Check Character Systems and Anti-symmetric Mappings*

Ralph-Hardo Schulz

Department of Mathematics and Computer Science, Free University of Berlin
Arnimallee 3, 14195 Berlin, Germany
schulz@math.fu-berlin.de

1 Introduction

1.1 First Definitions and Historical Remarks

A *check digit system* with one check character over an alphabet A is a code

$$c : \begin{cases} A^{n-1} \longrightarrow A^n \\ a_1 a_2 \ldots a_{n-1} \longmapsto a_1 a_2 \ldots a_{n-1} a_n . \end{cases}$$

which is used to detect (but not in general to correct) single errors (i.e. errors in one component) and other errors of certain patterns (discussed below).

Historically, among the first publications[1] are articles by FRIEDMAN & MENDELSOHN (1932; cf. [9]) based on code–tables (after an International Telegraph conference) and by Rudolf SCHAUFFLER (1956; cf. [19]) using algebraic structures. In his book VERHOEFF (1969; cf. [27]) presented basic results which are in use up to the present time.

1.2 Error Types to Be Detected

Which types of errors (of human operators) have to be detected ? This question was answered more or less by statistical sampling made by VERHOEFF in a Dutch postal office and by BECKLEY, see Table 1. They show that single errors and *adjacent transpositions* (neighbour transpositions), i.e. errors of the form $\ldots ab \ldots \rightsquigarrow \ldots ba \ldots$, are the most prevalent ones (beside insertion and deletion errors which can be detected easily when all codewords have the same length n).

Note that the last two digits of a word may be affected by single errors more than all the other digits ([27] p. 14).

1.3 Systems over Groups

The systems most commonly in use are defined over alphabets endowed with a group structure. For a group $G = (A, \cdot)$ one can determine the check digit a_n

* Based on a lecture given at the graduate school on May 31, 1999, and on [24], [25].
[1] as J.Dénes found

H. Alt (Ed.): Computational Discrete Mathematics, LNCS 2122, pp. 136–147, 2001.

Table 1. Error types and their frequencies

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

Source: Verhoeff [27](12,112 pairs, 6 digits), Beckley [1].

Table 2. Detection of other errors

Error type	*Detection possible if*
twin errors	$xT(x) \neq yT(y)$ for all $x, y \in G$ with $x \neq y$
jump transpositions	$xyT^2(z) \neq zyT^2(x)$ for all $x, y, z \in G$ with $x \neq z$
jump twin errors	$xyT^2(x) \neq zyT^2(z)$ for all $x, y, z \in G$ with $x \neq z$

such that the following (check) equation holds (for fixed permutations δ_i of G, $i = 1, \dots, n$, and an element e of G, for instance the neutral element).

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

Such a system detects all *single errors;* and it detects all *adjacent transpositions* iff for all $x, y \in G$ with $x \neq y$

$$x \cdot \delta_{i+1}\delta_i^{-1}(y) \neq y \cdot \delta_{i+1}\delta_i^{-1}(x). \tag{2}$$

The proofs are straightforward. Often, one chooses a fixed permutation T of G and puts $\delta_i := T^i$ for $i = 1, \dots, n$. Equation (2) then becomes[2]

$$x\ \mathrm{T}(y) \neq y\ \mathrm{T}(x) \quad \text{for all} \quad x, y \in G \ \text{ with } x \neq y. \tag{3}$$

A permutation T of G satisfying (3) is called **anti-symmetric**. Conditions for the detection of other errors are shown in Table 2.

1.4 First Examples

Well-known systems are

[2] Some authors take $a_{n-1} \dots a_1 a_0$ as the codeword numeration and therefore $\phi^{n-1}(a_{n-1}) \dots \phi(a_1)a_0 = e$ as the check equation. Then anti-symmetry is defined by $\phi(x)y \neq \phi(y)x$ for $x, y \in G, x \neq y$. Taking the inverse mapping T^{-1} as ϕ one can transform this condition into (3) and vice versa.

ISBN 3-411-17211-8

9 783411 172115

Fig. 1. Example of an EAN (with bar-code) and an ISBN.

- the **European Article Number code (EAN)** and (after adding 0 as first digit) the **Universal Product Code (UPC)** with $G = (\mathbb{Z}_{10}, +)$, $n = 13$, $e = 0, \delta_{2i-1}(a) = a =: L_1(a)$ and $\delta_{2i}(a) = 3a =: L_3(a)$; this system does not detect adjacent transpositions $\ldots ab \ldots \rightsquigarrow \ldots ba \ldots$ for $|a-b| = 5$: the mapping $L_3 L_1^{-1}$ is not anti-symmetric. An example of an EAN is shown in Figure 1.
- the **International Standard Book Number code (ISBN)** with $G = (\mathbb{Z}_{11}, +), n = 10, e = 0$ and $\delta_i(a) = ia =: L_i(a)$ for $i = 1, \ldots, 10$; this system detects all adjacent transpositions but needs an element $X \notin \{0, \ldots, 9\}$.
- the system of the **serial numbers of German banknotes** (see e.g. [20] p.64–67.) An example of a serial number is shown in Fig. 3. (The solution for the check digit ■ is given at the end of this article.) In this system, G is D_5, the dihedral group of order 10 (see below) and $n = 11$, $\delta_i = {T_0}^i$ for $i = 1, \ldots 10$ and $\delta_{11} =$ id ; here $T_0 = (01589427)(36)$ is an anti-symmetric permutation found by VERHOEFF (cf. [27]). Thus, the check equation is

$$T_0(a_1) * T_0^2(a_2) * \cdots * T_0^{10}(a_{10}) * a_{11} = 0.$$

Letters of the serial numbers are coded as follows:

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

The *dihedral group* D_m of order $2m$ is the symmetry group of the regular $m-$gon. Denoting the rotation through angle $2\pi/m$ by d and a reflection by s (see Fig. 2) one has $\mathrm{D}_m =< d, s \mid e = d^m = s^2 \ \wedge \ ds = sd^{-1} >$. The $2m$ elements are of the form $d^i s^j$ for $i = 0, \ldots, m-1$ and $j = 0, 1$.
For any natural number m one can identify the element $d^i s^j \in \mathrm{D}_m$ with the integer $i + j \cdot m$ $(i = 0, \ldots, m-1; j = 0, 1)$. Thus one obtains a representation of D_m on $\{0, \ldots, 2m-1\}$; we denote the induced operation by $*$. The composition table for the case $m = 5$ is shown in Table 3.

2 Anti-symmetric Mappings

2.1 The Abelian Case

For an abelian group G, condition (3) is equivalent to

$$xT(x)^{-1} \neq yT(y)^{-1} \text{ for all } x, y \in G \text{ with } x \neq y. \tag{4}$$

Table 3. The operation on $\{0, 1, \ldots, 8, 9\}$ induced by D_5.

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

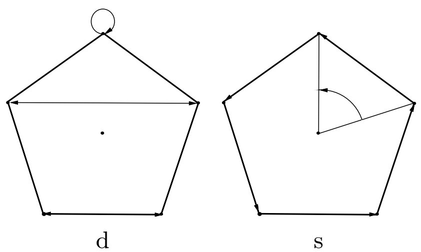

Fig. 2. Generators of D_5 (as symmetries of the regular pentagon).

Fig. 3. What does the last digit (■) of DK9673165S■ look like?

A permutation T satisfying (4) is called an *orthomorphism* or *perfect difference mapping* and $\frac{1}{T} : x \mapsto T(x)^{-1}$ is said to be a *complete mapping*, cf. MANN (1942) [17]. The theory of complete mappings is well developed. Thus one knows for example

2.1.1 Theorem. a) *A finite abelian group G admits a complete mapping iff G has odd order m or contains more than one involution;* (PAIGE 1947 [18]).

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 1955 [15]).

A consequence of this theorem is the following corollary for which DAMM [4] gave a short prove using groups with "sign", i.e. with a homomorphism $G \longrightarrow \{-1, +1\}$.

2.1.2 Corollary. (i) *A group of order $2m$ where m is odd does not admit a complete mapping.*

(ii) $\mathbb{Z}_{10}$ *does not admit a check digit system which detects all single errors and all adjacent transpositions.*

(iii) *Like the EAN, no other system using $\mathbb{Z}_{10}$ is able to detect all adjacent transpositions.* More generally:

(iv) *A cyclic group G admits an anti–symmetric mapping iff $|G|$ is odd.*

(v) *Groups of order $m = 2u$ with u odd, in particular* D_5 *and* $\mathbb{Z}_{10}$*, do not admit a check digit system which detects all twin errors or all jump twin errors.*

2.2 Further Examples

1. We mention several other anti–symmetric mappings of D_m. 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. [12]), namely $D_m \cong \{\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}_m \ \wedge \ a \in \{1, -1\}\}$. 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 $h_a(b) = u_a - ab$ with $u_1 \neq u_{-1}$ (see [21] 3.7).
Choosing $u_a = -at - c$ with $c, t \in \mathbb{Z}_m$ and $t \neq 0$ one gets the system of GUMM ([12] p.103), namely
$$T(d^k) = d^{c+t-k} \quad \text{and} \quad T(d^j s) = d^{t-c+j} s,$$
in particular for $t = r/2 = -c$ one of VERHOEFF's anti-symmetric mappings; and putting $u_{-1} = 0$ and $u_1 = 1 - m$ (or $c = t = (m-1)/2$ in GUMM l.c.) yields the system of BLACK ([2]) for $m = 5$ and of ECKER and POCH ([8] Th.4.4). If one puts $c = t = 1$ in GUMM's system, one gets the scheme of GALLIAN and MULLIN ([11]Th.2.1) for m odd: $T(d^k) = d^{2-k}$ and $T(d^j s) = d^j s$.
b) GALLIAN and MULLIN observed that for $m = 2k$ and $G = D_m$ the following mapping is anti–symmetric; ([11] l.c.; see as well [4] p.22).
$T(s) \ = e \qquad T(d^{-1}s) = ds \ T(d^j) \ = d^{1-j} \ {\scriptstyle (k+1 \leq j \leq m)}$
$T(d^j) \ = d^{1-j} s \ {\scriptstyle (1 \leq j \leq k)} \qquad T(d^j s) = d^{j+1} s \ {\scriptstyle (1 \leq j \leq k-1)}$
$T(d^j s) = d^{j+1} \ {\scriptstyle (k \leq j \leq m-2)}$
2. *Let $q = 2^m > 2$ and $K = \mathrm{GF}\,(q)$; put $u_{ac} = 1$ if $a^2 \neq c$ and otherwise $u_{ac} = u$ for a fixed $u \in K \setminus \{0, 1\}$ 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 [22] 3.1).
3. 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* and for $m = 2$ *quaternion group*; it is a group of order $4m$. *One obtains an anti–symmetric mapping* φ *in the following way* (cf. [11] Th.2.1 ii).

$$\varphi(a^i) = a^{-i} \quad (\text{for } 0 \le i \le m-1) \quad \textit{and } \varphi(a^i) = b \cdot a^{i-1} \quad (\text{for } m \le i \le 2m-1)$$
$$\varphi(ba^i) = ba^{i-1} \quad (\text{for } 0 \le i \le m-1) \quad \textit{and } \varphi(ba^i) = a^{-i} \quad (\text{for } m \le i \le 2m-1).$$

4. Further examples can be found below and, for example, in [8], [22], [21], [24].

2.3 Existence Theorems

The following theorem, similar to the abelian case, has a rather technical proof:

2.3.1 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. [11] Th.3.1).

An important tool for the construction of anti–symmetric mappings is the following.

2.3.2 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. [11]).

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 . □

In particular, the direct product of groups with anti–symmetric mappings has an anti–symmetric mapping; this was already known to GUMM [12] and, implicitly, to VERHOEFF. So one can extend the results on the existence of anti–symmetric mappings from $p-$ groups which are different from cyclic 2-groups to nilpotent groups with trivial or non–cyclic Sylow 2-subgroup. This led to the *Conjecture of Gallian and Mullin* ([11]) which has been confirmed by HEISS [13], [14]:

2.3.3 Theorem (HEISS). *Every finite non-abelian group admits an anti–symmetric mapping.*

2.4 Anti-automorphisms and Good Automorphisms

In this section we shall use automorphisms and anti-automorphisms to construct anti-symmetric mappings. We start with anti-automorphisms. 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.

2.4.1 Definition. A bijection $\psi : G \longrightarrow G$ of a group G is called an **anti-automorphism** if $\psi(xy) = \psi(y) \cdot \psi(x)$ for all $x, y \in G$.

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

2.4.2 Theorem (DAMM [4], [5]). (a) *If φ is anti-symmetric and ψ an anti-automorphism then $\psi \circ \varphi^{-1} \circ \psi^{-1}$ is anti-symmetric.*

(b) *For an anti–automorphism ψ the following are equivalent: (i) ψ is anti-symmetric. (ii) ψ is fixed point free. (iii) $\varphi^{-1} \circ \psi \circ \varphi$ is fixed point free for any (anti-) automorphism φ.*

We continue with group automorphisms.

2.4.3 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 identity element of G). When G is abelian, this is the case iff T operates fixed point freely on G;* (see [23] 3.1.)

When determining necessary and sufficient conditions for the detection of errors, one comes to the following

2.4.4 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.[3]).

2.4.5 Remarks. (i) *A good automorphism is anti-symmetric and detects single errors, adjacent transpositions, jump transpositions, twin errors and jump twin errors;* (see 2.4). (ii) *If G is abelian then the automorphism T detects 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.*

2.4.6 An Example (cf.[3]). 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 $q + 1$. Generalization:

2.4.7 Good Automorphisms on p-Groups. *Let P be a p-group and $T \in$* 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.[3]).

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

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

with $t \in \mathrm{GF}\,(q) \setminus \{0, 1\}$ acts fixed point freely on S. Therefore S admits a good automorphism and hence a check digit system which detects all single errors, *neighbour-transpositions, twin errors, jump transpositions and jump-twin errors;* (cf.[3]).

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

2.4.9 Theorem. *The Sylow 2–subgroup of a Chevalley group over* GF $(q), q = 2^m$*, admits a good automorphism* T *with* $o\,(T) \mid (q-1)$ *provided* q *is large enough;* (cf.[3] Result 2).

3 Equivalence of Check Digit Systems

Although the systems over Chevalley groups are able to detect all five types of prevalent errors we concentrate now on the dihedral group of order 10 since its elements can be interpreted as $0, 1, \ldots, 9$ in the decimal system.

Because there are (exactly) 34,040 anti–symmetric mappings over D_5 (VERHOEFF [27] p.92, DAMM [4] p.44, GIESE [10]) we want to define equivalences between these (and the corresponding schemes). There are several possibilities to do so. Throughout this section, let G be a group and T_1, T_2 permutations of G.

3.1 Weak Equivalence

3.1.1 Definition. T_1 and T_2 (and the related schemes) are called **weakly equivalent** if there exist elements $a, b \in G$ and an automorphism $\alpha \in$ 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. [27], [4] p.38, [24]). Weak equivalence is an equivalence relation.

3.1.2 Theorem. a) *If* T_1 *and* T_2 *are weakly equivalent and if* T_1 *is anti–symmetric, then* T_2 *is also anti-symmetric* ([27], [4]) .

b) *If* T_1 *and* T_2 *are weakly equivalent permutations of* G *then they detect the same percentage of twin errors* ([24], [10]).

c) *If* T_1 *is an* **automorphism** *of* G *and if* T_2 *is weakly 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* ([24], [10]).

Proof (Sketch). b) We have (for $\overline{x} = \alpha(bx)$ and $\overline{y} = \alpha(by)$):
$xT_2(x) \neq yT_2(y) \iff x\alpha^{-1}T_1\alpha(bx)a \neq y\alpha^{-1}T_1\alpha(by)a \iff \overline{x}\,T_1(\overline{x}) \neq \overline{y}\,T_1(\overline{y})$
c) 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 $\overline{y} = \alpha(y)T_1(\alpha(b))$. Similarly for jump twin errors. □

3.1.3 Weak Equivalence and Detection Rates. The following counterexample (cf. [10], [24]) shows that systems with weakly equivalent anti-symmetric permutations may have different detection rates. Let T_0 be the anti–symmetric mapping $T_0 = (01589427)(36)$ of VERHOEFF. It detects 94.22 % of jump transpositions and 94.22 % of jump twin errors. The weakly equivalent permutation

Table 4. Types of anti–symmetric mappings of D_5 and their detection rates

	I	IIa	IIb	III	IV	VIa/b	V
single errors	100%						
adjacent transpos.	100%						
twin errors	95.56	95.56	91.11	91.11	91.11	55.56	
jump transpositions	94.22	92	94.22	92	90.22	66,67	
jump twin errors	94.22	92	94.22	92	90.22	66.67	
Detection rate of all 5 error types (weighted)	99.90	99.87	99.87	99.84	99.82	99.30	99.85-99.42
number of classes	2	44	8	160	16	1/5	1470
elements in a class	20	20	20	20	20	20/4	20

Source: GIESE [10],[24].

$T_1 := R_4 \circ \mathrm{id} \circ T_0 \circ \mathrm{id} \circ L_3$, namely $T_1 = (079482)(36)$ detects only 87.56 % of all jump transpositions and jump twin errors respectively. Therefore, we look for equivalence relations preserving the detection rates.

3.2 Automorphism Equivalence and Strong Equivalence

3.2.1 Definition. T_1 and T_2 (and the related systems) are called **automorphism equivalent** if there exists an $\alpha \in \mathrm{Aut}\, G$ such that $T_2 = \alpha^{-1} \circ T_1 \circ \alpha$; and they are said to be **strongly equivalent** if they are automorphism equivalent or if there exists an anti-automorphism ψ with $T_2 = \psi^{-1} \circ T_1^{-1} \circ \psi$; ([24], [25]).

3.2.2 Proposition. *Automorphism equivalence and strong equivalence are equivalence relations; and if T_1 and T_2 are automorphism equivalent then T_1 and T_2 are weakly equivalent. If T_1 and T_2 are automorphism equivalent or strongly equivalent, then T_1 and T_2 detect the same percentage of adjacent transpositions, jump transpositions, twin errors and jump twin errors;* ([10], [24]).

3.2.3 The Dihedral Group of Order 10. a) *Types of equivalence classes.* 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 [10]. S. Giese distinguishes 6 types of classes according to the rate of detection of errors, see Table 4.

b) *Some representatives.* To Type I there belong e.g. T_0, (03986215)(47) and (07319854)(26) (VERHOEFF's mappings) ; the mappings of GUMM, SCHULZ, BLACK and WINTERS mentioned in 2.2 belong to Type VIb.

3.2.4 The Quaternion Group Case. By coding the elements of $Q_2 = \langle a, b | a^4 = e \wedge b^2 = a^2 \wedge ab = ba^{-1} \rangle$ by $a^i b^j \longmapsto i + 4j$ $(i = 0, \ldots, 3;\ j = 0, 1)$ one gets Table 5 as the multiplication table. There exist exactly 1,152 anti–symmetric mappings of Q_2which constitute 48 equivalence classes of size 24 each with respect to automorphism equivalence (as S. Ugan found out using C^{++}). The

Table 5. Multiplication table of the quaternion group.

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

Table 6. Multiplication in Q_3.

$i * j$	$0 \leq j \leq 5$	$6 \leq j \leq 11$
$0 \leq i \leq 5$	$(i+j)\text{MOD } 6$	$(i+j)\text{MOD } 6+6$
$6 \leq i \leq 11$	$(i-j)\text{MOD } 6+6$	$(i-j+3)\text{MOD } 6$

mapping of GALLIAN & MULLIN, (0)(1362745), belongs to Type I. (For more details see [26], [25]).

3.2.5 The Dicyclic Group of Order 12. (a) As defined in 2.2, Q_3 is $\langle a, b | a^6 = e \wedge b^2 = a^3 \wedge ab = ba^{-1} \rangle$. The elements of this group can be coded by the numbers 0 to 11 by $a^i b^j \longmapsto i+6j \quad (i = 0, \ldots, 5; \;\; j = 0, 1)$. This yields the multiplication shown in Table 6.

(b) According to a computer search by S. UGAN (1999)[26], see as well [25], there are exactly $1,403,136$ anti–symmetric mappings of Q_3; (this means that only approximately 0.3% of the 12! permutations of Q_3 are anti–symmetric). Further results are shown in Table 7.

c) *Representatives for Type I in Q_3.* Representatives of the 4 classes of Type I with respect to strong equivalence are (0 1 6 9 10 8 2 5 11 3 7 4),(0 2 6 11 7 9 3 8 1 5 4 10), (0 6 8 10 9 5 3 11 1 2 4 7),(0 6 1 3 4 11 8 9 7 5 2 10).

d) *The Mapping of Gallian and Mullin.* For $m = 3$, their anti–symmetric mapping is (0)(1 5 8 2 4 9 3 10 11 6 7); it has a detection rate of 81.82% for twin errors, of 92.42% for jump transpositions and jump twin errors respectively; the weighted rate for all 5 errors under consideration is 99.79% (cf. Ugan [26]).

4 Generalization to Quasigroups

$(Q, *)$ is called a **quasigroup** if the equations $x * b = c$ and $a * y = c$ have a unique solution x and y (respectively) for every $a, b, c \in Q$. Quasigroups are another way to describe **Latin squares**, cf. [6], [7], [16].

Let $(Q, *_i)$ be quasigroups; then one uses as check equation

$$(\ldots(x_n *_n x_{n-1}) *_{n-1} x_{n-2}) \ldots) *_1 x_0 = d$$

Of importance for error detection are now (i) the anti–symmetry of $(Q, *)$:

$$x * y = y * x \Longrightarrow x = y \quad (\text{for all } x, y \in Q)$$

Table 7. Types of check digit systems of Q_3 with detection rates of over 90% for each considered error type.

	Type I	Type II	Type III/IV
single errors	100%		
adjacent transpos.	100%		
twin errors	96.97%	96.97–93,94	96.97–90.91
jump transpositions	94.70%	95.71–93.94	95.96–90.15
jump twin errors	94.70%	95.45–93.18	95.96–90.15
all 5 error types (weighted)	99.92%	99.91	99.90-99.82
number of automorphism equivalence classes	8	204	804/26,464
number of strong equivalence classes	4	102	402/13,232
number of check digit systems	96	2,448	9,648/317,568

Source: Ugan [26],[25]

and (ii) the *total anti–symmetry*, that means anti–symmetry with

$$(c * x) * y = (c * y) * x \Longrightarrow x = y \quad (\text{for all } x, y \in Q).$$

For more details see e.g. [8], [22],[4].

5 Solution of the Exercise

The alpha-numeric serial number of the banknote of Figure 2 with hidden check digit is DK9673165S$\mathbf{\Lambda}$. Substituting the letters as indicated in section 1.4 one obtains 1396731656$\mathbf{\Lambda}$. Applying the check equation gives

$$T_0(1)*T_0^2(3)*T_0^3(9)*T_0^4(6)*T_0^5(7)*T_0^6(3)*T_0^7(1)*T_0^8(6)*T_0^9(5)*T_0^{10}(6)*\mathbf{\Lambda} = 0,$$

an equation equivalent to $\underbrace{5*3}_{7}*\underbrace{7*6}_{1}*\underbrace{9*3}_{6}*\underbrace{0*6}_{6}*\underbrace{8*6}_{2}*\mathbf{\Lambda} = 0$;

$7*1*6*6*2*\mathbf{\Lambda} = 0$ leads to $6*0*2*\mathbf{\Lambda} = 0$ which has $\mathbf{\Lambda} = 9^{-1} = 9$ as solution.

References

1. Dudley F. Beckley. An optimum system with modulus 11. *The Computer Bulletin*, 11:213–215, 1967.
2. William L. Black. Error detection in decimal numbers. *Proc IEEE (Lett.)*, 60:331–332, 1972.
3. Claudia Broecker, Ralph-Hardo Schulz, and Gernot Stroth. Check character systems using chevalley groups. *Designs, Codes and Cryptography, DESI.*, 10:137–143, 1997.

4. Michael Damm. Prüfziffersysteme über Quasigruppen. Diplomarbeit Universität Marburg, März 1998.
5. Michael Damm. Check digit systems over groups and anti-symmetric mappings. *Archiv der Mathematik*, to appear.
6. J. Dénes and A.D. Keedwell. *Latin Squares and their Applications.* Academic Press, New York, 1974.
7. J. Dénes and A.D. Keedwell. *Latin Squares. New Developments in the Theory and Applications.* North Holland, Amsterdam, 1991.
8. A. Ecker and G. Poch. Check character systems. *Computing*, 37(4):277–301, 1986.
9. W. Friedman and C. J. Mendelsohn. *Notes on Codewords. Am. Math. Monthly*, pages 394–409, 1932.
10. Sabine Giese. Äquivalenz von Prüfzeichensystemen am Beispiel der Diedergruppe D_5. Staatsexamensarbeit, FU Berlin. Jan. 1999.
11. Joseph A. Gallian and Matthew D. Mullin. Groups with antisymmetric mappings. *Arch.Math.*, 65:273–280, 1995.
12. H. Peter Gumm. A new class of check-digit methods for arbitrary number systems. *IEEE Trans. Inf. Th. IT*, 31:102–105, 1985.
13. Stefan Heiss. Antisymmetric mappings for finite solvable groups. *Arch. Math.*, 69(6):445–454, 1997.
14. Stefan Heiss. Antisymmetric mappings for finite groups. Preprint, 1999.
15. M. Hall and L.J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 5:541–549, 1955.
16. Charles F. Laywine and Gary L. Mullen. *Discrete Mathematics using Latin Squares.* J. Wiley & Sons, New York etc., 1998.
17. H.B. Mann. The construction of orthogonal latin squares. *Ann. Math. Statistics*, 13:418–423, 1942.
18. L.J. Paige. A note on finite abelian groups. *Bull. AMS*, 53:590–593, 1947.
19. R. Schauffler. Über die Bildung von Codewörtern. *Arch. Elektr. Übertragung*, 10(7):303–314, 1956.
20. R.-H. Schulz. *Codierungstheorie. Eine Einführung.* Vieweg Verlag, Braunschweig / Wiesbaden, 1991.
21. R.-H. Schulz. A note on check character systems using latin squares. *Discr. Math.*, 97:371–375, 1991.
22. R.-H. Schulz. Some check digit systems over non-abelian groups. *Mitt. der Math. Ges. Hamburg*, 12(3):819–827, 1991.
23. R.-H. Schulz. Check character systems over groups and orthogonal latin squares. *Applic. Algebra in Eng., Comm. and Computing, AAECC*, 7:125–132, 1996.
24. R.-H. Schulz. On check digit systems using anti-symmetric mappings. In I. Althöfer et al., editor. *Numbers, Information and Complexity*, pages 295–310. Kluwer Acad.Publ. Boston, 2000.
25. R.-H. Schulz. Equivalence of check digit systems over the dicyclic groups of order 8 and 12. In J. Blankenagel & W. Spiegel, editor, *Mathematikdidaktik aus Begeisterung für die Mathematik*, pages 227–237. Klett Verlag, Stuttgart, 2000.
26. Sehpahnur Ugan. Prüfzeichensysteme über dizyklischen Gruppen der Ordnung 8 und 12. Diplomarbeit, FU Berlin, Oct. 1999.
27. J. Verhoeff. *Error detecting decimal codes*, volume 29 of *Math. Centre Tracts.* Math. Centrum Amsterdam, 1969.