n-T-quasigroup codes with one check symbol and their error detection capabilities

Gary L. Mullen, Victor Shcherbacov

Abstract. It is well known that there exist some types of the most frequent errors made by human operators during transmission of data which it is possible to detect using a code with one check symbol. We prove that there does not exist an n-T-code that can detect all single, adjacent transposition, jump transposition, twin, jump twin and phonetic errors over an alphabet that contains 0 and 1. Systems that detect all single, adjacent transposition, jump transposition, twin, jump twin errors and almost all phonetic errors of the form $a0 \to 1a$, $a \neq 0$, $a \neq 1$ over alphabets of different, and minimal size, are constructed. We study some connections between the properties of anti-commutativity and parastroph orthogonality of T-quasigroups. We also list possible errors of some types (jump transposition, twin error, jump twin error and phonetic error) that the system of the serial numbers of German banknotes cannot detect.

Keywords: quasigroup, n-ary quasigroup, check character system, code, the system of the serial numbers of German banknotes

Classification: 94B60, 94B65, 20N05, 20N15

Introduction

Statistical investigations of J. Verhoeff [17] and D.F. Beckley [1] 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, i.e. errors of the form $\dots ab \cdots \longrightarrow \dots ba \dots$, and insertion or deletion errors. We note, if all codewords are of equal length, insertion and deletion errors can be detected easily.

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

Table 1: Error types and their frequencies ([15]).

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

The numbers of Table 1 can vary from sample to sample and may depend on the location of the affected digits; e.g. the rightmost two digits may be affected by single errors more than the other digits together ([17, p. 14], [15], [16]).

It is well known that it is possible to detect some types of the most frequent errors made by human operators during transmission of data using a code with one check symbol ([5], [6], [8], [9], [14]-[17]).

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 ([15], [16])**.** 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 $a_1 a_2 \dots a_n \in Q^n$:

$$\mathfrak{C} : \begin{cases} Q^n \longrightarrow Q^{n+1} \\ a_1 a_2 \dots a_n \longmapsto a_1 a_2 \dots a_n a_{n+1}. \end{cases}$$

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

In this article we verify that the systematic error-detecting codes constructed in [12] allow us to detect almost all errors from Table 1 with the exception of "other errors".

As in [12], we use in the present article the "quasigroup", or, more generally, "n-ary quasigroup" approach to study error-detecting codes with one check symbol.

n-ary quasigroup codes

We shall use basic quasigroup terms and concepts from the books [2], [3], [11], [13].

Let Q be a non-empty set, and let $n \geq 2$ be a natural number. A map f that maps all n-tuples over Q into elements of the set Q is called an *n-ary operation*, i.e. $f(x_1, x_2, \dots, x_n) = x_{n+1}$ for all $(x_1, x_2, \dots, x_n) \in Q^n$ and $x_{n+1} \in Q$.

A sequence $x_m, x_{m+1}, \dots, x_n$ will be denoted by x_m^n. Of course m, n are natural numbers with $m \leq n$. As usual in the study of n-quasigroups, $\overline{1, n} = \{1, 2, \dots, n\}$ ([4]).

Definition 2. 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 an *n-ary quasigroup* ([4]).

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.

Definition 3. We shall call the code $\mathfrak{C}$ with one check character a_{n+1} over an alphabet Q 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 an *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 $a_j \neq b_j$.

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 $g(a_1^n) \neq a_{n+1}$.

Theorem 1. *Any n-ary code (Q, g) detects all single errors if and only if it is an n-ary quasigroup code, i.e. an n-ary operation g is an n-ary quasigroup operation* ([9], [6], [12]).

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) ([4]).

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: $f^\sigma(x_{\sigma 1}, x_{\sigma 2},\ \dots,\ x_{\sigma n}) = x_{\sigma(n+1)}$ and $f(x_1, x_2, \dots, x_n) = x_{n+1}$ for all $x_1^{n+1} \in Q$.

For example, $f^{(132)}(x_{(132)1}, x_{(132)2}) = x_{(132)3}$ if and only if $f(x_1, x_2) = x_3$ and we have $f^{(132)}(x_3, x_1) = x_2$ if and only if $f(x_1, x_2) = x_3$.

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

$$f(x_1^{k_1-1}, a_1, x_{k_1+1}^{k_2-1}, a_2, \dots, x_{k_{m+1}}^n),$$

i.e. we obtain a new operation $g(x_1^{k_1-1}, x_{k_1+1}^{k_2-1}, \dots, x_{k_{m+1}}^n)$. The operation g is an $(n-m)$-ary quasigroup operation. An operation g obtained in such a manner is called *a retract* of the operation f ([4]).

Remark 1 ([12]). By using an n-ary quasigroup retract we can fix in the equality $f(x_1^n) = x_{n+1}$ the last element x_{n+1}.

PROOF: Recall that from the 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 $\sigma = (n, n+1)$. 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 an $(n+1)$*-retract of an n-ary quasigroup operation* f. $\square$

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 $x_1, \dots, x_n$ are information symbols, element x_{n+1} is a check symbol, the element e is a fixed element of the set Q and the operation f is an $(n+1)$-ary 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 an $(n+2)$-retract of an $(n+1)$-ary quasigroup operation $f(x_1^{n+1}) = x_{n+2}$.

The systems most commonly in use ([15]) 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, $i = 1, \dots, n$, and an element e of G, for instance the identity element)

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

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 [15]. We shall denote this code as $\mathfrak{C}_1$.

We give one more definition from [15]: Let $(Q, \star_i)$ be quasigroups; then one uses as check equation

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

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 $\mathfrak{C}_2$.

Theorem 2. *The code $\mathfrak{C}_1$ is an $(n-1)$-ary quasigroup code and the code $\mathfrak{C}_2$ is an n-ary quasigroup code, i.e. the $(n-1)$-ary operation (respectively the n-ary operation) defined by check equations* (1) *(resp.* (2)*) is an $(n-1)$-ary (n-ary) quasigroup operation* ([12]).

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

On a fixed place $(i, i+k)$ in any fixed codeword transposition and twin error cannot be in the same time. Therefore we can see on transposition, jump transposition, twin and jump twin errors as on two types of errors on two types of places, namely, transpositions $ab \to ba$ and twin errors $aa \to bb$ on places $(i, i+1)$, $(i, i+2)$ for all suitable $i \in \overline{1, n+1}$.

Lemma 1. *In any fixed quasigroup codeword* (a_1^{n+1}) *there cannot be more than* $2n-1$ *different transpositions and twin errors* ([12]).

We recall that a binary quasigroup $(Q, \cdot)$ is called *anti-commutative* (sometimes such a quasigroup is called an *anti-symmetric quasigroup* [6]) if and only if the following implication is true: $x \cdot y = y \cdot x \Rightarrow x = y$ for all $x, y \in Q$ [2].

Definition 4 ([12])**.** We shall call a binary quasigroup $(Q, \cdot)$ *totally anti-commutative* if and only if the following implications are true: $x \cdot y = y \cdot x \Rightarrow x = y$, $x \cdot x = y \cdot y \Rightarrow x = y$ for all $x, y \in Q$.

Definition 5. An n-ary quasigroup (n-quasigroup) of the form $\gamma g(x_1, x_2, \dots, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_n x_n$, where $(Q, +)$ is a group, $\gamma, \gamma_1, \dots, \gamma_n$ are permutations of the set Q, will be called an *n-ary group isotope* (Q, g).

Definition 6. An n-quasigroup of the form $g(x_1, x_2, \dots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n + a = \sum_{i=1}^{n} \alpha_i x_i + a$, where $(Q, +)$ is a group, $\alpha_1, \dots, \alpha_n$ 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 $(Q, +)$).

Definition 7. A linear n-ary quasigroup (Q, g) over an abelian group $(Q, +)$ is called an *n-T-quasigroup*.

Definition 8. An n-ary T-quasigroup (Q, g) of the form $g(x_1, x_2, \dots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n + a$ and with condition $\alpha_i \alpha_j = \alpha_j \alpha_i$ for all $i, j \in \overline{1, n}$ will be called an *n-ary medial quasigroup* ([4]).

Definition 9. 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) ([12]).

Theorem 3 ([12])**.** *A binary T-quasigroup* $(Q, \cdot)$ *of the form* $x \cdot y = \alpha x + \beta y + a$ *is 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*).*

Definition 10 ([12])**.** A retract of the 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 4. *The n-ary quasigroup code (Q, d) detects any transposition and twin error on places of the form $(i, i+k)$ ($i \in \overline{1, n-k}$, $k \in \overline{1, n-1}$, $i+k \leq n$) if and only if all $(i, i+k)$ binary retracts of the 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 a totally 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 a totally anti-commutative quasigroup, and again we have a contradiction.

□

Theorem 5. *Let (Q, d) be a finite n-ary quasigroup of order q. The $(n-1)$-ary quasigroup codes (Q, g_j) ($j \in \overline{1, q}$) with check equations $d_j(x_1^n) = e_j$ where the elements e_j are fixed different elements of the set Q detect any transposition and twin error on places of the form $(i, i+k)$ ($i \in \overline{1, n-k}$, $k \in \overline{1, n-1}$, $i+k \leq n$) if and only if all $(i, i+k)$ binary retracts of (Q, d) are totally anti-commutative quasigroups.*

Proof: Proof of this theorem is the similar to the proof of Theorem 4. □

Theorem 6. *The $(n-1)$-ary quasigroup code (Q, g) with check equation $d(x_1^n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n = e$, where the element e is a fixed element of the set Q, $(Q, +)$ is a group, detects any transposition and twin error on places of the form $(i, i+k)$ ($i \in \overline{1, n-k}$, $k \in \overline{1, n-1}$, $i+k \leq n$) with the exception of errors on place $(1, n)$ if and only if all $(i, i+k)$ ($(i, i+k) \neq (1, n)$) binary retracts of the 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

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

then, since $i \neq 1$ or $i+k \neq n$, it is possible to change the element a_1 or the element a_n in such a manner that

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

Therefore the binary retract $d(a_1^{i-1}, x, a_{i+1}^{i+k-1}, y, a_{i+k+1}^n)$ is not a totally 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

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

then, since $i \neq 1$, or $i+k \neq n$, it is possible to change the element a_1 or the element a_n in such manner that

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

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

□

Corollary 1. *The $(n-1)$-ary quasigroup code (Q, g) with check equation $d(x_1^n) = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_n x_n = e$, where the element e is a fixed element of the set Q, $(Q, +)$ is an abelian group, detects any transposition and twin error on places of the form $(i, i+k)$ $(i \in \overline{1, n-k},\ k \in \overline{1, n-1},\ i+k \leq n)$ if and only if all $(i, i+k)$ binary retracts of n-ary quasigroup (Q, d) are totally anti-commutative quasigroups.*

Proof: We only need to prove that anti-commutativity of binary retracts is a necessary condition to detect any transposition and twin error on the place $(1, n)$.

If we suppose that there are elements a_2^{n-1}, b, c, $(b \neq c)$ such that

$$d(b, a_2^{n-1}, c) = d(c, a_2^{n-1}, b) = k,$$

then, since the group $(Q, +)$ is an abelian group we have a possibility to change the element a_2 in a such manner that

$$d(b, a_2^{n-1}, c) = d(c, a_2^{n-1}, b) = e.$$

Therefore the binary retract $d(x, a_2^{n-1}, y)$ is not a totally anti-commutative quasigroup, the code (Q, g) cannot detect an error on the place $(1, n)$, and we have a contradiction.

If we suppose that there are elements a_2^{n-1}, b, c $(b \neq c)$ such that

$$d(b, a_2^{n-1}, b) = d(c, a_2^{n-1}, c) = k,$$

then, since the group $(Q, +)$ is an abelian group, it is possible to change the element a_2 in such a manner that

$$d(b, a_2^{n-1}, b) = d(c, a_2^{n-1}, c) = e.$$

Therefore the binary retract $d(x, a_2^{n-1} y)$ is not a totally anti-commutative quasigroup, and again we have a contradiction. □

Corollary 2. *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 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.*

Corollary 3. *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 $(i, i+k)$ $(i \in \overline{1, n-k},\ k \in \overline{1, n-1},\ i + k \leq n)$ if and only if all quasigroups of the form $\gamma_i x_i + \gamma_{i+k} x_{i+k}$ are totally anti-commutative quasigroups.*

Theorem 7. *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:*

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

Proof: This follows from Corollary 3 and Theorem 3, but we give direct proof of this theorem. The code (Q, g) can detect a transposition error $(a, b) \longrightarrow (b, a)$, $a \neq b$ on a place $(i, i+k)$ if and only if $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_i a + \cdots + \alpha_{i+k} b + \cdots + \alpha_n x_n \neq \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_i b + \cdots + \alpha_{i+k} a + \cdots + \alpha_n x_n$ for all $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{i+k-1}, x_{i+k+1}, \ldots, x_n \in Q$.

Using properties of abelian group $(Q,+)$ past cancellation we obtain, that the last inequality is equivalent to $\alpha_i a + \alpha_{i+k} b \neq \alpha_i b + \alpha_{i+k} a$, i.e., if $a \neq b$ (definition of a transposition error supposes this condition) then $a \circ b \neq b \circ a$, where $x \circ y = \alpha_i x + \alpha_{i+k} y$ for all $x, y \in Q$, or, equivalently, if $a \circ b = b \circ a$, then $a = b$.

Therefore the condition that the code (Q, g) has a possibility to detect any transposition error on the place $(i, i+k)$ is equivalent to the condition $x \circ y = y \circ x \Rightarrow x = y$ for all $x, y \in Q$.

The last condition is equivalent to the following condition (now we repeat the proof of Proposition 2 from [12]).

$$\begin{aligned}
&(\alpha_i x + \alpha_{i+k} y = \alpha_i y + \alpha_{i+k} x \Rightarrow x = y) \Leftrightarrow \\
&((\alpha_i - \alpha_{i+k})x = (\alpha_i - \alpha_{i+k})y \Rightarrow x = y) \Leftrightarrow \\
&((\alpha_i - \alpha_{i+k})(x - y) = 0 \Rightarrow x = y).
\end{aligned}$$

The last implication will be true for all $x, y \in Q$ if and only if $\alpha_i - \alpha_{i+k}$ is an automorphism of the group $(Q,+)$ (in general the mapping $\alpha_i - \alpha_{i+k}$ is an endomorphism of $(Q,+)$).

Case 2 is proved similarly. The code (Q, g) can detect a twin error $(a, a) \longrightarrow (b, b)$, $a \neq b$, on a place $(i, i+k)$ if and only if $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_i a + \cdots + \alpha_{i+k} a + \cdots + \alpha_n x_n \neq \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_i b + \cdots + \alpha_{i+k} b + \cdots + \alpha_n x_n$ for all $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{i+k-1}, x_{i+k+1}, \ldots, x_n \in Q$.

Using past cancellation in the last inequality, we obtain that the last inequality is equivalent to $\alpha_i a + \alpha_{i+k} a \neq \alpha_i b + \alpha_{i+k} b$, i.e., if $a \neq b$ (definition of a twin error supposes this inequality) then $a \circ a \neq b \circ b$, where $x \circ y = \alpha_i x + \alpha_{i+k} y$ for all $x, y \in Q$, or, equivalently, if $a \circ a = b \circ b$, then $a = b$.

Therefore the condition that the code (Q, g) has a possibility to detect any transposition error on the place $(i, i+k)$ is equivalent to the condition $x \circ x = y \circ y \Rightarrow x = y$ for all $x, y \in Q$.

The last condition is equivalent to the following condition (now we again repeat a proof of Proposition 2 from [12]).

$$\begin{aligned}
&(\alpha_i x + \alpha_{i+k} x = \alpha_i y + \alpha_{i+k} y \Rightarrow x = y) \Leftrightarrow \\
&((\alpha_i + \alpha_{i+k})(x - y) = 0 \Rightarrow x = y).
\end{aligned}$$

The last implication will be true for all $x, y \in Q$ if and only if $\alpha_i + \alpha_{i+k}$ is an automorphism. $\square$

Definition 11 ([12])**.** 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).

Let us give some corollaries of Theorem 7.

Theorem 8. *The existence of at least three different automorphisms α, β, γ of an abelian group $(Q,+)$ such that endomorphisms $\alpha+\beta$, $\alpha+\gamma$, $\beta+\gamma$, $\alpha-\beta$, $\alpha-\gamma$, $\beta-\gamma$ are automorphisms of this group is a necessary and sufficient condition for the existence of a 5-n-T-quasigroup code (Q,d) with check equation $d(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$.*

Proof: Sufficiency. Suppose that we have three different automorphisms of the group $(Q,+)$. If we take $\alpha_{3l+1} = \alpha$, $\alpha_{3l+2} = \beta$, $\alpha_{3l+3} = \gamma$, then we shall have a code (Q,d) with check equation $d(x_1^n) = \alpha x_1 + \beta x_2 + \gamma x_3 + \alpha x_4 + \cdots + \delta x_n = 0$, where ($\delta = \alpha$, if $n = 3k+1$, $\delta = \beta$, if $n = 3k+2$, $\delta = \gamma$, if $n = 3k$).

From Theorem 7 it follows that this code is a 5-n-T-quasigroup code, since it is easy to see that, if the endomorphism $\alpha - \beta$ is an automorphism of the group $(Q,+)$, then the endomorphism $\beta - \alpha$ is an automorphism of the group $(Q,+)$ too, and so on.

Necessity. If we suppose that we have an abelian group $(Q,+)$ and only two its different automorphisms α and β satisfying the conditions on $\alpha+\beta$, $\alpha-\beta$ (or one such automorphism), then it is easy to see, that it is impossible to construct a 5-n-T-quasigroup code. In particular, if we take $\alpha_1 = \alpha$ and $\alpha_2 = \beta$, then: if $\alpha_3 = \alpha$, then this code cannot detect jump transposition errors; if $\alpha_3 = \beta$, then this code cannot detect transposition errors on place $(2,3)$. □

In [17], [9], [8], [16], [6] and some other articles, systems that detect all single and transposition errors are studied.

Corollary 4. *The existence of at least two different automorphisms α, β of an abelian group $(Q,+)$ such that the endomorphism $\alpha - \beta$ is an automorphism of this group are necessary and sufficient conditions for the existence of an n-T-quasigroup code (Q,d) with check equation $d(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$ that detects all single and transposition errors.*

Proof: The proof of this corollary is easy to obtain from Theorem 8. □

Remark 2. It is easy to see that under the assumption of Corollary 4 it is impossible to have $\alpha - \beta = \alpha$, but it is possible that $\alpha - \beta = \beta$.

The following theorem helps to construct 5-n-quasigroup codes.

Theorem 9 ([12])**.** *The direct product of 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 $f = d \circ g$.*

The following theorem is in the spirit of the work [6].

Theorem 10. *There does not exist a 5-n-T-quasigroup code over a cyclic group Z_{2k} and Z_{3k}, where k is an odd number.*

Proof: We use Theorem 7. In the first case it is easy to see that all automorphisms of the group Z_{2m} are multiplying the elements of this group by some odd number. But a sum of two odd numbers is an even number.

In the second case any automorphism has form $3h+1$ or $3l+2$. Then either the sum of two given automorphisms is not an automorphism (if one of the automorphisms is of the form $3h+1$ and the other is of the form $3l+2$), or their difference is not an automorphism (if both have the form $3h+1$, or the form $3l+2$). □

Corollary 5. *There does not exist an n-T-quasigroup code over a cyclic group Z_{2k} that detects all single and transposition errors.*

n-T-quasigroup codes and the detection of phonetic errors

In this section we assume that all quasigroups are defined on a set Q such that $Q = \{0, 1, \ldots, m\}$. We can see a phonetic error $a0 \to 1a$, $a \neq 0$, $a \neq 1$, as a special kind of double error in a code word on a place of the form $(i, i+1)$.

Theorem 11. *A binary T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \alpha x + \beta y + b$ detects all phonetic errors if and only if $(\alpha - \beta)a \neq \alpha 1$ for all $a \in Q$ such that $a \neq 0$, $a \neq 1$.*

Proof: We find conditions when $a \cdot 0 = 1 \cdot a$. We have $a \cdot 0 = \alpha a + b$, $1 \cdot a = \alpha 1 + \beta a + b$. Then the quasigroup $(Q, \cdot)$ cannot detect a phonetic error if and only if $\alpha a + b = \alpha 1 + \beta a + b$, i.e. if and only if $(\alpha - \beta)a = \alpha 1$.

Therefore the T-quasigroup $(Q, \cdot)$ detects all phonetic errors if and only if $(\alpha - \beta)a \neq \alpha 1$ for all $a \in Q$, $a \neq 0$, $a \neq 1$. □

Theorem 12. *There does not exist an $(n-1)$-T-quasigroup code (Q, g) with check equation $d(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$ that simultaneously detects all transposition errors and all phonetic errors on all places of the form $(i, i+1)$.*

Proof: From Theorem 7 it follows, that to detect all transposition errors on a fixed place of the form $(i, i+1)$ the following condition must be fulfilled: the map $\alpha_i - \alpha_{i+1}$ is a permutation of the set Q.

From Theorem 11 it follows that the code (Q, g) detects all phonetic errors on a place $(i, i+1)$ if and only if for all $a \in Q$ such that $a \neq 0$, $a \neq 1$ the following inequality is true: $(\alpha_i - \alpha_{i+1})a \neq \alpha_i 1$.

But if the map $(\alpha_i - \alpha_{i+1})$ is a permutation of the set Q, then we can rewrite the last inequality in the form: $a \neq (\alpha_i - \alpha_{i+1})^{-1} \alpha_i 1$.

We prove that in the last relation $a \neq 0, 1$.

If we suppose that $a = 0$, then $\alpha_i^{-1}(\alpha_i - \alpha_{i+1})0 = 0$, since $\alpha_i, (\alpha_i - \alpha_{i+1})$ are automorphisms of the abelian group $(Q, +)$. Thus $0 = 1$ and we have a contradiction.

If we suppose that $a = 1$, then $(\alpha_i - \alpha_{i+1})1 = \alpha_i 1$, $\alpha_i 1 - \alpha_{i+1} 1 = \alpha_i 1$, $\alpha_{i+1} 1 = 0$, $0 = 1$ and we again have a contradiction.

Therefore if the map $(\alpha_i - \alpha_{i+1})$ is a permutation of the set Q, then there exists an element a of the set Q, $a \neq 0$, $a \neq 1$, such that $(\alpha_i - \alpha_{i+1})a = \alpha_i 1$. In this case the code (Q, g) cannot detect exactly one phonetic error on a fixed place $(i, i+1)$, namely, the phonetic error such that $a = (\alpha_i - \alpha_{i+1})^{-1} \alpha_i 1$. □

Corollary 6. *If in a binary T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \alpha x + \beta y + b$ the map $(\alpha - \beta)$ is a permutation of the set Q, then this quasigroup detects all phonetic errors with the exception of the following error: $c0 \to 1c$ where $c = (\alpha - \beta)^{-1}\alpha 1$.*

Proof: This follows from the proof of Theorem 12. □

Theorem 13. *Any 5-n-T-quasigroup code (Q, g) with check equation $d(x_1^{n+1}) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + \alpha_{n+1} x_{n+1} = 0$ detects all phonetic errors on all possible places of the form $(i, i+1)$ with the exception of one phonetic error on every place of the form $(i, i+1)$.*

Proof: It follows from Theorem 7 that in the code (Q, g) the maps $\alpha_i - \alpha_{i+1}$ are permutations of the set Q for all $i \in \overline{1, n}$.

Then from Corollary 6 it follows that there exists exactly one element c, $c \neq 0$, $c \neq 1$ in the set Q such that $(\alpha_i - \alpha_{i+1})c = \alpha_i 1$. Therefore on the place $(i, i+1)$ the code (Q, g) cannot detect only one phonetic error, namely, the error $c0 \to 1c$. □

Totally anti-commutative T-quasigroups and parastroph orthogonality of T-quasigroups

In this section we study connections between the properties of anti-commutativity and parastroph orthogonality of T-quasigroups.

Definition 12 ([7]). Two finite quasigroups $(Q, \cdot)$ and $(Q, *)$ defined on the same set Q are said to be *orthogonal* if the pair of equations $x \cdot y = a$ and $x * y = b$ (where a and b are any two given elements of Q) are satisfied simultaneously by a unique pair of elements x and y from Q.

A. Sade ([14], [7]) called a quasigroup $(Q, \cdot)$ *anti-abelian* if it is orthogonal to its (12)-parastroph $(Q, \star)$: that is, if $x \cdot y = z \cdot t$ and $y \cdot x = t \cdot z$ ($x \star y = z \star t$) then $x = z$ and $y = t$.

M. Damm ([6]) proved that any anti-abelian quasigroup is a totally anti-commutative quasigroup.

Theorem 14. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ over a commutative group $(Q, +)$ and its (12)-parastroph $(Q, \star)$ of the form $x \star y = \psi x + \varphi y + c$ are orthogonal if and only if the map $\varphi^{-1}\psi - \psi^{-1}\varphi$ is an automorphism of the group $(Q, +)$.*

Proof: A quasigroup $(Q, \cdot)$ and its (12)-parastroph $(Q, \star)$ are orthogonal if and only if the system of equations

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

has a unique solution. Using conditions of this theorem we can rewrite the last system in the form

$$\begin{cases} \varphi x + \psi y + c = a \\ \varphi y + \psi x + c = b. \end{cases}$$

If we apply the automorphism φ^{-1} to the first equation and $-\psi^{-1}$ to the second equation, then upon adding the equations, we shall obtain $(\varphi^{-1}\psi - \psi^{-1}\varphi)y = \varphi^{-1}a - \psi^{-1}b - \varphi^{-1}c + \psi^{-1}c$.

If we apply the automorphism ψ^{-1} to the first equation and $-\varphi^{-1}$ to the second equation, then upon adding the equations, we shall obtain $(\psi^{-1}\varphi - \varphi^{-1}\psi)x = \psi^{-1}a - \varphi^{-1}b - \psi^{-1}c + \varphi^{-1}c$.

It is easy to see that $(\varphi^{-1}\psi - \psi^{-1}\varphi) = -(\psi^{-1}\varphi - \varphi^{-1}\psi)$. Taking into consideration the fact that all automorphisms of an abelian group $(Q,+)$ lie in the ring $\mathrm{End}(Q,+,\cdot)$ of endomorphisms of the group $(Q,+)$, we have $-(\psi^{-1}\varphi - \varphi^{-1}\psi) = -\psi^{-1}\varphi + \varphi^{-1}\psi = \varphi^{-1}\psi - \psi^{-1}\varphi$.

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

We may prove the following

Theorem 15. *A T-quasigroup $(Q,\cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ is a totally anti-commutative quasigroup if and only if it is an anti-abelian quasigroup.*

Proof: From Theorem 3 it follows that a T-quasigroup $(Q,\cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ is totally anti-commutative if and only if the maps $\varphi - \psi$ and $\varphi + \psi$ are permutations of the set Q. From Theorem 14 it follows that a T-quasigroup of the form $x \cdot y = \varphi x + \psi y + c$ is anti-abelian if and only if the map $\varphi^{-1}\psi - \psi^{-1}\varphi$ is a permutation of the set Q.

Therefore to prove the theorem we must show an equivalence of the following conditions:

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

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

Then we have the following equivalence

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

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

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

are equivalent too. □

Let us remark that the implication "$\Leftarrow$" in Theorem 15 follows from the above mentioned result of M. Damm [6].

Theorem 16. *For a T-quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y+c$ over a commutative group $(Q,+)$ the following conditions are equivalent:*

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

Proof: The proof follows from Theorem 14 and Theorem 15. □

Remark 3. For a medial quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y+c$ over a commutative group $(Q,+)$ the following conditions are equivalent

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

Proof: From the definition of a medial quasigroup (Definition 8) we have that $\varphi\psi=\psi\varphi$. Then $(\varphi-\psi)(\varphi+\psi)=\varphi^2+\varphi\psi-\psi\varphi-\psi^2=\varphi^2-\psi^2$. □

Examples

In this section we give some examples of n-T-quasigroup codes that detect all single errors, adjacent transposition errors, jump transposition errors, twin errors, jump twin errors and all or almost all phonetic errors on all possible places of the form $(i,i+1)$.

Example 17. *The International Standard Book Number code (ISBN) uses* $(Z_{11},+)$, $n=10$, *and the check equation* $1\cdot x_1+2\cdot x_2+3\cdot x_3+4\cdot x_4+5\cdot x_5+6\cdot x_6+7\cdot x_7+8\cdot x_8+9\cdot x_9+10\cdot x_{10}\equiv 0 \pmod{11}$.

Using Theorem 7 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 $(5,6)$ as $5+6=11$.

From Corollary 6 it follows that this code cannot detect the following phonetic errors:

$10\,0 \to 1\,10$ on the place $(1,2)$; $9\,0 \to 1\,9$ on the place $(2,3)$;
$8\,0 \to 1\,8$ on the place $(3,4)$; $7\,0 \to 1\,7$ on the place $(4,5)$;
$6\,0 \to 1\,6$ on the place $(5,6)$; $5\,0 \to 1\,5$ on the place $(6,7)$;
$4\,0 \to 1\,4$ on the place $(7,8)$; $3\,0 \to 1\,3$ on the place $(8,9)$;
$2\,0 \to 1\,2$ on the place $(9,10)$.

In particular, on the place $(1,2)$ we have $c = (\alpha - \beta)^{-1}\alpha 1 = (1-2)^{-1} \cdot 1 \cdot 1 = (-1)^{-1}1 = -1 \cdot 1 = -1 = 10$, on the place $(2,3)$ we have $c = (2-3)^{-1} \cdot 2 \cdot 1 = (-1)^{-1}2 = -1 \cdot 2 = -2 = 9$ and so on.

We notice that in the ISBN code number 10 is not used on places $1, 2, \ldots, 9$.

The following code is a modification of the ISBN code ([12]).

Example 18. *We denote a code over the cyclic group $(Z_{11}, +)$ with the check equation $1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 10 \cdot x_6 + 9 \cdot x_7 + 8 \cdot x_8 + 7 \cdot x_9 + 6 \cdot x_{10} \equiv 0 \pmod{11}$ as a (Z_{11}, g)-code.*

Proof: It follows from Theorem 7 that the (Z_{11}, g)-code detects all single errors, transposition and twin errors on places $(i, i+1)$, $(i, i+2)$ for any permissible value of index i. This code detects 10 from 11 possible phonetic errors on any place of the form $(i, i+1)$ for any $i \in \overline{1, 9}$.

We can enumerate phonetic errors which the (Z_{11}, g)-code cannot detect.

$10\,0 \to 1\,10$ on the place $(1,2)$; $9\,0 \to 1\,9$ on the place $(2,3)$;
$8\,0 \to 1\,8$ on the place $(3,4)$; $7\,0 \to 1\,7$ on the place $(4,5)$;
$10\,0 \to 1\,10$ on the place $(5,6)$; $10\,0 \to 1\,10$ on the place $(6,7)$;
$9\,0 \to 1\,9$ on the place $(7,8)$; $8\,0 \to 1\,8$ on the place $(8,9)$;
$7\,0 \to 1\,7$ on the place $(9,10)$.

Note that on the place $(5,6)$ we have $c = 10$, as $(5-10)^{-1} \cdot 5 \cdot 1 = (-5)^{-1} \cdot 5 = 6^{-1} \cdot 5 = 2 \cdot 5 = 10$. □

Example 19. *Let $(Q, +) = (Z_m \times Z_m, +)$ where m is a natural number, $m \geq 2$,* G.C.D.$(m, 3) = 1$. *For instance, let $m = 2$ (minimal possible value of m) or $m = 5$. Let*

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

We define the $(n-1)$-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 the element x_n is a check character, $x_1^n \in Q$, ($\delta = \alpha$, if $n = 3k+1$, $\delta = \beta$, if $n = 3k+2$, $\delta = \gamma$, if $n = 3k$). This code 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: This example is a generalization of Example 6 from [12]. The proof is similar to the proof of Example 6 [12]. Taking into consideration Theorem 7 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 $(Z_m \times Z_m, +)$.

Let $\det(\alpha)$ denote the 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 also automorphisms of the group $(Z_m \times Z_m, +)$.

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 $i \in \overline{1, n-2}$. □

We calculate phonetic errors that this code cannot detect. Denote the element $(1;0)$ as 1 and the element $(0;0)$ as 0. The code cannot detect the error $(-1;-1)0 \to 1\,(-1;-1)$ on places of the form $(1+3k; 2+3k)$, the error $(1;-1)0 \to 1\,(1;-1)$ on places of the form $(2+3k; 3+3k)$, the error $(1;1)0 \to 1\,(1;1)$ on places of the form $(3+3k; 4+3k)$ where k is a natural number.

Remark 4. The last example shows that the existence of three different automorphisms of an abelian group $(Q,+)$ is a sufficient condition for the existence a 5-n-T-quasigroup code (Q,d) over this group with the check equation $d(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$.

Proof: If $m = 2$, then we have $\alpha = -\alpha$, $\beta = -\beta$, $\gamma = -\gamma$, $\alpha+\beta = \gamma$, $\alpha+\gamma = \beta$ and $\beta+\gamma = \alpha$. □

Example 20. *Let $(Q,+) = (Z_m \times Z_m, +)$ where m is a natural number, $m \geq 3$, G.C.D.$(m,5) = 1$. For example, let $m = 3$ (minimal possible value of m) or $m = 7$. Let*

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

We define the $(n-1)$-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 the element x_n is a check character, $x_1^n \in Q$, ($\delta = \alpha$, if $n = 3k+1$, $\delta = \beta$, if $n = 3k+2$, $\delta = \gamma$, if $n = 3k$), $0 = (0,0)$. This code 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: The proof is similar to proof of Example 19. □

Using Example 20 it is possible to construct a 5-n-T-quasigroup code over the group $(Z_3 \times Z_3, +)$.

Example 21. *We take a Cayley table of the group* $(Z_3 \times Z_3, +)$ *in the form*

+	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	3	1	5	6	4	8	9	7
3	3	1	2	6	4	5	9	7	8
4	4	5	6	7	8	9	1	2	3
5	5	6	4	8	9	7	2	3	1
6	6	4	5	9	7	8	3	1	2
7	7	8	9	1	2	3	4	5	6
8	8	9	7	2	3	1	5	6	4
9	9	7	8	3	1	2	6	4	5

and take $\rho = \varepsilon$, $\sigma = (1)\,(2\,4\,8\,9\,3\,7\,6\,5)$, $\tau = (1)\,(2\,5\,6\,7\,3\,9\,8\,4)$.

We define an $(n-1)$*-ary quasigroup code* $(Z_3 \times Z_3, f)$ *with check equation*

$$\rho x_1 + \sigma x_2 + \tau x_3 + \rho x_4 + \sigma x_5 + \cdots + \delta x_n = 1,$$

where elements x_1^{n-1} *are information symbols and the element* x_n *is a check character,* $x_i \in Z_3 \times Z_3$, $1 \leq i \leq n$, *(*$\delta = \rho$*, if* $n = 3k+1$*,* $\delta = \sigma$*, if* $n = 3k+2$*,* $\delta = \tau$*, if* $n = 3k$*). This code 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* $i \in \overline{1, n-2}$*. In this code there cannot be phonetic errors of the form* $a0 \to 1a$*,* $a \neq 0$*,* $a \neq 1$*.*

Proof: We take only a rewritten form of automorphisms α, β, γ from Example 20 for the group $(Z_3 \times Z_3, +)$. It is clear that $\alpha = \rho$, $\beta = \sigma$, $\gamma = \tau$. It follows from Example 20 that this code detects all five types of errors.

Since in the alphabet of this code there is no zero element, this code allows to avoid phonetic errors of the form $a0 \to 1a$, $a \neq 0$, $a \neq 1$. Therefore we may say that this code detects all errors from Table 1 with the exception of "other errors". □

Example 22 ([12])**.** *Let* $(Z_p, +)$ *be a cyclic group of prime order* $p \geq 7$*. An* $(n-1)$*-ary quasigroup code* (Z_p, g) *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 single error, any transposition and twin error on places* $(i, i+1)$ *where* $i \in \overline{1, n-1}$*,* $(i, i+2)$ *where* $i \in \overline{1, n-2}$*.*

We notice that this code cannot detect the following phonetic errors: $(-1; 0) \to (1; -1)$ on places of the form $(1+3k; 2+3k)$; $(-2; 0) \to (1; -2)$ on places of the form $(2+3k; 3+3k)$; $(2^{-1} \cdot 3; 0) \to (1; 2^{-1} \cdot 3)$ on places of the form $(3+3k; 4+3k)$.

Example 23. *Let $(Z_{2n+1}, +)$ be a cyclic group of order $(2n+1) \geq 7$ and the number $2n+1$ be prime. An n-ary quasigroup code (Z_{2n+1}, g) with check equation*

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

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

Proof: It is known that multiplying by elements of the group $(Z_{2n+1}, +)$ ($2n+1$ is a 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 all sums and differences of different automorphisms of the set of automorphism $\{1, 2, \ldots, n\}$ are automorphisms of the group $(Z_{2n+1}, +)$. It is easy to see that this is so.

Therefore our code can detect all single errors, transposition and twin errors on all places $(i, i+k)$, for all suitable values of i, k. □

Theorem 24. *There exists a 5-n-T-quasigroup code:*

- *of any prime order $p \geq 7$;*
- *of any order m^2, where $m > 1$;*
- *of any composite order d such that $d = m^2 p_1 p_2 \ldots p_s$, where $m \geq 1$, $p_i \geq 7$.*

Proof: The proof follows from Examples 22, 19, 20 and Theorem 9. □

Remark 5. It is possible to check that there does not exist an 5-T-quasigroup code (i.e. a code that detects 5 types of the errors) over an alphabet of order $3, 5, 6$. Some other results of such kind are available in [6].

On possibilities of the system of the serial numbers of German banknotes to detect the most frequent errors made by human operators during transmission of data

The system of the serial numbers of German banknotes is one of the oldest and the most famous check digit systems with one check symbol.

This system was constructed over the dihedral group $(D_5, +)$ of order 10 with the check equation $\delta^1 a_1 + \delta^2 a_2 + \cdots + \delta^{10} a_{10} + a_{11} = 0$, where numbers a_1^{10} are information symbols and the number a_{11} is a check digit, $\delta = (0\,1\,5\,8\,9\,4\,2\,7)(3\,6)$ is an anti-symmetric mapping ([15], [16]). This mapping was found by J. Verhoeff ([17]). It is well known that this code detects all single and all transposition errors [6]. We can enumerate twin, spring twin, spring transposition and phonetic errors that this code cannot detect. We used the following Cayley table of the group

$(D_5, +)$.

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

The system of the serial numbers of German banknotes cannot detect the following twin errors:

$66 \leftrightarrow 44$ $77 \leftrightarrow 99$ on the place $(1, 2)$;
$33 \leftrightarrow 99$ $22 \leftrightarrow 88$ on the place $(2, 3)$;
$44 \leftrightarrow 55$ $66 \leftrightarrow 88$ on the place $(3, 4)$;
$33 \leftrightarrow 55$ $99 \leftrightarrow 11$ on the place $(4, 5)$;
$11 \leftrightarrow 66$ $00 \leftrightarrow 88$ on the place $(5, 6)$;
$00 \leftrightarrow 33$ $55 \leftrightarrow 77$ on the place $(6, 7)$;
$11 \leftrightarrow 22$ $66 \leftrightarrow 77$ on the place $(7, 8)$;
$22 \leftrightarrow 33$ $00 \leftrightarrow 44$ on the place $(8, 9)$;
$66 \leftrightarrow 44$ $77 \leftrightarrow 99$ on the place $(9, 10)$
$11 \leftrightarrow 88$ $44 \leftrightarrow 77$ on the place $(10, 11)$.

We notice on place $(10, 11)$ this code cannot detect the transposition errors $18 \leftrightarrow 81$, $47 \leftrightarrow 74$.

On place $(1, 3)$ the code cannot detect the following errors:
$000 \leftrightarrow 202$, $303 \leftrightarrow 404$, $505 \leftrightarrow 909$, $002 \leftrightarrow 200$, $304 \leftrightarrow 403$, $509 \leftrightarrow 905$,
$212 \leftrightarrow 919$, $717 \leftrightarrow 818$, $219 \leftrightarrow 912$, $718 \leftrightarrow 817$,
$020 \leftrightarrow 525$, $222 \leftrightarrow 929$, $121 \leftrightarrow 626$, $025 \leftrightarrow 520$, $126 \leftrightarrow 621$, $229 \leftrightarrow 922$,
$232 \leftrightarrow 737$, $838 \leftrightarrow 939$, $237 \leftrightarrow 732$, $839 \leftrightarrow 938$,
$040 \leftrightarrow 545$, $141 \leftrightarrow 646$, $848 \leftrightarrow 949$, $045 \leftrightarrow 540$, $146 \leftrightarrow 641$, $849 \leftrightarrow 948$,
$050 \leftrightarrow 858$, $252 \leftrightarrow 757$, $058 \leftrightarrow 850$, $257 \leftrightarrow 752$,
$161 \leftrightarrow 464$, $363 \leftrightarrow 666$, $565 \leftrightarrow 767$, $164 \leftrightarrow 461$, $161 \leftrightarrow 464$, $366 \leftrightarrow 663$,
$070 \leftrightarrow 272$, $777 \leftrightarrow 878$, $072 \leftrightarrow 270$, $778 \leftrightarrow 877$,
$080 \leftrightarrow 888$, $383 \leftrightarrow 484$, $585 \leftrightarrow 989$, $088 \leftrightarrow 880$, $384 \leftrightarrow 483$, $589 \leftrightarrow 985$,
$191 \leftrightarrow 494$, $393 \leftrightarrow 696$, $595 \leftrightarrow 797$, $194 \leftrightarrow 491$, $396 \leftrightarrow 693$, $597 \leftrightarrow 795$.

As on place $(1, 3)$, on places $(2, 4)$ $(3, 5)$, $(4, 6)$, $(5, 7)$, $(6, 8)$, $(7, 9)$, $(8, 10)$ this code cannot detect 104 transposition and twin errors. On place $(9, 11)$ this code cannot detect 144 transposition and twin errors. The authors found a full list of twin and transpositions errors which the system of the serial numbers of German banknotes cannot detect on these places.

This system cannot detect the following phonetic errors: $20 \leftrightarrow 12$ on place $(5,6)$, $50 \leftrightarrow 15$ on place $(8,9)$ and $70 \leftrightarrow 17$ on place $(10,11)$.

Acknowledgment. The authors thank Professor G.B. Belyavskaya and Professor V.I. Arnautov for their helpful comments. The authors also thank the referee for her/his very useful remarks and comments.

References

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

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

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

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

[5] Belyavskaya G.B., Izbash V.I., Mullen G.L., *Check character systems using quasigroups, I and II*, preprints.

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

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

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

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

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

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

[12] Mullen G.L., Shcherbacov V., *Properties of codes with one check symbol from a quasigroup point of view*, Bul. Acad. Ştiinte Repub. Mold. Mat. 2002, no 3, pp. 71–86.

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

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

[15] Schulz R.-H., *Check Character Systems and Anti-symmetric Mappings*, H. Alt (Ed.): Computational Discrete Mathematics, Lecture Notes in Comput. Sci. 2122, 2001, pp. 136–147.

[16] Schulz R.-H., *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.

[17] Verhoeff J., *Error Detecting Decimal Codes*, Vol. 29, Math. Centre Tracts. Math. Centrum Amsterdam, 1969.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail: mullen@math.psu.edu

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

E-mail: scerb@math.md

(*Received* October 7, 2003, *revised* December 17, 2003)