Check digit systems with error correction

Ralph–Hardo Schulz

Abstract

We describe check character systems over finite abelian groups which can detect double errors and correct single errors and neighbour transpositions. The systems make use of fixed point free automorphisms; examples involve linear mappings or multiplication with field elements.

Key words:

Check digit systems, check character systems, codes, error detection, error correction, abelian groups, automorphisms, fixed point free, anti-symmetric, orthomorphisms, complete mappings, field extensions.

AMS-Classification-Nr. : 94B60; 11T71; 15A04

Introduction

Check digit systems are codes over an alphabet A which arise by appending either one or two check characters to every information $a_1 \dots a_n \in A^n$. Usually, they are used to *detect* errors caused during transmission. They were studied by FRIEDMAN and MENDELSON [FM] *, SCHAUFFLER [Schau] * , VERHOEFF [V] and many others, see f. i. [Schu_1] p. 56-73 or [Schu_3] p. 124-126. In a previous article ([Schu_2]) we described check character systems with two check digits which detect double errors, that are errors of the form

$$a_1 \dots a_i \dots a_j \dots a_{n+2} \rightsquigarrow a_1 \dots a_i' \dots a_j' \dots a_{n+2}$$

with $a_i \neq a_i'$ and $a_j \neq a_j'$. In the present paper we show that similar systems can be used as well to *correct* errors, namely single errors (errors in one component) and (although the codes have Hamming distance 3 only) even all adjacent transpositions (neighbour transpositions) i. e. errors of the form

$$a_1 \dots a_i a_{i+1} \dots a_{n+2} \rightsquigarrow a_1 \dots a_{i+1} a_i \dots a_{n+2}\,;$$

these errors are frequent during human transmission (see [V] or [Bec]). The fact that corrections of these types are possible at all was found out by SETHI, RAJARAMAN and KENJALE ([SRK]) whose results are generalized in the present article. Instead

*I am grateful to Dr. J. Dénes (Budapest) for calling my attention to these early papers.

restricting us to $A = (\mathbb{Z}_p, +)$ we use finite abelian groups and check equations

$$\sum_{i=1}^{n+2} \beta_i(a_i) = 0 = \sum_{i=1}^{n+2} \gamma_i(a_i)$$

where β_i and γ_j are group automorphisms – with the exception that β_{n+2} and γ_{n+1} may be the zero-endomorphism too (if one does not want to check the check digits). Of course, these automorphisms have to fulfill some additional conditions (see theorem 1.11 below). To illustrate the theory we descibe how to construct examples of single error correcting and adjacent transposition correcting codes (SEC-ATC-codes) using linear mappings or multiplication with field elements.

Previous work with similar but different aims

Single errors and adjacent transpositions can be corrected a forteriori by SEC-DAEC-codes (single error correcting double adjacent error correcting codes); these have been considered by ABRAMSON [†] [A_1], [A_2], but there does not exist a SEC-DAEC-code of length N with two parity bits: this can be seen by determining the size of an error ball as $|K| = 1 + N(q-1) + (N-1)(q-1)^2$ for each of the q^{N-2} codewords (with $|A| = q$) and showing that $q^{N-2} \cdot |K| > q^N$. What the starting point of ABRAMSON concerns, by restricting oneself to two equations and two parity characters, one gets special cases of $(**)$. Double adjacent error correcting codes are as well among the graphical codes considered by JUNGNICKEL and VANSTONE ([JV]). Here again one needs more than two check digits. The bit shift error correcting binary codes of LEVITIN and VAINSTEIN ([LeV]) correct adjacent transpositions but not single errors. Adjacent transpositions can be corrected as well by codes capable of correcting one deletion and one insertion; so the investigations of LEVENSHTEIN[†] [L] can be of relevance. Notice that there can not exist a binary code of length $N > 3$ with two parity bits which is one error-correcting ($2^{N-2}(1+N) > 2^N$) and, in the non-binary case, that there exist SEC-ATC-codes which do not allow to correct all pairs of insertions and deletions: the code with check equations

$$\sum_{i=1}^{N} w_i a_i = 0 = \sum_{i=1}^{N} w_i' a_i \quad \text{with} \quad A = \mathbb{Z}_{11} \quad , N = 4$$

and weights $w_i = i + 2$, $w_i' = (i+2)i$ fulfills the conditions (3.1) to (3.2) of SETHI et alii [SRK] and is therefore an SEC-ATC-code; but the code word 1645 can be changed by the deletion of 6 and the insertion of 0 to 1450 which is a codeword, too. So the theory of SEC-ATC-codes should be developed independently.

[†] I thank the Russian collegues who participated at the 1996 conference on coding and information theory at Oberwolfach for calling my attention to these articles.

1. Error correcting systems using many automorphisms

Throughout this paper, $(A,+)$ denotes a finite abelian group with neutral element 0. The zero–endomorphism is written as 0 as well. Similarly to [Schu$_2$] (2.10), we investigate a check digit system over the alphabet A of the following type.

1.1 Definition

Let $\beta_1,\ldots,\beta_{n+1},\gamma_1,\ldots,\gamma_n,\gamma_{n+2}$ be automorphisms of $(A,+)$ and $\beta_{n+2},\gamma_{n+1}\in \mathrm{Aut}A\cup\{0\}$. (In the whole article, n is supposed to be a natural number and $N := n+2$ to be the codeword length.) We study a check digit system

$$A^n \to A^{n+2} \quad \text{with} \quad a_1\ldots a_n \mapsto a_1\ldots a_n a_{n+1} a_{n+2}$$

and call it system $(*)$ if it has the following property. Given the *information digits* $a_1\ldots a_n$, the *check characters* a_{n+1}, a_{n+2} are chosen such that

$$(**) \qquad \sum_{i=1}^{n+2} \beta_i(a_i)=0 \qquad \text{and} \qquad \sum_{i=1}^{n+2}\gamma_i(a_i)=0$$

The equations have a unique solution (a_{n+1},a_{n+2}) for any n-tuple $a_1\ldots a_n$ if, for instance, $\gamma_{n+2}\,\beta_{n+2}=\beta_{n+2}\,\gamma_{n+2}$ and $\gamma_{n+2}\,\beta_{n+1}-\beta_{n+2}\,\gamma_{n+1}$ is invertable. This follows by applying γ_{n+2} and β_{n+2} respectively to the equations $(**)$ and subtracting one from the other. Then

$$a_{n+1} = (\beta_{n+2}\gamma_{n+1}-\gamma_{n+2}\beta_{n+1})^{-1}\sum_{i=1}^{n}(\gamma_{n+2}\beta_i-\beta_{n+2}\gamma_i)(a_i) \quad \text{and}$$
$$a_{n+2} = -\sum_{i=1}^{n+1}\gamma_{n+2}{}^{-1}\gamma_i\,(a_i)$$

are uniquely determined and satisfy $(**)$. The conditions mentioned are f. i. fulfilled for $\beta_{n+2}=0$.

1.2 Error detecting capabilities (cf. [Schu$_2$], 2.10)

The check digit system $(*)$ is single error detecting, and it is double error detecting iff the following conditions are fulfilled:

($\Diamond$) *The automorphisms $\beta_j^{-1}\beta_i\gamma_i^{-1}\gamma_j$ are fixed point free on A for all i,j with $i<j\le n+2$ for which β_i,β_j,γ_i and γ_j are different from 0.*

Here, as usual, an automorphism α of a group G is called *fixed point free* if the neutral element is the only element of G fixed by α.

1.3 Remarks

(i) Notice that $\alpha\beta$ is fixed point free if $\beta\alpha$ has this property (for automorphisms α, β of A). This can be seen by considering the image under α^{-1} of a fixed element of $\alpha\beta$. Furthermore, α and α^{-1} have the same fixed point behaviour.

(ii) If γ_{n+2} and β_{n+2} commute, condition ($\Diamond$) guarantees as well that $\gamma_{n+2}\,\beta_{n+1} - \beta_{n+2}\,\gamma_{n+1}$ is invertable, and therefore, that the check digits are determined (see 1.1). Here we use the fact that an automorphism α of an abelian group is fixed point free iff $\mathrm{id} - \alpha$ is injective (see as well 1.4 below).

(iii) The condition ($\Diamond$) corresponds to condition C3 in [SRK].

(iv) The set $\mathcal{C}$ of codewords of the system ($*$), i.e.

$$\mathcal{C} = \{\boldsymbol{x} \in A^{n+2} \,|\, \boldsymbol{x} = a_1 \dots a_{n+2} \text{ fulfills } (**)\}$$

has minimal Hamming distance $d_{\min}(\mathcal{C}) \leq 3$ (for definition see f.i. [Schu$_1$] 10.11, [Schu$_3$] or [McWSl]); and if the system is double error detecting, we have, of course, $d_{\min}(\mathcal{C}) = 3$. So, in the latter case, $\mathcal{C}$ can be considered as well as an 1–error *correcting* code (see f.i. [Schu$_1$] l.c.)

1.4 Remarks on orthomorphisms and fixed point free automorphisms

(i) Recall that, by definition, an *orthomorphism* (cf. [JDM]) is a permutation γ of a group $(G, \cdot)$ such that $\mathrm{id} \cdot \frac{1}{\gamma} : x \mapsto x \cdot \gamma(x)^{-1}$ is again a permutation of the set G. If γ is an orthomorphism then $\frac{1}{\gamma} : x \to \gamma(x)^{-1}$ is called a *complete* mapping (see as well [P], [HP], [DK], [Si], [B] or [Schu$_1$] §8). A permutation γ is called *anti-symmetric* if $x\gamma(y) \neq y\,\gamma(x)$ for all $x, y \in G$ with $x \neq y$ (see [GM], [He], [V], [Schu$_1$]§8 or [Schu$_4$] condition ($*$)).

(ii) Notice that, for a finite abelian group $(A, +)$ and $\alpha \in \mathrm{Aut}\, A$ the following conditions are equivalent (–here we put $1 := id_A$)

(1) α is fixed point free (2) $1 - \alpha$ is invertable (3) α is an orthomorphism
(4) α is anti-symmetric (5) $-\alpha$ is a complete mapping

As can be seen in [SRK], there exist schemes having distance 3 which can correct not only single errors but adjacent transpositions (neighbour transpositons), too. Generalizing the work of SETHI et alii (l.c.) we want to investigate under which conditions the systems ($*$) allow such corrections. In order to do so we define a syndrom–mapping in the obvious way:

1.5 Syndrom

The mapping $S : A^{n+2} \to A^2$ given by $a_1 \dots a_{n+2} \mapsto (S_1, S_2)$ with

$$S_1 = \sum_{i=1}^{n+2} \beta_i(a_i) \qquad \text{and} \qquad S_2 = \sum_{i=1}^{n+2} \gamma_i(a_i)$$

assigns to every word from A^{n+2} a *syndrom* $(S_1, S_2) \in A^2$. Since A is abelian, the syndrom mapping S is a homomorphism with $\mathcal{C} = \text{kernel}(S)$.

1.6 Single error analysis

We consider a check digit system with equations $(**)$ *having property* $(\Diamond)$. *Let* (S_1, S_2) *be the syndrom of a word* $\boldsymbol{a}' = a_1 \dots a_j' \dots a_{n+2}$ *with error in component* j *and, for* $d = a_j' - a_j \neq 0$, *with error vector* $\boldsymbol{e} = (0, \dots, 0, d, 0, \dots, 0)$. *Then* $S_1 = 0$ *iff* $\beta_{n+2} = 0$ *and* $j = n+2$; *for all other cases we have*

$$S_2 = \gamma_j \beta_j^{-1}(S_1) \quad \text{and} \quad S_2 \neq \gamma_k \beta_k^{-1}(S_1) \tag{1.6.1}$$

for $j \neq k$ and $k = 1, \dots, n+1$ and, in case $\beta_{n+2} \neq 0$ as well for $k = n+2$. *Therefore, by checking whether* $S_1 = 0$ *or* $S_2 = \gamma_j \beta_j^{-1}(S_1)$ *the error position* j *can be detected (under the condition that a single error has occured) and* d *calculated as* $\beta_j^{-1}(S_1)$ *if* $S_1 \neq 0$ *and as* $\gamma_j^{-1}(S_2)$ *if* $S_2 \neq 0$.

Proof: Let $\boldsymbol{a} = a_1 \dots a_j \dots a_{n+2} \in \mathcal{C}$ and $\boldsymbol{a}' = a_1 \dots a_j' \dots a_{n+2} = \boldsymbol{a} + \boldsymbol{e}$; since S is additive we have

$$S(\boldsymbol{a}') = (S_1, S_2) = (\beta_j(d), \gamma_j(d)). \tag{1.6.2}$$

Notice that, for single errors, $S_1 = 0$ iff $(j = n+2$ and $\beta_{n+2} = 0)$ and $S_2 = 0$ iff $(j = n+1$ and $\gamma_{n+1} = 0)$. Now, let $S_1 \neq 0$. Then $S_2 = \gamma_j(d) = \gamma_j \beta_j^{-1}(S_1)$; if $S_2 = 0$, then $j = n+1$. Hence suppose $S_2 \neq 0$ and $\gamma_k \beta_k^{-1}(S_1) = S_2 = \gamma_j \beta_j^{-1}(S_1)$. We get $\beta_j \gamma_j^{-1} \gamma_k \beta_k^{-1}(S_1) = S_1$ and therefore $j = k$ by $(\Diamond)$ and (1.3 (i)). $\Box$

1.7 Syndroms of neighbour transpositions

Let (S_1, S_2) *be the syndrom of a word* $\boldsymbol{a}' = a_1 \dots a_{i+1} a_i \dots a_{n+2}$ *(with* $i \in \{1, \dots, n+1\}$*) obtained from a codeword* $\boldsymbol{a} \in \mathcal{C}$ *by interchanging the adjacent components* a_i *and* a_{i+1}. *Then, if* $\beta_{i+1} - \beta_i$ *or* $\gamma_{i+1} - \gamma_i$ *has an inverse,*

$$S_2 = (\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1}(S_1) \quad \text{or} \quad S_1 = (\beta_{i+1} - \beta_i)(\gamma_{i+1} - \gamma_i)^{-1}(S_2). \tag{1.7.1}$$

(If both inverses exist the two equations are equivalent).

Proof: We have

$$\begin{aligned} S_1 = \quad S_1 - 0 = & \sum_{\substack{\ell=1\\ \ell\neq i,i+1}}^{n+2} \beta_\ell(a_\ell) + \beta_i(a_{i+1}) + \beta_{i+1}(a_i) - \sum_{\ell=1}^{n+2}\beta_\ell(a_\ell) \\ = \quad & \beta_i(a_{i+1}) + \beta_{i+1}(a_i) - \beta_i(a_i) - \beta_{i+1}(a_{i+1}) = (\beta_{i+1}-\beta_i)(a_i - a_{i+1}) \\ = \quad & (\beta_{i+1}-\beta_i)(D_i) \end{aligned}$$

with $D_i = a_i - a_{i+1}$. Similarly, we get $S_2 = (\gamma_{i+1}-\gamma_i)(D_i)$, in total

$$S(\boldsymbol{a}') = (S_1, S_2) = ((\beta_{i+1}-\beta_i)(D_i),\ (\gamma_{i+1}-\gamma_i)(D_i))\,. \tag{1.7.2}$$

If $(\beta_{i+1}-\beta_i)^{-1}$ exists, we have $D_i = (\beta_{i+1}-\beta_i)^{-1}(S_1)$ and therefore $S_2 = (\gamma_{i+1}-\gamma_i)(\beta_{i+1}-\beta_i)^{-1}(S_1)$. The second part of 1.7.1 follows similarly. □

1.8 Remark

If $\beta_i^{-1}\beta_{i+1}$ is an orthomorphism of the finite abelian group A, then $\beta_{i+1}-\beta_i = -\beta_i(1-\beta_i^{-1}\beta_{i+1})$ is a permutation of A (for $i \in \{1,\dots,n\}$). Hence the inverse $(\beta_{i+1}-\beta_i)^{-1}$ exists . The same situation is given if $i = n+1$ and $\beta_{n+2} \neq 0$. Vice versa, if $\beta_i \neq 0$ and $\beta_{i+1}-\beta_i$ is invertable then $-\beta_i(1-\beta_i^{-1}\beta_{i+1})$ is a permutation and $\beta_i^{-1}\beta_{i+1}$ an orthomorphism. If $\beta_{n+2} = 0$ then $\beta_{n+2}-\beta_{n+1} = -\beta_{n+1}$ has an inverse (by definition (1.1)). Similarly, if γ_i^{-1} exists and $\gamma_i^{-1}\gamma_{i+1}$ is an orthomorphism then $(\gamma_{i+1}-\gamma_i)^{-1}$ exists (for $i \in \{1,\dots,n+1\}$). If $\gamma_{n+1} = 0$ and ($i = n$ or $i = n+1$), then again $(\gamma_{i+1}-\gamma_i)$ is invertible.

1.9 Distinguishing single errors from adjacent transpositions

a) *Let $i \in \{1,\dots,n+1\}$, $j \in \{1,\dots,n\}$ or ($j = n+1$ and $\gamma_{n+1} \neq 0$) or ($j = n+2$ and $\beta_{n+2} \neq 0$). Then a condition sufficient for the possibility to distinguish a single error in position j from an adjacent transposition in position $(i, i+1)$ is the following*

$$\beta_j^{-1}(\beta_{i+1}-\beta_i)(D) \neq \gamma_j^{-1}(\gamma_{i+1}-\gamma_i)(D) \tag{1.9.1}$$

$$\textit{for all}\quad D \notin K_0 := \text{ kernel }(\beta_{i+1}-\beta_i) \cup \text{ kernel }(\gamma_{i+1}-\gamma_i)\,.$$

For j as above and $i < n$ this condition is as well necessary for distinguishing the errors in question by the syndroms alone.

b) *A single error in position $j = n+1$ if $\gamma_{n+1} = 0$ and in position $j = n+2$ if $\beta_{n+2} = 0$ can be distinguished from a neighbour transposition in position $(i, i+1)$ (with $i \in \{1,\dots,n+1\}$) if*

$$\text{kernel }(\beta_{i+1}-\beta_i) = \text{ kernel }(\gamma_{i+1}-\gamma_i) \tag{1.9.2}$$

Summerizing we have:

c) *Using the system* $(*)$ *with check equations* $(**)$ *every single error can be distinguished from every adjacent transposition if the following (sufficient) conditions are fulfilled for* $i = 1, \ldots, n+1$, $j = 1, \ldots, n$ *and, in case* $\gamma_{n+1} \neq 0$, *for* $j = n+1$, *in case* $\beta_{n+2} \neq 0$ *for* $j = n+2$.

($\Diamond\Diamond$) $\beta_{i+1} - \beta_i$ and $\gamma_{i+1} - \gamma_i$ *are invertable and* $\beta_j \gamma_j^{-1}(\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1}$ *operates fixed point freely on* A.

Proof: Assume that (S_1, S_2) is the syndrom both of a single error in position j of a codeword $\boldsymbol{a}$ and of a neighbour transposition in position $(i, i+1)$ of a codeword $\boldsymbol{b}$. Then, by (1.6.2) and (1.7.2), we get (with $d, D \in A \setminus \{0\}$ and $d := a_j' - a_j$, $D := b_i - b_{i+1}$):

$$(1.9.3) \qquad \beta_j(d) = S_1 = (\beta_{i+1} - \beta_i)(D) \qquad \text{and} \quad \gamma_j(d) = S_2 = (\gamma_{i+1} - \gamma_i)(D)$$

a) If $\beta_j, \gamma_j \in \operatorname{Aut} A$ then $\beta_j^{-1}(\beta_{i+1} - \beta_i)(D) = d = \gamma_j^{-1}(\gamma_{i+1} - \gamma_i)(D)$ and $D \in A \setminus K_0$, contradicting (1.9.1). If, vice versa, (1.9.1) is violated, there exists a $D \in A$ with $D \notin K_0$ such that $d := \beta_j^{-1}(\beta_{i+1} - \beta_i)(D) = \gamma_j^{-1}(\gamma_{i+1} - \gamma_i)(D) \neq 0$. For these elements D and d, equations (1.9.3) hold and supply the syndroms in question if a codeword $\boldsymbol{b} = b_1 \ldots b_{n+2}$ with $b_{i+1} = b_i - D$ can be found; for $i < n$ the existence of such an element of $\mathcal{C}$ is clear by the condition on the solvability of equations $(**)$, see (1.1).
b) If $j = n+1$ and $\gamma_{n+1} = 0$, equations (1.9.3) read $0 \neq \beta_{n+1}(d) = (\beta_{i+1} - \beta_i)(D)$ and $(\gamma_{i+1} - \gamma_i)(D) = 0$, contradicting (1.9.2). If $j = n+2$ and $\beta_{n+2} = 0$ we get $0 = (\beta_{i+1} - \beta_i)(D)$ and $\gamma_{n+2}(d) = (\gamma_{i+1} - \gamma_i)(D) \neq 0$, again a contradiction.
c) Let i and j be as in part a) and suppose that (1.9.1) is violated. Then $K_0 = \{0\}$ by ($\Diamond\Diamond$) and $\beta_j^{-1}(\beta_{i+1} - \beta_i)(D) = \gamma_j^{-1}(\gamma_{i+1} - \gamma_i)(D)$ for at least one $D \neq 0$. Put $\hat{D} := (\beta_{i+1} - \beta_i)(D)$; now $\hat{D} \neq 0$ and $\hat{D} = \beta_j \gamma_j^{-1}(\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1}(\hat{D})$, a contradiction to ($\Diamond\Diamond$). In the remaining cases, i and j are as in part b). Now condition ($\Diamond\Diamond$) assures that $\operatorname{kernel}(\beta_{i+1} - \beta_i) = \{0\} = \operatorname{kernel}(\gamma_{i+1} - \gamma_i)$. □

Remarks

(i) Notice that ($\Diamond\Diamond$) corresponds to (C5) and parts of (C2) of [SRK].

(ii) If ($\Diamond\Diamond$) is fulfilled $\gamma_j \beta_j^{-1}(\beta_{i+1} - \beta_i)(\gamma_{i+1} - \gamma_i)^{-1}$ is fixed point free, too (see 1.3(i)).

1.10 Distinguishing adjacent transpositions from each other

A condition sufficient for the possibility to localize an adjacent transposition (under the premise that an error of such a type has occured) by the syndrom alone is the following.

($\Diamond\Diamond\Diamond''$) $\quad \alpha_{ki} := (\gamma_{k+1} - \gamma_k)^{-1}(\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1}(\beta_{k+1} - \beta_k)$ *operates fixed point freely on* A *(for* $i < k \leq n+1$*).*

For $i < k < n$ these conditions are as well necessary. (Here we assume that the inverses of $(\gamma_{k+1} - \gamma_k)$ and $(\beta_{i+1} - \beta_i)$ exist.)

Remarks

(i) Conditions $(\Diamond\Diamond\Diamond'')$ correspond to (C4) of [SRK].

(ii) The mapping $(\beta_{k+1} - \beta_k)(\gamma_{k+1} - \gamma_k)^{-1}(\gamma_{i+1} - \gamma_i)(\beta_{i+1} - \beta_i)^{-1}$ is fixed point free iff α_{ki} has this property (see 1.3(i)).

Proof of 1.10: Suppose that neighbour transpositions in positions $(i, i+1)$ and $(k, k+1)$ lead to the same syndrom; without loss of generality $i < k$. Then, by (1.6.2),

$$(1.10.1) \qquad \begin{aligned} (\beta_{i+1} - \beta_i)(D_i) = S_1 = (\beta_{k+1} - \beta_k)(D_k) \quad &\text{and} \\ (\gamma_{i+1} - \gamma_i)(D_i) = S_2 = (\gamma_{k+1} - \gamma_k)(D_k) \quad &\text{for } D_i, D_k \in A \setminus \{0\}\,. \end{aligned}$$

Hence $D_k = (\gamma_{k+1} - \gamma_k)^{-1}(\gamma_{i+1} - \gamma_i)(D_i)$ and $D_i = (\beta_{i+1} - \beta_i)^{-1}(\beta_{k+1} - \beta_k)(D_k)$ showing that D_k is a fixed element of the mapping dealt with in $(\Diamond\Diamond\Diamond'')$, a contradiction.

Conversely, if α_{ki} has a fixed point $D \neq 0$, then (1.10.1) follows with $D_k := D$ and $D_i := (\beta_{i+1} - \beta_i)^{-1}(\beta_{k+1} - \beta_k)(D)$. For $i, k < n$ there exist codewords $\boldsymbol{a} = a_1 \ldots a_i a_{i+1} \ldots a_{n+2}$ and $\boldsymbol{b} = b_1 \ldots b_k b_{k+1} \ldots b_{n+2}$ such that $a_i - a_{i+1} = D_i$ and $b_{k+1} - b_k = D_k$; neighbour transpositions of these words in position $(i, i+1)$ and $(k, k+1)$ respectively lead to the same syndrom (S_1, S_2). (Remark: One can even choose these $\boldsymbol{a}$ and $\boldsymbol{b}$ such that $\boldsymbol{a} = \boldsymbol{b}$).
$\square$

Summing up our results, we get the following

1.11 Theorem

(i) *Let $(A, +)$ be a finite abelian group with $\beta_i, \gamma_i, \beta_{n+1}, \gamma_{n+2} \in \mathrm{Aut}\ A$ (for $i = 1, \ldots, n$ and $n \geq 2$); furthermore, let $\beta_{n+2}, \gamma_{n+1} \in \mathrm{Aut}\ A \cup \{0\}$ such that $\gamma_{n+2}\beta_{n+2} = \beta_{n+2}\gamma_{n+2}$. The check digit system*

$$(*) \quad A^n \to A^{n+2} \quad \textit{with} \quad a_1 \ldots a_n \mapsto a_1 \ldots a_n a_{n+1} a_{n+2}$$

and check equations

$$(**) \qquad \sum_{i=1}^{n+2} \beta_i(a_i) = 0 = \sum_{i=1}^{n+2} \gamma_i(a_i)$$

is double error detecting and single error and adjacent transposition correcting (SEC-ATC) if the following conditions are fulfilled.

$(\Diamond)$ $\beta_i \gamma_i^{-1} \gamma_j \beta_j^{-1}$ *is fixed point free on A (for all those i, j which satisfy $i < j \leq n+2$ and $\beta_i, \beta_j, \gamma_i, \gamma_j \neq 0$).*

($\Diamond\Diamond$) *$\beta_{i+1}-\beta_i$ and $\gamma_{i+1}-\gamma_i$ are invertable endomorphisms (for $i=1,\dots,n+1$). And $\beta_j\gamma_j^{-1}(\gamma_{i+1}-\gamma_i)(\beta_{i+1}-\beta_i)^{-1}$ operate fixed point freely on A (for $i=1,\dots,n+1$, $j=1,\dots,n$ and, in case $\gamma_{n+1}\neq 0$, for $j=n+1$, in case $\beta_{n+2}\neq 0$, for $j=n+2$).*

($\Diamond\Diamond\Diamond$) *$(\beta_{k+1}-\beta_k)(\gamma_{k+1}-\gamma_k)^{-1}\cdot(\gamma_{i+1}-\gamma_i)(\beta_{i+1}-\beta_i)^{-1}$ operate fixed point freely on A for all i,k with $i<k\leq n+1$.*

(ii) *If a single error or a double error has occured the erroneous word $\boldsymbol{b}'=b_1\dots b_{n+2}$ has a syndrom $(S_1,S_2):=(\sum_{i=1}^{n+2}\beta_i(b_i),\sum_{i=1}^{n+2}\gamma_i(b_i))$ which is different from $(0,0)$.*

(iii) *When a single error or an adjacent transposition has occured this error can be corrected by the syndrom (S_1,S_2) of the erroneous word $\boldsymbol{b}'$ by putting*

(1) $j=n+2$ if $S_1=0$ (and $\beta_{n+2}=0$) or determining

(2) $j\in\{1,\dots,n+2\}$ such that $S_2=\gamma_j\beta_j^{-1}(S_1)$ if $S_1\neq 0$,

(3) $i\in\{1,\dots,n+1\}$ such that $S_2=(\gamma_{i+1}-\gamma_i)(\beta_{i+1}-\beta_i)^{-1}(S_1)$.

Exactly one of these cases is possible under the assumptions.

In cases (1) and (2) a single error is detected and corrected by subtracting the error vector $(0\dots0\ d\ 0\dots0)$ with $d=\gamma_{n+2}^{-1}(S_2)$ or $d=\beta_j^{-1}(S_1)$ in position j respectively from $\boldsymbol{b}'$. Notice that here the syndrom should be $(\beta_j(d),\gamma_j(d))$.

In case (3) an adjacent transposition in position i is detected and correctable by interchanging b_i with b_{i+1}. Notice that here the syndrom should be of the form $((\beta_{i+1}-\beta_i)(D),(\gamma_{i+1}-\gamma_i)(D))$ with $D=b_{i+1}-b_i=a_i-a_{i+1}$.

1.12 Remark

Notice that in case $\gamma_{n+1}\neq 0$, for instance, the conditions of 1.11 can be rewritten in the following form. (In case $\beta_{n+2}\neq 0$ we suppose in addition that β_{n+2} and γ_{n+2} commute; then $\beta_{n+2}^{-1}\beta_{n+1}-\gamma_{n+2}^{-1}\gamma_{n+1}$ is invertable by (1.3 (ii)).)

($\Diamond'$) $(\beta_i^{-1}\beta_j)(\gamma_j^{-1}\gamma_i)$ are fixed point free (for i,j as in ($\Diamond$); see remark (1.3(i)).

($\Diamond\Diamond'$) $\beta_i(\beta_i^{-1}\beta_{i+1}-1)$ and $\gamma_i(\gamma_i^{-1}\gamma_{i+1}-1)$ are invertable and

$$\gamma_j^{-1}\gamma_i(\gamma_i^{-1}\gamma_{i+1}-1)\,(\beta_i^{-1}\beta_{i+1}-1)^{-1}\beta_i^{-1}\beta_j$$

operate fixed point freely (for $i,j=1,\dots,n+1$, and in case $\beta_{n+2}\neq 0$ as well for $j=n+2$, see (1.3 (i)).

($\Diamond\Diamond\Diamond'$) $(\gamma_k^{-1}\gamma_{k+1}-1)^{-1}\gamma_k^{-1}\gamma_i(\gamma_i^{-1}\gamma_{i+1}-1)(\beta_i^{-1}\beta_{i+1}-1)^{-1}\beta_i^{-1}\beta_k(\beta_k^{-1}\beta_{k+1}-1)$ operate fixed point freely on A for $i < k \le n+1$.

Thus, if $\beta_1, \dots, \beta_{n+2}$ and $\gamma_1, \dots, \gamma_{n+2}$ fulfill the above conditions, one can consider $\beta\,\beta_1, \dots, \beta\,\beta_{n+2}$ for a fixed $\beta \in \mathrm{Aut}A$ instead of $\beta_1, \dots, \beta_{n+2}$ and $\gamma\gamma_j$ instead of γ_j for a fixed γ as long as $\beta\,\beta_{n+2}$ and $\gamma\,\gamma_{n+2}$ commute (which is the case when β commutes with γ_{n+2} and γ centralizes β and β_{n+2}).

2. Systems using powers of one or two automorphisms

In this section we investigate system $(*)$ from 1.1 with the following special choice of β_i and γ_j which generalizes the methods of [SRK], p.74.

2.1 Special choices of automorphisms

Let the automorphisms of the check digit system $(*)$ with check equations $(**)$ be chosen as $\beta_i := \beta^{i+b}$ and $\gamma_j := \gamma^{j+d}$ $(i = 1, \dots, n+1,\ j = 1, \dots, n, n+2)$ for fixed elements $\beta, \gamma \in \mathrm{Aut}\,A$. With the observations of 1.12 we put $b = -1 = d$ (– to have one exponentiation less –) and choose

$$(2.1.1)\qquad \beta, \gamma \in \mathrm{Aut}\,A \quad \textit{and} \quad \beta_i := \beta^{i-1} \quad (i = 1, \dots, n+1),\ \beta_{n+2} \in \{0, \beta^{n+1}\},$$
$$\textit{furthermore} \quad \gamma_j := \gamma^{j-1} \quad (j = 1, \dots, n, n+2) \ \textit{and} \ \gamma_{n+1} \in \{0, \gamma^n\}\,.$$

In addition, to guarantee the solvability conditions of (1.1), we ask β and γ to commute.

Special case 1

First we specialize by choosing $\gamma = \beta^2$ for a fixed $\beta \in \mathrm{Aut}\,A$; furthermore we put $\beta_{n+2} := 0$ and $\gamma_{n+1} \neq 0$. (These are only a few cases out of many.)

2.2 Corollary 1

The check digit system $A^n \to A^{n+2}$ with $n \ge 2$ and check equations

$$(\bigtriangledown)\qquad \sum_{i=1}^{n+1} \beta^{i-1}(a_i) = 0 = \sum_{i=1}^{n+2} \beta^{2i-2}(a_i) \qquad \textit{with} \quad \beta \in \mathrm{Aut}\,A$$

is double error detecting and single error and adjacent transposition correcting if the following endomorphisms are automorphisms.

(a) $\beta^j - 1 \qquad (j = 2, \dots, n)$

(b) $\beta^{\ell+1}+\beta^{\ell}-1 \quad (\ell=1,\ldots,n-1)$ and $\beta^{m}-\beta-1\ (m=2,\ldots,n)$

(c) $\beta^{j+2}-\beta^{j}+1 \quad (j=1,\ldots,n)$ and $\beta^{k+1}-\beta^{k}+1\ (k=1,\ldots,n)$

Proof: The corollary follows by direct inspection or by 1.11 taking into account that an endomorphism α of A is fixed point free iff $\alpha-1$ is invertable. Furthermore one uses the fact that, being in the finite case, $\beta^2-1=(\beta+1)(\beta-1)$ can only be invertable if the factors are. □

2.3 Special case 2

Now we let $\beta_{n+2}\neq 0\neq\gamma_{n+1}$ and allow $\gamma\neq\beta^2$ as well. Taking $\beta_i=\beta^{i-1}$ and $\gamma_i=\gamma^{i-1}$ for $i=1,\ldots,n+2$ we can apply (1.11) again. Put $\alpha:=\beta\gamma^{-1}$ and $\delta:=\gamma^{-1}$. Then the slightly strenghtened conditions can be written in the following way.

The automorphisms α and δ commute and the following endomorphisms are invertable.

(1') $\alpha^k-1 \quad (k=1,\ldots,n+1)$

(2') $\delta-1,\delta-\alpha$ *and* $(\alpha^k-1)\delta-(\alpha^k-\alpha)$ *for* $k=-n,\ldots,-1,1,\ldots,n+1,\ k\neq 0.$

We consider now the image of a (possibly not regular) endomorphism of A of the form $\varphi=\sum_{k=-n}^{n+1}\sum_{m=0}^{1}c_{km}\,\alpha^k\delta^m$ with $c_{km}\in\{0,1,-1\}$. The image $\varphi(A)$ is, of course, a subgroup of A; since α and δ commute, this subgroup is fixed under α, namely (using the idea of the Lemma of SCHUR):

$$\alpha(\varphi(A))=\alpha(\sum_{k,m}c_{km}\alpha^k\delta^m(A))=\sum_{k,m}c_{km}\alpha^k\delta^m(\alpha(A))=\varphi(A)$$

So, let α be irreducible on A, that is it does not fix a proper subgroup $\neq 0$ of A (hence A is elementary abelian); then $\varphi(A)=A$ or $\varphi(A)=0$. In the first case φ is regular since A is finite, in the second case $\varphi=0$. Applying this to (2.3) we get

2.4 Corollary 2

Let α be an automorphism of the elementary abelian group $(A,+)$ which operates irreducible on A and has order $s\geqslant n+2$. Let δ be an automorphism commuting with α such that

$$\delta\notin\{1,\alpha\}\cup\{\frac{\alpha^k-\alpha}{\alpha^k-1}\,|\,k=-n,\ldots,-1,1,\ldots,n+1\}\,.$$

Then the system with check equations

$$\sum_{i=1}^{n+2}(\alpha\delta^{-1})^{i-1}(a_i)=0=\sum_{i=1}^{n+2}\delta^{-i+1}(a_i)$$

is double error detecting and single error and neighbour transposition correcting.

If one specializes from (2.3) to $\gamma = \beta^2$ one gets the following corollary using

$$(\alpha^k - 1)\alpha^2 - (\alpha^k - \alpha) = \alpha(\alpha - 1)(\alpha^k + \alpha^{k-1} - 1)$$

2.5 Corollary 3

Let $(A, +)$ be a finite abelian group and $\beta \in \operatorname{Aut} A$. The check digit system $A^n \to A^{n+2}$ with check equations

$$(\nabla\nabla) \qquad \sum_{i=1}^{n+2} \beta^{i-1}(a_i) \;=\; 0 \;=\; \sum_{i=1}^{n+2} \beta^{2i-2}(a_i)$$

is double error detecting and single error and adjacent transposition correcting (SEC-ATC) if the following endomorphisms are invertable

(1) $\beta^k - 1 \qquad (k = 1, \ldots, n+1)$

(2) $\beta^{\ell+1} + \beta^{\ell} - 1 \qquad (\ell = 1, \ldots, n)$ *and* $\beta^m - \beta - 1 \quad (m = 2, \ldots, n+1)$.

Though the computation of the check digits is more complicated than in case 1 the conditions on β are sometimes simpler to fulfill.

2.6 Remark

Let A be a finite dimensional vector space over the field $K = GF(q)$, without loss of generality $A = K^s$. Then any linear mapping induces an endomorphism α of the additive group $(A, +)$. Now, α can be represented by an $(s \times s)$-matrix M over K, and invertability of $P(M)$ for a polynomial $P(x) = \sum_{i=0}^{m} c_i x^i$ is equivalent to $\det(P(M)) \neq 0$. So one can construct examples of automorphisms fulfilling the conditions mentioned above quite easily, see the forthcoming paper [Schu$_5$] .

3. Systems using multipication in fields

In this section we consider automorphisms induced by multiplication in fields.

3.1 Corollary 4

Let $(A, +, \cdot)$ be a finite (commutative) integral domain with a subgroup $(G, \cdot)$ of the group of units in A. Choose $u_1, \ldots, u_{n+1}, w_1, \ldots, w_n, w_{n+2} \in G$ and $u_{n+2}, w_{n+1} \in G \cup \{0\}$.

For $v \in G \cup \{0\}$*, define* $\hat{v} : A \to A$ *with* $\hat{v}(x) := v \cdot x$*. Then* $\beta_i := \hat{u}_i$ *and* $\gamma_j := \hat{w}_j$ *are automorphisms of* $(A, +)$ *(for* $i = 1, \dots, n+2$ *except in the case* $i \in \{n+1, n+2\}$ *with* $u_{n+2} = 0$ *or* $w_{n+1} = 0$ *when giving the zero mapping* $\beta_{n+2} = 0$ *and* $\gamma_{n+1} = 0$ *respectively). Now, the check digit system with words* $x_1 \dots x_{n+2}$ *satisfying the check equations*

$$\sum_{i=1}^{n+2} u_i x_i = 0 = \sum_{i=1}^{n+2} w_i x_i$$

is well defined, double error detecting and single error correcting if

(1) $u_i w_j - u_j w_i \in G$ *for* $i < j \leq n+2$*;*

it is single error and adjacent transposition correcting (SEC-ATC) if, in addition, the following conditions hold.

(2) $\Delta u_i := u_{i+1} - u_i \in G$*,* $\Delta w_i := w_{i+1} - w_i \in G$ *(for* $i = 1, \dots, n+1$*) and*
$u_j \Delta w_i - w_j \Delta u_i \in G$ *(for* $i = 1, \dots, n+1$*,* $j = 1, \dots, n+2$*)*

(3) $\Delta u_j (\Delta w_j)^{-1} - \Delta u_i (\Delta w_i)^{-1} \in G$ *(for* $i < j \leq n+1$*).*

Proof: If $u_i, u_j, w_i, w_j \neq 0$ then (1) implies that $u_j^{-1} u_i w_i^{-1} w_j - 1$ is invertable hence $\beta_j^{-1} \beta_i \gamma_i^{-1} \gamma_j$ fixed point free; thus ($\Diamond$) is fulfilled. If w_j^{-1} exists and $u_j \neq 0$, from (2) we have $u_j w_j^{-1} \Delta w_i (\Delta u_i)^{-1} - 1 \in G$ which implies ($\Diamond\Diamond$). Similarly we get ($\Diamond\Diamond\Diamond$) from (3). Theorem 1.11 completes the proof. □

3.2 Remark

Observe that the conditions in 3.1 depend on $G \cup \{0\}$ and the ring operations $\tilde{+}, \tilde{\cdot}$ induced in it only. So, if it is possible to choose $(G \cup \{0\}, \hat{+}, \hat{\cdot})$ as $GF(p) \cong (\mathbb{Z}_p, +, \cdot)$ for a prime p, as for instance in $GF(p^\ell)$ one gets the results of SETHI et alii [SRK] with the only change that now the alphabet A may be bigger than $\mathbb{Z}_p$. But these results can as well be generalized to $GF(p^\ell)$ directly:

3.3 Special case 3

(i) Let A be a finite field and $\alpha \in A \setminus \{0, 1\}$. Put $u_i = \alpha^{bi}$ and $w_i = \alpha^{ci}$ (similar to [SKR] method 2). Applying corollary 4 we get the following

Corollary 5

Let A be a finite field containing $K = GF(q)$ with $q = p^\ell$ as a subfield and α be an element of $GF(q)^*$ of order $h > 1$. The check digit system over A with check equations

$$\sum_{i=1}^{n+2} \alpha^{bi} x_i = 0 = \sum_{i=1}^{n+2} \alpha^{ci} x_i$$

is double error detecting and single error and adjacent transposition correcting (SEC-ATC) *if $b, c \in \{1, \dots, h-1\}$ and*

(1') h is not a divisor of $(c-b)\,k$ for $k = 1, \dots, n+1$

(2') $\alpha^{(c-b)k} \neq \frac{\alpha^c - 1}{\alpha^b - 1}$ for $k = -n, \dots, 0, \dots, n+1$.

Proof: Specialization of corollary 4 to $(G, \cdot) = GF(q)^*$ and u_i, w_i as chosen. □

(ii) *Further specializations:*
Choose b, c as above but with $\gcd(h, c-b) = 1$. Then (1') reduces to the condition $n < h-1$ and $\alpha^{(c-b)k}$ takes distinct values for (mod h)-distinct values of k. If α is a generating element of $GF(q)^*$ and if $n \geq \frac{q-3}{2} = \frac{h}{2} - 1$ then $k = (q-1)-n, \dots, 0, \dots, n+1$ would cover all such values since $(q-1) - n \leq n+2$; thus inequality (2') would not have a solution. To have not too many cases to consider we specialize to

$$(1'') \quad n + 1 < \frac{h}{2}.$$

Subcase 3a)(cf. [SRK])
Let $p \neq 2, h$ even and $n + 2 \leq \frac{h}{2}$. If one finds b, c such that $\gcd(h, c-b) = 1$ and (2") $\alpha^b + \alpha^c = 2$, then $\frac{\alpha^c - 1}{\alpha^b - 1} = -1 = \alpha^{(c-b)h/2} \neq \alpha^{(c-b)k}$ for $k = h-n, \dots, 0, \dots, n+1$ (since $n + 1 < \frac{h}{2} < h - n$ and since $c - b$ is odd) and therefore (2').

Subcase 3b)
Choose $c = sb$ with $\gcd(h, (s-1)b) = 1$ and let $v \in \mathbb{N}$ be such that $n + 1 < v < h - n$; this is possible for $n + 1 < \frac{h}{2}$, take for instance $v = h - n - 1$. Furthermore, choose α such that

$$\alpha^{b(s-1)v} = \sum_{i=0}^{s-1} \alpha^{bi}.$$

Then $\frac{\alpha^c - 1}{\alpha^b - 1} \cdot \alpha^{-(c-b)v} = \sum_{i=0}^{s-1} \alpha^{bi} \cdot \alpha^{-b(s-1)v} = 1$. Therefore $\frac{\alpha^c - 1}{\alpha^b - 1} = \alpha^{b(s-1)v} \neq \alpha^{b(s-1)k}$ for $k \not\equiv v \pmod h$ and hence for all k with $-n \leq k \leq n+1$. Especially, when q is even and α a generating element of $GF(q)^*$, one has $h = q - 1$; choosing $s = 2$, $b = 2$ (hence $c = 4$) and $v = \frac{h+t}{2}$ the condition mentioned above is now $\alpha^t + \alpha^2 + 1 = 0$.

Using the analysis of (3.3), many examples can be constucted, see [Schu$_5$].

References

[**A**$_1$] Abramson, N. M. : *A class of systematic codes for non-independent errors.* IRE Transactions on Information Theory **5** (1959) 150-157.

[**A**$_2$] Abramson, N. M. : *Error-correcting codes from linear sequential circuits.* In: C. Cherry (ed.) Fourth London Sympos. on Info. Theory (Butterworth, London 1961) 26-40.

[**Bec**] Beckley, D. F. : *An optimum system with "modulus 11".* The Computer Bull. (Dec. 1967) 213-215.

[**Bed**] Bedford, D.: *Orthomorphisms and near orthomorphisms of groups and orthogonal Latin squares.* Bulletin of the ICA **15**(1995) 13–33.

[**BJL**] Beth, Th.; D. Jungnickel and H. Lenz: *Design Theory.* (BI–Verlag, Zürich 1985).

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

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

[**FM**] Friedman, W. and C.J. Mendelsohn: *Notes on codewords.* Am. Math. Monthly (1932) 394-409.

[**GM**] Gallian, J. A.and M. D. Mullin: *Groups with anti-symmetric mappings.* Arch. Math. **65** (1995) 273-280.

[**He**] Heiss, St.: *Antisymmetric mappings for finite solvable groups.* Arch. Math. accepted.

[**Hi**] Hill, R. H.: *A first course in coding theory* .(Clarendon Press. Oxford 1986).

[**HP**] Hall, M. and L.J. Paige: *Complete mappings of finite groups.* Pacific J. Math. **5**(1955) 541–549.

[**Hu**] Huppert, B. : *Endliche Gruppen I.* (Springer Verlag, Berlin etc. 1967).

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

[**JV**] Jungnickel, D. and Sc.A. Vanstone: *Graphical codes revisited.* IEEE Transactions on Information Theory. Submitted.

[**L**] Levenshtein, V. I. : *Binary codes capable of correcting deletions, insertions and reversals.* Soviet Physics-Doklady **10**/8 (1966) 707-710.

[LeV] Levitin, L.B. and F.S. Vainstein: *Single–error–correcting codes for magnetic recording.* Lecture, given by L. Levitin at the FU Berlin.

[LNC] Lidl, R.; H. Niederreiter and P.M. Cohn: *Finite fields.* (Addison Wesley. London etc. 1983).

[McWSl] MacWilliams, F.J. and N.J.A. Sloane: *The Theory of Error–Correcting Codes.* (North Holland, Amsterdam 1977).

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

[Schau] Schauffler, R.: *Über die Bildung von Codewörtern.* Arch. Elektr. Übertragung **10**/7(1956) 303-314.

[Schu$_1$] Schulz, R.–H.: *Codierungstheorie.* (Vieweg Verlag, Braunschweig/Wiesbaden 1991).

[Schu$_2$] Schulz, R.–H.: *Check character systems over groups and orthogonal Latin squares.* Applic. Algebra in Eng., Comm. and Computing, AAECC, **7** (1996) 125-132.

[Schu$_3$] Schulz, R.–H.: *Informations– und Codierungstheorie — eine Einführung;* in R.-H. Schulz (ed.): Mathematische Aspekte der angewandten Informatik. (BI–Wissenschaftsverlag, Mannheim etc. 1994).

[Schu$_4$] Schulz, R.–H.: Some check digit systems over non-Abelian groups. Mitt. Math. Ges. Hamb. **12**/3 (1991) 819–827.

[Schu$_5$] Schulz, R.–H.: *Check digit systems with error correction: Examples.* To appear.

[Si] Siemon, H.: *Anwendungen der elementaren Gruppentheorie in Zahlentheorie und Kombinatorik.* (Klett Verlag, Stuttgart 1981).

[SRK] Sethi, A.S.; V. Rajaraman and P.S. Kenjale: *An error–correcting coding scheme for alphanumeric data.* Information Processing Letters **7**/2(1978) 72–77.

[V] Verhoeff, J.: *Error Detecting Decimal Codes.* (Math. Centre Tracts **29**, Math. Centrum Amsterdam 1969).

Ralph-Hardo Schulz
2.Mathematisches Institut
Freie Universität Berlin
Arnimallee 3
D-14195 Berlin (Germany)
e-mail: schulz@math.fu-berlin.de