On Check Digit Systems using Anti–symmetric Mappings

Ralph–Hardo Schulz (FU Berlin)
Email: schulz@math.fu-berlin.de

Abstract

We consider check digit systems over a group G with check equation $T(a_1)T^2(a_2)\cdots T^n(a_n) = e$ for fixed $e \in G$ and permutation T of G. Such a system detects all single errors (i.e. errors in only one component); and it detects adjacent transpositions (i.e. errors of the form $\ldots ab \ldots \longrightarrow \ldots ba \ldots$) iff T is anti–symmetric that means that T fulfills the condition $x\ \mathrm{T}(y) \neq y\ \mathrm{T}(x)$ for all $x, y \in G$ with $x \neq y$. In this survey we shall report on the existence of groups with anti–symmetric mappings, define equivalence relations between check digit systems and describe, in the special case of the dihedral group D_5, the equivalence classes.

KEYWORDS: check digit system, check character system, error detecting code, anti–symmetric mapping, complete mapping, orthomorphism, dihedral group, Chevalley group.

1 Introduction

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

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

The aim of using such a system is to discover transmission errors. Empirical investigations by VERHOEFF [Ver69], and BECKLEY [Bec67] (see Table 1) show that *single errors*, i.e. errors in only one component, and *adjacent transpositions* (also called *neighbour transposition errors*), i.e. errors of the form $\ldots ab \ldots \longrightarrow \ldots ba \ldots$, are the most important errors made by human operators; (for insertion and deletion errors a detection rate of 100% is achieved by adding leading zeros to make all codewords of equal length).
Note that 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 ([Ver69] p. 14).
Choosing $G = (A, \cdot)$ as a set endowed with a group structure one can determine the check digit a_n by a (check) equation

$$(\Diamond) \qquad \delta_1(a_1)\delta_2(a_2)\ldots\delta_n(a_n) = e$$

Table 1: Error types and their frequencies

Error type			*Relative frequency*	
			Verhoeff	Beckley
single error	$\ldots a \ldots$	$\longrightarrow \ldots a' \ldots$	79.0% (60-95)	86%
adjacent transposition	$\ldots a\, b \ldots$	$\longrightarrow \ldots b\, a \ldots$	10.2 %	8%
jump transposition	$\ldots acb \ldots$	$\longrightarrow \ldots bca \ldots$	0.8%	
twin error	$\ldots aa \ldots$	$\longrightarrow \ldots bb \ldots$	0.6%	6%
phonetic error $(a \geq 2)$	$\ldots a0 \ldots$	$\longrightarrow \ldots 1a \ldots$	0.5%	
jump twin error	$\ldots aca \ldots$	$\longrightarrow \ldots bcb \ldots$	0.3%	
other error			8.6%	

Source: Verhoeff [Ver69](12,112 pairs, 6 digits), Beckley [Bec67].

for fixed permutations δ_i of G, $i = 1, \ldots, n$ and $e \in G$; a usual choice is $e = e_G$ where e_G denotes the neutral element of G. Often, δ_i is chosen such that $\delta_i = T^i$ for a fixed permutation T of G. A check digit system with this check equation detects all *single errors;* and it detects all adjacent transpositions iff $\delta_{i+1}\delta_i^{-1}$ is *anti–symmetric* for $(i = 1, \ldots, n-1)$; here we use the following definition.

1.1 Definition: Anti-symmetric mapping

A bijection T of a group G onto itself is called **anti-symmetric** iff it fulfills the condition

$$(**) \qquad x\ \mathrm{T}(y) \neq y\ \mathrm{T}(x) \quad \text{for all} \quad x, y \in G \ \text{ with } x \neq y.$$

(This is a generalization of a condition of SCHAUFFLER [Schau56]).

In this survey we shall report on the existence of groups with anti–symmetric mappings, define equivalence relations between check digit systems over the same group and describe, in the special case of the dihedral group D_5 of order 10, the equivalence classes with their error detection capacities. Note that we do not discuss check digit systems using general quasigroups and schemes using two or more check digits.

1.2 First examples

Examples of check digit systems are (see for instance [Beu95], [Sch91a], [Sch94]):

- the **European Article Number code (EAN)** and (after adding 0 as first digit) the **Universal Product Code (UPC)** with $G = (\mathbb{Z}_{10}, +)$,

$n = 13, \delta_{2i-1} = \text{id} = \delta_{13}$ and $\delta_{2i}(a) = 3a$ for $e = 0, i = 1, \ldots, 6$; this system does not detect adjacent transpositions $\ldots ab \ldots \longrightarrow \ldots ba \ldots$ for $|a-b| = 5$ (see 2.4(ii));

- the **International Standard Book Number code (ISBN)** with $G = (\mathbb{Z}_{11}, +), n = 10$ and $\delta_i(a) = ia$ for $e = 0, \quad i = 1, \ldots, 10$; this system detects all adjacent transpositions but needs an element $X \notin \{0, \ldots, 9\}$;
- the system of the **serial numbers of German banknotes** which uses an anti–symmetric mapping T_0 (found by VERHOEFF [Ver69], see 4.2) of the dihedral group $G = D_5$ with $e = e_G, \quad \delta_i = T_0{}^i$ for $i = 1, \ldots 10$ and $\delta_{11} = \text{id}$.

1.3 Detection of other errors

¿From now on we consider check digit systems over a group G of order q with codewords of length $n \geq 3$ and check equation

$$(*) \qquad T(a_1)T^2(a_2)\cdots T^n(a_n) = e.$$

The following Table 2, concerning the detection of other important errors, is a variation of VERHOEFF's table [Ver69] by GIESE [Gie99]. The numbers are under the assumption that all error locations and digits are of equal probability. In section 6 we shall use the detection rates of these errors to compare different anti–symmetric mappings of the same group.

Table 2: **Detection of other errors**

Errortype	*Detection set*	*Percentage of detection*
twin errors	$M_{\text{TE}} = \{(x,y) \in G^2 \mid xT(x) \neq yT(y)\}$	$\lvert M_{\text{TE}} \rvert / q(q-1)$
jump transpositions	$M_{\text{JT}} = \{(x,y,z) \in G^3 \mid xyT^2(z) \neq zyT^2(x)\}$	$\lvert M_{\text{JT}} \rvert / q^2(q-1)$
jump twin errors	$M_{\text{JZ}} = \{(x,y,z) \in G^3 \mid xyT^2(x) \neq zyT^2(z)\}$	$\lvert M_{\text{JZ}} \rvert / q^2(q-1)$

2 Orthomorphisms of abelian groups

If G is an abelian group the condition $(**)$ is equivalent to

$$(***) \quad x\ \mathrm{T}(x)^{-1} \neq y\ \mathrm{T}(y)^{-1} \quad \text{for all} \quad x, y \in G \quad \text{with } x \neq y.$$

We remind of the following definition.

2.1 Definition

For a group $(G, \cdot)$, a mapping $f : G \longrightarrow G$ of is denoted as **orthomorphism** (or *perfect difference mapping*) if both f and g with $g(x) := x \cdot f(x)^{-1}$ are permutations. In this case, $\mathrm{inv} \circ f$ with $x \mapsto f(x)^{-1}$ is called a **complete mapping** [Man42]. (Here "inv" denotes the mapping $x \mapsto 1/x$.) Hence h is complete iff h is a permutation with $xh(x) \neq yh(y)$ for all $x, y \in G$ with $x \neq y$. Thus we have

2.2 Proposition

If G is an abelian group and T a permutation of G then the following holds true.

$$\begin{aligned} T \textit{ is anti–symmetric.} &\iff T \textit{ is an orthomorphism.} \\ &\iff \mathrm{inv} \circ T \textit{ is a complete mapping.} \end{aligned}$$

The theory of complete mappings is well developed. So we know e.g. the following.

2.3 Theorem

a) *A finite abelian group G admits a complete mapping iff G has odd order m or contains more than one involution;* (PAIGE [Pai47]). Note that, for m odd, $x \mapsto 2x$ is anti–symmetric.

b) *A necessary condition for a finite group of even order to admit complete mappings is that its Sylow 2-subgroups be non-cyclic. For soluble groups this condition is also sufficient;* (HALL and PAIGE [HP55]).

Surveys on orthomorphism are given in [JDM61] and [Bed95]. The existence of complete mappings has been proved for many classical groups. In 1989, DENES and KEEDWELL [DK89] conjectured that all non-soluble groups admit a complete mapping. Consequences of HALL and PAIGE's theorem are the following. (For a proof see SIEMON [Sie81] and, shortened by using groups with signum, DAMM [Dam98]; here, a homomorphism $\mathrm{sgn}_G : G \longrightarrow \{1, -1\}$ is called signum , see DAMM [Dam98] and ŠIRÁŇ and ŠKOVIERA; such a signum exists iff G contains a subgroup of index 2.)

2.4 Corollary

(i) *A group of order $m = 2u$ with u odd does not admit a complete mapping and thus, in the abelian case, no anti–symmetric mapping.*

(ii) *There does not exist a check digit system over $\mathbb{Z}_{10}$ which detects all adjacent transpositions.* More general: *The cyclic group G admits an anti–symmetric mapping iff $|G|$ is odd;* (see as well 2.5 b).

(iii) *Groups of order $m = 2u$ with u odd, especially D_5 and $\mathbb{Z}_{10}$, don't admit a check digit system which detects all twin errors or all jump twin errors.*

PROOF of (iii). Otherwise, according to Table 2, the mappings T or $L_y \circ T^2$ would be complete; (here $L_y(z) := yz$ denotes the left multiplication with y).□

2.5 Examples

a) inv $= 1/\mathrm{id}$ *is an anti–symmetric mapping of a finite abelian group G iff $|G|$ is odd;* (variation of SIEMON [Sie81] 3.16; see as well 3.2.)

   PROOF. If $|G| = 2k + 1$, then $x = x^{2k+2} = (x^{k+1})^2$; thus $x \mapsto x^2$ is surjective, hence bijective. If $|G|$ is even this mapping is not injective. □

   Remark: A system using this mapping does not detect any twin error.

b) *For a finite cyclic group of order m the mapping $x \mapsto x^k$ is anti–symmetric iff $gcd\ (k, m) = 1 = gcd\ (k - 1, m)$;* (cf. SIEMON l.c. 3.18, [EP86] L. 4.3).

   PROOF. $x \mapsto x^k$ and $x \mapsto x^{k-1}$ have to be bijective; hence g^k and g^{k-1} must have order m if g is a generating element. □

   Remarks. 1.) If m is even then there is no k satisfying these conditions. 2.) If $\gcd(k, m) = 1$ then $x \mapsto x^k$ is an automorphism of G.

c) *If G is abelian and $T \in Aut\,G$ then T is anti–symmetric iff T is fixed point free on G;* (cf. [Sch96] 1.4, see as well subsection 5.3).

3 The general case

We come back to anti–symmetric mappings of not necessary commutative groups. Note that in [Gum85], [Win90], [GM95] and in [Dam98] the condition $(**)$ is replaced by

$$(**') \qquad \phi(x)y \neq \phi(y)x \quad \text{for all} \quad x, y \in G \ \text{ with } x \neq y.$$

The reason is that these authors use the check equation

$$(*') \qquad \phi^{n-1}(x_{n-1})\phi^{n-2}(x_{n-2}) \cdots \phi(x_1)x_0 = e$$

for codewords $x_{n-1}x_{n-2}\ldots x_1x_0$. By putting $T = \phi^{-1}$ and $\bar{x} = \phi(x), \bar{y} = \phi(y)$ one comes back to $(**)$. Having this in mind we have to reformulate results of these authors.

3.1 Examples

1. Examples for dihedral groups are given in sections 4 and 6.

2. *Let G be the group of all $m \times m$* **triangular matrices** *over $K = GF(q)$* **with diagonal 1...1**. *Define T by*

$$T : \begin{pmatrix} 1 & & & \\ & 1 & \mathrm{a}_{ij} & \\ & & \cdot & \\ & & & \cdot \\ 0 & & & 1 \end{pmatrix} \longmapsto \begin{pmatrix} 1 & & & \\ & 1 & \mathrm{f}_{ij}(\mathrm{a}_{ij}) & \\ & & \cdot & \\ & & & \cdot \\ 0 & & & 1 \end{pmatrix}$$

where the f_{ij}'s are orthomorphisms of $(GF(q), +)$. Then T is anti-symmetric; (cf. [Sch96] 1.2b). For instance, f_{ij} can be chosen to be the mapping $\hat{d}_{ij} : K \longrightarrow K$ with $x \mapsto d_{ij}x$ for $d_{ij} \in K \setminus \{0, 1\}$ and $j > i$.

3. *Let $q = 2^m > 2$ and $K = \mathrm{GF}(q)$; put $u_{ac} = 1$ if $a^2 \neq c$ and $u_{ac} = u$ for a fixed $u \in K \setminus \{0, 1\}$ otherwise. Then the mapping*

$$T : \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \longmapsto \begin{pmatrix} a^2 & 0 \\ u_{ac} \cdot b & c^2 \end{pmatrix}$$

is an anti–symmetric mapping of the group

$$G_0 = \{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b \in K \wedge a \cdot c \neq 0\}$$

of all regular 2×2- **triangular matrices** *over* $\mathrm{GF}(q)$; (see [Sch91c] 3.1).

4. *In the same way there can be defined an anti–symmetric mapping of the* **affine group**

$$A(1, q) = \{ \begin{pmatrix} 1 & 0 \\ b & c \end{pmatrix} \mid b, c \in \mathrm{GF}(q) \wedge c \neq 0\}$$

for $q = 2^m > 2$; (see [Sch91c] 3.2).

5. *Let $q = p^m > 2$ and t a prime with $t|(q-1)$ and $t > 2$; choose l from $\{2, 3, \ldots, t-1\}$ and $u_0 \in \mathrm{GF}(q) \setminus \{0, 1\}$; furthermore, put $u_j = ({d_1}^j)^{(l-2)}{d_2}^j$ for $j \in \{1, \ldots, t-1\}$ where d_1, d_2 are fixed elements of $K = GF(q)$ with $d_1 \neq d_2$ and ${d_1}^t = 1 = {d_2}^t$. Then the mapping*

$$T : \begin{pmatrix} {d_1}^j & 0 \\ k & {d_2}^j \end{pmatrix} \longmapsto \begin{pmatrix} {d_1}^{jl} & 0 \\ u_j k & {d_2}^{jl} \end{pmatrix}$$

is an anti–symmetric mapping of the **Îto group**

$$G = \{ \begin{pmatrix} {d_1}^j & 0 \\ k & {d_2}^j \end{pmatrix} | k \in K, j = 0, \ldots, t-1\}.$$

Choosing e.g. $q = 23,\ t = 11,\ l = 2,\ u_0 = 2 \in \mathrm{GF}(23)$ *or* $q = 29,\ t = 7,\ l = 2,\ u_0 = 4 \in \mathrm{GF}(29)$ *one gets a check digit system detecting all single, twin, jump twin errors and adjacent transpositions; the alphabet then contains* 253 *and* 203 *elements respectively;* (see [Sch91c] 3.4 and 3.6).

6. *Taking G as the group H of all $4 \times 4-$matrices over $K = GF(q)$ of the form*

$$[x,y,z] := \begin{pmatrix} 1 & x & y & z \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & -x \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

with $x, y, z \in K$, we get an anti–symmetric mapping by

$$T : [x,y,z] \mapsto [f(x), g_x(y), h_{xy}(z)]$$

if f, g_x, h_{xy} are orthomorphisms of $(K,+)$ for all $x, y \in K$; (see [Sch96] 1.2c).

7. For $m \geq 2$, the group

$$Q_m := < a, b \,|\, a^{2m} = b^4 = e,\ b^2 = a^m,\ ab = ba^{-1} >$$

is called a **dicyclic group** or (for m a power of 2) a **generalized quaternion group**; it is a group of order $4m$. *One gets an anti–symmetric mapping φ in the following way* (cf. [GM95] Th.2.1 ii).

$$\begin{array}{llll} \varphi(a^i) = a^{-i} & (\text{for } 0 \leq i \leq m-1) & \textit{and} \quad \varphi(a^i) = b \cdot a^{i-1} & (\text{for } m \leq i \leq 2m-1) \\ \varphi(ba^i) = ba^{i-1} & (\text{for } 0 \leq i \leq m-1) & \textit{and} \quad \varphi(ba^i) = a^{-i} & (\text{for } m \leq i \leq 2m-1). \end{array}$$

8. For anti–symmetric mappings of the **semi-dihedral groups** of order $8m$ with m even see [GM95] 2.1 (iii), (iv).

3.2 Theorem (GALLIAN and MULLIN)

Let G be a group and $g \in G$. The mapping φ with $\varphi(x) = gx^{-1}$ is anti–symmetric iff g commutes with no element of order 2; (cf. [GM95] Th.3.1).

The proof is technical and shows that g commutes with the involution $y^{-1}x$ if $x\varphi(y) = y\varphi(x)$ for $x \neq y$. □

3.3 Corollary

(i) *All groups of odd order admit anti–symmetric mappings;* ([GM95] 3.2).

(ii) *For $m > 2$, the symmetric group $\boldsymbol{S_m}$ and the alternating group $\boldsymbol{A_m}$ have anti–symmetric mappings;* (cf. [GM95] 3.3).

PROOF. (i) 3.2 . (ii) As the element g of 3.2, choose an $m-$cycle when m is odd and an $(m-1)-$cycle when m is even. $\Box$

Using the classification of finite simple groups and applying Theorem 3.2, GALLIAN and MULLIN state the following.

3.4 Theorem

Every finite simple group except $\mathbb{Z}_2$ has an anti–symmetric mapping; ([GM95]).

An important tool to construct anti–symmetric mappings is the Extension Theorem.

3.5 Extension–Theorem (GALLIAN and MULLIN)

If H is a normal subgroup of G and there exist anti–symmetric mappings φ and ψ of H and G/H respectively then there exists an anti–symmetric mapping of G; (cf. [GM95]).

PROOF(Sketch). Put $\gamma(u_i h) = \varphi(h)\psi^*(u_i)$ where ψ^* is the mapping induced by ψ on a set of representatives $\{u_i\}$ of the cosets of H . $\Box$

Especially, the direct product of groups with anti–symmetric mappings has an anti–symmetric mapping; this was known already to GUMM [Gum85] and, implicitely, to VERHOEFF. So one can extend the results on the existence of anti–symmetric mappings from $p-$ groups, see below, to nilpotent groups.

3.6 Proposition

Every non–trivial finite p–group which is not a cyclic $2-$group has an anti–symmetric mapping; ([GM95] Th. 7.1).

PROOF (Idea). If p is odd one can apply 3.3. If $p = 2$ then there exist two elements of order 2 generating a group of order 4; now one considers a maximal subgroup containing this group and constructs a normal subgroup with non-cyclic factor group for which one gets anti–symmetric mappings by induction. $\Box$

Now it is clear that nilpotent groups with trivial or non–cyclic Sylow 2-subgroup admit anti–symmetric mappings. This leeds GALLIAN and MULLIN ([GM95]) to the following conjecture.

3.7 Conjecture of Gallian and Mullin

All non-abelian groups have anti–symmetric mappings.

This conjecture has been confirmed by HEISS [Hei97] for soluble groups.

3.8 Theorem (HEISS)

Every finite non-abelian solvable group admits an anti–symmetric mapping.

PROOF (Idea): Recursive construction of anti–symmetric mappings starting from a normal subgroup of odd order and a cyclic 2-subgroup of a minimal counter–example. □.

In a lecture given at the DMV-ÖMG meeting 1997, HEISS announced to have proved the full conjecture of Gallian and Mullin.

There exist as well an upper bound for the size of $\mathrm{Ant}(G)$, the set of anti–symmetric mappings of a finite group G (cf. DAMM [Dam98] p.38 Th.9):

3.9 Theorem

If G is a group of order m then the following inequality holds (with e the Eulerian number). $|\mathrm{Ant}(G)| \leq m! - m\lceil (m-1)!(e-1)/e \rceil \leq m!/e + m/2$.
This bound is sharp for $m = 2, 3, 4$ but not e.g. for $m = 10$ (bound $1,334,960$ for $|\mathrm{Ant}(D_5)| = 34,040$, see section 6).

4 Anti–symmetric mappings of dihedral groups

4.1 Representations of dihedral groups

a) The **dihedral group** of order $2m$ is the symmetry group of the regular m–gon. Denoting the rotation through angle $2\pi/m$ by d and one of the reflections by s one gets

$$D_m =< d, s \mid d^m = e = s^2 \ \wedge \ ds = sd^{-1} >$$

The $2m$ elements are of the form $d^i s^j$ for $i = 0, \ldots, m-1$ and $j = 0, 1$.

b) If m is odd then, by defining $d = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ and $s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, the dihedral group D_m can be represented as a matrix group (see e.g. [Gum85]), namely

$$D_m \cong \{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}_m \ \wedge \ a \in \{1, -1\} \}.$$

c) More general, for any $m > 2$, we have

$$D_m \cong \{(f, x) \mid f \in \{1, -1\} \wedge x \in \mathbb{Z}_m\}$$

with operation (cf. [Gum85])

$$(f_1, x) \cdot (f_2, y) = (f_1 f_2, x f_2 + y).$$

d) For any natural number m one can identify the element $d^i s^j \in D_m$ with the integer $j \cdot m + i$ $(j = 0, 1, i = 0, \ldots, m-1)$ (or $(1, -i) \mapsto i$ and $(-1, i) \mapsto m + i$ for the description according to c). Thus one gets a representation of D_m on $\{0, \ldots, 2m-1\}$ with induced operation $*$. In case $m = 5$ this operation has the following composition table (see e.g. [Ver69], [EP86], [Gum85], [Sch91a], [Sch94], [Win90]); here k MOD m denotes the remainder of k under division by m.

$i * j$	$0 \leq j \leq 4$	$5 \leq j \leq 9$
$0 \leq i \leq 4$	$(i+j)$MOD 5	$5 + (i+j)$MOD 5
$5 \leq i \leq 9$	$5 + (i-j)$MOD 5	$(i-j)$MOD 5

or, full-length, as in Table 3.

Table 3: From D_5 induced operation on $\{0, 1, \ldots, 8, 9\}$

$*$	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

4.2 Verhoeff's anti-symmetric mappings of dihedral groups

(i) For the system of serial numbers of German banknotes, the anti–symmetric mapping used is the one found by VERHOEFF [Ver69] p.95:

$$T_0 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix} = (01589427)(36)$$

.

REMARK: Note that in the scheme used for the serial numbers of German banknotes there is used the check equation $(\diamond)$ (see the introduction) with $\delta_i = {T_0}^i$ for $i = 1, \ldots, 10$ and $\delta_{11} = \mathrm{id}$; (cf. e.g. [Sch91a]).

Furthermore, the alpha–numeric alphabet is encoded as in Table 4.

(ii) Further anti-symmetric permutations found by computer search are, among others, (07319854)(26) and (03986215)(47) ([Ver69] p.95).

Table 4: Encoding the letters of the serial numbers of German banknotes

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

(iii) For D_m with m odd and $r \neq 0 \text{ MOD } m$, the following mapping is anti–symmetric (cf. [Ver69] p.91.)

$$T(d^k) = d^{-k} \quad \text{and} \quad T(d^j s) = d^{j+r} s\,;$$

for $m = 5$ this yields the permutations $\rho = (14)(23)(56789)$, which is mentioned again in [Win90], and $(14)(23)(58697)$, see as well [Gum85].

4.3 Other anti–symmetric mappings of $\mathbf{D}_m$

In the following we mention several other anti–symmetric mappings of D_m. That they have this property is proved by direct and exhaustive calculation.

a) *For m odd the mapping*

$$T\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} := \begin{pmatrix} a & 0 \\ h_a(b) & 1 \end{pmatrix}$$

is anti–symmetric if h_a is injective and fulfills

$$bk - la \neq h_a(b) - h_k(l) \text{ for } (a, b) \neq (k, l);$$

(see [Sch91b] 3.7). It is sufficient to put $h_a(b) = u_a - ab$ with $u_1 \neq u_{-1}$.

Choosing $u_a = -at - c$ with $c, t \in \mathbb{Z}_m$ and $t \neq 0$ one gets the system of GUMM ([Gum85] p.103), namely

$$T(d^k) = d^{c+t-k} \quad \text{and} \quad T(d^j s) = d^{t-c+j} s,$$

especially for $t = r/2 = -c$ the system 4.2 (iii); and putting $u_{-1} = 0$ and $u_1 = 1 - m$ (or $c = t = (m-1)/2$ in GUMM l.c.) one has the systems of BLACK ([Bla72]) for $m = 5$ and ECKER and POCH ([EP86] Th.4.4)

$$T(d^k) = d^{m-k-1} \quad \text{and} \quad T(d^j s) = d^j s.$$

For $m = 5$, this mapping can be expressed as (04)(13).

Choosing $u_1 = 0$ and $u_{-1} = -1$ (or $c = 1/2 = -t$ in Gumm l.c.) yields the scheme of WINTERS (again for m odd):

$$T = (0)(1\ m{-}1)(2\ m{-}2)\ldots(\frac{m-1}{2}\ \frac{m+1}{2})(2m{-}1\ \ 2m{-}2\ldots m{+}1\ \ m) \text{ or}$$

$$T(d^k) = d^{-k} \text{ and } T(d^j s) = d^{j-1}s;$$

this is the system of VERHOEFF for $r = -1$. For $m = 5$ one gets the mapping ρ of 4.2(iii). If one puts $c = t = 1$ in GUMM's system, one gets the scheme of GALLIAN and MULLIN ([GM95]Th.2.1 (i)) for m odd:

$$T(d^k) = d^{2-k} \text{ and } T(d^j s) = d^j s.$$

b) Note that, for m odd, the mapping

$$D_m \to D_m \text{ with } x \mapsto ax^{-1}b$$

is anti–symmetric if $a \in \{d, \ldots, d^{m-1}\}$; (see 3.2 and 6.2 b). Choosing $a = d^t$ and $b = d^c$ yields the system of GUMM, see part (a).

c) GALLIAN and MULLIN observed that for $m = 2k$ and $G = D_m$ the following mapping is anti–symmetric; ([GM95] l.c.; see as well [Dam98]p.22).

$$\begin{array}{lll} T(s) & = e & T(d^{-1}s) = ds \\ T(d^j) & = d^{1-j} & (k+1 \le j \le m) \\ T(d^j) & = d^{1-j}s & (1 \le j \le k) \\ T(d^j s) & = d^{j+1}s & (1 \le j \le k-1) \\ T(d^j s) & = d^{j+1} & (k \le j \le m-2) \end{array}$$

What can be said about the detection of other errors with D_m ? An important answer gives the following theorem of DAMM (cf.[Dam98] p.55).

4.4 Theorem

For $m \geq 3$ odd there does not exist a check digit system over D_m which detects

(i) all jump transpositions (DAMM) *or*

(ii) all twin errors or all jump twin errors (HALL/PAIGE).

PROOF (Sketch). In order to prove that D_m does not admit a jump transposition detecting mapping T one shows that the mappings $L_y \circ T^2$ can not be anti–symmetric (see Table 2) for all $y \in D_m$: Using the terminology of 4.1c we define $T^2(f, x) = (g_1(f, x), g_2(f, x))$. There exists an element $(-1, x) \in D_m$ such that the component function g_1 of T^2 fulfills $-g_1(1, 0) = g_1(-1, x)$ (– otherwise there would be $m+1$ elements with the same signum, in contradiction to the fact that the positive elements of D_m form a subgroup of index 2). Then $L_c \circ T^2$ with $c = (1, \frac{1}{2}g_1(1, 0)(g_2(-1, x) - xg_1(1, 0) - g_2(1, 0)))$ is not anti–symmetric (in the sence of $(**)$) as a straight-forward calculation shows. For twin errors and jump twin errors the statement is part of 2.4 (iii). □

Therefore we are going to search for other groups with better detection rates. In connection with dihedral groups, there are still to mention the following results involving group–(anti–)automorphisms (– for definitions see 5.1).

4.5 Theorem (DAMM)

(i) *D_m allows no anti–symmetric automorphism for $m > 2$.*

(ii) *D_m admits an anti–symmetric anti–automorphism iff m is odd.*

PROOF (see DAMM [Dam98]p.57 Th.28). One can show that an automorphism of D_m has a fixed conjugacy class and hence can't be anti–symmetric, see 5.3 below and [Sch96] 1.5. If m is even then (1, m/2) is a fixed point of any (signum and order preserving) anti–automorphism. If m is odd then

$$\psi : x \mapsto (1,-1)x^{-1}(1,1)$$

is a fixed point free anti–automorphism. Now, the assertion follows from 5.2(b). $\square$

5 Anti-symmetric automorphisms and anti-automorphisms

In this part we shall use automorphisms and anti-automorphisms to construct anti-symmetric mappings. We start with anti-automorphisms which will be needed as well in 6.12. As seen in 2.5 and 3.2, the mapping inv: $x \longmapsto x^{-1}$ is, under certain conditions, an anti-symmetric mapping. On the other hand inv is, for every group, an anti-automorphism.

5.1 Definition

A bijection $\psi : G \longrightarrow G$ of a group G is called **anti-automorphism** if

$$\psi(xy) = \psi(y) \cdot \psi(x) \quad \text{for all} \quad x, y \in G.$$

The set of all anti-automorphisms of G is denoted by Antaut G. Note that Antaut G = Aut G $\circ$ inv. In [Dam98], DAMM uses anti-automorphisms to construct anti-symmetric mappings. He states:

5.2 Theorem (DAMM)

(a) *If φ is anti-symmetric and ψ an anti-automorphism then $\psi \circ \varphi^{-1} \circ \psi^{-1}$ is anti-symmetric;* ([Dam98] S.6 p.34).

(b) *For an anti–automorphism ψ holds:*
ψ is anti-symmetric $\iff$ ψ is fixed point free
$\iff$ $\varphi^{-1} \circ \psi \circ \varphi$ is fixed point free for any (anti-) automorphism φ.

An overview on conditions for error detection using anti–automorphisms is given in Table 5. The proofs are straight forward calculations.
We continue with group–automorphisms.

Table 5: Error detection for anti–automorphisms ψ

	Error type	Conditions on ψ (for all $x, y \in G$, $x \neq e$)
1.	single error	none
2.a)	adjacent transposition	$\psi(x) \neq x$
2.b)	jump transposition	$\psi^2(x) \neq y^{-1}xy$
3.a)	twin error	$\psi(x) \neq x^{-1}$
3.b)	jump twin error	$\psi^2(x) \neq y^{-1}x^{-1}y$
4.	phonetic error ($0 \hat{=} e, 1 \hat{=} g$)	$g^{-1}a \neq \psi(a) \neq ag^{-1}$ (for $a \hat{=} 2, \ldots, 9$)

Source: [Dam98] p.36

Table 6: Error detection for automorphisms T

	Error type	Conditions on T (for all $x, y \in G$, $x \neq e$)
1.	single error	none
2.a)	adjacent transposition	$T(x) \neq y^{-1}xy$
2.b)	jump transposition	$T^2(x) \neq y^{-1}xy$
3.a)	twin error	$T(x) \neq y^{-1}x^{-1}y$
3.b)	jump twin error	$T^2(x) \neq y^{-1}x^{-1}y$
4.	phonetic error ($0 \hat{=} e, 1 \hat{=} g$)	$T(a) \neq g^{-1}a$ (for $a \hat{=} 2, \ldots 9$)

Source: [BSS97], [Dam98]

5.3 Proposition

Let G be a finite group and $T \in \mathrm{Aut}\, G$. Then T is anti-symmetric iff T does not fix any conjugacy class of $G \setminus \{e\}$ (where e denotes the neutral element of G). When G is abelian, then this is the case iff T operates fixed point freely on G; (see [Sch96] 3.1 and 2.5 c).

PROOF. T is anti-symmetric iff $T(x)T(y)^{-1} = T(xy^{-1}) \neq x^{-1}(xy^{-1})x$ for all $x, y \in G$ with $x \neq y$. □

Sufficient (and for $n > 4$ also necessary) conditions on the automorphism T for the detection of errors are stated in Table 6 (cf. [BSS97]).

PROOF. Condition 2.a) follows from 5.3. Consider now type 3.a). The error is detected iff $T^i(a)T^{i+1}(a) \neq T^i(b)T^{i+1}(b)$ which is equivalent to $T(ba^{-1}) \neq b^{-1}(ba^{-1})^{-1}b$. The other conditions follow in a similar way. □

5.4 Definition

Let G be a finite group. An automorphism T of G is called **good** provided

$T(x)$ is not conjugate to x or x^{-1} and

$T^2(x)$ is not conjugate to x or x^{-1}

for all $x \in G, x \neq e$ (cf.[BSS97]).

5.5 Remarks

(i) *A good automorphism is anti-symmetric and detects single errors, adjacent transpositions, jump transpositions, twin errors and jump twin errors;* (see 5.3).

(ii) *If G is abelian then the automorphism T admits to detect single errors, adjacent transpositions, jump transpositions and twin errors if T^2 is fixed point free; and T is good if T^4 is fixed point free.*

(iii) Note that for any group G and automorphism T of odd order t already condition 2a) implies that T is good.

PROOF. Since $\gcd(4,t) = 1$ there are integers r, s with $4r + st = 1$; any conjugacy class fixed by T^4 must be fixed by $T = T^{4r+st}$ too. □

5.6 An example

Choose $q = 2^m > 2$ and G as the **Sylow 2–subgroup of the unitary group** $\mathrm{SU}(3,q^2)$ of order q^3, formed by the matrices

$$Q(x,y) = \begin{pmatrix} 1 & x & y \\ 0 & 1 & x^q \\ 0 & 0 & 1 \end{pmatrix} \quad \text{with } x, y \in GF(q^2) \text{ and } \; y + y^q + x^{q+1} = 0 \; .$$

The automorphism $T : Q(x,y) \longmapsto Q(x\lambda^{2q-1}, y\lambda^{q+1})$, induced by conjugation with

$$H_\lambda = \begin{pmatrix} \lambda^{-q} & 0 & 0 \\ 0 & \lambda^{q-1} & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

for $\lambda \in \mathrm{GF}(q^2) \setminus \{0\}$ is good iff the multiplicative order of λ is not a divisor of $q+1$ (BROECKER following a hint of G. STROTH). *The check character system using the automorphism T of order $q-1$ detects all single errors, adjacent-transpositions, twin errors, jump transpositions and jump-twin errors.* Generalization:

5.7 Good automorphisms on $p-$ groups

Let P be a p-group and $T \in \mathrm{Aut}\ P$. Suppose $\gcd\big(o(T), p(p-1)\big) = 1$. *Then T is good iff T is fixed point free on P;* (cf.[BSS97]).

PROOF (Sketch). Take $P_1 := \Omega_1\big(Z(P)\big)$ and define P_i inductively such that

$$P_i/P_{i-1} = \Omega_1\big(Z(P/P_{i-1})\big).$$

(Here $\Omega_1(G)$ denotes the subgroup of G generated by the elements of order p.) One gets a T-invariant chain $P_0 = \{e\} < P_1 < \ldots < P_n = P$. If T is fixed point free on P then it acts fixed point freely on each P_i/P_{i-1}. Choose $x \in P$ such that $T(x)$ is conjugate to x and let i be minimal with $x \in P_i$. Suppose $i > 0$ then one can show $T(< xP_{i-1} >) =< xP_{i-1} >$. As Aut $(< xP_{i-1} >)$ is cyclic of order $p-1$ this shows $T(xP_{i-1}) = xP_{i-1}$, a contradiction. So $i = 0$ and $x = e$. Hence T is good by 5.5 (iii). □

5.8 Corollary

Let S be the **Sylow 2–subgroup of PSL $(2, q)$** , $q = 2^m, m > 1$ *defined by*

$$S = \{\begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \mid v \in GF(q)\}; \quad \text{then} \quad T = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

with $t \in \mathrm{GF}(q) \setminus \{0, 1\}$ *acts fixed point freely on S. Therefore S admits a good automorphism hence a check digit system which detects all single errors, neigbour-transpositions, twin errors, jump transpositions and jump-twin errors;* (cf.[BSS97]).

Similarly, the **Sylow 2–subgroups of the Suzuki group Sz(q)**(for $q = 2^{2t+1}, q > 2$) admit a good automorphism. More general

5.9 Theorem

The **Sylow 2–subgroup of a Chevalley group** *over* $\mathrm{GF}(q), q = 2^m$, *admits a good automorphism T with $o(T) \mid (q-1)$ provided q is large enough;* (cf.[BSS97] Result 2).

6 Equivalence of check digit systems

Although the systems over Chevalley groups admit to detect all single errors, adjacent transpositions, twin errors, jump transpositions and jump-twin errors we concentrate now on the dihedral group of order 10 since their elements can be interpreted as $0, 1, \ldots, 9$ and used in the decimal system.
Because there are (exactly) 34,040 anti–symmetric mappings over D_5 (VERHOEFF [Ver69] p.92, DAMM [Dam98] p.44 with sieve methods , GIESE [Gie99]) we

want to define equivalences between these schemes. But there are several possibilities to do so. In the whole section, let G be a group and T_1, T_2 permutations of G.

A) Weak equivalence

6.1 Definition

T_1 and T_2 are called **weak equivalent** if there exist elements $a, b \in G$ and an automorphism $\alpha \in \mathrm{Aut}\ G$ such that

$$T_2 = R_a \circ \alpha^{-1} \circ T_1 \circ \alpha \circ L_b\,.$$

Here $R_a(x) := x \cdot a$ and, as before, $L_b(y) := by$; (cf. [Ver69], [Dam98] p.38, [Sch]).

6.2 Proposition

a) *Weak equivalence is an equivalence relation (i. e. reflexive, symmetric and transitive).*

b) *If T_1 and T_2 are weak equivalent and if T_1 is anti–symmetric, then T_2 is anti-symmetric;* ([Dam98] p.30, [Ver69]).

c) *If T_1 and T_2 are weak equivalent permutations of G then they detect the same percentage of twin errors;* ([Sch]).

d) *If T_1 is an* **automorphism** *of G and T_2 is weak equivalent to T_1 then T_1 and T_2 detect the same percentage of jump transpositions and the same percentage of jump twin errors;* ([Sch]).

PROOF. a) Straight forward calculation (cf.[Dam98] p.31). b) $xT_2(y) = yT_2(x)$ implies

$$\begin{array}{lll} xR_a \circ \alpha^{-1} \circ T_1 \circ \alpha \circ L_b(y) & = yR_a \circ \alpha^{-1} \circ T_1 \circ \alpha \circ L_b(x), & \text{therefore} \\ \alpha(b)\alpha(x)\alpha R_a \alpha^{-1} T_1 \alpha L_b(y) & = \alpha(b)\alpha(y)\alpha R_a \alpha^{-1} T_1 \alpha L_b(x), & \text{hence} \\ \alpha(bx) T_1\big(\alpha(by)\big) & = \alpha(by) T_1\big(\alpha(bx)\big) & \text{showing} \\ \alpha(bx) & = \alpha(by) \quad \text{and so} \quad x = y. & \end{array}$$

c) We have
$$\begin{array}{llll} xT_2(x) \neq yT_2(y) & \iff & x\alpha^{-1}T_1\alpha(bx)a & \neq y\alpha^{-1}T_1\alpha(by)a \\ & \iff & \overline{x}\,T_1(\overline{x}) & \neq \overline{y}\,T_1(\overline{y}) \end{array}$$
for $\overline{x} = \alpha(bx)$ and $\overline{y} = \alpha(by)$; therefore the detection sets $M_{\mathrm{TE}}(T_1)$ and $M_{\mathrm{TE}}(T_2)$ (see Table 2) have the same cardinality.

d) We get $xyT_2{}^2(z) \neq zyT_2{}^2(x) \iff \overline{x}\,\overline{y}\,T_1{}^2(\overline{z}) \neq \overline{z}\,\overline{y}\,T_1{}^2(\overline{x})$ for $\overline{x} = \alpha(bx), \overline{z} = \alpha(bz)$ and $\overline{y} = \alpha(y)T_1(\alpha(b))$; hence $|M_{\mathrm{JT}}(T_1)| = |M_{\mathrm{JT}}(T_2)|$ (see Table 2). A similar argument holds for jump twin errors. □

6.3 Weak equivalence and detection rates

The assertion of 6.2 d) might be wrong if T_1 and T_2 are not automorphisms; see the following counterexample (cf. [Gie99], [Sch]). Let T_0 be VERHOEFF's anti–symmetric mapping (see 4.2) $T_0 = (01589427)(36)$. It detects 94.22 % of jump transpositions and 94.22 % of jump twin errors. Consider the weak equivalent permutation $T_1 := R_4 \circ \mathrm{id} \circ T_0 \circ \mathrm{id} \circ L_3$, namely $T_1 = (079482)(36)$. This mapping detects only 87.56 % of all jump transpositions and jump twin errors respectively.

6.4 Weak equivalence in the case of $\mathbf{D}_5$

According to GIESE [Gie99], see as well DAMM [Dam98] p.32, there exist exactly 20 equivalence classes with respect to weak equivalence; one of it contains 40 elements (with (01)(24) as representative); and 4 further classes have 1,000 elements each; the other 15 classes all are of cardinality 2,000.

Since weak equivalence might not respect all error detecting capabilities, see 6.3, we restrict ourselves to stronger relations.

B) Automorphism-equivalence

6.5 Definition

T_1 and T_2 are called **automorphism equivalent** if there exists an $\alpha \in \mathrm{Aut}\ G$ such that $T_2 = \alpha^{-1} \circ T_1 \circ \alpha$; ([Sch]).

6.6 Proposition

(i) *Automorphism-equivalence is an equivalence relation; and if T_1 and T_2 are automorphism equivalent then T_1 and T_2 are weak equivalent.*

(ii) *If T_1 and T_2 are automorphism equivalent, then T_1 and T_2 detect the same percentage of adjacent transpositions, jump transpositions, twin errors and jump twin errors;* ([Sch], [Gie99]).

PROOF of (ii). The detection sets $M_{AT} = \{(x, y) \in G^2 \mid xT(y) \neq yT(x)\}$, M_{JT} and M_{JZ} of $T = T_1$ can be mapped bijectively on the corresponding sets of $T_2 = \alpha^{-1} \circ T_1 \circ \alpha$; for instance

$$\begin{aligned}
(x, y) \in M_{AT}(T_2) &\iff xT_2(y) \neq yT_2(x) \\
&\iff \alpha(x)\alpha\alpha^{-1}T_1\big(\alpha(y)\big) \neq \alpha(y)\alpha\alpha^{-1}T_1\big(\alpha(x)\big) \\
&\iff \big(\alpha(x), \alpha(y)\big) \in M_{AT}(T_1)
\end{aligned}$$

For twin errors, (ii) follows from (i) and 6.2 c). □

6.7 Types of equivalence classes over $\mathbf{D}_5$

According to computations by GIESE with the program package MAGMA there are 1,706 equivalence classes of anti-symmetric mappings with respect to automorphism-equivalence [Gie99]. Giese distinguishes 6 types of classes according to the rate of detection of errors, see Table 7.

Table 7: Types of anti–symmetric mappings of D_5 and their detection rates in %

	Type I	II a	II b	III	IV	V	VI
single errors	100%	100%	100%	100%	100%	100%	100%
adjacent transpos.	100%	100%	100%	100%	100%	100%	100%
twin errors	95.56	95.56	91.11	91.11	91.11	not of type VI	55.56
jump transpositions	94.22	92.00	94.22	92.00	90.22	and at least one	66,67
jump twin errors	94.22	92.00	94.22	92.00	90.22	rate below 90 %	66.67
Detection rate of all 5 error types weighted with their relative frequencies (without phonetic errors)	99.90	99.87	99.87	99.84	99.82	99.85–99.42	99.30

Source: [Gie99].

In type V and VI, there are contained all classes which have at least one detection rate below 90%. Class VI is distinguisted since it contains many of the systems already known before. Note that there exist classes of type V with a detection rate of 95.56 % for twin errors and of 89.78% for jump transpositions and of jump twin errors, thus giving an over all detection rate of 99.85 %. (The detection rates of systems of type I are in accordance with [Ver69]p.95, those of type VI with [Win90]p.304). To give another point of view, the unweighted error detection rates for some codeword lengths are calculated in Table 8.

6.8 Remarks on Tables 7 and 8

(i) The phonetic error detecting capability may alter between automorphism equivalent systems (see 6.11). Therefore, this error type is not considered in Table 7.

(ii) The relative frequency of errors used for the last row of Table 7 is based on the occurence among the non-coincidental errors without phonetic errors according to VERHOEFF's list (Table 1). So single errors are weighted with 86.909 %, adjacent transpositions with 11.221%, twin errors with 0.66%, jump transpositions with 0.88% and jump twin errors with 0.33% (of errors of these five types).

(iii) As basis for Table 8, we use the maximal number of possible errors of the considered type in a codeword of length n; (e.g. all adjacent entries are assumed to be different when considering adjacent transpositions.) The rates are gained from the following numbers of detected errors of the considered error types (with $x_{\mathrm{S}}, x_{\mathrm{AT}}, x_{\mathrm{TE}}, x_{\mathrm{JT}}$, and x_{JZ} the detection rates of single errors, adjacent transpositions, twin errors, jump transpositions, jump twin errors respectively), cf. [Gie99].

$$x_{\mathrm{S}}(q-1)n+x_{\mathrm{AT}}(n-1)+x_{\mathrm{TE}}(q-1)(n-1)+x_{JT}(n-2)+x_{\mathrm{JZ}}(q-1)(n-2)$$

as percentage of the maximal number of possible errors

$$(q-1)n+(n-1)+(q-1)(n-1)+(n-2)+(q-1)(n-2).$$

Table 8: Unweighted error detection rates (in %) for codewords of length n over D_5

	Type I	II a	II b	III	IV	V	VI
n=6	97.01	96.39	95.62	95.00	94.51	95.77–82.41	76.85
n=10	96.84	96.15	95.45	94.77	94.22	95.47–81.44	75.90
n=11	96.82	96.12	95.43	94.74	94.19	95.43–81.31	75.78

Source: [Gie99].

6.9 Description of equivalence classes over $\mathbf{D}_5$

An overview on the number of classes and their sizes is given in Table 9. Type I contains 2 equivalence classes with 20 elements each; a representative of one class is the anti-symmetric mapping (0 7 3 1 9 8 5 4) (2 6) found by VERHOEFF; the second class contains the mapping T_0 of 4.2 (i) used for the German banknotes and (0 3 9 8 6 2 1 5) (4 7). The equivalence class of type VIa is represented by (0849) (1735) (26) ; the 5 classes of type VIb with 4 elements each contain all systems of the equivalent schemes of GUMM [Gum85] and SCHULZ [Sch91b]. One of these classes has (04) (13) as a representative, the mapping found by BLACK [Bla72], see as well ECKER & POCH [EP86], one other consists of 4 mappings given by VERHOEFF, namely (14)(23)(56789), (14)(23)(58697) and their inverses, see 4.2 (iii).

Table 9: Number of automorphism–equivalence classes

	Type I	II a	II b	III	IV	V	VI a	VI b
Number of equivalence classes	2	44	8	160	16	1470	1	5
Size of classes	20	20	20	20	20	20	20	4

Source: [Gie99].

6.10 Phonetic errors

The calculation of phonetic error detection rates is problematic in several ways.

(i) The distibution of these errors depends on their position in the codeword. In VERHOEFF's statistics [Ver69], this distribution is $15, 0, 9, 1$ and 34 for positions $(j, j+1)$ with $j = 1, \ldots, 5$ respectively. Verhoeff explains this by the habit of quoting the words in pairs of decimals. When partitioning a word in blocks of size 3 the position is likewise important (e.g. 15,000 is taken for **50**,000 more easily than for 1**1**,**5**00 , cf. DAMM). But at other places, the error probability may be different from that which one gets by partitioning in blocks of size 2 completely. Therefore we consider unweighted detection rates mainly.

(ii) In VERHOEFF's random sample, the distribution of the errors $1x \longrightarrow x0$ and $x0 \longrightarrow 1x$ over x is that of Table 10.

This shows how strongly these errors depend on the language and the phonetic resemblance of pairs in it; for Dutch, the low frequency of 8 is typical. So there should be made an extra statistics for each language.

Table 10: Distribution of phonetic errors $1x \longrightarrow x0$ and $x0 \longrightarrow 1x$

x	2	3	4	5	6	7	8	9
%	5.1	20.3	16.9	15.3	6.8	11.9	1.7	22.0

Sources: [Ver69], [Sch].

6.11 Detection of phonetic errors

As mentioned before, the detection rate of phonetic errors may vary in an automorphism equivalent class. Taking the class of T_0 and word length $n = 10$ as example, the number of recognizable phonetic errors out of 72 possible errors is 69 (for T_0 and 4 other mappings) 61, 60 and 57 (as well for 5 mappings each) respectively.
Furthermore, for a permutation T which is anti–symmetric in the sense of $(**)$, the detection rate of phonetic errors using check equation $(*)$ may be different from that of T^{-1} when using check equation $(*')$. While the inverse mappings $\phi = T^{-1}$ of the examples T of Type I, III and VI of Table 11 have the same detection rates (for $n \leq 10$) as the corresponding mapping T, the permutation (146389725) given by DAMM ([Dam98]) with check equation $(*')$ has phonetic detection rates of $87.5\%, 85\%, 85.42\%, 87.5\%, 87.5\%$ and 87.5% for $n = 5, 6, 7, 8, 9$ and 10 respectively. (For Type VI the percentages differ from WINTERS assertion [Win90]).
If one wants to compare the error detection rates of some representatives one can take all non–coincidental errors as a base, so the weight–percentages are

Table 11: Detection rates of phonetic errors (in %) for some representatives

	Type I	II a	III	VI b
T	$T_0=$ (01589427)(36)	(152798364)	(175)(238694)	(14)(23)(59876)
Unweighted phonetic error detection rate for T using the group D_5, check equation $(*)$ and word length n	$n=5$ 96.9 $n=6$ 95.0 $n=7$ 95.8 $n=8$ 96.4 $n=9$ 95.3 $n=10$ 95.8	$n=5$ 87.5 $n=6$ 90.0 $n=7$ 87.5 $n=8$ 85.7 $n=9$ 87.5 $n=10$ 87.5	100 %	$n=5$ 56.3 $n=6$ 62.5 $n=7$ 56.3 $n=8$ 60.7 $n=9$ 56.3 $n=10$ 59.7
Detection rate for all non – random errors (using $(*)$ and word length $n=6$)	99.87 %	99.82 %	99.84 %	99.10 %

Sources: [Ver69], [Gie99], [Sch].

slightly different from those in 6.8(ii): 86.433, 11.160, 0.656, 0.875, 0.328 and (for phonetic errors) 0.547 %; (here the error $\ldots 12\ldots \longleftrightarrow \ldots 20\ldots$ is included as in Verhoeffs statistics). One gets detection rates according to Table 11.

Since the phonetic resemblance of 12 and 20 is, in German or English, not very large, DAMM does not count the error $\ldots 12\ldots \longleftrightarrow \ldots 20\ldots$. Using $(*')$, he gets a (weighted) phonetic error detection probability of 90.48% for $\phi = (146389725)$ and of 96.83% for $\phi = (07249851)(36)$. As well GIESE has calculated the (unweighted) detection rates of phonetic errors with $\ldots 12\ldots \longleftrightarrow \ldots 20\ldots$ excluded, see Table 12.

Table 12: Detection rates of phonetic errors without $(12 \leftrightarrow 20)$ for some representatives

	Type I	II a	III	VI b
T	$T_0=$ (01589427)(36)	(152798364)	(175)(238694)	(14)(23)(59876)
Unweighted phonetic error detection rate (without $12 \longleftrightarrow 20$) for T using D_5, check equation $(*)$ and word length n	$n=5$ 96.4 $n=6$ 97.1 $n=7$ 97.6 $n=8$ 98.0 $n=9$ 96.4 $n=10$ 96.8	$n=5$ 89.3 $n=6$ 91.4 $n=7$ 90.5 $n=8$ 89.8 $n=9$ 91.1 $n=10$ 90.5	100 %	$n=5$ 50.0 $n=6$ 57.1 $n=7$ 50.0 $n=8$ 55.1 $n=9$ 50.0 $n=10$ 54.0

Sources: [Gie99],[Sch].

REMARKS. (i) A similar investigation on eqivalence of anti–symmetric map-

pings of dicyclic groups and generalized quaternion groups is in progress of being made by Sehpanuhr UGAN for her diploma thesis.
(ii) Note that check digit systems using so called total anti–symmetric mappings of the quasi-groups $(\mathbb{Z}_{10}, *)$ with

$$x * y = \begin{cases} (x + y) \text{ MOD } 10 & \text{for } x \text{ even} \\ (x - y - 2) \text{ MOD } 10 & \text{for } x \text{ odd} \end{cases}$$

may have an error detecting rate of 99,89 % for all 6 non–random error types; (cf. DAMM [Dam98]) .

C) Strong equivalence

In view of Theorem 5.2 a) we define

6.12 Definition

T_1 and T_2 are called **strongly equivalent** if there exists an $\alpha \in \text{Aut } G$ such that $T_2 = \alpha^{-1} \circ T_1 \circ \alpha$ or a $\psi \in \text{Antaut } G$ with $T_2 = \psi^{-1} \circ {T_1}^{-1} \circ \psi$.

6.13 Proposition

a) *Strong equivalence is an equivalence relation; and if T_1, T_2 are strongly equivalent then T_1 is anti-symmetric iff T_2 is anti-symmetric.*

b) *If T_1 and T_2 are strongly equivalent then T_1 and T_2 detect the same percentage of adjacent transpositions, jump transpositions, twin errors and jump-twin errors;* ([Sch]).

PROOF. a) 6.2 b) and 5.2 a). b) In view of 6.6 it suffices to consider $T_2 = \psi^{-1} \circ {T_1}^{-1} \circ \psi$ for $\psi \in \text{Antaut } G$.

$$\begin{aligned}
(x, y) \in M_{AT}(T_2) \quad &\Longleftrightarrow \quad x\psi^{-1}\big(T_1^{-1} \circ \psi(y)\big) \neq y\psi^{-1}\big(T_1^{-1} \circ \psi(x)\big) \\
&\Longleftrightarrow \quad T_1^{-1} \circ \psi(y) T_1 T_1^{-1} \psi(x) \neq T_1^{-1} \circ \psi(x) T_1 T_1^{-1} \psi(y) \\
&\Longleftrightarrow \quad \big(T_1^{-1} \circ \psi(x), T_1^{-1} \circ \psi(y)\big) \in M_{AT}(T_1);
\end{aligned}$$

similarly

$$\begin{aligned}
(x, y) \in M_{TE}(T_2) \quad &\Longleftrightarrow \quad \big(T_1^{-1} \circ \psi(x), T_1^{-1} \circ \psi(y)\big) \in M_{TE}(T_1) \\
(x, y, z) \in M_{JT}(T_2) \quad &\Longleftrightarrow \quad xyT_2^2(z) \neq zyT_2^2(x) \\
&\Longleftrightarrow \quad xy(\psi^{-1} \circ T_1^{-1} \circ \psi) \circ (\psi^{-1} \circ T_1^{-1} \circ \psi)(z) \\
&\qquad\qquad \neq zy(\psi^{-1} \circ T_1^{-1} \circ \psi \circ \psi^{-1} \circ T_1^{-1} \circ \psi)(x) \\
&\Longleftrightarrow \quad T_1^{-2} \circ \psi(z)\psi(y)\psi(x) \neq T_1^{-2} \circ \psi(x)\psi(y)\psi(z) \\
&\Longleftrightarrow \quad \big(T_1^{-2} \circ \psi(x), \psi(y), T_1^{-2} \circ \psi(z)\big) \in M_{JT}(T_1);
\end{aligned}$$

analogously

$$(x, y, z) \in M_{JZ}(T_2) \quad \Longleftrightarrow \quad \big(T_1^{-2}\psi(x), \psi(y), T_1^{-2}\psi(z)\big) \in M_{JZ}(T_1). \qquad \square$$

6.14 Strong equivalence of schemes over D_5

According to computer calculations by GIESE [Gie99] (again using the program package MAGMA) there are 911 equivalence classes of anti-symmetric mappings of D_5 with respect to strong equivalence; 115 classes, containing 4,600 systems, belong to type I to IV (see 6.7). Type I consists now of 1 equivalence class; for types II to IV as well, two equivalence classes with respect to automorphism equivalence fuse to one class with respect to strong equivalence (with 40 elements each). But the classes of Type VI remain unchanged.

References

[Bec67] D. F. Beckley. An optimum system with modulus 11. *The Computer Bulletin*, 11:213–215, 1967.

[Bed95] D. Bedford. Orthomorphisms and near orthomorphisms of groups and orthogonal Latin squares. *Bulletin of the ICA*, 15:13–33, 1995. Addendum to orthomorphisms .... Bulletin of the ICA 18:p.86,1996.

[Beu95] Albrecht Beutelspacher. Vertrauen ist gut, Kontrolle ist besser! Vom Nutzen elementarer Mathematik zum Erkennen von Fehlern. In *Jahrbuch Überblicke Mathematik 1995*, pages 27–37. Vieweg, 1995.

[Bla72] William L. Black. Error detection in decimal numbers. *Proc IEEE (Lett.)*, 60:331–332, 1972.

[BSS97] C. Broecker, R.-H. Schulz, and G. Stroth. Check character systems using Chevalley groups. *Designs, Codes and Cryptography, DESI.*, 10:137–143, 1997.

[Dam98] H.Michael Damm. Prüfziffersysteme über Quasigruppen. Diplomarbeit Universität Marburg, März 1998.

[DK89] J. Dénes and A.D. Keedwell. A new conjecture concerning admissibility of groups. *Europ. J. of Combin.*, 10:171–174, 1989.

[EP86] A. Ecker and G. Poch. Check character systems. *Computing*, 37 (4): 277–301, 1986.

[Gie99] Sabine Giese. Äquivalenz von Prüfzeichensystemen am Beispiel der Diedergruppe D_5. Staatsexamensarbeit FU Berlin, 1999.

[GM95] Joseph A. Gallian and Matthew D. Mullin. Groups with antisymmetric mappings. *Arch.Math.*, 65:273–280, 1995.

[Gum85] H.Peter Gumm. A new class of check-digit methods for arbitrary number systems. *IEEE Trans. Inf. Th. IT*, 31:102–105, 1985.

[Hei97] Stefan Heiss. Antisymmetric mappings for finite solvable groups. *Arch. Math.*, 69(6):445–454, 1997.

[HP55] Marshall Hall and L.J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 5:541–549, 1955.

[JDM61] D.M. Johnson, A.L. Dulmage, and N.S. Mendelsohn. Orthomorphisms of groups and orthogonal Latin squares I. *Canad. J. Math.*, 13: 356–372, 1961.

[Man42] H.B. Mann. The construction of orthogonal Latin squares. *Ann. Math. Statistics*, 13:418–423, 1942.

[Pai47] L.J. Paige. A note on finite abelian groups. *Bull. AMS*, 53:590–593, 1947.

[Schau56] Rudolf Schauffler. Über die Bildung von Codewörtern. *Arch. Elektr. Übertragung*, 10(7):303–314, 1956.

[Sch] R.-H. Schulz. Private communication with S.Giese.

[Sch91a] R.-H. Schulz. *Codierungstheorie. Eine Einführung.* Vieweg Verlag, Braunschweig/Wiesbaden, 1991.

[Sch91b] R.-H. Schulz. A note on check character systems using Latin squares. *Discr. Math.*, 97:371–375, 1991.

[Sch91c] R.-H. Schulz. Some check digit systems over non-abelian groups. *Mitt. der Math. Ges. Hamburg*, 12(3):819–827, 1991.

[Sch94] R.-H. Schulz. Informations– und Codierungstheorie – eine Einführung. In R.-H. Schulz (editor), *Mathematische Aspekte der angewandten Informatik*, pages 89–127. BI–Wissenschaftsverlag, Mannheim etc. 1994.

[Sch96] R.-H. Schulz. Check character systems over groups and orthogonal Latin squares. *Applic. Algebra in Eng., Comm. and Computing, AAECC*, 7:125–132, 1996.

[Sie81] Helmut Siemon. *Anwendungen der elementaren Gruppentheorie in Zahlentheorie und Kombinatorik.* Klett–Verlag, Stuttgart, 1981.

[Ver69] J. Verhoeff. *Error detecting decimal codes*, volume 29 of *Math. Centre Tracts*. Math. Centrum Amsterdam, 1969.

[Win90] Steven J. Winters. Error detecting schemes using dihedral groups. *The UMAP Journal*, 11(4):299–308, 1990.

Index