Algebra and Discrete Mathematics RESEARCH ARTICLE
Number 2. **(2003).** pp. 1–13

On check character systems over quasigroups and loops

G. B. Belyavskaya

Communicated by Kashu A.I.

Abstract. In this article we study check character systems that is error detecting codes, which arise by appending a check digit a_n to every word $a_1a_2...a_{n-1}$: $a_1a_2...a_{n-1} \to a_1a_2...a_{n-1}a_n$ with the check formula $(...((a_1 \cdot \delta a_2) \cdot \delta^2 a_3)...) \cdot \delta^{n-2} a_{n-1}) \cdot \delta^{n-1} a_n = c$, where $Q(\cdot)$ is a quasigroup or a loop, δ is a permutation of Q, $c \in Q$. We consider detection sets for such errors as transpositions ($ab \to ba$), jump transpositions ($acb \to bca$), twin errors ($aa \to bb$) and jump twin errors ($aca \to bcb$) and an automorphism equivalence (a weak equivalence) for a check character systems over the same quasigroup (over the same loop). Such equivalent systems detect the same percentage (rate) of the considered error types.

1. Introduction

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

$$a_1a_2 \dots a_{n-1} \to a_1a_2 \dots a_{n-1}a_n.$$

In praxis the examples used are among others the following: the European Article Number (EAN) Code, the Universal Product Code (UPC),

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).

2001 Mathematics Subject Classification: *20N05, 20N15, 94B60, 94B65.*

Key words and phrases: *quasigroup, loop, group, automorphism, check character system, code.*

the International Book Number (ISNB) Code, the system of the serial numbers of German banknotes.

The control digit a_{n+1} can calculate by different check formulas (check equations), in particular, with the help of a quasigroup (a loop, a group) $Q(\cdot)$.

The most general check formula is the following:

$$(\ldots((a_1 \cdot \delta_1 a_2) \cdot \delta_2 a_3) \ldots) \cdot \delta_{n-1} a_n = c,$$

where $Q(\cdot)$ is a quasigroup, c is a fixed element of Q, $\delta_1, \delta_2, \ldots, \delta_{n-1}$ are some fixed permutations of Q.

Such a system is called a system over a quasigroup and always detects all single errors (that is errors in only one component of a code word) and can detect other errors of certain patterns arisen during transmission of date if the quasigroup $Q(\cdot)$ has some properties.

The work [9] of J.Verhoeff is the first significant publication relating to these systems with a survey the decimal codes known in the 1970s. The statistical sampling made by J.Verhoeff shows that such errors (of human operators) as single errors ($a \to b$), adjacent transpositions ($ab \to ba$), jump transpositions ($acb \to bca$), twin errors ($aa \to bb$) and jump twin errors ($aca \to bcb$) can arise, where single errors and transpositions are the most prevalent ones.

A.Ecker and G.Poch in [5] 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 systems was explained and new codes were presented that stem from the theory quasigroups.

Studies of check character systems over groups and abelian groups are continued by R.-H.Shulz in a number of papers. In [4] H.M.Damm surveys the results about check character systems over groups and over quasigroups and studies the last ones.

In the article [1] ([2]) the check character systems over arbitrary quasigroups (over T-quasigroups) $Q(\cdot)$ with the control equations

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

and

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

which detect completely single errors, transpositions, jump transpositions, twin errors and jump twin errors, were investigated.

In this article we continue research of check character systems with the check formula (2) over quasigroups and loops. In particular, we consider detection sets of the pointed errors and two equivalences between permutations δ of Q from (2) (between the related systems over the same quasigroup). Namely, we introduce an automorphism equivalence of permutations for a quasigroup and a weak equivalence of permutations for a loop. These equivalences are generalization of the respective equivalence relations considered by J.Verhoeff in [9],H.M.Damm in [4] and R.-H. Schulz in [6,7,8] for the check character systems over groups and characterize systems over the same quasigroup (loop) detecting the same percentage of the considered errors.

2. Check character systems over a quasigroup

In Table 2 of [6] R.-H. Schulz gives an information about detection of errors by check character systems over a group $Q(\cdot)$ with the check formula (2), $n \geqslant 3$. Namely, he reduces detection sets and a rate (percentage) of detection of different error types for these systems. This information we give in Table 1, where

$$\begin{aligned} M_T =& \{(a,b) \in Q^2 \mid a \cdot \delta b \neq b \cdot \delta a, a \neq b\}, \\ M_{JT} =& \{(a,b,c) \in Q^3 \mid ab \cdot \delta^2 c \neq cb \cdot \delta^2 a, b \neq c\}, \\ M_{TE} =& \{(a,b) \in Q^2 \mid a \cdot \delta a \neq b \cdot \delta b, a \neq b\}, \\ M_{JTE} =& \{(a,b,c) \in Q^3 \mid ab \cdot \delta^2 a \neq cb \cdot \delta^2 c, a \neq c\}. \end{aligned}$$

Table 1. 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 $Q(\cdot)$ be an arbitrary quasigroup. In [1] the following statement (Theorem 3) is proved.

Theorem 1 ([1]). *A check character system using a quasigroup $Q(\cdot)$ and coding (2) for $n > 4$ is able to detect all*

I. single errors;

II. transpositions iff for all $a, b, c, d \in Q$ with $b \neq c$ in the quasigroup $Q(\cdot)$ the inequalities (α_1) $b \cdot \delta c \neq c \cdot \delta b$ and (α_2) $ab \cdot \delta c \neq ac \cdot \delta b$ hold;

III. jump transpositions iff $Q(\cdot)$ has properties (β_1) $bc \cdot \delta^2 d \neq dc \cdot \delta^2 b$ and (β_2) $(ab \cdot c) \cdot \delta^2 d \neq (ad \cdot c) \cdot \delta^2 b$ for all $a, b, c, d \in Q, b \neq d$;

IV. twin errors iff $Q(\cdot)$ *has properties* (γ_1) $b \cdot \delta b \neq c \cdot \delta c$ *and* (γ_2) $ab \cdot \delta b \neq ac \cdot \delta c$ *for all* $a, b, c \in Q, b \neq c$;

V jump twin errors iff in $Q(\cdot)$ *the inequalities* (σ_1) $bc \cdot \delta^2 b \neq dc \cdot \delta^2 d$ *and* (σ_2) $(ab \cdot c) \cdot \delta^2 b \neq (ad \cdot c) \cdot \delta^2 d$ *hold for all* $a, b, c, d \in Q, b \neq d$.

Denote the check character system over a quasigroup $Q(\cdot)$ with the check formula (2), $n > 4$ by $S(Q(\cdot), \delta)$. Define for it detection sets

$$M_T^\delta,\ M_{JT}^\delta,\ M_{TE}^\delta,\ M_{JTE}^\delta$$

of transpositions, jump transpositions, twin errors, jump twin errors respectively in the following way

$M_T^\delta = U_1^\delta \cup V_1^\delta$, 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 $U_2^\delta = \{(b, c, d) \in Q^3 \mid bc \cdot \delta^2 d \neq dc \cdot \delta^2 b,\ b \neq d\}, V_2^\delta = \{(a, b, c, d) \in Q^4 \mid (ab \cdot c) \cdot \delta^2 d \neq (ad \cdot c) \cdot \delta^2 b,\ b \neq d\}$;

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

$M_{JTE}^\delta = U_4^\delta \cup V_4^\delta$, where $U_4^\delta = \{(b, c, d) \in Q^3 \mid bc \cdot \delta^2 b \neq dc \cdot \delta^2 d,\ b \neq d\}, V_4^\delta = \{(a, b, c, d) \in Q^4 \mid (ab \cdot c) \cdot \delta^2 b \neq (ad \cdot c) \cdot \delta^2 d,\ b \neq c\}$.

Remark 1. If $Q(\cdot)$ is a quasigroup, then from $(b, c) \in U_1^\delta$, $(b, c, d) \in U_2^\delta$, $(b, c) \in U_3^\delta$, $(b, c, d) \in U_4^\delta$ it can follow respectively that $(a, b, c) \in V_1^\delta$, $(a, b, c, d) \in V_2^\delta$, $(a, b, c) \in V_3^\delta$, $(a, b, c, d) \in V_4^\delta$ for some $a \in Q$ and conversely. For example, if $(b, c) \in U_1^\delta\, (\in U_3^\delta)$ and the elements b, c are such that $f_b = f_c = a$ (where $f_b b = b, f_c c = c$), then $(a, b, c) \in V_1^\delta\, (\in V_3^\delta)$ for this element a and conversely: if $(a, b, c) \in V_1^\delta$ and $a = f_b = f_c$, then $(b, c) \in U_1^\delta$. When $(b, c, d) \in U_2^\delta\, (\in U_4^\delta)$ and $f_b = f_d = a$, then $(a, b, c, d) \in V_2^\delta\, (\in V_4^\delta)$ and conversely.

The set $U_i^\delta, i = 1, 2, 3, 4$, points out the corresponding detected errors in the first digits of code words, while the set $V_i^\delta, i = 1, 2, 3, 4$, defines the detected errors in the rest positions beginning with the second position.

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

Now we note that

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

and

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

so

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

and

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

Taking into account Remark 1 and above mentioned we can estimate percentage (rate) r^δ of detection errors for the system $S(Q(\cdot), \delta)$ over a quasigroup $Q(\cdot)$ in the following Table 2.

Table 2. Detection of errors by systems over quasigroups of order q

Error types	Detection set	Percentage of detection
transpositions	$M_T^\delta = U_1^\delta \cup V_1^\delta$	$r_1^\delta \leqslant \frac{(\lvert U_1^\delta\rvert + \lvert V_1^\delta\rvert)}{q(q^2-1)}$
jump transpositions	$M_{JT}^\delta = U_2^\delta \cup V_2^\delta$	$r_2^\delta \leqslant \frac{(\lvert U_2^\delta\rvert + \lvert V_2^\delta\rvert)}{q^2(q^2-1)}$
twin errors	$M_{TE}^\delta = U_3^\delta \cup V_3^\delta$	$r_3^\delta \leqslant \frac{(\lvert U_3^\delta\rvert + \lvert V_3^\delta\rvert)}{q(q^2-1)}$
jump twin errors	$M_{JTE}^\delta = U_4^\delta \cup V_4^\delta$	$r_4^\delta \leqslant \frac{(\lvert U_4^\delta\rvert + \lvert V_4^\delta\rvert)}{q^2(q^2-1)}$

Let $Q(\cdot)$ be a quasigroup with the left identity e ($ex = x$ for all $x \in Q$) or a loop with the identity e ($ex = xe = x$ for all $x \in Q$).

In this case elements (e, b, c) from V_1^δ (from V_3^δ), (e, b, c, d) from V_2^δ (from V_4^δ) define the elements (b, c) of U_1^δ (of U_3^δ), (b, c, d) of U_2^δ (of U_4^δ) respectively and conversely. So we obtain percentage of detection in Table 3.

Table 3. Detection of errors by systems over quasigroups with a 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, then it is evident that

$$(b, c) \in U_1^\delta \; ((b, c) \in U_3^\delta) \text{ iff } (a, b, c) \in V_1^\delta \; ((a, b, c) \in V_3^\delta)$$

and

$$(b, c, d) \in U_2^\delta \; ((b, c, d) \in U_4^\delta) \text{ iff } (a, b, c, d) \in V_2^\delta \; ((a, b, c, d) \in V_4^\delta),$$

where a is an arbitrary element of Q.

Hence, the sets V_1^δ, V_2^δ, V_3^δ, V_4^δ define completely the sets U_1^δ, U_2^δ, U_3^δ, U_4^δ respectively and we have the rate of error detection in Table 1, since

$$|V_i^\delta| = q|U_i^\delta|, \; i = 1, 2, 3, 4,$$

and

$$r_i^\delta = |V_i^\delta|/q^2(q-1) = |U_i^\delta|/q(q-1), \; i = 1, 3,$$
$$r_i^\delta = |V_i^\delta|/q^3(q-1) = |U_i^\delta|/q^2(q-1), \; i = 2, 4.$$

By analogy with the check character systems over groups (see [6]) we give the following

Definition 1. *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*

$$\delta_2 = \alpha\delta_1\alpha^{-1}.$$

Let $AutQ(\cdot)$ denote the group of automorphisms of a quasigroup $Q(\cdot)$.

The following proposition for quasigroups repeats Proposition 6.6 of [6] for groups.

Proposition 1. (i) *Automorphism equivalence is an equivalence relation (that is reflexive, symmetric and transitive).*

(ii) *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).*

Proof. (i) Straight forward calculation.

(ii) Let $\alpha \in AutQ(\cdot)$, $\delta_2 = \alpha\delta_1\alpha^{-1}$, $(b, c) \in U_1^{\delta_1}$, that is $b\cdot\delta_1 c \neq c\cdot\delta_1 b$, then $\alpha(b \cdot \delta_1 c) \neq \alpha(c \cdot \delta_1 b)$, $\alpha b \cdot \alpha\delta_1 c \neq \alpha c \cdot \alpha\delta_1 b$ or $\alpha b \cdot \alpha\delta_1\alpha^{-1}(\alpha c) \neq \alpha c \cdot \alpha\delta_1\alpha^{-1}(\alpha b)$.

Hence, $(\alpha b, \alpha c) \in U_1^{\delta_2}$.

If $(a, b, c) \in V_1^{\delta_1}$, that is $ab\cdot\delta_1 c \neq ac\cdot\delta_1 b$, then $(\alpha a\cdot\alpha b)\cdot\alpha\delta_1\alpha^{-1}(\alpha c) \neq (\alpha a \cdot \alpha c)\cdot\alpha\delta_1\alpha^{-1}(\alpha b)$. Thus, $(\alpha a, \alpha b, \alpha c) \in V_1^{\delta_2}$.

It is evident that if $(b, c) \in U_1^{\delta_1}$ and $(a, b, c) \in V_1^{\delta_1}$, then $(\alpha b, \alpha c) \in U_1^{\delta_2}$ and $(\alpha a, \alpha b, \alpha c) \in V_1^{\delta_2}$ and conversely, that is

$$|M_T^{\delta_1}| = |M_T^{\delta_2}|.$$

The other cases follow in a similar way. $\square$

Taking into account this proposition we can say that the systems $S(Q(\cdot), \delta_1)$ and $S(Q(\cdot), \delta_2)$ with $\delta_1 \sim \delta_2$ are automorphism equivalent with respect to all considered error types.

3. Equivalence of check character systems over loops

Consider the system $S(Q(\cdot),\delta)$, where $Q(\cdot)$ is a loop with the identity e. The detection sets and a percentage of detection for these systems are given in Table 3.

In [6] the following equivalence between two permutations δ_1 and δ_2 on Q is defined for a group $Q(\cdot)$.

Permutations δ_1 and δ_2 are called weak equivalent if there exist elements $a, b \in Q$ and an automorphism $\alpha \in AutQ(\cdot)$ such that

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

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

We shall generalize the weak equivalence for a loop using the concept of a nucleus of a loop.

Recall that the left, right, middle nuclei of a loop $Q(\cdot)$ are respectively the sets [3]:

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

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

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

All these nuclei are subgroups in the loop [3]. In a group $Q(\cdot)$ the nucleus N coincides with Q.

Definition 2. *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.

It is evident that if $\delta_2 \sim \delta_1$, then $\delta_2 \overset{w}{\sim} \delta_1$ (by $p = q = e$). Note, that if $p \in N, \alpha \in AutQ(\cdot)$, then $\alpha N = N$ and $R_p^{-1}x = R_{p-1}x,\ L_p^{-1}x = L_{p-1}x$ for all $x \in Q$, where p^{-1} is the inverse element for p in the group N (that is $p \cdot p^{-1} = p^{-1} \cdot p = e$). Indeed, $(xp^{-1})p = x \cdot p^{-1}p = xe = x$ for all $x \in Q$, that is

$$R_pR_{p-1}x = x \quad \text{or} \quad R_p^{-1} = R_{p^{-1}};$$

$q(q^{-1}x) = qq^{-1} \cdot x = ex = x$ for all $x \in Q$. Hence, $L_q^{-1} = L_{q^{-1}}$. If a permutation δ_1 of Q is such that $\delta_1 N = N$, then $\delta_2 N = N$ also for every permutation δ_2, which is weakly equivalent to δ_1. Evidently, that it is true if $\delta_1 \in AutQ(\cdot)$.

Proposition 2. *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).*

Proof. a) It is evident that $\delta \overset{w}{\sim} \delta$ by $p = q = e,\ \alpha = \varepsilon$, where ε is the identity permutation of Q.

If $\delta_2 = R_p\alpha\delta_1\alpha^{-1}L_q$, that is $\delta_2 \overset{w}{\sim} \delta_1$, then

$$\delta_1 = \alpha^{-1}R_p^{-1}\delta_2 L_q^{-1}\alpha = \alpha^{-1}R_{p^{-1}}\delta_2 L_{q^{-1}}\alpha = R_{\alpha^{-1}p^{-1}}\alpha^{-1}\delta_2\alpha L_{\alpha^{-1}q^{-1}},$$

where p^{-1} (q^{-1}) is the element inverse to p (q) in the group N, since

$$\alpha R_a x = R_{\alpha a}\alpha x,\ \alpha L_a x = L_{\alpha a}\alpha x$$

for all $a \in Q$ and $\alpha p \in N$ if $p \in N$. Thus, $\delta_1 \overset{w}{\sim} \delta_2$.

Let $\delta_1 \overset{w}{\sim} \delta_2 \overset{w}{\sim} \delta_3$, then $\delta_2 = R_p\alpha\delta_1\alpha^{-1}L_q = R_{p_1}\beta\delta_3\beta^{-1}L_{q_1}$ where $\alpha,\beta \in AutQ(\cdot),\ p,q,p_1,q_1 \in N$.

From these equalities it follows that

$$\delta_1 = \alpha^{-1}R_{p^{-1}}R_{p_1}\beta\delta_3\beta^{-1}L_{q_1}L_{q^{-1}}\alpha = R_{\alpha^{-1}(p_1p^{-1})}\gamma\delta_3\gamma^{-1}L_{\alpha^{-1}(q_1q^{-1})},$$

where $\gamma = \alpha^{-1}\beta \in AutQ(\cdot)$, since $R_aR_bx = (xb)\cdot a = x\cdot ba = R_{ba}x, ba \in N$ and $L_aL_bx = a(bx) = ab\cdot x = L_{ab}x$ if $a,b \in N$. Hence, $\delta_1 \overset{w}{\sim} \delta_3$ and the weak equivalence is an equivalence relation.

b) Let $\delta_1 = R_p\alpha\delta\alpha^{-1}L_q$, $p,q \in N$ and $(a,b,c) \in M_T^{\delta_1} = V_1^{\delta_1}$, that is

$$ab\cdot\delta_1 c \neq ac\cdot\delta_1 b \quad \text{or} \quad ab\cdot R_p\alpha\delta\alpha^{-1}L_q c \neq ac\cdot R_p\alpha\delta\alpha^{-1}L_q b.$$

Then, taking into account that $p \in N$ and $ab = aq^{-1}\cdot qb$ for all $a,b \in Q$ if $q \in N$, we obtain

$$\begin{gathered} ab\cdot(\alpha\delta\alpha^{-1}(qc)\cdot p) \neq ac\cdot(\alpha\delta\alpha^{-1}(qb)\cdot p) \Longleftrightarrow \\ ab\cdot\alpha\delta\alpha^{-1}(qc) \neq ac\cdot\alpha\delta\alpha^{-1}(qb) \Longleftrightarrow \\ (aq^{-1}\cdot qb)\cdot\alpha\delta\alpha^{-1}(qc) \neq (aq^{-1}\cdot qc)\cdot\alpha\delta\alpha^{-1}(qb) \Longleftrightarrow \\ (\alpha^{-1}(aq^{-1})\cdot\alpha^{-1}(qb))\cdot\delta\alpha^{-1}(qc) \neq (\alpha^{-1}(aq^{-1})\cdot\alpha^{-1}(qc))\cdot\delta\alpha^{-1}(qb) \Longleftrightarrow \\ \bar a\bar b\cdot\delta\bar c \neq \bar a\bar c\cdot\delta\bar b,\ \bar b \neq \bar c, \end{gathered}$$

where $\bar a = \alpha^{-1}(aq^{-1}),\ \bar b = \alpha^{-1}(qb),\ \bar c = \alpha^{-1}(qc)$. Thus, $(\bar a,\bar b,\bar c) \in V_1^{\delta} = M_T^{\delta}$.

Now consider twin errors. Let $(a,b,c) \in V_3^{\delta_1} = M_{TE}^{\delta_1}$, then

$$ab \cdot R_p\alpha\delta\alpha^{-1}L_q b \neq ac \cdot R_p\alpha\delta\alpha^{-1}L_q c,$$
$$ab \cdot \alpha\delta\alpha^{-1}(qb) \neq ac \cdot \alpha\delta\alpha^{-1}(qc),$$
$$(aq^{-1} \cdot qb) \cdot \alpha\delta\alpha^{-1}(qb) \neq (aq^{-1} \cdot qc) \cdot \alpha\delta\alpha^{-1}(qc),$$
$$(a^{-1}(aq^{-1}) \cdot \alpha^{-1}(qb)) \cdot \delta\alpha^{-1}(qb) \neq (\alpha^{-1}(aq^{-1}) \cdot \alpha^{-1}(qc)) \cdot \delta\alpha^{-1}(qc),$$

or

$$\bar{a}\bar{b} \cdot \delta\bar{b} \neq \bar{a}\bar{c} \cdot \delta\bar{c},\ \bar{b} \neq \bar{c},$$

where $\bar{a} = \alpha^{-1}(aq^{-1}),\ \bar{b} = \alpha^{-1}(qb),\ \bar{c} = \alpha^{-1}(qc)$. Hence, $(\bar{a},\bar{b},\bar{c}) \in V_3^{\delta} = M_{TE}^{\delta}$. The inverse transformations are also correct.

c) The statement with respect to transpositions and twin errors follows from b).

Consider jump transpositions and jump twin errors if δ is an automorphism of a loop $Q(\cdot)$.

Let $(a,b,c,d) \in M_{JT}^{\delta_1} = V_2^{\delta_1},\ \delta_1 = R_p\alpha\delta\alpha^{-1}L_q$, that is $(ab \cdot c) \cdot \delta_1^2 d \neq (ad \cdot c) \cdot \delta_1^2 b$ or
$(ab \cdot c) \cdot R_p\alpha\delta\alpha^{-1}L_qR_p\alpha\delta\alpha^{-1}L_q d \neq (ad \cdot c) \cdot R_p\alpha\delta\alpha^{-1}L_qR_p\alpha\delta\alpha^{-1}L_q b$.
Then

$$(ab \cdot c) \cdot (\alpha\delta\alpha^{-1}(q \cdot (\alpha\delta\alpha^{-1}(qd) \cdot p)) \cdot p) \neq$$
$$\neq (ad \cdot c) \cdot (\alpha\delta\alpha^{-1}(q \cdot (\alpha\delta\alpha^{-1}(qb) \cdot p)) \cdot p),$$

where $p \in N,\ \alpha\delta\alpha^{-1} \in AutQ(\cdot),\ \alpha\delta\alpha^{-1}p \in N$. So we have

$$(ab \cdot c) \cdot \alpha\delta\alpha^{-1}(q \cdot (\alpha\delta\alpha^{-1}(qd) \cdot p)) \neq (ad \cdot c) \cdot \alpha\delta\alpha^{-1}(q \cdot (\alpha\delta\alpha^{-1}(qb) \cdot p)),$$

$$(ab \cdot c) \cdot (\alpha\delta\alpha^{-1}q \cdot \alpha\delta^2\alpha^{-1}(qd)) \neq (ad \cdot c) \cdot (\alpha\delta\alpha^{-1}q \cdot \alpha\delta^2\alpha^{-1}(qb)).$$

But $ab = aq^{-1} \cdot qb$ and $\alpha\delta\alpha^{-1}q \in N$, so

$$(((aq^{-1} \cdot qb) \cdot c) \cdot \alpha\delta\alpha^{-1}q) \cdot \alpha\delta^2\alpha^{-1}(qd) \neq$$
$$\neq (((aq^{-1} \cdot qd) \cdot c) \cdot \alpha\delta\alpha^{-1}q) \cdot \alpha\delta^2\alpha^{-1}(qb),$$

$$(aq^{-1} \cdot qb)(c \cdot \alpha\delta\alpha^{-1}q) \cdot \alpha\delta^2\alpha^{-1}(qd) \neq$$
$$\neq (aq^{-1} \cdot qd)(c \cdot \alpha\delta\alpha^{-1}q) \cdot \alpha\delta^2\alpha^{-1}(qb),$$

$$((\alpha^{-1}(aq^{-1}) \cdot \alpha^{-1}(qb)) \cdot \bar{c}) \cdot \delta^2\alpha^{-1}(qd) \neq$$
$$\neq ((\alpha^{-1}(aq^{-1}) \cdot \alpha^{-1}(qd)) \cdot \bar{c}) \cdot \delta^2\alpha^{-1}(qb)$$

or

$$(\bar{a}\bar{b} \cdot \bar{c}) \cdot \delta^2 \bar{d} \neq (\bar{a}\bar{d} \cdot \bar{c}) \cdot \delta^2 \bar{b},$$

where

$$\bar{a} = \alpha^{-1}(aq^{-1}),\ \bar{b} = \alpha^{-1}(qb),\ \bar{c} = \alpha^{-1}(c \cdot \alpha\delta\alpha^{-1}q),\ \bar{d} = \alpha^{-1}(qd).$$

Hence, $(\bar{a}, \bar{b}, \bar{c}, \bar{d}) \in V_2^{\delta} = M_{JT}^{\delta}$.

It remains to consider jump twin errors. Let $(a, b, c, d) \in V_4^{\delta_1} = M_{JTE}^{\delta_1}$, that is $(ab \cdot c) \cdot \delta_1^2 b \neq (ad \cdot c) \cdot \delta_1^2 d$. Then

$$(ab \cdot c) \cdot R_p\alpha\delta\alpha^{-1}L_qR_p\alpha\delta\alpha^{-1}L_qb \neq (ad \cdot c) \cdot R_p\alpha\delta\alpha^{-1}L_qR_p\alpha\delta\alpha^{-1}L_qd.$$

In a similar way with jump transpositions we obtain the following inequality

$$(ab \cdot c) \cdot \alpha\delta\alpha^{-1}(q \cdot \alpha\delta\alpha^{-1}(qb)) \neq (ad \cdot c) \cdot \alpha\delta\alpha^{-1}(q \cdot \alpha\delta\alpha^{-1}(qd)).$$

Carrying out the same transformations as in the case of jump transpositions we get

$$(\bar{a}\bar{b} \cdot \bar{c}) \cdot \delta^2 \bar{b} \neq (\bar{a}\bar{d} \cdot \bar{c}) \cdot \delta^2 \bar{d},$$

where

$$\bar{a} = \alpha^{-1}(aq^{-1}),\ \bar{b} = \alpha^{-1}(qb),\ \bar{c} = \alpha^{-1}(c \cdot \alpha\delta\alpha^{-1}q),\ \bar{d} = \alpha^{-1}(qd).$$

Thus, $(a, b, c, d) \in V_4^{\delta_1} = M_{JTE}^{\delta_1}$ and the proof is completed. □

Note that Preposition 2 is a generalization of the analogous Proposition 6.2 of [6] proved for systems over groups.

From Proposition 2 it follows

Corollary 1. *Let $Q(\cdot)$ be a loop (a group), N be its nucleus, $p, q \in N$ ($p, q \in Q$), then*
a) systems $S(Q(\cdot), \varepsilon)$ and $S(Q(\cdot), R_pL_q)$ detect the same percentage of transpositions (jump transpositions, twin errors and jump twin errors);
b) systems $S(Q(\cdot), R_pL_q)$ over a loop (over a group) can not detect all transpositions (all jump transpositions).

Proof. a) Follows from the point c) of Proposition 2 by $\delta_1 = \varepsilon$, $\delta_2 = R_pL_q$.
b) According to Theorem 4 and Proposition 3 of [1] the system $S(Q(\cdot), \varepsilon)$ over a loop can not detect all transpositions (all jump transpositions). Now use a). □

Remind that a loop $Q(\cdot)$ is called a Moufang loop if it satisfies the identity $(xy \cdot z)y = x(y \cdot zy)$.

Corollary 2. *A system $S(Q(\cdot), R_pL_q)$ over a Moufang loop of odd order with nucleus N, $p, q \in N$ detects all twin errors and all jump twin errors.*

Proof. It is sufficiently to note that according to Corollary 4 of [1] the system $S(Q(\cdot), \varepsilon)$ over a Mounfag loop of odd order detects all twin errors and all jump twin errors. □

Example. Now we shall illustrate the results obtained above on a (noncommutative) loop of order 8.

Let $Q(\cdot)$, where $Q = \{1, 2, ..., 8\}$, be a loop of order 8 with the unity 1 which has the Cayley table given in Table 4.

*Table 4.*Cayley table of the loop $Q(\cdot)$

$(\cdot)$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	7	8	5	6
3	3	4	1	2	6	5	8	7
4	4	3	2	1	8	7	6	5
5	5	6	7	8	2	1	4	3
6	6	5	8	7	4	3	2	1
7	7	8	5	6	1	2	3	4
8	8	7	6	5	3	4	1	2

Computer search carried out by A.Diordiev showed that this loop has the group of automorphisms of order 4 which consists of the following permutations:

$$(12345678), (13247856), (12348765), (13246857).$$

We do not write the first row of permutations in the natural order. The nucleus N contains four elements:

$$N = \{1, 2, 3, 4\}.$$

Among permutations δ of Q such that $\delta 1 = 1$ for this loop there exist the set P_1 of 52 permutations satisfying the condition (α_2) (and (α_1), since $Q(\cdot)$ is a loop) of Theorem 1 for all $a, b, c \in Q$, $b \neq c$, and the set P_2 of 16 permutations satisfying the condition (γ_2) (and (γ_1)) for all $a, b, c \in Q$, $b \neq c$ ($P_1 \cup P_2 = \varnothing$). According to Theorem 1 it means that a system $S(Q(\cdot), \delta)$ with $\delta \in P_1$ ($\delta \in P_2$) can detect all transpositions (all twin errors).

There exist 16 permutations which are weakly equivalent to the permutation

$$\delta_0 = (13426785) \in P_1.$$

These permutations have the form $R_p\alpha\delta_0\alpha^{-1}L_q$, where $\alpha \in AutQ(\cdot)$, $p, q \in N$ (here the permutations multiply from the right to the left) and are given below:

$$(13426785), (24315876), (31248567), (42137658),$$
$$(13428567), (24317658), (31246785), (42135876),$$
$$(14237865), (23148756), (32415687), (41326578),$$
$$(14238756), (23147865), (32416578), (41325687).$$

By Proposition 2 each system $S(Q(\cdot), \delta)$, where δ is one of these permutations detects all transpositions also.

For the permutation

$$\delta_1 = (13564278) \in P_2$$

there exist 32 permutations which are weakly equivalent to it. By Proposition 2 all systems $S(Q(\cdot), \delta)$ with δ from these permutations detect all twin errors.

For the systems $S(Q(\cdot), \delta_0)$ and $S(Q(\cdot), \delta_1)$ by computer search the following percentage of detection of transpositions, jump transpositions, twin errors and jump twin errors respectively was obtained:

$$r_1^{\delta_0} = 100, \quad r_2^{\delta_0} = 67, \quad r_3^{\delta_0} = 85, \quad r_4^{\delta_0} = 67$$
$$r_1^{\delta_1} = 78, \quad r_2^{\delta_1} = 87, \quad r_3^{\delta_1} = 100, \quad r_4^{\delta_1} = 87.$$

References

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

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

[3] V.D.Belousov, Foundation of the Theory of Quasigroups and Loops. (Russian), Nauka, Moscow, 1967.

[4] H.M.Damm, Prufziffersysteme uber Quasigruppen, Diplomarbeit Universitat Marburg, Marz, 1998.

[5] A.Ecker and G.Poch, Check character systems, Computing 37/4 (1986), pp. 277-301.

[6] R.-H. Schulz, On check digit systems using anti-symmetric mappings, In J.Althofer et al. editors. Numbers, Information and Complexity, Kluwer Acad. Publ. Boston (2000), pp. 295-310.

[7] R.-H. Schulz, Equivalence of check digit systems over the dicyclic groups of order 8 and 12, In J.Blankenagel & W.Spiegel, editors, Mathematikdidaktik aus Begeisterung fur die Mathematik, Klett Verlag, Stuttgart (2000), pp 227-237.

[8] R.-H. Schulz, Check Character Systems and Anti-symmetric mappings, H.Alt (Ed): Computational Discrete Mathematics, LNCS 2122 (2001), pp 136-147.

[9] J.Verhoeff, Error detecting decimal codes, Math. Center Tracts 29, Amsterdam, 1969.

Contact information

G. B. Belyavskaya Institute of Mathematics and Computer Science, Academy of Sciences of Moldova, str. Academiei, 5, MD-2028, Chishinau, Moldova
E-Mail: gbel@math.md

Received by the editors: 23.04.2003
and final form in 11.07.2003.