Quasigroups and Related Systems **18** (2010), 7 – 16

# Check character systems and totally conjugate orthogonal T-quasigroups

*Galina B. Belyavskaya*

Devoted to the memory of Valentin D. Belousov (1925-1988)

**Abstract.** We continue investigations of check character systems with one check character over quasigroups under check equations without a permutation. These systems always detect all single errors (i.e., errors in only one component of a code word) and can detect some other errors occuring during transmission of data. For construction of such systems we use totally conjugate orthogonal $T$-quasigroups. These quasigroups are isotopic to abelian groups and have six mutually orthogonal conjugate quasigroups. We prove that a check character system over any totally conjugate orthogonal $T$-quasigroup is able to detect all transpositions and twin errors and establish additional properties of a totally conjugate orthogonal $T$-quasigroup by which such system can detect all jump transpositions and all jump twin errors. Some models of totally conjugate orthogonal $T$-quasigroups which satisfy all of the required properties for detection of each of the considered types of errors and an information with respect to the spectrum of such quasigroups are given.

## 1. Introduction

In this article we deal with error detecting systems (codes) with a single control symbol. Such systems have specific applications and are used for the detection of certain types of errors. More exactly, we study check character (or digit) systems with one check character.

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

2000 Mathematics Subject Classification: 94B60, 20N05
Keywords: check character system, $T$-quasigroup, conjugate orthogonal quasigroup, orthomorphism.

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. These errors can be distinct types: single errors (that is errors in only one component of a code word), (adjacent) 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 so on can be made by human operators. Single errors and transpositions are the most prevalent ones.

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 work of I. Verhoeff [13] is the first significant publication relating to these systems. In this work decimal codes known in the 1970s are presented. A. Ecker and G. Poch in [8] have given a survey of check character systems and their analysis from a 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. Studies of check character systems were continued by R.-H. Schulz in [12]. He established necessary and sufficient conditions for a quasigroup with control formula (3) (see below) to detect transpositions and jump transpositions not only in information digits but, in addition, in the control digit of a code word $a_1a_2...a_n$. The complete survey of check character systems using quasigroups one can find in [3] due to G.B. Belyavskaya, V.I. Izbash, and V.A. Shcherbacov.

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.

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

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

$$(\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3)\dots) \cdot \delta_n a_n = c \tag{2}$$

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

It is easy to see that a CCS with check formula (1) or (2) 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 $\delta_i$ in (1), (2) is chosen such that $\delta_i = \delta^{i-1}$, $i = 1, \ldots, n$, for a fixed permutation $\delta$ of $Q$. In this case we obtain the following check formulas respectively:

$$a_n = (\ldots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3)\ldots) \cdot \delta^{n-2} a_{n-1}, \tag{3}$$

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

In [4] CCSs over quasigroups with the check equation (3) or (4) are studied. In the article [5], which is a continue of [4], CCSs over $T$-quasigroups are considered, some properties of a $T$-quasigroup so that the CCS over it is able to detect transpositions, jump transpositions, twin errors and jump twin errors are established. Besides, some models of $T$-quasigroups, which satisfy all of the required properties for detection of errors of each of the considered types are given.

It is known that if a CCS over a quasigroup detects some of five considered types of errors, then this quasigroup has orthogonal mate (see, for example, [4, Corollary 1 and Corollary 5], [2, Proposition 3]).

On the other hand, in the article [6] the quasigroups, all six conjugates of which are distinct and pairwise orthogonal, are studied. Such quasigroups were called totally conjugate orthogonal quasigroups (shortly, *totCO*-quasigroups). Necessary and sufficient conditions that a $T$-quasigroup be a *totCO*-quasigroup (a *totCO*-$T$-quasigroup) are established.

In this article we continue to research check character systems with one check character over quasigroups under the check equation (3) or (4) when $\delta = \varepsilon$, $n > 4$. For constructing of such systems we use totally conjugate orthogonal $T$-quasigroups. These quasigroups generalize medial quasigroups and have six mutually orthogonal conjugate quasigroups.

We prove that a CCS over any totally conjugate orthogonal $T$-quasigroup is able to detect, besides single errors, all transpositions and all twin errors and establish additional properties of a totally conjugate orthogonal $T$-quasigroup such that a system over it can detect all jump transpositions and all jump twin errors. Some models of totally conjugate orthogonal $T$-quasigroups which satisfy all of the required properties to detect each of the considered types of errors and an information with respect to the spectrum of such quasigroups are given.

## 2. Check character systems over T-quasigroups

In this section we remind some necessary notions and results of [4,5] with respect to the check character systems using T-quasigroups.

A *quasigroup* is an ordered pair $(Q, A)$ (or $(Q, \cdot)$) where $Q$ is a set and $A$ (or $\cdot$) is a binary operation defined on $Q$ such that each of the equations $A(a, y) = b$ and $A(x, a) = b$ is uniquely solvable for any pair of elements $a, b$ in $Q$. It is known that the multiplication table of a finite quasigroup defines a Latin square [7].

A quasigroup $Q(\cdot)$ is called a *$T$-quasigroup* if there exist an abelian group $Q(+)$, with automorphisms $\varphi$ and $\psi$, and an element $c \in Q$ such that

$$x \cdot y = \varphi x + \psi y + c$$

for all $x, y \in Q$. Such quasigroups were considered by T. Kepka and P. Nemec in [10]. They are special cases of quasigroups, which are isotopic to abelian groups and generalize the well-known class of *medial quasigroups* when, in addition, the automorphisms $\varphi$ and $\psi$ commute, that is $\varphi\psi = \psi\varphi$. Note that below maps in a composition act from the right to the left.

A permutation $\alpha$ of a group $Q(+)$ is called an *orthomorphism* (respectively a *complete mapping*) if $x - \alpha x = \beta x$ ($x + \alpha x = \beta x$) where $\beta$ is a permutation of $Q$ and $-x = Ix$ is the inverse element for $x$ in the group $Q(+)$ [9]. It is easy to see (cf. [9]) that an automorphism $\alpha$ of a finite group $Q(+)$ is an orthomorphism if and only if $\alpha$ is a regular automorphism, that is the identity 0 of the group $Q(+)$ is the only element of $Q$ fixed by $\alpha$ : $\alpha x \neq x$ if $x \neq 0$. If $\alpha$ is an orthomorphism, then $I\alpha$ is a complete mapping of $Q(+)$. A *complete mapping* of a quasigroup $Q(\cdot)$ 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 $Q$.

Denote by $OrtQ(+)$ the set of all orthomorphisms of a group $Q(+)$. In [5] the following theorems with respect to check character systems over $T$-quasigroups were proved (Theorem 1, Theorem 2 and Theorem 4 of [5] respectively) which we shall use.

**Theorem 1. [5]** *A check character system using a finite $T$-quasigroup $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ and check formula* (3) *with $n > 4$ is able to detect*

1. *single errors;*
2. *transpositions if and only if $\psi\delta\varphi^{-1}$, $\psi\delta\psi^{-1}\varphi^{-1}$, $I\psi\delta^{n-2} \in OrtQ(+)$;*
3. *jump transpositions if and only if $\psi\delta^2\varphi^{-2}$, $\psi\delta^2\psi^{-1}\varphi^{-2}$, $I\varphi\psi\delta^{n-3}$ are in $OrtQ(+)$;*

4. *twin errors if and only if* $i\psi\delta\varphi^{-1}$, $I\psi\delta\psi^{-1}\varphi^{-1}$, $\psi\delta^{n-2} \in OrtQ(+)$;
5. *jump twin errors if and only if* $I\psi\delta^2\varphi^{-2}$, $I\psi\delta^2\psi^{-1}\varphi^{-2}$, $\varphi\psi\delta^{n-3}$ *are in* $OrtQ(+)$. □

**Theorem 2. [5]** *In Theorem* 1 *let* $\delta = \varepsilon$. *Then a check character system detects*

1. *single errors;*
2. *transpositions if and only if the automorphisms* $\varphi\psi^{-1}$, $\varphi$, $I\psi$ *are regular;*
3. *jump transpositions if and only if the automorphisms* $\varphi^2\psi^{-1}$, $\varphi^2$, $I\varphi\psi$ *are regular;*
4. *twin errors if and only if the automorphisms* $I\varphi\psi^{-1}$, $I\varphi$, $\psi$ *are regular;*
5. *jump twin errors if and only if the automorphisms* $I\varphi^2\psi^{-1}$, $I\varphi^2$, $\varphi\psi$ *are regular.* □

**Theorem 3. [5]** *A check character system using a finite* $T$*-quasigroup* $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ *and check formula* (4) *with* $\delta = \varepsilon$, $n > 4$, *detects*

1. *single errors;*
2. *transpositions if and only if the automorphisms* $\varphi$ *and* $\varphi\psi^{-1}$ *are regular;*
3. *jump transpositions if and only if the automorphisms* $\varphi^2$ *and* $\varphi^2\psi^{-1}$ *are regular;*
4. *twin errors if and only if the automorphisms* $I\varphi$, $I\varphi\psi^{-1}$ *are regular;*
5. *jump twin errors if and only if the automorphisms* $I\varphi^2$ *and* $I\varphi^2\psi^{-1}$ *are regular.* □

## 3. Totally conjugate orthogonal T-quasigroups

In this section we shall give some necessary notions and results of [6] with respect to the totally conjugate orthogonal $T$-quasigroups.

With any quasigroup $(Q, A)$ the system $\Sigma$ of six (not necessarily distinct) *conjugates* (*parastrophes*) is connected:

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

where $A(x, y) = z \Leftrightarrow A^{-1}(x, z) = y \Leftrightarrow {}^{-1}A(z, y) = x \Leftrightarrow A^*(y, x) = z$.

It is known [11] that the number of distinct conjugates in $\Sigma$ can be 1,2,3 or 6. Using suitable Belousov's designation of conjugates of a quasigroup $(Q, A)$ of [1] we have the following system $\Sigma$ of conjugates:

$$\Sigma = \left\{A,\ {}^{r}A,\ {}^{l}A,\ {}^{lr}A,\ {}^{rl}A,\ {}^{s}A\right\},$$

where ${}^{1}A = A$, ${}^{r}A = A^{-1}$, ${}^{l}A = {}^{-1}A$, ${}^{lr}A = {}^{-1}(A^{-1})$, ${}^{rl}A = ({}^{-1}A)^{-1}$, ${}^{s}A = A^{*}$. Note that $\left({}^{-1}(A^{-1})\right)^{-1} = {}^{rlr}A = {}^{-1}\left(({}^{-1}A)^{-1}\right) = {}^{lrl}A = {}^{s}A$ and ${}^{rr}A = {}^{ll}A = A$, ${}^{\sigma\tau}A = {}^{\sigma}({}^{\tau}A)$.

Two quasigroups $(Q, A)$ and $(Q, B)$ are *orthogonal* if the system of equations $\{A(x, y) = a,\ B(x, y) = b\}$ is uniquely solvable for all $a, b \in Q$.

A set $\Sigma = \{A_1, A_2, ..., A_n\}$ of quasigroups, defined on the same set, is orthogonal if any two quasigroups of it are orthogonal.

Quasigroups which are *orthogonal* to some their conjugates or two conjugates of which are orthogonal (known as *conjugate orthogonal or parastrophic-orthogonal quasigroups*) have encouraged great interest.

In [6] the quasigroups $(Q, A)$ all conjugates of which are pairwise orthogonal and the spectrum of such quasigroups were considered. For these quasigroups the set of all conjugates $\Sigma = \left\{A,\ {}^{r}A,\ {}^{l}A,\ {}^{lr}A,\ {}^{rl}A,\ {}^{s}A\right\}$ is orthogonal.

**Definition 1. [6]** A quasigroup $(Q, A)$ is called *totally conjugate orthogonal* (shortly, a *totCO-quasigroup*) if all its conjugates are pairwise orthogonal.

It is clear that a *totCO*-quasigroup is invariant with respect to the transformation of conjugation ( that is if a quasigroup $(Q, A)$ is a *totCO*-quasigroup then the quasigroup $(Q, {}^{\sigma}A)$ is also a *totCO*-quasigroup for any conjugate ${}^{\sigma}A$) and that all conjugates of a *totCO*-quasigroup are distinct.

Let $\varphi$ and $\psi$ be automorphisms of an abelian group $(Q, +)$ and $(\varphi + \psi)x = \varphi x + \psi x$ for any $x \in Q$, then $\varphi + \psi$ is an endomorphism of group $(Q, +)$. It is known that all endomorphisms of an abelian group form an associative ring with a unity under the operations of addition and multiplication.

**Theorem 4. [6]** *Let $(Q, A)$ be a finite or infinite $T$-quasigroup of the form $A(x, y) = \varphi x + \psi y$. Then two its conjugates are orthogonal if and only if the maps corresponding to these conjugates:*

$(1 \perp l \text{ or } s \perp lr) \to \varphi + \varepsilon$, $(r \perp rl) \to \varphi + \varepsilon$ *and* $\varphi - \varepsilon$,

$(1 \perp r \text{ or } s \perp rl) \to \psi + \varepsilon$, $(l \perp lr) \to \psi + \varepsilon$ *and* $\psi - \varepsilon$,

$(1 \perp lr \text{ or } s \perp l) \to \varphi + \psi^2$, $(1 \perp rl \text{ or } s \perp r) \to \varphi^2 + \psi$,

*$(r \perp lr$ or $rl \perp l) \to \varphi - \psi$, $(1 \perp s) \to \varphi - \psi$ and $\varphi + \psi$,*
*$(l \perp r$ or $lr \perp rl) \to \psi\varphi - \varepsilon$ are permutations.* □

As it was noted in [6], for a $T$-quasigroup of the form $A(x,y) = \varphi x + \psi y + c$ with $c \neq 0$ the conditions of Theorem 4 are the same and do not depend on the element $c$. So if a $T$-quasigroup $(Q, A)$: $A(x,y) = \varphi x + \psi y$ is a *totCO*-quasigroup, then the $T$-quasigroup $(Q, B)$: $B(x,y) = \varphi x + \psi y + c$ is also a *totCO*-quasigroup for any $c \in Q$.

**Theorem 5. [6]** *A $T$-quasigroup $(Q, A)$: $A(x,y) = \varphi x + \psi y + c$ is a totCO-quasigroup if and only if all maps $\varphi + \varepsilon$, $\varphi - \varepsilon$, $\psi + \varepsilon$, $\psi - \varepsilon$, $\varphi^2 + \psi$, $\psi^2 + \varphi$, $\varphi - \psi$, $\varphi + \psi$, $\psi\varphi - \varepsilon$ are permutations.* □

The conditions of Theorem 5 we can write otherwise:

**Theorem 5a.** *A $T$-quasigroup (a medial quasigroup) $(Q, A)$: $A(x,y) = \varphi x + \psi y + c$ is a totCO-quasigroup if and only if all maps $\varphi^2 - \varepsilon$, $\psi^2 - \varepsilon$, $\varphi^2 + \psi$, $\psi^2 + \varphi$, $\varphi - \psi$, $\varphi + \psi$, $\psi\varphi - \varepsilon$ (all maps $\varphi^2 - \varepsilon$, $\psi^2 - \varepsilon$, $\varphi^2 + \psi$, $\psi^2 + \varphi$, $\varphi^2 - \psi^2$, $\psi\varphi - \varepsilon$ respectively) are permutations.*

*Proof.* Indeed, $(\varphi + \varepsilon)(\varphi - \varepsilon) = \varphi^2 - \varepsilon$, $(\psi + \varepsilon)(\psi - \varepsilon) = \psi^2 - \varepsilon$, and in the case of a medial quasigroup $(\varphi - \psi)(\varphi + \psi) = \varphi^2 - \psi^2$. □

Note that an operation $A$ of the form $A(x,y) = (ax + by + c) \pmod n$, $n \geqslant 2$, is a quasigroup if and only if the numbers $a, b$ modulo $n$ are relatively prime to $n$. In this case $\varphi = L_a$, $\psi = L_b$, where $L_a x = ax \pmod n$, $x \in Q = \{0, 1, 2, ..., n-1\}$, are permutations (automorphisms of the additive group modulo $n$) and the quasigroup $Q(A)$ is a $T$-quasigroup (moreover, a medial quasigroup).

In [6] the following statement (Corollary 2 of [6]) is proved:

**Corollary 1. [6]** *A medial quasigroup $(Q, A)$: $A(x,y) = (ax+by) \pmod n$ is a totCO-quasigroup if and only if all elements $a+1, a-1, b+1, b-1, a^2 + b, b^2 + a, a - b, a + b, ab - 1$ modulo $n$ are relatively prime to $n$.* □

This corollary can be rewrite otherwise:

**Corollary 1a.** *A medial quasigroup $(Q, A)$: $A(x,y) = (ax + by) \pmod n$ is a totCO-quasigroup if and only if all elements $a^2 - 1, b^2 - 1, a^2 + b, b^2 + a, a^2 - b^2, ab - 1$ modulo $n$ are relatively prime to $n$.* □

The following theorem (Theorem 3 of [6]) gives an information with respect to the spectrum of *totCO*-quasigroups.

**Theorem 6.** [6] *For any integer $n \geqslant 11$ which is relatively prime to $2, 3, 5$ and $7$ there exists a totCO-quasigroup of order $n$.* □

## 4. Totally conjugate orthogonal T-quasigroups

Now we shall prove that a CCS over a *totCO-T*-quasigroup with check formulas (3) or (4) is able to detect some errors.

**Theorem 7.** *A check character system using a finite totCO-T-quasigroup* $Q(\cdot): x \cdot y = \varphi x + \psi y + c$ *and check formulae (3) with* $\delta = \varepsilon$, $n > 4$, *detects*

1. *single errors;*
2. *transpositions;*
3. *jump transpositions if and only if the mappings* $\psi - \varphi^2$ *and* $\varepsilon + \varphi\psi$ *are permutations;*
4. *twin errors;*
5. *jump twin errors if and only if the mapping* $\varepsilon + \varphi^2$, $\varphi\psi - \varepsilon$ *are permutations.*

*Proof.* From Theorem 5 it follows that all conditions for transpositions of Theorem 2 are fulled if we take into account that the automorphism $\varphi\psi^{-1}$ is regular if and only if the mapping $\varepsilon - \varphi\psi^{-1}$ (the same $\psi - \varphi$ or $\varphi - \psi$) is a permutation and the automorphism $\varphi$ ( $I\psi$) is regular if and if $\varepsilon - \varphi$ (respectively $\varepsilon + \psi$) is a permutation.

By Theorem 2 a CCS detects jump transpositions if and only if the automorphisms $\varphi^2\psi^{-1}$, $\varphi^2$, $I\varphi\psi$ are regular that is when the mappings $\varepsilon - \varphi^2\psi^{-1}$ (the same $\psi - \varphi^2$), $\varepsilon - \varphi^2$ and $\varepsilon + \varphi\psi$ are permutations. But by Theorem 5a in a *totCO-T*-quasigroup the mapping $\varepsilon - \varphi^2$ is a permutation.

According to Theorem 2 a CCS detects twin errors if and only if the automorphisms $I\varphi\psi^{-1}$, $I\varphi$, $\psi$ are regular, that is the mappings $\varepsilon + \varphi\psi^{-1}$ (the same $\psi + \varphi$), $\varepsilon + \varphi$ and $\varepsilon - \psi$ are permutations. This is by Theorem 5.

At last, by Theorem 2 a CCS detects jump twin errors if and only if the automorphisms $I\varphi^2\psi^{-1}$, $I\varphi^2$, $\varphi\psi$ are regular. It means that the maps $\varepsilon + \varphi^2\psi^{-1}$ (the same $\psi + \varphi^2$), $\varepsilon + \varphi^2$ and $\varepsilon - \varphi\psi$ are permutations. By Theorem 5 the mapping $\psi + \varphi^2$ is a permutation. □

**Corollary 2.** *If in Theorem 7 a totCO-quasigroup* $Q(\cdot)$ *is medial, then in item 5 the condition* $\varphi\psi - \varepsilon$ *can be eliminated.*

*Proof.* Indeed, in any medial quasigroup $Q(\cdot): x \cdot y = \varphi x + \psi y + c$ the automorphisms $\varphi$ and $\psi$ commute, so the mapping $\varphi\psi - \varepsilon = \psi\varphi - \varepsilon$ is a permutation in a *totCO-T*-quasigroup. □

**Theorem 8.** *A check character system using a finite totCO-T-quasigroup* $Q(\cdot): x \cdot y = \varphi x + \psi y + c$ *and check formula* (4) *with* $\delta = \varepsilon$, $n > 4$, *detects*

1. *single errors;*
2. *transpositions;*
3. *jump transpositions if and only if the mapping* $\psi - \varphi^2$ *is a permutation;*
4. *twin errors;*
5. *jump twin errors if and only if the mapping* $\varepsilon + \varphi^2$ *is a permutation.*

*Proof.* Follows from the proof of Theorem 7, if we take into account that for jump transpositions and jump twin errors in Theorem 3 there are less conditions than in Theorem 2. □

As a consequence of Theorems 7, 8 and Corollary 2 we obtain

**Theorem 9.** *A check character system using a finite medial totCO-quasigroup* $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ *and check formula* (3) (resp.(4)) *with* $\delta = \varepsilon$, $n > 4$, *detects single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the mappings* $\psi - \varphi^2$, $\varepsilon + \varphi\psi$ *and* $\varepsilon + \varphi^2$ ($\psi - \varphi^2$ *and* $\varepsilon + \varphi^2$ *respectively*) *are permutations.*

**Corollary 3.** *A check character system using a medial totCO-quasigroup* $Q(\cdot) : x \cdot y = (ax + by + c) \pmod n$ *and check formula* (3) (resp.(4)) *with* $\delta = \varepsilon$, $n > 4$, *detects single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the mappings* $a^2 - b$, $1 + ab$ *and* $1 + a^2$ ($a^2 - b$ *and* $1 + a^2$ *respectively*) *modulo* $n$ *are relatively prime to* $n$.

*Proof.* Indeed, in this case the maps

$$\begin{aligned} \varphi^2 - \psi &: (\varphi^2 - \psi)x = (L_a^2 - L_b)x = (a^2 - b)x \pmod n, \\ \varepsilon + \varphi\psi &: (\varepsilon + \varphi\psi)x = (\varepsilon + L_a L_b)x = (1 + ab)x \pmod n, \\ \varepsilon + \varphi^2 &: (\varepsilon + \varphi^2)x = (\varepsilon + L_a^2)x = (1 + a^2)x \pmod n \end{aligned}$$

are permutations if and only if the corresponding elements modulo $n$ are relatively prime to $n$. Note that in this case the elements $a, b$ are also relatively prime to $n$, since $(Q, \cdot)$ is a quasigroup. □

**Theorem 10.** *For any integer* $n \geqslant 11$ *which is relatively prime to* $2, 3, 5$ *and* $7$ *there exists a medial totCO-quasigroup of order* $n$ *such that the check character system over this quasigroup with the check formulas* (3) *or* (4), $\delta = \varepsilon$, $n > 4$, *detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors.*

*Proof.* Let $\overline{a}$ be the element $a$ modulo $n$ and $(m, n)$ be the greatest common divisor of $m$ and $n$. Consider the medial quasigroup $(Q, \cdot)$: $x \cdot y = 3x + 5y$

(mod $n$) where $(3,n)=1$ and $(5,n)=1$, $Q=\{0,1,2,...,n-1\}$. In this case $a=3, b=5$. According to Proposition 1 of [6] this quasigroup is a $totCO$-quasigroup for any $n$ relatively prime to 2,3,5 and 7.

Check the conditions of Corollary 3 for this quasigroup: $(a^2-b)x = (9-5)x = 4x$, $(1+ab)x = 16x$, $(1+a^2)x = (1+9)x = 10x$ modulo $n$, $x \in Q$. Since $n \geqslant 11$ then the maps $4x, 10x$ modulo $n$ are permutations if $n$ is relatively prime to 2 and 5. Let $n$ be relatively prime to 2,3,5 and 7, then $n \neq 16$ and $n < 16$ only for $n = 11, 13$. These orders are prime numbers, so $(\overline{16}, n) = 1$ for every of these numbers. If $n > 16$, then $\overline{16} = 16$ and $(16,n) = 1$ since $n$ is relatively prime to 2. Thus, the quasigroup $A(x,y) = 3x+5y \pmod{n}$ is the needed $totCO$-quasigroup for any $n$ which is relatively prime to 2,3,5 and 7. □

# References


[1] **V.D. Belousov**, *Parastrophic-orthogonal quasigroups*, Quasigroups and Related Systems **13** (2005), 25 – 72.

[2] **G. Belyavskaya, A. Diordiev**, *On quasi-identities in finite quasigroups*, Bul. Acad. Sci. Republ. Moldova, Matematica **3(49)**, (2005), 19 – 32.

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

[4] **G.B. Belyavskaya, V.I. Izbash, and G.L. Mullen**, *Check character systems using quasigroups, II*, Designs, Codes and Cryptography **37** (2005), 405 – 419.

[5] **G.B. Belyavskaya, V.I. Izbash, and V.A. Shcherbacov**, *Check character systems over quasigroups and loops*, Quasigroups Related Systems **10** (2003), 1 – 28.

[6] **G.B. Belyavskaya, T.V. Popovich**, *Totally conjugate orthogonal quasigroups and complete graphs*, (to appear).

[7] **J. Dénes and A. D. Keedwell**, *Latin Squares and Their Applications*, Academic Press New York; Akademiai Kiado, Budapest, 1974.

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

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

[10] **T. Kepka and P. Nemec**, *T-quasigroups*, Acta Univ. Carolinae Math. Phys. **12** (1971), Part I, No.1, 39 – 49, Part II, No.2, 31 – 39.

[11] **C. C. Lindner and D. Steedly**, *On the number of conjugates of a quasigroup*, Algebra Univ. **5** (1975), 191 – 196.

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

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


Received April 9, 2010

Institute of Mathematics and Computer Science, Academy of Sciences, Academiei str. 5, MD-2028, Chisinau, Moldova, E-mail: gbel1@rambler.ru