Elements of quasigroup theory and some its applications in code theory and cryptology

Victor Shcherbacov

1 Introduction

1.1 The role of definitions.

This course is an extended form of lectures which author have given for graduate students of Charles University (Prague, Czech Republic) in autumn of year 2003.

In this section we follow books [56, 59].

In mathematics one should strive to avoid ambiguity. A very important ingredient of mathematical creativity is the ability to formulate useful definitions, ones that will lead to interesting results.

Every definition is understood to be an if and only if type of statement, even though it is customary to suppress the only if. Thus one may define: "A triangle is isosceles if it has two sides of equal length", really meaning that a triangle is isosceles if and only if it has two sides of equal length.

The basic importance of definitions to mathematics is also a structural weakness for the reason that not every concept used can be defined.

1.2 Sets.

A set is well-defined collection of objects. We summarize briefly some of the things we shall simply assume about sets.

1. A set S is made up of elements, and if a is one of these elements, we shall denote this fact by $a \in S$.

2. There is exactly one set with no elements. It is the empty set and is denoted by $\varnothing$.

3. We may describe a set either by giving a characterizing property of the elements, such as "the set of all members of the United State Senate", or by listing the elements, for example $\{1, 3, 4\}$.

4. A set is well defined, meaning that if S is a set and a is some object, then either a is definitely in S, denoted by $a \in S$, or a is definitely not in S, denoted by $a \notin S$. Thus one should never say "Consider the set S some positive numbers", for it is not definite whether $2 \in S$ or $2 \notin S$.

1.3 Partitions and equivalence relations.

Definition. A partition of set is a decomposition of the set into cells such

that every element of the set is in exactly one of the cells. Two cells (or sets) having no elements in common are disjoint. Let $a \sim b$ denote that a is is in the same cell as b for a given partition of a set containing both a and b. Clearly the following properties are always satisfied: $a \sim a$; if $a \sim b$, then $b \sim a$; if $a \sim b$ and $b \sim c$, then $a \sim c$, i.e. if a is in the same cell as b and b is in the same cell as c, then a is in the same cell as c.

Theorem. Let S be a nonempty set and let $\sim$ be a relation between elements of S that satisfies the following properties:

1. (Reflexive) $a \sim a$ for all $a \in S$.
2. (Symmetric) If $a \sim b$, then $b \sim a$.
3. (Transitive) If $a \sim b$ and $b \sim c$, then $a \sim c$.

Then $\sim$ yields a natural partition of S, where $\bar{a} = \{x \in S \,|\, x \sim a\}$ is the cell containing a for all $a \in S$. Conversely, each partition of S gives rise to a natural relation $\sim$ satisfying the reflexive, symmetric, and transitive properties if $a \sim b$ is defined to mean that $a \in \bar{b}$.

Definition. A relation $\sim$ on a set S satisfying the reflexive, symmetric, and transitive properties is an equivalence relation on S. Each cell $\bar{a}$ in the natural partition given by an equivalence relation is an equivalence class.

Definition. The Cartesian product of sets $S_1, S_2, \ldots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in S_i$. The Cartesian product is denoted by either $S_1 \times S_2 \times \cdots \times S_n$ or by $\prod_{i=1}^{n} S_i$. If $S_1 = S_2 = \cdots = S_n = S$, then we have $S \times S \times \cdots \times S = S^n = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in S\}$ (the n-th power of the set S).

1.4 Maps.

One of the truly universal concepts that runs through almost every phase of mathematics is that of a function or mapping from one set to another. One could safely say that there is no part of mathematics where the notion does not arise or play a central role. The definition of a function from one set to another can be given in a formal way in terms of a subset of the Cartesian product of these sets. Instead, here, we shall give an informal and admittedly nonrigorous definition of a mapping (function) from one set to another.

Let S, T be sets; function or mapping f from S to T is a rule that assigns to each element $s \in S$ unique element $t \in T$.

Definition. The mapping $f : S \to T$ is onto or surjective if every $t \in T$ is the image under f of some $s \in S$; that is, if and only if, given $t \in T$, there

exists an $s \in S$ such that $t = f(s)$.

Definition. A mapping $f : S \to T$ is said to be one-to-one (written 1-1) or injective if for $s_1 \neq s_2$ in S, $f(s_1) \neq f(s_2)$ in T. Equivalently, f is 1-1 if $f(s_1) = f(s_2)$ implies $s_1 = s_2$.

Definition. A mapping $f : S \to T$ is said to be 1-1 correspondence or bijection if f is both 1-1 and onto (i.e. f is injective and surjective map).

We shall consider the set $A(S)$ all bijections of S onto itself. When S has finite number of elements, say n, then $A(S)$ has a special name. It is called the symmetric group of degree n and it will be denoted as S_n. Its elements are called permutations of S. In the investigation of finite groups and quasigroups, S_n plays a central role.

A sequence $x_m, x_{m+1}, \ldots, x_n$, where m, n are natural numbers and $m \leq n$, will be denoted by x_m^n, a sequence $x, \ldots, x$ (k times) will be denoted by $\overline{x}^k$. The expression $\overline{1,n}$ designates a set $\{1, 2, \ldots, n\}$ of natural numbers [14].

An n-ary operation defined on a non-empty set Q is a map $A : Q^n \longrightarrow Q$ such that $D(A) = Q^n$, i.e. this map is defined for any n-tuple. The number n is called arity of operation A. If the element c corresponds to the n-tuple $(b_1, b_2, \ldots, b_n)$, then we shall write this fact in the following form $A(b_1, b_2, \ldots, b_n) = c$, or in the form $A : (b_1, b_2, \ldots, b_n) \longmapsto c$.

If $n = 2$, then the operation A is called a binary operation, if $n = 1$, then the operation A is called unary operation, if $n = 0$, then the operation A is called nul-ary operation ($\forall a \in Q\ A(a) = e$, where e is a fixed element of the set Q).

2 Objects

2.1 Groupoids and quasigroups.

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

Often one uses different symbols to denote a binary operation, for example, $\circ, \star, \cdot$, i.e. we may write $x \circ y$ instead $A(x, y)$.

An n-ary groupoid (G, A) is understood to be a non-empty set G together with an n-ary operation A.

There exists a bijection (1-1 correspondence) between the set of all binary (n-ary, arity is fixed) operations defined on a set Q and the set of all

groupoids, defined on the set Q. Really, $A \longleftrightarrow (Q, A)$.

As usual $a_1^n = (a_1, a_2, \ldots, a_n)$, $\overline{1,n} = \{1, 2, \ldots, n\}$. We shall say that operations A and B coincide, if $A(a_1^n) = B(a_1^n)$ for all $a_i \in Q$, $i \in \overline{1,n}$.

The order of n-ary groupoid (Q, A) is cardinality $|Q|$ ($\bar{\bar{Q}}$) of the carrier set Q. An n-ary groupoid $(Q, \cdot)$ is said to be finite whenever its order is finite.

Any finite n-ary groupoid (not a very big size) (Q, A) it is possible to define as a set of $(n+1)$-tuples $(a_1, a_2, \ldots, a_n, A(a_1^n))$. In binary case any finite binary groupoid it is possible to define as a set of triplets or with help of square table, for example, as:

$\cdot$	a	b	c
a	a	a	b
b	b	c	a
c	c	a	b

where $a \cdot c = b$. This table is called Cayley table of groupoid $(Q, \cdot)$, where $Q = \{a, b, c\}$.

Note. Usually it is supposed that elements of carried set Q are arranged. So the groupoid $(Q, \circ)$ defined with help of the following Cayley table

$\circ$	b	c	a
b	c	a	b
c	a	b	c
a	a	b	a

is equal (as set of triplets) to the groupoid $(Q, \cdot)$, but $(Q, \cdot) \neq (Q, *)$, where groupoid $(Q, *)$ has the following Cayley table:

$*$	b	c	a
b	a	a	b
c	b	c	a
a	c	a	b

.

Definition 1. An n-ary groupoid (Q, A) with n-ary operation A such that in the equality $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ knowledge of any n elements of $x_1, x_2, \ldots, x_n, x_{n+1}$ uniquely specifies the remaining one is called n-ary quasigroup ([14]).

In binary case this definition is equivalent to the following:

Definition 2. Binary groupoid $(Q, \circ)$ is called a quasigroup if for all ordered pairs $(a, b) \in Q^2$ there exist unique solutions $x, y \in Q$ to the equations $x \circ a = b$ and $a \circ y = b$ ([12]).

Let $(G, \cdot)$ be a groupoid and let a be a fixed element in G. The so-called translation maps L_a and R_a can be defined by $L_a x = a \cdot x$, $R_a x = x \cdot a$ for all $x \in G$. It follows that $L_a : G \longrightarrow G$ and $R_a : G \longrightarrow G$ for each $a \in G$. These maps will play a prominent role in much of what we do.

Example of quasigroup and its left and right translations.

$\cdot$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

For this quasigroup we have the following left and right translations: $L_a = (bc); L_b = (ac); L_c = (ab); R_a = (bc); R_b = (ac); R_c = (ab)$.

It is easy to see that in Cayley table of a quasigroup $(Q, \cdot)$ each row and each column is a permutation of the set Q. So we may give the following definition of a quasigroup.

Definition 3. A groupoid $(G, \cdot)$ is called a quasigroup if the maps $L_a : G \longrightarrow G$, $R_a : G \longrightarrow G$ are bijections for all $a \in G$ ([95]).

Note. Condition "the equation $x \circ a = b$ has unique solution for all $a, b \in Q$" and "R_a is bijection of the set G for any $a \in G$" are equivalent. Similarly, are equivalent conditions "the equation $a \circ y = b$ has unique solution for all $a, b \in Q$" and "L_a is bijection of the set G for any $a \in G$".

Really, if we fix the element a, we see that for any element $b \in Q$ there exist unique elements $x, y \in Q$ such that $R_a^\circ x = b$ and $L_a^\circ y = b$, i.e. translations R_a°, L_a° are bijections. If translations R_a° and L_a° are bijections, then $x = (R_a^\circ)^{-1} b$, $y = (L_a^\circ)^{-1} b$.

Note. An unbordered Cayley table of a quasigroup is a Latin square.

A groupoid $(Q, \circ)$ is called a *right quasigroup* if, for all $a, b \in Q$, there exists a unique solution $x \in Q$ to the equation $x \circ a = b$, i.e. in this case any right translation of the groupoid $(Q, \circ)$ is a permutation of the set Q.

A groupoid $(Q, \circ)$ is called a *left quasigroup* if, for all $a, b \in Q$, there exists unique solution $y \in Q$ to the equation $a \circ y = b$, i.e. in this case any left translation of the groupoid $(Q, \circ)$ is a permutation of the set Q.

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

2.2 Parastrophy. Quasigroup as algebra with three binary operations.

From Definition 1 it follows that in binary case with any quasigroup (Q, A) it possible to associate else $(3! - 1) = 5$ quasigroups, so-called parastrophes of quasigroup (Q, A): $A(x_1, x_2) = x_3 \Leftrightarrow A^{(12)}(x_2, x_1) = x_3 \Leftrightarrow A^{(13)}(x_3, x_2) = x_1 \Leftrightarrow A^{(23)}(x_1, x_3) = x_2 \Leftrightarrow A^{(123)}(x_2, x_3) = x_1 \Leftrightarrow A^{(132)}(x_3, x_1) = x_2$.

In other words

$$A^{\sigma}(x_{\sigma 1}, x_{\sigma 2}) = x_{\sigma 3} \Leftrightarrow A(x_1, x_2) = x_3,$$

where $\sigma \in S_3$. For example, $A^{(132)}(x_3, x_1) = x_2 \Leftrightarrow A(x_1, x_2) = x_3$: that is,

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

Usually the operation ${}^{(12)}A$ is denoted as " $*$ ", the operation ${}^{(13)}A$ is denoted as "/", the operation ${}^{(23)}A$ is denoted as "\".

Note. Notion of parastrophy has sense and for groupoids. Now we give a theorem on parastrophes of groupoids without a proof. We hope, below we will be able to prove more general theorem.

Theorem. *(1) If* $(1\,3)$*-parastrophe of a groupoid* (Q, A) *is a groupoid, then* (Q, A) *is a right quasigroup.*

(2) If $(2\,3)$*-parastrophe of a groupoid* (Q, A) *is a groupoid, then* (Q, A) *is a left quasigroup.*

(3) If $(1\,2\,3)$*-parastrophe of a groupoid* (Q, A) *is a groupoid, then* (Q, A) *is a quasigroup.*

(4) If $(1\,3\,2)$*-parastrophe of a groupoid* (Q, A) *is a groupoid, then* (Q, A) *is a quasigroup.*

(5) If $(1\,2)$*-parastrophe of a left quasigroup* (Q, A) *is a groupoid, then* (Q, A) *is a quasigroup.*

(6) If $(1\,2)$*-parastrophe of a right quasigroup* (Q, A) *is a groupoid, then* (Q, A) *is a quasigroup.*

(7) If $(2\,3)$*-parastrophe of a right quasigroup* (Q, A) *is a groupoid, then* (Q, A) *is a quasigroup.*

(8) If $(2\,3)$*-parastrophe of a left quasigroup* (Q, A) *is a groupoid, then* (Q, A) *is a quasigroup.*

It was happened that class of quasigroups in signature with one binary operation is not closed relatively homomorphic images, i.e. homomorphic image of a quasigroup can be only division groupoid, but not a quasigroup [9]. Below we give some definitions in order to make situation more clear.

Definition. A groupoid $(G, \cdot)$ is called left cancellation, if the following implication fulfilled: $a \cdot x = a \cdot y \Rightarrow x = y$ for all $a, x, y \in G$, i.e. translation L_a is injective map for any $a \in G$.

A groupoid $(G, \cdot)$ is called right cancellation, if the following implication fulfilled: $x \cdot a = y \cdot a \Rightarrow x = y$ for all $a, x, y \in G$, i.e. translation R_a is injective map for any $a \in G$ ([62]).

A groupoid $(G, \cdot)$ is called cancellation, if it is left and right cancellation.

EXAMPLE. Let $x \circ y = 2x + 3y$ for all $x, y \in Z$, where $(Z, +, \cdot)$ is ring of integers. It is possible to check that $(Z, \circ)$ is cancellation groupoid.

A groupoid $(G, \cdot)$ is said to be a left (right, resp.) division groupoid if L_a (R_a, resp.) is surjective for every $a \in G$; it said to be division groupoid if it is a left and right division groupoid ([62]).

We can give equivalent definition of division groupoid.

Definition. A groupoid $(G, \cdot)$ is called division groupoid, if equations $a \cdot x = b$ and $y \cdot a = b$ have solutions (not necessary unique solutions) for any ordered pair of elements $a, b \in Q$.

EXAMPLE. Let $x \circ y = x^2 \cdot y^3$ for all $x, y \in \mathbb{C}$, where $(\mathbb{C}, +, \cdot)$ is field of complex numbers. It is possible to check that $(\mathbb{C}, \circ)$ is a division n groupoid.

Theorem. *Finite cancellation groupoid is a quasigroup, finite division groupoid is a quasigroup.*

Proof. We remember well known fact that, if Q is a finite set, then any injective ($x \neq y \Rightarrow \varphi x \neq \varphi y$) map φ on this set ($\varphi(Q) \subseteq Q$) is a bijective map, any surjective map ψ of this set into itself ($\psi(Q) = Q$) is a bijective map, too.

Since any left and right translation of a cancellation groupoid $(G, \cdot)$ is an injective map, then in case when the set G is finite, we have that $(G, \cdot)$ is a quasigroup.

Similarly, since any left and right translation of division groupoid $(G, \cdot)$ is a surjective map, then in case, when the set G is finite, we have that any division groupoid is a quasigroup.

It is true the following

Theorem. *Any homomorphic image of a quasigroup* $(Q, \cdot)$ *is a division groupoid.*

We hope, we will be able to prove this theorem below.

Problem. Number N of all binary quasigroups of order n is more than $n!(n-1)!(n-2)!\ldots 2!1!$ (i.e. this is lower bound of number N) ([34]). To find exact formula for number of all binary (m-ary, $m \geq 3$) quasigroups of a fixed finite order n.

Definition 4. A groupoid $(Q, \cdot)$ is called a quasigroup, if on the set Q there exist operations "$\backslash$" and "$/$" such that in algebra $(Q, \cdot, \backslash, /)$ the following identities are fulfilled:

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

$$(y/x) \cdot x = y, \tag{2}$$

$$x\backslash(x \cdot y) = y, \tag{3}$$

$$(y \cdot x)/x = y. \tag{4}$$

Note. Identities (1) and (2) provide existence of solutions of equations $x \cdot a = b$ and $a \cdot y = b$, identities (3) and (4) provide uniqueness of solutions in these equations. See below.

Prove equivalence Definitions 2 and 4.

(Definition 2 $\Rightarrow$ Definition 4). Let $(Q, \cdot)$ be a quasigroup. Since for every pair of elements $a, b \in Q$ there exists an unique element x such that $a \cdot x = b$, we can associate with this equation an operation on the set Q, namely $a \cdot x = b \leftrightarrow a\backslash b = x$. If we substitute the last expression in equality $a \cdot x = b$, then we obtain $a \cdot (a\backslash b) = b$ for all $a, b \in Q$. We received identity (1) from Definition 4.

Similarly, $y \cdot a = b \leftrightarrow b/a = y$, $(b/a) \cdot a = b$ for all $a, b \in Q$ and we obtain identity (2).

Identities (3) and (4) follow from definitions of operations $\backslash$ and $/$. Really, $x\backslash(x \cdot y) = y \leftrightarrow x \cdot y = x \cdot y$, $(y \cdot x)/x = y \leftrightarrow y \cdot x = y \cdot x$.

(Definition 4 $\Rightarrow$ Definition 2). Let $(Q, \cdot, /, \backslash)$ be an algebra with three binary operations such that in this algebra identities (1), (2), (3) and (4) hold.

We need to prove the existence and the uniqueness of solutions of equations $a \cdot x = b$ and $y \cdot a = b$.

(Existence). Let $x = a\backslash b$. Then $a \cdot x = a(a\backslash b) \overset{(1)}{=} b$. Similarly, if $y = b/a$, then $y \cdot a = (b/a) \cdot a \overset{(2)}{=} b$.

(Uniqueness). Suppose that there exist two solutions x_1 and x_2 of equation $a \cdot x = b$, i.e. $a \cdot x_1 = b$ and $a \cdot x_2 = b$. Then $x_1 = a\backslash b$ and further we have

$$x_1 = a\backslash b = a\backslash(ax_2) \overset{(3)}{=} x_2.$$

Similarly, if $y_1 \cdot a = b$ and $y_2 \cdot a = b$, then $y_1 = b/a$,

$$y_1 = b/a = (y_2 \cdot a)/a \overset{(4)}{=} y_2.$$

Note. Often Definition 4 it is used by study word problems, free objects in Quasigroup Theory.

It is possible to rewrite identities (1)-(4) on language of translations in the following form:

$$\begin{array}{llll} L_x^{(\cdot)} L_x^{(\backslash)} y = y & (1)^\star & R_x^{(\cdot)} R_x^{(/)} y = y & (2)^\star \\ L_x^{(\backslash)} L_x^{(\cdot)} y = y & (3)^\star & R_x^{(/)} R_x^{(\cdot)} y = y & (4)^\star \end{array}$$

We defined left and right translations of a groupoid and, therefore, of a quasigroup. But for quasigroups it is possible to define and the third kind of translations, namely $P_a : x \longmapsto P_a(x)$, and $x \cdot P_a x = a$ ([16]).

In the following table there are connections between different kinds of translations in different parastrophes of a quasigroup $(Q, \cdot)$.

Table 1.

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

Thus, in Table 1, for example, $R^{(23)} = P^{(\cdot)}$.

Exercise. To prove that following identities hold in algebra $(Q, \cdot, \backslash, /)$:

$$x/(y\backslash x) = y, \tag{5}$$

$$(x/y)\backslash x = y, \tag{6}$$

or, equivalently, $L_x^{(/)} R_x^{(\backslash)} y = y, R_x^{(\backslash)} L_x^{(/)} y = y$.

Solving. From Table 1 it follows that $L_x^{(/)} = P_x^{-1}$, $R_x^{(\backslash)} = P_x$.

We recall, we use the following order by multiplication of permutations: $(\alpha\beta)x = \alpha(\beta x)$, where α, β are permutations of the set Q, $x \in Q$.

Remark. Equalities $(1)^\star - (4)^\star$ help to construct Cayley tables of quasigroups $(Q, \backslash)$ and $(Q, /)$. From $(1)^\star$ we have $L_x^{(\backslash)} y = (L_x^{(\cdot)})^{-1} y$, from $(2)^\star$ we have $R_x^{(/)} y = (R_x^{(\cdot)})^{-1} y$

Problem. Research properties of algebra $(Q, \cdot, /, \backslash)$ with various combinations of identities (1)-(6).

2.3 Ochadkova-Snasel binary quasigroup based cryptosystem.

Eliska Ochodkova and Vaclav Snasel ([92]) proposed to use quasigroups for secure encoding of file system.

A quasigroup $(Q, \cdot)$ and its (23)-parastroph $(Q, \backslash)$ satisfy the following identities $x\backslash(x \cdot y) = y$, $x \cdot (x\backslash y) = y$ (identities (1) and (3)). The authors propose to use this property of the quasigroups to construct a stream cipher.

Definition. Let A be a non-empty alphabet, k be a natural number, $u_i, v_i \in A$, $i \in \{1, ..., k\}$. A fixed element l ($l \in A$) is called leader. Then $f(u_1 u_2 ... u_k) = v_1 v_2 ... v_k \Leftrightarrow v_1 = l \cdot u_1, v_{i+1} = v_i \cdot u_{i+1}, i = 1, 2, ..., k-1$ is an ciphering algorithm.

An enciphering algorithm is constructed in the following way:

$$f^{(\backslash)}(v_1 v_2 ... v_k) = u_1 u_2 ... v_k \Leftrightarrow u_1 = l\backslash v_1, u_{i+1} = v_i \backslash v_{i+1}, i = 1, 2, ..., k-1.$$

Authors say that this cipher is resist to the brute force attack and to the statistical attack.

Example.

Table 1. Let quasigroups $(A, \cdot)$ and $(A, \backslash)$ are defined by following Cayley tables

$\cdot$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

$\setminus$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

Let $l = a$ and $u = b\,b\,c\,a\,a\,c\,b\,a$. Then the cipher text is $v = c\,b\,b\,c\,a\,a\,c\,a$. Applying of decoding function on v we get $b\,b\,c\,a\,a\,c\,b\,a = u$.

Remark. There exists a sense to study possibilities of use an n-ary quasigroup and its parastrophes in Ochodkova-Snasel construction.

2.4 Identity elements

Definition. An element $f(b)$ of a quasigroup $(Q, \cdot)$ is called left local identity element of an element $b \in Q$, if $f(b) \cdot b = b$, in other words, $f(b) = b/b$, or $f(b) = R_b^{-1}b$.

An element $e(b)$ of a quasigroup $(Q, \cdot)$ is called right local identity element of an element $b \in Q$, if $b \cdot e(b) = b$, in other words, $e(b) = b\backslash b$, or $e(b) = L_b^{-1}b$.

An element e is a left (right) identity element for quasigroup $(Q, \cdot)$ means that $e = f(x)$ for all $x \in Q$ (respectively, $e = e(x)$ for all $x \in Q$).

An element e is identity element for a quasigroup $(Q, \cdot)$ means that $e(x) = f(x) = e$ for all $x \in Q$, i.e. all left and right local elements for quasigroup $(Q, \cdot)$ coincide.

Definition. A quasigroup $(Q, \cdot)$ with an identity element $e \in Q$ is called a *loop*.

Theorem. A quasigroup $(Q, \cdot)$ with identity $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (identity associativity) is a loop (is a group).

The following identities are called Moufang identities: $x(y \cdot xz) = (xy \cdot x)z$, $(zx \cdot y)x = z(x \cdot yx)$, $yx \cdot zy = y(xz \cdot y)$.

Theorem. A quasigroup $(Q, \cdot)$ with any from Moufang identities is a loop.

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

Problem. It is easy to see that in loops $1 \cdot ab = 1a \cdot 1b$. Describe quasigroups with the property $f(ab) = f(a)f(b)$ for all $a, b \in Q$, where

$f(a)$ is left local element of element a. Medial quasigroups (with identity $xy \cdot uv = xu \cdot yv$), right F-quasigroup (with identity $yz \cdot x = yf(x) \cdot zx$) possess such property ([13]).

2.5 Multiplication group of quasigroups.

Let $(Q, \cdot)$ be a quasigroup. With every element $a \in Q$ it is possible to associate left (L_a), right (R_a) and middle (P_a) translations. These translations are some permutations of the set Q. They can be considered as elements of the symmetric group S_Q.

With any quasigroup $(Q, \cdot)$ it is possible associate sets of all left translations $(\mathbb{L})$, right translations $(\mathbb{R})$, middle translations $(\mathbb{P})$. We denote groups generated by all left, right and middle translations of a quasigroup $(Q, \cdot)$ as $LM(Q, \cdot)$, $RM(Q, \cdot)$ and $PM(Q, \cdot)$, respectively.

The group generated by all left and right translations of a quasigroup $(Q, \cdot)$ is called (following articles of A.A. Albert) multiplication group of a quasigroup. This group usually denoted as $M(Q, \cdot)$. This group play important role by study of quasigroups, especially by study of loops.

By $FM(Q, \cdot)$ we shall denote a group generated by sets $\mathbb{L}, \mathbb{R}, \mathbb{P}$ of a quasigroup $(Q, \cdot)$.

There is a sense to name the approach to study quasigroups with help of their multiplication groups as Albert's way.

Theorem. (A.A. Albert.) The center of a loop $(Q, \cdot)$ is isomorphic to the center of the group $M(Q, \cdot)$.

On a quasigroup $(Q, \cdot)$ of finite order n it is possible to see as on a set $\mathbb{T}$ of permutations of the group S_n with the property: if $\alpha, \beta \in \mathbb{T}$ and there exists an element $x \in Q$ such that $\alpha^{-1}\beta x = x$, then $\alpha = \beta$.

A set $\mathbb{T}$ of permutations on a finite set Q is called sharply transitive, if for any pair of elements $a, b \in Q$ there exists exactly one permutation $\alpha \in \mathbb{T}$ such that $\alpha a = b$.

Set of all left (right, middle) translations of a quasigroup $(Q, \cdot)$ give us a sharply transitive set of permutations on the set Q.

Center Z of a group G is a set (a subgroup) of elements of this group such that $ax = xa$ for all elements $x \in G, a \in Z$.

Theorem. If Q is a group, then $LM(Q) \cong Q$, $M/Z \cong Q/Z \times Q/Z$, $FM \cong M \leftthreetimes Z_2$, $FM(Q, \cdot) \cong PM(Q, \cdot)$ ([100]).

The importance of multiplication groups lies in the connections between the structure of a quasigroup and structure of its multiplication group. Sometimes it is easier to gain insight into a quasigroup or a loop by studying its multiplication group. Especially important role multiplication groups play in the theory of normality of quasigroups and loops.

Let $(Q,\cdot)$ be a quasigroup. The group $\mathbb{I}_h = \{\alpha \in M(Q,\cdot) | \alpha h = h\}$ is called inner mapping group of a quasigroup $(Q,\cdot)$ relatively an element $h \in Q$. Group $\mathbb{I}_h$ is stabilizer of element h by action ($\alpha : x \longmapsto \alpha(x)$ for all $\alpha \in M(Q,\cdot)$, $x \in Q$) of group $M(Q,\cdot)$ on the set Q. In loop case usually it is studied the group $\mathbb{I}_1(Q,\cdot) = \mathbb{I}(Q,\cdot)$, where 1 is the identity element of a loop $(Q,\cdot)$.

It is possible to define "inner mapping groups" for groups $LM(Q,\cdot)$, $RM(Q,\cdot)$, $PM(Q,\cdot)$, $FM(Q,\cdot)$ of a quasigroup $(Q,\cdot)$, namely, it is possible to define groups $LI_h(Q,\cdot)$, $RI_h(Q,\cdot)$, $PI_h(Q,\cdot)$, $FI_h(Q,\cdot)$. Of course, it is possible to define "inner mapping groups" for other "multiplication groups" of a quasigroup $(Q,\cdot)$.

Since all listed above multiplication groups of a quasigroup $(Q,\cdot)$ act transitively on the set Q, inner mapping groups relatively different elements of the set Q are isomorphic, for example, $PI_h(Q,\cdot) \cong PI_g(Q,\cdot)$, $FI_h(Q,\cdot) \cong FI_g(Q,\cdot)$ and so on.

Theorem. (V.D. Belousov). In a quasigroup $(Q,\cdot)$

$$\mathbb{I}_h(Q,\cdot) =< R_{a,b}, L_{a,b}, T_a \,|\, a,b \in Q >,$$

where $R_{a,b} = R^{-1}_{a\bullet b} R_b R_a$, $h(a \bullet b) = (ha)b$, $L_{a,b} = L^{-1}_{a\circ b} L_a L_b$, $(a \circ b)h = a(bh)$, $T_a = L^{-1}_{\sigma a} R_a$, $\sigma = R^{-1}_h L_h$.

Theorem. ([102]). In a quasigroup $(Q,\cdot)$

$$\mathbb{I}_h(Q,\cdot) =< L_{a,b}, T_{a,b} \,|\, a,b \in Q >,$$

where $L_{a,b} = L^{-1}_{a\circ b} L_a L_b$, $(a \circ b)h = a(bh)$, $T_{a,b} = L^{-1}_{a\star b} R_b L_a$, $(a \star b)h = ah \cdot b$.

Corollary. (R.H. Bruck). In a loop $(Q,\cdot)$

$$\mathbb{I}_h(Q,\cdot) =< R_{a,b}, L_{a,b}, T_a \,|\, a,b \in Q >,$$

where $R_{a,b} = R^{-1}_{ab} R_b R_a$, $L_{a,b} = L^{-1}_{ab} L_a L_b$, $T_a = L^{-1}_a R_a$.

Proposition.([101]). In a quasigroup $(Q,\cdot)$

$$LI_h(Q,\cdot) =< L_{a,b} \,|\, a,b \in Q >,$$

where $L_{a,b} = L^{-1}_{a\circ b} L_a L_b$, $(a \circ b)h = a(bh)$.

Proposition.([102]). In a loop $(Q, \cdot)$

$$PI_h(Q, \cdot) =< P_{a,b} \,|\, a, b \in Q >,$$

where $P_{a,b} = P^{-1}_{a\backslash b} P_a P_b$.

Problems. To describe groups that can be or cannot be multiplication group of a loop (of a quasigroup). We hope, our reader will be able to generalize this problem on other "multiplication groups" of quasigroups and loops (or left quasigroups).

We notice, there are many articles in which properties of quasigroups (or loops) are studied with various conditions on their various kinds inner multiplication groups (articles of T. Kepka, A. Drapal, M. Nimenmaa and their pupils).

2.6 Transversals. "Come back way".

If we gave a quasigroup $(Q, \cdot)$, then we have a possibility to generate (to obtain) groups $M(Q, \cdot)$, $LM(Q, \cdot)$, $\mathbb{I}_h(Q, \cdot)$, $LI(Q, \cdot)$ and so on.

Transversals give us a possibility to construct any loop from a group and a subgroup of this group. Let $(G, \cdot)$ be a group, $(H, \cdot)$ is its subgroup, 1 is the identity element of this group. A complete system T of representatives of the left cosets aH, $a \in G$ is called a left transversal in group $(G, \cdot)$ by (to) subgroup $(H, \cdot)$.

I.e., from any coset $a_i \cdot H$ we take only one element, for example, element a_i. Thus $G = 1 \cdot H \sqcup a_1 \cdot H \sqcup a_2 \cdot H \sqcup \dots a_n \cdot H \sqcup \dots$ and $T = \{1, a_1, a_2, \dots, a_n, \dots\}$ is a left transversal.

Define on the set T an operation $\star$ in the following way: $a \star b = a \cdot b \pmod H$. Probably R.Baer was the first who defined this operation on a transversal ([6, 7]). It is possible to check that that $(T, \star)$ is a right quasigroup with identity element 1, i.e. equation $a \star x = b$ has unique solution for any $a, b \in Q$ and $1 \star x = x \star 1 = x$ for all $x \in T$.

If $(T, \star)$ is a loop, then is called a loop transversal.

In general, any quasigroup $(Q, \circ)$ it is possible to construct in this way, i.e. as a left transversal of a group by its subgroup with operation $\star$. Really, we can take $(G, \cdot) = LM(Q, \circ)$ and $(H, \cdot) = IL_h(Q, \circ)$.

Example. Let $G = S_3 = \{a, b \,|\, a^3 = b^2 = (ab)^2 = 1\} = \{1, a, a^2, b, ab, a^2b\}$, $H =< b >$. We have the following set of left cosets: $H = \{1, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$. Elements $\{b, ab, a^2b\}$ form transversal T. We can construct Cayley table of right quasigroup $(T, \star)$.

$\star$	b	ab	a^2
b	b	a^2	ab
ab	ab	b	a^2
a^2	a^2	b	ab.

If we denote b as 1, ab as 2, a^2 as 3, then we obtain the following Cayley table:

$\star$	1	2	3
1	1	3	2
2	2	1	3
3	3	1	2.

3 Morphisms

3.1 Isotopy of groupoids and quasigroups.

An ordered $(n+1)$-tuple of permutations (bijections) of a set G is called an isotopism (an isotopy).

Definition. Set $\mathcal{T}$ of all isotopisms of a set Q forms a group $S_Q^{n+1} = S_Q \times S_Q \times \cdots \times S_Q$ which is a direct sum $(n+1)$ copies of the group S_Q relatively the following operation (multiplication of $(n+1)$-tuples): $(\mu_1, \mu_2, \ldots, \mu_{n+1}) * (\nu_1, \nu_2, \ldots, \nu_{n+1}) = (\mu_1\nu_1, \mu_2\nu_2, \ldots, \mu_{n+1}\nu_{n+1})$.

Let $\mathcal{G}$ be a class of all n-ary groupoids (arity is fixed) defined on a set Q, $\mathcal{Q}$ be a class quasigroups defined on a set Q. Define action of elements of the group $\mathcal{T}$ on classes $\mathcal{G}, \mathcal{Q}$ in the following way: if (Q, f) is n-ary groupoid, $T = (\nu_1, \nu_2, \ldots, nu_n, n_{n+1}) \in \mathcal{T}$, then $(Q, f)T = \nu_{n+1}^{-1} f(\nu_1 x_1, \nu_2 x_2, \ldots, \nu_n x_n)$ for all $x_1, x_2, \ldots, x_n$.

Theorem. (i) $\mathcal{GT} = \mathcal{G}$, (ii) $\mathcal{QT} = \mathcal{Q}$.

Proof. (i). If (Q, f) is an n-ary groupoid, $T = (\nu_1, \nu_2, \ldots, nu_n, n_{n+1}) \in \mathcal{T}$, then $(Q, f)T$ define some other n-ary groupoid (Q, g) since the operation $g(x_1^n) = \nu_{n+1}^{-1} f(\nu_1 x_1, \nu_2 x_2, \ldots, \nu_n x_n)$ is defined for all $x_1, \ldots, x_n \in Q$.

(ii). Prove this theorem for binary case. For n-ary ($n > 2$) the proof is similar. Let $(Q, \cdot)$ be a quasigroup and $T = (\alpha, \beta, \gamma)$ is an isotopy. Prove that operation $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$ is a quasigroup operation. From (i) it follows, that $(Q, \circ)$ is a binary groupoid.

For any fixed element x the map L_x° is a permutation of the set Q, since $L_x^\circ y = \gamma^{-1} L_{\alpha x}^{\cdot} \beta y$ and product of permutations is a permutation. The map $R_y^\circ x = \gamma^{-1} R_{\beta y}^{\cdot} \alpha x$ is a permutation, too. Taking into consideration Definition 3 of a quasigroup, we conclude, that groupoid $(Q, \circ)$ is a quasigroup.

Corollary. Any isotope of a left (right) quasigroup $(Q, \circ)$ is a left (right) quasigroup.

Problem. To describe identities such that a class $\mathcal{K}$ of n-ary (binary) groupoids (quasigroups, left quasigroups) with these identities is closed relatively isotopisms, i.e. $\mathcal{KT} = \mathcal{K}$. Class of binary groups is closed relatively isotopisms, class of quasigroups isotopic to G-loops, (to groups) is such class, too.

We give and more traditional definition of isotopy. We say that n-ary groupoid (G, f) is an *isotope of n-ary groupoid* (G, g) if there exist permutations $\mu_1, \mu_2, \ldots, \mu_n, \mu$ of the set G such that

$$f(x_1, x_2, \ldots, x_n) = \mu^{-1} g(\mu_1 x_1, \ldots, \mu_n x_n) \tag{1}$$

for all $x_1, \ldots, x_n \in G$. We can write this fact and in the form $(G, f) = (G, g)T$ where $T = (\mu_1, \mu_2, \ldots, \mu_n, \mu)$.

If in (1) $f = g$, then $(n+1)$-tuple $(\mu_1, \mu_2, \ldots, \mu_n, \mu)$ of permutations of the set G is called an *autotopy of n-groupoid* (Q, f). The last component of an autotopy of an n-groupoid is called a *quasiautomorphism* (by analogy with binary case).

A set of all autotopies of a groupoid (Q, f) forms the group of autotopies relatively the usually defined operation on this set: if $T_1 = (\mu_1, \mu_2, \ldots, \mu_n, \mu)$ and $T_2 = (\nu_1, \nu_2, \ldots, \nu_n, \nu)$ are autotopies of groupoid (Q, f), then $T_1 T_2 = (\mu_1\nu_1, \mu_2\nu_2, \ldots, \mu_n\nu_n, \mu\nu)$ is an autotopy of groupoid (Q, f). Autotopy group of a groupoid (Q, f) will be denoted as $\mathfrak{T}(Q, f)$.

If in (1) $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then groupoids (Q, f) and (Q, g) are isomorphic.

At last, if in (1) the n-ary operations f and g are equal and $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then we obtain an *automorphism of groupoid* (Q, f), i.e. a permutation μ of the set Q is said an automorphism of an n-groupoid (Q, f) if for all $x_1, \ldots, x_n \in Q$ the following relation is fulfilled: $\mu f(x_1, \ldots, x_n) =$

$f(\mu_1 x_1, \ldots, \mu_n x_n)$. We denote by $Aut(Q, f)$ automorphism group of an n-ary groupoid (Q, f).

We list some properties of isotopisms. As usual ε denotes identity permutation.

Lemma 1. If $\alpha, \beta, \gamma)$ is an isotopism, then $(\alpha, \beta, \gamma) = (\alpha, \beta, \varepsilon) * (\varepsilon, \varepsilon, \gamma) = (\alpha, \varepsilon, \varepsilon) * (\varepsilon, \beta, \varepsilon) * (\varepsilon, \varepsilon, \gamma) = (\varepsilon, \beta, \varepsilon) * (\varepsilon, \varepsilon, \gamma) * (\alpha, \varepsilon, \varepsilon)$ and so on.

The last Lemma helps by construction of Cayley tables of isotopic image of a finite quasigroup (groupoid).

Remark. If $(Q, \circ) = (Q, \cdot)(\alpha, \varepsilon, \varepsilon)$, i.e. $x \circ y = \alpha x \cdot y$ for all $x, y \in Q$, then $L^{\circ}_x y = L_{\alpha x} y$.

If $(Q, \circ) = (Q, \cdot)(\varepsilon, \beta, \varepsilon)$, i.e. $x \circ y = x \cdot \beta y$ for all $x, y \in Q$, then $R^{\circ}_y x = R_{\beta y} x$.

Let $(Q, \circ) = (Q, \cdot)(\varepsilon, \varepsilon, \gamma)$, i.e. $x \circ y = \gamma^{-1}(x \cdot y)$ for all $x, y \in Q$. Therefore, if $x \cdot y = a$, then $x \circ y = \gamma^{-1} a$.

This Remark helps us to find Cayley table of isotopic image of a groupoid in the following way: if we have isotopy (α, β, γ), then we permute rows by the rule $L^{\circ}_x = L_{\alpha x}$, past this we permute columns by the rule $R^{\circ}_y = R_{\beta y}$, and finally we rename elements into Cayley table by the following rule: if $x \cdot y = a$, then $x \circ y = \gamma^{-1} a$. As it follows from Lemma 1, we can change order of execution of steps 1, 2, 3.

Example. Let $T = ((1234), (12)(34), (123))$. Let a quasigroup $(Q, \cdot)$ has the following Cayley table:

$\cdot$	1	2	3	4
1	2	1	3	4
2	3	2	4	1
3	4	3	1	2
4	1	4	2	3.

If we apply to this quasigroup isotopy $((1234), \varepsilon, \varepsilon)$ (change of rows), then we obtain the following Cayley table

$*$	1	2	3	4
1	2	1	3	4
2	3	2	4	1
3	4	3	1	2
4	1	4	2	3,

further, if we ally to this quasigroup the isotopy $(\varepsilon, (12)(34), \varepsilon)$ (we change order of columns in previous Cayley table), then we obtain such quasigroup

$\circ$	1	2	3	4
1	2	3	1	4
2	3	4	2	1
3	4	1	3	2
4	1	2	4	3,

finally, with help of isotopy $(\varepsilon, \varepsilon, (123))$ $(\gamma^{-1} = (132))$ we rename elements inside the last Cayley table:

$\bullet$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	4	3	2	1
4	3	1	4	2.

Definition. Isotopism of the form $(\alpha, \beta, \varepsilon)$ is called a principal isotopism.

Usually we shall write the fact that groupoids (Q, A) and (Q, B) are isotopic in such form: $(Q, A) \sim (Q, B)$

Lemma. Any isotopism up to isomorphism is a principal isotopism.

Proof. Let (Q, A) and (Q, B) are isotopic groupoids. If $(Q, B) = (Q, A)(\alpha, \beta, \gamma)$, then $(Q, B)(\gamma^{-1}, \gamma^{-1}, \gamma^{-1}) = (Q, A)(\alpha\gamma^{-1}, \beta\gamma^{-1}, \varepsilon)$. Therefore $(Q, C) = (Q, A)(\alpha\gamma^{-1}, \beta\gamma^{-1}, \varepsilon)$, where $(Q, C) = (Q, B)(\gamma^{-1}, \gamma^{-1}, \gamma^{-1})$.

Definition. Let $(Q, \cdot)$ be a quasigroup, a, b be any fixed elements of the set Q. Isotopism of the form $(R_a^{-1}, L_b^{-1}, \varepsilon)$ where L_b, R_a are left and right translations of the quasigroup $(Q, \cdot)$ is called LP-isotopy (loop isotopy).

Theorem. Any LP-isotope of a quasigroup $(Q, \cdot)$ is a loop.

Proof. Prove that quasigroup $(Q, \circ)$, where $x \circ y = R_a^{-1}x \cdot L_b^{-1}y$, is a loop. Let $1 = b \cdot a$. Then we have $(x = 1)$ $1 \circ y = R_a^{-1}ba \cdot L_b^{-1}y = R_a^{-1}R_a b \cdot L_b^{-1}y = b \cdot L_b^{-1}y = L_b L_b^{-1}y = y$. If we take $y = 1$, then we have $x \circ 1 = R_a^{-1}x \cdot L_b^{-1}ba = R_a^{-1}x \cdot a = R_a R_a^{-1}x = x$. Element 1 is the identity element of the quasigroup $(Q, \circ)$.

Theorem. If $(Q,\circ)=(Q,\cdot)(\alpha,\beta,\varepsilon)$ and $(Q,\circ)$ is a loop, then there exist elements $a,b\in Q$ such that $\alpha=R_a^{-1}$, $\beta=L_b^{-1}$, where $R_ax=x\cdot a$, $L_bx=b\cdot x$.

Proof. Let $x\circ y=\alpha x\cdot\beta y$. If $x=1$, then we have $1\circ y=y=\alpha 1\cdot\beta y$. Therefore $L_{\alpha 1}\beta=\varepsilon$, $\beta=L_{\alpha 1}^{-1}$. If we take $y=1$, then we have $x\circ 1=x=\alpha x\cdot\beta 1$, $R_{\beta 1}\alpha=\varepsilon$, $\alpha=R_{\beta 1}^{-1}$.

Albert Theorem. If $(Q,\circ)=(Q,\cdot)(\alpha,\beta,\varepsilon)$, $(Q,\cdot)$ is a group, $(Q,\circ)$ is a loop, then $(Q,\circ)$ is a group isomorphic to group $(Q,\cdot)$.

Proof. By previous theorem $\alpha=R_a^{-1}$, $\beta=L_b^{-1}$.

But in a group $R_a^{-1}=R_{a^{-1}}$. Really, $R_a^{-1}x\cdot a=R_aR_a^{-1}x=x$. Therefore $R_a^{-1}x=x\cdot a^{-1}=R_{a^{-1}}x$, i.e. $R_a^{-1}x=x\cdot a^{-1}$.

Similarly, in any group $L_b^{-1}=L_{b^{-1}}$. Really $b\cdot L_b^{-1}x=L_bL_b^{-1}x=x$. Then $L_b^{-1}x=b^{-1}x=L_{b^{-1}}x$.

Therefore $x\circ y=R_a^{-1}x\cdot L_b^{-1}y=xa^{-1}\cdot b^{-1}y=x(a^{-1}b^{-1})y$. Denote the element $a^{-1}b^{-1}$ as c. Then $(x\circ y)\cdot c=(x\cdot c)\cdot(y\cdot c)$, $R_c(x\circ y)=R_cx\cdot R_cy$.

Hence $(Q,\circ)\cong(Q,\cdot)$. If $a\cdot b=1$, then $(Q,\circ)=(Q,\cdot)$.

3.2 Connection between parastrophy and isotopy.

If $T=(\alpha_1,\alpha_2,\alpha_3)$ is an isotopy, σ is a parastrophy of a quasigroup (Q,A), then we shall denote by T^σ the triple $(\alpha_{\sigma 1},\alpha_{\sigma 2},\alpha_{\sigma 3})$.

Lemma. ([12]). In a quasigroup (Q,A): (i) $(AT)^\sigma=A^\sigma T^\sigma$; (ii) $(T_1T_2)^\sigma=T_1^\sigma T_2^\sigma$.

Proof. (i) We have $AT=(\alpha_1x_1,\alpha_2x_2,\alpha_3x_3)$, where $x_3=A(x_1,x_2)$. By definition of parastrophy we have $A^\sigma=(x_{\sigma 1},x_{\sigma 2},x_{\sigma 3})$. Then we have

$$(AT)^\sigma=(\alpha_1x_1,\alpha_2x_2,\alpha_3x_3)^\sigma=(\alpha_{\sigma 1}x_{\sigma 1},\alpha_{\sigma 2}x_{\sigma 2},\alpha_{\sigma 3}x_{\sigma 3})=A^\sigma T^\sigma.$$

(ii) Let $T_1=(\beta_1,\beta_2,\beta_3)$, $T_2=(\gamma_1,\gamma_2,\gamma_3)$. Then we have

$$(T_1T_2)^\sigma=(\beta_1\gamma_1,\beta_2\gamma_2,\beta_3\gamma_3)^\sigma=(\beta_{\sigma 1}\gamma_{\sigma 1},\beta_{\sigma 2}\gamma_{\sigma 2},\beta_{\sigma 3}\gamma_{\sigma 3})=T_1^\sigma T_2^\sigma.$$

3.3 Autotopisms of quasigroups.

Definition. An autotopism (sometimes we shall call autotopism and as autotopy) is an isotopism of a quasigroup $(Q,\cdot)$ into itself, i.e. a triple (α,β,γ) of permutations of the set Q is an autotopy if the equality $x\cdot y=\gamma^{-1}(\alpha x\cdot\beta y)$ is fulfilled for all $x,y\in Q$.

Denote set of all autotopies of a quasigroup $(Q,\cdot)$ as $Top(Q,\cdot)$. It is clear that defined on this set operation $\star$ of multiplication of autotopies $(\alpha_1,\beta_1,\gamma_1)\star(\alpha_2,\beta_2,\gamma_2)=(\alpha_1\alpha_2,\beta_1\beta_2,\gamma_1\gamma_2)$ is a group operation. We have a possibility to speak on group $(Top(Q,\cdot),\star)$.

Lemma. Set of all the first (the second, the third) components of autotopies of a quasigroup $(Q,\cdot)$ forms a group.

Theorem. ([14]). *If n-ary quasigroups (Q,f) and (Q,g) are isotopic with isotopy T, i.e. $(Q,f)=(Q,g)T$, then $Top(Q,f)=T^{-1}Top(Q,g)T$.*

Proof. Quasigroups (Q,f) and (Q,g) are in one orbit (they are isotopic) by action of the group $\mathcal{T}$ on the set $\mathcal{Q}$ of all quasigroups of a fixed arity n. Autotopy groups of these quasigroups are stabilizers of elements (Q,f) and (Q,g) by this action. It is known that stabilizers of elements of a set S from one orbit by action of a group G on the set S are isomorphic ([64, 56]), moreover, they are conjugate subgroups of the group S_Q^3.

Lemma. If T is an autotopy, then any its two components define the third by unique way.

Proof. If (α_1,β,γ) and (α_2,β,γ) are autotopies, then $(\alpha_2^{-1},\beta^{-1},\gamma^{-1})$ is an autotopy and $(\alpha_1\alpha_2^{-1},\beta\beta^{-1},\gamma\gamma^{-1})=(\alpha_1\alpha_2^{-1},\varepsilon,\varepsilon)$ is an autotopy too. We can re-write the last form of autotopy in such form: $\alpha_1\alpha_2^{-1}x\cdot y=x\cdot y$, then $\alpha_1=\alpha_2$.

If $(\varepsilon,\varepsilon,\gamma_1\gamma_2)$ is an autotopy, then we have $x\cdot y=\gamma_1\gamma_2^{-1}(x\cdot y)$. If we put in the last equality $y=e(x)$, then we obtain $x=\gamma_1\gamma_2^{-1}x$ for all $x\in Q$, i.e. $\gamma_1=\gamma_2$.

There exists and more strong form of the last result.

Lemma. If $(Q,\cdot)$ is a loop, then any its autotopy has the form

$$(R_a^{-1},L_b^{-1},\varepsilon)(\gamma,\gamma,\gamma).$$

Proof. Let $T=(\alpha,\beta,\gamma)$ be an autotopy of a loop $(Q,\cdot)$, i.e. $\alpha x\cdot\beta y=\gamma(x\cdot y)$. If we put $x=1$, then we obtain $\alpha 1\cdot\beta y=\gamma y$, $\gamma=L_{\alpha 1}\beta$, $\beta=L_{\alpha 1}^{-1}\gamma$. If we put $y=1$, then, by analogy, we obtain, $\alpha=R_{\beta 1}^{-1}\gamma$.

Therefore $T=(R_{\beta 1}^{-1}\gamma,L_{\alpha 1}^{-1}\gamma,\gamma)=(R_k^{-1},L_d^{-1},\varepsilon)(\gamma,\gamma,\gamma)$, where $\beta 1=k$, $\alpha 1=d$.

We can obtain more detail information on autotopies of a group, and, since autotopy groups of isotopic quasigroups are isomorphic, on autotopies of quasigroups that are some group isotopes.

Theorem. Any autotopy of a group $(Q,+)$ has the form

$$(L_a\delta, R_b\delta, L_aR_b\delta),$$

where L_a is a left translation of the group $(Q,+)$, R_b is a right translation of this group, δ is an automorphism of this group.

Proof. Let $T=(\alpha,\beta,\gamma)$ be an autotopy of a group $(Q,+)$, i.e. for all $x,y\in Q$ equality

$$\alpha x+\beta y=\gamma(x+y) \tag{1}$$

is true.

If in equality (1) we put $x=y=0$, then we obtain $\alpha 0+\beta 0=\gamma 0$.

If in equality (1) we put only $x=0$, then $\alpha 0+\beta y$, $L_{\alpha 0}\beta=\gamma$, $\beta=L_{-\alpha 0}\gamma$.

If in equality (1) we put only $y=0$, then $\alpha x+\beta 0=\gamma x$, $R_{\beta 0}\alpha=\gamma$, $\alpha=R_{-\beta 0}\gamma$.

Now we can re-write equality (1) in such form: $R_{-\beta 0}\gamma x+L_{-\alpha 0}\gamma y=\gamma(x+y)$, i.e. $\gamma x-\beta 0-\alpha 0+\gamma y=\gamma(x+y)$. Denote $-\beta 0-\alpha 0$ as c, and, it is easy to receive, that $-c=\alpha 0+\beta 0$. From the last equality we have $\gamma x+c+\gamma y+c=\gamma(x+y)+c$, i.e. $R_c\gamma$ is an automorphism of the group $(Q,+)$.

Let $\theta=R_c\gamma$. Then we have that $\gamma=R_{-c}\theta$, $\alpha x=R_{-\beta 0}\gamma x=R_{-\beta 0}R_{-c}\theta x=\theta x+\alpha 0+\beta 0-\beta 0=\theta x+\alpha 0=\alpha 0-\alpha 0+\theta x+\alpha 0=L_{\alpha 0}I_{\alpha 0}\theta x$, where $I_{\alpha 0}x=-\alpha 0+x+\alpha 0$ is an inner automorphism of the group $(Q,+)$.

Similarly, $\beta x=L_{-\alpha 0}\gamma x=L_{-\alpha 0}R_{-c}\theta x=-\alpha 0+\theta x+\alpha 0+\beta 0=R_{\beta 0}I_{\alpha 0}\theta x$.

We can write the permutation γ and in the following form: $\gamma x=\theta x+\alpha 0+\beta 0=\alpha 0-\alpha 0+\theta x+\alpha 0+\beta 0=L_{\alpha 0}R_{\beta 0}I_{\alpha 0}\theta x$.

If we rename $\alpha 0$ as a, $\beta 0$ as b, $I_{\alpha 0}\theta$ as δ, then we obtain the following form of any autotopy of a group $(Q,+)$:

$$(L_a\delta, R_b\delta, L_aR_b\delta).$$

Theorem.([80]) If $(Q,+)$ is a group, then

$$Top(Q,+)\cong((Q,+)\times(Q,+))\leftthreetimes Aut(Q,+).$$

3.4 G-loops and G-quasigroups.

In this subsection we follow [13, 95].

Definition. A bijection θ on a set Q is called a right pseudo-automorphism of a quasigroup $(Q,\cdot)$ if there exists at least one element $c \in Q$ such that $\theta x \cdot (\theta y \cdot c) = (\theta(x \cdot y)) \cdot c$ for all $x, y \in Q$, i.e. $(\theta, R_c\theta, R_c\theta)$ is an autotopy a quasigroup $(Q,\cdot)$. The element c is called a companion of θ.

(This definition belongs to R.H. Bruck.)

Theorem. If a quasigroup $(Q,\cdot)$ possesses a right pseudo-automorphism θ with companion c, then $(Q,\cdot)$ possesses a right identity $e = \theta^{-1}f(c)$, where $f(c)$ is the local left identity of c.

Proof. From $\theta x \cdot (\theta y \cdot c) = (\theta(x \cdot y)) \cdot c$ with $y = \theta^{-1}f(c)$ we have $\theta x \cdot c = \theta(x \cdot \theta^{-1}f(c)) \cdot c$, $x = x \cdot \theta^{-1}f(c)$, i.e. $\theta^{-1}f(c)$ is right identity element of the quasigroup $(Q,\cdot)$, i.e. any quasigroup with at least one non-trivial pseudo-automorphism is a right loop.

Corollary. If $(Q,\cdot)$ is a loop, then $\theta 1 = 1$.

Proof. Really, in a loop with identity element 1 $f(c) = 1$, $e = 1$.

Theorem. Set of all right pseudo-automorphisms of a quasigroup $(Q,\cdot)$ forms a group relatively operation of multiplication of these pseudo-automorphisms as autotopisms of the quasigroup $(Q,\cdot)$.

Proof. If $R_a\varphi$, $R_b\psi$ are the second components of the right pseudo-automorphisms $(\varphi, R_a\varphi, R_a\varphi)$ and $(\psi, R_b\psi, R_b\psi)$ respectively, then we have $R_a\varphi R_b\psi x = R_a\varphi(\psi x \cdot b) = (\varphi(\psi x \cdot b)) \cdot a \overset{def.ofps.-aut.}{=} \varphi\psi x \cdot (\varphi b \cdot a) = R_{\varphi b \cdot a}\varphi\psi x$.

Then $(\varphi, R_a\varphi, R_a\varphi) * (\psi, R_b\psi, R_b\psi) = (\varphi\psi, R_{\varphi b \cdot a}\varphi\psi, R_{\varphi b \cdot a}\varphi\psi)$.

Let us prove that $(\varphi, R_a\varphi, R_a\varphi)^{-1} = (\varphi^{-1}, R_{\varphi^{-1}a}\varphi^{-1}, R_{\varphi^{-1}a}\varphi^{-1})$, where $a^{-1} \cdot a = e$, the element e is the right identity element of the quasigroup $(Q,\cdot)$.

Really,

$$(\varphi, R_a\varphi, R_a\varphi) * (\varphi^{-1}, R_{\varphi^{-1}a}\varphi^{-1}, R_{\varphi^{-1}a}\varphi^{-1}) =$$
$$(\varepsilon, R_{\varphi\varphi^{-1}a^{-1}\cdot a}\varphi\varphi^{-1}, R_{\varphi\varphi^{-1}a^{-1}\cdot a}\varphi\varphi^{-1}) =$$
$$(\varepsilon, \varepsilon, \varepsilon).$$

Further we have

$$(\varphi^{-1}, R_{\varphi^{-1}a}\varphi^{-1}, R_{\varphi^{-1}a}\varphi^{-1}) * (\varphi, R_a\varphi, R_a\varphi) =$$
$$(\varepsilon, R_{\varphi^{-1}a\cdot\varphi^{-1}a^{-1}}, R_{\varphi^{-1}a\cdot\varphi^{-1}a^{-1}}).$$

Prove, that $\varphi^{-1}a \cdot \varphi^{-1}a^{-1} = e$. Since φ is a right pseudo-automorphism with companion a, we have $\varphi(\varphi^{-1}a \cdot \varphi^{-1}a^{-1}) \cdot a = \varphi\varphi^{-1}a \cdot (\varphi\varphi^{-1}a^{-1} \cdot a) = a \cdot (a^{-1} \cdot a) = a \cdot e = a$. Therefore $\varphi(\varphi^{-1}a \cdot \varphi^{-1}a^{-1}) = f(a)$. Hence $\varphi^{-1}a \cdot \varphi^{-1}a^{-1} = \varphi^{-1}f(a) = e$.

Definition. G-loop is a loop which is isomorphic to all its loop isotopes (LP-isotopes).

Theorem. ([12]). A loop $(L, \cdot)$ is G-loop if and only if every element $x \in L$ is a companion of some right and some left pseudo-automorphism of $(L, \cdot)$.

Definition. A quasigroup $(Q, \cdot)$ is called a right G-quasigroup, if any its element is a companion of some its right pseudo-automorphism.

We notice that it is possible to prove that any right G-quasigroup is a loop.

Problem. Research G-loops and right G-loops. Whether there is a right G-loop which is not a G-loop?

4 Sub-objects.

4.1 Subquasigroups. Nuclei and centre.

Definition. A non-empty subset H of a set Q is subquasigroup (subloop, subgroup) of a quasigroup $(Q, \cdot)$ means that $(H, \cdot)$ is a quasigroup (loop, group).

Definition [95]. Let $(Q, \cdot)$ be a groupoid and let $a \in Q$. The element a is left (middle, right) nuclear element in $(Q, \cdot)$ means that $L_{ax} = L_aL_x \Leftrightarrow ax \cdot y = a \cdot xy$ ($L_{xa} = L_xL_a \Leftrightarrow xa \cdot y = x \cdot ay$, $R_{xa} = R_aR_x \Leftrightarrow y \cdot xa = yx \cdot a$) for all $x, y \in Q$.

An element a is nuclear in groupoid $(Q, \cdot)$ means that a is left, right, and middle nuclear element in $(Q, \cdot)$.

Definition [95]. Let $(Q, \cdot)$ be a groupoid. The left nucleus N_l (middle nucleus N_m, right nucleus N_r) of $(Q, \cdot)$ is the set of all left (middle, right) nuclear elements in $(Q, \cdot)$ and nucleus is given by $N = N_l \cap N_r \cap N_m$.

In other words

$$N_l = \{a \in Q | a \cdot xy = ax \cdot y, x, y \in Q\},$$

$$N_m = \{a \in Q | xa \cdot y = x \cdot ay, x, y \in Q\},$$
$$N_r = \{a \in Q | xy \cdot a = x \cdot ya, x, y \in Q\}.$$

R.H. Bruck defined a center of a loop $(Q, \cdot)$ as $Z(Q, \cdot) = N \cap C$, where $C = \{a \in Q | a \cdot x = x \cdot a \ \forall x \in Q\}$.

Exercise. Prove that for a loop (even for a groupoid) $Z = N_l \cap N_r \cap C$.

Theorem. Let $(Q, \cdot)$ be a groupoid. If N_l (N_m, N_r) is non empty, then N_l (N_m, N_r) is a subgroupoid of $(Q, \cdot)$.

Proof. Let $L_{ax} = L_a L_x$, $L_{bx} = L_b L_x$ for all $x \in Q$. Prove, that $L_{ab \cdot x} = L_{ab} L_x$. We have

$$L_{ab \cdot x} = L_{L_{ab} x} = L_{L_a L_b x} = L_{a \cdot bx} = L_a L_{bx} = L_a L_b L_x = L_{ab} L_x.$$

Theorem. [95]. Let $(Q, \cdot)$ be a quasigroup. If $N_m \neq \varnothing$, then N_m is a subgroup of $(Q, \cdot)$ and the identity element e of $(N_m, \cdot)$ is the identity element of $(Q, \cdot)$. If $N_l \neq \varnothing$, then N_l is a subgroup of $(Q, \cdot)$ and the identity element of $(N_l, \cdot)$ is a left identity element of $(Q, \cdot)$. If $N_r \neq \varnothing$, then N_r is a subgroup of $(Q, \cdot)$ and the identity element of $(N_r, \cdot)$ is a right identity element of $(Q, \cdot)$.

M.D. Kitaroage ([72]) gives the following definition of nuclei of a quasigroup $(Q, \cdot)$:

$$N_l(h) = \{a \in Q | ax \cdot y = a \cdot L_h^{-1}(hx \cdot y) \ \forall x, y \in Q\},$$
$$N_m(h) = \{a \in Q | R_h^{-1}(xa) \cdot y = x \cdot L_h^{-1}(ay), \ \forall x, y \in Q\},$$
$$N_r(h) = \{a \in Q | yx \cdot a = R_h^{-1}(y \cdot xh) \cdot a, \ \forall x, y \in Q\}.$$

Let $(Q, \cdot)$ be a quasigroup. We recall that inner mapping group $\mathbb{I}_h(Q, \cdot)$ of a quasigroup $(Q, \cdot)$ is generated by following permutations: $R_{a,b}, L_{a,b}, T_a$, where $R_{a,b} = R_{a \bullet b}^{-1} R_b R_a$, $h(a \bullet b) = (ha)b$, $L_{a,b} = L_{a \circ b}^{-1} L_a L_b$, $(a \circ b)h = a(bh)$, $T_a = L_{\sigma a}^{-1} R_a$, $\sigma = R_h^{-1} L_h$.

The permutation $R_{a,b}$ will be denoted as $R_{a,b}^h$, the permutation $L_{a,b}$ will be denoted as $L_{a,b}^h$, the permutation T_a will be denoted as T_a^h.

Definition.[22, 21]. A left h-nucleus N_l^h of a quasigroup $(Q, \cdot)$ is called the maximal subset H of the set Q such that

(1) $R_{a,b}^h a = a \cdot e(h)$ for all $x, y \in Q$, $a \in H$;

(2) $H \cdot e(h) = H$.

Definition.[22, 21]. A right h-nucleus N_l^h of a quasigroup $(Q, \cdot)$ is called the maximal subset H of the set Q such that
(1) $L_{a,b}^h a = f(a) \cdot a$ for all $x, y \in Q$, $a \in H$;
(2) $f(h) \cdot H = H$.

P.I. Grama defined a center of a quasigroup $(Q, \cdot)$ as a set C of all elements $a \in Q$ such that $R_{x,y}^h a = a$, $L_{x,y}^h a = a$, $T_x^h a = a$ for all $x, y \in Q$.

Later G.B. Belyavskaya and J.D.H. Smith give more general definition of center of a quasigroup. J.D.H. Smith have given definition of center of a quasigroup on language of universal algebra (Congruence Theory). G.B. Belyavskaya gives the following definition of center of a quasigroup.

Definition.[22, 21]. The maximal subset H of the set Q that consists from elements $a \in Q$ such that
(1) $R_{x,y}^h a = a \cdot e(a)$, $L_{x,y}^h a = f(h) \cdot a$, $T_x^h a = \sigma_h^{-1} a$ for all $x, y \in Q$, $a \in H$;
(2) $H \cdot e(h) = f(h) \cdot H = H$, $h \in R_h^{-1} a \cdot H$, for all $a \in H$,
where $R_h^{-1} a \cdot H = \{R_h^{-1} a \cdot b \,|\, b \in H\}$ is called a center Z_h of a quasigroup $(Q, \cdot)$.

4.2 Regular permutations.

Notion of regular permutations is very closed with notions of autotopy and nucleus.

Definition. A permutation λ (ρ) of a set Q is called a left (right) regular permutation for a quasigroup $(Q, \cdot)$, if $\lambda x \cdot y = \lambda^\star(xy)$ ($x \cdot \rho y = \rho^\star(xy)$) for all $x, y \in Q$. A permutation φ is middle regular if $\varphi x \cdot y = x \cdot \varphi^\star y$.

A quasigroup $(Q, \cdot)$ is called $\mathcal{L}$-transitive (respectively $\mathcal{R}$-transitive, Φ-transitive), if group $\mathcal{L}$ ($\mathcal{R}$, Φ) of all left (right, middle) regular permutations is transitive on the set Q.

Theorem. $\mathcal{L}$-transitivity and $\mathcal{L}^\star$-transitivity (respectively $\mathcal{R}$ and $\mathcal{R}^\star$-transitivity, Φ and $\Phi^\star$-transitivity) are equivalent properties for a quasigroup.

"Nuclear" and "central" properties of a quasigroup are closed with property of "linearity" of a quasigroup. See below.

4.3 Congruences, normal subquasigroups, homotopy of quasigroups.

Definition. A quasigroup $(Q, \cdot)$ is a homotopic image of a quasigroup $(P, \circ)$ if there exist surjective maps $\alpha, \beta, \gamma \in Q^P$ ($\alpha \in Q^P \Leftrightarrow \alpha : P \to Q$) such that $\gamma(x \circ y) = \alpha x \cdot \beta y$ for all $x, y \in Q$.

If $\alpha = \beta = \gamma$, then homotopy (homotopism) is a homomorphism.

Theorem. A quasigroup $(P, \circ)$ then and only then is homotopic to a quasigroup $(Q, \cdot)$, when a LP-isotope of the quasigroup $(P, \circ)$ is homotopically mapped on a LP-isotope of the quasigroup $(Q, \cdot)$.

Let $\varphi : (Q, \cdot) \longrightarrow (Q', \circ)$ is an homomorphism of a quasigroup $(Q, \cdot)$ on a quasigroup $(Q', \circ)$. Define in $(Q, \cdot)$ the following binary relation: $a \sim b \leftrightarrow \varphi a = \varphi b$. The binary relation $\sim$ is an equivalence relation. Moreover, $\varphi(a \cdot c) = \varphi a \circ \varphi c$, $\varphi(b \cdot c) = \varphi b \circ \varphi c$. So, if $a \sim b \leftrightarrow \varphi a = \varphi b$, then

$$\varphi(ac) = \varphi a \circ \varphi c = \varphi b \circ \varphi c = \varphi(ab),$$

i.e. $ac \sim bc$. Similarly, $a \sim b \to ca \sim cb$. Then, $\sim$ is a congruence on $(Q, \cdot)$. The following implications are fulfilled too:

(1) $ac \sim bc \longrightarrow a \sim b$,

(2) $ca \sim cb \longrightarrow a \sim b$.

We prove (1).

$$ac \sim bc \to \varphi(ac) = \varphi(bc) \Longleftrightarrow \varphi a \circ \varphi c = \varphi b \circ \varphi c.$$

Since $(Q', \circ)$ is a quasigroup, then $\varphi a = \varphi b \leftrightarrow a \sim b$.

Exercise. If $a \sim b$ and $c \sim d$, then $ac \sim bd$.

A congruence $\sim$ with conditions (1), (2) is called normal congruence.

Exercise. In a group $(G, \cdot, ^{-1}, 1)$ any congruence is normal.

Definition. A quasigroup $(Q, \cdot)$ with identities $xy = yx$, $x \cdot xy = y$, $xy \cdot y = x$ is called TS-quasigroup.

Exercise. In any TS-quasigroup any congruence is normal.

Let θ be a normal congruence of a quasigroup $(Q, \cdot)$. Let $\theta(a) = \{x \,|\, x\theta a\}$ be a coset class of an element a. We list some properties of $\theta(a)$:

- if $b \in \theta(a)$, then $\theta(b) = \theta(a)$;
- $\theta(a) = \theta(b)$ or $\theta(a) \cap \theta(b) = \varnothing$;
- $a \cdot \theta(b) = \theta(a \cdot b) = (\theta a) \cdot b$;
- $\theta(a) \cdot \theta(b) = \theta(a \cdot b)$.

Define an operation $\circ$ on the set$\bar{Q}$ of all cosets of normal congruence θ ($\bar{Q} = \{\theta(a) \,|\, a \in Q\}$) in the following way: $\theta(a) \circ \theta(b) = \theta(a \cdot b)$. It is possible to check that $(\bar{Q}, \circ)$ is a quasigroup. A map $\varphi : a \longrightarrow \bar{a} = \theta(a)$ is a homomorphism of a quasigroup $(Q, \cdot)$ onto quasigroup $(\bar{Q}, \circ)$.

The quasigroup $(\bar{Q}, \circ)$ is called a factor-quasigroup of a quasigroup $(Q, \cdot)$ by the normal congruence θ. The $(\bar{Q}, \circ)$ is denoted as Q/θ.

Theorem. If φ is a homomorphism of a quasigroup $(Q, \cdot)$ onto quasigroup $(\bar{Q}, \circ)$, then there exists a normal congruence θ on quasigroup $(Q, \cdot)$, such that

$$(\bar{Q}, \circ) \cong (Q, \cdot)/\theta$$

and vice versa.

Definition. A subquasigroup $(H, \cdot)$ of a quasigroup $(Q, \cdot)$ is called normal (or normal divisor) if H is a a coset of a normal congruence θ and we shall denote this fact as follows: $H \trianglelefteq Q$.

Theorem. A coset $H = \theta(h)$ of a normal congruence θ of a quasigroup $(Q, \cdot)$ is a subquasigroup if and only if $h \; \theta \; h^2$.

Theorem. Let $(Q, \cdot)$ be a loop with the identity element 1 and N be a normal subloop, i.e. $N = \theta(1)$ for a normal congruence θ. Then
(1) $x \cdot N = N \cdot x$ for all $x \in Q$;
(2) $x \cdot (y \cdot N) = (x \cdot y) \cdot N$, $(N \cdot x) \cdot y = N \cdot (x \cdot y)$ for all $x, y \in Q$;
(3) $(x \cdot N) \cdot (y \cdot N) = (a \cdot b) \cdot N$ for all $x, y \in Q$.

Theorem. A subquasigroup H of a quasigroup Q is normal if and only if $\mathbb{I}_k H \subseteq H$ for all $k \in H$.

A.A. Albert studied normal subloops of a loop $(L, \cdot)$ using normal subgroups of the group $M(L, \cdot)$ ([2, 3]).

4.4 Constructions.

Direct product of quasigroups is standard algebraic construction.

We give construction of crossed product of quasigroups ([12]). Let $(P, \cdot)$ be a some quasigroup, defined on a set $P = \{u, v, w, \dots\}$ and let on a set Q defined a system of quasigroups Σ. For any ordered pair of elements $u, v \in P$ we correspond an operation $A \in \Sigma$, i.e. we define a map $\delta : P^2 \longrightarrow \Sigma$.

On the set $M = P \times Q$ we define the following operation $\circ$:

$$(u, a) \circ (v, b) = (v \cdot v, A_{u,v}(a, b)),$$

where $u, v \in P, a, b \in Q$. Therefore $(M, \circ)$ is a groupoid.

Theorem. If $(P, \cdot)$ is a quasigroup, Σ is a system of quasigroups defined on a set Q, then $(M, \circ)$ is a quasigroup. $(M, \circ)$ is a loop if and only if $(P, \cdot)$ is a loop and and there exist an element $c \in Q$ such that

$$A_{u,1}(a, e) = A_{1,v}(e, a) = a$$

for all $a \in Q$, $u, v \in P$. In this case the identity element of the loop $(M\circ)$ will be the pair $(1, e)$.

Remark. If $\Sigma = \{(Q, A)\}$, then $(M, \circ) \cong (P, \cdot) \times (Q, A)$.

5 Some quasigroup classes

5.1 Medial quasigroups.

A quasigroup $(Q, \cdot)$ with the identity

$$xy \cdot uv = xu \cdot yv \tag{1}$$

is called medial. Remarkable Toyoda theorem (T-theorem) ([12], [13], [90], [111], [24]) says that every medial quasigroup $(Q, \cdot)$ it is possible to present as an special kind isotope of abelian group:

$$x \cdot y = \varphi x + \psi y + a, \tag{2}$$

where $(Q, +)$ is an abelian group, φ, ψ are automorphisms of $(Q, +)$ such that $\varphi\psi = \psi\varphi$, $x, y \in Q$, a is a some fixed element from the set Q.

In view of T-theorem theory of medial quasigroup is very closed with theory of abelian groups but it is not exactly theory of abelian groups. For example, a very simple for abelian groups fact that every simple abelian group is finite was proved for medial quasigroups only in 1977 [7].

Medial quasigroups as and other classes of quasigroups isotopic to groups give us a possibility to construct quasigroups with preassigned properties. Often these properties it is possible to express on language of properties of groups and components of isotopy. Systematically this approach was used by study of T-quasigroups in [61]. By study of automorphisms of linear group isotopes this approach was used in [99].

An element d such that $d \cdot d = d$ is called an idempotent element of a binary quasigroup $(Q, \cdot)$.

Any quasiautomorphism of a group $(Q, +)$ has a form $L_a^+\beta$, where $a \in Q$, $\beta \in Aut(Q, +)$ [12]. Obviously $\beta 0 = 0$, where, as usually, 0 is neutral element of $(Q, +)$.

Theorem *A quasigroup $(Q, \cdot)$ is a medial quasigroup if and only if there exist an abelian group $(Q, +)$, its automorphisms α, φ, $\alpha\varphi = \varphi\alpha$, an element $a \in Q$, such that $x \cdot y = \alpha x + \varphi y + a$ for all $x, y \in Q$.*

($\Longrightarrow$). By proving this implication in the main we follow the book [13]. Let us consider a LP-isotope $(Q, +)$ of a medial quasigroup $(Q, \cdot)$ of a form: $x + y = R_{r(0)}^{-1} \cdot L_0^{-1}$ where $0 \cdot r(0) = 0$, i.e. $r(0)$ is a right local identity element of the element 0. This LP-isotope $(Q, +)$ is a loop with the identity element $0 \cdot r(0) = 0$. Denote $R_{r(0)}$ by α and L_0 by β. We remark that $R_{r(0)}0 = 0$, then $\alpha 0 = 0$.

Using our notations we can write medial identity in the following form:

$$\alpha(\alpha x + \beta y) + \beta(\alpha u + \beta v) = \alpha(\alpha x + \beta u) + \beta(\alpha y + \beta v). \tag{5}$$

By $x = 0, y = \beta^{-1}0$ from (5) we have

$$\beta(\alpha u + \beta v) = \alpha\beta u + \beta(\alpha\beta^{-1}0 + \beta v). \tag{6}$$

Therefore permutation β is a quasiautomorphism of the loop $(Q, +)$.

By $u = 0, v = \beta^{-2}0$ in (5) we have

$$\alpha(\alpha x + \beta y) = \alpha(\alpha x + \beta 0) + \beta(\alpha y + \beta^{-1}0) \tag{7}$$

and we obtain that the permutation α is a quasiautomorphism of the loop $(Q, +)$.

If we use equalities (6) and (7) in (5), then we have

$$\begin{array}{l}(\alpha R_{\beta 0}\alpha x+\beta R_{\beta^{-1}0}\alpha y)+(\alpha\beta u+\beta L_{\alpha\beta^{-1}0}\beta v)=\\ (\alpha R_{\beta 0}\alpha x+\beta R_{\beta^{-1}0}\alpha u)+(\alpha\beta y+\beta L_{\alpha\beta^{-1}0}\beta v).\end{array} \tag{8}$$

If we change in equality (8) the element x by the element $\alpha^{-1}R^{-1}_{\beta 0}\alpha^{-1}x$, the element y by $\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y$, the element u by the element $\beta^{-1}\alpha^{-1}u$, the element v by the element $\beta^{-1}L^{-1}_{\alpha\beta^{-1}0}\beta^{-1}v$.

Then we have

$$(x+y)+(u+v)=(x+\beta R_{\beta^{-1}0}\alpha\beta^{-1}\alpha^{-1}u)+(\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y+v).$$

If we take $u=0$ in the last equality then we have

$$(x+y)+v=(x+\beta R_{\beta^{-1}0}\alpha\beta^{-1}0)+(\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y+v). \tag{9}$$

If we take in (9) $v=0$, then we obtain $x+y=(x+r)+\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y$ where $r=\beta R_{\beta^{-1}0}\alpha\beta^{-1}0$ is a fixed element of the set Q.

If we change in equality (9) $x+y$ by the right side of the last equality, then we have

$$((x+r)+\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y)+v=(x+r)+(\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y+v).$$

From the last equality it follows that the loop $(Q,+)$ is associative, i.e. is a group.

Since α is quasiautomorphism of the group and $\alpha 0=0$ we have that permutation α is an automorphism of the group $(Q,+)$. The permutation β has a form $\beta=R_a\varphi$ where $\varphi\in Aut(Q,+)$.

Then we can re-write the medial identity in the form $\alpha^2x+\alpha\varphi y+\alpha a+\varphi\alpha u+\varphi^2v+\varphi a+a=\alpha^2x+\alpha\varphi u+\alpha a+\varphi\alpha y+\varphi^2v+\varphi a+a$ or, past reduction in the last equality we obtain

$$\alpha\varphi y+\alpha a+\varphi\alpha u=\alpha\varphi u+\alpha a+\varphi\alpha y. \tag{10}$$

From the last equality by $u=0$ we have $\alpha\varphi y+\alpha a=\alpha a+\varphi\alpha y$ and by $y=0$ we have $\alpha a+\varphi\alpha u=\alpha\varphi u+\alpha a$. Using these last equalities we can re-write equality (10) in the such form $\alpha a+\alpha\varphi y+\varphi\alpha u=\alpha a+\alpha\varphi u+\varphi\alpha y$, hence $\alpha\varphi y+\varphi\alpha u=\alpha\varphi u+\varphi\alpha y$. By $u=0$ we have $\alpha\varphi y=\varphi\alpha y$.

Then from equality (10) it follows that $\alpha\varphi y+\alpha\varphi u=\alpha\varphi u+\alpha\varphi y$, $y+u=u+y$. Therefore $x\cdot y=\alpha x+\varphi y+a$ where $(Q,+)$ is an abelian group, α,φ are such automorphisms of $(Q,+)$ that $\alpha\varphi=\varphi\alpha$.

($\Longleftarrow$). We have $\alpha(\alpha x+\varphi y+a)+\varphi(\alpha u+\varphi v+a)+a=\alpha(\alpha x+\varphi u+a)+\varphi(\alpha y+\varphi v+a)+a$, $\alpha^2x+\alpha\varphi y+\alpha a+\varphi\alpha u+\varphi^2v+\varphi a+a=\alpha^2x+\alpha\varphi u+\alpha a+\varphi\alpha y+\varphi^2v+\varphi a+a$, $\alpha\beta y+\alpha\beta u=\alpha\beta u+\alpha\beta y$, $0=0$.

5.2 Linear quasigroups

An n-ary quasigroup of a form

$$\gamma g(x_1, x_2, \ldots, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n,$$

where $(Q, +)$ is a group, $\gamma, \gamma_1, \ldots, \gamma_n$ are some permutations of the set Q, is called *n-ary group isotope* (Q, g). Of course this equality (as often analogous equalities that will appear later in these lectures) is true for all $x_1, x_2, \ldots, x_n \in Q$.

An n-quasigroup of a form

$$g(x_1, x_2, \ldots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a = \sum_{i=1}^{n} \alpha_i x_i + a, \quad (1)$$

where $(Q, +)$ is a group, $\alpha_1, \ldots, \alpha_n$ are some automorphisms of the group $(Q, +)$, the element a is some fixed element of the set Q, will be called *linear n-ary quasigroup* (Q, g) (over group $(Q, +)$).

A linear quasigroup over an abelian group is called *n-T-quasigroup* ([110]). The following identity of n-ary quasigroup (Q, g)

$$\begin{array}{l} g(g(x_{11}, x_{12}, \ldots, x_{1n}), g(x_{21}, x_{22}, \ldots, x_{2n}), \ldots, g(x_{n1}, x_{n2}, \ldots, x_{nn})) = \\ g(g(x_{11}, x_{21}, \ldots, x_{n1}), g(x_{12}, x_{22}, \ldots, x_{n2}), \ldots, g(x_{1n}, x_{2n}, \ldots, x_{nn})) \end{array} \quad (2)$$

is called medial identity ([14]).

An n-ary quasigroup with identity (2) is called *medial n-ary quasigroup*.

In binary case from identity (2) we obtain usual medial identity: $xy \cdot uv = xu \cdot yv$ ([24, 90]).

Definition. A quasigroup of the form $x \cdot y = \alpha x + \beta y + c$, where $(Q, +)$ is a group, $\alpha, \beta \in Aut(Q, +)$, the element c is a fixed element of the set Q is called a linear quasigroup.

This definition belongs to V.D. Belousov ([15]). There exists a possibility to generalize this definition, namely, to change a group $(Q, +)$ on a "good" loop, to change automorphisms α, β on "good" permutations.

G.B. Belyavskaya described class of T-quasigroups with help of identities in "quasigroup" algebra with three binary operations $\cdot, /, \backslash$: $xy \cdot uv = xu \cdot (\alpha_u y \cdot v)$, $xy \cdot uv = (\beta_x v \cdot y) \cdot ux$, where $\alpha_u = R^{-1}_{e(u)} \sigma_u^{-1} L_{f(u)}$ where $\sigma_u = R_u^{-1} L_u$ and $\beta_x = R^{-1}_{e(x)} \sigma_x L_{f(u)}$.

Now theory of medial quasigroups and T-quasigroups is developed sufficiently good.

Importance of T-quasigroups follows from the following theorems. Below we use notion of nuclei and center of a quasigroup in sense of G.B. Belyavskaya.

Theorem. Let $(Q,\cdot)$ be a T-quasigroup. Then $N_l^h(Q,\cdot) = N_h^r(Q,\cdot)$ for any $h \in Q$; $Z_h(Q,\cdot) = (Q,\cdot)$.

A quasigroup $(Q,\cdot)$ with identities $x\cdot yz = xy\cdot xz$ (left distributivity) and $xy\cdot z = xz\cdot yz$ (right distributivity) is called distributive quasigroup.

A loop $(Q,+)$ with identity $(x+x)+(y+z) = (x+y)+(x+z)$ is called commutative Moufang loop (C.M.L. for short).

Theorem. V.D. Belousov. ([12, 13, 95]) Any distributive quasigroup is isotope of a C.M.L.

A quasigroup $(Q,\cdot)$ with identities $x\cdot yz = xy\cdot e(x)z$ (left F-identity) and $zy\cdot x = zf(x)\cdot yx$ (right F-identity) is called F-quasigroup.

Any F-quasigroup is an isotope of a Moufang loop (T. Kepka, J.D. Philips, M. Kinyon, 2003).

Definition. A quasigroup $(Q,\cdot)$ with identities $x(xy) = y$, $xy = yx$ such that any its three elements generate a medial subquasigroup is called CH-quasigroup (Manin quasigroup).

Any CH-quasigroup $(Q,\circ)$ it is possible to obtain with help of the following construction: $x\circ y(-x-y)+d$, where the element d is an element from the center of C.L.M. $(Q,+)$ and $(-x)+x = 0$.

Medial quasigroups, distributive quasigroups, T-quasigroups, CH-quasigroups, F-quasigroups are linear quasigroups in sense of the following definition:

Definition. A quasigroup $(Q,\cdot)$ is called linear over a loop $(Q,+)$ if there exist automorphisms $\varphi,\psi \in Aut(Q,+)$, an element c (usually c is an element from a nucleus of the loop) such that $x\cdot y = (\varphi x+\psi y)+c$ for all $x,y\in Q$.

A quasigroup $(Q,\cdot)$ is called left linear, if $x\cdot y = \varphi x + a + \beta y$, where $(Q,+)$ is a group, $\varphi \in Aut(Q,+)$, $\beta \in S_Q$.

A quasigroup $(Q,\cdot)$ is called alinear, if $x\cdot y = \overline{\varphi}x + a + \beta y$, where $(Q,+)$ is a group, $\overline{\varphi}$ is an anti-automorphism, $\beta \in S_Q$.

Theorem. A.H. Tabarov, G.B. Belyavskaya. $N_m^h = Q$ if and only a quasigroup $(Q,\circ)$ is alinear quasigroup.

$N_l^h = N_r^h = Q$ if and only if a quasigroup $(Q, \cdot)$ is a linear over a group quasigroup.

$N_l^h = N_r^h = N_m^h = Q$ if and only if a quasigroup $(Q, \cdot)$ is a T-quasigroup.

In any distributive quasigroup $N_l^h = N_r^h = N_m^h = Z_h = Q$.

A quasigroup $(Q, \cdot, /, \backslash)$ is linear from the right if and only if holds the identity $(x(u\backslash y))z = (x(u\backslash u)) \cdot (u\backslash yz)$.

5.3 Various kind of inverse quasigroups

Almost all the well-known (classical) kinds of quasigroup and loop such as IP-, LIP-, WIP- and CI-loops and quasigroups are included among the classes of quasigroup which have some kind of inverse property. Most recently, (r, s, t)-inverse quasigroups were defined as a generalization of various kinds of "crossed-inverse" property quasigroup and loop: in particular, they generalize CI-, WIP- and m-inverse loops [65].

1) A quasigroup $(Q, \circ)$ has the *LIP-inverse-property* if there exists a permutation λ of the set Q such that

$$\lambda x \circ (x \circ y) = y \tag{1}$$

for all $x, y \in Q$ [12];

2) a quasigroup $(Q, \circ)$ has the *RIP-inverse-property* if there exists a permutation ρ of the set Q such that

$$(x \circ y) \circ \rho y = x \tag{2}$$

for all $x, y \in Q$ [12];

3) a quasigroup $(Q, \circ)$ has the *IP-inverse-property* if it is LIP- and RIP-inverse quasigroup [12];

4) a quasigroup $(Q, \circ)$ has the *rst-inverse-property* if there exists a permutation J of the set Q such that

$$J^r(x \circ y) \circ J^s x = J^t y \tag{3}$$

for all $x, y \in Q$ [69];

5) a quasigroup $(Q, \circ)$ has the *n-inverse-property* if there exists a permutation J of the set Q such that

$$J^n(x \circ y) \circ J^{n+1} x = J^n y \tag{4}$$

for all $x, y \in Q$ [65];

6) a quasigroup $(Q, \circ)$ has the *weak-inverse-property* if there exists a permutation J of the set Q such that

$$x \circ J(y \circ x) = Jy \tag{5}$$

for all $x, y \in Q$ [7, 109, 69];

7) a quasigroup $(Q, \circ)$ has the *crossed-inverse-property* if there exists a permutation J of the set Q such that

$$(x \circ y) \circ Jx = y \tag{6}$$

for all $x, y \in Q$ [4, 69];

There exist potential applications of m-inverse quasigroups with long inverse cycles to cryptography.

In a loop $(Q, \cdot)$ define x^{-1} as an element such that $x \cdot x^{-1} = 1$, ${}^{-1}x$ as ${}^{-1}x \cdot x = 1$ for all $x \in Q$.

Lemma. In a LIP-loop $(Q, \cdot)$ ${}^{-1}x = x^{-1}$.

Proof. ${}^{-1}x \cdot (x \cdot x^{-1}) = {}^{-1}x \cdot 1 = {}^{-1}x$. Applying LIP-property we have ${}^{-1}x \cdot (x \cdot x^{-1}) = x^{-1}$. Therefore ${}^{-1}x = x^{-1}$.

We give some properties of an IP-quasigroup $(Q, \cdot)$.

Theorem.

1. $\rho^2 = \lambda^2 = \varepsilon$.
2. $(y \cdot \rho x) \cdot x = y$, $x \cdot (\lambda x \cdot y) = y$.
3. $a \cdot x = b \Rightarrow x = \lambda a \cdot b$, $y \cdot a = b \Rightarrow y = b \cdot \rho a$.
4. $\rho(x \cdot y) = \lambda y \cdot \lambda y$.
5. $L_{\lambda a} = L_a^{-1}$, $R_{\rho a} = R_a^{-1}$.
6. $\rho R_a \lambda = L_a^{-1}$, $\lambda L_a \rho = R_a^{-1}$.
7. $\rho L_a \lambda = R_{\lambda a}$, $\lambda R_a \rho = L_{\rho a}$.

Theorem. Any parastrophe of IP-quasigroup $(Q, \cdot)$ is isotopic to $(Q, \cdot)$.

Proof. If $(x \cdot y) \cdot \rho y = x$, then $x/y = x \cdot \rho y$. If $\lambda x \cdot (x \cdot y) = y$, then $x \backslash y = \lambda x \cdot y$. And so on.

We recall, the following identities are called Moufang identities: $x(y \cdot xz) = (xy \cdot x)z$, $(zx \cdot y)x = z(x \cdot yx)$, $yx \cdot zy = y(xz \cdot y)$. In a loop (in a quasigroup) all these identities are equivalent. The identity $x(y \cdot xz) = (x \cdot yx)z$ is called left Bol identity. A loop with any from Moufang identities is called Moufang loop, a loop with left Bol identity is called left Bol loop.

Theorem. If any loop, that is isotopic to a loop $(Q, \cdot)$ is IP-loop, then $(Q, \cdot)$ is Moufang loop.

Theorem. If any loop, that is isotopic to a loop $(Q, \cdot)$ is LIP-loop, then $(Q, \cdot)$ is left Bol loop.

6 Quasigroups and combinatorics

6.1 Orthogonality of quasigroups

A Latin square is an arrangement of m symbols $x_1, x_2, \ldots, x_m$ into m rows and m columns such that no row and now column contains any of the symbols $x_1, x_2, \ldots, x_m$ twice [34, 35]. It is well known that unbordered (i.e. without of the first row and the first column) Cayley table of any finite quasigroup is a Latin square.

Definition. Binary groupoids (Q, A) and (Q, B) are called orthogonal if system of equations

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

has unique solution (x_0, y_0) for any fixed pair of elements $a, b \in Q$. We shall denote this fact as follows: $(Q, A) \perp (Q, B)$.

Example. We give an example of pair of orthogonal groupoids of order 6.

A	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6

B	1	2	3	4	5	6
1	1	2	3	4	5	6
2	1	2	3	4	5	6
3	1	2	3	4	5	6
4	1	2	3	4	5	6
5	1	2	3	4	5	6
6	1	2	3	4	5	6

It is proved that does not exists a pair of orthogonal Latin squares of order 6.

Example. We give an example of pair of orthogonal Latin squares of order 10([79]). In any cell the first number is from the first Latin square, the second number from the second Latin square.

$\cdot, \star$	0	1	2	3	4	5	6	7	8	9
0	12	23	31	46	59	64	78	87	95	00
1	74	42	27	09	61	58	85	90	33	16
2	51	14	45	67	08	80	93	22	76	39
3	07	71	10	38	83	92	44	56	12	65
4	35	57	73	82	94	11	06	49	60	28
5	20	05	52	91	77	36	19	63	48	84
6	43	30	04	55	26	79	62	18	81	97
7	89	98	66	24	32	03	50	75	17	41
8	68	86	99	70	15	47	21	34	02	53
9	96	69	88	13	40	25	37	01	54	72

Example. Quasigroups $(Z_{11}, \star)$ and $(Z_{11}, \circ)$, where $x \star y = x + 2 \cdot y$, $x \circ y = 3 \cdot x + y$ for all $x, y \in Z_{11}$, $(Z_{11}, +, \cdot)$ is ring of residues modulo 11, are orthogonal.

Denote by $N(n)$ number of mutually (in pairs) orthogonal Latin squares of order n.

Theorem. $N(n) \leq (n-1)$.

Problem. Find triple of mutually orthogonal Latin squares of order 10.

There exists and concept of orthogonality for n-ary groupoids.

Definition. n-Ary groupoids $(Q, A_1), \ldots, (Q, A_n)$ are called orthogonal if system of equations

$$\begin{cases} A_1(x_1^n) = a_1 \\ A_2(x_1^n) = a_2 \\ \ldots\ldots\ldots\ldots \\ A_n(x_1^n) = a_n \end{cases}$$

has unique solution (b_1^n) for any fixed n-tuple of elements $a_1^n \in Q$.

6.2 About signs of Bol loop translations

Let $\mathbf{L} = \{L_a \mid a \in Q\}$, $\mathbf{R} = \{R_a \mid a \in Q\}$, $\mathbf{I} = \{I_a \mid a \in Q\}$ be the sets of all left, right and middle translations of a quasigroup $(Q, \cdot)$, where $L_a x = ax$, $R_a x = xa$, $x \cdot I_a x = a$, respectively.

Under the sign function we mean homomorphism of the symmetric group S_n onto the group Z_2 of order 2, $Z_2 = \{1, -1\}$. If $\alpha \in S_n$ is a product of the even number of cycles of length 2 (2-cycles), then $sgn\,\alpha = 1$. If α is a product of the odd number of 2-cycles, then $sgn\,\alpha = -1$.

We shall mention some properties of the sign function. Let $\alpha, \beta, \gamma \in S_n$. Then $sgn(\alpha\beta) = sgn\,\alpha \cdot sgn\,\beta = sgn\,\beta \cdot sgn\,\alpha = sgn(\beta\alpha)$, $sgn(\alpha(\beta\gamma)) = sgn((\alpha\beta)\gamma)$, because the associative and commutative identities hold in the group Z_2.

Let $(Q, \cdot)$ be a finite quasigroup of order n. We use the known notions $sgn\,\mathbf{L} = \prod_{i=1}^{n} sgn(L_{a_i})$, $sgn\,\mathbf{R} = \prod_{i=1}^{n} sgn(R_{a_i})$, $sgn\,\mathbf{I} = \prod_{i=1}^{n} sgn(I_{a_i})$, where $a_i \in Q$; moreover let's define $tsgn\,Q = \langle sgn\,\mathbf{L}, sgn\,\mathbf{R}, sgn\,\mathbf{I}\rangle$.

A loop $(Q, \cdot)$ with identity $x(y \cdot xz) = (xy \cdot x)z$ is called a Moufang loop; a loop with identity $x(y \cdot xz) = (x \cdot yx)z$ is called a left Bol loop. We shall consider only left Bol loops and shall call them Bol loops omitting the word "left" for short.

Theorem. ([82]). Let Q be a finite Bol loop.

- If $\mid Q \mid = 4k$, then $tsgn\,Q = \langle 1, 1, 1\rangle$;
- if $\mid Q \mid = 4k + 1$, then $tsgn\,Q = \langle 1, 1, 1\rangle$;
- if $\mid Q \mid = 4k + 2$, then $tsgn\,Q = \langle -1, -1, -1\rangle$.

Corollary. Let Q be a finite Moufang loop.

- If $\mid Q \mid = 4k$, then $\mathrm{t}sgn\, Q = \langle 1, 1, 1\rangle$;
- if $\mid Q \mid = 4k+1$, then $\mathrm{t}sgn\, Q = \langle 1, 1, 1\rangle$;
- if $\mid Q \mid = 4k+2$, then $\mathrm{t}sgn\, Q = \langle -1, -1, -1\rangle$;
- if $\mid Q \mid = 4k+3$, then $\mathrm{t}sgn\, Q = \langle 1, 1, -1\rangle$.

Let $(Q, \circ)$ be a quasigroup. Denote as $sgn\, Q$ the following product $sgn\, Q = \mathrm{s}gn\mathbf{L} \cdot \mathrm{s}gn\, \mathbf{R} \cdot \mathrm{s}gn\, \mathbf{I}$.

Theorem. Let Q be a finite quasigroup.

- If $\mid Q \mid = 4k$, then $sgn\, Q = 1$;
- if $\mid Q \mid = 4k+1$, then $sgn\, Q = 1$;
- if $\mid Q \mid = 4k+2$, then $sgn\, Q = -1$;
- if $\mid Q \mid = 4k+3$, then $sgn\, Q = -1$.

7 (r, s, t)-inverse quasigroups

7.1 Some general properties of (r, s, t)-inverse quasigroups

In this section we shall use "right" form by writing of acting of a permutation on an element, i.e. $x\alpha$ instead of αx.

Now we shall speak on rst-inverse quasigroups and loops. Results of this section there are in [69]. As it was observed in [66], every (r, s, t)-inverse loop relatively a permutation J such that $1J = 1$ is an $(r, r+1, r)$-inverse loop: that is, it is an r-inverse loop.

Proposition. $(x \circ y)J^r \circ xJ^s = yJ^t$ for all $x, y \in Q \Longleftrightarrow xJ^{-s} \circ (y \circ x)J^{-t} = yJ^{-r}$ for all $x, y \in Q$.

In particular, a weak-inverse-property loop (which satisfies the relation $x \circ (y \circ x)J = yJ$) is a $(-1, 0, -1)$-inverse loop. We discuss such loops (and quasigroups) in more detail below.

Moreover, since $(x \circ y) \circ xJ = y \Longrightarrow xJ^{-1} \circ (y \circ x) = y \Longrightarrow z \circ (y \circ zJ) = y$, where $z = xJ^{-1}$, we have the well-known result that a crossed inverse loop may be defined by the latter relation instead of the former.

Theorem. *If the identity* $(a \cdot b)\alpha \cdot a\beta = b\gamma$ *holds in a quasigroup* $(Q, \cdot)$, *where* α, β, γ *are cyclically (or pairwise) permutable permutations of the set* Q, *then* $\alpha\beta\gamma$ *is an automorphism of the quasigroup* $(Q, \cdot)$.

Corollary. (1) J^{r+s+t} *is an automorphism of an* (r, s, t)*-inverse quasigroup.* (2) J^2 *is an automorphism of a weak inverse property quasigroup.*

Remark. If the quasigroup $(Q, \circ)$ is an (r, s, t)-inverse quasigroup with respect to the permutation J and $J^h \in Aut(Q, \circ)$ for some integer h, then $(Q, \circ)$ is $(r + uh, s + uh, t + uh)$-inverse for any $u \in Z$.

Remark. Since J is an automorphism of a $(0, 1, 0)$-inverse quasigroup, it follows from previous Remark that such a quasigroup is also a $(1, 2, 1)$-inverse quasigroup. that is, every CI-quasigroup has the weak inverse property.

Definition. A *left linear quasigroup* over the loop $(Q, +)$ is a quasigroup $(Q, \cdot)$ such that $x \cdot y = c + x\varphi + y\psi$ for all $x, y \in Q$, where φ is in $Aut(Q, +)$, ψ is a permutation of the set Q such that $\psi 0 = 0$ (where the symbol 0 denotes the identity element of the loop) and c is in the left nucleus N_l of the loop. It becomes a *linear quasigroup* if φ and ψ are both automorphisms of $(Q, +)$.

As a special case of this, a quasigroup $(Q, \cdot)$ defined over an abelian group $(Q, +)$ by $x \cdot y = c + x\varphi + y\psi$, where c is a fixed element of Q and φ and ψ are both automorphisms of the group $(Q, +)$, is called a *T-quasigroup.*

(The latter concept was first introduced in [70] and [71].)

Theorem 1. *A left linear quasigroup* $(Q, \cdot)$ *over a loop* $(Q, +)$ *is an* (r, s, t)*-inverse quasigroup with respect to the permutation* J *of the set* Q, *where* $J^r \in Aut(Q, +)$ *and* $0J = 0$ *if and only if*

(i) $c + cJ^r\varphi = 0$, (iii) $x\varphi J^r\varphi + xJ^s\psi = 0$ *for all* $x \in Q$,
(ii) $\psi = J^t\varphi^{-1}J^{-r}$, (iv) $(Q, +)$ *is a CI-loop.*

Remark. When the conditions of Theorem 1 hold, $J^{r+s+t} = (J^r\varphi)^3 I_0$, where I_0 is defined by $x + xI_0 = 0$ for all $x \in Q$. Consequently, J^{r+s+t} is in $Aut(Q, +)$ as well as being in $Aut(Q, \cdot)$.

Remark. Since a non-abelian group cannot have the crossed inverse property, it follows immediately from Theorem 3.1 that (r, s, t)-inverse left (or right) linear quasigroups over a non-abelian group do not exist.

Example 1. $J : z \longrightarrow 2z \pmod{11}$ in the cyclic group $(Z_{11}, +)$. Since $2^{10} \equiv 1 \pmod{11}$, we require $r + s + t = 10$. Let $r = 6, s = t = 2$. Then the quasigroup $(Z_{11}, \cdot)$ defined by $x \cdot y = c + (2^{-6}x)I_0 + (2^2 y)I_0$ is a $(6, 2, 2)$-inverse quasigroup.

Example 2. $J : z \longrightarrow 2z \pmod{9}$ in the cyclic group $(Z_9, +)$. Since $2^6 \equiv 1 \pmod{9}$, we require $r + s + t = 6$. Let $r = 2, s = 3, t = 1$. Then the quasigroup $(Z_9, \cdot)$ defined by $x \cdot y = c + (2^{-2}x)I_0 + (2y)I_0$ is a $(2, 3, 1)$-inverse quasigroup.

Remark 3. Note that, in the above two examples, the mapping J is an automorphism of the cyclic group but not of the quasigroup constructed from it.

Remark 4. Since an m-inverse quasigroup is an $(m, m + 1, m)$-inverse quasigroup, we can construct an m-inverse quasigroup over $(Z_n, +)$ in the above manner only when $J : z \longrightarrow hz$ with h relatively prime to n and $h^{3m+1} \equiv 1 \bmod n$.

We observe that a special case of Theorem 1 is the following:

Theorem 2. *A left linear quasigroup $(Q, \cdot)$ over a loop $(Q, +)$, where $x \cdot y = c + x\varphi + y\psi$, is a CI-quasigroup relative to the permutation J, where $0J = 0$, if and only if $c + c\varphi = 0$, $\psi = \varphi^{-1}$, $x\varphi^3 + xJ = 0$ for all $x \in Q$ and $(Q, +)$ is a CI-loop.*

Remark 5. Since $\psi = \varphi^{-1}$, it follows that, if φ is an automorphism, so is ψ. Therefore, a left linear *CI*-quasigroup over a loop must in fact be a linear *CI*-quasigroup.

7.2 WIP-quasigroups

We pointed out that a weak-inverse-property loop (WIP-loop) is a $(-1, 0, -1)$-inverse loop. If we use additive notation for the loop and denote the identity by 0, we have

Definition 1. A loop $(Q, +)$ with the property that

$$x + (y + x)I_0 = yI_0 \tag{1}$$

for all $x, y \in Q$, where I_0 is the permutation of Q such that $x + xI_0 = 0$, is called a *weak-inverse-property loop.*

Evidently, we can generalize this definition to that of a WIP-quasigroup as follows:

Definition 2. A quasigroup $(Q, \circ)$ is said to be a *WIP-quasigroup* with respect to the permutation J of Q if

$$x \circ (y \circ x)J = yJ \tag{2}$$

for all $x, y \in Q$.

In this Section we obtain necessary and sufficient conditions for such a quasigroup to be a principal isotope of a WIP-loop. (This then provides a method by which WIP-quasigroups may be constructed.)

Remark 1. A definition very similar to that of Definition 2 was earlier made by Steinberger [109] who studied what he called *$T - WI$-groupoids*.

Lemma 1. *Let $(Q, \circ)$ be a quasigroup defined over the loop $(Q, +)$ by $x \circ y = x\varphi + y\psi$, where φ and ψ are permutations of Q such that $0\varphi = 0$ and $0\psi = 0$. Then, sufficient conditions for $(Q, \circ)$ to be a WIP-quasigroup with respect to the permutation J of Q are (i) $J\psi = \varphi^{-1}J \in Aut(Q, +)$; (ii) $x\varphi + x\psi J\psi = 0$ for all $x \in Q$; and (iii) $(Q, +)$ is a CI-loop.*

When $(Q, +)$ is a CI-loop, we have $u + (v + uI_0) = v$ for all $u, v \in Q$, as we showed in Section 2 of this paper, so $x \circ (y \circ x)J = yJ$ follows.

Lemma 2. *Let $(Q, \circ)$ be a quasigroup defined over the loop $(Q, +)$ by $x \circ y = x\varphi + y\psi$, where φ and ψ are permutations of Q such that $0\varphi = 0$ and $0\psi = 0$. Then, necessary conditions for $(Q, \circ)$ to be a WIP-quasigroup with respect to the permutation J of Q such that $0J = 0$ are (i) $J\psi = \varphi^{-1}J$ and (ii) $x\varphi + x\psi J\psi = 0$ for all $x \in Q$; or, equivalently, (i)* $J = \psi^{-1}\varphi I_0\psi^{-1}$ and (ii)* $[\varphi^{-1}, \psi] = I_0\psi^{-1}I_0^{-1}\varphi^{-1}$.*

From Lemmas 1 and 2, we easily obtain the following theorem:

Theorem 1. *Let $(Q, \circ)$ be a quasigroup defined over the loop $(Q, +)$ by $x \circ y = x\varphi + y\psi$, where φ and ψ are permutations of Q such that $0\varphi = 0$ and $0\psi = 0$. Then, if the permutation J of Q is such that $J\psi = \varphi^{-1}J \in Aut(Q, +)$, necessary and sufficient conditions for $(Q, \circ)$ to be a WIP-quasigroup with respect to the permutation J of Q are (i) $x\varphi + x\psi J\psi = 0$ for all $x \in Q$; and (ii) $(Q, +)$ is a CI-loop.*

Remark 2. The first sentence in the statements of Lemmas 1, 2 and Theorem 1 could alternatively be re-phrased as "Let $(Q, \circ)$ be any principal

isotope $(\varphi, \psi, \epsilon)$ of the loop $(Q, +)$ such that $0\varphi = 0\psi = 0$, where 0 is the identity of $(Q, +)$".

The next theorem gives an alternative set of necessary and sufficient conditions for a quasigroup $(Q, \circ)$ of the above form to be a WIP-quasigroup.

Theorem 2. *Let $(Q, \circ)$ be a quasigroup defined over the loop $(Q, +)$ by $x \circ y = x\varphi + y\psi$, where φ, $\psi \in Aut(Q, +)$. Then $(Q, \circ)$ is a WIP-quasigroup with respect to the permutation J of Q if and only if (i) $J = \psi^{-1}\varphi I_0 \psi^{-1}$; (ii) $[\varphi^{-1}, \psi] = \psi^{-1}\varphi^{-1}$; and (iii) $(Q, +)$ is a WIP-loop.*

Remark 3. It follows from Theorem 2 of previous section that a linear quasigroup $(Q, \circ)$ of the form $x \circ y = x\varphi + y\varphi^{-1}$, defined over a loop $(Q, +)$, is a CI-quasigroup relative to the permutation $J = \varphi^3 I_0$ if and only if $(Q, +)$, is a CI-loop.

Similarly, it follows from Theorem 2 that a linear quasigroup of the above form is a WIP-quasigroup relative to the permutation $J = \varphi^3 I_0$ if and only if $(Q, +)$, is a WIP-loop.

7.3 Direct products of (r, s, t)-quasigroups.

First we look at the special case of m-inverse quasigroups and give a generalization of Theorem 4.1 of [66].

Definition 1. Let $(Q_1, \cdot)$ and $(Q_2, \circ)$ be respectively an (r_1, s_1, t_1)-inverse quasigroup with respect to the permutation J_1 of Q_1 and an (r_2, s_2, t_2)-inverse quasigroup with respect to the permutation J_2 of Q_2. Define $(x_1, x_2)J = (x_1 J_1, x_2 J_2)$, where J is a permutation of $Q_1 \times Q_2$. Let the binary operation $(*)$ be defined on $Q = Q_1 \times Q_2$ by $(x_1, x_2) * (y_1, y_2) = (x_1 \cdot y_1, x_2 \circ y_2)$. Then $(Q, *)$ is the *direct product* of the quasigroups $(Q_1, \cdot)$ and $(Q_2, \circ)$.

Notation. Throughout this Section, we shall suppose that $|Q_1| = n_1$ and $|Q_2| = n_2$, that h_1, h_2 are the least positive integers for which $J^{h_1} \in Aut(Q_1, \cdot)$ and $J^{h_2} \in Aut(Q_2, \cdot)$ and that H_1, H_2 are the least positive integers for which $J_1^{H_1} = I$ and $J_2^{H_2} = I$.

Theorem 1. *Let $(Q_1, \cdot)$ and $(Q_2, \circ)$ be respectively an m_1-inverse quasigroup with respect to the permutation J_1 of Q_1 and an m_2-inverse quasigroup with respect to the permutation J_2 of Q_2 respectively. Then the direct product $(Q, *) = (Q_1, \cdot) \times (Q_2, \circ)$ will be an m-inverse quasigroup of order $n_1 n_2$ relative to the permutation J if there exists a natural number t such that*

$m_1 - m_2 = (h_1, h_2)t$. *In this case,* m *is a solution of the two congruences given below and* $J^H = I$, *where* H *is the least common multiple of* H_1 *and* H_2.

Lemma 1. *Let* $(Q, \cdot)$ *be a quasigroup and* J *be a permutation of* Q *of order* H *(so that* $J^H = I$*) and suppose that* $J^f \in Aut(Q, \cdot)$. *Then also* $J^h \in Aut(Q, \cdot)$, *where* $h = (f, H)$ *is the greatest common divisor of* f *and* H.

Remark 1. We can deduce that, in Theorem 1, $h_1 \leq (3m + 1, H_1)$ and $h_2 \leq (3m + 1, H_2)$.

However, it is possible to obtain a much more general theorem:

Lemma 2. *Let* $(Q_1, \cdot)$ *and* $(Q_2, \circ)$ *be respectively an* (r_1, s_1, t_1)*-inverse quasigroup* $(Q_1, \cdot)$ *with respect to the permutation* J_1 *of* Q_1 *and an* (r_2, s_2, t_2)*-inverse quasigroup* $(Q_2, \circ)$ *with respect to the permutation* J_2 *of* Q_2. *Then the direct product* $(Q, *) = (Q_1, \cdot) \times (Q_2, \circ)$ *will be an* (r, s, t)*-inverse quasigroup relative to the permutation* J *of* Q *for the particular integers* r, s, t *if and only if*

$$(x_1 \cdot y_1)J_1^r \cdot x_1 J_1^s = y_1 J_1^t \quad \textit{and} \quad (x_2 \circ y_2)J_2^r \circ x_2 J_2^s = y_2 J_2^t. \tag{1}$$

We can state the following theorem:

Theorem 2. *The direct product* $(Q, *) = (Q_1, \cdot) \times (Q_2, \circ)$ *will be an* (r, s, t)*-inverse quasigroup relative to the permutation* J *for the particular integers* r, s, t *if there exist integers* u_1 *and* u_2 *such that*

$$r - r_1 = s - s_1 = t - t_1 = u_1 h_1 \quad \textit{and} \quad r - r_2 = s - s_2 = t - t_2 = u_2 h_2, \tag{2}$$

where h_1 *and* h_2 *are defined in the same way as before.*

Remark 2. Theorem 2 can be stated as "if and only if" provided that the two equations which appear in the proof of the theorem are not satisfied for any indices except $r_i + u_i h_i$, etc. $(i = 1, 2)$. However, this is not always the case as the next Remark and Theorem show.

Remark 3. A quasigroup $(Q, \cdot)$ which is an (r, s, t)-inverse quasigroup relative to the permutation J is also an $(r + uh, s + uh, t + uh)$-inverse quasigroup for all $u \in \mathbf{Z}$, where $J^h \in Aut(Q, \cdot)$, but it may happen that $(Q, \cdot)$ is also an (R, S, T)-inverse quasigroup, where $(R, S, T) \notin \{(r + uh, s + uh, t + uh) : u \in \mathbf{Z}\}$ for any choice of h such that $J^h \in Aut(Q, \cdot)$.

Theorem 3. *Let $(Q,\cdot)$ be a quasigroup which is an (r_1,s_1,t_1)-quasigroup relative to the permutation J of Q. Then $(Q,\cdot)$ is also an (r_2,s_2,t_2)-quasigroup (relative to J), where $(r_2,s_2,t_2) \notin \{(r_1+uh, s_1+uh, t_1+uh) : u \in \mathbf{Z}\}$ for any choice of h such that $J^h \in Aut(Q,\cdot)$ if and only if $(J^{s_2-s_1}, J^{t_2-t_1}, J^{r_2-r_1})$ is an autotopism of the quasigroup $(Q,\cdot)$.*

Taking into account both Theorem 2 and Theorem 3, we may state:

Theorem 4. *Suppose that $(Q_1,\cdot)$ and $(Q_2,\circ)$ are respectively an (r_1,s_1,t_1)-inverse quasigroup $(Q_1,\cdot)$ with respect to the permutation J_1 of Q_1 and an (r_2,s_2,t_2)-inverse quasigroup $(Q_2,\circ)$ with respect to the permutation J_2 of Q_2 and that $(Q_1,\cdot)$ and $(Q_2,\circ)$ have no autotopisms of the forms $(J_1^{a_1}, J_1^{b_1}, J_1^{c_1})$ and $(J_2^{a_2}, J_2^{b_2}, J_2^{c_2})$ respectively other than automorphisms. Then the direct product $(Q,*) = (Q_1,\cdot) \times (Q_2,\circ)$ will be an (r,s,t)-inverse quasigroup relative to the permutation J of Q for the particular integers r,s,t if and only if there exist integers u_1 and u_2 such that*

$$r - r_1 = s - s_1 = t - t_1 = u_1 h_1 \quad \textit{and} \quad r - r_2 = s - s_2 = t - t_2 = u_2 h_2.$$

Remark 5. Clearly, it is not possible to meet the conditions of Theorem 4 unless $r_1 - r_2 = s_1 - s_2 = t_1 - t_2$ and unless the greatest common divisor of h_1 and h_2 divides each of these integers.

8 n-ary quasigroups and check character systems.

8.1 Introduction

This section based on results published in [89].

Statistical investigations of J. Verhoeff [112] and D.F. Beckley [11] have shown that the most frequent errors made by human operators during transmission of data are single errors (i.e. errors in exactly one component), adjacent transpositions (in other words errors made by interchanging adjacent digits, i.e. errors of the form $\ldots ab \ldots \longrightarrow \ldots ba \ldots$), and insertion or deletion errors. We note, if all codewords are of equal length, insertion and deletion errors can be detected easily.

To detect single errors and adjacent transpositions one often uses check digit systems; these usually consist of codewords $a_1 \dots a_{n+1}$ containing, besides the information digits $a_1 \dots a_n$, one control character a_{n+1}.

Definition 1 ([104], [105]). A check digit system with one check character is a systematic error detecting code over an alphabet Q which arises by appending *a check digit* a_{n+1} to every word $a_1 a_2 \dots a_n \in Q^n$:

$$\mathfrak{C} : \left\{ \begin{array}{rcl} Q^n & \longrightarrow & Q^{n+1} \\ a_1 a_2 \dots a_n & \longmapsto & a_1 a_2 \dots a_n a_{n+1}. \end{array} \right.$$

Here the word "systematic" means that the check character is the last symbol of any codeword of the code $\mathfrak{C}$.

Check character systems over quasigroups have been studied in [23, 28, 53].

As usual in the study of n-quasigroups $\overline{1,n} = \{1, 2, \dots, n\}$ [14]. We recall definition of n-ary quasigroup.

Definition 2 ([12]). A non-empty set Q with an n-ary operation f such that in the equation $f(x_1, x_2, \dots, x_n) = x_{n+1}$ knowledge of any n elements of $x_1, x_2, \dots, x_n, x_{n+1}$ uniquely specifies the remaining one is called *n-ary quasigroup*.

We can view the code $\mathfrak{C}$ as a mapping over an alphabet Q such that the check symbol a_{n+1} is obtained from information symbols $a_1, a_2, \dots, a_n$ in the following manner: $g(a_1, a_2, \dots, a_n) = a_{n+1}$, where g is an n-ary operation on the set Q. We shall call this code $\mathfrak{C}$ with one check character a_{n+1} over an alphabet Q as an *n-ary code* (Q, g). If in an n-ary code (Q, g) the operation g is an n-ary quasigroup operation, then this code will be called *n-quasigroup code* (Q, g).

We shall say that codewords $a_1 \dots a_{n+1}$ and $b_1 \dots b_{n+1}$ are equal if and only if $a_i = b_i$ for all $i \in \{1, \dots, n+1\}$. Sometimes a codeword $a_1 \dots a_{n+1}$ will be denoted as a_1^{n+1}.

By an error in a codeword a_1^{n+1} of a code $\mathfrak{C}$ over an alphabet Q we mean any word $b_1^{n+1} \in Q^{n+1}$ such that there exists at least one index $j \in \overline{1, n+1}$ such that $a_j \neq b_j$.

As usual an n-ary code (Q, g) detects an error in a received transmission word $a_1 \dots a_n a_{n+1}$ if and only if $g(a_1^n) \neq a_{n+1}$.

Proposition 1. *Any n-ary code (Q, g) detects all single errors if and only if it is an n-quasigroup code, i.e. an n-ary operation g is an n-ary quasigroup operation.*

Proof. This fact follows from properties of a n-ary quasigroup and of n-ary quasigroup code (Q, g) since any n elements uniquely specifies the remaining one in both cases. □

With any n-ary quasigroup (Q, f) it is possible to associate $((n+1)!-1)$ n-ary quasigroups, so-called *parastrophes of the quasigroup* (Q, f) [14].

Let σ be a permutation of the set $\overline{1, n+1}$. Operation f^σ is called a σ-parastroph of the operation f if and only if the following equalities are equivalent: $f^\sigma(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}) = x_{\sigma(n+1)}$ and $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ for all $x_1^n \in Q$.

Let (Q, f) is an n-ary quasigroup, $f(x_1^n) = x_{n+1}$ for all $x_1, \ldots, x_{n+1} \in Q$. Let m be a natural number, with $m \leq n$. If in the last expression we change elements $x_{k_1}, \ldots, x_{k_m}$ respectively by some fixed elements $a_1, \ldots, a_m \in Q$, then this expression takes the form

$$f(x_1^{k_1-1}, a_1, x_{k_1+1}^{k_2-1}, a_2, \ldots, x_{k_m}^n),$$

i.e. we obtain a new operation $g(x_1^{k_1-1}, x_{k_1+1}^{k_2-1}, \ldots, x_{k_m}^n)$. The operation g is an $(n-m)$-ary quasigroup operation. An operation g obtained in such manner is called *a retract* of operation f [14].

Remark 1. By using an n-ary quasigroup retract we can fix in the equality $f(x_1^n) = x_{n+1}$ and the last element x_{n+1}. Really from definition of a parastrophy we have $f(x_1^n) = x_{n+1}$ if and only if $f^\sigma(x_1^{n-1}, x_{n+1}) = x_n$ where the operation f^σ is a σ-parastroph of the quasigroup operation f and $\sigma = (n+1, n+2)$. Then $f(x_1^n) = a_{n+1}$ if and only if $f^\sigma(x_1^{n-1}, a_{n+1}) = x_n$. Since in this case any $(n-1)$ elements uniquely specify the remaining one, we also obtain an $(n-1)$-ary quasigroup operation $g(x_1^{n-1}) = x_n$. We shall call the $(n-1)$-ary operation g as $(n+1)$-*retract of an n-ary quasigroup operation* f.

Let (Q, f) and (Q, g) are n-ary and m-ary quasigroups respectively. Let

$$h(x_1^{m+n-1}) = g(x_1^{i-1}, f(x_i^{i+n-1}), x_{i+n}^{m+n-1}).$$

Then (Q, h) will be an $(m+n-1)$-ary quasigroup. This quasigroup is obtained by the *superposition* of the quasigroup (Q, f) with the quasigroup (Q, g) on the i-th place [14].

In order to define a systematic n-ary code $\mathfrak{C}$ one often uses a check equation of the following form: $f(x_1^{n+1}) = e$ where elements $x_1, \ldots, x_n$ are information symbols, element x_{n+1} is a check symbol, the element e is a fixed element of the set Q, the operation f is an $(n+1)$-ary operation.

It is easy to see that an n-ary code (Q, g) is defined with the help of the check equation $f(x_1^{n+1}) = e$ if and only if the equality $f(x_1^n, g(x_1^n)) = e$ is true for all elements $x_1, \ldots, x_n \in Q$.

If in an n-ary code (Q, g) with check equation $f(x_1^{n+1}) = e$ the operation f is a quasigroup operation, then $x_{n+1} = f^\sigma(x_1^n, e)$ where the operation f^σ is a σ-parastroph of the quasigroup operation f and $\sigma = (n+1, n+2)$. Therefore in this case we have $x_{n+1} = g(x_1^n) = f^\sigma(x_1^n, e)$.

Statement 1. *Any n-ary quasigroup code (Q, g) it is possible to define with help of a check equation $f(x_1^{n+1}) = e$ such that this equation is an $(n+2)$-retract (we fix the $(n+2)$-th place) of an $(n+1)$-ary quasigroup operation.*

Proof. Let $A(x, y) = z$ be a binary group operation on the set Q with the identity element e. We construct the following $(n+1)$-ary quasigroup operation $A(g(x_1^n), y) = z$. Then $A((g(x_1^n), e) = x_{n+1}$ where the element x_{n+1} is a check digit of the information symbols x_1^n of the code (Q, g).

Thus the equation $f(x_1^{n+1}) = A^{(23)}(g(x_1^n), x_{n+1}) = e$ is a check equation of the code (Q, g) such that this equation is an $(n+2)$-retract of an $(n+1)$-ary quasigroup operation. □

Below we shall suppose that the check equation $f(x_1^{n+1}) = e$ of an n-ary quasigroup code (Q, g) is obtained as the $(n+2)$-th retract of an $(n+1)$-ary quasigroup operation $f(x_1^{n+1}) = x_{n+2}$.

The systems most commonly in use are defined over alphabets endowed with a group structure. For a group G = (A, $\cdot$) one can determine the check digit a_n such that the following (check) equation holds (for fixed permutations δ_i of $G, i = 1, ..., n$, and an element e of G, for instance the identity element)

$$\delta_1(a_1)\delta_2(a_2)\ldots\delta_n(a_n) = e \tag{1}$$

Such a system detects all single errors; and it detects all adjacent transpositions if and only if for all $x, y \in G$ with $x \neq y$

$$x \cdot \delta_{i+1}\delta_i^{-1}(y) \neq y \cdot \delta_{i+1}\delta_i^{-1}(x).$$

The proofs are straightforward, see [104]. We shall denote this code as $\mathfrak{C}_1$.

We give one more definition from [104]: Let $(Q, \star_i)$ be quasigroups; then one uses as check equation

$$(\ldots(x_n \star_n x_{n-1}) \star_{n-1} x_{n-2})\ldots) \star_1 x_0 = e. \tag{2}$$

In this definition the element e is any fixed element of the set Q. If elements x_0^{n-1} are information symbols, then element x_n is some check symbol. We shall denote this code as $\mathfrak{C}_2$.

Corollary 1. *The code $\mathfrak{C}_1$ is an $(n-1)$-ary quasigroup code and the code $\mathfrak{C}_2$ is an n-ary quasigroup code.*

Proof. The left-hand side of the check equation (1) defines an n-ary quasigroup operation f [14]. Check equation (1) is obtained as the $(n+1)$-th retract (we fix the $(n+1)$-th place) of the n-ary quasigroup operation f. Therefore the code $\mathfrak{C}_1$ is an $(n-1)$-ary quasigroup code.

The code $\mathfrak{C}_2$ is an n-ary quasigroup code by the same arguments. We see that the check equation (2) is n-ary operation $h : h(x_0^n) = d$. This operation is the $(n+2)$-th retract of the operation $h^\star : h^\star(x_0^n) = x_{n+1}$ for all $x_0, \ldots, x_{n+1} \in Q$. Since the operation $h^\star$ is a superposition of n binary quasigroup operations $\star_1, \star_2, \ldots, \star_n$, then by [14] the operation $h^\star$ is an $(n+1)$-ary quasigroup operation. Therefore the code $\mathfrak{C}_2$ is an n-ary quasigroup code. □

8.2 On possibilities of n-ary quasigroup codes to detect errors

Now we would like to show that all n-ary quasigroup codes (Q, d) over the same alphabet Q and with different quasigroup operations d (arity n is fixed) have equal possibilities to detect errors.

As usual

$$C_n^k = \frac{n!}{k!(n-k)!}$$

denotes a binomial coefficient. We shall call an error on k places in a codeword as *k-error*.

Theorem 1. *Any n-quasigroup code (Q, d) over a fixed alphabet Q, $(|Q| = q)$ and with a fixed finite number n of information symbols and one check digit can detect:*

a) $q^{n+1} - q^n$ errors in n information digits and in one check symbol of any quasigroup codeword (a_1^{n+1});

b) $q^n - q^{n-1}$ errors all possible types in the first n information symbols of any quasigroup codeword (a_1^{n+1});

c) $C_{n+1}^k (q-1)^{k-1}(q-2)$ k-errors $(k > 1)$ in any quasigroup codeword (a_1^{n+1});

d) $C_n^k(q-1)^{k-1}(q-2)$ *k-errors* $(k>1)$ *in the first n information symbols of any quasigroup codeword* (a_1^{n+1}).

Proof. a) If we fix a codeword (a_1^{n+1}) of an n-ary quasigroup code (Q,d) (i.e. for this word the equality $a_{n+1}=d(a_1,\dots,a_n)$ holds), then all other possible words (x_1^{n+1}) where $x_1,\dots,x_{n+1}\in Q$ will be errors. Then there exist $q^{n+1}-1$ possible errors.

The n-ary quasigroup code (Q,d) can not detect errors in q^n-1 quasigroup codewords because for these codewords the check equation $x_{n+1}=d(x_1^n)$ does not detect any errors. Therefore an n-ary quasigroup code (Q,d) detects $q^{n+1}-1-q^n+1=q^{n+1}-q^n$ errors.

b) In this case we suppose that a check symbol a_{n+1} was transmitted without error. The case b) is proved by analogy with the case a). There exist q^n-1 possible errors and there exist $q^{n-1}-1$ quasigroup codewords for which the check equation $a_{n+1}=d(x_1^n)$ does not detect any error.

Therefore an n-ary quasigroup code (Q,d) detects q^n-q^{n-1} errors in the first n information symbols of any quasigroup code word (a_1^{n+1}).

c) We have $C_{n+1}^k(q-1)^k$ words that differ from the quasigroup codeword (a_1^{n+1}) on k places $\{i_1,i_2,\dots,i_k\}$ with $i_1<i_2<\dots<i_k$. Such a set of k places we shall call a k-place.

Really there exist $(q-1)^k$ words that differ from the codeword (a_1^{n+1}) on k fixed places. And we have C_{n+1}^k different k-places. As usual two k-places are different if they are different as sets that consist of k elements.

Any word that differs from the codeword (a_1^{n+1}) on k places $\{i_1,\dots,i_k\}$ has the form

$$(a_1^{i_1-1},x_1,a_{i_1+1}^{i_2-1},x_2,a_{i_2+1},\dots,a_{i_k-1},x_k,a_{i_k+1},\dots,a_{n+1})$$

where $x_1\in Q\setminus\{a_{i_1}\},x_2\in Q\setminus\{a_{i_2}\},\dots,x_k\in Q\setminus\{a_{i_k}\}$.

Let $k=2$. Since for any fixed element $x_0\in Q\setminus\{a_{i_1}\}$ there exists exactly one element $y_0\in Q\setminus\{a_{i_2}\}$ such that $d(a_1^{i-1},x_0,a_{i+1}^{j-1},y_0,a_{j+1}^n)=a_{n+1}$, (i.e. the word $a_1^{i-1},x_0,a_{i+1}^{j-1},y_0,a_{j+1}^n,a_{n+1}$ is a quasigroup code word), then an n-ary quasigroup code (Q,d) can not detect $q-1$ errors on two fixed places i_1,i_2 because for these codewords the check equation $x_{n+1}=d(x_1^n)$ does not show any error. Therefore the code (Q,d) can not detect $C_{n+1}^2(q-1)$ 2-errors.

By analogy since our n-ary quasigroup code (Q,d) can not detect $(q-1)^{k-1}$ errors on k fixed places, it can not detect $C_{n+1}^k(q-1)^{k-1}$ k-errors on all k-places.

Then any n-ary quasigroup code detects

$$C_{n+1}^{k}(q-1)^{k}-C_{n+1}^{k}(q-1)^{k-1}=C_{n+1}^{k}(q-1)^{k-1}(q-1-1)=C_{n+1}^{k}(q-1)^{k-1}(q-2)$$

errors on k places in any quasigroup word (a_1^{n+1}).

d) In this case we suppose that the check symbol a_{n+1} was transmitted without error. The case d) is proved by analogy with the case c). □

Now we are in need of some additional n-ary quasigroup theory. We say that an n-ary quasigroup (Q, f) is an isotope of the n-ary quasigroup (Q, g) if there exist permutations $\mu_1, \mu_2, \ldots, \mu_n, \mu$ that

$$f(x_1, x_2, \ldots, x_n) = \mu^{-1} g(\mu_1 x_1, \ldots, \mu_n x_n) \tag{3}$$

for all $x_1, \ldots, x_n \in Q$. We can write this fact also in the form: $(Q, f) = (Q, g)T$ where $T = (\mu_1, \mu_2, \ldots, \mu_n, \mu)$.

If in (3) $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then the quasigroups (Q, f) and (Q, g) are isomorphic.

We shall say that n-ary quasigroup codes (Q, d) and (Q, g) are *isotopic* if their n-ary quasigroup operations (Q, d) and (Q, g) are isotopic.

Remark 2. From Theorem 1 it follows that isotopic n-ary quasigroup codes detect equal numbers of errors of all types and equal number of k-errors for any suitable k.

Corollary 2.
a) *The relative frequency detected by an n-ary quasigroup code (Q, d) of errors in n information digits and in one check symbol of any quasigroup codeword (a_1^{n+1}) is equal to*

$$\frac{q^n}{q^n + q^{n-1} + \cdots + 1} > \frac{q-1}{q};$$

b) *The relative frequency of detected by n-ary quasigroup code (Q, d) of errors all possible types in the first n information symbols of any quasigroup codeword (a_1^{n+1}) is equal to*

$$\frac{q^{n-1}}{q^{n-1} + q^{n-2} + \cdots + 1} > \frac{q-1}{q};$$

c) *The relative frequency of detected by n-ary quasigroup code (Q, d) of k-errors is equal to*

$$\frac{q-2}{q-1};$$

d) *The relative frequency of detected by n-ary quasigroup code (Q, d) of k-errors in the first n information symbols of any quasigroup codeword (a_1^{n+1}) is equal to*

$$\frac{q-2}{q-1}.$$

Proof. a) From Theorem 1 we have

$$\frac{q^{n+1}-q^n}{q^{n+1}-1} = \frac{q^n(q-1)}{(q-1)(q^n+q^{n-1}+\cdots+1)} = \frac{q^n}{(q^n+q^{n-1}+\cdots+1)}.$$

Further

$$\frac{q^{n+1}-q^n}{q^{n+1}-1} > \frac{q^{n+1}-q^n}{q^{n+1}} = \frac{q-1}{q}.$$

b) This case is proved by analogy with the case a).

c) We have

$$\frac{C_{n+1}^2(q-1)(q-2)}{C_{n+1}^2(q-1)^2} = \frac{q-2}{q-1}.$$

d) Case d) is proved by analogy with the case c). □

Human operators often make two types of errors on two types of places so it is possible to detect using an n-ary quasigroup code (Q, d), namely: transpositions $ab \to ba$ and twin errors $aa \to bb$ on places $(i, i+1)$, $(i, i+2)$ for all suitable $i \in \overline{1, n+1}$.

Statement 2. *In any fixed quasigroup codeword (a_1^{n+1}) there cannot be more than $2n-1$ different transpositions and twin errors.*

Proof. There exist n places of the form $(i, i+1)$ and $n-1$ places of the form $(i, i+2)$. At every such place can be a transposition as error (when $a_i \neq a_{i+1}$ or $a_i \neq a_{i+2}$) or twin error (when $a_i = a_{i+1}$ or $a_i = a_{i+2}$). □

8.3 Totally anti-commutative quasigroups and possibilities of n-ary quasigroup codes to detect transposition and twin errors

We recall that a binary quasigroup $(Q, \cdot)$ is called *anti-commutative* (sometimes such quasigroup is called as *anti-symmetric quasigroup* [28]) if and only if the following implication is true: $x \cdot y = y \cdot x \Rightarrow x = y$ for all $x, y \in Q$ [12].

Definition 3. We shall call a binary anti-commutative quasigroup $(Q, \cdot)$ *totally anti-commutative* if and only if the following implication is true $x \cdot x = y \cdot y \Rightarrow x = y$ for all $x, y \in Q$.

Remark 3. We would like to note that our definition of a totally anti-commutative quasigroup is similar to the definition of a totally anti-symmetric quasigroup [28]: an anti-symmetric quasigroup $(Q, \cdot)$ is *totally anti-symmetric* if and only if the following implication is true $(c \cdot x) \cdot y = (c \cdot y) \cdot x \Rightarrow x = y$ for all $x, y \in Q$. For example, in the case when the quasigroup is a loop and $c = 1$ we have $x \cdot y = y \cdot x \Rightarrow x = y$ for all $x, y \in Q$.

Definition 4. A retract of a form $f(a_1^{i-1}, x_i, a_{i+1}^{i+k-1}, x_{i+k}, a_{i+k+1}^n)$, of an n-ary quasigroup (Q, f) where $a_1^{i-1}, a_{i+1}^{i+k-1}, a_{i+k+1}^n$ are some fixed elements of the set Q, $i \in \overline{1, n-k}, k \in \overline{1, n}$ is called an $(i, i+k)$ *binary retract of an n-ary quasigroup* (Q, f).

Theorem 2. *An $(n-1)$-ary quasigroup code (Q, g) with check equation $d(x_1^n) = e$ where the element e is a fixed element of the set Q detects any transposition and twin error on places of the form $(i, i+k)$ $(i \in \overline{1, n-k}, k \in \overline{1, n-1})$ if and only if all $(i, i+k)$ binary retracts of n-ary quasigroup (Q, d) are totally anti-commutative quasigroups.*

Proof. If we suppose that all $(i, i+k)$ binary retracts of an n-ary quasigroup (Q, d) are totally anti-commutative quasigroups, then from the definition of totally anti-commutative binary quasigroups it follows that the code (Q, g) detects any transposition and twin error in the place $(i, i+k)$.

Conversely, if we suppose that there is a place $(i, i+k)$ and there are elements $a_1^{i-1}, b, a_{i+1}^{i+k-1}, c, a_{i+k+1}^n$ $(b \neq c)$ such that

$$d(a_1^{i-1}, b, a_{i+1}^{i+k-1}, c, a_{i+k+1}^n) = d(a_1^{i-1}, c, a_{i+1}^{i+k-1}, b, a_{i+k+1}^n),$$

then the binary retract $d(a_1^{i-1}, x, a_{i+1}^{i+k-1}, y, a_{i+k+1}^n)$ is not an anti-commutative quasigroup, and we have a contradiction.

If we suppose that there is a place $(i, i+k)$ and there are elements $a_1^{i-1}, b, a_{i+1}^{i+k-1}, c, a_{i+k+1}^n$ $(b \neq c)$ such that

$$d(a_1^{i-1}, b, a_{i+1}^{i+k-1}, b, a_{i+k+1}^n) = d(a_1^{i-1}, c, a_{i+1}^{i+k-1}, c, a_{i+k+1}^n),$$

then the binary retract $d(a_1^{i-1}, x, a_{i+1}^{i+k-1}, y, a_{i+k+1}^n)$ is not an anti-commutative quasigroup, and again we have a contradiction. □

Definition 5. An n-ary quasigroup (n-quasigroup) of the form $\gamma g(x_1, x_2, \ldots, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n$ where $(Q, +)$ is a group, $\gamma, \gamma_1, \ldots, \gamma_n$ are

permutations of the set Q will be called an *n-ary group isotope* (Q, g). Of course this equality is true for all $x_1, x_2, \ldots, x_n \in Q$.

An n-quasigroup of the form

$$g(x_1, x_2, \ldots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a = \sum_{i=1}^{n} \alpha_i x_i + a$$

where $(Q, +)$ is a group, $\alpha_1, \ldots, \alpha_n$ are automorphisms of the group $(Q, +)$, and the element a is some fixed element of the set Q, will be called a *linear n-ary quasigroup* (Q, g) (over the group $(Q, +)$). A linear n-ary quasigroup over an abelian group is called an *n-T-quasigroup* (Q, g).

If in an n-ary quasigroup code (Q, g) the operation g or the operation d from the check equation $d(x_1^{n+1}) = e$ of this code is an n-T-quasigroup operation, then the code (Q, g) will be called an *n-T-quasigroup code* (Q, g).

Corollary 3. *In an n-ary group isotope (Q, g) of the form $g(x_1, x_2, \ldots, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n$:*

a) all its $(i, i+1)$ ($i \in \overline{1, n-1}$) binary retracts are totally anti-commutative quasigroups if and only if all its binary retracts of the form $\gamma_i x_i + \gamma_{i+1} x_{i+1}$ are totally anti-commutative quasigroups;

b) all its $(i, i+k)$ ($i \in \overline{1, n-k}, k \in \overline{1, n-1}$) binary retracts are totally anti-commutative quasigroups if and only if all its binary retracts of the form $\gamma_i x_i + a_{i+1} + \cdots + a_{i+k-1} + \gamma_{i+k} x_{i+k}$ for any fixed elements $a_{i+1}, \ldots, a_{i+k-1} \in Q$ are totally anti-commutative quasigroups.

Proof. a) Assume all binary retracts of the form $\gamma_i x_i + \gamma_{i+1} x_{i+1}$ of n-ary group isotope (Q, g) are totally anti-commutative quasigroups.

If we suppose that there is a place $(i, i+1)$ and there are elements $a_1^{i-1}, b, c, a_{i+2}^n$ $(b \neq c)$ such that $g(a_1^{i-1}, b, c, a_{i+2}^n) = g(a_1^{i-1}, c, b, a_{i+2}^n)$, i.e. that

$$\begin{gathered}\gamma_1 a_1 + \cdots + \gamma_{i-1} a_{i-1} + \gamma_i b + \gamma_{i+1} c + \gamma_{i+1} a_{i+1} + \cdots + \gamma_n a_n = \\ \gamma_1 a_1 + \cdots + \gamma_{i-1} a_{i-1} + \gamma_i c + \gamma_{i+1} b + \gamma_{i+1} a_{i+1} + \cdots + \gamma_n a_n\end{gathered}$$

or, upon cancellation, that $\gamma_i b + \gamma_{i+1} c = \gamma_i c + \gamma_{i+1} b$, then we obtain a retract of the form $\gamma_i x_i + \gamma_{i+1} x_{i+1}$ which is not a totally anti-commutative quasigroup. We have a contradiction with conditions of this corollary.

If we suppose that there is a place $(i, i+1)$ and there are elements $a_1^{i-1}, b, c, a_{i+2}^n$ $(b \neq c)$ such that $g(a_1^{i-1}, b, b, a_{i+2}^n) = g(a_1^{i-1}, c, c, a_{i+2}^n)$, i.e. that

$$\begin{gathered}\gamma_1 a_1 + \cdots + \gamma_{i-1} a_{i-1} + \gamma_i b + \gamma_{i+1} b + \gamma_{i+1} a_{i+1} + \cdots + \gamma_n a_n = \\ \gamma_1 a_1 + \cdots + \gamma_{i-1} a_{i-1} + \gamma_i c + \gamma_{i+1} c + \gamma_{i+1} a_{i+1} + \cdots + \gamma_n a_n\end{gathered}$$

or, upon cancellation, that $\gamma_i b+\gamma_{i+1}b = \gamma_i c+\gamma_{i+1}c$, then we obtain a retract of the form $\gamma_i x_i+\gamma_{i+1}x_{i+1}$ which is not totally anti-commutative quasigroup. We have again a contradiction with conditions of this corollary.

Therefore, if all binary retracts of the form $\gamma_i x_i + \gamma_{i+1}x_{i+1}$ of the n-ary group isotope (Q, g) are totally anti-commutative quasigroups, then all $(i, i+1)$ $(i \in \overline{1, n-1})$ binary retracts of this n-ary group isotope are totally anti-commutative quasigroups.

Converse assertion is obvious.

b) This case is proved by analogy with case a). □

There is a possibility to re-formulate Corollary 3 in the language of binary quasigroups which are retracts of the n-ary quasigroup (Q, g).

Corollary 3*. *In an n-ary group isotope (Q, g) of the form $g(x_1^n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n$:*

a) all of the $(i, i+1)$ $(i \in \overline{1, n-1})$ binary retracts are totally anti-commutative quasigroups if and only if all binary quasigroups of the form $\gamma_i x_i + \gamma_{i+1}x_{i+1}$ are totally anti-commutative quasigroups;

b) all of the $(i, i+k)$ $(i \in \overline{1, n-k}, k \in \overline{1, n-1})$ binary retracts are totally anti-commutative quasigroups if and only if all binary quasigroups of the form $\gamma_i x_i + t + \gamma_{i+k}x_{i+k}$, for any fixed element t, are totally anti-commutative quasigroups.

Proof. It is sufficiently to denote the element $a_{i+1}+\cdots+a_{i+k-1}$ by the letter t. □

Corollary 4. *An $(n-1)$-ary group isotope code (Q, g) with check equation $\sum\limits_{i=1}^{n} \gamma_i x_i = 0$ where the element 0 is the identity element of the group $(Q, +)$ detects any transposition and twin error on places $(i, i+1)$ $(i \in \overline{1, n-1})$, $(i, i+2)$ $(i \in \overline{1, n-2})$ if and only if all quasigroups of the form $\gamma_i x_i+\gamma_{i+1}x_{i+1}$ and of the form $\gamma_i x_i + a_i + \gamma_{i+2}x_{i+2}$ for any fixed $a_i \in Q$, are totally anti-commutative quasigroups.*

Proof. This follows from Corollary 3. □

Corollary 5. *In an n-ary group isotope (Q, g) of the form $g(x_1, x_2, \ldots, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n$ where the group $(Q, +)$ is abelian all of its $(i, i+k)$ $(i \in \overline{1, n-k}, k \in \overline{1, n-1})$ binary retracts are totally anti-commutative quasigroups if and only if all binary retracts of the form $\gamma_i x_i + \gamma_{i+k}x_{i+k}$ are totally anti-commutative quasigroups.*

Proof. If we suppose that there is a place $(i, i+k)$ and there are elements a_1^{i-1}, b, a_{i+1}^{i+k-1}, c, a_{i+k+1}^{n} $(b \neq c)$ such that

$$g(a_1^{i-1}, b, a_{i+1}^{i+k-1}, c, a_{i+k+1}^{n}) = g(a_1^{i-1}, c, a_{i+1}^{i+k-1}, b, a_{i+k+1}^{n}),$$

i.e. that $\gamma_1 a_1 + \cdots + \gamma_{i-1}a_{i-1} + \gamma_i b + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}c + \gamma_{i+k+1}a_{i+k+1} + \cdots + \gamma_n a_n = \gamma_1 a_1 + \cdots + \gamma_{i-1}a_{i-1} + \gamma_i c + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}b + \gamma_{i+k+1}a_{i+k+1} + \cdots + \gamma_n a_n$, then upon cancellation we have $\gamma_i b + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}c = \gamma_i c + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}b$.

Since the group $(Q, +)$ is commutative we further obtain that $\gamma_i b + \gamma_{i+k}c = \gamma_i c + \gamma_{i+k}b$.

Thus we see that the retract of the form $\gamma_i x_i + \gamma_{i+k}x_{i+k}$ is not a totally anti-commutative quasigroup. We have a contradiction with conditions of this corollary.

If we suppose that there is a place $(i, i+k)$ and there are elements $a_1^{i-1}, b, a_{i+1}^{i+k-1}$, c, a_{i+k+1}^{n} $(b \neq c)$ such that

$$g(a_1^{i-1}, b, a_{i+1}^{i+k-1}, b, a_{i+k+1}^{n}) = g(a_1^{i-1}, c, a_{i+1}^{i+k-1}, c, a_{i+k+1}^{n}),$$

i.e. that $\gamma_1 a_1 + \cdots + \gamma_{i-1}a_{i-1} + \gamma_i b + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}b + \gamma_{i+k+1}a_{i+k+1} + \cdots + \gamma_n a_n = \gamma_1 a_1 + \cdots + \gamma_{i-1}a_{i-1} + \gamma_i c + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}c + \gamma_{i+k+1}a_{i+k+1} + \cdots + \gamma_n a_n$, then upon cancellation we have $\gamma_i b + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}b = \gamma_i c + \gamma_{i+1}a_{i+1} + \cdots + \gamma_{i+k-1}a_{i+k-1} + \gamma_{i+k}c$.

Since the group $(Q, +)$ is commutative we further obtain that $\gamma_i b + \gamma_{i+k}b = \gamma_i c + \gamma_{i+k}c$.

Thus we have that a retract of the form $\gamma_i x_i + \gamma_{i+k}x_{i+k}$ is not totally anti-commutative quasigroup, and we have a contradiction with conditions of this corollary.

Therefore, if all binary retracts of the form $\gamma_i x_i + \gamma_{i+k}x_{i+k}$ of the n-ary group isotope (Q, g) over an abelian group $(Q, +)$ are totally anti-commutative quasigroups, then all $(i, i+k)$ $(i \in \overline{1, n-k}, k \in \overline{1, n-1})$ binary retracts of this n-ary group isotope are totally anti-commutative quasigroups.

The converse is obvious. □

Corollary 6. *An $(n-1)$-ary abelian group isotope code (Q, g) with check equation $\sum_{i=1}^{n} \gamma_i x_i = 0$ where the element 0 is the identity element of the abelian group $(Q, +)$ detects any transposition and twin error on places $(i, i+$*

1) $(i \in \overline{1, n-1})$, $(i, i+2)$ $(i \in \overline{1, n-2})$ *if and only if all quasigroups of the form* $\gamma_i x_i + \gamma_{i+1} x_{i+1}$ *and of the form* $\gamma_i x_i + \gamma_{i+2} x_{i+2}$ *are totally anti-commutative quasigroups.*

Proof. This follows from Corollary 5. □

Proposition 2. *A binary T-quasigroup* $(Q, \cdot)$ *of the form* $x \cdot y = \alpha x + \beta y + a$ *will be a totally anti-commutative quasigroup if and only if the mappings* $\alpha - \beta$ *and* $\alpha + \beta$ *are automorphisms of the group* $(Q, +)$ *(i.e. they are permutations of the set* Q*).*

Proof. For a T-quasigroup $(Q, \cdot)$ the property of anti-commutativity $x \cdot y = y \cdot x \Rightarrow x = y$ for all $x, y \in Q$ can be rewritten in the form:

$$(\alpha x + \beta y = \alpha y + \beta x \Rightarrow x = y) \Leftrightarrow$$
$$((\alpha - \beta)x = (\alpha - \beta)y \Rightarrow x = y) \Leftrightarrow$$
$$((\alpha - \beta)(x - y) = 0 \Rightarrow x = y).$$

The last implication will be true only if $\alpha - \beta$ is an automorphism of group $(Q, +)$ (in general the mapping $\alpha - \beta$ is an endomorphism of the group $(Q, +)$).

The implication $x \cdot x = y \cdot y \Rightarrow x = y$ for all $x, y \in Q$ can be rewritten in the form

$$(\alpha x + \beta x = \alpha y + \beta y \Rightarrow x = y) \Leftrightarrow$$
$$((\alpha + \beta)(x - y) = 0 \Rightarrow x = y).$$

The last implication will be true only if $\alpha + \beta$ is an automorphism.

Conversely, if the map $\alpha - \beta$ is an automorphism (a permutation on the set Q), then the implication $(\alpha - \beta)(x - y) = 0 \Rightarrow x = y$ is true since the automorphism $\alpha - \beta$ has the identity as its kernel.

If the map $\alpha + \beta$ is an automorphism, then the implication $x \cdot x = y \cdot y \Rightarrow x = y$ holds in the T-quasigroup $(Q, \cdot)$. □

Theorem 3. *Any* $(n-1)$*-T-quasigroup code* (Q, g) *with check equation* $d(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$ *detects:*

a) any transposition error on the place $(i, i+1)$, $i \in \overline{1, n-1}$, *if and only if the mapping* $\alpha_i - \alpha_{i+1}$ *is an automorphism of the group* $(Q, +)$*;*

b) any transposition error on the place $(i, i+2)$ *(i.e. jump transposition error),* $i \in \overline{1, n-2}$, *if and only if the mapping* $\alpha_i - \alpha_{i+2}$ *is an automorphism of the group* $(Q, +)$*;*

c) any twin error on the place $(i, i+1)$, $i \in \overline{1, n-1}$, *if and only if the mapping* $\alpha_i + \alpha_{i+1}$ *is an automorphism of the group* $(Q, +)$*;*

d) any twin error on the place $(i, i+2)$ *(i.e. jump twin error),* $i \in \overline{1, n-2}$, *if and only if the mapping* $\alpha_i + \alpha_{i+2}$ *is an automorphism of the group* $(Q, +)$.

Proof. This follows from Corollary 2 and Proposition 2. □

We shall call an n-quasigroup code (Q, d) that detects any transposition and twin error on places $(i, i+1)$ where $i \in \overline{1, n-1}$ and on places $(i, i+2)$ where $i \in \overline{1, n-2}$ an *5-n-quasigroup code* (Q, d) (since such code detects five types of errors).

Theorem 4. *The direct product of a a 5-n-quasigroup code* (Q_1, d) *and 5-n-quasigroup code* (Q_2, g) *is a 5-n-quasigroup code* $(Q_1 \times Q_2, f)$ *where* $f = d \circ g$.

Proof. This follows from standard definition of direct product and the statement that the direct product of anti-commutative quasigroups is an anti-commutative quasigroup. The last statement follows from well known fact that a class of universal algebras of fixed signature defined with identities and quasi-identities is closed with respect to the direct product [74].

We recall that it is possible to define a quasigroup as an algebra $(Q, \cdot, /, \backslash)$ with binary operations $\cdot, /, \backslash$ such that the following identities hold: $x \cdot (x \backslash y) = y$, $(y/x) \cdot x = y$, $x \backslash (x \cdot y) = y$, $(y \cdot x)/x = y$. □

Remark 4. Theorem 4 is true for n-quasigroup codes that detect any transposition and twin error on the same set of places of the form $(i, i+k)$.

8.4 Examples

Example 1. It is used now the International Standard Book Number code (ISBN) with $(Z_{11}, +)$, $n = 10$, and the check equation $1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8 \cdot x_8 + 9 \cdot x_9 + 10 \cdot x_{10} \equiv 0 \pmod{11}$.

"... this system detects all adjacent transpositions but needs an element $X \notin \{0, ..., 9\}$" [104].

Using Theorem 3 we can say that this system detects all single errors, transposition and twin errors on places $(i, i+1)$, $(i, i+2)$ for any possible value of index i with the exception of twin error on place $(5, 6)$.

If we take the check equation

$$1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 10 \cdot x_6 + 9 \cdot x_7 + 8 \cdot x_8 + 7 \cdot x_9 + 6 \cdot x_{10} \equiv 0 \pmod{11}$$

or

$$1 \cdot x_1 + 3 \cdot x_2 + 5 \cdot x_3 + 7 \cdot x_4 + 9 \cdot x_5 + 10 \cdot x_6 + 8 \cdot x_7 + 6 \cdot x_8 + 4 \cdot x_9 + 2 \cdot x_{10} \equiv 0 \pmod{11},$$

then these 9-ary-T-quasigroup codes over the group $(Z_{11}, +)$ detect all single errors, transposition and twin errors on places $(i, i+1)$, $(i, i+2)$ for any permissible value of index i.

Of course, in the last check equations we may change the group $(Z_{11}, +)$ by any group $(Z_p, +)$ where p is a prime number, $p \geq 7$ and we can take any finite number $n \geq 4$ of items (4 because we must have check symbol and a possibility to receive jump errors).

For $p = 7$ we have the following systematic code with the check equation

$$x_1 + 2x_2 + 3x_3 + 6x_4 + 5x_5 + 4x_6 + x_7 + 2x_8 + \cdots + ax_n \equiv 0 \pmod 7,$$

where $a = 1$, if $n \equiv 1 \pmod 6$, $a = 2$, if $n \equiv 2 \pmod 6$, $a = 3$, if $n \equiv 3 \pmod 6$, $a = 6$, if $n \equiv 4 \pmod 6$, $a = 5$, if $n \equiv 5 \pmod 6$, $a = 4$, if $n \equiv 0 \pmod 6$ or

$$x_1 + 3x_2 + 5x_3 + 6x_4 + 4x_5 + 2x_6 + x_7 + 3x_8 + \cdots + ax_n \equiv 0 \pmod 7,$$

where $a = 1$, if $n \equiv 1 \pmod 6$, $a = 3$, if $n \equiv 2 \pmod 6$, $a = 5$, if $n \equiv 3 \pmod 6$, $a = 6$, if $n \equiv 4 \pmod 6$, $a = 4$, if $n \equiv 5 \pmod 6$, $a = 2$, if $n \equiv 0 \pmod 6$, $x_i \in Z_7$ for any $i \in \overline{1, n}$.

Example 2. "The European Article Number code (EAN) and (after adding 0 as first digit) the Universal Product Code (UPC) with $G = (Z_{10}, +)$, $n = 13$, $e = 0$, $\delta_{2i-1}(a) = a = L_1(a)$ and $\delta_{2i}(a) = 3a = L_3(a)$ ... " [104].

In other words the EAN code is the code with the check equation

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13} = 0$$

where $x_i \in Z_{10}$, $i \in \overline{1, 13}$.

"... this system (EAN code - G.M., V.Shch.) does not detect adjacent transpositions $\ldots ab \cdots \to \ldots ba \ldots$ for $|a - b| = 5$ " [104].

Moreover, this system does not detect errors of the form $\ldots\ acb\ \ldots \to \ldots\ bca\ \ldots$, i.e. so called jump transposition errors for any pair of elements $a, b \in Z_{10}$.

Really, let we have jump transposition $\ldots acb \cdots \to \ldots bca$. Passing to group operation we have the following expressions $\ldots 3a{+}c{+}3b \ldots, \ldots 3b{+}c{+}3a \ldots$ or $\ldots a{+}3c{+}b \ldots, \ldots b{+}3c{+}a \ldots$. Since the group Z_{10} is commutative we obtain $\ldots 3a + c + 3b \cdots = \ldots 3b + c + 3a \ldots$ or $\ldots a + 3c + b \cdots = \ldots b + 3c + a \ldots$. Therefore EAN code does not detect "jump transpositions errors".

The EAN code does not detect twin errors $(\dots aa\cdots \to \dots bb\dots)$ for $|a-b| = 5$. Really, passing to group operation, we obtain the following expressions $\cdots + 3a + a + \cdots = \cdots + 4a\dots$, $\cdots + 3b + b + \cdots = \cdots + 4b + \dots$ or $\cdots + a + 3a + \cdots = \cdots + 4a + \dots$, $\cdots + b + 3b + \cdots = \cdots + 4b + \dots$.

In the case when $4a = 4b$ the EAN code will not detect this twin error. We can re-write the last equality in such form $4(a-b) \equiv 0 \pmod{10}$. Therefore $(a-b) \equiv 0 \pmod 5$, $|a-b| = 5$ since $a, b \in \{0,1,2,3,4,5,6,7,8,9\}$.

By analogy it is possible to prove that the EAN code can not detect and jump twin errors $(\dots aca\cdots \to \dots bcb\dots)$ for any pair of elements $a, b \in Z_{10}$ such that $|a-b| = 5$.

Therefore the EAN code does not detect adjacent transpositions, twin errors, jump twin errors for any pair of elements $a, b \in Z_{10}$ such that $|a-b| = 5$ and it does not detect jump transposition for any pair of elements $a, b \in Z_{10}$.

We propose the following code with the check equation

$$x_1 + 3x_2 + 9x_3 + 7x_4 + x_5 + 3x_6 + 9x_7 + 7x_8 + x_9 + 3x_{10} + 9x_{11} + 7x_{12} + x_{13} = 0$$

where $x_i \in Z_{10}, i \in \overline{1,13}$ as a small modification of EAN code. For convenience we shall call it as *the EAN-1 code*.

As it follows from Theorem 3 the EAN-1 code detects all single errors since multiplication of elements of the group Z_{10} by elements 1, 3, 7, 9 is automorphism of this group.

The EAN-1 code does not detect transposition errors, jump transposition errors, twin errors for any pair of elements $a, b \in Z_{10}$ such that $|a-b| = 5$ and it does not detect jump twin errors for any pair of elements $a, b \in Z_{10}$.

Our computer investigations show that there is not an anti-commutative quasigroup $(Z_{10}, \circ)$ of the form $x \circ y = \alpha x + y$ over the group Z_{10} with $\alpha \in S_{10}$, but there exist more than 140.000 of totally anti-commutative quasigroups of the form $x \circ y = \alpha x + \beta y$ over the group Z_7 with $\alpha, \beta \in S_7$.

Example 3. We can propose a code $\mathfrak{C}$ over Z_{10} with the following check equation:

$$x_1 + \alpha x_2 + \beta x_3 + x_4 + \alpha x_5 + \beta x_6 + \cdots \equiv 0 \pmod{10},$$

where $\alpha = (0\,8\,7\,6\,3\,9\,1\,2\,5)(4)$, $\beta = (0\,4\,5\,7\,8\,1\,6\,3\,2)(9)$.

This code does not detect two transposition errors, two jump transposition errors, not more than eight twin errors and jump twin errors on any place of form $(i, i+1), (i, i+2)$.

Proof. Cayley tables of quasigroups $x \cdot y = x + \alpha y$, $x \circ y = \alpha x + \beta y$ and $x * y = \beta x + y$ are the following:

$\cdot$	0	1	2	3	4	5	6	7	8	9
0	8	2	5	9	4	0	3	6	7	1
1	9	3	6	0	5	1	4	7	8	2
2	0	4	7	1	6	2	5	8	9	3
3	1	5	8	2	7	3	6	9	0	4
4	2	6	9	3	8	4	7	0	1	5
5	3	7	0	4	9	5	8	1	2	6
6	4	8	1	5	1	6	9	2	3	7
7	5	9	2	6	2	7	0	3	**4**	8
8	6	0	3	7	3	8	1	**4**	5	9
9	7	1	4	8	4	9	2	5	6	0

$\circ$	0	1	2	3	4	5	6	7	8	9
0	2	4	8	0	3	5	1	6	9	7
1	6	8	2	4	7	9	5	0	**3**	1
2	9	1	5	7	0	2	8	3	6	4
3	3	5	9	1	4	6	2	7	0	8
4	8	0	4	6	9	1	7	2	5	3
5	4	6	0	2	5	7	3	8	1	9
6	7	9	3	5	8	0	6	1	4	2
7	0	2	6	8	1	3	9	4	7	5
8	1	**3**	7	9	2	4	0	5	8	6
9	5	7	1	3	6	8	4	9	2	0

$*$	0	1	2	3	4	5	6	7	8	9
0	4	5	6	7	8	9	0	1	2	3
1	6	7	8	9	0	1	2	3	4	5
2	0	1	2	3	4	5	6	7	8	9
3	2	3	4	5	6	7	8	9	0	1
4	5	6	7	8	9	0	1	**2**	3	4
5	7	8	9	0	1	2	3	4	5	6
6	3	4	5	6	7	8	9	0	1	2
7	8	9	0	1	**2**	3	4	5	6	7
8	1	2	3	4	5	6	7	8	9	0
9	9	0	1	2	3	4	5	6	7	8

In the quasigroup $(Q, \cdot)$ only elements 7 and 8 are permutable: $8 \cdot 7 = 7 \cdot 8 = 4$. Therefore this code does not detect only transposition errors $78 \to 87$ and $87 \to 78$ on places of the form $(1+3j; 2+3j)$ for any suitable j. On these places this code does not detect the following twin errors $00 \leftrightarrow 44$ (i.e. $00 \to 44$, $44 \to 00$), $11 \leftrightarrow 77$, $55 \leftrightarrow 88$.

In the quasigroup $(Q, \circ)$ only the elements 1 and 8 are permutable. Therefore the code $\mathfrak{C}$ does not detect transposition errors $18 \leftrightarrow 81$ on places of the form $(2 + 3j; 3 + 3j)$ for any suitable j. On these places the code does not detect and twin errors $11 \leftrightarrow 88$.

Only the elements 4 and 7 commute in the quasigroup $(Q, *)$. Therefore the code $\mathfrak{C}$ does not detect transposition errors $47 \leftrightarrow 74$ on places of the form

$(3+3j;4+3j)$ for any suitable j. On these places the code does not detect the following eight twin errors: $33 \leftrightarrow 77$, $44 \leftrightarrow 66 \leftrightarrow 88$.

On places of the form $(1+3j, 3+3j)$ code $\mathfrak{C}$ can not detect the same set errors as on the places of the form $(3+3j;4+3j)$, on places of the form $(2+3j, 4+3j)$ code $\mathfrak{C}$ can not detect the same set errors as on the places of the form $(1+3j;2+3j)$ and on places of the form $(3+3j, 5+3j)$ code $\mathfrak{C}$ can not detect the same set errors as on the places of the form $(2+3j;3+3j)$.

Example 4. Let $(Z_{2n+1}, +)$ is a cyclic group of order $(2n+1) \geq 7$ and the number $2n+1$ is prime. An n-ary quasigroup code (Z_{2n+1}, d) with check equation

$$1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + \cdots + n \cdot x_n + 1 \cdot x_{n+1} + 2 \cdot x_{n+2} + \cdots \equiv 0 \pmod{2n+1}$$

where element 0 is identity element of the group $(Z_{2n+1}, +)$ detects single errors, any transposition and twin errors on places $(i, i+1)$, $(i, i+2)$ for all suitable values of natural number i.

Proof. It is known that multiplying of elements of the group $(Z_{2n+1}, +)$ ($2n+1$ is prime number) on element k, $k \in \{1, 2, 3, \ldots, 2n\}$, is an automorphism of the group Z_{2n+1}.

Taking into consideration Theorem 3 we only have to show that the following sums of automorphisms of the group $(Z_{2n+1}, +)$ $1+2=3, 1+3=4, 2+3=5, \ldots, n-1+n=2n-1, \ldots, 1-2=-1, 1-3=-2, \ldots, n-1-1=n-2, n-1, n-2$ are automorphisms of the group $(Z_{2n+1}, +)$. Easy to see that it is so.

Therefore our code can detect all single errors, transposition and twin errors on places $(i, i+1)$, $(i, i+2)$ for any suitable value of i.

Example 5. Let $(Z_p, +)$ be a cyclic group of prime order $p \geq 7$. An $(n-1)$-ary quasigroup code (Z_p, d) with the check equation

$$1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 1 \cdot x_4 + 2 \cdot x_5 + 3 \cdot x_6 + \cdots + \alpha x_n \equiv 0 \pmod{p}$$

where elements x_1^{n-1} are information symbols and element x_n is a check character, ($\alpha = 1$, if $n = 3k+1$, $\alpha = 2$, if $n = 3k+2$, $\alpha = 3$, if $n = 3k$) detects any transposition and twin error on places $(i, i+1)$ where $i \in \overline{1, n-1}$, $(i, i+2)$ where $i \in \overline{1, n-2}$.

Proof. Taking into consideration Theorem 3 we only have to show that the following sums of automorphisms of the group $(Z_p, +)$ $1+2=3, 1+3=4, 2+3=5, 1-2=-1=p-1, 1-3=-2=p-2, 2-3=-1=p-1, 2-1=$

$1, 3-1 = 2, 3-2 = 1$ are automorphisms of the group $(Z_p, +)$. Since multiplication of elements of the group Z_p on numbers $1, 2, 3, 4, 5, p-2, p-1$ are automorphisms of the group $(Z_p, +)$ our code can detect all single errors, transposition and twin errors on places $(i, i+1)$ where $i \in \overline{1, n-1}$, $(i, i+2)$ where $i \in \overline{1, n-2}$.

Example 6. Let $(Q, +) = (Z_p \times Z_p, +)$ where p is prime number. For example, let $p = 2$ (minimal possible value of p) or $p = 5$. Let

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \ \gamma = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

It is well known that these maps are automorphisms of the group $(Z_p \times Z_p, +)$, see, for example, [64].

An $(n-1)$-ary quasigroup code (Q, d) with check equation

$$\alpha x_1 + \beta x_2 + \gamma x_3 + \alpha x_4 + \beta x_5 + \cdots + \delta x_n = 0$$

where elements x_1^{n-1} are information symbols and element x_n is check character, $x_1^n \in Q$, ($\delta = \alpha$, if $n = 3k+1$, $\delta = \beta$, if $n = 3k+2$, $\delta = \gamma$, if $n = 3k$) detects any transposition and twin errors on places $(i, i+1)$ where $i \in \overline{1, n-1}$ and on places $(i, i+2)$ where $i \in \overline{1, n-2}$.

Proof. Taking into consideration Theorem 3 we only have to show that the following sums of automorphisms $\alpha + \beta$, $\alpha - \beta$, $\beta - \alpha$, $\alpha + \gamma$, $\alpha - \gamma$, $\gamma - \alpha$, $\beta + \gamma$, $\beta - \gamma$, $\gamma - \beta$ are automorphisms of the group $(Z_p \times Z_p, +)$.

As usually $det(\alpha)$ means determinant of the matrix α. We have $det(\alpha + \beta) = 1$, $det(\alpha - \beta) = -1$, $det(\beta - \alpha) = -1$, $det(\alpha + \gamma) = 1$, $det(\alpha - \gamma) = -1$, $det(\gamma - \alpha) = -1$, $det(\beta + \gamma) = -3$, $det(\beta - \gamma) = -1$, $det(\gamma - \beta) = -1$. Therefore all these sums of automorphisms are automorphisms of the group $(Z_p \times Z_p, +)$, too.

Thus our code can detect all single errors, transposition and twin errors on places $(i, i+1)$ where $i \in \overline{1, n-1}$ and on places $(i, i+2)$ where $i \in \overline{1, n-2}$.

Example 7. Let $(Z_p, +)$, $(Z_q, +)$ are cyclic groups of prime order $p, q \geq 7$. An $(n-1)$-ary quasigroup code $(Q, d) = (Z_p \times Z_q, d)$ with the check equation

$$1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 1 \cdot x_4 + 2 \cdot x_5 + 3 \cdot x_6 + \cdots + \alpha x_n \equiv 0 \pmod{pq}$$

where binary operation $+$ is the operation of the group $(Z_p \times Z_q, +)$, elements x_1^{n-1} are information symbols and element x_n is a check character, $x_1^n \in Q$,

$\alpha = 1$, if $n = 3k + 1$, $\alpha = 2$, if $n = 3k + 2$, $\alpha = 3$, if $n = 3k$ detects any transposition and twin error on places $(i, i + 1)$ where $i \in \overline{1, n - 1}$, $(i, i + 2)$ where $i \in \overline{1, n - 2}$.

Proof. We can take into consideration Theorem 4 and Example 5.

Example 8. An $(n-1)$-ary quasigroup code $(Q, d) = (Z_p \times Z_p \times Z_q, d)$ with the check equation

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \alpha_3 \cdot x_3 + \alpha_1 \cdot x_4 + \alpha_2 \cdot x_5 + \alpha_3 \cdot x_6 + \cdots + \delta x_n = 0$$

where elements x_1^{n-1} are information symbols and element x_n is a check character, $x_1^n \in Q$, $\delta = \alpha_1$, if $n = 3k + 1$, $\delta = \alpha_2$, if $n = 3k + 2$, $\delta = \alpha_3$, if $n = 3k$ detects any transposition and twin error on places $(i, i + 1)$ where $i \in \overline{1, n - 1}$ and on places of the form $(i, i + 2)$ where $i \in \overline{1, n - 2}$, $\alpha_1 x_i = (\alpha x'_i; 1 \cdot y'_i)$, $\alpha_2 x_i = (\beta x'_i; 2 \cdot y'_i)$, $\alpha_3 x_i = (\gamma x'_i; 3 \cdot y'_i)$ where α, β, γ are defined as in Example 6, $x'_i \in Z_p \times Z_p$, $y'_i \in Z_q$.

Proof. We can take into consideration Theorem 4 and Examples 6, 7. In other words we construct this code taking direct product of codes defined in Examples 6 and 7.

9 On some known possible applications of quasigroups in cryptology

9.1 Introduction

Almost all results obtained in branch of application of quasigroups in cryptology and coding theory to the end of eighties years of the XX-th century are described in [34, 35]. In the present survey the main attention is devoted more late articles in this direction.

Basic facts on quasigroup theory it is possible to find in these lectures and in more details [12, 13, 14, 95]. Information on basic fact in cryptology it is possible to find in many books see, for example, [8, 25, 87, 79].

Cryptology is a science that consists form two parts: cryptography and cryptanalysis. Cryptography is a science on methods of transformation (ciphering) of information with the purpose of a protection this information from an unlawful user. Cryptanalysis is a science on methods and ways of breaking down of ciphers ([46]).

In some sense cryptography is a "defense", i.e. this is a science on construction of new ciphers, but cryptanalysis is an "attack", i.e. this is a science and some kind "art", a set of methods on breaking of ciphers. This situation is similar to situation with intelligence and contr-intelligence.

These two objects (cryptography and cryptanalysis) are very closed and there does not exist a good cryptographer that do not know methods of cryptanalysis.

It is clear, that cryptology depends from a level of development of a society and a level of development of technology.

We recall, a cipher is a way (a method, an algorithm) of a transformation of information with purpose of its defense. A key is some hidden part (a little bit, usually) or parameter of a cipher.

Steganography is a set of means and methods of hiddenness of a fact of sending (or passing) of information, for example, a communication or a letter. Now there exist methods of hiddenness of a fact of sending information by usual post, by e-mail post and so on.

In this survey Coding Theory (Code Theory) will be meant a science on defense of information from accidental errors by transformation and sending (passing) this information.

By sending of important and confidential information, as it seems us, there exists a sense to use methods of Code Theory, Cryptology, and Steganography all together.

In cryptology often one uses the following Kerkhoff's (1835-1903) rule: an opponent (an unlawful user) knows all ciphering procedure (sometimes a part of plaintext or ciphertext) with exception of a key.

Many authors of books devoted cryptology divide this science (sometimes and do not taking for attention this fact) on two parts: before article of Diffie and Hellman ([44]) (so-called cryptology with non-public (symmetric) key) and past this work (a cryptology with public or non-symmetric key). Especially fast development of the second part of cryptology is connected with very fast development of Personal Computers and Nets of Personal Computers, other electronics technical devices in the end of XX-th century. Many new mathematical, cryptographical problems are appeared in this direction and some of them have not solved. Solving of these problems have big importance for practice.

Almost all known construction of error detecting and error correcting codes, cryptographic algorithms and enciphering systems have made use of associative algebraic structures such as groups and fields, see, for example,

[81]. There exists a possibility to use such non-associative structures as quasigroups and neofields in almost all branches of coding theory, and especially in cryptology.

Codes and ciphers based on non-associative systems show better possibilities than known codes and ciphers based on associative systems [36, 76].

There is a sense to notice that in the last years the quantum code theory and quantum cryptology ([106, 54, 114]) have been developed intensively.

Efficacy of applications of quasigroups in cryptology is based on the fact that quasigroups are "generalized permutations" of some kind and the number of quasigroups of order n is larger than $n! \cdot (n-1)! \cdot ... \cdot 2! \cdot 1!$ ([34]).

It is worth noting that several of the early professional cryptographers, in particular, A.A. Albert, A. Drisko, J.B. Rosser, E. Schönhardt, C.I. Mendeson, R. Schaufler, M.M. Gluhov were connected with the development of Quasigroup Theory. The main known "applicants" of quasigroups in cryptology were and are J.Denes and A.D. Keedwell [34, 35, 36].

Of course, one of the most effective cipher methods is to use unknown, non-standard or very rare language. Probably the best enciphering method was and is to have a good agent (a good spy).

9.2 Application of quasigroups in "classical" cryptology

There exist two main elementary methods by ciphering of information.

(i). Symbols in a plaintext (or in its piece (its bit)) are permuted by some law. The first known cipher of such kind is cipher "Scital" (Sparta, 2500 years ago).

(ii). All symbols in a fixed alphabet are changed by a law on other letters of this alphabet. One of the first ciphers of such kind was Cezar's cipher ($x \to x+3$ for any letter of Latin alphabet, for example $a \to d, b \to d$ and so on).

In many contemporary ciphers (DES, Russian GOST, Blowfish ([87, 45])) are used methods (i) and (ii) with some modifications.

Trithemius cipher makes use of 26×26 square array containing the 26 letters of alphabet (assuming that the language is English) arranged in a Latin square. Different rows of this square array are used for enciphering the various letters of the plaintext in a manner prescribed by the keyword or key-phrase ([8, 63]). Since a Latin square is the multiplication table of

a quasigroup, this may be regarded as the earliest use of a non-associative algebraic structure in cryptology. There exists a possibility to develop this direction using quasigroup approach, in particular, using orthogonal systems of binary or n-ary quasigroups.

R. Schaufler in his Ph.D. dissertation ([97]) of 1948 discussed the minimum amount of plaintext and corresponding ciphertext which would be required to break the Vigenere cipher (i.e. Trithemius cipher). That is, he considered the minimum member of entries of particular Latin square which would determine the square completely.

Recently this problem has re-arisen as the problem of determining so-called critical sets in Latin squares, see [68, 30, 31, 32, 33], and, possibly, future A.D. Keedwell's survey on BCC'03. See, also, articles, devoted Latin trades, for example, [10].

More recent enciphering systems which may be regarded as extension of Vigenere's idea are mechanical machines such as Jefferson's wheel and the M-209 Converter (used by U.S.Army until the early 1950's) and the electronically produced stream ciphers of the present day ([75, 87]). We recall, a cipher is called a stream cipher, if by ciphering of a block (a letter) B_i of a plaintext is used the previous ciphered block C_{i-1}.

In [75] (see also [76, 77]) C. Koscielny has shown how quasigroups/neofields-based stream ciphers may be produced which are both more efficient and more secure than those based on groups/fields.

In [83] the authors introduce a stream cipher with almost public key, based on quasigroups for defining suitable encryption and decryption. They consider the security of this method. It is shown that the key (quasigroups) can be public and still having sufficient security. A software implementation is also given.

In [78] a public-key cryptosystem, using generalized quasigroup-based streamciphers is presented. It is shown that such a cryptosystem allows one to transmit securely both a cryptogram and a secret portion of the enciphering key using the same insecure channel. The system is illustrated by means of a simple, but nontrivial, example.

During the second World War R.Shauffler while working for the German Cryptography service, developed a method of error detection based on the use of generalized identities (as they were later called by V.D. Belousov) in which the check digits are calculated by means of an associative system of quasigroups (see also [28]). He pointed out that the resulting message would

be more difficult to decode by unauthorized receiver than is the case when a single associative operation is used for calculation ([98]).

Therefore it is possible to assume that information on systems of quasigroups with generalized identities (see, for example, works of Yu. Movsisyan ([88]) may be applied in cryptography of the present day.

Definition. A bijective mapping $\varphi : g \rightarrowtail \varphi(g)$ of a finite group $(G, \cdot)$ onto itself is called an orthomorphism if the mapping $\theta : g \rightarrowtail \theta(g)$ where $\theta(g) = g^{-1}\varphi(g)$ is again a bijective mapping of G onto itself. The orthomorphism is said to be in canonical form if $\varphi(1) = 1$ where 1 is the identity element of $(G, \cdot)$.

A direct application of group orthomorphisms to cryptography is described in [85, 86].

9.3 "Neo-classic" cryptology and quasigroups

In [36] some applications of CI-quasigroups in cryptology with non-symmetric key are described.

Definition. Suppose that there exists a permutation J of the elements of a quasigroup $(Q, \circ)$ such that, for all $x, y \in Q$ $J^r(x \circ y) \circ J^s x = J^t y$, where r, s, t are integers. Then $(Q, \circ)$ is called an (r, s, t)-inverse quasigroup ([69]).

In the special case when $r = t = 0$, $s = 1$, we have a definition of CI-quasigroup.

Example ([36, 67]). A CI-quasigroup can be used to provide a one-time pad for key exchange (without the intervention of a key distributing center).

The sender S selects arbitrary (using a physical random number generator (see [76] on random number generator based on quasigroups) an element $c^{(u)}$ of the CI-quasigroup $(Q, \circ)$ and sends both $c^{(u)}$ and enciphered key (message) $c^{(u)} \circ m$. The receiver R uses this knowledge of the algorithm for obtaining $Jc^{(u)} = c^{(u+1)}$ from $c^{(u)}$ and hence he computes $(c^{(u)} \circ m) \circ c^{(u+1)} = m$.

Remark. In previous example Kerkhof's rule is not fulfilled, so, this example need to be improved. Maybe there exists a sense to use in this example, as and in the next example rst-inverse quasigroups.

Example ([36]). A CI-quasigroup with a long inverse cycle $(c\, c'\, c'' \ldots c^{t-1})$ of length t and suppose that all the users U_i $(i = 1, 2, \ldots)$ are provided with apparatus (for example, a chip card) which will compute $a \circ b$ for any given $a, b \in Q$. We assume that only the key distributing center has a knowledge of the long inverse cycle which serves as a look-up table for keys.

Each user U_i has a public key $u_i \in Q$ and a private key Ju_i, both supplied in advance by the key distributing center. User U_s wishes to send a message m to user U_t. He uses U_t's public key u_t to compute $u_t \circ m$ and sends that to U_t. U_t computes $(u_t \circ m) \circ Ju_t = m$.

Remark. It is not very difficult to understand that opponent which knows the permutation J may decipher a message encrypted by this method.

9.3.1 Secret sharing systems

Definition ([79]). A critical set C in a Latin square L of order n is a set $C = \{(i; j; k) \mid i, j, k \in \{1, 2, \ldots, n\}\}$ with the following two properties:

(1) L is the only Latin square of order n which has symbols k in cell (i, j) for each $(i; j; k) \in C$;

(2) no proper subset of C has property (1).

A critical set is called minimal if it is a critical set of smallest possible cardinality for L. In other words a critical set is a partial Latin square which is supplemented uniquely to a Latin square of order n.

If the scheme has k participants, a (t, k)-secret sharing scheme is a system where k pieces of information called shares or shadows of a secret key K are distributed so that each participant has a share such that

(1) the key K can be reconstructed from knowledge of any t or more shares;

(2) the key K cannot be reconstructed from knowledge of fewer than t shares.

Such systems were first studied in 1979. Simmons ([107]) surveyed various secret sharing schemes. Secret sharing schemes based on critical sets in Latin squares are studied in [26]. We note, critical sets of Latin squares give rise possibilities to construct secret-sharing systems.

Critical sets of Latin squares were studied in sufficiently big number of articles. We survey results from some of these articles. The paper ([44]) gives constructive proofs that critical sets exist for all sizes between $[n^2/4]$ and $[(n^2 - n)/2]$, with the exception of size $n^2/4 + 1$ for n even.

In the paper [30] presents a solution to the interesting combinatorial problem of finding a minimal number of elements in a given Latin square of odd order n by which one may restore the initial form of this square. In particular, it is proved that in every cyclic Latin square of odd order n the minimal number of elements equals $n(n - 1)/2$.

The paper [31] contains lists of (a) theorems on the possible sizes of critical sets in Latin squares of order less than 11, (b) publications, where these theorems are proved, (c) concrete examples of such type of critical sets. In [32] an algorithm for writing any Latin interchange as a sum of intercalates is corrected.

Remark. See also Introduction for other application of critical sets of Latin squares in cryptology.

Some secret-sharing systems are pointed in [35]. One of such systems is the Reed-Solomon code over a Galois field $GF[q]$ with generating matrix $C(a_{ij})$ of size $k \times (q-1)$, $k \leq q-1$. The determinant formed by any k columns of G is a non-zero element of $GF[q]$. The Hamming distance d of this code is maximal ($d = q-k$) and any k from $q-1$ keys unlock the secret.

In [18] an approach to some Reed-Solomon codes as a some kind of orthogonal systems of n-ary operations is developed.

There exist generalizations of notion of orthogonality in some directions. We recall that in [19, 35] notion of partial orthogonality for binary quasigroups is studied. On application of this notion in code theory see [34]. Notion of partial orthogonality has good perspectives in cryptology (private communication from Russian mathematicians).

9.3.2 Cryptosystems based on power sets of Latin squares and on row-Latin squares

A Latin square is an arrangement of m symbols $x_1, x_2, \ldots, x_m$ into m rows and m columns such that no row and no column contains any of the symbols $x_1, x_2, \ldots, x_m$ twice. It is well known that Cayley table of any finite quasigroup is a Latin square ([34]).

Two Latin squares are called orthogonal if when one is superimposed upon the other every ordered pair of symbols $x_1, x_2, \ldots, x_m$ occurs once in the resulting square.

Each row and column of a Latin square L of order m can be thought of as a permutation of the elements of an m-set. The product of two Latin squares L_1 and L_2 of order m is an $m \times m$ matrix whose ith row is the composition of the permutations comprising the ith rows of L_1 and L_2. Pick the smallest positive m such that $L^{m+1} = L$.

In general product of two Latin squares is row Latin square since in row-Latin square only rows are permutations of the set $x_1, x_2, \ldots, x_m$. If $L, L^2, \ldots, L^{m-1}$ are all Latin squares, then they form a set called a Latin

power set. D. A. Norton ([91]) has shown that the Latin squares in a Latin power set are mutually orthogonal.

Power sets of Latin squares were studied in [40], [20].

The authors of article [40] conjecture that if $n \neq 2$ or 6 then there exists a Latin power set consisting of at least two Latin squares of order n. This would provide another disproof of the Euler conjecture that a pair of orthogonal Latin squares fails to exist for orders $n \equiv 2 \pmod 4$. The authors use resolvable Mendelsohn triple systems to establish their conjecture if $n \geq 7$ and $n \equiv 0, 1 (\text{mod } 3)$. The authors also discuss some related conjectures.

A possible application in cryptology of Latin power sets is proposed in [39].

In [43] an encrypting device is described, based on row-Latin squares with maximal period equal to the Mangoldt function.

In our opinion big perspectives has an application of row-Latin squares in various branches of contemporary cryptology ("neo-cryptology"). In [79] it is proposed to use row-Latin squares to generate an open key, a conventional system for transmission of a message that is the form of a Latin square, row-Latin square analogue of the RSA system and on row-Latin squares based procedure of digital signature.

Example.

Let

$$L = \begin{matrix} 2 & 3 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 3 & 2 & 4 & 1 \\ 4 & 3 & 1 & 2 \end{matrix}.$$

Then

$$L^7 = \begin{matrix} 4 & 1 & 2 & 3 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 3 & 4 & 2 & 1 \end{matrix},$$

$$L^3 = \begin{matrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{matrix}.$$

Then

$$L^{21} = \begin{matrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{matrix}$$

is a common key for a user A with the key L^3 and a user B with key L^7.

9.3.3 NLPN sequences over GF[q]

Non-binary pseudo-random sequences over GF[q] of length $q^m - 1$ called PN sequences have been known for a long time ([57]). PN sequences over a finite field GF[q] are unsuitable directly for cryptology because of their strong linear structure ([76]). Usually PN sequences are defined over a finite field and often it is used an irreducible polynomial for their generation.

In article [76] definition of PN sequence was generalized with the purpose to use this sequences in cryptology.

We notice, in some sense ciphering is making a "pseudo-random sequence" from a plaintext, and cryptanalysis is a science how to reduce a check of all possible variants (cases) by deciphering of some ciphertext.

These new sequences were called NLPN-sequences (non-linear pseudo-noise sequences). C.Koscielny proposed the following method for construction of NLPN-sequences. Let $\overrightarrow{a}$ be a PN sequence of length $q^m - 1$ over GF[q], $q > 2$. Let $\overrightarrow{a}^i$ be its cyclic shift i places to the right. Let $Q = (SQ, \cdot)$ be a quasigroup of order q defined on the set of elements of the field GF[q]. Then $\overrightarrow{b} = \overrightarrow{a} \cdot \overrightarrow{a}^i$, $\overrightarrow{c} = \overrightarrow{a}^i \cdot \overrightarrow{a}$, where $b_j = a_j \cdot a_j^i$, $c_j = a_j^i \cdot a_j$ for any suitable value of index j ($j \in \{1, 2, \ldots, q^m - 1\}$) are called NLPN sequences.

NLPN sequences have much more randomness than PN sequences. As notice C.Koscielny the method of construction of NLPN sequences is especially convenient for fast software encryption. It is proposed to use NLPN sequences by generation of keys. See also [73].

9.3.4 Quasigroups and authentication of a message and some other problems

By authentication of message we mean that it is made possible for a receiver of a message to verify that the message has not been modified in transit, so that it is not possible for an interceptor to substitute a false message for a legitimate one.

By identification of a message we mean that it is made possible for the receiver of a message to ascertain its origin, so that it is not possible for an intruder to masquerade as someone else.

By non-repudiation we mean that a sender should not be able later to deny falsely that he had sent a message.

In [36] some quasigroup approaches to problems of identification of a message, problem of non-repudiation of a message, production of dynamic password and to digital fingerprinting are discussed. See also [27].

In [37] authors suggested a new authentication scheme based on quasigroups (Latin squares). See also [35, 36, 29]

In [96] several cryptosystems based on quasigroups upon various combinatorial objects such as orthogonal Latin squares and frequency squares, block designs, and room squares are considered.

Let $2 \leq t < k < v$. A generalized $S(t, k, v)$ Steiner system is a finite block design $(T, \mathcal{B})$ such that (1) $|T| = v$; (2) $\mathcal{B} = \mathcal{B}' \cup \mathcal{B}''$, where any $B' \in \mathcal{B}'$, called a maximal block, has k points and $2 \leq |B''| < k$ for any $B'' \in \mathcal{B}''$, called a small block; (3) for any $B'' \in \mathcal{B}''$ there exists a $B' \in \mathcal{B}'$ such that $B'' \subseteq B'$; (4) every subset of T with t elements not belonging to the same $B'' \in \mathcal{B}''$ is contained in exactly one maximal block.

In [84] (see also [55]) an application of generalized $S(t, k, v)$ Steiner systems in cryptology is proposed, namely, it is introduced a new authentication scheme based on the generalized Steiner systems, and the properties of such scheme are studied in the generalized affine planes. The generalized affine planes are investigated, in particular, it is proved that they are generalized $S(2, n, n^2)$ Steiner systems. Some important cases of generalized Steiner systems are the generalized affine planes considered by the authors.

9.3.5 Hamming distance between quasigroups

Very important by construction of quasigroup based cryptosystems is a question: how big distance is between different binary or n-ary quasigroups? Information on Hamming distance between quasigroup operation there is in the articles [47, 48, 49, 50, 51, 52, 113].

We recall, if α and β are two n-ary operations on a finite set Ω, then the Hamming distance of α and β is defined by $\mathrm{dist}(\alpha, \beta) = |\{(u_1, \ldots, u_n) \in \Omega^n : \alpha(u_1, \ldots, u_n) \neq \beta(u_1, \ldots, u_n)\}|$.

The author in [47] discusses Hamming distances of algebraic objects with binary operations. He also explains how the distance set of two quasigroups

yields a 2-complex, and points out a connection with dissections of equilateral triangles.

For a fixed group $G(\circ)$, $\delta(G(\circ))$ is defined to be the minimum of all such distances for $G(\star)$ not equal to $G(\circ)$ and $\nu(G(\circ))$ the minimum for $G(\star)$ not isomorphic to $G(\circ)$.

In [50] it is proved that $\delta(G(\circ))$ is $6n-18$ if n is odd, $6n-20$ if $G(\circ)$ is dihedral of twice odd order and $6n-24$ otherwise for any group $G(\circ)$ of order greater than 50. In [113] it is showed that $\delta(G(\circ)) = 6p-18$ for $n = p$, a prime, and $p > 7$. In the article [49] are listed a number of group orders for which the distance is less than the value suggested by the above theorems.

New results obtained in this direction there are in [52].

9.3.6 On one-way function

A function $F : X \to Y$ is called one-way function, if the following conditions are fulfilled:

- there exists a polynomial algorithm of calculation of $F(x)$ for any $x \in X$;
- there does not exist a polynomial algorithm of inverting of the function F, i.e. there does not exist any polynomial time algorithm for a solving of equation $F(x) = y$ relatively variable x.

It is proved that the problem of the existence of one-way function is equivalent to well known problem of coincidence of classes P and NP.

One of better candidates to be an one-way function is so-called function of discrete logarithms ([79]).

A neofield $(N, +, \cdot)$ of order n consists of a set N of n symbols on which two binary operations $+$ and $\cdot$ are defined such that $(N, +)$ is a loop with identity element 0 say, $(N\backslash\{0\}, \cdot)$ is a group and $\cdot$ distributes from the left and right over $+$ ([36]).

Let $(N, +, \cdot)$ be a finite Galois field or a cyclic ($(N\backslash\{0\}, \cdot)$ is a cyclic group) neofield. Then each non-zero element u of the additive group or loop $(N, +)$ can be represented in the form $u = a^{\nu}$, where a is a generator of the multiplication group $(N\backslash\{0\}, \cdot)$. ν is called the discrete logarithm of u to the base a, or, sometimes, the exponent or index of u.

Given ν and a, it is easy to compute u in a finite field, but, if the order of the finite field is a sufficiently large prime p and also is appropriately chosen

it is believed to be difficult to compute ν when u (as a residue modulo p) and a are given.

In [36] discrete logarithms are studied over a cyclic neofield whose addition is a CI-loop.

In [79] the discrete logarithm problem for the group RL_n of all row-Latin squares of order n is defined (p.103) and, on pages 138 and 139, some illustrations of applications to cryptography are given.

9.4 Conclusion remarks

In many cases in cryptography it is possible to change associative systems on non-associative ones and practically in any case this change gives in some sense better results than use of associative systems. Quasigroups in spite of their simplicity, have various applications in cryptology. Many new cryptographical algorithms can be formed on the basis of quasigroups.

10 On some Belousov problems

This section is a part of survey [103].

Before conference LOOPS'99 Prof. H.O. Pflugfelder asked on 20 Belousov's problems. These problems are presented at the end of V.D.Belousov's book:

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

In this note some information about these problems is given.

Problem 1a). Find necessary and sufficient conditions that a special loop

is isotopic to a left F–quasigroup.

This problem is solved partially.

I.A. Florea, M.I. Ursul: *F–kvasigruppy so svoistvom obratimosti.* Voprosy teorii kvasigrupp i lup. Kishinev, Shtiintsa, 1970, 145–156.

They proved that a left F–quasigroup with IP property is isotopic to an A–loop.

Problem 1b). Is some identity fulfilled in a special loop?

Yes.

L.R. Soikis: *O spetsial'nyh lupah.* Voprosy teorii kvasigrupp i lup. Kishinev, Shtiintsa, 1970, 122–131.

Problem 1c). To what loops are isotopic two–sided F–quasigroups?

A left (right) F–quasigroup is isotopic to a left (right) M–loop.

V.D. Belousov: *Elementy teorii kvasigrupp.* Uchebnoe posobie po spetskursu. Kishinev, 1981, 115 ss.

Interesting results appear in Kepka's articles.

T. Kepka: *F–quasigroups isotopic to Moufang loops.* Czehoslovak Mathem. Journal, 29, (104), 1979, 62–83.

T. Kepka posed the following problem. All known examples of two-sided F-quasigroup are isotopic to a Moufang loop. Is it true, that every two-sided F-quasigroup is isotopic to a Moufang loop?

Problem 2. Let $Q(\cdot)$ be a group and let $x \circ y = {z_1}^{\varepsilon_1} {z_2}^{\varepsilon_2} \dots {z_n}^{\varepsilon_n}$, where $z_i = x$ or $z_i = y$, $\varepsilon = \pm 1$ $(i = 1, 2, \dots, n)$. For what sequence of values of ε_i groupoid $Q(\circ)$ is a quasigroup?

Partial results there are given in the article

S.V. Larin: *Ob odnoi kvasigruppovoi operatsii na gruppe.* Matem. zapiski Krasnoyarskogo gos. ped. instituta, 1970, vyp. 3, 20–26.

Problem 3. A quasigroup $Q(\cdot)$ is called a Stein quasigroup, if the identity $x \cdot xy = yx$ holds in the quasigroup $Q(\cdot)$. To what loops are isotopic Stein quasigroups?

Semisymmetric ($x \cdot yx = y$) Stein quasigroup is isotopic to loop of exponent 2; see:

G.B. Belyavskaya, A.M. Cheban: *O polusimmetricheskih kvasigruppah Steina.* Matem. issledov. VII:3(25), 1972, 231–237.

General case: it is not known anything to us.

Acknowledgement. The author wish to thank Prof. Alesh Drapal which has found an opportunity to invite him in Charles University (Prague, Czech Republic).

References

[1] A. Akritis, *Foundations of Computer Algebra with Applications.* Mir, Moscow, 1994 (in Russian).

[2] A.A. Albert: Quasigroups I, *Trans. Amer. Math. Soc.*, **54**(1943), 507 - 519.

[3] A.A. Albert: Quasigroups II, *Trans. Amer. Math. Soc.*, **55**(1944), 401 - 419.

[4] R. Artzy: Crossed-inverse and related loops, *Trans. Amer. Math. Soc.*, **91**(1959), 480 - 492.

[5] M.N. Arshinov, L.E. Sadovskii, *Codes and Mathematics.* Nauka, Moscow, 1983 (in Russian).

[6] R. Baer: Nets and groups, I, *Trans. Amer. Math. Soc.*, **46**(1939), 110 - 141.

[7] R. Baer: Nets and groups, II, *Trans. Amer. Math. Soc.*, **47**(1940), 435 - 439.

[8] H.J. Baker and F.Piper, *Cipher Systems: the Protection of Communications.* Northwood, London, 1982.

[9] G.E. Bates, F. Kiokemeister: A note on homomorphic mappings of quasigroups into multiplicative systems, *Bull. Amer. Math. Soc.* **54**(1948), 1180-1185.

[10] R. Bean, D. Donovan, A. Khodkar, A.P. Street, *Steiner trades that give rise to completely decomposable Latin interchanges,* Int. J. Comput. Math. 79, No.12, 2002, 1273-1284.

[11] D.F. Beckley, *An optimum systems with modulo 11*, The Computer Bulletin, 11, pp. 213-215, (1967).

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

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

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

[15] V.D. Belousov: *Balanced identities on quasigroups*, Mat. sbornik, **70 (112):1**, (1966), 55-97, (in Russian).

[16] V.D. Belousov: *On a group associated to a quasigroups*, Matem. Issledovaniya, 4:3, Shtiinta, Kishinev, 1969, 21 – 39 (in Russian).

[17] V.D. Belousov: *Inverse quasigroups*, Quasigroups, Mat. Issled., Kishinev, Shtiinta. **95** (1987), 3-22, (in Russian).

[18] G.B. Belyavskaya, *Secret-sharing systems and orthogonal systems of operatins,* Applied and Industrial Mathematics, Abstracts, Chisinau, Moldova, 1995, p. 2.

[19] G.B. Belyavskaya, *On spectrum of partial admissibility of finite quasigroups (Latin squares)*, Matem. Zametki, 32, No. 6, 1982, 777-788.

[20] G.B. Belyavskaya, *Quasigroup power sets and cyclic S-systems*, Quasigroups and Related Systems, 32, V.9, 2002, 1-17.

[21] G. B. Belyavskaya: *Nuclei and center of a quasigroup*, Research of operations and quasigroups, Mat. Issled., Kishinev, Shtiinta. **102** (1988), 37-52, (in Russian).

[22] G. B. Belyavskaya: *Quasigroup theory: nuclei, center, commutants*, Bul. A.Ş. a R.M., matematica, 1996, No. 2(21), pp.47-71 (in Russian).

[23] G.B. Belyavskaya, V.I. Izbash, and G.L. Mullen, *Check character systems using quasigroups,I and II* (preprints).

[24] R.H. Bruck: *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **47**, (1941), 134 – 138.

[25] A. Beutelspacher, *Cryptology: An introduction to the science of encoding, concealing and hiding*, Wiesbaden: Vieweg, 2002, (in German).

[26] J. Cooper, D. Donovan and J. Seberry, *Secret sharing schemes arising from Latin squares*, Bull. Inst. Combin. Appl., 12, 1994, 33-43.

[27] D. Coppersmith, *Weakness in quaternion signatures*, J. Cryptology, 14, 2001, 77-85.

[28] M. Damm, *Prüfziffersysteme über Qasigruppen*, Diplomarbeit, Philipps-Universität Marburg, 1998.

[29] E. Dawson, D. Donowan, A. Offer, *Ouasigroups, isotopisms and authentification schemes*, Australasian J. of Comb., 13, 1996, 75-88.

[30] D. Donowan, *Critical sets for families of Latin squares*, Util. Math. 53, 1998, 3-16.

[31] D. Donowan, *Critical sets in Latin squares of order less than 11*, J. Comb. Math. Comb. Comput. 29, 1999, 223-240.

[32] D. Donowan, E.S. Mahmoodian, *Correction to a paper on critical sets*, Bull. Inst. Comb. Appl. 37, 2003,44.

[33] D. Donowan, A. Howse, *Towards the spectrum of critical sets*, Australasian J. of Comb., 21, 2000, 107-130.

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

[35] J. Dénes, A. D. Keedwell, *Latin Squares: New Development in the Theory and Applications*, Annals of Discrete Math., v.46, Norht Holland, Amsterdam, 1990.

[36] J. Dénes, A. D. Keedwell, *Some applications of non-associative algebraic systems in cryptology*, PU.M.A. 12, No.2, 2002, 147-195.

[37] J. Dénes, A. D. Keedwell, *A new authentification scheme based on Latin squres*,Discrete Math., 106/107, 1992, 157-161.

[38] J. Dénes, *Latin Squares and non-binary encoding*, Proc. conf. information theory, CNRS, Paris, 1979, 215-221.

[39] J. Dénes, P.Petroczki, *A digital encrypting communication systems*, Hungarian Patent, No. 201437A, 1990.

[40] J. Dénes, G.L. Mullen and S.J.Suchower, *A note on power sets of latin squares*, J. Combin. Math. Combin. Computing, 16, 1994, 27-31.

[41] J. Dénes, T. Dénes, *Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack*, Quasigroups and Related Systems, 8, 2001, 7 - 14.

[42] T. Dénes, *Cardano and the cryptography. Mathematics of the enciphering grill*, (Hungarian), Középiskolai Matematikai és Fizikai Lapok, 6, 2001, 325-335.

[43] J. Dénes, *On Latin squares and a digital encrypting communication system* , PU.M.A., Pure Math. Appl. 11, No.4, 2000, 559-563.

[44] W. Diffie, M.F. Hellman, *New directions in Cryptography*, IEEE, Transactions of Information Theory, IT-22. 1976, 644-654.

[45] V. Domashev, V. Popov, D. Pravikov, I. Prokof'ev, A. Shcherbakov, *Programming of algorithms of defense of information*, Nolidge, Moscow, 2000, (in Russian).

[46] S.A. Dorichenko, V.V. Yashchenko, *25 sketches on ciphers*, Teis, Moscow, 1994, (in Russian).

[47] A. Drapal, *Hamming distances of groups and quasi-groups*, Discrete Math. 235, No. 1-3, 2001, 189-197.

[48] A. Drapal, *On groups that differ in one of four squares*, Eur. J. Comb. 23, No. 8, 2002, 899-918.

[49] A. Drapal, *On distances of multiplication tables of groups*, Campbell, C. M. (ed.) et al., Groups St. Andrews 1997 in Bath. Selected papers of the international conference, Bath, UK, July 26-August 9, 1997. Vol. 1. Cambridge: Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 260, 1999, 248-252.

[50] A. Drapal, *How far apart can the group multiplication tables be?*, Eur. J. Comb. 13, No. 5, 1992, 335-343.

[51] A. Drapal, *Non-isomorphic 2-groups Coincide at Most in Three Quartes of their Multiplication Table*, Eur. J. Comb. 21, 2000, 301-321.

[52] A. Drapal, N. Zhukavets, *On multiplication tables of groups that agree on half of the columns and half of the rows*, Glasgow Math. J., 45, 2003, 293-308.

[53] A. Ecker and G. Poch, *Check character systems,* Computing 37/4, p.277-301, (1986).

[54] A. Ekert, *From quantum, code-making to quantum code-breaking,* Huggett, S. A. (ed.) et al., The geometric universe: science, geometry, and the work of Roger Penrose. Proceedings of the symposium on

geometric issues in the foundations of science, Oxford, UK, June 1996 in honour of Roger Penrose in his 65th year. Oxford: Oxford University Press, 1998, 195-214.

[55] F. Eugeni, A. Maturo, *A new authentication system based on the generalized affine planes*, J. Inf. Optimization Sci. 13, No.2, 1992,183-193.

[56] John B. Fraleigh: *A First Course in Abstract Algebra*, Addison-Wesley, London, 1982.

[57] S.W. Golomb, *Shift Register Sequences,* San Francisco, Holden Day, 1967.

[58] S.W. Golomb, R.E. Peile, H. Taylor, *Nonlinear shift registers that produce all vectors of weight* $\leq t$*,* IEEE Trans. Inf. Theory 38, No.3, 1992, 1181-1183.

[59] I.N. Herstein: *Abstract Algebra*, Macmillian Publishing Company, New York, 1990.

[60] D.F. Hsu, *Cyclic neofields and combinatorial designs,* Lectures Notes in Mathematics, 824, Springer, Berlin, 1980.

[61] J. Ježek, T. Kepka: *Varieties of abelian quasigroups*, Czech. Mathem. J., **27**, (1977), $473 - 503$.

[62] J. Ježek, T. Kepka: *Medial groupoids*, Rozpravy Československe Academie VĚD, 1983, Ročnik 93, sešit 2, Academia, Praha.

[63] D. Kahn, *The codebreakers: the story of secret writing,* Wiedenfield and Nicolson, London, 1967.

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

[65] B. B. Karklin´š, V. B. Karklin´: Inverse loops, In "Nets and groups", *Mat. Issled.*(Kishinev) **39**(1976), 87-101.

[66] A. D. Keedwell, V. A. Shcherbacov: On m-inverse loops and quasigroups with a long inverse cycle, *Australasian Journal of Combinatorics,* v.26, 2002, p. 99-119.

[67] A. D. Keedwell, *Crossed inverse quasigroups with long inverse cycles and applications to cryptography*, Australasian J.of Comb., 20, 1999, 241-250.

[68] A. D. Keedwell, *Critical sets for Latin Squares, graphs and block designs: a survey*, Congressus Numeratium, 113, 1996, 231-245.

[69] A.D. Keedwell and V. Shcherbacov, *Construction and properties of (r,s,t)-inverse quasigroups, I,* Discrete Math., 266, 2003, 275-291.

[70] P. Němec, T. Kepka: T-quasigroups. Part I, *Acta Universitatis, Carolinae Math. et Physica.* **12**, no.1, (1971), 39-49.

[71] T. Kepka, P. Němec: T-quasigroups. Part II, *Acta Universitatis, Carolinae Math. et Physica.* **12**, no.2, (1971), 31-49.

[72] M. D. Kitoroagè: *Nuclei in quasigroups*, Mat. Issled. (Kishinev) 7(1972), 60-71 (in Russian).

[73] A. Klapper, *On the existence of secure keystream generators*, J. Cryptology, 14, 2001, 1-15.

[74] P.M. Kohn, *Universal Algebra,* Harper & Row, New York, 1965.

[75] C. Koscielny, *A method of constructing quasigroup-based stream ciphers*, Appl. Math. and Comp. Sci. 6, 1996, 109-121.

[76] C. Koscielny, *NLPN Sequences over GF(q)*, Quasigroups and Related Systems, v.4, 1997, 89-102.

[77] C. Koscielny, *Generating quasigroups for cryptographic applications*, Int. J. Appl. Math. Comput. Sci. 12, No.4, 2002, 559-569.

[78] C. Koscielny, G.L. Mullen *A quasigroup-based public-key cryptosystem*, Int. J. Appl. Math. Comput. Sci. 9, No.4, 1999, 955-963.

[79] Charles F. Laywine and Gary L. Mullen, *Discrete Mathematics Using Latin Squares,* New York, John Wiley & Sons, Inc., 1998.

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

[81] S.S. Magliveras, D.R. Stinson, Tran van Trung, *New approach to designing public key cryptosystems using one-way function and trapdoors in finite groups,* J.Cryptology, 15, 2002, 285-297.

[82] A. Marini, V. Shcherbacov: About signs of Bol loop translations. *Izvestiya AN RM. Matematica.* No 3, 1998, p. 87-92.

[83] S. Markovski, D. Gligoroski, B. Stojcevska, *Secure two-way online communication by using quasigroup enciphering with almost public key,* Novi Sad J. Math. 30, No.2, 2000,43-49.

[84] Antonio Maturo and Mauro Zannetti, *Redei blocking sets with two Redei lines and quasigroups,* J. Discrete Math. Sci. Cryptography 5, No.1, 2002, 51-62.

[85] L. Mittenhal, *Block substitutions using orthomorphic mappings,* Advances in Applied Mathematics, 16, 1995, 59-71.

[86] L. Mittenhal, *A source of cryptographically strong permutations for use in block ciphers,* Proc. IEEE, International Sympos. on Information Theory, 1993, IEEE, New York, 17-22.

[87] N.A. Moldovyan, *Problems and methods of cryptology,* S.-Peterburg, S.-Peterburg University Press, 1998 (in Russian).

[88] Yu. Movsisyan, *Hyperidentities in algebras and varieties,* Russ. Math. Surv. 53, No.1, 1998, 57-108.

[89] Gary L. Mullen, V.A. Shcherbacov, *Properties of codes with one check symbol from a quasigroup point of view,* Izvestiya AN RM. Matematica. No 3, 2002, p. 71–86.

[90] D.C. Murdoch: *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **49**, (1941), 392 – 409.

[91] D. A. Norton, Pac. J. Math. 2, 1952, 335-341.

[92] E. Ochadkova, V. Snasel, *Using quasigroups for secure encoding of file system*, Abstract of Talk on Conference "Security and Protection of information", Brno, Czech Republic, 9-11.05.2001, 24 pages.

[93] V. I. Onoi: Solution of a problem on inverse loops, (in Russian), In "General algebra and discrete geometry", *Shtiintsa*(Kishinev) **71**(1980), 53-58.

[94] M. Osborn: Loops with the weak inverse property, *Pacific J. Math.*, **10**(1960), 295 - 304.

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

[96] D.G. Sarvate and J. Seberry, *Encryption methods based on combinatorial designs,* Ars Combinatoria, 21A, 1986, 237-246.

[97] R. Schauffler, *Eine Anwendung zyklischer Permutationen und ihre Theorie*, Ph.D. Thesis, Marburg University, 1948.

[98] R. Schauffler, *Über die Bildung von Codewörter*, Arch. Elektr. Übertragung, 10, 1956, 303-314.

[99] V.A. Shcherbacov: *On linear quasigroups and their automorphism groups*, Binary and n-ary quasigroups. Mat. Issled., Issue 120, Shtiinta, Kishinev, (1991), $104 - 114$, (in Russian).

[100] V.A. Shcherbacov: *Some properties of full associated group of IP-loop,* Izvestia AN MSSR. Ser. fiz.-techn. i mat. nauk, No. 2, 1984, p. 51-52 (in Russian).

[101] V.A. Shcherbacov: *On automorphism groups of leftdistributive quasigroups,* Izvestiya AN RM. Matematica. No 2, 1994, p. 79-86 (in Russian).

[102] V.A. Shcherbacov: *On automorphism groups and congruences of quasigroups,* IM AN MSSR. Thesis of Ph. Degree. Kishinev. 1991, 88 pages. (in Russian).

[103] V.A. Shcherbacov: *On 20 Belousov's problems,* Preprint IAMI, 99.8, Milan, 1999, 6 pages.

[104] R.-H. Schulz, *Check Character Systems and Anti-symmetric Mappings.* H. Alt(Ed): Computational Discrete Mathematics, LNCS 2122, pp. 136-147, 2001.

[105] R.-H. Schulz, *Equivalence of check digit systems over the dicyclic groups of order 8 and 12*. In J. Blankenagel & W. Spiegel, editor, Mathematikdidaktik aus Begeisterung für die Mathematik, pp. 227- 237. Klett Verlag, Stuttgart, 2000.

[106] P.W. Shor, *Quantum computing*, Proc. Intern. Congress of Mathematicians, Berlin, v.1, 1998, 467-486.

[107] G.J. Simmons (ed.), *Contemporary Cryptology - The Science of Information Integrity*, IEEE Press, New York, 1992.

[108] J.D.H. Smith: *Mal'cev Varieties*, Lecture Notes in Mathematics, **v. 554**, 1976.

[109] M. Steinberger: On loops with a general weak inverse property, em Mitt. Math. Ges. Hamburg, **10**(1979), 573-586.

[110] P.N. Syrbu: *On congruences on n-ary T-quasigroups*, Quasigroups and related systems, **V. 6**, (1999), 71 – 80.

[111] K. Toyoda: *On axioms of linear functions*, Proc. Imp. Acad. Tokyo, **17**, (1941), 221 – 227.

[112] J. Verhoeff, *Error Detecting Decimal Codes,* Vol. 29, Math. Center Tracts. Math. Centrum Amsterdam, 1969.

[113] P. Vojtechovsky, *Distances of groups of prime order*, Contrib. Gen. Algebra 11, 1999, 225-231.

[114] H. Zbingen, N. Gisin, B. Huttner, A. Muller and W. Tittel, *Practical aspects of quantum cryptographical key distributions*, J. Cryptology, 13, 2000, 207-220.