COMBINATORICA 3 (1) (1983) 21—33

ALGEBRAIC TECHNIQUES FOR NONLINEAR CODES

H. BAUER, B. GANTER and F. HERGERT

Received 3 April 1982

Revised 21 September 1982

We introduce some techniques for nonlinear systematic error-correcting codes over the two-element alphabet. As an application, we construct new perfect 1-error-correcting (15, 11)-codes.

Introduction

The rich theory of error-correcting codes, as presented for example in the book of MacWilliams and Sloane, has its most powerful results for *linear* codes, i.e. codes which are subspaces of (finite) vector spaces. The present paper is devoted to developing an algebraic theory of systematic nonlinear block codes over $\{0, 1\}$. The main tool is the *Jacobian matrix* of a code, which generalizes the parity check matrix of a linear code.

The usefulness of this concept is demonstrated by constructing new perfect codes. The celebrated "perfect code theorem", which classifies the perfect codes over prime power alphabets, leaves the possibility of unknown perfect one-error-correcting codes. We show that indeed there are such codes.

1. The Jacobian of a systematic code

This paper deals with systematic codes and, though some of our results can be generalized, we shall restrict our considerations to codes over the alphabet $\mathbf{F}_2 = \{0, 1\}$.

Two binary codes C and C' are said to be equivalent, if one can be obtained from the other by permuting the coordinates and adding a constant vector, i.e. there is a permutation π and a vector $\underline{a}$ such that $C' = \{(c_{\pi(1)}, \ldots, c_{\pi(n)}) + \underline{a} \mid (c_1, \ldots, c_n) \in C\}$. Therefore there is no loss of generality if in this paper we shall *always* assume that $\underline{0} \in C$ and that the systematic places of the systematic code C are the first k coordinates, or more formally: We define an (n, k)-*code* to be

AMS subject classification 1980: 94 B 60

a set $C \subseteq \mathbf{F}_2^n$ such that for each $\underline{x} := (x_1, \ldots, x_k) \in \{0, 1\}^k$ there is a *unique* element

$$c(\underline{x}) = (x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \in C$$

and $\underline{0} := (0, 0, \ldots, 0) \in C$. Since the entries $x_{k+1}, \ldots, x_n$ are uniquely determined by $x_1, \ldots, x_k$, we can write C in the form

$$C = \{(x_1, \ldots, x_k, f_1(\underline{x}), f_2(\underline{x}), \ldots, f_r(\underline{x})) \mid \underline{x} := (x_1, \ldots, x_k) \in \mathbf{F}_2^k\},$$

where $r := n - k$.

Every mapping $f : \mathbf{F}_2^k \to \mathbf{F}_2$ can be written as a (reduced) polynomial over the two-element field $\mathbf{F}_2$, we thus shall refer to $f_1, \ldots, f_r$ as the *redundancy polynomials* of C in the variables $x_1, \ldots, x_k$. The function $F : \mathbf{F}_2^k \to \mathbf{F}_2^n$, defined by $F(\underline{x}) := (f_1(\underline{x}), \ldots, f_r(\underline{x}))^T$ is called the *redundancy function* of C. As already mentioned, we assume that $F(\underline{0}) = \underline{0}$. Since every $\mathbf{F}_2$-polynomial f in variables $x_1, \ldots, x_k$ formally looks like a (square free) real polynomial, we can form the *formal derivative* f_{x_i} *of* f with respect to the variable x_i, which again can be viewed as an $\mathbf{F}_2$-polynomial.

The *Jacobian* of an (n, k)-code C with redundancy function $F := (f_1, \ldots, f_r)^T$ is defined to be the $r \times k$-matrix ($r := n - k$)

$$\operatorname{jac}(C) := \begin{pmatrix} f_{1x_1}, \ldots, f_{1x_k} \\ \vdots \qquad\quad \vdots \\ f_{rx_1}, \ldots, f_{rx_k} \end{pmatrix} = (F_{x_1} | F_{x_2} | \ldots | F_{x_k}).$$

Since the entries of $\operatorname{jac}(C)$ are polynomials, $\operatorname{jac}(C)$ depends on $x_1, x_2, \ldots, x_k$. We write $\operatorname{jac}(C)[\underline{x}] := (F_{x_1}(\underline{x}) | F_{x_2}(\underline{x}) | \ldots | F_{x_k}(\underline{x}))$. The Jacobian matrix uniquely determines the code C (since we assume $\underline{0} \in C$).

Examples 1. Let C be the (5, 3)-code given here.

x_1	x_2	x_3	f_1	f_2
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	0	0

The redundancy function of this code is

$$F(\underline{x}) = \begin{pmatrix} f_1(x_1, x_2, x_3) \\ f_2(x_1, x_2, x_3) \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + x_3 \\ x_2 + x_3 + x_1 x_2 + x_1 x_3 \end{pmatrix}$$

and the Jacobian is

$$\operatorname{jac}(C) = \begin{pmatrix} 1 & x_3 & x_2 \\ x_2 + x_3 & 1 + x_1 & 1 + x_1 \end{pmatrix}.$$

2. If we have a linear code C with parity check matrix $H = (M | I_r)$, then $\operatorname{jac}(C) = M$.

There is a simple criterion for deciding whether a given matrix can be interpreted as the Jacobian of a code.

1.1. Lemma. *The $r\times k$-matrix $M=(H_1|H_2|\ldots|H_k)$ is the Jacobian of some code, i.e. $M=(F_{x_1}|F_{x_2}|\ldots F_{x_k})$ for some function F, if and only if $H_{ix_i}=0$ and $H_{ix_j}=H_{jx_i}$ for all $1\leqq i,j\leqq k$.*

1.2. Proposition. *Let f be an $\mathbf{F}_2$-polynomial in the variables $x_1, x_2, \ldots, x_k$. Then*

$$f(x_1,\ldots,x_i+1,\ldots,x_k)=f(x_1,\ldots,x_i,\ldots,x_k)+f_{x_i}(x_1,\ldots,c_i,\ldots,x_k).$$

Proof (for $i=1$). f is of the form $f(x_1,\ldots,x_k)=x_1g(x_2,\ldots,x_k)+h(x_2,\ldots,x_k)$, and thus $f_{x_1}(x_1,\ldots,x_k)=g(x_2,\ldots,x_k)$. Then $f(x_1+1,x_2,\ldots,x_k)=(x_1+1)g(x_2,\ldots,x_k)+h(x_2,\ldots,x_k)=f(x_1,\ldots,x_k)+f_{x_1}(x_1,\ldots,x_k)$.

In view of proposition 1.2 we can now see how to interpret the Jacobian of a code: The value of the i-th column of jac (C) at the point $\underline{x}=(x_1,x_2,\ldots,x_k)\in\mathbf{F}_2^k$ gives the change of the redundancy function F, if we move from codeword $c(x_1,\ldots,x_i,\ldots,x_k)$ to $c(x_1,\ldots,x_i+1,\ldots,x_k)$. If C is a linear code, then the columns of jac (C) are all constant. If we allow the columns to vary, but with the restriction that the columns of jac $(C)[\underline{x}]$ are only permuted, we get a class of nonlinear codes, which is closely related to linear codes. To every (n,k)-code C we can associate a linear code C_0 by jac $(C_0):=$jac $(C)[\underline{0}]$. The redundancy function of C_0 is denoted by F_0.

1.3. Lemma. *Let C be an (n,k)-code and suppose for every $\underline{x}\in\mathbf{F}_2^k$ the matrix* jac $(C)[\underline{x}]$ *equals* jac (C_0) *up to some permutation of the columns (depending on $\underline{x}$). Then there is a weight preserving bijection $\Phi:\mathbf{F}_2^k\to\mathbf{F}_2^k$ such that $F(\Phi(\underline{x}))=F_0(\underline{x})$ for all $\underline{x}\in\mathbf{F}_2^k$. Moreover C is distance invariant and has the same weight distribution as C_0.*

For a proof see [3].

In section 3 we shall give several examples of such codes.

To generalize Proposition 1.2 we introduce the following notation: Let $\mathbf{N}_k:=\{1,2,\ldots,k\}$, and for a set $M\subseteqq\mathbf{N}_k$ let $\underline{\varepsilon}_M$ be the characteristic vector of M, i.e. $\underline{\varepsilon}_M:=(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_k)\in\mathbf{F}_2^k$, where

$$\varepsilon_i:=\begin{cases}0 & \text{if } i\notin M\\ 1 & \text{if } i\in M.\end{cases}$$

Let $F:\mathbf{F}_2^k\to\mathbf{F}_2^r$ be a mapping, and let $M\subseteqq\mathbf{N}_k$. F^M is defined inductively by

$$F^{\emptyset}:=0 \quad\text{and}\quad F^{N\dot\cup\{i\}}:=F^N+(F+F^N)_{x_i}.$$

For example we find that

$$F^{\{1,2,3\}}=F_{x_1}+F_{x_2}+F_{x_3}+F_{x_1x_2}+F_{x_1x_3}+F_{x_2x_3}+F_{x_1x_2x_3}.$$

1.4. Lemma. *Let f be an $\mathbf{F}_2$-polynomial in the variables $x_1,\ldots,x_k$. For every $M\subseteqq\{1,2,\ldots,k\}$*

$$f(\underline{x}+\underline{\varepsilon}_M)=f(\underline{x})+f^M(\underline{x}).$$

The proof is a simple inductive application of 1.2.

If C is an (n, k)-code with redundancy function F then, by 1.4, $c(\underline{x}) + c(\underline{x}+\underline{\varepsilon}_M) = (\underline{\varepsilon}_M | F^M(\underline{x}))$, in other words, we have:

1.5. Corollary. *Let C be an (n, k)-code with redundancy function F. For every set $M \subseteq \mathbf{N}_k$ the codewords $c(\underline{x})$ and $c(\underline{x}+\underline{\varepsilon}_M)$ satisfy*

$$\operatorname{dist}(c(\underline{x}), c(\underline{x}+\underline{\varepsilon}_M)) = |M| + \operatorname{wt}(F^M(\underline{x})).$$

(Here dist *denotes the (Hamming) distance and* wt *the (Hamming) weight of binary tuples.)*

For a function $F : \mathbf{F}_2^k \to \mathbf{F}_2^r$ we define $\operatorname{wt}(F) := \min\{\operatorname{wt}(F(\underline{x})) | \underline{x} \in \mathbf{F}_2^k\}$.

1.6. Theorem. *Let C be an (n, k)-code with redundancy function F. C has minimum distance at least d $(d(C) \geqq d)$ if and only if*

$$\operatorname{wt}(F^M) \geqq d - |M|$$

for every nonempty subset $M \subseteq \{1, 2, \ldots, k\}$.

Proof. $d(C) = \min\{\operatorname{dist}(c(\underline{x}), c(\underline{x}+\underline{\varepsilon}_M)) | \underline{x} \in \mathbf{F}_2^k,\ \emptyset \neq M \subseteq \mathbf{N}_k\}$

$= \min\{|M| + \operatorname{wt}(F^M) | \emptyset \neq M \subseteq \mathbf{N}_k\}$.

2. Systematic codes as unions of cosets

Let C be an (n, k)-code and let $T_C \subseteq C$ be the set of all codewords with respect to which the code C is translation invariant, i.e.

$$T_C := \{\underline{c} \in C | \underline{c} + C = C\}.$$

Clearly T_C is a subvectorspace of $\mathbf{F}_2^n$. If C is linear, then of course $T_C = C$, the other extreme would be $T_C = \{\underline{0}\}$. We call T_C the *linear kernel* of C, as is motivated by the next proposition:

2.1. Proposition. *C is a union of cosets of T_C, and T_C is the maximal subspace of $\mathbf{F}_2^n$ with this property.*

Proof. By definition $\underline{a} \in \underline{a} + T_C \subseteq C$ for every $\underline{a} \in C$, thus $C = \bigcup_{\underline{a} \in C} \underline{a} + T_C$. On the other hand, if $C = \bigcup_{\underline{a} \in C} \underline{a} + U$ for some subspace U, then for every $\underline{u} \in U$ we have $C + \underline{u} = \bigcup_{\underline{a} \in C} \underline{a} + U + \underline{u} = \bigcup_{\underline{a} \in C} \underline{a} + U = C$, i.e. $U \subseteq T_C$. ∎

For nonlinear (n, k)-code C we define the *rank* of C as $\operatorname{rank} C := k - \dim T_C$. In other words: A nonlinear code has rank $\leqq m$, if and only if it is the union of 2^m cosets of some subspace. According to this definition, a linear code should have rank $= 0$. But since rank $C = 1$ can not occur (a binary code with rank $= 1$ is already linear) it is convenient to define rank $C = 1$, if C is linear. Equivalent codes clearly have equal rank. The degree of the redundancy function of a code

C gives us a lower bound on rank C. We define the *degree* of a polynomial f over $\mathbf{F}_2$ as the largest number s of variables in a product $x_{i_1} \dots x_{i_s}$ occuring in f.

2.2. Theorem. *The degree of an (n, k)-code C with redundancy function $F = (f_1, f_2, \dots, f_r)^T$, defined by*

$$\deg C = \max \{\text{degree } f_i | 1 \leqq i \leqq r\}$$

satisfies

$$\deg C \leqq \text{rank } C.$$

Proof. In case C is linear, the theorem is true by definition. Since T_C is a subspace of $\mathbf{F}_2^n$ and also a subset of an (n, k)-code, T_C is systematic with respect to some $j := \dim T_C$ of the first k entries. W.l.o.g. we assume, that T_C is systematic in the first j entries: T_C is an (n, j)-code with the *linear* redundancy function, say, $T := (t_{j+1}, \dots, t_k, g_1, \dots, g_r)^T$. Therefore, in every coset of T_C in C there is a unique codeword of C with j initial zeroes, we call this set of codewords N_C. If we omit the first j coordinates we get

$$N_C^* := \{(x_{j+1}, \dots, x_n) | (0, 0, \dots, 0, x_{j+1}, \dots, x_n) \in C\}.$$

Clearly N_C^* is an $(n-j, k-j)$-code with redundancy function, say, $N := (h_1, \dots, h_r)^T$ (observe that $\text{rank } N_C^* = k-j$). Now every codeword in C has a unique representation as the sum of a vector from T_C and N_C:

$$\begin{array}{l} (x_1, x_2, \dots, x_j, t_{j+1}(\underline{y}), \dots, t_k(\underline{y}), g_1(\underline{y}), \dots, g_r(\underline{y})) \in T_C \\ +(\ 0,\ 0,\ \dots,\ 0,\quad z_{j+1}, \dots,\quad z_k, h_1(\underline{z}), \dots, h_r(\underline{z})) \in N_C \\ \hline (x_1, x_2, \dots, x_j,\quad x_{j+1}, \dots,\quad x_k, f_1(\underline{x}), \dots, f_r(\underline{x})) \in C \end{array}$$

where $\underline{y} := (x_1, x_2, \dots, x_j)$; $x_{j+i} = t_{j+i}(\underline{y}) + x_{j+i}$, $1 \leqq i \leqq k-j$; $\underline{z} := (z_{j+1}, \dots, z_k)$. Now the redundancy function $F = (f_1, \dots, f_r)^T$ can easily be retained from T and N:

$$f_i(x_1, x_2, \dots, x_k) = h_i(z_{j+1}, \dots, z_k) + g_i(x_1, x_2, \dots, x_j) =$$

$$= h_i(t_{j+1}(x_1, x_2, \dots, x_j) + x_{j+1}, \dots, t_k(x_1, x_2, \dots, x_j) + x_k) + g_i(x_1, x_2, \dots, x_i).$$

Since the functions t_i, g_i are linear, we have

$$\text{degree } f_i \leqq \text{degree } h_i \leqq \deg N_C^* \leqq k-j = \text{rank } C. \quad \blacksquare$$

Note that the degree (and also the numbers of nonlinear redundancy polynomials) is not invariant under equivalence of codes.

Another estimation of the degree can be given in terms of the *dual distance* of C. For this we need the following proposition which is immediate from Theorem 13.1 in [5]:

2.3. Proposition. *Let $f(x_1, \dots, x_k)$ be an $\mathbf{F}_2$-polynomial. The monomial $x_1 x_2 \dots x_j$ is a summand of f if and only if*

$$\sum_{b_1, \dots, b_j \in \mathbf{F}_2} f(b_1, \dots, b_j, 0, \dots, 0) = 1.$$

2.4. Corollary. *Let C be an (n, k)-code with redundancy function $F=(f_1, \ldots, f_r)^T$ and let $M \subseteq \mathbf{N}_k$. The monomial $\prod_{j \in M} x_j$ is a summand of $f_i(x_1, \ldots, x_k)$ if and only if the number of codewords $c(x_1, \ldots, x_k)$ with $x_j=0$ for all $j \notin M$ and $f_i(x_1, \ldots, x_k)=1$ is odd.*

Theorem 5.8 of [5] states that the *dual distance* d' of an (n, k)-code C is the largest number with the property that for any set $N=\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, n\}$ with $|N|=s<d'$ and any s-tuple $(\varepsilon_1, \ldots, \varepsilon_s) \in \mathbf{F}_2^s$ the number of codewords $(x_1, \ldots, x_n) \in C$ with $x_{i_j}=\varepsilon_j$, $j=1, \ldots, s$, is exactly 2^{k-s}. We use this to prove:

2.5. Theorem. *If C is an (n, k)-code with dual distance $d' \leqq k$ then*

$$\deg C \leqq k+1-d'.$$

Proof. Let f_i be one of the redundancy polynomials and let $M \subseteq \mathbf{N}_k$ be any set with $|M|>k+1-d'$. We prove that the monomial $\prod_{j \in M} x_j$ is not a summand of f_i. Let $N:=(\{1, \ldots, k\} \setminus M) \cup \{k+i\}$. Then $s:=|N|=k-|M|+1<d'$, let $\{i_1, \ldots, i_s\}:=N$, $i_s=k+i$. The number of codewords $(x_1, \ldots, x_n)$ with $(x_{i_1}, \ldots, x_{i_s})=(0, 0, \ldots, 0, 1)$ is 2^{k-s}, which is even since $s<k$. Now the theorem follows from Corollary 2.4. ∎

If $d'=k+1$, which is the maximum d' can attain, C is an MDS code (cf. chapter 11 [5]). So the MDS codes are excluded in this theorem, which is not much loss of generality, since all binary MDS codes are trivial. We return to the theme of this paragraph and develop a method for computing the rank of a code. Unfortunately, the method is successful only in the case that $\deg C=2$.

2.6. Proposition. *Let C be an (n, k)-code with redundancy function F, and let $c(\underline{\varepsilon}_M)=c(\varepsilon_1, \ldots, \varepsilon_k) \in C$ be a codeword. The Jacobian of the translated code $C+c(\underline{\varepsilon}_M)$ is*

$$\operatorname{jac}(C+c(\underline{\varepsilon}_M)) = (F_{x_1}+F^M_{x_1} | F_{x_2}+F^M_{x_2} | \ldots | F_{x_k}+F^M_{x_k}).$$

Proof. Let $\hat{F}$ be the redundancy function of $C+c(\underline{\varepsilon}_M)$. Then $\hat{F}(\underline{x}+\underline{\varepsilon}_M)=F(\underline{x})+F(\underline{\varepsilon}_M)$, i.e. $\hat{F}(\underline{x})=F(\underline{x}+\underline{\varepsilon}_M)+F(\underline{\varepsilon}_M) \overset{1.4}{=} F(\underline{x})+F^M(\underline{x})+F(\underline{\varepsilon}_M)$. Since $F(\underline{\varepsilon}_M)$ is constant, $\hat{F}_{x_i}=F_{x_i}+F^M_{x_i}$. ∎

2.7. Corollary. *Let C be an (n, k)-code with redundancy function F. The following are equivalent:*

1) $C=C+c(\underline{\varepsilon}_M)$, *i.e.* $c(\underline{\varepsilon}_M) \in T_C$.
2) $F^M \equiv F(\underline{\varepsilon}_M)$.
3) F^M *is a constant function.*
4) $F^M_{x_i} \equiv 0$ *for* $i=1, \ldots, k$.

If $\deg C=2$, all third derivatives vanish and $F^M_{x_i}=\sum_{j \in M} F_{x_j x_i}=(\sum_{j \in M} F_{x_j})_{x_i}$ is always constant.

2.8. Corollary. *Let C be an (n, k)-code with $\deg C=2$. Then $C=C+c(\underline{\varepsilon}_M)$ if and only if $\sum_{j \in M} F_{x_j}$ is a constant function.*

Example. The (11, 4)-code whose Jacobian matrix is shown here (this is a shortened Nadler-code, cf. [5]) is translation invariant with respect to $c(1, 1, 1, 1)$.

$$\begin{array}{|cccc|}
\hline
1 & 1+C+D & 1+B+D & 1+B+C \\
1+B+C & 1+A+D & A+D & B+C \\
B+D & A+D & 1 & 1+A+B \\
1+C+D & C+D & 1+A+B & A+B \\
B+C & 1+A+C & A+B & 1 \\
1+B+D & A+C & B+D & 1+A+C \\
C+D & 1 & 1+A+D & A+C \\
\hline
F_A & F_B & F_C & F_D
\end{array}$$

To demonstrate how Corollary 2.8 can be applied to determine the rank of a code of degree 2, we introduce the *homogeneous Jacobian* matrix $\mathrm{jac}_H(C)$, which is obtained from $\mathrm{jac}(C)$ by deleting the constants, i.e.

$$\mathrm{jac}_H(C) := \mathrm{jac}(C) + \mathrm{jac}(C)[\underline{0}].$$

The columns are $\tilde{F}_{x_i} := F_{x_i} + F_{x_i}(\underline{0})$. Via Corollary 2.8 we have $c(\underline{\varepsilon}_M) \in T_C$ if and only if $\sum_{i \in M} \tilde{F}_{x_i} = \underline{0}$. If we interpret the variables in $\mathrm{jac}_H(C)$ as linearly independent elements of some $\mathbf{F}_2$-vectorspace, then $\sum_{i \in M} \tilde{F}_{x_i} = \underline{0}$ tells us that the columns $\{\tilde{F}_{x_i} | i \in M\}$ are linearly dependent. So, defining the *column-rank* $\mathrm{c\,rank}(\mathrm{jac}_H(C))$ as the dimension of the vectorspace generated by the columns of $\mathrm{jac}_H(C)$, we get

2.9. Theorem. *Let C be an (n, k)-code with* $\deg(C) = 2$. *Then*

1) $\mathrm{rank}(C) = \mathrm{c\,rank}(\mathrm{jac}_H(C))$.
2) $T_C = \{c(x_1, \ldots, x_k) | \underline{x} := (x_1, \ldots, x_k) \in F_2^k, (\mathrm{jac}_H(C)) \cdot \underline{x}^T = \underline{0}\}$.

2.10. Example. From the (16, 8)-Nordstrom-Robinson-code one can obtain a (14, 7)-code with the following homogeneous Jacobian:

$$\tilde{J} = \begin{array}{|cccc|}
\hline
0 & C+D+E+G & B+E+F+G & B+E+F+G \\
C+D+E+G & 0 & A+D+E+F & A+C+F+G \\
B+E+F+G & A+D+E+F & 0 & B+E+F+G \\
B+E+F+G & A+C+F+G & B+E+F+G & 0 \\
B+C+D+F & A+C+F+G & A+B+D+G & A+C+F+G \\
C+D+E+G & C+D+E+G & A+B+D+G & A+B+C+E \\
B+C+D+F & A+D+E+F & A+D+E+F & A+B+C+E \\
\hline
\end{array}$$

$$\begin{array}{|ccc|}
\hline
B+C+D+F & C+D+E+G & B+C+D+F \\
A+C+F+G & C+D+E+G & A+D+E+F \\
A+B+D+G & A+B+D+G & A+D+E+F \\
A+C+F+G & A+B+C+E & A+B+C+E \\
0 & A+B+D+G & B+C+D+F \\
A+B+D+G & 0 & A+B+C+E \\
B+C+D+F & A+B+C+E & 0 \\
\hline
\end{array}$$

The column rank of $\tilde{J}$ is 3, the column space is generated by $\tilde{F}_A, \tilde{F}_B, \tilde{F}_C$. Thus the dimension of the linear kernel is 4. The following codewords form a basis for for T_C: $c(1, 0, 1, 1, 0, 0, 0)$, $c(1, 1, 1, 0, 1, 0, 0,)$, $c(1, 1, 0, 0, 0, 1, 0)$ and $c(0, 1, 1, 0, 0, 1)$.

3. Applications to 1-error-correcting perfect codes

Part of the well-known perfect code theorem is that any nontrivial perfect binary code except the Golay code has to have the parameters of a Hamming code. There are non-linear perfect codes with these parameters, known as the Vasil'ev-codes. In this paragraph we give a simple representation of the Vasil'ev-codes and construct some new perfect (15, 11)-codes.

3.1. Theorem. *Let C be an (n, k)-code. C is 1-error-correcting $(d(C) \geqq 3)$ if and only if for every $\underline{x} \in \mathbf{F}_2^k$ the columns of* jac $(C)[\underline{x}]$ *are all distinct and of weight $\geqq 2$.*

Proof. By 1.6, C is one-error-correcting if and only if

1) $\text{wt}(F_{x_i}) \geqq 2$ for $i = 1, \ldots, k$, and
2) $\text{wt}(F_{x_i} + F_{x_j} + F_{x_i x_j}) = \text{wt}(F^{(i,j)}) \geqq 1$ for $1 \leqq i < j \leqq k$.

Condition 1) is satisfied if and only if the columns of jac $(C)[\underline{x}]$ all have weight $\geqq 2$ for each $\underline{x}$.

Now suppose that for some $i \neq j$ and some $\underline{u} \in \mathbf{F}_2^k$ we find $F_{x_i}(\underline{u}) = F_{x_j}(\underline{u})$, say $i = 1, j = 2$. Then the codewords $\underline{c}_1 := c(u_1 + 1, u_2, u_3, \ldots, u_k) = (u_1 + 1, u_2, \ldots, u_k | F(\underline{u}) + F_{x_1}(\underline{u}))$ and $\underline{c}_2 := c(u_1, u_2 + 1, u_3, \ldots, u_k) = (u_1, u_2 + 1, \ldots, u_k | F(\underline{u}) + F_{x_2}(\underline{u}))$ would have distance 2, a contradiction.

If, on the other hand, all columns of jac $(C)[\underline{x}]$ are distinct, then condition 2) is satisfied too. Suppose there were x_i, x_j (say x_1, x_2) such that

$$\text{wt}(F_{x_1}(\underline{u}) + F_{x_2}(\underline{u}) + F_{x_1 x_2}(\underline{u})) = 0 \quad \text{for some} \quad \underline{u} \in \mathbf{F}_2^k.$$

Consider the codewords $c(\underline{y}), c(\underline{z})$, where $\underline{y} := (u_1 + 1, u_2, u_3, \ldots, u_k)$, $\underline{z} := (u_1 + 1, u_2 + 1, u_3, \ldots, u_k)$.

From $F^{(1,2)}(\underline{u}) = 0$ we obtain, using 1.4, that $F(\underline{z}) = F(\underline{u}) + F^{(1,2)}(\underline{u}) = F(\underline{u})$ and thus $F(\underline{y}) + F_{x_1}(\underline{y}) = F(\underline{u}) = F(\underline{z}) = F(\underline{y}) + F_{x_2}(\underline{y})$, which implies $F_{x_1}(\underline{y}) = F_{x_2}(\underline{y})$, a contradiction. ∎

3.2. Corollary. *A (binary) (n, k)-code with $n = 2^r - 1$, $k = 2^r - 1 - r$ is 1-error-correcting and perfect if and only if for every $\underline{x} \in \mathbf{F}_2^k$ the columns of* jac $(C)[\underline{x}]$ *run through all r-tuples of weight $\geqq 2$.*

In other words, a perfect 1-error-correcting code is "locally Hamming", i.e. satisfies the condition of Lemma 1.3, where C_0 is the Hamming code. From this lemma we obtain the following well known result:

3.3. Corollary. *A binary 1-error-correcting perfect code is distance invariant and has the same weight distribution as the corresponding Hamming code.*

Since the dual distance of a Hamming code of length $n=2^r-1$ is just the minimal distance of the corresponding simplex code, i.e. $d'=2^{r-1}$, we can also apply 2.5 and obtain

3.4. Corollary. *Every 1-error-correcting perfect $(2^r-1, 2^r-1-r)$-code C satisfies*

$$\deg C \leqq 2^{r-1}-r.$$

In particular we obtain that a 1-error-correcting (7, 4)-code must be linear (remember $\underline{0}\in C$) and that a 1-error-correcting (15, 11)-code has degree $\leqq 4$.

It is rather easy to give examples of Jacobian matrices satisfying the conditions of 3.2. The next theorem gives a first construction (Vasil'ev's construction).

3.5. Theorem. *Let C be a 1-error-correcting perfect (n, k)-code, and let* $\operatorname{jac}(C)$, *the Jacobian of C, be written in variables $\underline{v}=(v_1, \ldots, v_k)$. Let $g(v_1, \ldots, v_k)$ be an arbitrary function $g: \mathbf{F}_2^k \to \mathbf{F}_2$ with $g(\underline{0})=0$. With the substitution $\underline{v}=\underline{x}+\underline{z}$, the matrix*

$$J(x_1, \ldots, x_k, y_1, \ldots, y_r, z_1, \ldots, z_k) := \left[\begin{array}{c|c|c} \dfrac{\operatorname{jac}(C)[\underline{x}+\underline{z}]}{\underline{1}+\lambda(\underline{x}+\underline{z})} & I_r & \dfrac{\operatorname{jac}(C)[\underline{x}+\underline{z}]}{\lambda(\underline{x}+\underline{z})} \\ & 11\ldots1 & \end{array}\right]$$

where $r=n-k$ and $\lambda=(g_{x_1}, g_{x_2}, \ldots, g_{x_k})=(g_{z_1}, g_{z_2}, \ldots, g_{z_k})$, is a Jacobian matrix defining a perfect 1-error-correcting code.

Proof. Lemma 1.1 tells us, that this matrix is indeed a Jacobian and it is quite obvious that this matrix satisfies the conditions of 3.2. ∎

The nonlinear codes obtained by 3.5 are exactly the systematic Vasil'ev codes. We will sketch the proof here: The Vasil'ev codes are defined as follows (cf. [5]): Let C_r be a perfect 1-error-correcting code of length $n=2^r-1$, $g: C_r \to \mathbf{F}_2$ a mapping with $g(\underline{0})=0$ strictly nonlinear, i.e. there exist $\underline{c}, \underline{c}' \in C_r$ such that $g(\underline{c}+\underline{c}') \neq g(\underline{c})+g(\underline{c}')$. Set $\pi(\underline{u})=0$ or 1 depending on whether $\operatorname{wt}(u)$ is even or odd, $\pi(\underline{u}) := \sum_{i=1}^{n} u_i$. Then

$$\mathscr{V} = \left\{(\underline{u}|\underline{u}+\underline{v}|\pi(\underline{u})+g(\underline{v}))\in \mathbf{F}_2^{2^r+1-1} \mid \underline{u}\in \mathbf{F}_2^{2^r-1}, \underline{v}\in C_r\right\}$$

is a perfect 1-error-correcting nonlinear code. If C_r is systematic, then w.l.o.g. we may assume that it is systematic in the first $k=2^r-r-1$ places, $\mathscr{V}$ then is systematic in the first $k+n$ places.

Let us denote the redundancy polynomials of C_r by $p_1, p_2, \ldots, p_r$. Furthermore $g: C_r \to \mathbf{F}_2$ can be interpreted as a mapping depending only on the first k entries $v_1, v_2, \ldots, v_k$ (the systematic places) of C_r. So a codeword $\underline{c}\in\mathscr{V}$ looks like:

$$\underline{c} = u_1, \ldots, u_k, u_{k+1}, \ldots, u_n, u_1+v_1, \ldots, u_k+v_k, u_{k+1}+p_1(v_1, \ldots, v_k), \ldots,$$

$$\ldots, u_n+p_r(v_1, \ldots, v_k), \sum_{i=1}^{n} u_i + g(v_1, \ldots, v_k)$$

$$= x_1, \ldots, x_k, y_1, \ldots, y_r, z_1, \ldots, z_k, f_1(\underline{x}, \underline{y}, \underline{z}), \ldots, f_r(\underline{x}, \underline{y}, \underline{z}), f_{r+1}(\underline{x}, \underline{y}, \underline{z}).$$

If we rename the variables as it is indicated above and substitute v_i by

x_i+z_i, then we find for the redundancy function $F=(f_1, f_2, \ldots, f_{r+1})^T$ of $\mathscr{V}$:

$$f_i(\underline{x}, \underline{y}, \underline{z}) = u_{k+i}+p_i(v_1, \ldots, v_k) = y_i+p_i(x_1+z_1, \ldots, x_k+z_k) \quad \text{for} \quad 1 \leqq i \leqq r$$

$$f_{r+1}(\underline{x}, \underline{y}, \underline{z}) = \sum_{i=1}^{n} u_i+g(v_1, \ldots, v_k) = \sum_{i=1}^{k} x_i+\sum_{i=1}^{r} y_i+g(x_1+z_1, \ldots, x_k+z_k)$$

and we get exactly the construction in 3.5.

Example. We construct a (15, 11)-Vasil'ev code from a (7,4)-Hamming code with Jacobian matrix $\begin{pmatrix}1&1&0&1\\1&0&1&1\\0&1&1&1\end{pmatrix}$ and from the nonlinear function $g(v_1, v_2, v_3, v_4) := v_1 \cdot v_2 \cdot v_3+v_3 \cdot v_4$. We obtain the (transposed) Jacobian:

	f_1	f_2	f_3	f_4
F_{x_1}	1	1	0	$1+(x_2+z_2) \cdot (x_3+z_3)$
F_{x_2}	1	0	1	$1+(x_1+z_1) \cdot (x_3+z_3)$
F_{x_3}	0	1	1	$1+x_4+z_4+(x_1+z_1) \cdot (x_2+z_2)$
F_{x_4}	1	1	1	$1+x_3+z_3$
F_{y_1}	1	0	0	1
F_{y_2}	0	1	0	1
F_{y_3}	0	0	1	1
F_{z_1}	1	1	0	$(x_2+z_2) \cdot (x_3+z_3)$
F_{z_2}	1	0	1	$(x_1+z_1) \cdot (x_3+z_3)$
F_{z_3}	0	1	1	$x_4+z_4+(x_1+z_1) \cdot (x_2+z_2)$
F_{z_4}	1	1	1	x_3+z_3

3.6. Lemma. *A Vasil'ev code $\mathscr{V}$ of length* 15 *has rank* $\leqq 4$.

Proof. Since the only perfect code of length 7 is the *linear* Hamming code, Vasil'ev's construction yields a code with exactly one nonlinear redundancy function, namely f_4. Since f_4 is linear in y_1, y_2, y_3 the codewords $c(\varepsilon_{\{5\}})$, $c(\varepsilon_{\{6\}})$, $c(\varepsilon_{\{7\}})$ are in $T_{\mathscr{V}}$. Use 2.7.4 to find that the four vectors $c(\varepsilon_{\{i,7+i\}})$, corresponding to the pair of variables x_i, z_i $1 \leqq i \leqq 4$, are in $T_{\mathscr{V}}$. Since these 7 vectors are linearly independent, we have rank $\mathscr{V} = 11-\dim T_{\mathscr{V}} \leqq 11-7=4$. ∎

Corollary 3.2 can be used to construct other perfect codes. We give some examples:

3.7. Examples. a) Let $\mathscr{NV}_1$ be the (15, 11)-code with the redundancy function $F := (f_1, f_2, f_3, f_4)^T$ given by

$$f_1 = E+F+G+H+I+J+K$$
$$f_2 = B+C+D+H+I+J+K$$
$$f_3 = A+B+D+E+G+I+K+(H+I) \cdot (J+K)$$
$$f_4 = A+C+D+F+G+J+K+(E+G) \cdot (H+I+J+K).$$

The transposed Jacobian of $\mathcal{NH}_1$ is

	f_1	f_2	f_3	f_4
F_A	0	0	1	1
F_B	0	1	1	0
F_C	0	1	0	1
F_D	0	1	1	1
F_E	1	0	1	$H+I+J+K$
F_F	1	0	0	1
F_G	1	0	1	$1+H+I+J+K$
F_H	1	1	$J+K$	$E+G$
F_I	1	1	$1+J+K$	$E+G$
F_J	1	1	$H+I$	$1+E+G$
F_K	1	1	$1+H+I$	$1+E+G$

b) Let $\mathcal{NH}_2$ be the (15, 11)-code with the redundancy function $F:=(f_1, f_2, f_3, f_4)^T$ given by

$$f_1 = E+F+G+H+I+J+K+(C+F)\cdot(B+D+E+G)$$

$$f_2 = B+C+D+H+I+J+K+(C+F)\cdot(B+D+E+G)$$

$$f_3 = A+B+D+E+G+I+K+(J+K)\cdot(H+I)$$

$$f_4 = A+C+D+F+G+J+K+(B+D+E+G)\cdot(H+I+J+K)$$

The transposed Jacobian of $\mathcal{NH}_2$ is

	f_1	f_2	f_3	f_4
F_A	0	0	1	1
F_B	$C+F$	$1+C+F$	1	$H+I+J+K$
F_C	$B+D+E+G$	$1+B+D+E+G$	0	1
F_D	$C+F$	$1+C+F$	1	$1+H+I+J+K$
F_E	$1+C+F$	$C+F$	1	$H+I+J+K$
F_F	$1+B+D+E+G$	$B+D+E+G$	0	1
F_G	$1+C+F$	$C+F$	1	$1+H+I+J+K$
F_H	1	1	$J+K$	$B+D+E+G$
F_I	1	1	$1+J+K$	$B+D+E+G$
F_J	1	1	$H+I$	$1+B+D+E+G$
F_K	1	1	$1+H+I$	$1+B+D+E+G$

c) Let $\mathcal{NV}_3$ be the (15, 11)-code with the redundancy function $F:=(f_1, f_2, f_3, f_4)^T$ given by

$$f_1 = E+F+G+H+I+J+K+(D+G)\cdot(B+C+E+F)$$
$$f_2 = B+C+D+H+I+J+K+(D+G)\cdot(B+C+E+F)$$
$$f_3 = A+B+D+E+G+I+K+(H+K)\cdot(B+C)+(I+J)\cdot(E+F)$$
$$f_4 = A+C+D+F+G+J+K+(H+K)\cdot(B+C)+I+J)\cdot(E+F).$$

The transposed Jacobian of $\mathcal{NV}_3$ is

	f_1	f_2	f_3	f_4
F_A	0	0	1	1
F_B	$D+G$	$1+D+G$	$1+H+K$	$H+K$
F_C	$D+G$	$1+D+G$	$H+K$	$1+H+K$
F_D	$B+C+E+F$	$1+B+C+E+F$	1	1
F_E	$1+D+G$	$D+G$	$1+I+J$	$I+J$
F_F	$1+D+G$	$D+G$	$I+J$	$1+I+J$
F_G	$1+B+C+E+F$	$B+C+E+F$	1	1
F_H	1	1	$B+C$	$B+C$
F_I	1	1	$1+E+F$	$E+F$
F_J	1	1	$E+F$	$1+E+F$
F_K	1	1	$1+B+C$	$1+B+C$

3.8. Theorem. *The codes $\mathcal{NV}_1, \mathcal{NV}_2, \mathcal{NV}_3$ are mutually nonequivalent 1-error-correcting perfect codes which are not equivalent to any Vasil'ev code.*

Proof. It is straightforward to check that the Jacobians of these codes satisfy the conditions of 3.2.

To see that they are nonequivalent, we use 2.9 to find that
rank $(\mathcal{NV}_1)=3$, basis: $\tilde{F}_E, \tilde{F}_H, \tilde{F}_J$
rank $(\mathcal{NV}_2)=4$, basis: $\tilde{F}_B, \tilde{F}_C, \tilde{F}_H, \tilde{F}_J$
rank $(\mathcal{NV}_3)=5$, basis: $\tilde{F}_B, \tilde{F}_D, \tilde{F}_E, \tilde{F}_H, \tilde{F}_I$.
It is slightly more difficult to prove that no Vasil'ev code is equivalent to one of $\mathcal{NV}_1, \mathcal{NV}_2, \mathcal{NV}_3$. ∎

Lemma 3.6 implies, that $\mathcal{NV}_3$ is "non-Vasil'ev". Another possibility is the classification via the Steiner triple systems formed by the codewords of weight 3.

It has been shown by [2] that there are, up to isomorphism, only two Steiner triple systems associated with the (15, 11)-Vasil'ev codes (namely the STS No. 1 and 2 in the list of [1] (see [4])). The Steiner triple systems associated with $\mathcal{NV}_1$, $\mathcal{NV}_2$, $\mathcal{NV}_3$ are not isomorphic with these.

So far, we have not been able to give a complete classification of the perfect (15, 11)-codes. Using the methods established in this paper, a classification of the *systematic* perfect (15, 11)-codes seems possible, but the question whether there is a nonsystematic code with these parameters remains open.

A generalization of 3.2 to other prime-power alphabets has been given by [3].

References

[1] F. C. BUSSEMAKER and J. J. SEIDEL, Symmetric Hadamard matrices of order 36, *Technological University Eindhoven Report* 70 *WSK*—02 (1970).
[2] G. GRUMBACH, 1-Fehler-korrigierende, perfekte Codes über F_q, *Diplomarbeit TH Darmstadt* (1980) *(unpublished)*.
[3] F. HERGERT, Beiträge zur Theorie nichtlinearer Fehler-korrigierender Codes, *Diplomarbeit TH Darmstadt* (1980) *(unpublished)*.
[4] M. LIMBOS, Projective embeddings of small "Steiner Triple Systems", *Annals of Discrete Mathematics* 7 (1980), 151—173.
[5] F. J. MACWILLIAMS and N. J. A. SLOANE, *The theory of error-correcting codes*, North-Holland Publ. Comp. (1978).

H. Bauer, B. Ganter, F. Hergert

Technische Hochschule Darmstadt
Fachbereich Mathematik, Arbeitsgruppe 1
D-6100 Darmstadt, West Germany