ELSEVIER

Journal of Statistical Planning and Inference 51 (1996) 229–242

journal of statistical planning and inference

On the existence of error-correcting pairs

Ruud Pellikaan [1]

Department of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, Netherlands

Abstract

Algebraic-geometric codes have a t-error-correcting pair which corrects errors up to half the designed minimum distance. A generalization of the Roos bound is given from cyclic to linear codes. An MDS code of minimum distance 5 has a 2-error-correcting pair if and only if it is an extended-generalized-Reed–Solomon code.

Keywords: Decoding; Algebraic-geometric codes; Error-correcting pairs

AMS classifications: 94B25

1. Introduction

The concept of an error-correcting pair seems to be the basic idea common to many papers on decoding linear codes up to half the minimum distance. In this paper we investigate whether every linear code has an error-correcting pair. In Section 2 we give the basic properties of error-correcting pairs and in Section 3 we give a generalization of the Roos bound from cyclic codes to arbitrary linear codes. In Section 4 we show that algebraic-geometric codes have a t-error-correcting pair, where t is equal to half the designed minimum distance. It turns out that the MDS property is important for an error-correcting pair to hold; we investigate this in Section 5. In Section 6 we prove that an $[n, n-4, 5]$ code has a 2-error-correcting pair if and only if it is an extended-generalized-Reed–Solomon code.

Notation. The dimension of a linear code C is denoted by $k(C)$ and its minimum distance by $d(C)$. The standard inner product on $\mathbb{F}_q^n$ is defined by $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \sum a_i b_i$. The dual $C^\perp$ of C is by definition $C^\perp = \{\boldsymbol{x} \in \mathbb{F}_q^n \mid \langle \boldsymbol{x}, \boldsymbol{c} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\}$. We define $A \perp B$ if and only if $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = 0$ for all $\boldsymbol{a} \in A$ and $\boldsymbol{b} \in B$. The starproduct is defined by coordinate wise multiplication $\boldsymbol{a} * \boldsymbol{b} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Furthermore $A * B = \{\boldsymbol{a} * \boldsymbol{b} \mid \boldsymbol{a} \in A \text{ and } \boldsymbol{b} \in B\}$.

[1] Email: ruudp@win.tue.nl.

SSDI 0378-3758(95)00088-7

2. Error-correcting pairs

Definition 2.1. Let C be an $\mathbb{F}_q$-linear code of length n. We call a pair (A,B) of $\mathbb{F}_{q^N}$-linear codes of length n a *t-error-correcting pair* for C over $\mathbb{F}_{q^N}$ if the following properties hold:

$$(1)\ (A*B)\perp C,\quad (2)\ k(A)>t,\quad (3)\ d(B^{\perp})>t,\quad (4)\ d(A)+d(C)>n\ .$$

We say that C has an *error-correcting pair* if it has a t-error-correcting pair over some finite extension of $\mathbb{F}_q$, where $t=\lfloor (d(C)-1)/2)\rfloor$.

Remark 2.2. (1) We showed (Pellikaan, 1992) that a code of length n which has a t-error–correcting pair over $\mathbb{F}_{q^N}$, has a decoding algorithm which corrects all received words with at most t errors in complexity $0((nN)^3)$. In particular, the minimum distance of C is at least $2t+1$. The concept of an error-correcting pair was also introduced independently by Kötter (1992). It turned out that the concept of an error-correcting pair is fruitful in the decoding of cyclic and algebraic-geometric codes, see Sections 3 and 4. For many cyclic codes Duursma and Kötter (1993,1994) have found error-correcting pairs which correct beyond the designed BCH capacity.

(2) If C is a code in $\mathbb{F}_q^n$ of minimum distance d, then it has not a t-error-correcting pair over $\mathbb{F}_q$, where $t=\lfloor (d-1)/2\rfloor$, in case $d>(q-1)/(q+1)\,n$ and n is sufficiently large, see Remark 2.17 of Pellikaan (1992) and notice the misprint.

(3) We defined (Pellikaan, 1992) for every subset I of $\{1,\ldots,n\}$ the projection map $\pi_I:\ \mathbb{F}_q^n\to\mathbb{F}_q^t$ by $\pi_I(\boldsymbol{x})=(x_{i_1},\ldots,x_{i_t})$, where $I=\{i_1,\ldots,i_t\}$ and $1\leqslant i_1<\cdots<i_t\leqslant n$. We denoted the image of π_I by A_I and the kernel of π_I by $A(I)$, i.e., $A(I)=\{\boldsymbol{a}\in A\mid a_i=0 \text{ for all } i\in I\}$. We showed (Pellikaan, 1992, Lemma 2.7) the following property: $\dim(A_I)=|I|$ for all I with at most t elements if and only if $d(A^{\perp})>t$

In the following proposition we rephrase Theorem 5 of Van Lint and Wilson (1986).

Proposition 2.3. *If A,B and C are linear codes of length n over $\mathbb{F}_q$ such that $(A*B)\perp C$ and $d(A^{\perp})>a>0$ and $d(B^{\perp})>b>0$, then $d(C)\geqslant a+b$.*

Proof. Let $\boldsymbol{c}$ be a nonzero codeword in C with support I, that is to say $I=\{i\mid c_i\neq 0\}$. Let $t=|I|$. Without loss of generality we may assume that $a\leqslant b$. We have

$$\dim(A_I)+\dim(B_I)\geqslant\begin{cases}2t & \text{if } t\leqslant a,\\ a+t & \text{if } a<t\leqslant b,\\ a+b & \text{if } b<t\end{cases}$$

by Remark 2.2.(3). But $(A*B)\perp C$, so $(\boldsymbol{c}*A)_I\perp B_I$. Moreover $\dim((\boldsymbol{c}*A)_I)=\dim(A_I)$, since $c_i\neq 0$ for all $i\in I$. Therefore $\dim(A_I)+\dim(B_I)\leqslant|I|=t$. This is only possible in case $t\geqslant a+b$. Thus $d(C)\geqslant a+b$. $\square$

Proposition 2.4. *Let t be a positive integer. If A is an $[n,t+1,n-t]$ code and B is an $[n,t,n-t+1]$ code, both over $\mathbb{F}_{q^N}$, and C is a linear code over $\mathbb{F}_q$ of length n*

such that $(A * B) \perp C$, *then* C *has minimum distance at least* $2t+1$ *and* (A,B) *is a* t*-error-correcting pair of* C *over* $\mathbb{F}_{q^N}$.

Proof. The code A is MDS, so the dual of A is also MDS and has therefore parameters $[n, n-t-1, t+2]$, by the works of MacWilliams and Sloane (1977) and of Oberst and Dür (1985), so $d(A^\perp) > t+1$. In the same way we have that $d(B^\perp) > t$. Thus $d(C) \geqslant 2t+1$, by Proposition 2.3. The dimension of A is $t+1$, by assumption, so $k(A) > t$. Moreover $d(A) + d(C) \geqslant (n-t) + (2t+1) = n+t+1 > n$. Thus (A,B) is a t-error-correcting pair for C over $\mathbb{F}_{q^N}$. □

Proposition 2.5. *If* C *is an* $[n, n-2t, 2t+1]$ *code and* (A,B) *is a* t*-error-correcting pair for* C, *then* A *is an* $[n, t+1, n-t]$ *code.*

Proof. We have $(A * B) \perp C$, thus $(B * C) \perp A$. Furthermore C is an MDS code, thus $C^\perp$ is an $[n, 2t, n-2t+1]$ code, so $d(C^\perp) > n-2t$. The code $B^\perp$ has minimum distance at least $t+1$, since (A,B) is a t-error-correcting pair. Thus $d(A) \geqslant t + (n-2t) = n-t$, by Proposition 2.3. Moreover $k(A) \geqslant t+1$, by assumption. Thus A is an MDS code with parameters $[n, t+1, n-t]$. □

Remark 2.6. Condition (4) in Definition 2.1 implies that the map π_I is an isomorphism between A and A_I for every I which is the support of a nonzero codeword $\boldsymbol{c}$ of C. Since, if $\boldsymbol{c} \in C$ and $\boldsymbol{c} \neq \boldsymbol{0}$ and $I = \{i \mid c_i \neq 0\}$, and $\boldsymbol{a}$ is a nonzero element of $A(I)$, the kernel of π_I, then $a_i = 0$ for all $i \in I$, so

$$n \geqslant |I| + \mathrm{wt}(\boldsymbol{a}) \geqslant d(C) + d(A) ,$$

which contradicts condition (4).

Proposition 2.7. *Let* C *be a linear code of minimum distance* $2t+1$ *and length* n. *If* (A,B) *is a* t*-error-correcting pair for* C *and* $d(B) + d(C) > n$, *then* B *is an* $[n, t, n-t+1]$ *code.*

Proof. Let $\boldsymbol{c}$ be a nonzero element of C of minimum weight and support I. Then $|I| = 2t+1 = d(C)$. Furthermore $\dim(A) = \dim(A_I)$ by Remark 2.6, and $\dim(B) = \dim(B_I)$ by the assumption $d(B) + d(C) > n$. Moreover $(\boldsymbol{c} * A)_I \perp B_I$ in $\mathbb{F}_q^{2t+1}$, so $\dim(A_I) + \dim(B_I) \leqslant 2t+1$. Therefore

$$(t+1) + \dim(B) \leqslant \dim(A) + \dim(B) \leqslant 2t+1 .$$

So $k(B) \leqslant t$. Thus $k(B^\perp) \geqslant n-t$ and $d(B^\perp) \geqslant t+1$ by condition (3) of a t-error-correcting pair. Therefore $B^\perp$ is MDS, so B is MDS and has parameters $[n, t, n-t+1]$. □

Remark 2.8. In Section 5 we will see that if C has an error-correcting pair (A,B), then after a finite extension of $\mathbb{F}_q$, we can find a code B_t with parameters $[n, t, n-t+1]$ such that (A, B_t) is a t-error-correcting pair for C.

3. Error-correcting pairs and cyclic codes

In this section we will not prove that many cyclic codes have error-correcting pairs, for this we refer to Duursma and Kötter (1992,1994), but we want to show the great similarity between the concept of an error-correcting pair and the techniques used by Van Lint and Wilson (1986). An instance of this we have seen already in Proposition 2.3. In the following proposition we will generalize the Roos bound from cyclic codes to arbitrary linear codes.

Proposition 3.1. *Let C be an $\mathbb{F}_q$-linear code of length n. Let (A,B) be a pair of $\mathbb{F}_{q^N}$-linear codes of length n such that $(A*B)\perp C$ and $k(A)+d(A)+d(B^\perp)\geqslant n+3$ and A is not degenerate, that is to say a generating matrix of A has no zero column. Then $d(C)\geqslant k(A)+d(B^\perp)-1$.*

Proof. Let $a = k(A)-1$ and $b = d(B^\perp)$, then one can restate the conditions of this proposition similar to the conditions of an error-correcting pair as follows: If (1) $(A*B)\perp C$, (2) $k(A) > a$, (3) $d(B^\perp) > b$, (4) $d(A)+a+b > n$ and (5) $d(A^\perp) > 1$, then $d(C)\geqslant a+b+1$. One can give two proofs. The first proof is the same as the proof given by Van Lint and Wilson (1986, Example 2) of the Roos bound and is as follows. Let $\mathscr{A}$ be a generator matrix of A. Let $\mathscr{A}_I$ be the submatrix of $\mathscr{A}$ consisting of the columns indexed by I. Then $\operatorname{rank}(\mathscr{A}_I) = \dim(A_I)$. Condition (5) implies that $\mathscr{A}$ has no zero column, so $\operatorname{rank}(\mathscr{A}_I)\geqslant 1$ for all I with at least one element. Let I be an index set such that $|I|\leqslant a+b$, then any two words of A differ in at least one place of I, since $d(A) > n-(a+b)\geqslant n-|I|$, by condition (4). So A and A_I have the same number of code words, so $\operatorname{rank}(\mathscr{A}_I)\geqslant k(A)\geqslant a+1$. Hence for any I such that $b < |I|\leqslant a+b$ we have that $\operatorname{rank}(\mathscr{A}_I)\geqslant |I|-b+1$. Let $\mathscr{B}$ be a generator matrix of B. Then condition (3) implies

$$\operatorname{rank}(\mathscr{B}_I) = \begin{cases} |I| & \text{if } |I|\leqslant b, \\ \geqslant b & \text{if } |I| > b, \end{cases}$$

by Remark 2.2.(3). Therefore,

$$\operatorname{rank}(\mathscr{A}_I)+\operatorname{rank}(\mathscr{B}_I) > |I| \text{ for } |I|\leqslant a+b.$$

Now let $\boldsymbol{c}$ be a nonzero element of C with support I, then $\operatorname{rank}(\mathscr{A}_I)+\operatorname{rank}(\mathscr{B}_I)\leqslant |I|$, as we have seen in the proof of Proposition 2.3. Thus $|I| > a+b$, so $d(C) > a+b$.

The second proof is more straightforward and is as follows. Let $\boldsymbol{c}$ be a nonzero element of C with support I. If $|I|\leqslant b$, then take $i\in I$. There exists an $\boldsymbol{a}\in A$ such that $a_i\neq 0$, by condition (5). So $\boldsymbol{a}*\boldsymbol{c}$ is not zero, its weight is at most b and is an element of $B^\perp$, by condition (1), but this contradicts condition (3). If $b < |I|\leqslant a+b$, then we can choose index sets I_- and I_+ such that $I_-\subseteq I\subseteq I_+$, and I_- has b elements and I_+ has $a+b$ elements. Now $k(A) > a$ and $I_+\setminus I_-$ has a elements, so $A(I_+\setminus I_-)$ is not zero. Let $\boldsymbol{a}$ be a nonzero element of $A(I_+\setminus I_-)$. The vector $\boldsymbol{c}*\boldsymbol{a}$ is an element of $B^\perp$ and has support in I^-. Furthermore $|I^-| = b < d(B^\perp)$, hence $\boldsymbol{a}*\boldsymbol{c} = 0$, so $a_i = 0$ for all

$i \in I_+$. Therefore $\boldsymbol{a}$ is a nonzero element of A of weight at most $n - |I_+| = n - (a+b)$, which contradicts condition (4). Thus $|I| > a + b$, so $d(C) > a + b$. $\square$

Example 3.2. In this example we show that the assumption that A is nondegenerate is necessary. Let $A, B^\perp$ and C be the binary codes with generating matrices $(011), (111)$ and (100), respectively. Then $A * C \subseteq B^\perp$ and $k(A) = 1, d(A) = 2, n = 3$ and $d(B^\perp) = 3$, so $k(A) + d(A) + d(B^\perp) = 6 = n + 3$, but $d(C) = 1$.

Corollary 3.3. *Let α be a primitive element of $\mathbb{F}_{q^N}$. Let $\mathbb{F}_{q^N}$ contain all nth roots of unity. Let U and V be nonempty subsets of nonzero elements of $\mathbb{F}_{q^N}$. If $V = \{\alpha^{i_1}, \ldots, \alpha^{i_v}\}$ with $i_1 < \cdots < i_v$, then we denote the set $\{\alpha^i | i_1 \leqslant i \leqslant i_v\}$ by $\bar{V}$. Let U be a defining set of a cyclic code with minimum distance d_U over $\mathbb{F}_{q^N}$ and if V is a set of nth roots of unity such that $|\bar{V}| \leqslant |V| + d_U - 2$, then the code with defining set UV has minimum distance $d \geqslant |V| + d_U - 1$ over $\mathbb{F}_{q^N}$ and thus also over $\mathbb{F}_q$.*

Proof. Remark that it is not clearly stated in Theorem 3 of van Lint and Wilson (1986) that the d_U denotes the minimum distance of the cyclic code over $\mathbb{F}_{q^N}$, instead of $\mathbb{F}_q$, with defining set U. Let A and B be the cyclic codes over $\mathbb{F}_{q^N}$ with generating set V and U, respectively. Then A has dimension $|V|$ and its minimum distance is at least $n - |\bar{V}| + 1$. A generating matrix of A has no zero column, since otherwise A would be zero, since A is cyclic; but A is not zero, since V is not empty. So A is not degenerate. Moreover $d(B^\perp) = d_U$, by assumption. Let C be the cyclic code over $\mathbb{F}_{q^N}$ with defining set UV. Then $(A * B) \perp C$ and $k(A) + d(A) + d(B^\perp) \geqslant |V| + (n - |\bar{V}| + 1) + d_U \geqslant n + 3$, so $d(C) \geqslant k(A) + d(B^\perp) - 1 = |V| + d_U - 1$. $\square$

A special case of Proposition 3.1, in the reformulation given in the proof, is obtained if we take $a = b = t$.

Corollary 3.4. *Let C be an $\mathbb{F}_q$-linear code of length n. Let (A, B) be a pair of $\mathbb{F}_{q^N}$-linear codes of length n such that the following properties hold:* (1) $(A * B) \perp C$, (2) $k(A) > t$, (3) $d(B^\perp) > t$, (4) $d(A) + 2t > n$ *and* (5) $d(A^\perp) > 1$, *then* $d(C) \geqslant 2t + 1$.

Remark 3.5. In this way we get at the same time the lower bound $2t + 1$ for the minimum distance of the code $C := (A * B)^\perp$ and a t-error-correcting pair for C, for any pair (A, B) which satisfies the five conditions of Corollary 3.4. Thus we can find t-error-correcting pairs in abundance. Notice that the four conditions in the definition of a t-error-correcting pair imply that $d(C) \geqslant 2t + 1$, but that this is not longer true if we replace the fourth condition of Definition 2.1 or Corollary 3.4 by '$d(A) + 2t + 1 > n$' as the following example shows.

Example 3.6. Let $\alpha_3, \ldots, \alpha_n$ be $n - 2$ distinct elements of $\mathbb{F}_q$. Let A be generated by the all one vector and $(0, 0, \alpha_3, \ldots, \alpha_n)$. Let B be generated by the all one vector. Let C be the dual of A. Then A is an $[n, 2, n-2]$ code, the minimum distance of C and the

duals of A and B is two, and clearly $A * B \perp C$, so A, B and C satisfy all conditions of Corollary 3.5 with $t = 1$ except condition (4).

Remark 3.7. The generalization of 'shifting' in the paper of Van Lint and Wilson to arbitrary linear codes is still an open question. A candidate for this could be the concept of an error-correcting array, see Pellikaan and Kirfel (1993).

4. Error-correcting pairs for algebraic-geometric codes

For the details of this section we refer to pellikaan (1989, 1992). Let X be a curve over the finite field $\mathbb{F}_q$ of genus g. Let $\mathbb{F}_q(X)$ be the function field of X over $\mathbb{F}_q$. Let $P_1, \ldots, P_n$ be n distinct points on X and let $D = P_1 + \cdots + P_n$. Let G be a divisor of degree m and support disjoint from D. Let $L(G) = \{f \in \mathbb{F}_q(X) | \ f = 0 \text{ or } (f) \geqslant -G\}$. The algebraic-geometric code $C_L(D, G)$ is defined as the image of the evaluation map $\mathrm{ev}_D : L(G) \to \mathbb{F}_q^n$, where $\mathrm{ev}_D(f) = (f(P_1), \ldots, f(P_n))$. If $m < n$, then the dimension of $C_L(D, G)$ is at least $m + 1 - g$, and the minimum distance is at least $n - m$. If $m > 2g - 2$, then the dual code has parameters $[n, \geqslant n + g - m - 1, \geqslant m - 2g + 2]$. The dual can also be described by means of differential forms and it is denoted by $C_\Omega(D, G)$. Both codes $C_L(D, G)$ and $C_\Omega(D, G)$ are called algebraic geometric (AG) or geometric Goppa codes. We are concerned with finding an error-correcting pair for codes of the form $C_\Omega(D, G)$, and we call $m - 2g + 2$ the designed minimum distance and denote it by d^*. If we construct AG codes over $\mathbb{F}_{q^N}$, then we denote them by $C_L(D, G, \mathbb{F}_{q^N})$ and $C_\Omega(D, G, \mathbb{F}_{q^N})$, respectively.

Proposition 4.1. *An algebraic-geometric code of designed minimum distance d^* from a curve over $\mathbb{F}_q$ of genus g, has a t-error-correcting pair over $\mathbb{F}_q$, where $t = \lfloor (d^* - 1 - g)/2 \rfloor$.*

Proof. See Pellikaan(1989,1992).

Proposition 4.2. *An algebraic-geometric code of designed minimum distance d^* from a curve over $\mathbb{F}_q$, has a t-error-correcting pair over $\mathbb{F}_{q^N}$, where $t = \lfloor (d^* - 1)/2 \rfloor$, in case*

$$N > \log_q \left(2\binom{n}{t} + 2\binom{n}{t+1} + 1\right).$$

Remark 4.3. A consequence of Proposition 4.1 is that one can correct AG codes up to $\lfloor (d^* - 1 - g)/2 \rfloor$ errors with complexity $\mathrm{O}(n^3)$. From Proposition 4.2 and Remark 2.2 it follows that one can correct AG codes up to $\lfloor (d^* - 1)/2 \rfloor$ errors with complexity $\mathrm{O}(n^6)$, since

$$\log_q \left(\binom{n}{t} + \binom{n}{t+1} + 1\right) = \mathrm{O}(n) \text{ for } n \to \infty.$$

The drawback of Proposition 4.2 is that it says that there exists such a pair, but it does not give a method how to find such a pair efficiently, and probably the complexity of finding such a pair grows exponentially with n. This is not the case with Proposition 4.1; one has an efficient way to find such a pair.

One might wonder whether every geometric Goppa code has a t-error-correcting pair, where $t = \lfloor (d-1)/2 \rfloor$ and d the true minimum distance of the geometric Goppa code. But this is not true, since every linear code is an algebraic-geometric code in a weak sense, i.e. without any restriction on the degree of the divisors used with respect to the length of the code and the genus of the curve, by Pellikaan et al. (1991), and in Section 6 we will see examples of linear codes which have no error-correcting pair.

Proof of Proposition 4.2. We give a sketch of the proof in the case m is odd. Let $t = \lfloor (d^* - 1)/2 \rfloor$. We claim that there exists a divisor F on X of degree $t+g$, which is rational over $\mathbb{F}_{q^N}$, in such a way that both the codes A and B are MDS with parameters $[n, t+1, n-t]$ and $[n, t, n-t+1]$, respectively, where $A = C_L(D, F, \mathbb{F}_{q^N})$ and $B = C_L(D, G-F, \mathbb{F}_{q^N})$. F is a divisor of degree $t+g$, so $G-F$ is a divisor of degree $t+g-1$, therefore $\ell(F) \geqslant t+1$ and $\ell(G-F) \geqslant t$, where we denote the dimension of $L(F)$ by $\ell(F)$. If A has minimum distance strictly smaller than $n-t$, then there exists a nonzero function $f \in L(F, \mathbb{F}_q)$, which has at least $t+1$ zeros. Thus there exists a divisor Q such that $0 \leqslant Q \leqslant D$ and $\deg(Q) = t+1$ and $(f) \geqslant -F+Q$, so $(f) = -F+Q+E$, for some effective divisor E of degree $g-1$. Consider the divisor class $[F]$ in the Picard group $\mathrm{Pic}(X,N)$ of divisors on X which are rational over $\mathbb{F}_{q^N}$, modulo principal divisors (f) of $f \in \mathbb{F}_{q^N}(X)$. Then $[F]$ is in the $t+g$ graded part $\mathrm{Pic}_{t+g}(X,N)$ of $\mathrm{Pic}(X,N)$, and is equal to $[E+Q]$. Thus conversely, if for all divisors Q of degree $t+1$ such that $0 \leqslant Q \leqslant D$ we have that $L(F-Q) = 0$, then A has at least minimum distance $n-t$. In particular $L(F-D) = 0$, thus $\dim C_L(D, F, \mathbb{F}_{q^N}) = \ell(F) \geqslant t+1$. Therefore $C_L(D, F, \mathbb{F}_{q^N})$ is MDS with parameters $[n, t+1, n-t]$. For the following counting argument we refer to Pellikaan (1989) and Vlăduţ (1990). There are $\binom{n}{t+1}$ divisors Q of degree $t+1$ such that $0 \leqslant Q \leqslant D$. We denote by $a_j(N)$ the number of effective divisors of degree j on X which are rational over $\mathbb{F}_{q^N}$. We denote by $h(N)$ the number of elements of $\mathrm{Pic}_0(X,N)$. We have the following inequality

$$a_{g-1}(N) \leqslant 2h(N)/(q^N - 1) ,$$

by a result of Vlăduţ (1990). The number of divisor classes of the form $[E+Q]$, as mentioned above, is at most $\binom{n}{t+1} a_{g-1}(N)$. In the same way we get that $C_L(D, G-F, \mathbb{F}_{q^N})$ is an $[n, t, n-t+1]$ code if $[F]$ is not of the form $[G-E'-Q']$, where E' is an effective divisor of degree $g-1$ and Q' a divisor of degree t such that $0 \leqslant Q' \leqslant D$. There are $\binom{n}{t} a_{g-1}$ divisors of the form $[G-E'-Q']$ for a fixed divisor G. We assumed

$$N > \log_q \left(2\binom{n}{t} + 2\binom{n}{t+1} + 1 \right) ,$$

so

$$\left(\binom{n}{t}+\binom{n}{t+1}\right)\frac{2}{q^N-1}<1\,,$$

thus

$$a_{g-1}(N)\left(\binom{n}{t}+\binom{n}{t+1}\right)<h(N)\,.$$

Therefore there exists a divisor F of degree $t+g$ such that $[F]\neq[E+Q]$ and $[F]\neq[G-E'-Q']$ for all divisors Q and Q' of degree $t+1$ and t, respectively, such that $0\leqslant Q\leqslant D$ and $0\leqslant Q'\leqslant D$, and for all effective divisors E and E' both of degree $g-1$. Thus there exists a divisor F which satisfies the above claim. In case m is even the proof is as for proving A and B are both $[n,t+1,n-t]$ codes. In both cases we get that (A,B) is a t-error-correcting pair for C. □

5. MDS codes

We have seen in Section 2 how the MDS property of either one of the three codes A,B or C, in case (A,B) is an error-correcting pair for C, implies the MDS property of one of the other codes. The main result of this section is that we may assume that B is an $[n,t,n-t+1]$ code in case C has an error-correcting pair (A,B).

We have already used some of the properties of so called maximum distance separable (MDS) codes, these are $[n,k,d]$ codes which satisfy the Singleton bound $k+d\leqslant n+1$ with equality. An $[n,k]$ code is MDS if and only if the determinants of all $(k\times k)$ submatrices of a $(k\times n)$ generator matrix are nonzero. If a code is MDS, then its dual is MDS too. Well known examples are (extended)(generalized) Reed–Solomon codes, these are in fact algebraic-geometric codes on the projective line.

Proposition 5.1. *Let B be a q-ary code. If $d(B^\perp)>t$ and $q^N>\max\left\{\binom{n}{i}\;\middle|\;1\leqslant i\leqslant t\right\}$, then there exists a sequence $\{B_r\mid 0\leqslant r\leqslant t\}$ of q^N-ary codes such that $B_{r-1}\subseteq B_r$ and B_r is an $[n,r,n-r+1]$ code and contained in the $\mathbb{F}_{q^N}$-linear code generated by B for all $0\leqslant r\leqslant t$.*

Corollary 5.2. *Let C be a q-ary code of minimum distance d. If $q^N>\max\left\{\binom{n}{i}\;\middle|\;1\leqslant i\leqslant d-1\right\}$, then C is contained in a q^N-ary MDS code of the same minimum distance as C.*

Remark 5.3. The Corollary follows from Proposition 5.1 by taking $B=C^\perp$ and $t=d-1$. This result was proved by Oberst and Dür (1985) with the weaker assumption $q^N>\binom{n-1}{d-1}-\binom{n-k-1}{d-1}$, where C is an $[n,k,d]$ code; but our Proposition gives a stronger conclusion and the proof is more straightforward.

Proof of Proposition 5.1. The proof goes by induction on t. In case $t = 0$, there is nothing to prove, we can take $B_0 = 0$. Suppose the statement is proved for t. Let B be a code such that $d(B^\perp) > t+1$ and suppose $q^N > \max\left\{ \binom{n}{i} \;\middle|\; 1 \leqslant i \leqslant t+1 \right\}$. By induction we may assume that there is a sequence $\{B_r \mid 0 \leqslant r \leqslant t\}$ of q^N-ary codes such that $B_{r-1} \subseteq B_r \subseteq \mathbb{F}_{q^N} B$ and B_r is an $[n, r, n-r+1]$ code for all r, $0 \leqslant r \leqslant t$. So B has a generator matrix G with entries g_{ij} for $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant n$, such that the first r rows of G give a generator matrix G_r of B_r. In particular the determinants of all $(t \times t)$-submatrices of G_t are nonzero. Let $\Delta(j_1, \ldots, j_t)$ be the determinant of $G_t(j_1, \ldots, j_t)$, which is the matrix obtained from G_t by taking the columns numbered by $j_1, \ldots, j_t$, where $1 \leqslant j_1 < \cdots < j_t \leqslant n$. For $t < i \leqslant n$ and $1 \leqslant j_1 < \cdots < j_{t+1} \leqslant n$ we define $\Delta(i; j_1, \ldots, j_{t+1})$ to be the determinant of the $(t+1) \times (t+1)$ submatrix of G formed by taking the columns numbered by $j_1, \ldots, j_{t+1}$ and the rows numbered by $1, \ldots, t, i$. Now consider for every $(t+1)$-tuple $\boldsymbol{j} = (j_1, \ldots, j_{t+1})$ such that $1 \leqslant j_1 < \cdots < j_{t+1} \leqslant n$, the linear equation in the variables $X_{t+1}, \ldots, X_n$ given by

$$\sum_{s=1}^{t+1} (-1)^s \Delta(j_1, \ldots, \hat{j}_s, \ldots, j_{t+1}) \Big(\sum_{i>t} g_{ij_s} X_i \Big) = 0 \ ,$$

where $(j_1, \ldots, \hat{j}_s, \ldots, j_{t+1})$ is the t-tuple obtained from $\boldsymbol{j}$ by deleting the s-th element. We can rewrite this equation as follows:

$$\sum_{i>t} \Delta(i; \boldsymbol{j}) X_i = 0 \ .$$

If for a given $\boldsymbol{j}$ the coefficients $\Delta(i; \boldsymbol{j})$ are zero for all $i > t$, then all the rows of the matrix $G(\boldsymbol{j})$, which is the submatrix of G consisting of the columns numbered by $j_1, \ldots, j_{t+1}$, are dependent on the first t rows of $G(\boldsymbol{j})$. Thus $\operatorname{rank}(G(\boldsymbol{j})) \leqslant t$, so G has $t+1$ columns which are dependent. But G is a parity check matrix for $B^\perp$, therefore $d(B^\perp) \leqslant t+1$, which contradicts the assumption in the induction hypothesis. We have therefore proved that for a given $(t+1)$-tuple, at least one of the coefficients $\Delta(i, \boldsymbol{j})$ is nonzero. Therefore the above equation defines a hyperplane $H(\boldsymbol{j})$ in a vector space over $\mathbb{F}_{q^N}$ of dimension $n - t$. We assumed $q^N > \binom{n}{t+1}$, so

$$(q^N)^{n-t} > \binom{n}{t+1} (q^N)^{n-t-1} \ .$$

Therefore $(\mathbb{F}_{q^N})^{n-t}$ has more elements than the union of all $\binom{n}{t+1}$ hyperplanes of the form $H(\boldsymbol{j})$. Thus there exists an element $(x_{t+1}, \ldots, x_n) \in (\mathbb{F}_{q^N})^{n-t}$ which does not lie in this union. Now consider the code B_{t+1}, defined by the generator matrix G_{t+1} with entries $(g'_{ij} \mid 1 \leqslant i \leqslant t+1,\ 1 \leqslant j \leqslant n)$, where

$$g'_{ij} = \begin{cases} g_{ij} & \text{if } 1 \leqslant i \leqslant t, \\ \sum_{i>t} g_{ij} x_i & \text{if } i = t+1. \end{cases}$$

Then B_{t+1} is a subcode of $\mathbb{F}_{q^N}B$, and for every $(t+1)$- tuple $\boldsymbol{j}$, the determinant of the corresponding $(t+1)\times(t+1)$ submatrix of G_{t+1} is equal to $\sum_{i>t}\Delta(i;\boldsymbol{j})x_i$, which is not zero, since $\boldsymbol{x}$ is not an element of $H(\boldsymbol{j})$. Thus B_{t+1} is an $[n,t+1,n-t]$ code. □

Corollary 5.4. *If C has a t-error-correcting pair (A,B) over $\mathbb{F}_{q^N}$ and $q^N > \max\{\binom{n}{i} \mid 1\leqslant i\leqslant t\}$, then C has a t-error-correcting pair (A,B_t) such that B_t is an $[n,t,n-t+1]$ code.*

Proof. Let (A,B) be a t-error-correcting pair for C. So $d(B^\perp) > t$. There exists an $[n,t,n-t+1]$ subcode B_t of B by Proposition 5.1. Moreover $(A*B_t)\perp C$, since $A*B_t\subseteq A*B$ and $(A*B)\perp C$. Thus (A,B_t) is a t-error-correcting pair for C. □

Corollary 5.5. *If C is an $[n,n-2t,2t+1]$ code and has a t-error-correcting pair (A,B) over $\mathbb{F}_{q^N}$ and $q^N > \max\left\{\binom{n}{i} \;\middle|\; 1\leqslant i\leqslant t\right\}$, then A is an $[n,t+1,n-t]$ code and there exists an $[n,t,n-t+1]$ code B_t, which is contained in B, such that (A,B_t) is a t-error-correcting pair over $\mathbb{F}_{q^N}$.*

Proof. This follows from Proposition 2.5 and Corollary 5.4. □

6. Error-correcting pairs for MDS codes of minimum distance 5

If we could prove that every MDS code C has an error-correcting pair, that is a $\lfloor(d(C)-1)/2\rfloor$-error-correcting pair over some extension of $\mathbb{F}_q$, then every linear code has an error-correcting pair, by Corollary 5.2. Formulated in other words: if we want to find an example of a code which does not have an error-correcting pair, then we may as well try to find an MDS code which has not an error-correcting pair. Every code of minimum distance 3 has an error-correcting pair, since C is contained in an $[n,n-2,3]$ code C_3 over a finite extension of $\mathbb{F}_q$. Let $A=C_3^\perp$ and $B=\langle(1,\ldots,1)\rangle$, then A is an $[n,2,n-1]$ code and $d(B^\perp)=2>1$, so $k(A)>1$ and $d(A)+d(C)=n+2>n$. Thus (A,B) is a 1-error-correcting pair. So the first candidate for trying to find a code without an error-correcting pair is a $[n,n-4,5]$ code. Before we give a characterization of $[n,n-4,5]$ codes with an error-correcting pair, we need some preparations.

Definition 6.1. Two codes C_1 and C_2 in $\mathbb{F}_q^n$ are called isometric if there exists an n-tuple $\boldsymbol{x}=(x_1,\ldots,x_n)$ of nonzero elements of $\mathbb{F}_q$ such that $C_2=\boldsymbol{x}*C_1$. In such a case we have $C_1=\boldsymbol{x}^{-1}*C_2$, where $\boldsymbol{x}^{-1}=(x_1^{-1},\ldots,x_n^{-1})$. Usually one allows permutations in the definition of isometric too, but we will not for simplicity.

Lemma 6.2. *If (A,B) is a t-error-correcting pair for C and $\boldsymbol{x},\boldsymbol{y}\in(\mathbb{F}_q^*)^n$, then $(\boldsymbol{x}^{-1}*\boldsymbol{y}^{-1}*A,\boldsymbol{x}*B)$ is a t-error-correcting pair for $\boldsymbol{y}*C$.*

Proof. This follows immediately from the definitions. □

Definition 6.3. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of n distinct elements of $\mathbb{F}_q$. The Reed–Solomon code $\mathrm{RS}_k(\boldsymbol{\alpha})$ of dimension k defined by $\boldsymbol{\alpha}$ is given by

$$\mathrm{RS}_k(\boldsymbol{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in \mathbb{F}_q[X],\ \deg(f) < k\}\ .$$

The code $\mathrm{RS}_k(\boldsymbol{\alpha})$ has parameters $[n, k, n-k+1]$ and has a generator matrix of the form

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}.$$

A generalized-Reed–Solomon (GRS) code is a code isometric to a Reed–Solomon code, that is to say of the form $\boldsymbol{y} * \mathrm{RS}_k(\boldsymbol{\alpha})$. A Cauchy matrix is a $k \times (n-k)$ matrix with entries $(b_i - b_{j-k})^{-1}$ for $1 \leqslant i \leqslant k < j \leqslant n$, where $b_1, \ldots, b_n$ are n distinct elements of $\mathbb{F}_q$. An extended-generalized-Reed–Solomon (EGRS) code is isometric with a code with generator matrix

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} & 1 \end{pmatrix}.$$

Remark 6.4. The dual of an extended-generalized-Reed–Solomon code is again EGRS A code is GRS if and only if it is isometric with a code with generator matrix of the form $(I_k P)$, where I_k is the $(k \times k)$-identity matrix and P is a $k \times (n-k)$ Cauchy matrix, see the works of MacWilliams and Sloane (1977) and Oberst and Dür (1985). The length of a GRS code over $\mathbb{F}_q$ is by definition at most q. Now take the 2 dimensional EGRS code with generator matrix G, with

$$G = \begin{pmatrix} 1 & \ldots & 1 & 0 \\ b_1 & \ldots & b_q & 1 \end{pmatrix},$$

where $b_1, \ldots, b_q$ is an enumeration of the q elements of $\mathbb{F}_q$. Then clearly the code over $\mathbb{F}_q$ with generator matrix G is not GRS over $\mathbb{F}_q$. Let a be an element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The code over $\mathbb{F}_{q^2}$ with generator matrix G is isometric to the code with generator matrix

$$G = \begin{pmatrix} 1 & \ldots & 1 & 1 \\ \dfrac{b_1}{a+b_1} & \ldots & \dfrac{b_q}{a+b_q} & 1 \end{pmatrix}$$

which is GRS over $\mathbb{F}_{q^2}$. Thus a matrix can generate over $\mathbb{F}_q$ a code which is not GRS, but can be GRS over an extension of $\mathbb{F}_q$. This cannot happen with the notion EGRS, that is to say, if G is a matrix with entries in $\mathbb{F}_q$ which generates an EGRS over an extension of $\mathbb{F}_q$, then it generates an EGRS code over $\mathbb{F}_q$. This fact is not used in this paper and it can be proved by the fact that the n columns of a generator matrix of a

EGRS code of dimension k can be viewed as homogeneous coordinates of n points on a normal rational curve in projective space of dimension $k-1$ over $\mathbb{F}_q$, and conversely. Moreover any $k+2$ points in projective space of dimension $k-1$, which are in general position, lie on a unique normal rational curve. The set of EGRS codes is equal to the set of geometric Goppa codes on the projective line. Every GRS code is EGRS. If $n < q$, then a code of length n is GRS if and only if it is EGRS.

Theorem 6.5. *An $[n, n-4, 5]$ code over $\mathbb{F}_q$ has a 2-error-correcting pair over a finite extension of $\mathbb{F}_q$ if and only if it is an extended-generalized-Reed-Solomon code.*

Proof. Extended-generalized-Reed-Solomon codes are algebraic-geometric codes on the projective line, that is on a curve of genus zero, and therefore have an error-correcting pair by Proposition 4.1, see also Pellikaan (1992). Now suppose C is an $[n, n-4, 5]$ code and has a 2-error-correcting pair (A, B). Then we may assume that B is an $[n, 2, n-1]$ code which contains a $[n, 1, n]$ code and A is a $[n, 3, n-2]$ code over a finite extension of $\mathbb{F}_q$, by Propositions 5.1 and 25 and Corollary 5.4. So B contains a word $\boldsymbol{x}$ of weight n and we may replace B by $\boldsymbol{x}^{-1} * B$ by Lemma 6.2. Thus we may assume that B is a $[n, 2, n-1]$ code and contains the all one word; but $A * B \perp C$, so $A \perp C$. Therefore we may assume that the first 3 rows of a parity check matrix of C is a generator matrix of A. Moreover every set of k elements between 1 and n form an information set for A, since A is MDS. Therefore we may assume that the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ b_1 & b_2 & b_3 & b_4 & \dots & b_n \end{pmatrix}$$

constitute a generator matrix of B, where $b_1, \dots, b_n$ are n distinct elements, and that the parity check matrix H of C is given by

$$\begin{pmatrix} 1 & 0 & 0 & a_{14} & \dots & a_{1n} \\ 0 & 1 & 0 & a_{24} & \dots & a_{2n} \\ 0 & 0 & 1 & a_{34} & \dots & a_{3n} \\ 0 & 0 & 0 & a_{44} & \dots & a_{4n} \end{pmatrix},$$

where the first three row vectors $\boldsymbol{a}_1, \boldsymbol{a}_2$ and $\boldsymbol{a}_3$ of H generate A. The code C is MDS, so the dual of C is MDS, therefore all the entries a_{ij} for $1 \leqslant i \leqslant 4 \leqslant j \leqslant n$, are nonzero. Let $\boldsymbol{x} = (1, 1, 1, a_{44}, \dots a_{4n})$. By replacing A by $\boldsymbol{x}^{-1} * A$ and C by $\boldsymbol{x} * C$, we may assume that $a_{4j} = 1$ for $4 \leqslant j \leqslant n$. Let $\boldsymbol{y} = (a_{14}, a_{24}, a_{34}, 1, \dots, 1)$. By replacing A by $\boldsymbol{y} * A$ and C by $\boldsymbol{y}^{-1} * C$, we may assume that $a_{i4} = 1$ for $1 \leqslant i \leqslant 3$. Let $\boldsymbol{b} = (b_1, \dots, b_n)$. Then $\boldsymbol{a}_i * \boldsymbol{b} \in C^{\perp}$ and $\boldsymbol{a}_i b_i \in C^{\perp}$. So

$$\boldsymbol{a}_i * \boldsymbol{b} - \boldsymbol{a}_i b_i = (0, 0, 0, (b_4 - b_i),\ a_{i5}(b_5 - b_i), \dots, a_{in}(b_n - b_i) \in C^{\perp}\ .$$

Therefore it must be a multiple of $(0, 0, 0, 1, \dots, 1)$ which is the fourth row of H. Thus

$$b_4 - b_i = a_{ij}(b_j - b_i) \quad \text{for } 1 \leqslant i \leqslant 3 < j \leqslant n\ .$$

Now we subtract the fourth row from the first three rows. Then we get a parity check matrix H' of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & & \\ 0 & 1 & 0 & 0 & & a'_{ij} \\ 0 & 0 & 1 & 0 & & \\ 0 & 0 & 0 & 1 & 1 \ldots & 1 \end{pmatrix},$$

where

$$a'_{ij} = a_{ij} - 1 = \frac{b_4 - b_i}{b_j - b_i} - 1 = \frac{b_4 - b_j}{b_j - b_i}.$$

Let $z = (1, 1, 1, -1, b_4 - b_5, \ldots, b_4 - b_n)$. We may replace C by $z * C$, which has parity check matrix $(I_4 P)$, where P is the $k \times (n-k)$ Cauchy matrix with entries $(b_i - b_{j-4})^{-1}$ for $1 \leqslant i \leqslant 4 < j \leqslant n$. Therefore $C^{\perp}$ is a GRS code, so C is an EGRS code, by Remark 6.4. □

Example 6.6. For the following we refer to Oberst and Dür (1985). If q is large enough with respect to n, then the majority of all $[n, k]$ codes over $\mathbb{F}_q$ are MDS. In fact one can consider the set of all $[n, k]$ codes with the first k positions as information set, as the affine space of dimension $k(n-k)$, with coordinates $(X_{ij} \mid 1 \leqslant i \leqslant k < j \leqslant n)$. We assume $1 < k < n - 1$. Those codes which are not MDS form a hypersurface in this affine space, obtained as the zero set of the polynomial which is the product of the determinants of all square submatrices of the matrix with entries (X_{ij}). The GRS codes form a closed subvariety, in fact a complete intersection of dimension $(2n - 4)$ in the variety of MDS codes and they coincide if and only if $k(n - k) = 2n - 4$, i.e. if and only if $k = 2$ or $k = n - 2$. Thus, if q is large enough with respect to n, then the GRS codes are scarce among all MDS codes of given length n and dimension k, in case $2 < k < n - 2$. In particular there exist $[n, n - 4, 5]$ codes which are not GRS, and therefore not EGRS, in case $n < q$, and thus have not a 2-error-correcting pair, by Theorem 6.5.

Acknowledgements

I want to thank I.M. Duursma for noticing that the assumption on the nondegeneracy of A is necessary in Proposition 3.1 and for the second proof of this proposition, and L. Tolhuizen for a simplification of the first proof of the same proposition.

References

Duursma, I.M. (1993). Decoding codes from curves and cyclic codes, PhD. thesis, Eindhoven University of Technology.

Duursma, I.M. and R. Kötter (1994). Error-locating pairs for cyclic codes. *IEEE Trans. Inform. Theory* **40**, 1108–1121.

Kötter, R (1992). A unified description of an error locating procedure for linear codes *Proc. Algebraic and Combinatorial Coding Theory*, Voneshta Voda, 1992, 113–117.

Mac Williams, F.J. and N.J.A. Sloane (1977). *The Theory of Error-correcting Codes*. North–Holland, Amsterdam.

Oberst, U. and A. Dür (1985) A constructive characterization of all optimal linear codes. In: *Séminaire d'Algèbre*, Paul Dubreil et Marie-Paule Malliavin 1983–1984, Lecture Notes in Math. **1146** Springer, Berlin, 176–213.

Pellikaan, R. (1992). On decoding by error location and dependent sets of error positions. *Discrete Math.* **106/107** 369–381.

Pellikaan, R. (1989). On a decoding algorithm for codes on maximal curves. *IEEE Trans. Inform. Theory* **35**, 1228–1232.

Pellikaan R. and C. Kirfel (1993). The minimum distance of codes in an array coming from telescopic semigroups, preprint.

Pellikaan, R. B.-Z. Shen and G.J.M. van Wee (1991). Which linear codes are algebraic-geometric ?, *IEEE Trans. Inform. Theory*. **37**, 583–602.

van Lint, J.H. and R.M. Wilson (1986) On the minimum distance of cyclic codes. *IEEE Trans. Inform. Theory* **32**, 23–40.

Vlăduţ, S.G. (1990). On the decoding of algebraic-geometric codes over $\mathbb{F}_q$, for $q \geqslant 16$, *IEEE Trans. Inform. Theory* **36**, 1461–1463.