Quasigroups and Related Systems **10** (2003), 1 – 28

Check character systems over quasigroups and loops

Galina B. Belyavskaya, Vladimir I. Izbash, Victor A. Shcherbacov

Abstract

In this paper we survey the known results concerning check character (or digit) systems with one check character based on quasigroups (loops, groups). These are codes with one control symbol detecting errors of specific types.

This survey includes the following sections: 1. Introduction. 2. Check character systems over groups. 3. Check character systems over quasigroups. 4. Check character systems over T-quasigroups. 5. Detection sets and detection rate. 6. Equivalence of check character systems. 7. Check character systems as n-ary operations.

1. Introduction

The aim of the present article is to survey the known results concerning check character (or digit) systems with one check character based on quasigroups (loops, groups).

A check digit system with one check character is an error detecting code $\mathfrak{C}$ over an alphabet A which arises by appending *a check digit* (symbol) a_n to every word $a_1a_2\dots a_{n-1} \in A^{n-1}$:

$$\mathfrak{C}: \begin{cases} A^{n-1} & \longrightarrow & A^n \\ a_1a_2\dots a_{n-1} & \longmapsto & a_1a_2\dots a_{n-1}a_n. \end{cases}$$

2000 Mathematics Subject Classification: 20N05, 20N15, 94B60, 94B65

Keywords: quasigroup, loop, group, automorphism, orthomorphism, code, n-ary quasigroup, check character system

The research described in this publication was made possible in part by Award No. MM2-3017 of the Moldovan Research and Development Association (MRDA) and the U.S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

The purpose of using such a system is to detect transmission errors (which can arise once in a code word), in particular, made by human operators during typing of data.

The examples of check character systems used in practice are the following:

- the European Article Number (EAN) Code,
- the Universal Product Code (UPC),
- the International Standard Book Number (ISNB) Code,
- the system of the serial numbers of German banknotes,
- different bar-codes used in the service of transportation, automation of various processes and so on.

The control digit of a system based on a quasigroup (system over a quasigroup) is calculated by distinct check formulas (check equations) using quasigroup operations.

D. F. Beckley [1] and J. Verhoeff [27] investigated statistically errors made by human operators. They classified them as single errors (that is errors in only one component of a code word), (adjacent or neighbour) transpositions, i.e. errors of the form $\dots ab \dots \longrightarrow \dots ba \dots$, jump transpositions ($\dots abc \cdots \to \dots cba \dots$), twin errors ($\dots aa \cdots \to \dots bb \dots$), jump twin errors ($\dots aca \cdots \to \dots bcb \dots$) and phonetic errors ($\dots a0 \cdots \to \dots 1a \dots$, $a \geqslant 2$). Single errors and transpositions are the most prevalent ones.

Table 1: Error types and their frequencies ([23]).

Error type		Relative frequency %	
		Verhoeff	Beckley
single error	$\dots a \cdots \to \dots b \dots$	79.0 (60-95)	86
adjacent transposition	$\dots ab \cdots \to \dots ba \dots$	10.2	8
jump transposition	$\dots abc \cdots \to \dots cba \dots$	0.8	
twin error	$\dots aa \cdots \to \dots bb \dots$	0.6	6
phonetic error ($a \geqslant 2$)	$\dots a0 \cdots \to \dots 1a \dots$	0.5	
jump twin error	$\dots aca \cdots \to \dots bcb \dots$	0.3	
other error		8.6	

Phonetic errors depend on the language and we shall not consider them here.

The work [27] of J. Verhoeff is the first significant publication that systematically studies systems for detection of errors made by human operators. It contains a survey of the decimal codes known in the begin of 1970-th.

A. Ecker and G. Poch in [12] have given a survey of elementary methods for the construction of check character systems (that is of the methods that do not use any mathematics other than simple arithmetical computations) and their analysis from mathematical point of view. In particular, the group-theoretical background of the known methods was explained and new codes were presented that stem from the theory of quasigroups. All methods using the modulo 10 sum can be described in the following way.

Let $a_1a_2\dots a_{n-1}$ $(n \geqslant 3)$ be a word over the alphabet $A = \{0, 1, \dots, 9\}$. The decimal code with one check digit $a_n \in A$ is defined by permutations $\delta_1, \delta_2, \dots, \delta_n$ on A together with the check equation

$$\sum_{i=1}^{n} \delta_i a_i \equiv c \pmod{10}, \quad c \in A$$

(usually $c = 0$), that is

$$a_n = \delta_n^{-1}(c - \sum_{i=1}^{n-1} \delta_i a_i) \pmod{10}.$$

Note that everywhere we do not use brackets for an application of a mapping. For example, we write αb instead of $\alpha\,(b)$.

So, the IBM code defined by the permutation

$$\delta = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 0\,2\,4\,6\,8\,1\,3\,5\,7\,9 \end{pmatrix}$$

and the check equation

$$a_n + \delta a_{n-1} + a_{n-2} + \delta a_{n-3} + \dots \equiv c \pmod{10}, \quad c \in A,$$

detects all single errors. Transposition errors will not be detected completely as the transposition 0 and 9 goes undetected. None of the jump transpositions or jump twin errors are detected. The generalized IBM code with the check equation

$$\sum_{i=1}^{n} \delta^{i-1} a_{n+1-i} \equiv c \pmod{10}, \quad c \in A,$$

detects jump transpositions and jump twin errors with the defined accuracy.

In the paper [12] many other known elementary check systems modulo 10, 11 and $k > 11$ are presented with a short discussion concerning each system. More general group theoretical investigations are also considered which include all systems modulo different numbers. For that it is sufficient to take an arbitrary abelian (or non-abelian) group $G = G(+)$ and the following check equation

$$\sum_{i=1}^{n} \delta_i a_i = c \in G, \tag{1}$$

where $\delta_1, \delta_2, \ldots, \delta_n$ are fixed permutations of G.

So, the Universal Product Code (UPC) is a code with $G = Z_{10}(+)$, $n = 13$, $\delta_{2i-1} = \varepsilon = \delta_{13}$ and $\delta_{2i}a = 3a$ for $i = 1, \ldots, 6$, $c = 0$, where ε denotes the identity permutation. The check equations of the European Article Number (EAN) Code and the International Standard Book Number (ISNB) Code see in the end of the present article.

In Section 5 of [12] the possibility of constructing of check character systems based on Latin squares (or on quasigroups) is also investigated. The error detecting capability of such code may be better than of a modulo m check system.

A *Latin square of order* n is a square matrix with entries of n distinct elements each occurring exactly once in each row and column ([10]).

A *quasigroup* $Q(\cdot)$ is a binary operation $(\cdot)$ defined on the set Q such that for any two elements $a, b \in Q$ each of the equations $a \cdot x = b$, $y \cdot a = b$ has exactly one solution [10].

A *loop* is a quasigroup with the identity element e ($x \cdot e = e \cdot x = x$ for all $x \in Q$).

For example, the operation

$$a \cdot b = (ha + kb + l) \pmod{n}$$

where h, k, l are fixed integers from $Z_n = \{0, 1, \ldots, n-1\}$ with h and k relative prime to n defines a quasigroup on the set Z_n.

It is easy to verify that the multiplication table of a finite quasigroup is a Latin square. Conversely, a Latin square may be interpreted as a quasigroup.

H. P. Gumm [15] considers a check character system as an n-ary operation with the properties permitting to detect all single errors and all transposition errors. Later M. Damm in [8] and G. L. Mullen with V. Shcherbacov in [18] continued this approach and studied the considered systems related

to n-ary operations (quasigroups). The work [8] of M. Damm contents as well a good survey of check character systems over groups and groups which are able to detect all transpositions (and all single errors).

Choosing $Q(\cdot)$ as a finite set endowed with an binary algebraic structure (a groupoid) one can take the following general check formulas for calculation of the control symbol a_n:

$$a_n = (\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3)\dots) \cdot \delta_{n-1} a_{n-1} \tag{2}$$

or

$$(\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3)\dots) \cdot \delta_n a_n = c \tag{3}$$

for fixed permutations δ_i of Q, $i = 1, 2, \dots, n$ and a fixed element c of Q.

It is easy to see that a (finite) check character system with check formula (2) or (3) detects all single errors if and only if $Q(\cdot)$ is a quasigroup. The other errors will be detected if and only if this quasigroup has specific properties.

Often a permutation δ_i in (2), (3) is chosen such that $\delta_i = \delta^{i-1}$, $i = 1, \dots, n$, for a fixed permutation δ of Q. In this case we obtain the following check formulas respectively:

$$a_n = (\dots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3)\dots) \cdot \delta^{n-2} a_{n-1} \tag{4}$$

and

$$(\dots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3)\dots) \cdot \delta^{n-1} a_n = c. \tag{5}$$

In the following sections we shall survey the check character systems over groups, quasigroups, loops, T-quasigroups, the check character systems considered as n-ary quasigroups, equivalences of check character systems.

The main attention will be focussed on check character systems over quasigroups and loops.

2. Check character systems over groups

Let $G(= G(\cdot)$ be a group with the identity e. Then the most general check equation is the equation (1) (usually $c = e$) and the formula (5) has the form

$$a_1 \cdot \delta a_2 \cdot \delta^2 a_3 \cdot \dots \cdot \delta^{n-1} a_n = e. \tag{6}$$

In [27] and [12] the conditions on a permutation δ_i (or δ) are given that make it possible to detect errors of different types. The error detection conditions for abelian groups (see Table 2) can be expressed by certain concepts that are recalled below. These conditions get more complicated when G is assumed to be non-abelian (see Table 3).

Before recall required concepts.

Definition 2.1 [10]. A *complete mapping* of a quasigroup (a group) is a bijective mapping $x \to \theta x$ of Q onto Q such that the mapping $x \to \eta x$ defined by $\eta x = x \cdot \theta x$ is again a bijective mapping of Q onto Q.

Definition 2.2 [11]. A permutation α of a group $G(+)$ is called an *orthomorphism* if $x - \alpha x = \beta x$ where β is a permutation of G and $-x$ is the opposite element for x in the group.

Definition 2.3 [23]. A permutation δ of $G(\cdot)$ is called *anti-symmetric* in a group (in a quasigroup) G if it fulfills the condition $x \cdot \delta y \neq y \cdot \delta x$ for all $x, y \in G, \quad x \neq y$.

In this paper are always composed from the right to the left.

Table 2: Conditions for error detection by (1) (by (6)), $n > 4$ with a finite abelian group

Error type	Conditions for all i
single error	δ_i (δ) permutation
adjacent transposition	$\delta_{i+1}\delta_i^{-1}$ (δ) orthomorphism
jump transposition	$\delta_{i+2}\delta_i^{-1}$ (δ^2) orthomorphism
twin error	$\delta_{i+1}\delta_i^{-1}$ (δ) complete mapping
jump twin error	$\delta_{i+2}\delta_i^{-1}$ (δ^2) complete mapping

Table 3: Conditions for error detection by (1), $n > 4$ with a finite non-abelian group

Error type	Conditions for all i, x, y, z
single error	δ_i permutation
adjacent transposition	$\delta_{i+1}\delta_i^{-1}$ anti-symmetric permutation
jump transposition	$x \cdot y \cdot \delta_{i+2}\delta_i^{-1} z \neq z \cdot y \cdot \delta_{i+2}\delta_i^{-1} x, \quad x \neq z$
twin error	$\delta_{i+1}\delta_i^{-1}$ complete mapping
jump twin error	$x \cdot y \cdot \delta_{i+2}\delta_i^{-1} x \neq z \cdot y \cdot \delta_{i+2}\delta_i^{-1} z, \quad x \neq z$

As it was pointed the transpositions are the most prevalent errors and their detection is connected with anti-symmetric mappings (see Table 3), so in the works [8], [9] of M. Damm and in the articles [13], [16], [17], [21], [22], [23], [24], [25] and [26] much attention is given to research of groups with anti-symmetric mappings. A survey of anti-symmetric mappings in different groups can be found in the article [23] of R. H. Schulz.

For the completeness we shall give the main results on the groups having anti-symmetric mappings in the order of their publication. Note that the results for abelian groups often follow as corollaries of known results concerning complete mappings.

- Abelian groups of order $m = 2n$ with n odd do not admit anti-symmetric mappings [23].

- The cyclic group G admits an anti-symmetric mapping if and only if $|G|$ is odd [23].

- All groups of odd order admit an anti-symmetric mappings [13].

- For $m > 2$ the symmetric group S_m and the alternating group A_m have anti-symmetric mappings [13].

- Every finite simple group except Z_2 has an anti-symmetric mapping [13].

- Every non-trivial finite p-group which is not a cyclic 2-group has anti-symmetric mappings [13].

- Every finite nilpotent group with a trivial or the non-cyclic Sylow 2-subgroup has an anti-symmetric mapping [13].

Taking into account these results J. A. Gallian and M. D. Mullin made the following

Conjecture 2.4 [13]. *All non-abelian groups have anti-symmetric mappings.*

This conjecture has been confirmed by S. Heiss at first for soluble groups in [16], later for each non-abelian group.

Theorem 2.5 [17]. *Every non-abelian group admits an anti-symmetric mapping.*

J. Verhoeff [27] has pointed out a number of anti-symmetric mappings of the dihedral groups D_5 and D_m, $m > 5$. We remember that the dihedral group D_m is a group of order $2m$ of such form

$$D_m = \langle d, s \,|\, d^m = e = s^2, \quad ds = sd^{-1} \rangle.$$

Note that within the group theory the dihedral group with $2m$ elements is usually denoted by D_{2m}.

Other anti-symmetric mappings of the dihedral groups were found in [15], [12], [13]. All these mappings give a possibility to obtain check character systems detecting all transpositions.

M. Damm proved the following important theorem.

Theorem 2.6 [8]. *For $m \geqslant 3$ odd there does not exist a check digit system over D_m which detects all jump transpositions or all twin errors or all jump twin errors.*

In [26] (see also [24]) all anti-symmetric mappings, automorphisms and anti-automorphisms of the dicyclic groups Q_2 (it is the quaternion group) and Q_3 of order 8 and 12, respectively, were obtained by computer search. These groups are

$$Q_2 = \langle a, b \mid a^4 = e, \quad b^2 = a^2, \quad ab = ba^{-1} \rangle$$

and

$$Q_3 = \langle a, b \mid a^6 = e, \quad b^2 = a^3, \quad ab = ba^{-1} \rangle.$$

Recall that an automorphism α of a group with the identity e is called regular if $\alpha x \neq x$ for each $x \neq e$ (such permutation α is called a fixed point free permutation).

Anti-symmetric automorphisms and anti-automorphisms of groups were considered by R. H. Schulz in [22], [23] and M. Damm in [8]. So, the following statement is proved.

Proposition 2.7 [23]. *An automorphism δ of a finite group G with the identity e is anti-symmetric if and only if δ does not fix any conjugacy class of $G\backslash\{e\}$. When G is abelian, then this is the case if and only if the automorphism δ is regular.*

Due to the works [27], [7], [12] necessary and sufficient conditions on a permutation (or on an automorphism) δ for detection each of five error types by a check digit system over a group G with check formula (6), $n > 4$ can be given in the following Table 4, where S_G (Aut$G$) denotes the set of all permutations (or the automorphism group, respectively) of G.

TABLE 4: ERROR DETECTION OF SYSTEMS OVER GROUPS WITH (6), $n > 4$

Error type	Conditions on δ, for all $x, y, z \in G$	
	$\delta \in S_G$	$\delta \in \operatorname{Aut} G$, $x \neq e$
single errors	none	none
transpositions	$x \cdot \delta y \neq y \cdot \delta x, x \neq y$	$\delta x \neq y^{-1}xy$
jump transpositions	$xy \cdot \delta^2 z \neq zy \cdot \delta^2 x$, $x \neq z$	$\delta^2 x \neq y^{-1}xy$
twin errors	$x \cdot \delta x \neq y \cdot \delta y$, $x \neq y$	$\delta x \neq y^{-1}x^{-1}y$
jump twin errors	$xy \cdot \delta^2 x \neq zy \cdot \delta^2 z$, $x \neq z$	$\delta^2 x \neq y^{-1}x^{-1}y$

Definition 2.8 [7]. Let G be a finite group. An automorphism δ of G is called *good* provided δx is not conjugate to x or x^{-1} and $\delta^2 x$ is not conjugate to x or x^{-1} for all $x \in G$, $x \neq e$, where x^{-1} is the inverse element for x.

Proposition 2.9 [7]. *A good automorphism is anti-symmetric and detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors.*

In [7] it is shown that there are many groups possessing a good automorphism.

The class of groups having anti-symmetric mappings is extension closed according to

Theorem 2.10 [13]. *If G is a group with a normal subgroup H and there exist anti-symmetric mappings φ on H and ψ on G/H, then there exists an anti-symmetric mapping γ on G.*

3. Check character systems over quasigroups and loops

In this section we shall mainly survey new results concerning check character systems over quasigroups with check formulas (4) or (5) which are able to detect single errors, transpositions, jump transpositions, twin errors and jump twin errors in all digits of a code word (including the control digit).

Consider the following conditions which hold for all $a, b, c, d \in Q$ in a quasigroup $Q(\cdot)$, $\delta \in S_Q$:

(α_1) $\quad b \cdot \delta c \neq c \cdot \delta b$, if $b \neq c$;

(α_2) $ab \cdot \delta c \neq ac \cdot \delta b$, if $b \neq c$;
(α_3) $(a = d \cdot \delta^{n-2} b \quad and \quad b = d \cdot \delta^{n-2} a) \Rightarrow (a = b)$;
(β_1) $dc \cdot \delta^2 b \neq bc \cdot \delta^2 d$, *if* $b \neq d$;
(β_2) $(ad \cdot c) \cdot \delta^2 b \neq (ab \cdot c) \cdot \delta^2 d$, *if* $b \neq d$;
(β_3) $(d = (a \cdot \delta^{n-3} b) \cdot c \quad and \quad b = (a \cdot \delta^{n-3} d) \cdot c) \Rightarrow (b = d)$;
(γ_1) $b \cdot \delta b \neq c \cdot \delta c$ if $b \neq c$;
(γ_2) $ab \cdot \delta b \neq ac \cdot \delta c$ if $b \neq c$;
(γ_3) $(a = d \cdot \delta a \quad and \quad b = d \cdot \delta b) \Rightarrow (b = a)$;
(σ_1) $bc \cdot \delta^2 b \neq dc \cdot \delta^2 d$, *if* $b \neq d$;
(σ_2) $(ab \cdot c) \cdot \delta^2 b \neq (ad \cdot c) \cdot \delta^2 d$, *if* $b \neq d$;
(σ_3) $(d = (a \cdot \delta^{n-3} d) \cdot c \quad and \quad b = (a \cdot \delta^{n-3} b) \cdot c) \Rightarrow (b = d)$.

The main theorem of [4] that points necessary and sufficient conditions for detection of considered five error types by a check character system over a quasigroup with the check formula (4) or (5), $n > 4$ it is convenient to give in Table 5.

Table 5: Error detection of systems over quasigroups

Error type	Conditions on $\delta \in S_Q$, $n > 4$	
	Check formula (4)	Check formula (5)
single errors	none	none
transpositions	$(\alpha_1), (\alpha_2)$ and (α_3)	(α_1) and (α_2)
jump transpositions	$(\beta_1), (\beta_2)$ and (β_3)	(β_1) and (β_2)
twin errors	$(\gamma_1), (\gamma_2)$ and (γ_3)	(γ_1) and (γ_2)
jump twin errors	$(\sigma_1), (\sigma_2)$ and (σ_3)	(σ_1) and (σ_2)

It is clear from this table why formula (5) should be preferred. Note that the conditions for formula (5) do not depend on the size of n.

The conditions for transpositions, and jump transpositions with the check formula (4) were established earlier by R. H. Schulz in [20].

If a quasigroup $Q(\cdot)$ is a group and the check formula (5) is used, then the conditions (α_1), (β_1), (γ_1) and (δ_1) are both necessary and sufficiently, as they coincide with the conditions of Table 4, respectively.

If $Q(\cdot)$ is a quasigroup with the left identity e ($ex = x$ for all $x \in Q$) or a loop ($ex = xe = x$ for all $x \in Q$), then such conditions are correspondingly (α_2), (β_2), (γ_2) and (δ_2) [4].

Let $L_a x = ax, R_a x = xa$ for all $x \in Q$ in a quasigroup $Q(\cdot)$. The following statement is a corollary of the conditions from Table 5.

Proposition 3.1 [4]. *Let $Q(\cdot)$ be a finite quasigroup. Then*

- *condition (γ_1) holds if and only if the permutation δ is a complete mapping;*
- *condition (γ_2) holds if and only if the permutation δL_a^{-1} is a complete mapping for all $a \in Q$;*
- *condition (σ_1) holds if and only if the permutation $\delta^2 R_c^{-1}$ is a complete mapping for all $c \in Q$;*
- *condition (σ_2) holds if and only if the permutation $\delta^2 L_a^{-1} R_c^{-1}$ is a complete mapping for all $a, c \in Q$.*

In Corollary 3.2 below we shall observe that each conditions (γ_2), (σ_1) and (σ_2) can be associated with the notion of orthogonal Latin squares. That makes these conditions, in certain sense, "strong".

Two Latin squares $L_1 = ||a_{ij}||$ and $L_2 = ||b_{ij}||$ on m symbols are said to be *orthogonal* if every ordered pair of symbols occurs exactly once among the m^2 pairs (a_{ij}, b_{ij}), $i, j = 1, 2, \ldots, m$ [10].

A *pair of orthogonal quasigroups* corresponds to a pair of orthogonal Latin squares and conversely.

Two quasigroups $Q(\cdot)$ and $Q(\circ)$ are called *orthogonal* if the system of equations

$$\begin{cases} x \cdot y = a \\ x \circ y = b \end{cases}$$

has an unique solution for all $a, b \in Q$.

Corollary 3.2 [4]. *If a finite quasigroup $Q(\cdot)$ satisfies the conditions γ_2 ((σ_1) or (σ_2)), then it has an orthogonal mate (pair).*

We can say more when $Q(\cdot)$ is a loop and δ is the identity permutation.

Recall that a *Moufang loop* is a loop which satisfies the Moufang identity $(zx \cdot y) \cdot x = z(x \cdot yx)$ (see [2], [10]).

Proposition 3.3 [4]. *If $Q(\cdot)$ is a loop, $\delta = \varepsilon$, $n > 4$, then*

- *properties (α_1) and (β_1) do not hold;*
- *from (σ_2) it follows (γ_2);*
- *in a Moufang loop (in particular, in a group) conditions (γ_1), (γ_2), (σ_1) and (σ_2) are equivalent.*

Corollary 3.4 [4].

- *It is impossible using a loop to detect all transpositions (jump transpositions, twin errors or jump twin errors) if check formula* (4) *is applied with* $\delta = \varepsilon$, $n > 4$.

- *A finite Moufang loop (a finite group) with check formula* (5), $\delta = \varepsilon$, $n > 4$ *does not detect all transpositions and jump transpositions, but detects all twin errors and all jump twin errors if and only if* $b^2 \neq d^2$ *for all* $b \neq d$ *(that is the identity permutation is a complete mapping).*

- *A check character system using a Moufang loop (a group) of odd order and check formula* (5) *with* $\delta = \varepsilon$, $n > 4$ *detects all twin errors and all jump twin errors.*

- *A check character system using an abelian group and coding formula* (5) *with* $\delta = \varepsilon$, $n > 4$ *detects all twin errors and all jump twin errors if and only if the group has odd order.*

These results show that check character systems over loops (groups) with formula (4) or (5) with $\delta = \varepsilon$, $n > 4$ cannot detect all transpositions and jump transpositions. In this case it is possible to use formula (4) or (5) with $\delta \neq \varepsilon$ for a quasigroup or it is possible to use formula (1) for a group.

4. Check character systems over T-quasigroups

There is another way to use groups for construction of check digit systems detecting these errors as well. Namely, instead of a group $Q(\circ)$ it is possible to take a quasigroup $Q(\cdot)$ which is isotopic to this group:

$$x \cdot y = \gamma^{-1}(\alpha x \circ \beta y)$$

where α, β, γ are permutations of Q [10, 2]. Such an idea is used in this section.

A quasigroup $Q(\cdot)$ is called a *T-quasigroup* if there exist an abelian group $Q(+)$ with automorphisms φ and ψ and a fixed element $g \in Q$ such that $x \cdot y = \varphi x + \psi y + g$ for all $x, y \in Q$ [19].

The concept of a T-quasigroup is a particular case of the concept of a quasigroup which is isotopic to an abelian group and it generalizes the concept of a medial quasigroup (see, for example, [2]).

Denote by $\operatorname{Ort} Q(+)$ the set of all orthomorphisms of a group $Q(+)$. Necessary and sufficient conditions for error detection of systems with formula (4) or (5), $n > 4$ are presented in Table 6 (see Theorems 1 and 3 of [5], respectively), where $Ix = -x$. The respective permutations that appear in Table 6 must be in $\operatorname{Ort} Q(+)$.

TABLE 6: ERROR DETECTION OF SYSTEMS OVER T-QUASIGROUPS
$x \cdot y = \varphi x + \psi y + g$

Error type	Conditions on δ permutations of $\operatorname{Ort} Q(+)$	
	Check formula (4)	Check formula (5)
single errors	none	none
transpositions	$\psi\delta\varphi^{-1},\ \psi\delta\psi^{-1}\varphi^{-1},$ $I\psi\delta^{n-2}$	$\psi\delta\varphi^{-1},\ \psi\delta\psi^{-1}\varphi^{-1}$
jump transpositions	$\psi\delta^2\varphi^{-2},\ \psi\delta^2\psi^{-1}\varphi^{-2},$ $I\varphi\psi\delta^{n-3}$	$\psi\delta^2\varphi^{-2},\ \psi\delta^2\psi^{-1}\varphi^{-2}$
twin errors	$I\psi\delta\varphi^{-1},\ I\psi\delta\psi^{-1}\varphi^{-1},$ $\psi\delta$	$I\psi\delta\varphi^{-1}, I\psi\delta\psi^{-1}\varphi^{-1}$
jump twin errors	$I\psi\delta^2\varphi^{-2},\ I\psi\delta^2\psi^{-1}\varphi^{-2},$ $\varphi\psi\delta^{n-3}$	$I\psi\delta^2\varphi^{-2},\ I\psi\delta^2\psi^{-1}\varphi^{-2}$

In the both cases of the check formulas the conditions do not depend on the element $g \in Q$ and in the case of formula (5) the conditions do not depend on length $n > 4$ of a code word.

Corollary 4.1 [5]. *If in Table 6 δ is an automorphism of the abelian group $Q(+)$, then all described errors are detected if and only if the respective permutations are regular automorphisms.*

In [5] the conditions are also given when $\delta = I,\ \varepsilon,\ \varphi$ or ψ^{-1}. If $\delta = \varepsilon$, we obtain the conditions of Table 7.

According to Proposition 2 of [5] direct product of T-quasigroups detecting all errors of some type detects also all errors of the same type if formula (4) (or (5)) with $\delta = \varepsilon,\ n > 4$ is used.

In [5] a number of T-quasigroups is given satisfying all conditions from Table 6 (Table 7) if formula (4) (or (5)) is used with $\delta = \varepsilon$ and consequently, check character systems over such T-quasigroups with $\delta = \varepsilon$ are able to

detect all of the five error types in contrast to check character systems over loops or groups (see Corollary 3.4).

TABLE 7: ERROR DETECTION OF SYSTEMS OVER T-QUASIGROUPS
$x \cdot y = \varphi x + \psi y + g$

Error type	Conditions on φ, ψ if $\delta = \varepsilon, n > 4$ in (5)
single errors	none
transpositions	φ, $\varphi\psi^{-1}$ are regular
jump transpositions	φ^2, $\varphi^2\psi^{-1}$ are regular
twin errors	$I\varphi^1$, $I\varphi\psi^{-1}$ are regular
jump twin errors	$I\varphi^2$, $I\varphi^2\psi^{-1}$ are regular

5. Detection sets and detection rate of check digit systems

For any check character system over a quasigroup it is possible to define a detection set and a detection rate (percentage) of errors of each type. In Table 2 of [23] (see also [27] and [14]) a rate of detection for a check character system over a group of order q with check formula (6), $n > 4$ is pointed out. This information we give in Table 8, where detection sets M_T, M_{jT}, M_{TE}, M_{jTE} of transpositions, twin errors and jump twin errors respectively are defined in the following way:

$$M_T = \{(a,b) \in Q^2 \mid a \cdot \delta b \neq b \cdot \delta a,\ a \neq b\},$$

$$M_{jT} = \{(a,b,c) \in Q^3 \mid ab \cdot \delta^2 c \neq cb \cdot \delta^2 a,\ a \neq c\},$$

$$M_{TE} = \{(a,b) \in Q^2 \mid a \cdot \delta a \neq b \cdot \delta b,\ a \neq b\},$$

$$M_{jTE} = \{(a,b,c) \in Q^3 \mid ab \cdot \delta^2 a \neq cb \cdot \delta^2 c,\ a \neq c\}.$$

Note that these sets are considered as detection sets of the respective errors, since if $(a,b) \in M_T$ (or $(a,b) \in M_{TE}$), then the transposition $\ldots ab \cdots \to \ldots ba \ldots$ (or the twin error $\ldots aa \cdots \to \ldots bb \ldots$, respectively) will be detected.

If $(a,b,c) \in M_{jT}$ (or $(a,b,c) \in M_{jTE}$), then the jump transposition $\ldots abc \cdots \to \ldots cba \ldots$ (or the jump error $\ldots aba \cdots \to \ldots cbc \ldots$, respectively) will be defined.

The maximal number of the pairs (a, b) with $a \neq b$ (the triples (a, b, c) with $a \neq c$) in a group of order q is $q(q-1)$ (or $q^2(q-1)$, respectively), so we obtain a percentage (or a rate) of detection from Table 8 (compare with Table 4).

Table 8: Detection of errors by check character systems over groups of order q

Error type	Detection set	Percentage of detection
transpositions	M_T	$\lvert M_T\rvert/q(q-1)$
jump transpositions	M_{jT}	$\lvert M_{jT}\rvert/q^2(q-1)$
twin errors	M_{TE}	$\lvert M_{TE}\rvert/q(q-1)$
jump twin errors	M_{jTE}	$\lvert M_{jTE}\rvert/q^2(q-1)$

Let $S(Q(\cdot), \delta)$ denote a check character system over a quasigroup of order q with the check formula (5), $n > 4$. For such a system detection sets M_T^δ, M_{jT}^δ, M_{TE}^δ and M_{jTE}^δ are more complicated and are defined in the following way [6]:

$$M_T^\delta = U_1^\delta \cup V_1^\delta,$$

where

$$U_1^\delta = \{(b, c) \in Q^2 \mid b \cdot \delta c \neq c \cdot \delta b,\ b \neq c\},$$
$$V_1^\delta = \{(a, b, c) \in Q^3 \mid ab \cdot \delta c \neq ac \cdot \delta b,\ b \neq c\};$$

$$M_{jT}^\delta = U_2^\delta \cup V_2^\delta,$$

where

$$U_2^\delta = \{(b, c, d) \in Q^3 \mid bc \cdot \delta^2 d \neq dc \cdot \delta^2 b,\ b \neq d\},$$
$$V_2^\delta = \{(a, b, c, d) \in Q^4 \mid (ab \cdot c) \cdot \delta^2 d \neq (ad \cdot c)\delta^2 b,\ b \neq d\};$$

$$M_{TE}^\delta = U_3^\delta \cup V_3^\delta,$$

where

$$U_3^\delta = \{(b, c) \in Q^2 \mid b \cdot \delta b \neq c \cdot \delta c,\ b \neq c\},$$
$$V_3^\delta = \{(a, b, c) \in Q^3 \mid ab \cdot \delta b \neq ac \cdot \delta c,\ b \neq c\};$$

$$M^{\delta}_{jTE} = U^{\delta}_4 \cup V^{\delta}_4,$$

where

$$U^{\delta}_4 = \{(b,c,d) \in Q^3 \mid bc \cdot \delta^2 b \neq dc \cdot \delta^2 d,\ b \neq d\},$$

$$V^{\delta}_4 = \{(a,b,c,d) \in Q^4 \mid (ab \cdot c) \cdot \delta^2 b \neq (ad \cdot c)\delta^2 d,\ b \neq d\}.$$

The set U^{δ}_i, $i = 1,2,3,4$, points out the corresponding detected errors in the first digits of code words, while the set V^{δ}_i, $i = 1,2,3,4$, defines the detected errors in the rest positions beginning with the second position.

Generally, the sets U^{δ}_i and V^{δ}_i are dependent, moreover, for quasigroups with the left identity e the set V^{δ}_i completely defines the set U^{δ}_i (by $a = e$) $i = 1,2,3,4$.

Now we note that

$$\max(|U^{\delta}_i|) = q(q-1),\ \ \max(|V^{\delta}_i|) = q^2(q-1) \ \text{ for } \ i = 1,3$$

and

$$\max(|U^{\delta}_i|) = q^2(q-1),\ \ \max(|V^{\delta}_i|) = q^3(q-1) \ \text{ for } \ i = 2,4,$$

so

$$\max(|U^{\delta}_i| + |V^{\delta}_i|) = q(q^2-1) \ \text{ for } \ i = 1,3$$

and

$$\max(|U^{\delta}_i| + |V^{\delta}_i|) = q^2(q^2-1) \ \text{ for } \ i = 2,4.$$

Taking into account the above-mentioned we shall obtain Table 9 and Table 10 which contain estimations of percentage (i.e. the rate) r^{δ} of detection errors for a system $S(Q(\cdot), \delta)$ over a quasigroup $Q(\cdot)$, over a quasigroup with the left identity or over a loop, respectively [6].

Table 9: Detection of errors by systems over quasigroups of order q

Error types	Detection set	Percentage of detection
transpositions	$M^{\delta}_T = U^{\delta}_1 \cup V^{\delta}_1$	$r^{\delta}_1 \leqslant (\lvert U^{\delta}_1\rvert + \lvert V^{\delta}_1\rvert)/q(q^2-1)$
jump transpositions	$M^{\delta}_{JT} = U^{\delta}_2 \cup V^{\delta}_2$	$r^{\delta}_2 \leqslant (\lvert U^{\delta}_2\rvert + \lvert V^{\delta}_2\rvert)/q^2(q^2-1)$
twin errors	$M^{\delta}_{TE} = U^{\delta}_3 \cup V^{\delta}_3$	$r^{\delta}_3 \leqslant (\lvert U^{\delta}_3\rvert + \lvert V^{\delta}_3\rvert)/q(q^2-1)$
jump twin errors	$M^{\delta}_{JTE} = U^{\delta}_4 \cup V^{\delta}_4$	$r^{\delta}_4 \leqslant (\lvert U^{\delta}_4\rvert + \lvert V^{\delta}_4\rvert)/q^2(q^2-1)$

Table 10: Detection of errors by systems over quasigroups with the left identity or over loops of order q

Error type	Detection set	Percentage of detection
transpositions	$M_T^\delta = V_1^\delta$	$r_1^\delta = \lvert V_1^\delta\rvert/q^2(q-1)$
jump transpositions	$M_{JT}^\delta = V_2^\delta$	$r_2^\delta = \lvert V_2^\delta\rvert/q^3(q-1)$
twin errors	$M_{TE}^\delta = V_3^\delta$	$r_3^\delta = \lvert V_3^\delta\rvert/q^2(q-1)$
jump twin errors	$M_{JTE}^\delta = V_4^\delta$	$r_4^\delta = \lvert V_4^\delta\rvert/q^3(q-1)$

If $Q(\cdot)$ is a group of order q, then $|V_i| = q|U_i|$ and we obtain from Table 10 the detection rates of Table 8.

6. Equivalence of check character systems

The concepts of detection sets and detection rate allow to consider equivalence relations between check character systems over the same quasigroup (loop or group) as systems with the same detection rate of the same error type by means of a classification of permutations δ.

In [27] J. Verhoeff suggested some transformations preserving detection rate using automorphisms and translations of a group. These ideas were used by M. Damm in [8] and R. H. Schulz in [23, 24, 25].

The concept of automorphism equivalent permutations δ_1 and δ_2 for a group of [23] one can carry over a quasigroup.

Definition 6.1 [6]. A permutation δ_2 is called *automorphism equivalent to a permutation* δ_1 ($\delta_2 \sim \delta_1$) for a quasigroup $Q(\cdot)$ if there exists an automorphism α of $Q(\cdot)$ such that $\delta_2 = \alpha\delta_1\alpha^{-1}$.

The following proposition for quasigroups repeats Proposition 6.6 of [23] for a groups.

Proposition 6.2 [6]. *Automorphism equivalence is an equivalence relation (that is reflexive, symmetric and transitive).*

If δ_1 and δ_2 are automorphism equivalent for a quasigroup $Q(\cdot)$, then the systems $S(Q(\cdot), \delta_1)$ and $S(Q(\cdot), \delta_2)$ detect the same percentage of transpositions (jump transpositions, twin errors, jump twin errors).

According to computations by S. Giese [14] there are 1706 equivalence classes of anti-symmetric mappings (these detect all transpositions) with

respect to automorphism equivalence in the dihedral group D_5 of order 10. S. Giese distinguished 6 types of classes according to the detection rate of other errors in this group and defined detection rate of all 5 error types weighted with their relative frequencies. Unweighted error detection rate in D_5 depends on length n of code words (see Table 8 of [23]).

There exist exactly 1152 anti-symmetric mappings in the quaternion group, which constitute 48 equivalence classes of size 24 each with respect to automorphism equivalence [26, 24, 25]. In these articles it is pointed out that the dicyclic group Q_3 has 1.403.136 anti-symmetric mappings. They form 3.456 equivalence classes with respect to automorphism equivalence. Types of check digit systems over the groups Q_2 and Q_3 and their detection rates are presented as well in these articles.

Definition 6.3 [23]. Permutations δ_1 and δ_2 are called *weak equivalent for a group* $G(\cdot)$ if there exist elements $a, b \in G$ and an automorphism $\alpha \in \mathrm{Aut}\, G(\cdot)$ such that

$$\delta_2 = R_a \alpha^{-1} \delta_1 \alpha L_b, \quad a, b \in G,$$

where $R_a x = xa,\ L_a x = ax$ for all $x \in G$.

For a loop the notion of weak equivalence was generalized in [6].

Recall that the left, right, middle nuclei of a loop $Q(\cdot)$ are respectively the sets [2]:

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

The nucleus N of a loop is the intersection of the left, right and middle nuclei:

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

In a group $Q(\cdot)$ the nucleus N coincides with Q.

Definition 6.4 [6]. A permutation δ_2 of a set Q is called *weakly equivalent to a permutation* δ_1 ($\delta_2 \overset{w}{\sim} \delta_1$) *for a loop* $Q(\cdot)$ if there exist an automorphism α of the loop and elements $p, q \in N$ such that

$$\delta_2 = R_p \alpha \delta_1 \alpha^{-1} L_q,$$

where $R_p x = xp,\ L_q x = qx,\ N$ is the nucleus of the loop.

The following statement is generalization for loops of Proposition 6.2 of [23] (see also [8], [27]) for groups.

Proposition 6.5 [6].

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

b) *If* $\delta_1 \overset{w}{\sim} \delta_2$, *then systems* $S(Q(\cdot), \delta_1)$ *and* $S(Q(\cdot), \delta_2)$ *over a loop* $Q(\cdot)$ *detect the same percentage of transpositions* (*twin errors*).

c) *If, in addition,* δ_1 *is an automorphism of the loop* $Q(\cdot)$, *then these systems detect the same percentage of transpositions* (*jump transpositions, twin errors and jump twin errors*).

Corollary 6.6 [6]. *If* $Q(\cdot)$ *is a loop* (*a group*), N *is its nucleus,* $p, q \in N$ (*or* $p, q \in Q$, *respectively*), *then*

a) *systems* $S(Q(\cdot), \varepsilon)$ *and* $S(Q(\cdot), R_p L_q)$ *detect the same percentage of transpositions* (*jump transpositions, twin errors and jump twin errors*);

b) *systems* $S(Q(\cdot), R_p L_q)$ *over a loop can not detect all transpositions* (*all jump transpositions*).

Corollary 6.7 [6]. *A system* $S(Q(\cdot), R_p L_q)$ *over a Moufang loop of odd order with nucleus* N, $p, q \in N$ *detects all twin errors and all jump twin errors.*

In [6] there can be found an example of an eight-element loop together with weak equivalent permutations of this loop that are related to check character systems which have the equal detection percentage of the same errors.

7. Check character systems as n-ary operations

It is possible to consider a code $Q^n \to Q^{n+1} : a_1 a_2 \dots a_n \to a_1 a_2 \dots a_n a_{n+1}$ with one control symbol a_{n+1} as an n-ary operation f, setting

$$f(a_1, a_2, \dots, a_n) = a_{n+1}.$$

Such approach to check character systems detecting all single errors and all adjacent transpositions was used by H. P. Gumm in [15] and later by M. Damm in [8]. G. L. Mullen and V. Shcherbacov [18] considered

check character systems with n-ary quasigroup operation detecting (jump) transpositions and (jump) twin errors not only in adjacent positions.

Definition 7.1 [3]. A non-empty set Q with n-ary operation f such that in the equation $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ any n elements of $x_1, x_2, \ldots, x_n, x_{n+1}$ define the last one uniquely is called an *n-ary quasigroup* (or an n-quasigroup) $Q(f)$.

Definition 7.2 [8]. Let $g : D^{n+1} \to D$, where $D = \{0, 1, \ldots, m-1\}$, $c \in D$, be a mapping. The set

$$P_{g,c} = \{(d_n, d_{n-1}, \ldots, d_0) \in D^{n+1} \mid g(d_n, \ldots, d_0) = c\}$$

is called an *implicit check system over base m* if

1. $g(d_n, \ldots, d_i, \ldots, d_0) = g(d_n, \ldots, d_i', \ldots, d_0) = c$ implies $d_i = d_i'$.
2. $g(d_n, \ldots, d_i, d_{i-1}, \ldots, d_0) = g(d_n, \ldots, d_{i-1}, d_i, \ldots, d_0) = c$ implies $d_i = d_{i-1}$.
3. for all $d_n, \ldots, d_1 \in D$ there exists $d_0 \in D$ such that

$$g(d_n, \ldots, d_1, d_0) = c.$$

Definition 7.3 [8]. Let $D = \{0, 1, \ldots, m-1\}$ and let $f : D^n \to D$ be a mapping. The set

$$P_f' = \{(d_n, \ldots, d_0) \in D^{n+1} \mid f(d_n, \ldots, d_1) = d_0\}$$

is called an *explicit check system over base m* if

1. $f(d_n, \ldots, d_i, \ldots, d_1) = f(d_n, \ldots, d_i', \ldots, d_1)$ implies $d_i = d_i'$.
2. $f(d_n, \ldots, d_i, d_{i-1}, \ldots, d_1) = f(d_n, \ldots, d_{i-1}, d_i, \ldots, d_1)$ implies $d_i = d_{i-1}$.
3. $f(d_n, \ldots, d_2, d_0) = d_1$, where $f(d_n, \ldots, d_1) = d_0$ implies $d_1 = d_0$.

Both these check systems detect all single errors and adjacent transpositions including the control symbol. The operation f from Definition 7.3 is a finite n-ary quasigroup (see property 1) with additional properties 2 and 3. M. Damm proved the following general result concerning the existence of implicit (explicit) check systems (see [15] as well).

Theorem 7.4 [8]. *For each base $m > 2$ and all $n \geqslant 2$ there exists a mapping $f : D^n \to D$ (respectively $D^{n+1} \to D$) such that P_f ($P_{g,c}$) defines a check system.*

A connection between an implicit check system and some explicit check system over base m is established in [8] when an n-ary ($(n+1)$-ary) operation f (g) is a composition of binary quasigroups.

Theorem 7.5 [8].

1. *For each explicit check system P_f where f is a composition of $n-1$ binary quasigroups $*_i$, that is*

   $$f(d_n, d_{n-1}, \ldots, d_1) = (\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-2} \ldots) *_2 d_1$$

   there exists a quasigroup $*_1$ and an element $c \in D$ such that the equivalence

   $$f(d_n, \ldots, d_1) = d_0 \Longleftrightarrow g(d_n, \ldots, d_0) = c$$

   holds for $g(d_n, \ldots, d_0) = f(d_n, \ldots, d_1) *_1 d_0$.

2. *For every implicit check system $P(g, c)$ where g is a composition of n quasigroups $*_i$:*

   $$g(d_n, \ldots, d_0) = (\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-2} \ldots) *_1 d_0$$

   there exists a quasigroup $*'_2$ such that the equivalence

   $$f(d_n, \ldots, d_1) = d_0 \Longleftrightarrow g(d_n, \ldots, d_0) = c$$

   holds for $f = ((\ldots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-2} \ldots) *_3 d_2) *'_2 d_1$.

Definition 7.6 [8]. An n-ary quasigroup $Q(f)$ is called *anti-symmetric* if

$$f(x_n, \ldots, x_i, x_{i-1}, \ldots, x_1) = f(x_n, \ldots, x_{i-1}, x_i, \ldots, x_1)$$

implies $x_i = x_{i-1}$.

The following statement is often useful.

Lemma 7.7 [8]. *If $Q(f)$ is an anti-symmetric n-quasigroup and φ, ψ are permutations of Q, then $Q(\bar{f})$ where*

$$\bar{f}(x_n, \ldots, x_1) = \psi^{-1} f(\varphi x_n, \varphi x_{n-1}, \ldots, \varphi x_1)$$

is an anti-symmetric n-quasigroup.

From Theorem 7.4 it follows

Corollary 7.8 [15]. *For each $n \geqslant 2$ and all $m > 2$ there exists an anti-symmetric n-quasigroup of base m.*

Let

$$\hat{f}(x_n, x_{n-1}, \ldots, x_1) = x_0 \Longleftrightarrow f(x_0, x_1, \ldots, x_{n-1}) = x_n.$$

It is valid the following

Theorem 7.9 [8].

1. *Every n-quasigroup detects all single errors. If g is an anti-symmetric n-quasigroup, then $P_{g,c}$ is an implicit check system for any $c \in D$.*
2. *P'_f is an explicit check system if and only if $P'_{\hat{f}}$ is an explicit check system.*
3. *P'_f is an explicit check system if and only if f and $\hat{f}$ are anti-symmetric n-quasigroups.*

Implicit check systems with the check formula

$$g(x_n, x_{n-1}, \ldots, x_0) = (\ldots((x_n *_n x_{n-1}) *_{n-1} x_{n-2})\ldots) *_1 x_0 = c, \quad (7)$$

where $*_i$, $i = 1, 2, \ldots, n$, is a binary quasigroup, occupy a special position among the check systems researched by M. Damm.

Theorem 7.10 [8]. *$(n+1)$-Ary quasigroup $Q(g)$, where*

$$g(x_n, \ldots, x_0) = (\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_1 x_0$$

is anti-symmetric if and only if $*_n$ is anti-symmetric and each row of the quasigroup $*_{i+1}$ is an anti-symmetric mapping of $*_i$, $i = 1, 2, \ldots, (n-1)$.

Theorem 7.11 [8]. *Every quasigroup $*_i$ in a check system with the formula (7) has an anti-symmetric mapping. If such system detects all twin errors, then each quasigroup has a complete mapping. If it defines all jump twin errors, then every quasigroup, except $*_n$, has a complete mapping.*

Theorem 7.12 [8]. *Let $Q(*_i)$ be a quasigroup in a check system with the check formula (7) which detects all twin errors. Then the quasigroup $Q(*_i)$, $i = 1, 2, \ldots, n-1$, is orthogonal to the quasigroup $*'_i$ defined by*

$$x *'_i y = z \Longleftrightarrow z *_{i+1} y = x.$$

Definition 7.13 [8]. A binary quasigroup $Q(*)$ is called *total anti-symmetric* if it is anti-symmetric ($x * y = y * x$ implies $x = y$) and the equality $(c * x) * y = (c * y) * x$ implies $x = y$ for all $c, x, y \in Q$.

M. Damm in [8] has pointed out that a check system with the check formula

$$(\dots((x_n * x_{n-1}) * x_{n-2})\dots) * x_0 = d,$$

where $*$ is a binary quasigroup, defines (implicit) check system if and only if $*$ is a total anti-symmetric quasigroup. He also gives an algorithm of computer construction of total anti-symmetric binary quasigroups. For the following check formula

$$\varphi^n x_n * \varphi^{n-1} x_{n-1} * \varphi^{n-2} x_{n-2} * \dots * \varphi x_1 * x_0 = 0,$$

where $Q(*)$ is the dihedral group D_3 (D_4 or D_5), M. Damm in [8] using computer found total anti-symmetric permutations with good possibilities to detect errors of all five types.

G. L. Mullen and V. Shcherbacov [18] continued research of check character systems as n-ary operations, considering a code $a_1a_2\dots a_n \longrightarrow a_1a_2\dots a_na_{n+1}$ over a finite alphabet Q as an n-ary operation f, setting

$$f(a_1, a_2, \dots, a_n) = a_{n+1}.$$

Such code they call an *n-ary code* (Q, f). If f is an n-ary quasigroup operation, then this code is called an *n-quasigroup code*.

An n-ary code detects all single errors if and only if it is an n-quasigroup code.

In [18] it is shown that all n-ary quasigroup codes (Q, f) over the same alphabet Q ($|Q| = q$) (arity n is fixed) have in some sense equal possibilities to detect all possible types of errors.

More refined n-ary quasigroup codes which are able to detect transpositions and twin errors (not necessary in adjacent positions) are being researched.

Let x_m^n, where $m \leqslant n$, denote the sequence $x_m, x_{m+1}, \dots, x_n$, and $\overline{1, n} = \{1, 2, \dots, n\}$, let $Q(f)$ be an n-ary quasigroup: $f(x_1^n) = x_{n+1}$.

Changing in $f(x_1^n)$ elements $x_{k_1}, x_{k_2}, \dots, x_{k_m}$ respectively for some fixed elements $a_1, a_2, \dots, a_m$ we obtain a new $(n-m)$-ary quasigroup operation which is called a *retract* of the quasigroup $Q(f)$ [3].

Definition 7.14 [18]. A retract of a form $f\left(a_i^{i-1}, x_i, a_{i+1}^{i+k-1}, x_{i+k}, a_{i+k+1}^{n}\right)$ of an n-ary quasigroup $Q(f)$ where a_i^{i-1}, a_{i+1}^{i+k-1}, a_{i+k+1}^{n} are some fixed elements of Q, $i \in \overline{1, n-k}$, $k \in \overline{1, n-1}$ is called an $(i, i+k)$ *binary retract* of the quasigroup $Q(f)$.

Definition 7.15 [18]. A binary anti-symmetric quasigroup $Q(\cdot)$ is called *totally anti-commutative* if $x \cdot x = y \cdot y$ implies $x = y$ for all $x, y \in Q$ (compare with the Definition 7.13).

The following theorem determines properties of n-ary quasigroup codes which are able to detect all (not necessarily neighbour) transpositions and twin errors in the information symbols of a code word.

Theorem 7.16. *An $(n-1)$-ary quasigroup code (Q, f), $n > 3$ with check equation $f(x_1^{n-1}) = x_n$ detects each transposition and twin error on the places $(i, i+k)$, $i \in \overline{1, n-k-1}$, $k \in \overline{1, n-2}$ if and only if all $(i, i+k)$ binary retracts of the n-ary quasigroup $Q(f)$ are totally anti-commutative.*

Remark. Note that for the check formula $g(x_1^n) = c$, where c is a fixed element, analogous properties in general case are sufficient but not necessary as it is pointed in Theorem 2 of [18]. However, it is valid when g is an n-ary abelian group isotope (see Theorems 7.20 and 7.22).

Definition 7.17 [18]. An n-ary quasigroup $Q(g)$ 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, $\gamma_1, \gamma_2, \ldots, \gamma_n$ are permutations of Q is called an *n-ary group isotope*.

Definition 7.18 [18]. An n-quasigroup $Q(g)$ 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 an abelian group, $\alpha_1, \alpha_2, \ldots, \alpha_n$ are automorphisms of the group $Q(+)$, a is a fixed element of Q, is called an *n-T-quasigroup*.

Proposition 7.19 [18]. *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 $(i, i+1)$ $(i \in \overline{1, n-1})$ 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;*

b) *all* $(i, i+k)$ $(i \in \overline{1, n-k},\ k \in \overline{1, n-1})$ *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 all fixed element* t*, are totally anti-commutative.*

Theorem 7.20 [18]. *A code* $Q(g)$*, where* g *is an abelian group isotope, with the check equation* $\sum_{i=1}^{n} \gamma_i x_i = 0$*, where* 0 *is the zero of the abelian group* $Q(+)$*, detects any transposition and twin error on the places* $(i, i+1)$*,* $i \in \overline{1, n-1}$*,* $(i, i+2)$*,* $i \in \overline{1, n-2}$ *if and only if all binary 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.*

Proposition 7.21 [18]. *A binary T-quasigroup* $Q(\cdot)$ *of the form* $x \cdot y = \alpha x + \beta y + a$ *is totally anti-commutative if and only if the mappings* $\alpha - \beta$ *and* $\alpha + \beta$ *are automorphisms of the group* $Q(+)$*.*

Theorem 7.22 [18]. *A code* (Q, g)*, where* g *is an* n*-T-quasigroup, with the check equation*

$$g(x_1, x_2, \ldots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$$

detects

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

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* $Q(+)$*;*

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

We note that the check formula of Theorem 7.22 is the check formula (1) where the permutations $\alpha_1, \alpha_2, \ldots, \alpha_n$ are automorphisms of the abelian group $Q(+)$.

G. L. Mullen and V. Shcherbacov use Theorem 7.22 for construction a number of examples of codes based on n-T-quasigroups which detect all five types of the considered errors. They also give modifications of the ISBN-code and the EAN-code with better possibilities than the known codes.

In the ISBN-code (Z_{11}, g), $n = 10$ the check formula

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

is changed for

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

The last check formula allows to detect single errors and all error types of Theorem 7.22.

In the EAN-code (Z_{10}, g), $n = 13$, instead of the check formula

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

the formula

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

is proposed which has the better capability then the first one.

Acknowledgment. The authors thank A. Diordiev for the help at design of the given survey.

References

[1] **D. F. Beckley**: *An optimum systems with modulo* 11, The Computer Bulletin **11** (1967), 213 – 215.

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

[3] **V. D. Belousov**: *n-Ary Quasigroups*, (in Russian), Stiinta, Kishinev 1972.

[4] **G. B. Belyavskaya, V. I. Izbash, and G. L. Mullen**: *Check character systems using quasigroups: I* , (to appear).

[5] **G. B. Belyavskaya, V. I. Izbash, and G. L. Mullen**: *Check character systems using quasigroups: II*, (to appear).

[6] **G. B. Belyavskaya**: *On check character systems over quasigroups and loops*, Algebra and Discrete Math., (to appear).

[7] **C. Broecker, R. H. Schulz and G. Stroth**: *Check character systems using Chevalle groups*, Designs, Codes and Cryptography, DESI. **10** (1997), 137 – 143.

[8] **H. M. Damm**: *Prüfziffersysteme über Qasigruppen*, Diplomarbeit, Philipps-Universität Marburg 1998.

[9] **H. M. Damm**: *Check digit systems over groups and anti-symmetric mappings*, Archiv der Mathematik **75** (2000), 413 – 421.

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

[11] **A. L. Dulmage, D. M. Johnson and N. S. Mendelsohn**: *Orthomorphisms of groups and orthogonal Latin squares, I,* Canad. J.Math. **13** (1961), 356 – 372.

[12] **A. Ecker and G. Poch**: *Check character systems*, Computing **37** (1986), 277 – 301.

[13] **J. A. Gallian and M. D. Mullin**: *Groups with anti-symmetric mappings*, Arch. Math. **65** (1995), 273 – 280.

[14] **S. Giese**: *Äquivalenz von Prüfzeichensystemen am Beispil der Diedergruppe* D_5, Staatsexamensarbeit FU Berlin, 1999.

[15] **H. P. Gumm**: *A new class of check-digit methods for arbitrary number systems*, IEEE Trans. Inf. Th. IT, **31** (1985), 102 – 105.

[16] **S. Heiss**: *Anti-symmetric mappings for finite solvable groups*, Arch. Math. **69** (1997), 445 – 454.

[17] **S. Heiss**: *Anti-symmetric mappings for finite groups*, Preprint, 1999.

[18] **G. L. Mullen and V. A. Shcherbacov**: *Properties of codes with one check symbol from a quasigroup point of view*, Bulletinul Acad. Sci. Rep. Moldova, ser. Matematica no. **3** (2002), 71 – 86.

[19] **P. Nemec and T. Kepka**: *T-quasigroups, I,* Acta Univ. Carolinae **12** (1971), 39 – 49.

[20] **R. H. Schulz**: *A note on check character systems using Latin squares*, Diskrete Math. **97** (1991), 371 – 375.

[21] **R. H. Schulz**: *Some check digit systems over non-abelian group*, Mitt. der Math. Ges. Hamburg **12** (1991), 819 – 827.

[22] **R. H. Schulz**: *Check character systems over groups and orthogonal Latin squares*, Applic. Algebra in Eng., Comm. and Computing, AAECC, **7** (1996), 125 – 132.

[23] **R. H. Schulz**: *On check digit systems using anti-symmetric mappings*, In it Numbers, Information and Complexity, Kluwer Acad. Publ. Boston 2000, 295 – 310.

[24] **R. H. Schulz**: *Equivalence of check digit systems over the dicyclic groups of order 8 and 12*, In *Mathematikdidaktik aus Begeisterung für die Mathematik*, Klett Verlag, Stuttgart 2000, 227 – 237.

[25] **R. H. Schulz**: *Check character systems and anti-symmetric mappings*, In *Computational Discrete Mathematics, LNCS* **2122** (2001), 136 – 147.

[26] **S. Ugan**: *Prüfzeichensysteme über dizyklishen Gruppen der Ordnung* 8 *und* 12, Diplomarbeit, FU Berlin, FB Mathematik & Informatik 1999.

[27] **J. Verhoeff**: *Error detecting decimal codes*, **29**, Math. Centre Tracts. Math. Centrum Amsterdam, 1969.

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

e-mail: gbel@math.md (G.B.Belyavskaya)
vizb@math.md (V.I.Izbash)
scerb@math.md (V.A.Shcherbacov)

Received May 28, 2003