BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(46), 2004, Pages 17–24
ISSN 1024–7696

On check character systems over groups

G. Belyavskaya, A. Diordiev

Abstract. In this note we study check character systems (with one control symbol) over groups (over abelian groups) and the check formula $a_1 \cdot \delta a_2 \cdot \delta^2 a_3 \cdot \cdots \cdot \delta^n a_{n+1} = e$, where e is the identity of a group, δ is an automorphism (a permutation) of a group. For a group we consider strongly regular automorphisms (anti-automorphisms), their connection with good automorphisms and establish necessary and sufficient conditions in order that a system to be able to detect all single errors, transpositions, jump transpositions, twin errors and jump twin errors simultaneously.

Mathematics subject classification: 20D45, 94B60.
Keywords and phrases: Group, abelian group, automorphism, complete mapping, orthomorphism, code, check character system.

1 Introduction

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

$$a_1 a_2 \dots a_n \to a_1 a_2 \dots a_n a_{n+1}$$

by some rule.

The aim of using such a system is to discover transmission errors of certain patterns. The examples used in praxis among others are the following:

the Universal Product Code (UPC),

the European Article Number (EAN) Code,

the International Book Number (ISBN) Code,

the system of the serial numbers of German banknotes.

Among the first publications with respect to these systems are articles of W. Friedman and C. J. Mendelsohn [5], based on code-tables, and by R. Schauffler [10] using algebraic structures. In his book [14] J. Verhoeff presented basic results which were in use up to 1970. Later the article of A. Ecker and G. Poch [4] was published where the group-theoretical background of the known methods was explained and new codes were presented that stem from the theory of quasigroups.

Acknowledgment: 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).

Empirical investigations of J. Verhoeff [14] and Beckley [2] show that single errors ($\dots a \cdots \to \dots b \dots$), i.e. errors in only one component of a code word, (adjacent) transpositions ($\dots ab \cdots \to \dots ba \dots$), jump transpositions ($\dots acb \cdots \to \dots bca \dots$), twin errors ($\dots aa \cdots \to \dots bb \dots$) and jump twin errors ($\dots aca \cdots \to \dots bcb \dots$) are the most important errors made by human operators (see Table 8 in [8] of frequency of these error types).

The control digit a_{n+1} in a check character system can be calculated by different check formulas (check equations) in some algebraic structure (a group, a loop, a quasigroup). In the case of a group the most general check formula is the following

$$a_1 \cdot \delta_1 a_2 \cdot \delta_2 a_3 \cdot \dots \cdot \delta_n a_{n+1} = e, \tag{1}$$

where e is the identity of a group G, $\delta_1, \delta_2, \dots, \delta_n$ are some fixed permutations of G. Such a system is called a system over a group and always detects any single error. A survey of the known results concerning check character systems based on quasigroups (loops, groups) one can find in [1].

Often, one chooses a fixed permutation δ of G and puts $\delta_i = \delta^i$ for $i = 1, 2, \dots, n$. Equation (1) then becomes

$$a_1 \cdot \delta a_2 \cdot \delta^2 a_3 \cdot \dots \cdot \delta^n a_{n+1} = e. \tag{2}$$

There are many publications on check character systems over groups with check equation (2), detecting some error types or all of the pointed above error types.

We study check character systems over a finite group which detect all single errors, transpositions, jump transpositions, twin errors and jump twin errors simultaneously using such concepts as a complete mapping, an orthomorphism, a regular automorphism and a new concept of a strongly regular automorphism (anti-automorphism) of a group. For any group we consider the case when δ from (2) is an automorphism ($\delta \in AutG$) and reduce conditions for a good automorphism [3]. For an abelian group δ may be a permutation.

2 Good automorphisms and check character systems over groups

Denote by $S(G, \delta)$ a check character system over a group G with check formula (2), $n > 4$, where δ is a permutation on G.

According to the known results (see, for example, [11], Table 2) a system $S(G, \delta)$ detects all single errors and all

a) transpositions if and only if $x \cdot \delta y \neq y \cdot \delta x$ for all $x, y \in G$, $x \neq y$;

b) jump transpositions if and only if $xy \cdot \delta^2 z \neq zy \cdot \delta^2 x$ for all $x, y, z \in G$, $x \neq z$;

c) twin errors if and only if $x \cdot \delta x \neq y \cdot \delta y$ for all $x, y \in G$, $x \neq y$;

d) jump twin errors if and only if $xy \cdot \delta^2 x \neq zy \cdot \delta^2 z$ for all $x, y, z \in G$, $x \neq z$.

In Table of [3] sufficient (and necessary for $n > 4$) conditions on an automorphism δ of a group G with the identity e for error detection are given. These conditions we give in Table 1.

Table 1. Error detection for automorphism δ

Error types	Conditions on δ (for all $x, y \in G$, $x \neq e$)
single errors	none
transpositions	$\delta x \neq y^{-1}xy$
jump transpositions	$\delta^2 x \neq y^{-1}xy$
twin errors	$\delta x \neq y^{-1}x^{-1}y$
jump twin errors	$\delta^2 x \neq y^{-1}x^{-1}y$

If G is an abelian group, these conditions are, respectively, the following: $\delta x \neq x$, $\delta^2 x \neq x$, $\delta x \neq Ix$, $\delta^2 x \neq Ix$, if $x \neq e$, where $Ix = x^{-1}$: $x \cdot Ix = Ix \cdot x = e$.

A permutation δ satisfying the inequality $x \cdot \delta y \neq y \cdot \delta x$ for all $x, y \in G$, $x \neq y$ is called *anti-symmetric mapping* of a group G.

Groups with anti-symmetric mappings (check character systems over them detect all single errors and all transpositions according to condition a)) were studied in many articles (see, for example, [6–8] and [11–13]).

In [3] check character systems $S(G, \delta)$ over a finite group G with an automorphism δ, which detect all considered above error types simultaneously, were studied and the following concept of a good automorphism was introduced.

Definition 1 [3]. *Let G be a finite group. An automorphism δ of G is called good if δx is not conjugate to x or x^{-1} and $\delta^2 x$ is not conjugate to x or x^{-1} for all $x \in G$, $x \neq e$.*

In [3] it was also shown that there are many groups possessing a good automorphism. In particular, the following results were noted.

If G is abelian, then a good automorphism δ satisfies the conditions for detecting transpositions, jump transpositions and twin errors if δ^2 is regular (that is fixed point free on G, the same $\delta x \neq x$, if $x \neq e$) and δ is good if δ^4 is regular.

For any group G and an automorphism δ of odd order the condition $\delta x \neq y^{-1}xy$ (for all $x, y \in G$, $x \neq e$) implies that δ is good.

The following statement is also useful.

Lemma 1 [3]. *Let G be a p-group and $\delta \in \operatorname{Aut} G$. Suppose $gcd(\mathrm{o}(\delta), p(p-1)) = 1$ ($\mathrm{o}(\delta)$ is the order of δ). Then δ is good if and only if it is fixed point free.*

The conditions of Table 1 (the same the conditions of a good automorphism) are sufficient and necessary for detection of all single errors, transpositions, jump transpositions, twin errors and jump twin errors if $n > 4$ [3].

Thus, we have the following statement.

Proposition 1. *A system $S(G, \delta)$ over a group G where $\delta \in \operatorname{Aut} G$, detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the automorphism δ is good.*

3 Strongly regular automorphisms and check character systems over groups

Now we introduce the following useful concept.

Definition 2. *An automorphism (an anti-automorphism) δ of a group G is called strongly regular if*

$$\delta(xy) \neq yx$$

for all $x, y \in G$, $y \neq Ix$.

It is easy to see that a strongly regular automorphism (anti-automorphism) δ is regular and δ^{-1} is also strongly regular.

In abelian groups the concepts of a regular automorphism and a strongly regular automorphism coincide.

Recall that *a complete mapping* of a group G is a bijective mapping $x \to \theta x$ of G onto G such that the mapping $x \to \eta x$ defined by $\eta x = x \cdot \theta x$ is again a bijective mapping of G onto G.

A permutation α of G is called *an orthomorphism* of a group G, if the mapping $\beta: \ \beta x = x \cdot I\alpha x$ is also a permutation of G [9].

According to [9] an automorphism α is an orthomorphism if and only if the automorphism α is regular.

It is evident that if α is an orthomorphism, then $I\alpha$ is a complete mapping and conversely.

An automorphism is called complete if it is a complete mapping.

Proposition 2. *Let G be a group, $\delta \in \operatorname{Aut} G$. Then the following statements are equivalent:*

(i) $\delta x \neq y^{-1}xy$ *for all* $x, y \in G$, $x \neq e$;

(ii) δ *is strongly regular;*

(iii) δ *is anti-symmetric;*

(iv) δ *satisfies the inequality* $xy \cdot \delta z \neq zy \cdot \delta x$ *for all* $x, y, z \in G$, $x \neq z$.

Proof. (i)$\Leftrightarrow$(ii): let $x \neq e$, then $\delta x \neq y^{-1}xy \overset{x \rightleftarrows yx}{\Longleftrightarrow} \delta(yx) \neq y^{-1}(yx)y = xy$, if $y \neq Ix$.

(ii)$\Leftrightarrow$(iii): let $x \neq z$, then $x \cdot \delta z \neq z \cdot \delta x \Longleftrightarrow Iz \cdot x \neq \delta x \cdot I\delta z = \delta x \cdot \delta Iz \overset{z \rightleftarrows Iz}{\Longleftrightarrow} zx \neq \delta(xz)$, if $x \neq Iz$, since $I\delta = \delta I$.

(iii)$\Leftrightarrow$(iv): let $x \neq z$, then $x \cdot \delta z \neq z \cdot \delta x \overset{x \rightleftarrows xy, \ z \rightleftarrows zy}{\Longleftrightarrow} xy \cdot \delta(zy) \neq zy \cdot \delta(xy) \Longleftrightarrow xy \cdot \delta z \neq zy \cdot \delta x$, if $x \neq z$, since $\delta \in AutG$. □

Proposition 3. *Let G be a finite group, $\delta \in \operatorname{Aut} G$. Then the following statements are equivalent:*

(i) $\delta x \neq y^{-1}x^{-1}y$ *for all* $x, y \in G$, $x \neq e$;

(ii) the anti-automorphism $I\delta$ is strongly regular;

(iii) δ is a complete mapping;

(iv) δ satisfies the inequality $xy \cdot \delta x \neq zy \cdot \delta z$ for all $x, y, z \in G$, $x \neq z$.

Proof. (i)$\Leftrightarrow$(ii): let $x \neq e$, then $\delta x \neq y^{-1}x^{-1}y \overset{x \rightleftarrows yx^{-1}}{\Longleftrightarrow} \delta(yx^{-1}) \neq y^{-1}(xy^{-1})y = y^{-1}x = I(x^{-1}y) \overset{x \rightleftarrows Ix}{\Longleftrightarrow} \delta(yx) \neq I(xy) \Longleftrightarrow I\delta(yx) \neq xy$, if $y \neq Ix$.

(ii)$\Leftrightarrow$(iii): let $x \neq Iy$, $I\delta(yx) \neq xy \Longleftrightarrow \delta(yx) \neq I(xy) \overset{x \rightleftarrows Ix}{\Longleftrightarrow} \delta y \cdot \delta Ix \neq Iy \cdot x \Longleftrightarrow y \cdot \delta y \neq x \cdot \delta x$, if $x \neq y$, since $\delta I = I\delta$. Thus, δ is a complete automorphism, since G is a finite group.

(iii)$\Leftrightarrow$(iv): let $x \neq z$, then $x \cdot \delta x \neq z \cdot \delta z \overset{x \rightleftarrows xy,\ z \rightleftarrows zy}{\Longleftrightarrow} xy \cdot \delta(xy) \neq zy \cdot \delta(zy) \Longleftrightarrow xy \cdot \delta x \neq zy \cdot \delta z$, since $x \neq z$ and $\delta \in AutG$. □

Proposition 4. *An automorphism δ (anti-automorphism $I\delta$) of a finite group G is strongly regular if and only if δ ($I\delta$) is regular on the conjugacy classes of G (that is it does not fix any conjugacy class of $G\backslash\{e\}$).*

Proof. By Proposition 2 an automorphism δ is strongly regular if and only if δ is anti-symmetric. But by Proposition 4.3 of [11] δ is anti-symmetric if and only if it does not fix any conjugacy class $H \neq \{e\}$ of G.

According to Proposition 3 the anti-automorphism $I\delta$ is strongly regular if and only if $\delta x \neq y^{-1}x^{-1}y$ or $I\delta x \neq y^{-1}xy$ if $x \neq e$ for all $x, y \in G$. It means that $I\delta H \neq H$ for any conjugacy class H of G if $H \neq \{e\}$ (that is the anti-automorphism $I\delta$ is regular on the conjugacy classes, since it maps a class in a class). □

Proposition 5. *Let $\delta \in \mathrm{Aut}\, G$ and δ^2 be a strongly regular automorphism of a finite group G. Then the automorphism δ and the anti-automorphism $I\delta$ are also strongly regular.*

Proof. Let an automorphism δ^2 be strongly regular, then by Proposition 4 $\delta^2 H \neq H$ for any conjugacy class of G if $H \neq \{e\}$. From this it follows that $\delta H \neq H$ and $\delta H \neq IH$ (otherwise, $\delta^2 H = \delta(\delta H) = \delta(IH) = I\delta H = I^2 H = H$, contradiction) if $H \neq \{e\}$.

Thus, according to Proposition 4 δ and $I\delta$ are strongly regular. □

Note that this proposition means that from anti-symmetry of δ^2 anti-symmetry and completeness of δ follows (see Proposition 2 and Proposition 3).

Theorem 1. *An automorphism δ of a finite group G is good if and only if the automorphism δ^2 and the anti-automorphism $I\delta^2$ are strongly regular.*

Proof. The conditions of Definition 1 mean that an automorphism δ is good if and only if $\delta x \neq y^{-1}xy$, $\delta x \neq y^{-1}x^{-1}y$, $\delta^2 x \neq y^{-1}xy$ and $\delta^2 x \neq y^{-1}x^{-1}y$ for all $x, y \in G$, $x \neq e$ or $\delta H \neq H$, $\delta H \neq IH$, $\delta^2 H \neq H$ and $\delta^2 H \neq IH$ respectively for any conjugacy class H of G, $H \neq \{e\}$.

Taking into account Proposition 4 for the automorphisms δ and δ^2 (for the anti-automorphisms $I\delta$ and $I\delta^2$) we obtain that an automorphism δ of G is good if and only if $\delta,\ I\delta,\ \delta^2$ and $I\delta^2$ are strongly regular. Now use Proposition 5. $\square$

Thus, the first two from four conditions of Definition 1 of a good automorphism are unnecessary.

From Proposition 1 and Theorem 1 it follows

Corollary 1. *A check character system $S(G,\delta)$ over a finite group G with $\delta \in \operatorname{Aut} G$ detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the automorphism δ^2 and the anti-automorphism $I\delta^2$ are strongly regular.*

By Proposition 2 (Proposition 3) δ^2 ($I\delta^2$) is a strongly regular automorphism (anti-automorphism) if and only if δ^2 is anti-symmetric (δ^2 is complete). So we obtain the following

Corollary 2. *A system $S(G,\delta)$ over a finite group G with $\delta \in \operatorname{Aut} G$ detects all five error types considered above if and only if δ^2 is an anti-symmetric and complete mapping.*

Corollary 3. *A system $S(G,\delta)$ over a finite abelian group with $\delta \in \operatorname{Aut} G$ detects all five error types considered above if and only if δ^2 is an orthomorphism and a complete mapping.*

Indeed, in this case the automorphism δ^2 is anti-symmetric if and only if it is regular (by Proposition 2 for δ^2), that is δ^2 is an orthomorphism.

As it was remarked after Definition 1 an automorphism δ of an abelian group admits to detect single errors, transpositions, jump transpositions and twin errors if δ^2 is fixed point free (that is regular).

Now consider check character systems $S(G,\delta)$ over a finite abelian group G where δ is a permutation on G ($\delta \in S_G$).

Theorem 2. *A check character system $S(G,\delta)$ over a finite abelian group G with $\delta \in S_G$ detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the permutations δ and δ^2 are orthomorphisms and complete mappings (that is all permutations $\delta,\ \delta^2,\ I\delta$ and $I\delta^2$ are complete mappings).*

Proof. In an abelian group G we have from conditions a) – b) in the beginning of section 2:

$$x \cdot \delta y \neq y \cdot \delta x \Longleftrightarrow x \cdot I\delta x \neq y \cdot I\delta y$$

for all $x \neq y$, that is δ is an orthomorphism;

$$xy \cdot \delta^2 z \neq zy \cdot \delta^2 x \Longleftrightarrow x \cdot \delta^2 z \neq z \cdot \delta^2 x \Longleftrightarrow x \cdot I\delta^2 x \neq z \cdot I\delta^2 z$$

for all $x \neq z$, that is δ^2 is an orthomorphism.

Condition c) means that δ is a complete mapping; for codition d) we have

$$xy \cdot \delta^2 x \neq zy\delta^2 z \Longleftrightarrow x \cdot \delta^2 x \neq z \cdot \delta^2 z$$

for all $x \neq z$, that is δ^2 is a complete mapping. □

According to Theorem 2.3 of [11] a finite abelian group G admits a complete mapping if and only if G has odd order or contains more than one involution (that is an element $a \in G$, $a \neq e$ such that $a^2 = e$), so we have from Theorem 2 the following

Corollary 4. *A check character system $S(G, \delta)$ over an abelian group (with one involution) and $\delta \in S_G$ is not able to detect all transpositions (jump transpositions, twin errors or jump twin errors).*

Example. Consider the abelian group $Z_2^3 = Z_2 \times Z_2 \times Z_2$ of order 8. Its Cayley Table is given in Table 2. In this group the permutation I is the identity permutation, so each complete mapping is an orthomorphism and conversely. According to [9] in Z_2^3 there are 48 regular automorphisms (that is orthomorphisms) which enter in eight subgroups of order 7. As computer research has shown one of such subgroups is the following:

$\varepsilon = (0\,1\,2\,3\,4\,5\,6\,7)$, $\delta_0 = (0\,2\,6\,5\,3\,7\,4\,1)$, $\delta_0^2 = (0\,6\,4\,7\,5\,1\,3\,2)$,
$\delta_0^3 = (0\,4\,3\,1\,7\,2\,5\,6)$, $\delta_0^4 = (0\,3\,5\,2\,1\,6\,7\,4)$, $\delta_0^5 = (0\,5\,7\,6\,2\,4\,1\,3)$, $\delta_0^6 = (0\,7\,1\,4\,6\,3\,2\,5)$.

We do not write the first row of permutations in the natural order.

Table 2. $Z_2^3 = Z_2 \times Z_2 \times Z_2$.

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	4	5	2	3	7	6
2	2	4	0	6	1	7	3	5
3	3	5	6	0	7	1	2	4
4	4	2	1	7	0	6	5	3
5	5	3	7	1	6	0	4	2
6	6	7	3	2	5	4	0	1
7	7	6	5	4	3	2	1	0

By Corollary 3 (or Theorem 2) each of six systems $S(Z_2^3, \delta)$, where δ is one of these automorphisms, $\delta \neq \varepsilon$, detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors.

References

[1] Belyavskaya G.B., Izbash V.I., Shcherbacov V.A. *Check character systems over quasigroups and loops.* Quasigroups and related systems, 2003, **10**, p. 1–28.

[2] Beckley D.F. *An optimum system with modulus 11.* The Computer Bulletin, 1967, **11**, p. 213–215.

[3] Broecker C., Schulz P.-H., Stroth G. *Check character systems using Chevalley groups.* Design, Codes and Cryptography, DESI., 1997, **10**, p. 137–143.

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

[5] Friedman W., Mendelsohn C.J. *Notes on Codewords.* Am. Math. Monthly, 1932, p. 394–409.

[6] Gallian J.A., Mullin M.D. *Groups with anti-symmetric mappings.* Arch. Math., 1995, **65**, p. 273–280.

[7] Heiss S. *Antisymmetric mappings for finite solvable groups.* Arch. Math., 1997, **69**, p. 445–454.

[8] Heiss S. *Antisymmetric mappings for finite groups.* Preprint, 1999.

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

[10] Schauffler R. *Über die Bilding von Codewörtern.* Arch. Electr. Übertragung, 1957, N 10(7), p. 303– 314.

[11] Schulz R.-H. *On check digit systems using anti-symmetric mappings.* In J. Althofer et al, editors. Numbers, Information and Complexity, Kluwer Acad. Dubl. Boston, 2000, p. 295–310.

[12] Schulz R.-H. *Equivalence of check digit systems over the dicyclic groups of order 8 and 12.* In J. Blankenagel & W. Spiegel editor, Matematikdidaktik aus Begeisterung für die Mathematik. Klett Verlag, Stuttgart, 2000, p. 227–237.

[13] Schulz R.-H. *Check Character Systems and Anti-symmetric Mappings.* H. Alt. (Ed): Computational Discrete Mathematics, LNCS 2122, 2001, p. 136–147.

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

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str.
Chişinău, MD-2028
Moldova
E-mail: *gbel@math.md*

Received November 11, 2004