $(Q;+)$ *is a group,* φ *is its automorphism,* 0 *is its neutral element and the identities*

$$\varphi^n x + a = a + x, \qquad \varphi^s a = a \tag{2}$$

are valid;

2) a decomposition of the operation f *has the following form*

$$f(x_0, \ldots, x_n) = x_0 + \varphi x_1 + \cdots + \varphi^{n-1} x_{n-1} + \varphi^n x_n + a. \tag{3}$$

And vice versa, if the conditions 1) hold, then the groupoid $(Q;f)$ *defined by (3) is a polyagroup of the kind* (s,n).

In that case, the group $(Q;+)$ is called a *decomposition group*, and the triple $(+,\varphi,a)$ is a *decomposition* of the polyagroup $(Q;f)$.

Let $\overset{k}{a}$ denote a sequence $a, \ldots, a$ (k times).

An operation g of the arity $n+1$ is called *weak* i*-cross isomorphic of the type* $\vec{\imath} := (i_0, \ldots, i_k)$, where $0 \leqslant i_0 < \cdots < i_k \leqslant n$, or *weak cross isomorphic of the type* $(m, \vec{\imath})$ to $(n+1)$-ary operation f if $i_m = i$ and there exist a substitution α and an m-invertible operation h of the arity $k+1$ such that the equality

$$g(x_0, \ldots, x_n) = \alpha^{-1} f(\alpha x_0, \ldots, \alpha x_{i-1}, \alpha h(x_{i_0}, \ldots, x_{i_k}), \alpha x_{i+1}, \ldots, \alpha x_n) \tag{4}$$

holds for all $x_0, \ldots, x_n \in Q$. The pair $(\alpha; h)$ is called a *weak cross isomorphism of the type* $(m, \vec{\imath})$ *of the arity* $k+1$. A cross isomorphism is called *principal* if $\alpha = \varepsilon$. If $k = n$, then i-th cross isomorphism is called i-th cross isomorphism of the *maximal type.*

A weak cross isomorphism $(\alpha; h)$ is called *strong* if h is a selector-like operation, i.e. if for arbitrary substitution τ of Q and for all $x \in Q$ the equality

$$h(\overset{m}{x}, \tau x, \overset{k-m}{x}) = \tau x \tag{5}$$

holds.

An operation g is called *commutative* if for all permutation σ of the set $\{0, 1, \ldots, n\}$ the identity

$$g(x_{\sigma 0}, x_{\sigma 1}, \ldots, x_{\sigma n}) = g(x_0, x_1, \ldots, x_n) \tag{6}$$

is true.

Lemma 2 [7]. *If there exist transformations* α, β, γ, δ *of the group* $(Q;+)$ *such that the equality*

$$\alpha x + \beta y = \gamma y + \delta x$$

holds for all x, $y \in Q$ *and at least one element of each of the sets* $\{\alpha, \delta\}$ *and* $\{\beta, \gamma\}$ *is a substitution of* Q, *then the group* $(Q;+)$ *is commutative.*

The relation (4) implies the following identity

$$g_0(x_0,\dots,x_n)=f(x_0,\dots,x_{i-1},h_0(x_{i_0},\dots,x_{i_k}),x_{i+1},\dots,x_n),$$

where

$$g_0(x_0,\dots,x_n)=\alpha g(\alpha^{-1}x_0,\dots,\alpha^{-1}x_n),\ h_0(x_{i_0},\dots,x_{i_k})=\alpha h(\alpha^{-1}x_{i_0},\dots,\alpha^{-1}x_{i_k}),$$

i.e. groupoids $(Q;g)$ and $(Q;g_0)$ are isomorphic. To clarify the truth of a formula for cross isotopes it is enough to clarify it for principal cross isotopes. So from here on we will consider principal cross isotopes only.

Let $(n+1)$-ary groupoid $(Q;g)$ be a principal cross isomorph of the type $(m,\vec{\imath})$ of an $(n+1)$-ary polyagroup $(Q;f)$ with a decomposition $(+,\varphi,a)$, where $\vec{\imath}:=(i_0,\dots,i_k)$. Combining the identities (3) and (4) we obtain a decomposition of the operation g

$$\begin{aligned} g(x_0,\dots,x_n)= &\ x_0+\varphi x_1+\dots+\varphi^{i-1}x_{i-1}+\varphi^i h(x_{i_0},\dots,x_{i_k})+\\ &+\varphi^{i+1}x_{i+1}+\dots+\varphi^n x_n+a. \end{aligned} \tag{7}$$

3 Commutativity

The next theorem gives a criterion when a cross isomorphism of a polyagroup is commutative.

Theorem 3. *Let $(Q;f)$ be a polyagroup with a decomposition $(+,\varphi,a)$ and let $(\varepsilon,h)f$ be a principal cross isomorph of a nonmaximal type $(m,\vec{\imath})$ of the operation f, where $\vec{\imath}:=(i_0,\dots,i_k)$ and $i:=i_m$. Then the operation $(\varepsilon,h)f$ is commutative if and only if the following relationships are true:*

1) *the group $(Q;+)$ is commutative;*

2) *$p\equiv \ell \pmod{|\varphi|}$ if $p,\ell\notin\vec{\imath}$, where $|\varphi|$ denotes the order of the automorphism φ;*

3) *a decomposition of the operation h is the following*

$$\begin{aligned} h(x_{i_0},\dots,x_{i_k})=\varphi^{-i}\big((\varphi^p-\varphi^{i_0})x_{i_0}+\dots+(\varphi^p-\varphi^{i_{m-1}})x_{i_{m-1}}+\varphi^p x_i+\\ +(\varphi^p-\varphi^{i_{m+1}})x_{i_{m+1}}+\dots+(\varphi^p-\varphi^{i_k})x_{i_k}\big)+b \end{aligned} \tag{8}$$

for some $p\notin\vec{\imath}$ and $b\in Q$.

Proof. Let the operation g be commutative, then the identities (6) and (7) are true. Since the type $\vec{\imath}$ is not maximal then there exists a nonnegative integer $p\leqslant n$, which does not belong to the cross isomorphism type $\vec{\imath}$.

We replace all variables, except x_i and x_p, with the neutral element 0 of $(Q;+)$ in (6). From the commutativity of the operation g we have:

$$g(\overset{p}{0}, x_p, \overset{i-p}{0}, x_i, \overset{n-i}{0}) = g(\overset{p}{0}, x_i, \overset{i-p}{0}, x_p, \overset{n-i}{0}), \quad \text{if } p < i,$$

$$g(\overset{i}{0}, x_i, \overset{p-i}{0}, x_p, \overset{n-p}{0}) = g(\overset{i}{0}, x_p, \overset{p-i}{0}, x_i, \overset{n-p}{0}), \quad \text{if } p > i.$$

Taking into account (7), we obtain

$$\begin{aligned} &\varphi^p x_p + \varphi^i \lambda x_i = \varphi^p x_i + \varphi^i \lambda x_p, \quad \text{when } p < i, \\ &\varphi^i \lambda x_i + \varphi^p x_p = \varphi^i \lambda x_p + \varphi^p x_i, \quad \text{when } p > i, \end{aligned} \tag{9}$$

where $\lambda x := h(\overset{m}{0}, x, \overset{k-m}{0})$. Therefore, according to Lemma 2, the group $(Q;+)$ is commutative.

We denote $b := h(0, \ldots, 0)$ and put $x_p = 0$ in (9):

$$\varphi^i \lambda x = \varphi^i b + \varphi^p x. \tag{10}$$

We notice that the commutativity of g implies the identity

$$g(x_0^{p-1}, x_p, x_{p+1}^{q-1}, x_q, x_q^n) = g(x_0^{p-1}, x_q, x_{p+1}^{q-1}, x_p, x_q^n) \tag{11}$$

for arbitrary numbers p, q.

To find a decomposition of the operation h we set $q = i_r$ for some $r \in \{0, \ldots, m+1, m-1, \ldots, k\}$ and $p \notin \vec{\imath}$ in (11) and replace the operation g with its decomposition (7):

$$\begin{aligned} &\varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_k}) + \sum_{j=0, j\neq i}^{n} \varphi^j x_j + a = \\ &= \varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_{r-1}}, x_p, x_{i_{r+1}}, \ldots, x_{i_k}) + \\ &+ \sum_{j=0, j\neq i, i_r, p}^{n} \varphi^j x_j + \varphi^p x_{i_r} + \varphi^{i_r} x_p + a. \end{aligned} \tag{12}$$

After canceling the same summands and setting $x_p = 0$, we obtain

$$\varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_k}) + \varphi^{i_r} x_{i_r} = \varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_{r-1}}, 0, x_{i_{r+1}}, \ldots, x_{i_k}) + \varphi^p x_{i_r}.$$

Thence

$$\varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_k}) = \varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_{r-1}}, 0, x_{i_{r+1}}, \ldots, x_{i_k}) + (\varphi^p - \varphi^{i_r}) x_{i_r}.$$

We shall use this equality successively for $r = 0, \ldots, m+1, m-1, \ldots, k$:

$$\begin{aligned} \varphi^i h(x_{i_0}, x_{i_1}, \ldots, x_{i_k}) &= \varphi^i h(0, x_{i_1}, \ldots, x_{i_k}) + (\varphi^p - \varphi^{i_0}) x_{i_0} = \\ &= \varphi^i h(0, 0, x_{i_2}, \ldots, x_{i_k}) + (\varphi^p - \varphi^{i_0}) x_{i_0} + (\varphi^p - \varphi^{i_1}) x_{i_1} = \cdots = \\ &= \varphi^i h(\overset{m}{0}\ x_{i_m}, \overset{k-m}{0}) + \sum_{r=0, j\neq m}^{k} (\varphi^p - \varphi^{i_r}) x_{i_r} = \\ &\overset{(10)}{=} \varphi^p x_{i_m} + \varphi^i b + \sum_{j=0, r\neq m}^{k} (\varphi^p - \varphi^{i_r}) x_{i_r}. \end{aligned}$$

Thence we obtain the equality (8).

Let us set up in the equality (11) all variables with 0, except x_p and x_ℓ, if $q = \ell$. Taking into account decomposition (7) and commutativity of the decomposition group after respective cancellation we obtain $\varphi^p x_p + \varphi^\ell x_\ell = \varphi^p x_\ell + \varphi^\ell x_p$. Setting $x_p = 0$ in the preceding equality, we obtain $\varphi^p = \varphi^\ell$. It follows that $\varphi^{p-\ell} = \varepsilon$, therefore $|\varphi|$ divides $p - \ell$, i.e. $p \equiv \ell \pmod{|\varphi|}$.

It is easy to prove the inverse statement. □

Putting $b = 0$ in Theorem 3, we obtain a theorem for polyagroup strong cross isomorphs.

4 Mediality

We shall clarify the conditions when a principal cross isomorph $(Q; g)$ is medial, i.e. when the following identity

$$\begin{aligned} &g(g(x_{00}, x_{01}, \ldots, x_{0n}), g(x_{10}, x_{11}, \ldots, x_{1n}), \ldots, g(x_{n0}, x_{n1}, \ldots, x_{nn})) = \\ &= g(g(x_{00}, x_{10}, \ldots, x_{n0}), g(x_{01}, x_{11}, \ldots, x_{n1}), \ldots, g(x_{0n}, x_{1n}, \ldots, x_{nn})) \end{aligned} \tag{13}$$

is true. The next theorem can give an answer to this question.

Theorem 4. *Let a pair (ε, h) be a principal weak cross isomorphism of a nonmaximal type $(m, \vec{\imath})$, where $\vec{\imath} := (i_0, i_1, \ldots, i_k)$, between an $(n+1)$-ary groupoid $(Q; g)$ and $(n+1)$-ary polyagroup $(Q; f)$ with a decomposition $(+, \varphi, a)$ and let $n > 2k$. A groupoid $(Q; g)$ is medial if and only if there exist endomorphisms $\lambda_0, \ldots, \lambda_{m-1}, \lambda_{m+1}, \ldots, \lambda_k$, an automorphism λ_m and an element b of the group $(Q; +)$ such that:*

1) *$(Q; +)$ is commutative;*

2) *the relation*

$$h(y_0, y_1, \ldots, y_n) = \lambda_0 y_0 + \lambda_1 y_1 + \cdots + \lambda_k y_k + b \tag{14}$$

holds for all $y_0, y_1, \ldots, y_k \in Q$;

3) *for arbitrary $r = 0, 1, \ldots, k$ and $p \notin \vec{\imath}$ the following relations are true*

$$\lambda_r \varphi^p = \varphi^p \lambda_r, \tag{15}$$

$$(\lambda_r \varphi^i + \varphi^{i_r})\lambda_m = \lambda_m(\varphi^i \lambda_r + \varphi^{i_r}), \tag{16}$$

4) *for arbitrary $i_{r_1}, i_{r_2} \in \vec{\imath}$ and $i_{r_1} \neq i_{r_2} \neq i$ the following equality is valid*

$$\lambda_{r_1}(\varphi^i \lambda_{r_2} + \varphi^{i_{r_2}}) + \varphi^{i_{r_1}} \lambda_{r_2} = \lambda_{r_2}(\varphi^i \lambda_{r_1} + \varphi^{i_{r_1}}) + \varphi^{i_{r_2}} \lambda_{r_1}. \tag{17}$$

Proof. Suppose that the groupoid $(Q;g)$ is medial, i.e. (13) holds, the equality (7) implies

$$g(0,\ldots,0) = \varphi^i b + a, \tag{18}$$

where $b := h(0,\ldots,0)$. Nonmaximality of the type $\vec{\imath}$ means the existence of a number p not belonging to $\vec{\imath}$. We replace all variables in (13), except x_{pi} and x_{ip}, with the neutral element 0 of the group $(Q;+)$. Then there exist transformations μ_1, μ_2, μ_3, μ_4, which are compositions of translations of $(Q;+)$ and m-th translations of h such that

$$\mu_1 x_{pi} + \mu_2 x_{ip} = \mu_1 x_{ip} + \mu_2 x_{pi}.$$

The cross isotopy definition means m-invertibility of h, so that these transformations are substitutions of Q. So, according to Lemma 2 the operation $(+)$ is commutative.

We replace the operation h and the element a with the operation h_0 and the element a_0, determined with the following equalities

$$h_0(y_0,\ldots,y_k) := h(y_0,\ldots,y_k) - h(0,\ldots,0),$$
$$a_0 := \varphi^i h(0,\ldots,0) + a = \varphi^i b + a.$$

Therefore, taking into account commutativity of $(Q;+)$, the decomposition (7) of g can be written in the form:

$$g(x_0,\ldots,x_n) = \varphi^i h_0(x_{i_0},\ldots,x_{i_k}) + \sum_{j=0,j\neq i}^{n} \varphi^j x_j + a_0. \tag{19}$$

We recall that $h_0(0,\ldots,0) = 0$.

Now we replace the first occurence of g in left and right sides of (13) with its decomposition (19):

$$\begin{aligned}
&\varphi^i h_0(g(x_{i_0 0},\ldots,x_{i_0 n}),\ldots,g(x_{i_k 0},\ldots,x_{i_k n})) + \\
&\qquad + \sum_{j=0,j\neq i}^{n} \varphi^j g(x_{j0},\ldots,x_{jn}) + a_0 = \\
&= \varphi^i h_0(g(x_{0i_0},\ldots,x_{ni_0}),\ldots,g(x_{0i_k},\ldots,x_{ni_k})) + \\
&\qquad + \sum_{j=0,j\neq i}^{n} \varphi^j g(x_{0j},\ldots,x_{nj}) + a_0.
\end{aligned} \tag{20}$$

Let us consider the second summands in the left and right sides of this equality. The summand of the left side is equal to

$$\begin{aligned}
&\sum_{j=0,j\neq i}^{n} \varphi^j g(x_{j0},\ldots,x_{jn}) = \\
&\overset{(19)}{=} \sum_{j=0,j\neq i}^{n} \varphi^j \left(\varphi^i h_0(x_{ji_0},\ldots,x_{ji_k}) + \sum_{u=0,u\neq i}^{n} \varphi^u x_{ju} + a_0\right) = \\
&= \sum_{j=0,j\neq i}^{n} \varphi^{i+j} h_0(x_{ji_0},\ldots,x_{ji_k}) + \sum_{j=0,j\neq i}^{n} \sum_{u=0,u\neq i}^{n} \varphi^{j+u} x_{ju} + \sum_{j=0,j\neq i}^{n} \varphi^j a_0.
\end{aligned}$$

By analogy we obtain a decomposition of the second summand of the right side:

$$\sum_{j=0,j\neq i}^{n} \varphi^j g(x_{0j},\dots,x_{nj}) =$$
$$= \sum_{j=0,j\neq i}^{n} \varphi^{i+j} h_0(x_{i_0 j},\dots,x_{i_k j}) + \sum_{j=0,j\neq i}^{n}\sum_{u=0,u\neq i}^{n} \varphi^{j+u} x_{uj} + \sum_{j=0,j\neq i}^{n} \varphi^j a_0.$$

We notice that the following equality is obvious

$$\sum_{j=0,j\neq i}^{n}\sum_{u=0,u\neq i}^{n} \varphi^{j+u} x_{ju} + \sum_{j=0,j\neq i}^{n} \varphi^j a_0 = \sum_{j=0,j\neq i}^{n}\sum_{u=0,u\neq i}^{n} \varphi^{j+u} x_{uj} + \sum_{j=0,j\neq i}^{n} \varphi^j a_0,$$

therefore (20) can be cancelled on these summands and element a_0.

$$\varphi^i h_0(g(x_{i_0 0},\dots,x_{i_0 n}),\dots,g(x_{i_k 0},\dots,x_{i_k n})) + \sum_{j=0,j\neq i}^{n} \varphi^{i+j} h_0(x_{j i_0},\dots,x_{j i_k}) =$$
$$= \varphi^i h_0(g(x_{0 i_0},\dots,x_{n i_0}),\dots,g(x_{0 i_k},\dots,x_{n i_k})) + \sum_{j=0,j\neq i}^{n} \varphi^{i+j} h_0(x_{i_0 j},\dots,x_{i_k j}).$$

After mentioned transformations we can apply the automorphism φ^{-i} to the equality

$$h_0(g(x_{i_0 0},\dots,x_{i_0 n}),\dots,g(x_{i_k 0},\dots,x_{i_k n})) + \sum_{j=0,j\neq i}^{n} \varphi^{j} h_0(x_{j i_0},\dots,x_{j i_k}) =$$
$$= h_0(g(x_{0 i_0},\dots,x_{n i_0}),\dots,g(x_{0 i_k},\dots,x_{n i_k})) + \sum_{j=0,j\neq i}^{n} \varphi^{j} h_0(x_{i_0 j},\dots,x_{i_k j}).$$

We replace all occurences of g with its decomposition (19):

$$h_0\left(\varphi^i h_0(x_{i_0 i_0},\dots,x_{i_0 i_k}) + \sum_{j=0,j\neq i}^{n} \varphi^j x_{i_0 j} + a_0;\dots;\varphi^i h_0(x_{i_k i_0},\dots,x_{i_k i_k}) + \right.$$
$$\left. + \sum_{j=0,j\neq i}^{n} \varphi^j x_{i_k j} + a_0\right) + \sum_{j=0,j\neq i}^{n} \varphi^j h_0(x_{j i_0},\dots,x_{j i_k}) =$$
$$= h_0\left(\varphi^i h_0(x_{i_0 i_0},\dots,x_{i_k i_0}) + \sum_{j=0,j\neq i}^{n} \varphi^j x_{j i_0} + a_0;\dots;\varphi^i h_0(x_{i_0 i_k},\dots,x_{i_k i_k}) + \right.$$
$$\left. + \sum_{j=0,j\neq i}^{n} \varphi^j x_{j i_k} + a_0\right) + \sum_{j=0,j\neq i}^{n} \varphi^j h_0(x_{i_0 j},\dots,x_{i_k j}). \tag{21}$$

Let $p \notin \vec{\imath}$. We replace all variables, except $x_{i_0 p}$, $\dots$, $x_{i_k p}$, with 0. Inasmuch as $h_0(0,\dots,0) = 0$, then (21) can be given in the form

$$\varphi^p h_0(x_{i_0 p},\dots,x_{i_k p}) = h_0(\varphi^p x_{i_0 p} + a_0,\dots,\varphi^p x_{i_k p} + a_0) - h_0(a_0,\dots,a_0). \tag{22}$$

We add to the both sides of (21) the element $(n-k)(-h_0(a_0,\dots,a_0))$ and apply (22) to the last summands of (21). Then the equality (21) in the case $x_{uv} = 0$ for all $u, v \in \vec{\imath}$ gives

$$h_0\left(\sum_{j=0,j\notin\vec{\imath}}^{n}\varphi^j x_{i_0j}+a_0;\dots;\sum_{j=0,j\notin\vec{\imath}}^{n}\varphi^j x_{i_kj}+a_0\right)+$$
$$+\sum_{j=0,j\notin\vec{\imath}}^{n} h_0\left(\varphi^j x_{ji_0}+a_0;\dots;\varphi^j x_{ji_k}+a_0\right)=$$
$$=h_0\left(\sum_{j=0,j\notin\vec{\imath}}^{n}\varphi^j x_{ji_0}+a_0;\dots;\sum_{j=0,j\notin\vec{\imath}}^{n}\varphi^j x_{ji_k}+a_0\right)+$$
$$+\sum_{j=0,j\notin\vec{\imath}}^{n} h_0\left(\varphi^j x_{i_0j}+a_0;\dots;\varphi^j x_{i_kj}+a_0\right).$$

Let us replace $\varphi^j y + a_0$ with y for all variables y appearing in the last identity:

$$h_0\left(\sum_{j=0,j\notin\vec{\imath}}^{n}x_{i_0j};\dots;\sum_{j=0,j\notin\vec{\imath}}^{n}x_{i_kj}\right)+\sum_{j=0,j\notin\vec{\imath}}^{n}h_0(x_{ji_0},\dots,x_{ji_k})=$$
$$=h_0\left(\sum_{j=0,j\notin\vec{\imath}}^{n}x_{ji_0};\dots;\sum_{j=0,j\notin\vec{\imath}}^{n}x_{ji_k}\right)+\sum_{j=0,j\notin\vec{\imath}}^{n}h_0(x_{i_0j},\dots,x_{i_kj}). \tag{23}$$

Inasmuch as $n > 2k$, then there exist at least $k+1$ numbers which do not belong to $\vec{\imath}$. We denote them by p_0, p_1,..., p_k and replace all variables in (23), except $x_{p_0i_0}$, $x_{p_1i_1}$, ..., $x_{p_ki_k}$, with 0:

$$h_0(x_{p_0i_0},\overset{k}{0})+h_0(0,x_{p_1i_1},\overset{k-1}{0})+\dots+h_0(\overset{k}{0},x_{p_ki_k})=h_0(x_{p_0i_0},x_{p_1i_1},\dots,x_{p_ki_k}).$$

Denoting $y_j := x_{p_ji_j}$ and $\lambda_j x := h_0(\overset{j}{0}, x, \overset{k-j}{0})$ for all $j = 0, 1, \dots, k$, we obtain

$$h_0(y_0,y_1,\dots,y_k)=\lambda_0y_0+\lambda_1y_1+\dots+\lambda_ky_k. \tag{24}$$

It implies a decomposition (14) of h.

In the identity (23) we replace all variables, except $x_{i_rp_0}$ and $x_{i_rp_1}$, with 0 and replace h_0 with its decomposition:

$$\lambda_r(x_{i_rp_0}+x_{i_rp_1})=\lambda_rx_{i_rp_0}+\lambda_rx_{i_rp_1},$$

i.e. λ_r is an endomorphism of the group $(Q;+)$.

Let us replace h_0 with its decomposition (24) in (21). Since every of λ_0, ..., λ_k is an endomorphism of commutative group $(Q;+)$, then left and right sides of the obtained equality can be cancelled on $\lambda_0 a_0 + \dots + \lambda_k a_0$:

$$\lambda_0 \left(\varphi^i(\lambda_0 x_{i_0 i_0} + \dots + \lambda_k x_{i_0 i_k}) + \sum_{j=0, j\neq i}^{n} \varphi^j x_{i_0 j} \right) + \dots$$
$$\dots + \lambda_k \left(\varphi^i(\lambda_0 x_{i_k i_0} + \dots + \lambda_k x_{i_k i_k}) + \sum_{j=0, j\neq i}^{n} \varphi^j x_{i_k j} \right) +$$
$$+ \sum_{j=0, j\neq i}^{n} \varphi^j(\lambda_0 x_{j i_0} + \dots + \lambda_k x_{j i_k}) =$$
$$= \lambda_0 \left(\varphi^i(\lambda_0 x_{i_0 i_0} + \dots + \lambda_k x_{i_k i_0}) + \sum_{j=0, j\neq i}^{n} \varphi^j x_{j i_0} \right) + \dots$$
$$\dots + \lambda_k \left(\varphi^i(\lambda_0 x_{i_0 i_k} + \dots + \lambda_k x_{i_k i_k}) + \sum_{j=0, j\neq i}^{n} \varphi^j x_{j i_k} \right) +$$
$$+ \sum_{j=0, j\neq i}^{n} \varphi^j(\lambda_0 x_{i_0 j} + \dots + \lambda_k x_{i_k j}). \qquad (25)$$

Let us consider the equality (25). Let $i_r \in \vec{\imath}$, $p \notin \vec{\imath}$. Replacing all variables, except $x_{i_r p}$, with 0 we obtain the relationship (15).

We replace all variables in (25) with 0, except $x_{i_r i}$:

$$\lambda_r \varphi^i \lambda_m + \varphi^{i_r} \lambda_m = \lambda_m(\varphi^i \lambda_r + \varphi^{i_r}).$$

It implies (16).

Let $r_1, r_2 \in \{0, \dots, m-1, m+1, \dots, k\}$. If we replace all variables in (25) with 0, except $x_{i_{r_1} i_{r_2}}$, then in the left side of the equality we have $\lambda_{r_1}(\varphi^i \lambda_{r_2} + \varphi^{i_{r_2}}) + \varphi^{i_{r_1}} \lambda_{r_2}$, and in the right side we obtain $\lambda_{r_2}(\varphi^i \lambda_{r_1} + \varphi^{i_{r_1}}) + \varphi^{i_{r_2}} \lambda_{r_1}$. i.e. (17) is true.

Vice versa, let $(Q;+)$ be commutative group, $\lambda_0, \dots, \lambda_k$ be its endomorphisms; λ_m be its automorphism; b be an arbitrary element of Q; an operation h be determined by (14), and let the relationships (15)–(17) be valid. Thus, the operation g has a decomposition

$$g(x_0, \dots, x_n) = \sum_{j=0, j\notin \vec{\imath}}^{n} \varphi^j x_j + \sum_{r=0, r\neq m}^{k} (\varphi^{i_r} + \varphi^i \lambda_r) x_r + \varphi^i \lambda_m x_i + \varphi^i b + a. \qquad (26)$$

All coefficients of g's decomposition are endomorphisms of the group $(Q;+)$. From the relationships (15), (16), (17) it follows that the coefficients pairwise commute. It is easy to prove that every such operation is medial. □

If a cross isomorphism is strong, then the operation h is idempotent (it follows that $b = h(0, \dots, 0) = 0$). Hence, Theorem 4 with $b = 0$ states a mediality criterion for a polyagroup strong cross isomorph.

5 Neutral elements

Every group isotop with a neutral element is derived. But for group cross isotop it is not true. The set of all identity elements of derived group is a subgroup of its decomposition group center. The structure of the set of all neutral elements of a cross isotop is still unknown. Here we consider a neutrality criterion in medial polyagroup cross isotopes only, i.e. having commutative decomposition groups.

Theorem 5. *Let $(Q; g)$ be i-cross isomorph of the type $\vec{\imath} := (i_0, i_1, \ldots, i_k)$, where $i = i_m$, of an $(n+1)$-ary medial polyagroup $(Q; f)$ with decomposition $(+, \varphi, a)$ and let (ε, h) be respective cross isomorphism. Then element e of the set Q is neutral in $(Q; g)$ if and only if*

1) $\varphi^p = \varepsilon$, *when* $p \notin \vec{\imath}$;
2) *for all* $r = 0, \ldots, m-1, m+1, \ldots, k$

$$h(\overset{r}{e}, x, \overset{k-r}{e}) = b + \varphi^{-i}(x - e) - \varphi^{i_r - i}(x - e); \tag{27}$$

3) *for all* x *from* Q

$$h(\overset{m}{e}, x, \overset{k-m}{e}) = b + \varphi^{-i}(x - e); \tag{28}$$

4) $g(e, \ldots, e) = e$.

Proof. Let e be a neutral element of $(Q; g)$, i.e. for arbitrary $j = 0, \ldots, n$

$$g(\overset{j}{e}, x, \overset{n-j}{e}) = x \tag{29}$$

holds for all $x \in Q$. In particular, when $x = e$ we obtain item 4) of Theorem 5. Taking into account the decomposition (7) and the relation $\varphi^n x + a = a + x$, we have

$$\varphi^i b + c = 0, \tag{30}$$

where $b := h(e, \ldots, e)$, $c := a + \sum\limits_{j=0, j \neq i}^{n-1} \varphi^j e$.

If p does not belong to $\vec{\imath}$, then (29) with decomposition (7) implies the equality

$$\varphi^i b + c + e - \varphi^p e + \varphi^p x = x$$

for all $x \in Q$. Taking into account (30), we obtain

$$\varphi^p x = x + \varphi^p e - e.$$

If $x = 0$ then $\varphi^p e = e$, which together with the previous equality give $\varphi^p = \varepsilon$, i.e. item 1) of Theorem 5 is valid.

We suppose that r is one of the numbers $0, 1, \ldots, k$, then (29) means that

$$\varphi^i h(\overset{r}{e}, x, \overset{k-r}{e}) + c - \varphi^{i_r} e + \varphi^{i_r} x + e = x.$$

Taking into account (30), we have

$$\varphi^i h(\overset{r}{e}, x, \overset{k-r}{e}) - \varphi^i b - \varphi^{i_r} e + \varphi^{i_r} x + e = x.$$

It implies (27).

If $j=i$, the equality (29) has the form

$$g(e,\dots,e)+\varphi^i h(\overset{m}{e},x,\overset{k-m}{e})-\varphi^i h(e,\dots,e)=x.$$

This equality is equivalent to $\varphi^i h(\overset{m}{e},x,\overset{k-m}{e})-\varphi^i b=x-e$. Hence (28) is valid.

Vice versa, let the conditions 1) – 4) of the theorem for some element e be true. We shall show that e is a neutral element. If $j\in\vec{\imath}$, then

$$g(\overset{j}{e},x,\overset{n-j}{e})\overset{(20)}{=}e+\varphi e+\ldots+\varphi^{i-1}e+\varphi^i h(\overset{k+1}{e})+\varphi^{i+1}e+\ldots+\varphi^n e+$$

$$+a-\varphi^j e+\varphi^j x\overset{1),3)}{=}g(e,\dots,e)-e+x=e-e+x=x.$$

If $j\neq i$ and $j\in\vec{\imath}$, i.e. $j=i_r$ for some number $r\in\{0,\dots,m-1,m+1,\dots,k\}$, then

$$g(\overset{j}{e},x,\overset{n-j}{e})\overset{(7)}{=}e+\varphi e+\ldots+\varphi^{i-1}e+\varphi^i h(\overset{r}{e},x,\overset{k-r}{e})+\varphi^{i+1}e+\ldots+\varphi^n e+$$

$$+a+\varphi^{i_r}x-\varphi^{i_r}e=g(e,\dots,e)-\varphi^i b+\varphi^i h(\overset{r}{e},x,\overset{k-r}{e})+\varphi^{i_r}x-\varphi^{i_r}e$$

$$\overset{(27)}{=}e-\varphi^i b+\varphi^i b+x-e-\varphi^{i_r}(x-e)+\varphi^{i_r}(x-e)=x.$$

At last, let $j=i=i_m$, then

$$g(\overset{i}{e},x,\overset{n-i}{e})\overset{(7)}{=}e+\varphi e+\ldots+\varphi^{i-1}e+\varphi^i h(\overset{m}{e},x,\overset{k-m}{e})+\varphi^{i+1}e+\ldots+\varphi^n e+a=$$

$$=g(e,\dots,e)-\varphi^i b+\varphi^i h(\overset{m}{e},x,\overset{k-m}{e})\overset{(28)}{=}e-\varphi^i b+\varphi^i b+x-e=x. \qquad \square$$

References

[1] Sokhatsky F.M. *On cross isotopy and cross isomorphism.* Trudy instytuta prykladnoyi matematyky i mekhaniky NAN Ukrainy, 2005, vyp. 11, p. 23–33 (in Ukrainian).

[2] Yurevych O.V. *On cross isotopy of polyagrups.* Trudy instytuta prykladnoyi matematyky i mekhaniky NAN Ukrainy, 2005, vyp. 11, p. 34–49 (in Ukrainian).

[3] Belousov V.D. *Cross isotopy of quasigroups.* Quasigroups and their systems. Chishinau, Shtiintsa, 1990, p. 14–20 (in Russian).

[4] Kuznetsov E.A. *Transversals in groups. 4.* Quasigroups and Related Systems, 2002, **9**, p. 67–84.

[5] Sokhatsky F.N. *On poliadic groups.* Sovremennaya algebra: Mezhvuzovsky sbornik nauchnykh trudov, 1997, vyp. 2(22), p. 79–94 (in Russian).

[6] Sokhatsky F.N. *On associativity of multiary operation.* Diskretnaya mathematika, 1992, **4**, vyp. 1, p. 66–84 (in Russian).

[7] Sokhatsky F.M. *On isotopes group I.* Ukrainian mathematical journal, 1995, N 10, p. 1387–1398.

Vinnytsia University
32 Ostrozka Street
Vinnytsia 21100, Ukraine
E-mail: *fedir@vinnitsa.com*

Received December 13, 2005

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 153–164
ISSN 1024–7696

Cores of Bol loops and symmetric groupoids *

A. Vanžurová

Abstract. The notion of a core was originally invented by R.H. Bruck for Moufang loops, [3], and the construction was generalized by V.D. Belousov for quasigroups in [2] (we will discuss 1-cores here). It is well known that cores of left Bol loops, particularly cores of Moufang loops, or groups, are left distributive, left symmetric, and idempotent, [2]. Among others, our aim is to clarify the relationship between cores and the variety of left symmetric left distributive idempotet groupoids, $\underline{SID}$, or its medial subvariety, $\underline{SIE}$, respectively. The class of cores of left Bol loops is not closed under subalgebras, therefore is no variety (even no quasivariety), and we can ask what variety is generated by cores: the class of left Bol loop cores (even the class of group cores) generates the variety of left distributive left symmetric idempotent groupoids, while cores of abelian groups generate the variety of idempotent left symmetric medial groupoids.

It seems that the variety $\underline{SID}$ of left distributive left symmetric idempotent groupoids ("symmetric groupoids") aroused attention especially in connection with symmetric spaces in 70' and 80' [15, 16, 18, 19] and the interest continues. Recently, it was treated in [8, 26, 27], and also in [29], from the view-point of hypersubstitutions. The right symmetric idempotent and medial case was investigated e.g. in [1, 21–24].

Mathematics subject classification: 20N05.
Keywords and phrases: Groupoid, variety of algebras, quasigroup, loop, Bol identity, core.

1 Preliminaries

We use the standard notation of universal algebra here, [5–7]. $T_\tau(X)$ denotes the set of all terms of a type τ over a non-empty set X. An algebra with the carrier set A and the sequence $F = (f_i)_{i\in I}$ of operation symbols is denoted by $\mathcal{A} = (A; F)$. The fundamental operation corresponding to the operation symbol f_i in the algebra $\mathcal{A}$ is denoted by ${f_i}^{\mathcal{A}}$. If $\mathcal{A} = (A; F)$ is an algebra and $\tilde{F} = (f_i)_{i\in\tilde{I}}$, $\tilde{I} \subset I$ a subsequence of the sequence F of operation symbols then $\tilde{\mathcal{A}} = (A; \tilde{F})$ is called a *reduct* of $\mathcal{A}$, [20].

If the class V of algebras is defined by identities, i.e. is a variety of algebras (equivalently speaking, is closed under homomorphic images of subalgebras of products), [6], let us denote it by $\underline{V}$, and denote $Id\underline{V}$ the set of all identities valid in $\underline{V}$. If Σ is the defining set of identities of the variety $\underline{V}$ we write $\underline{V} = Mod(\Sigma)$ (Mod means "models").

More generally, a class of algebras closed under subalgebras and products is called a *quasivariety*.

*Supported by grant No201/05/2707 of The Grant Agency of Czech Republic.

2 Symmetric groupoids

2.1 Some identities in groupoids. Under *left* (*right*) *cancellation* we understand the quasi-identity $(C_l) : xy = xy' \Rightarrow y = y'$ (or $(C_r) : xy = x'y \Rightarrow x = x'$, respectively). We will pay attention to the following identities:

(S_l) $\quad x \cdot (x \cdot y) = y \quad$ (left symmetry);
(S_l) $\quad x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z) \quad$ (left self-distributivity);
(I) $\quad x \cdot x = x \quad$ (idempotency);
(E) $\quad (x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u) \quad$ (mediality, or entropy).

Note that the identity (S_l) is also called left keyes identity [10]. Consider the variety of *left symmetric* groupoids $\underline{S} = Mod(S_l)$. Analogously, *right symmetric* groupoids are introduced by the mirror identity (S_r): $(y \cdot x) \cdot x = y$ and form a variety $\underline{RS} = Mod(S_r)$. Evidently, due to the mirror symmetry of both theories, it is sufficient to investigate one of them, we prefer the left one.

Any left symmetric groupoid $\mathcal{A} = (A; \cdot) \in \underline{S}$ is left cancellative, and left translations $L_a : x \mapsto ax$, $a, x \in A$, are permutations of the underlying set. A groupoid is left symmetric if and only if every left translation is an involutive permutation. Any left translation may be decomposed into disjoint cycles of length at most two. Moreover, the algebra $(A; \cdot, \cdot)$ is a left quasigroup (indeed, if $c = a \cdot b$ then $b = a \cdot c$ for $a, b, c \in A$, another speaking, $u = a \cdot b$ is a unique solution in A of the equation $a \cdot u = b$ with $a, b \in A$). Analogously for right translations in the right symmetric case.

A groupoid $(A; \cdot)$ is idempotent iff each singleton $\{a\}$ is a subalgebra. A product of n copies of $a \in A$ is again a, independently of the placement of brackets. Not much can be proved about $\underline{I} = Mod(I)$, but idempotency combined with further identities leads to more interesting structures.

Medial idempotent groupoids are distributive (i.e. left and right distributive).

Mediality of a groupoid $(A; \cdot)$ means that the basic operation yields a homomorphism $(a, b) \mapsto ab$, $(A^2; \cdot) \to (A; \cdot)$. The following consequence of mediality might be of some interest: the set of endomorphisms of a medial groupoid is closed under multiplication (which is not the case for groupoids in general):

Lemma 2.1. *Let $\mathcal{A} = (A; \cdot)$ be a medial groupoid, and $End(\mathcal{A})$ the set of its endomorphisms. Given φ, $\psi \in End(\mathcal{A})$, define $(\varphi \cdot \psi)(x) := \varphi(x) \cdot \psi(x)$. Then $\varphi \cdot \psi \in End(\mathcal{A})$.*

Proof. In fact, given $\mathcal{A}$ medial, φ, $\psi \in End(\mathcal{A})$ and $a, b \in A$ we calculate $(\varphi \cdot \psi)(a \cdot b) = \varphi(a \cdot b) \cdot \psi(a \cdot b) = (\varphi(a) \cdot \varphi(b)) \cdot (\psi(a) \cdot \psi(b)) = (\varphi(a) \cdot \psi(a)) \cdot (\varphi(b) \cdot \psi(b)) = ((\varphi \cdot \psi)(a)) \cdot ((\varphi \cdot \psi)(b))$. $\square$

Let us consider $\underline{SI} = Mod(\{(S_l), (I)\})$, i.e. groupoids which are both idempotent and left symmetric. In $\underline{SI}$ the following holds: $x^n \cdot y^m = x \cdot y$ for $n, m \in \mathbb{N}$,

$$\underbrace{x \cdot (x \cdot (\cdots (x \cdot y) \dots))}_{k\text{-times}} = y \text{ for } k \text{ even}, \quad \underbrace{x \cdot (x \cdot (\cdots (x \cdot y) \dots))}_{k\text{-times}} = x \cdot y \text{ for } k \text{ odd},$$

$$x^m \cdot (x^n \cdot y) = x \cdot y \text{ for } k \text{ even}, \; x^m \cdot (x^n \cdot y) = y \text{ for } k \text{ odd}.$$

In the variety of left distributive groupoids $\underline{D} = Mod(\{(D_l)\})$, the identities $x(yx) = (xy)(xx)$, $x(xy) = (xx)(xy)$ and $x(xx) = (xx)(xx)$ hold. In $\underline{SD} = Mod(\{(S_l),(D_l)\})$, the identities $x(yz) = (x(y(xz))$, $x(xy{\cdot}xz) = yz$, $y(yx{\cdot}z) = x(yz)$ and $y(yx \cdot y) = x(yy)$ are satisfied. Quasigroups belonging to $\underline{SD}$ are sometimes called *reflection quasigroups* [10] or *left-sided* quasigroups.

Left distributive quasigroups are idempotent:

Lemma 2.2. *Let $(A;\cdot,\backslash,/)$ be a quasigroup*[1] *such that the groupoid $(A;\cdot)$ is left distributive. Then*

(i) $(A;\cdot)$ *is idempotent,*

(ii) *for any $a \in A$, if $a \cdot b = b$ then $b = a$.*

Proof. Let $a, b \in A$. Then $b \cdot a \underset{(D_l)}{=} b \cdot (b \cdot (b\backslash a)) \underset{(D_l)}{=} (b \cdot b) \cdot (b \cdot (b\backslash a)) = (b \cdot b) \cdot a$, and we use (C_r). Cancelling a, we obtain $b \cdot b = b$, i.e. (i) holds, and (ii) is a consequence. □

In algebra and geometry, examples of algeras belonging to the variety $\underline{SID} = Mod(\{(S_l),(I),(D_l)\})$ of left symmetric left self-distributive idempotent groupoids arise in a natural way. E.g. let us mention cores of left Bol loops, particularly of Moufang loops and groups. Another famous class of (infinite) examples comes from differential geometry, [12]: a symmetric space is in fact an $\underline{SID}$-groupoid defined on a smooth manifold such that the binary operation is a smooth map (with respect to the manifold structure), and a certain local condition is satisfied. If we accept only topological structure we can say that a *symmetric space* $(A;*,\mathcal{T})$ is a groupoid $(A;*) \in \underline{SID}$ together with a topology $\mathcal{T}$ on A such that the binary operation $*$ is continuous and satisfies: each $a \in A$ has a neighborhood $U \subset A$ such that for all $u \in U$, if $a * u = u$ then $u = a$.

$\underline{SID}$-groupoids, or their mirrors, right distributive right symmetric idempotent groupoids (forming the variety $\underline{RSID}$), are known and studied under various names. They were introduced by M. Takasaki in [29] as *kei*, investigated as *symmetric groupoids* in [15, 16], they were also called *symmetric sets* in the finite case, [18] etc. They can be described even in the terminology of quandles (structures with two binary operations, which were used as classifying invariants for knots, [9]): $\underline{RSID}$ may be regarded equivalent with the variety of the so called involutory quandles.

For the sake of brevity, $x_1x_2\dots x_{n-1}x_n$ stands for $x_1(x_2\dots(x_{n-1}x_n)\dots)$, $n \geq 2$; such products will be called *right associated*).

Lemma 2.3. *In $\underline{SID}$, the following identities hold:*

(i) $(xy)z = x(y(xz))$,

(ii) $(y_1y_2\dots y_{m-1}y_m) \cdot z = y_1y_2\dots y_{m-1}y_my_{m-1}\dots y_2y_1z$,

(iii) $(xy)x = x(yx)$.

Proof. First, $x(y(xz)) = (xy)(x(xz)) = (xy)z$ by left distributivity and left symmetry. To prove (ii) we either use (i) $(m-1)$-times, or go by induction on m: for

[1] For the terminology from the theory of quasigroups and loops, e.g. [2, 17].

$m = 2$, the formula follows from (i). Assume that (ii) holds for a natural number $m \geq 2$. Then by (i) and the induction assumption

$$(y_1 y_2 \dots y_m y_{m+1}) \cdot z = (y_1[y_2 \dots y_m y_{m+1}]) \cdot z =$$

$$= y_1([y_2 \dots y_m y_{m+1}](y_1 z)) = y_1(y_2(\dots(y_m(y_{m+1}(y_m(\dots(y_2(y_1 z)\dots).$$

Hence the statement holds for $m+1$, and therefore for all $m \geq 2$. (iii) is a consequence. □

It was noted that group cores are not the only natural examples of $\underline{SID}$-groupoids arising from groups. Given a group $\mathcal{G}$ and an involutory automorphism $f \in Aut(\mathcal{G})$ of the group $\mathcal{G}$, the carrier set G along with the binary operation $(a,b) \mapsto a \diamond_f b := af(a^{-1}b)$ is an $\underline{SID}$-groupoid $(G; \diamond_f)$. If for all x from $\mathcal{G}$, $xf(x)$ is in the center $Z(\mathcal{G})$ for an involutory automorphism $f \in Aut(\mathcal{G})$ of the group $\mathcal{G}$ then $(G; \star_f)$ is also an $\underline{SID}$-groupoid where $a \star_f b = af(ba^{-1})$. The medial case will be discussed separately.

3 Cores of left Bol loops

3.1 Bol loops and cores. Originally, cores were introduced by R.H. Bruck in connection with invariants of isotopism classes of Moufang loops (isotopic Moufang loops have isomorphic cores [3, p. 120–121]). A more general definition was created by V.D. Belousov [2, p. 157]: a *(left) core* (in Russian, 1-*serdcevina*) of a loop $\mathcal{Q} = (\mathcal{Q}; \cdot, \backslash, /, \rceil)$ is a groupoid $Core(\mathcal{Q}) := (\mathcal{Q}; \circ)$ with

$$(a,b) \mapsto a \circ b := a(b \backslash a). \tag{3.1}$$

Under a left Bol loop we usually understand a loop (i.e. a quasigroup with identity element) which satisfies

(B_l) $x(y(xz)) = (x(yx))z$ (left Bol identity).

Alternatively, the variety of left Bol loops may be introduced also in type $(2,1,0)$ and signature $(\cdot, {}^{-1}, e)$, e.g. as

$$\underline{B} = Mod(\{xe = ex = x, (x^{-1})^{-1} = x, x^{-1}(xy) = y, (B_l)\}).$$

For a left Bol loop $\mathcal{B} = (\mathcal{Q}; \cdot, {}^{-\infty}, \rceil) \in \underline{\mathcal{B}}$, the core operation takes the form $a \circ b := a \cdot (b^{-1} \cdot a)$, $a, b \in Q$. Particularly, for Moufang loops (including groups), $a \circ b = ab^{-1}a$ (brackets are not necessary since each pair of elements generates a subgroup). For commutative groups, the core operation is more famous in the notation $a \circ b = 2a - b$.

3.2 Cores as examples of symmetric groupoids. A core $Core(\mathcal{B}) = (\mathcal{Q}; \circ)$ of a Bol loop satisfies the identities (S_l), (D_l) and (I). The proof given by V.D. Belousov in [2, p. 211–215] is based on geometrical considerations, namely on evaluation of coordinates of points and lines in the corresponding Bol net. Let us give here a purely algebraic proof of the statement[2].

[2]Another proof is given in [14, p. 102].

Proposition 3.1. *The core $Core(\mathcal{B})$ of a Bol loop $\mathcal{B} \in \underline{B}$ satisfies:*

$$[a \circ b]^{-1} = a^{-1} \circ b^{-1} \quad \textit{for} \quad a, b \in Q \quad \textit{(automorphic inverse property)},$$

$$[a_n \circ a_{n-1} \circ \cdots \circ a_2 \circ a_1]^{-1} = a_n^{-1} \circ a_{n-1}^{-1} \circ \cdots \circ a_2^{-1} \circ a_1^{-1}, \quad n \geq 2.$$

Proof. Using (B_l), $(x^{-1})^{-1} = x$, and left inverse property we get $a^{-1} \circ b^{-1} = a^{-1}((b^{-1})^{-1}a^{-1}) = a^{-1}(ba^{-1})$, and $(a \circ b) \cdot (a^{-1} \circ b^{-1}) = (a(b^{-1}a)) \cdot (a^{-1}(ba^{-1})) = e$. Hence the second formula holds for $n = 2$. Suppose it holds for a fixed natural number $n \geq 2$. Then $[a_{n+1} \circ (a_n \circ a_{n-1} \circ \cdots \circ a_2 \circ a_1)]^{-1} = a_{n+1}^{-1} \circ [a_n^{-1} \circ a_{n-1}^{-1} \circ \cdots \circ a_2^{-1} \circ a_1^{-1}]$ as claimed. □

Proposition 3.2. *For any left Bol loop $\mathcal{B} \in \underline{B}$, the core $Core(\mathcal{B})$ belongs to the variety $\underline{SID}$.*

Proof. Let $(Q; \circ)$ be a core of a Bol loop and $a, b, c \in Q$. Then $a \circ a = a(a^{-1}a) = a \cdot e = a$, and (I) holds. Further,

$$a \circ (a \circ b) = a \circ \big(a(b^{-1}a)\big) = a\big([a(b^{-1}a)]^{-1}a\big) = a\big((a^{-1}(ba^{-1})) \cdot a\big) \underset{(B_l)}{=}$$

$$\underset{(B_l)}{=} a \cdot \big(a^{-1}[b(a^{-1}a)]\big) = a(a^{-1}b) = b$$

which proves (S_l). To prove (D_l) we can either use the fact that $[x(y^{-1}x)]^{-1} = x^{-1}(yx^{-1})$ is satisfied in $\underline{B}$,

$$a \circ (b \circ c) = a \circ (b \circ (a \circ (a \circ c))) = a\big([b \circ (a \circ (a \circ c))]^{-1}a\big) =$$

$$= a\big(\big[b \circ (a((a \circ c)^{-1}a))\big]^{-1}a\big) = a\big(\big[b([a((a \circ c)^{-1}a)]^{-1}b)\big]^{-1}a\big) =$$

$$= a\big(\big[b^{-1}([a((a \circ c)^{-1}a)]b^{-1})\big]a\big) \underset{(B_l)}{=} a\big(b^{-1}([a((a \circ c)^{-1}a)](b^{-1}a))\big) =$$

$$= a\big(b^{-1}[a((a \circ c)^{-1} \cdot (a(b^{-1}a)))]\big) = (a \circ b) \cdot \big((a \circ c)^{-1} \cdot (a \circ b)\big) = (a \circ b) \circ (a \circ c),$$

another way is to apply Proposition 3.1. □

Cores of differentiable loops are studied in [14] and in [13, p. 299–307].

3.3 Cores of groups, normal forms for terms. The subclass constituted in $\underline{SID}$ by all cores of groups is no variety, even no quasivariety. The reason is that it is not closed under subgroupoids: in cores of groups there might exist $\underline{SID}$-subgroupoids which do not arise as cores of subgroups (consequently, the same for the class of cores of Moufang loops, or cores of Bol loops, respectively). E.g. in the non-entropic $\underline{SID}$-groupoid $Core(S_3)$ there is a non-entropic subgroupoid of order four which is neither a group core nor a Bol loop core:

Example 3.1. The first non-commutative group is the symmetric group S_3, the permutation group of the three-element set. Let us denote $\Pi_1 = id$, $\Pi_2 = (2,3)$, $\Pi_3 = (1,2,3)$, $\Pi_4 = (1,2)$, $\Pi_5 = (1,3)$, $\Pi_6 = (1,3,2)$. Under the isomorphism

$\Pi_k \mapsto k$, $Core(S_3)$ is isomorphic with a groupoid on a six-element set $A = \{1, \dots, 6\}$ endowed with a binary operation "$\circ$" defined by a multiplication table the rows of which (=left translations in the core $Core(S_3) = (A, \circ)$) are given as follows: $L_1 = (3,6)$, $L_2 = (4,5)$, $L_3 = (1,6)$, $L_4 = (2,5)$, $L_5 = (2,4)$, $L_6 = (1,3)$ (cycles of length two). Mediality does not hold in the core of S_3. In fact, there exists a four-element subgroupoid with the carrier set $B = \{2,3,4,5\}$ which is not medial since $(3 \circ 4) \circ (2 \circ 5) = 4$ while $(3 \circ 2) \circ (4 \circ 5) = 2$. $(B, \circ)$ cannot be a core of a group. Indeed, up to isomorphism, there are only two groups of order four, the cyclic group Z_4 and the direct product $Z_2 \oplus Z_2$, [M. Hall Jr., The Theory of Groups, 1959]. Both are abelian, therefore must have medial cores.

But $(B, \circ)$ cannot be a core of a Bol loop, either. By R.P. Burn, [4], any Bol loop of order $2p$ and p^2, p prime, is necessarily a group.

We can ask for the variety generated by cores. Let $\underline{CG} = \langle \{Core(\mathcal{G}) | \mathcal{G} \in \underline{\mathcal{G}}\} \rangle$ denote the subvariety generated by the set of group cores in the variety $\underline{SID}$. Similarly, we might assume the subvariety $\underline{CM}$ generated by cores of Moufang loops, or $\underline{CB}$ generated by cores of left Bol loops, respectively, and the corresponding chain of subvarieties, but it appears that it is quite sufficient to consider group cores only.

Lemma 3.1. *The varieties $\underline{SID}$ and $\underline{CG}$ are identical (and consequently coincide also with $\underline{CB}$, $\underline{CM}$).*

This fact apperas already in [15, 4.12]. The statement follows e.g. from the result of [26, 27]: $\underline{SID}$ is generated by cores of groups. As a (weaker) consequence, $\underline{SID}$ is generated by cores of left Bol loops. The explanation is as follows. With respect to the variety $\underline{SID}$, any term $t \in T_{(2)}(X)$ is equivalent to a (right associated) term of the form

$$w = x_1 x_2 \dots z_{n-1} x_n, \quad z_{i+1} \neq x_i, \quad i = 1, \dots, n-1, \quad x_1, \dots, x_n \in X. \tag{3.2}$$

The proof goes on induction on complexity of terms: for a variable $t \equiv x \in X$, the statement is trivial. Let $t = t_1 t_2$ be a composed term, and let $t_1 = y_1 y_2 \dots y_{m-1} y_m$, $t_2 = z_1 \dots z_k$ are of the form (3.2). The identity (ii) from Lemma 2.3 gives

$$t_1 \cdot t_2 = y_1 y_2 \dots y_{m-1} y_m y_{m-1} \cdots y_2 y_1 t_2,$$

and if $y_1 \neq z_1$ we are done. If $y_1 = z_1$ we may use left symmetry repeatedly to get rid of equal subsequent couples of variables with exception of the last two places. If the last two variables are equal then one of them can be skipped according to (I). We obtain the desired form.

Now we would like to check that (3.2) are normal forms for terms. It remains to show that for each term $t \in T_{(2)}(X)$, a term w of the form (3.2) equivalent to t in $\underline{SID}$ is uniquely determined. The proof is rather standard. Let $Z = \{z_1, z_2, \dots\}$ be a (fixed) countable infinite set. In the core $Core(\mathcal{F}_{\underline{B}}(Z)) = (T_{(2,1,0)}(Z)/Id\,\underline{B}; \circ)$ of the free Bol loop $\mathcal{F}_{\underline{B}}(Z) = (T_{(2,1,0)}(Z)/Id\,\underline{B}; \cdot, ^{-1}, e)$ freely generated by the alphabet Z (or particularly, in the core of the free group), the following formula holds for $n \geq 2$:

$$z_n \circ z_{n-1} \circ \dots \circ z_2 \circ z_1 = z_n z_{n-1}^{-1} \dots z_2^{\epsilon_2} z_1^{\epsilon_1} z_2^{\epsilon_2} \dots z_{n-1}^{-1} z_n, \quad \epsilon_i = (-1)^{n-i}. \tag{3.3}$$

For $n = 2$, the formula holds by definition of $\circ$. We proceed by induction on n. Let (3.3) be satisfied for a fixed natural number $n \geq 2$. Let us evaluate $z = z_{n+1} \circ (z_n \circ (z_{n-1} \circ (\dots (z_2 \circ z_1) \dots))$ for $z_1, \dots, z_{n+1} \in Z$. We obtain

$$z = z_{n+1} \cdot ([z_n \circ (z_{n-1} \circ \cdots \circ z_2 \circ z_1)]^{-1} \cdot z_{n+1}]) =$$

$$= z_{n+1} \cdot ([z_n^{-1} \circ z_{n-1}^{-1} \circ \cdots \circ z_2^{-1} \circ z_1^{-1}] \cdot z_{n+1}) =$$

$$= z_{n+1} \cdot z_n^{-1} \cdot z_{n-1} \cdot \cdots \cdot z_2^{-\epsilon_2} \cdot z_1^{-\epsilon_1} \cdot z_2^{-\epsilon_2} \dots z_{n-1} \cdot z_n^{-1} \cdot z_{n+1}.$$

Hence the power of z_i is now $-\epsilon_i = (-1)^{n+1-i}$.

In the $\underline{SID}$-groupoid $Core(\mathcal{F}_{\underline{B}(Z)})$, let us consider the subgroupoid $\mathcal{Z}$ generated by the set Z. Let us identify term variables $z_1, z_2, \dots$ from the alphabet Z with elements of the basis Z of $\mathcal{Z}$. Keeping the above notation we prove that words of the form (3.2) must be pairwise non-equivalent.

Let w, w' be a couple of different terms in the standard form (3.2). Then $w^{\mathcal{Z}}$, ${w'}^{\mathcal{Z}}$ are different term functions of the groupoid $\mathcal{Z}$. Indeed, let $z_1, \dots, z_n \in Z$ with $z_{i+1} \neq z_i$ for $i = 1, \dots, n-1$, and apply the term function $w^{\mathcal{Z}}$. We obtain $w^{\mathcal{Z}}(z_1, \dots, z_n) = z_n z_{n-1}^{-1} \dots z_i^{\epsilon_i} \dots z_2^{\epsilon_2} z_1^{\epsilon_1} z_2^{\epsilon_2} \dots z_{n-1}^{-1} z_n$, $\epsilon_i = (-1)^{n-i}$. Clearly, the last expression cannot be reduced by means of Bol loop identities $Id\,\underline{B}$ (or by group identities $Id\,\underline{G}$, either) since the subsequent variables are different.

That is why two different terms of the form (3.2) yield different term functions in the algebra $\mathcal{Z} \in \underline{\mathcal{SID}}$. Hence elements of the free $\underline{SID}$-groupoid $\mathcal{F}_{\underline{SID}}(Z) = (T_{(2)}(Z)/Id\,\underline{SID}, \text{juxtaposition})$ freely generated by our set Z can be presented exactly as words of the form (3.2) which proves

Lemma 3.2. *For each term t of the free $\underline{SID}$-groupoid $\mathcal{F}_{\underline{SID}}(X)$, $X \neq \emptyset$, there exists a unique right associated term w of the form (3.2) which is equivalent to t in $\underline{SID}$.*

Let us call w the *normal form* of t in $\underline{SID}$ and write $NF(t) := w$.

Keeping convention about omitting brackets let us introduce a mapping $\mathcal{L} : \mathcal{F}_{\underline{SID}}(Z) \to \mathcal{Z}$ as follows. For any equivalence class $[w]$ where $w \in T_{(2)}(X)$ with $NF(w) = z_1 z_2 \dots z_{n-1} z_n$ define $\mathcal{L}([w]) := z_1 \circ z_2 \circ \cdots \circ z_{n-1} \circ z_n$.

Lemma 3.3. *The mapping $\mathcal{L} : \mathcal{F}_{\underline{SID}}(Z) \to \mathcal{Z}$, $\mathcal{L}([z_1(z_2(\dots(z_{n-1}z_n)\dots))]) = z_1 \circ (z_2 \circ (\cdots \circ (z_{n-1} \circ z_n) \dots))$ is an isomorphism of groupoids.*

Proof. We have proven already that two different terms of the form (3.2) (representants of different classes) are mapped onto different elements in the algebra $\mathcal{Z}$. So $\mathcal{L}$ is injective. $\mathcal{L}$ is also surjective since according to Lemma 2.3 (ii), each element of $\mathcal{Z}$ can be written in a (reduced) right associated form $z_1 \circ \cdots \circ z_n$, and hence considered as an image of a word from the free algebra. Let us verify that $\mathcal{L}([ts]) = \mathcal{L}([t]) \circ \mathcal{L}([s])$ holds. In fact, let $t = x_1 \dots x_n$, $s = y_1 \dots y_m$ be terms from $T_{(2)}(X)$ written in normal form (3.2). Then $\mathcal{L}([t]) = x_1 \circ x_2 \circ \cdots \circ x_{n-1} \circ x_n$, $\mathcal{L}([s]) = y_1 \circ y_2 \circ \cdots \circ y_{m-1} \circ y_m$, $NF([ts]) = x_1 \dots x_n \dots x_1 y_1 \dots y_m$, $\mathcal{L}([ts]) = \mathcal{L}([NF(ts)]) = x_1 \circ \cdots \circ x_n \circ \cdots \circ x_1 \circ y_1 \circ \cdots \circ y_m$. Finally, again by (ii) from Lemma

2.3, $\mathcal{L}([t]) \circ \mathcal{L}([s]) = (x_1 \circ \cdots \circ x_n) \circ (y_1 \circ \cdots \circ y_m) = x_1 \circ \cdots \circ x_n \circ \cdots \circ x_1 \circ y_1 \circ \cdots \circ y_m$, and $\mathcal{L}$ is a homomorphism. □

Consequently, due to isomorphism, $\mathcal{F}_{\underline{SID}}(Z)$, $\mathcal{Z} \in \underline{\mathcal{CG}}$ and $\mathcal{Z} \in \underline{\mathcal{CB}}$ are free infinitely generated algebras in $\underline{SID}$. Hence we obtain

Corollary 3.1. *The varieties $\underline{CB}$, $\underline{CG}$ and $\underline{SID}$ are equivalent.*

Remark 3.1. In the core $Core(\mathcal{F}_{\underline{CML}}(Z))$ of the free commutative Moufang loop $\mathcal{F}_{\underline{CML}}(Z)$ over Z,

$$z_n \circ z_{n-1} \circ \cdots \circ z_2 \circ z_1 = z_n^2 z_{n-1}^{-2} \ldots z_2^{2\epsilon_2} z_1^{\epsilon_1}, \quad \epsilon_i = (-1)^{n-i} \tag{3.4}$$

holds for $n \geq 2$ (the same formula is satisfied for commutative groups). In fact, we can write (using flexibility, left alternative law and (B_l))

$$z_n((z_{n-1}^{-1}([\ldots[z_2^{\epsilon_2}(z_1^{\epsilon_1} z_2^{\epsilon_2})]\ldots]z_{n-1}^{-1})z_n) = z_n((z_{n-1}^{-1}([\ldots[z_2^{\epsilon_2}(z_2^{\epsilon_2} z_1^{\epsilon_1})]\ldots]z_{n-1}^{-1})z_n) =$$

$$= z_n((z_{n-1}^{-1}([\ldots(z_3^{\epsilon_3}([z_2^{2\epsilon_2} z_1^{\epsilon_1}]z_3^{\epsilon_3}))\ldots]z_{n-1}^{-1})z_n) =$$

$$= z_n((z_{n-1}^{-1}([\ldots(z_3^{2\epsilon_3}[z_2^{2\epsilon_2} z_1])\ldots]z_{n-1}^{-1})z_n) = \cdots = z_n^2(z_{n-1}^{-2}(\ldots(z_2^{2\epsilon_2} z_1^{\epsilon_1})\ldots)).$$

In $\underline{CML}$, the last word cannot be reduced (obviously, it can be reduced for commutative groups).

4 Mediality

4.1 $\underline{SIE}$-groupoids and mediality of group cores.

First let us pay attention to commutative groups. Denote by $\underline{AG}$ the variety of abelian groups, and by $\underline{CAG}$ the subvariety generated by cores of abelian groups in the variety $\underline{SID}$. Cores of commutative groups are medial. Indeed, for x, y, z, u from $\mathcal{G} \in \underline{\mathcal{AG}}$, $(x \circ y) \circ (z \circ u) = (x^2 y^{-1})^2 (z^2 u^{-1})^{-1} = (x^2 z^{-1})(y^2 u^{-1})(x^2 z^{-1}) = (x \circ z) \circ (y \circ u)$, hence (E) is satisfied.

Let $\underline{SIE} = Mod(\{(S_l), (I), (E)\})$. Groupoids of this variety are (left and right) distributive, elastic (=flexible), and may be regarded as a generalization of distributive quasigroups.

Note that cores of abelian groups appear also as important examples of modes. Right symmetric idempotent and medial groupoids are named *kei modes* in [19, p. 88–89]. The variety $\underline{RSIE} = Mod(\{(S_r), (I), (E)\})$ was investigated in [1, 21–24] (and denoted SIE).

Example 4.1. Let $x \circ y := 2x - y$ for $x, y \in \mathbb{R}$. Then $(\mathbb{R}; \circ)$ is a $\underline{SIE}$-groupoid, and $(\mathbb{Z}; \circ)$ is its subgroupoid ($\mathbb{R}$ are reals, $\mathbb{Z}$ denotes integers). In geometric words, $x \circ y$ is a point reflexion at x of the point y on the real line. The free $\underline{SIE}$-groupoid on two generators $\mathcal{F}_{\underline{SIE}}(\{x, y\})$ is isomorphic to the core $\mathcal{Q}_1 := Core(\mathbb{Z}; +) = (\mathbb{Z}; \circ)$ with generators 0 and 1 [11, Th. 12, p. 118], [16, p. 89–90].

Now we may paraphrase Theorem 10.5. from [9, p. 48], as follows (for the variety $\underline{RSIE}$ [21, Th. 3.1, p. 265]).

Example 4.2. On $\mathbb{R}^n$, $n \in \mathbb{N}$, let us introduce a binary operation $(x_1, \ldots, x_n) \circ (y_1, \ldots, y_n) := (2x_1 - y_1, \ldots, 2x_n - y_n)$. Then $(\mathbb{R}^n; \circ)$ is a $\underline{SIE}$-groupoid, and $(\mathbb{Z}^n; \circ) = Core(\mathbb{Z}^n; +)$ forms its subgroupoid. In $(\mathbb{Z}^n; \circ)$, let us consider a subgroupoid $\mathcal{Q}_n = (Q_n; \circ)$ with the carrier set Q_n consisting of all n-tuples $(k_1, \ldots, k_n)$ from $\mathbb{Z}^n$ such that at most one k_i is odd. Then the free groupoid on $n+1$ free generators $\mathcal{F}(n+1) = \mathcal{F}_{\underline{SIE}}(\{x_0, x_1, \ldots, x_n\})$ is isomorphic to $\mathcal{Q}_n = (Q_n; \circ)$ with free generators $(0, \ldots 0)$, $(1, 0, \ldots, 0), \ldots$, and $(0, \ldots, 0, 1)$.

Proposition 4.1. *The variety $\underline{SIE}$ is generated by cores of commutative groups.*

Proof. The statement can be proved directly from the results of D. Joyce. Since the free groupoid on n elements $\mathcal{F}(n)$ is (up to isomorphism) a subgroupoid $\mathcal{Q}_{n-1}$ of $Core(\mathbb{Z}^{n-1}; +) \in \underline{CAG} \subset \underline{SIE}$, and $\underline{SIE} = HSP(\{\mathcal{F}_{\underline{SIE}}(n) \,|\, n \in \mathbb{N}\})$ (e.g. [7, Satz 6.3.16, p. 93])[3] the assertion follows. □

Of course, commutative groups are not the only quasigroups with medial cores. In [21, Ex. 1.6, p. 4] the following is suggested.

Proposition 4.2. *A core $Core(\mathcal{G})$ of a group $\mathcal{G} = (G, \cdot, ^{-1}, e)$ (non-commutative in general) is medial if and only if $\mathcal{G}$ is nilpotent of class at most two*[4] *.*

Proof. Mediality (E) for group cores takes the form

$$xy^{-1}xz^{-1}uz^{-1}xy^{-1}x = xz^{-1}xy^{-1}uy^{-1}xz^{-1}x$$

which is equivalent (due to left and right cancellation in $\underline{G}$) with the condition

$$xyzuzyx = zyxuxyz \qquad \text{for all} \qquad x, y, z, u \in G. \tag{4.1}$$

Let $Core(\mathcal{G})$ of a group $\mathcal{G}$ be medial. Let us set $z = e$ in (4.1), and use $xy = yx \cdot [x, y]$ where $[x, y] = x^{-1}y^{-1}xy$ denotes the commutator. Then $yx[x, y]uyx = yxuyx[x, y]$ holds for $x, y, u \in G$. Further by cancellation, $[x, y]uyx = uyx[x, y]$. The last condition is equivalent with the condition $[x, y]g = g[x, y]$ for all $g \in G$ (if $g \in G$ is given the corresponding u takes the form $u = gx^{-1}y^{-1}$), which is satisfied iff $[x, y] \in Z(G)$. Hence nilpotency of class at most two is a necessary condition for a group to have medial core.

Vice versa, let $\mathcal{G}$ be a nilpotent group of class at most two, that is, all commutators $[a, b]$ for $a, b \in G$ are in the center $Z(\mathcal{G})$ of $\mathcal{G}$. Using commutators we can write $xyz = xzy[y, z] = zyx[x, zy][y, z]$ and similarly for zyx. Now (4.1) holds if and only if

$$zyx[x, y][xy, z]uxyz[z, xy][y, x] = zyxuxyz \tag{4.2}$$

[3] Here P denotes forming of products, S means taking of subalgebras, and H means homomorphic images.

[4] In a group $\mathcal{G}$, its centre $Z(\mathcal{G})$ is a normal subgroup, we have the canonical projection $p : \mathcal{G} \to \mathcal{G}/Z(\mathcal{G})$, and the inverse image $C_2(\mathcal{G}) = p^{-1}(Z(\mathcal{G}/Z(\mathcal{G})))$ of $Z(\mathcal{G}/Z(\mathcal{G}))$ in $\mathcal{G}$. A group is called *nilpotent of class at most two* if $C_2(\mathcal{G}) = \mathcal{G}$. A necessary and sufficient condition is that for any pair of elements of the group, the commutator belongs to the center $Z(\mathcal{G})$.

is satisfied for all $x, y, z, u \in G$. But we easily check that $[x, y][xy, z][z, xy][y, x] = e$ is valid in G. So if all commutators are in the center of the group then the condition (4.2) is satisfied, and consequently $\mathcal{G}$ has a medial core. $\square$

4.2 Remarks on normal forms for terms in $\underline{SIE}$. Every term of the free algebra $\mathcal{F}_{\underline{SIE}}(X)$, $X \neq \emptyset$ is equivalent (in the variety $\underline{SIE}$) to a term of the form

$$w = x_n x_{n-1} \dots x_2 x_1 \qquad x_{i+1} \neq x_i, \quad i = 1, \dots, n-1, \quad x_1, \dots, x_n \in X \tag{4.3}$$

where each variable on an odd position (from the left) is different from all variables on even positions, i.e. $\{x_n, x_{n-2}, \dots\} \cap \{x_{n-1}, x_{n-3}, \dots\} = \emptyset$. The prove is based on Lemma 3.1 and Lemma 3.2. Indeed, if two variables are equal, one of them on an odd position and the other on an even one, we can use a suitable transposition so that equal variables stand on neighbour positions, and then we can use either (S_l) or (I), respectively, to reduce the term.

An infinitely countable set Z generates a $\underline{SIE}$-subgroupoid $\mathcal{Z}'$ in the core of a free abelian group $Core(\mathcal{F}_{\underline{AG}}(Z))$, and it can be checked that the formula (3.4) holds in $Core(\mathcal{F}_{\underline{AG}}(Z))$ for $n \geq 2$. The last term from (3.4) can be reduced if and only if some variable on an odd position (from the left) is equal to some variable on an even position, e.g. $z_1 \circ z_3 \circ z_2 \circ z_1 = z_2 \circ z_3 \circ z_1$ since $z_1^2 z_3^{-2} z_2^2 z_1^{-1} = z_2^2 z_3^{-2} z_2^2 z_1^1$. Therefore different terms w, w' of the form (4.3) give different term functions $w^{\mathcal{Z}'}$, ${w'}^{\mathcal{Z}'}$ of the groupoid $\mathcal{Z}'$.

Normal forms for terms over X in $\underline{SIE}$ can be now constructed as follows. Choose a linear order on X, $(X, \leq)$. Let us rearrange the variables in the term $w = x_n x_{n-1} \dots x_2 x_1$ of the form (4.3) in such a way that the resulting term denoted by $Nf(w)$ satisfies $x_n \leq x_{n-2} \leq \dots$ and $x_{n-1} \leq x_{n-3} \leq \dots$ (naturally also $\{x_n, x_{n-2}, \dots\} \cap \{x_{n-1}, x_{n-3}, \dots\} = \emptyset$). Then $Nf(w)$ can be called a *normal form* of w with respect to $\underline{SIE}$.

Again, we can introduce a mapping $\mathcal{L}' : \mathcal{F}_{\underline{SIE}}(Z) \to \mathcal{Z}'$ similarly as above[5]. For any equivalence class $[w]$, $w \in T_{(2)}(Z)$, with $Nf(w) = z_1 z_2 \dots z_{n-1} z_n$ define $\mathcal{L}'([w]) := z_1 \circ z_2 \circ \dots \circ z_{n-1} \circ z_n$. It can be easily seen that $\mathcal{L}'$ is a surjective homomorphism. Different terms over Z in normal form (i.e. representatives of two distinct classes from the free algebra $\mathcal{F}_{\underline{SIE}}(Z)$) obviously yield different elements of the groupoid $\mathcal{Z}' \in \underline{AGC}$. Therefore $\mathcal{L}'$ is also injective, and the groupoids $\mathcal{F}_{\underline{SIE}}(Z)$, $\mathcal{Z}'$ are isomorphic, particularly, $\mathcal{Z}'$ is free infinitely generated in $\underline{SIE}$. Hence we obtain another proof of the fact that the varieties $\underline{CAG}$ and $\underline{SIE}$ coincide (Proposition 4.1).

Lemma 4.1. *In the variety $\underline{SIE}$ the following identities are satisfied:*

$$u(z(yx)) = y(z(ux)), \tag{4.5}$$

$$y_n x_n \dots y_1 x_1 = y_{\sigma(n)} x_n \dots y_{\sigma(1)} x_1, \quad \sigma \in S_n, \tag{4.6}$$

$$x_n y_{n-1} x_{n-1} \dots x_2 y_1 x_1 = x_{\sigma(n)} y_{n-1} x_{\sigma(n-1)} \dots x_{\sigma(2)} y_1 x_1 \tag{4.7}$$

[5] Note that the equivalence classes of terms are now different, coarser.

where $\sigma \in S_n$ *is a permutation such that* $\sigma(1) = 1$. *Moreover, the identities* (4.5) *and* (E) *are equivalent in the variety* $\underline{SID}$.

Proof. By (D_l), (E) and (S_l), $u(z(yx)) = (uz)((uy)(ux)) = (u(uy))(z(ux)) = y(z(ux))$, and (4.5) holds. Since every permutation can be composed from transpositions, (4.6) follows from (4.5). If we take (y_1x_1) instead of x_1, y_i instead of x_i for $i = 2, \dots, n-1$, and x_{i+1} instead of y_i for $i = 1, \dots, n-1$ we get $x_n y_{n-1} x_{n-1} \dots y_2 x_2 (y_1 x_1) = x_{\sigma(n)} y_{n-1} x_{\sigma(n-1)} \dots y_2 x_{\sigma(2)} (y_1 x_1)$, i.e. (4.7) holds. Finally, $(xy)(zu) = x[y(x(zu))]$ holds in $\underline{SID}$, and using (4.5) we can rewrite the last term as $x[z(x(yu))] = (xz)(yu)$. □

Hence $Mod(\{(S_l), (D_l), (I), (4.5)\}) = Mod(\{(S_l), (I), (E)\})$.

4.3 Mediality of Bol loop cores. Finally, let us express mediality of a core for a Bol loop.

Lemma 4.3. *A core* $Core(\mathcal{B})$ *of a Bol loop* $\mathcal{B} = (B, \cdot, ^{-1}, e) \in \underline{B}$ *is medial if and only if the following identity holds in* $\mathcal{B}$*:*

$$y(x(z(u(z(xy))))) = z(x(y(u(y(xz))))). \tag{4.8}$$

Proof. For Bol loop cores, mediality $(x \circ y) \circ (z \circ u) = (x \circ z) \circ (y \circ u)$ takes the form $(x(y^{-1}x)) \cdot ((z \circ u)^{-1} \cdot (x \circ y)) = (x(z^{-1}x)) \cdot ((y \circ u)^{-1} \cdot (x \circ z))$ or equivalently, using (B_l), $x(y^{-1}(x(z \circ u)^{-1} \cdot (x \circ y)))) = x(z^{-1}(x(y \circ u)^{-1} \cdot (x \circ z))))$ for x, y, z, u from B. Let us write y, z instead of y^{-1}, z^{-1}, and use left cancellation. Then our condition is equivalent with $y(x((z \circ u^{-1}) \cdot (x(yx)))) = z(x((y \circ u^{-1}) \cdot (x(zx))))$ for all $x, y, z, u \in B$. Using (B_l) again we can write the formula as $(y((x((z \circ u^{-1}) \cdot x)) \cdot y)) \cdot x = (z((x((y \circ u^{-1}) \cdot x)) \cdot z)) \cdot x$ or, using right cancellation, in a simplified form $y((x((z(uz)) \cdot x)) \cdot y) = z((x((y(uy)) \cdot x)) \cdot z)$. Now using left Bol identity (B_l) twice we obtain that mediality holds in a Bol loop core if and only if the condition $y(x(z(u(z(xy))))) = z(x(y(u(y(xz))))$ is satisfied for all $x, y, z, u \in B$. □

Open problem 1: Is it possible to formulate mediality condition for Bol (Moufang, or commutative Moufang, respectively) loop cores similarly as in Proposition 4.1?

Open problem 2: Describe an equational theory for the variety generated by cores of commutative Moufang loops. Is the variety generated by cores of $\underline{CML}$ a proper subvariety of $\underline{SID}$?

References

[1] Arworn Sr., Denecke K. *Hyperidentities and hypersubstitutions in the variety of symmetric, idempotent, entropic groupoids.* Dem. Math., 1999, **XXXII**, N 4, p. 677–686.

[2] Belousov V.D. *Foundations of the theory of quasigroups and loops.* Moscow, Nauka, 1967.

[3] Bruck R.H. *A Survey of Binary Systems.* Berlin, Springer, 1958.

[4] Burn R.P. *Finite Bol loops.* Math. Proc. Cambridge Philos. Soc., 1978, **84**, p. 377–385.

[5] Denecke K., Wismath Sh.L. *Universal Algebra and Applications in Theoretical Computer Science*. Chapman and Hall/CRC, Boca Raton-London-New York-Washington D.C., 2002.

[6] Grätzer G. *Universal Algebra*. Van Nostrand Co., Princeton–New Yersey, 1968.

[7] Ihringer Th. *Allgemeine Algebra*. Teubner, Stuttgart, 1988.

[8] Jeřábek E., Kepka T., Stanovský D. *Non-idempotent left symmetric left distributive groupoids*. Preprint.

[9] Joyce D. *Aclassifying invariant of knots, the knot quandle*. Jour. of Pure and Appl. Alg., 1982, **23**, p. 37–65.

[10] Kinyon M.K. *Global left loop structures o spheres*. Comment. Math. Univ. Carolinae, 2000, **41**, N 2, p. 325–346.

[11] sc Lindner C.C., Mendelsohn N.S. *Constructions of n-cyclic quasigroups and applications*. Aequat. Math., 1976, **14**, p. 111–121.

[12] 2 Loos O. *Symmetric Spaces*. J. Benjamin, New York, 1969.

[13] Nagy P.T., Strambach K. *Loops, their cores and symmetric spaces*. Israel Jour. of Math., 1998, **105**, p. 285–322.

[14] Nagy P.T., Strambach K. *Loops in Group Theory and Lie Theory*. De Gruyter, Berlin–New York, 2002.

[15] Nobusawa N. *On symmetric structures of a finite set*. Osaka J. Math., 1974, **11**, p. 569–575.

[16] Nobusawa N. *Simple symmetric sets and simple groups*. Osaka J. Math., 1977, **14**, p. 411–415.

[17] Pflugfelder H.O. *Quasigroups and Loops, Introduction*. Heldermann Verlag, Berlin, 1990.

[18] Pierce R.S. *Symmetric Groupoids*. Osaka J. Math., 1978, **15**, p. 51–76.

[19] Pierce R.S. *Symmetric Groupoids II*. Osaka J. Math., 1979, **16**, p. 317–348.

[20] Romanowska A., Smith J.D.H. *Modal Theory, An Algebraic Approach to Order, Geometry, and Convexity*. Berlin, Heldermann Verlag, 1985.

[21] Roszkowska B. *The lattice of varieties of symmetric idempotent entropic groupoids*. Demonstratio Math., 1987, **XX**, N 1-2, p. 259–275.

[22] Roszkowska B. *On some varieties of symmetric idempotent entropic groupoids*. Universal and Applied Algebra (eds. K. Hałkowska, B. Stawski), World Scientific, 1989, p. 254–274.

[23] Roszkowska-Lech B. *A representation of symmetric idempotent and entropic groupoids*. Demonstratio Math., 1999, **XXXII**, N 2, p. 247–262.

[24] Roszkowska-Lech B. *Subdirectly irreducible symmetric idempotent and entropic groupoids*. Demonstratio Math., 1999, **XXXII**, N 3, p. 469–484.

[25] Smith J.D.H. *Modes and modals*. Discussiones Math., Algebra and Stochastic Methods, 1999, **19**, p. 9–40.

[26] Stanovský D. *Left distributive groupoids*. Diploma Thesis, Charles Univ. Prague.

[27] Stanovský D. *Left symmetric left distributive operations on a group*. Preprint.

[28] Takasaki M. *Abstractions of symmetric functions*. Tôhoku Math. J., 1943, **49**, p. 147–207.

[29] Vanžurová A. *Normal form hypersubstitutions with respect to the variety of left symmetric left distributive idempotent groupoids*. Contributions in General Algebra, 2004, **14**, p. 173–187.

Faculty Sciences
Department Algebra and Geometry
Palacký University
Tomkova 40, 779 00 Olomouc
Czech Republic
E-mail: *vanzurov@inf.upol.cz*

Received August 11, 2005