ON DECODING LINEAR CODES BY ERROR LOCATING PAIRS

by Ruud Pellikaan
Department of Mathematics & Computing Science
Eindhoven University of Technology
P.O. Box 513
5600 MB Eindhoven
The Netherlands

Introduction

Abstracted from the work of Skorobogatov and Vlădut [12] on the decoding of algebraic geometric codes, which generalized the ideas of Justesen et all [12], we present a decoding algorithm, based on error locating pairs, for arbitrary linear codes.
Basically an error locating pair for a linear code C in $\mathbb{F}^n$ is a pair of codes A and B in $\mathbb{F}^n$ such that their star product is contained in $C^\perp$. A linear map E_w from A to B^V is used to locate the errors of a received word.
Translated in generating matrices $\mathbf{A}$ and $\mathbf{B}$ of A en B respectively, $\mathbf{A} * \mathbf{B}$ is part of a parity check matrix for C, this is pursued in the paper of Van Lint and Wilson [14], where properties of the minimum distance of C in terms of $\mathbf{A}$ and $\mathbf{B}$ are derived, in particular the Roos bound for BCH codes.
One can define a notion of error correcting pairs for subfield subcodes and get a similar result as Feng and Tzeng [5], on decoding BCH codes beyond the designed minimal distance.

Notation. Let $\mathbb{F}$ be a finite field and C a code over $\mathbb{F}$. We denote the wordlength of C by $n(C)$ and its minimal distance by $d(C)$. If C is a linear code we denote its dimension by $k(C)$.
The ball of radius r and center a is denoted by $B(\mathbf{a}, r)$, i.e. $B(\mathbf{a}, r) = \{\mathbf{b} \in \mathbb{F}^n \mid d(\mathbf{a}, \mathbf{b}) \leq r\}$ for $\mathbf{a} \in \mathbb{F}^n$. Let $\underline{n} = \{1, \cdots, n\}$. Define the support of $\mathbf{a} \in \mathbb{F}^n$ by $\mathrm{supp}(\mathbf{a}) = \{i \in \underline{n} \mid a_i \neq 0\}$ and the zero set of a by $z(\mathbf{a}) = \{i \in \underline{n} \mid a_i = 0\}$.
We say that w has t errors supported at I if $\mathbf{w} = \mathbf{c} + \mathbf{e}$ with $\mathbf{c} \in C$ and $I = \mathrm{supp}\ \mathbf{e}$ and

$$|I| = t = d(\mathbf{w}, C).$$

If C is a linear code over $\mathbb{F}$ then we denote the vector space of $\mathbb{F}$ linear functionals on C by C^V.

$$C^V := \{\gamma \mid \gamma : C \to \mathbb{F} \text{ is an } \mathbb{F} \text{ linear map}\}.$$

If C is a linear subspace of $\mathbb{F}^n$ then we denote the orthogonal complement of C in $\mathbb{F}^n$ by $C^\perp$, also called the dual of C.

$$C^{\perp} := \{\mathbf{b} \in \mathbb{F}^n \mid <\mathbf{b}, \mathbf{c}> = 0 \text{ for all } \mathbf{c} \in C\},$$

where $<\mathbf{b}, \mathbf{c}> = \sum b_i c_i$ for $b, c \in \mathbb{F}^n$.

We can add and multiply elements of $\mathbb{F}^n$ coordinatewise

$$(\mathbf{v} + \mathbf{w})_i = v_i + w_i$$

$$(\mathbf{v} * \mathbf{w})_i = v_i w_i.$$

For two subsets A and B of $\mathbb{F}^n$ we denote by $A * B$ the set

$$A * B = \{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A, \mathbf{b} \in B\}.$$

§1. The decoding problem

Let C be a code in $\mathbb{F}^n$. We say that C is *completely decoded* if we can find a map D

$$D : \mathbb{F}^n \to C$$

such that

$$d(D\mathbf{w}, \mathbf{w}) = d(C, \mathbf{w}) \text{ for all } \mathbf{w} \in \mathbb{F}^n.$$

In particular is $D\mathbf{c} = \mathbf{c}$ for all $\mathbf{c} \in C$.
This method is called *maximum likelyhood decoding* and is based on the assumption that the probability that an error will take place at i is the same for all i.
The problem: "with input the pair $(C, \mathbf{w})$, where C is a code in $\mathbb{F}^n$ and $\mathbf{w}$ a word in $\mathbb{F}^n$, and output $\mathbf{c} \in C$, such that $d(\mathbf{c}, \mathbf{w}) = d(C, \mathbf{w})$", is an NP-complete problem [Berlekamp, Mc Eliece, Van Tilborg]. But it is not known whether there is an algorithm $\mathbf{A}_C$ with input $\mathbf{w}$ and output $\mathbf{c} \in C$ of minimum distance to $\mathbf{w}$, such that $\mathbf{A}_C$ is polynomial in memory space and computing time in n, where $n = d(C)$. Put it differently: it is feasible that it takes a research laboratory a lot of time and work to produce a device for a given code C, which decodes C completely in such a way that it works efficiently for all its costumers.

Let C be a linear code in $\mathbb{F}^n$. Define for $\mathbf{w} \in \mathbb{F}^n$ and $v \in C^{\perp}$ the syndrome of $\mathbf{w}$ with respect to $\mathbf{v}$.

$$s(\mathbf{w}, \mathbf{v}) := <\mathbf{w}, \mathbf{v}>.$$

Define the linear map

$$s : \mathbb{F}^n \to (C^{\perp})^V$$

$$\mathbf{w} \mapsto (\mathbf{v} \mapsto s(\mathbf{w}, \mathbf{v})).$$

We call $s(\mathbf{w})$ the *syndrome of* $\mathbf{w}$ and s the *syndrome map*.

Remark that $\mathbf{w}$ is a codeword of C if and only if $s(\mathbf{w}) = 0$. If $\mathbf{w}$ is a word with error $\mathbf{e}$, that is to say $\mathbf{w} = \mathbf{c} + \mathbf{e}$ with $\mathbf{c} \in C$, then $s(\mathbf{w}) = s(\mathbf{e})$.
Thus we have an exact sequence of vector spaces over $\mathbb{F}$

$$0 \to C \to \mathbb{F}^n \xrightarrow{s} (C^\perp)^V \to 0$$

that is to say $\operatorname{Ker} s = C$ and s is surjective, since $\dim (C^\perp)^V = n - \dim C$.
And we see that there is a one-to-one correspondence between syndromes in $(C^\perp)^V$ and cosets of C in $\mathbb{F}^n$. A *coset leader* is an element of a coset of C of minimum weight.
A complete decoding algorithm $\mathbf{A}_C$ could consist of a memory of a complete set of coset leaders. It searches among these coset leaders the unique $\mathbf{w}_0$ with the property $s(\mathbf{w}_0) = s(\mathbf{w})$ and $\mathbf{w}$ is decoded by $\mathbf{w} - \mathbf{w}_0$. But $\mathbf{A}_C$ needs a memory of q^{n-k} coset leaders, which grows exponentially in $n - k$.

Remark that the restriction of s to $B(C, e)$ is injective

$$s : B(C, e) \to (C^\perp)^V$$

, where $e = \lfloor \frac{1}{2}(d-1) \rfloor$.
Let $t \leq e$ then a *t-error correcting* algorithm is a method which sends $\mathbf{w} \in \mathbb{F}^n$ to the unique code word $\mathbf{c}$ with $\mathbf{w} = \mathbf{c} + \mathbf{e}$ if $\mathbf{w} \in B(C, t)$ and detects when $\mathbf{w}$ is not in $B(C, t)$. We will be concerned with t-error correcting algorithms and not with complete decoding algorithms.

§2. t-error locating pairs

Let A, B and C be linear codes in $\mathbb{F}^n$. Define the *error locator map* $E_{\mathbf{w}}$ by

$$E_{\mathbf{w}} : A \to B^V$$

$$\alpha \mapsto (\mathbf{b} \mapsto s(\mathbf{w}, \mathbf{a} * \mathbf{b})).$$

Now suppose

$$A * B \subseteq C^\perp.$$

(2.1) If w is a word with error e then $E_{\mathbf{w}} = E_{\mathbf{e}}$.

(2.2) Define for a subset I of $\underline{n}$

$$A(I) := \{\mathbf{a} \in A \mid a_i = 0 \text{ for all } i \in I\}.$$

(2.3) If $\mathbf{w}$ is a word with error supported at I then $\operatorname{Ker} E_{\mathbf{w}}$ contains $A(I)$.
The inclusion of $B(I) \to B$ induces a dual map $B^V \to B(I)^V$.

(2.4) The following sequence is a complex of vector spaces over $\mathbb{F}$

$$0 \to A(I) \to A \xrightarrow{E_w} B^V \to B(I)^V \to 0$$

, that is to say the composition of two consecutive maps is zero.

Now we are interested in the case that Ker $E_{\mathbf{w}} = A(I)$. Then $E_{\mathbf{w}}$ can be used to locate the errors of $\mathbf{w}$. Before proving a proposition of that effect we need a lemma.

(2.5) Let I be a subset of $\underline{n}$ with t elements.
Define the map

$$\phi_I : B \to \mathbb{F}^t$$

by $\phi_I(\mathbf{b}) = (b_{i_1}, \cdots, b_{i_t})$, where $I = \{i_1, \cdots, i_t\}$ and $i_1 < \cdots < i_t$.

(2.6) **Lemma.** The following statements are equivalent

i) $d(B^\perp) > t$

ii) codim $B(I) = t$ for every $I \subseteq \underline{n}$ with $| I | = t$

iii) the map ϕ_I surjective for every $I \subseteq \underline{n}$ with $| I | = t$.

Proof. ii) is equivalent with iii), since Ker $\phi_I = B(I)$. ii) implies i) suppose $d(B^\perp) \leq t$. Then there exists a non zero element $\mathbf{y}$ of $B^\perp$ such that $w\,t(\mathbf{y}) \leq t$. Let G be a generating matrix of B. Then $G^T \mathbf{y} = 0$. Hence G has t dependant columns say at the places $i_1, \cdots, i_t$. Let $I = \{i_1, \cdots, i_t\}$. Then $B(I) = \bigcap_{j=1}^{t} B(i_j)$ is the intersection of t dependant hyperplanes, hence codim $B(I) < t$. The converse is proved similarly.

(2.7) **Corollary.** $\dfrac{d-1}{2} \leq C\,R(C) \leq n - d^\perp + 1$

where $d = d(C)$, $d^\perp = d(C^\perp)$ and $C\,R(C)$ is the covering radius of C.

Proof. The first inequality is well known. The second too? Let $t = d^\perp - 1$. Then $d(C^\perp) > t$. Hence the map $\phi_I : C \to \mathbb{F}^t$ is surjective with $I = \{1, \cdots, t\}$. Thus for every $\mathbf{w} \in \mathbb{F}^n$ there exists an element $\mathbf{c}$ of C such that $\phi_I(\mathbf{w}) = \phi_I(\mathbf{c})$. Hence $d(\mathbf{w}, \mathbf{c}) \leq n - t$. Therefore $C\,R(C) \leq n - d^\perp + 1$.

(2.8) **Proposition.** If A, B and C are linear codes in $\mathbb{F}^n$ such that $A * B \subseteq C^\perp$ and $d(B^\perp) > r$ and $\mathbf{w}$ is a word with r errors supported at I then

$$\text{Ker}\, E_w = A(I).$$

Proof. We already noticed that $A(I) \subseteq \text{Ker}\, E_{\mathbf{w}}$ in (2.3). Let $\mathbf{w}$ be a word with r errors supported at I that is to say $\mathbf{w} = \mathbf{c} + \mathbf{e}$ with $\mathbf{c} \in C$ and $I = \text{supp}\,\mathbf{e}$. The map ϕ_I is surjective by Lemma (2.6),

since $d(B^{\perp}) > r$. So there exists a basis $\mathbf{b}_1, \cdots, \mathbf{b}_l$ of B such that $\mathbf{b}_{j,i_k} = \delta_{j,k}$ for $1 \leq j, k \leq r$, where $I = \{i_1, \cdots, i_r\}$.
If $\mathbf{a} \in \operatorname{Ker} E_{\mathbf{w}}$ then $E_{\mathbf{w}}(\mathbf{a}) = 0$ hence

$$0 = s(\mathbf{w}, \mathbf{a} * \mathbf{b}_j) = s(\mathbf{e}, \mathbf{a} * \mathbf{b}_j) = \sum_{k=1}^{r} \mathbf{e}_{i_k} \mathbf{a}_{i_k} \mathbf{b}_{j,i_k} = \mathbf{e}_{i_j} \mathbf{a}_{i_j}$$

for all $j = 1, \cdots, r$. Thus $\mathbf{a}_i = 0$ for all $i \in I$, since $e_i \neq 0$ for all $i \in I = \operatorname{supp}(\mathbf{e})$. Therefore $\mathbf{a} \in A(I)$. This proves the proposition.

(2.9) Let $\mathbf{a}$ be an element of $\mathbb{F}^n$ and $z(\mathbf{a}) = \{j_1, \cdots, j_r\}$.
Let $s_{\mathbf{a}}$ be the restriction of the map s to the coordinates $j_1, \cdots, j_r$, that is to say

$$s_{\mathbf{a}} : \mathbb{F}^r \to (C^{\perp})^V$$

$$\mathbf{v} \mapsto (y \mapsto \sum_{i=1}^{r} v_i y_{i_1}).$$

Define the projection map

$$\pi_{\mathbf{a}} : \mathbb{F}^n \to \mathbb{F}^r$$

$$\mathbf{w} \mapsto (w_{j_1}, \cdots, w_{j_r}).$$

Define the inclusion map

$$i_{\mathbf{a}} : \mathbb{F}^r \to \mathbb{F}^n$$

by

$$i_{\mathbf{a}}(\mathbf{v})_j := \begin{cases} v_i & \text{if } j = j_i \text{ for some } 1 \leq i \leq r \\ 0 & \text{otherwise.} \end{cases}$$

Then $\pi_{\mathbf{a}} \circ i_{\mathbf{a}}$ is the identity map on $\mathbb{F}^r$ and $s_{\mathbf{a}} = s \circ i_{\mathbf{a}}$.

(2.10) **Proposition.** Let A and C be linear codes in $\mathbb{F}^n$.
Let $\mathbf{w} \in \mathbb{F}^n$. Suppose $\mathbf{w} = \mathbf{c} + \mathbf{e}$ and $\mathbf{c} \in C$ and $wt(\mathbf{e}) = d(\mathbf{w}, C)$. Let $\mathbf{a}$ be an element of A. If $\operatorname{supp}(\mathbf{e}) \subseteq z(\mathbf{a})$ then the equation $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has a solution $\pi_{\mathbf{a}}(\mathbf{e})$. If moreover $n < d(A) + d(C)$ then this solution is unique.

Proof. If $\operatorname{supp}(\mathbf{e}) \subseteq z(\mathbf{a})$ then $i_{\mathbf{a}} \circ \pi_{\mathbf{a}}(\mathbf{e}) = \mathbf{e}$. Hence

$$s_{\mathbf{a}}(\pi_{\mathbf{a}}(\mathbf{e})) = s(i_{\mathbf{a}} \circ \pi_{\mathbf{a}}(\mathbf{e})) = s(\mathbf{e}) = s(\mathbf{w}).$$

Therefore $\pi_{\mathbf{a}}(\mathbf{e})$ is a solution of the equation $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$. If moreover $n < d(A) + d(C)$ and $\mathbf{x}$ is a solution then

$$s(i_{\mathbf{a}}(\mathbf{x})) = s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w}) = s(\mathbf{e}).$$

Hence $s(i_{\mathbf{a}}(\mathbf{x}) - \mathbf{e}) = 0$, so $i_{\mathbf{a}}(\mathbf{x}) - \mathbf{e} \in C$. Both $i_{\mathbf{a}}(\mathbf{x})$ and $\mathbf{e}$ are supported at $z(\mathbf{a})$. Thus

$$wt(i_{\mathbf{a}}(\mathbf{x}) - \mathbf{e}) \leq \#\, z(\mathbf{a}) \leq n - d(A) < d(C).$$

So $i_{\mathbf{a}}(\mathbf{x}) - \mathbf{e} = 0$. Hence $\pi_{\mathbf{a}}(\mathbf{e}) = \pi_{\mathbf{a}} \circ i_{\mathbf{a}}(\mathbf{x}) = \mathbf{x}$. Therefore the equation $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has the unique solution $\pi_{\mathbf{a}}(\mathbf{e})$. This proves the proposition.

(2.11) **Definition.** Let A, B and C be linear codes in $\mathbb{F}^n$. We call (A, B) a *t-error locating pair* for C if

1) $A * B \subseteq C^{\perp}$

2) $k(A) > t$

3) $d(B^{\perp}) > t$

If moreover

4) $n < d(A) + d(C)$

then we call (A, B) a *t-error correcting pair* for C.

(2.12) **Algorithm.**

0. Begin.

1.1. Compute Ker $E_{\mathbf{w}}$.

1.2. If Ker $E_{\mathbf{w}} = 0$ then goto 3.2.

1.3. If Ker $E_{\mathbf{w}} \neq 0$ then choose a non zero element $\mathbf{a}$ of Ker $E_{\mathbf{w}}$.

2.1. Computation of a solution of $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$.

2.2. If $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has no or more than one solution then goto 3.2.

2.3. If $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has the unique solution $\mathbf{x}_0$ then compute $wt(\mathbf{x}_0)$.

2.4. If $wt(\mathbf{x}_0) > t$ then goto 3.2.

3.1. Print: "The received word is decoded by";
Print: $\mathbf{w} - i_{\mathbf{a}}(\mathbf{x}_0)$; goto 4.

3.2. Print: "The received word has more than t errors".

4. End.

(2.13) **Theorem.** If (A, B) is a t-error correcting pair for C and $t \leq \frac{1}{2}(d-1)$ then algorithm (2.12) corrects t errors with complexity $O(n^3)$.

Proof. Let $r = d(w, C)$. Then there exist $\mathbf{c} \in C$ and $\mathbf{e}$ such that $\mathbf{w} = \mathbf{c} + \mathbf{e}$ and $wt(\mathbf{e}) = r$. Let supp$(\mathbf{e}) = I$. If Ker $E_{\mathbf{w}} = 0$ then $r > t$, since $A(I) = \bigcap_{i \in I} A(i)$ is the intersection of r hyperplanes in A

and dim $A > t$ and this intersection is contained in Ker $E_{\mathbf{w}}$. Hence w has more than t errors.
Now suppose Ker $E_{\mathbf{w}} \neq 0$ and **a** is a non zero element of Ker $E_{\mathbf{w}}$.
If the equation $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has no solution or more than one solution then w has more than t errors, since otherwise $r \leq t$, so Ker $E_{\mathbf{w}} = A(I)$ by Proposition (2.8). So supp(**e**) $\subseteq z(\mathbf{a})$ and therefore $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has the unique solution $\pi_{\mathbf{a}}(\mathbf{e})$ by Proposition (2.10).
If the equation $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$ has the unique solution $\mathbf{x}_0$ then $\mathbf{w} - i_{\mathbf{a}}(\mathbf{x}) \in C$ and $\mathbf{w} = (\mathbf{w} - i_{\mathbf{a}}(\mathbf{x})) + i_{\mathbf{a}}(\mathbf{x})$. If $w\,t(i_{\mathbf{a}}(\mathbf{x})) > t$ then w has more than t errors. Since otherwise $r \leq t$ and $\mathbf{e} - i_{\mathbf{a}}(\mathbf{x}) \in C$. Hence $w\,t(\mathbf{e} - i_{\mathbf{a}}(\mathbf{x})) \leq 2t < d$, so $\mathbf{e} = i_{\mathbf{a}}(\mathbf{x})$. This is in contradiction with the assumption $w\,t(i_{\mathbf{a}}(\mathbf{x})) > t$.
As for the complexity. In the algorithm one has to compute a matrix for $E_{\mathbf{w}}$ with respect to bases for A and B^V. One has to compute a kernel of $E_{\mathbf{w}}$. This amounts to a set of at most n linear equations in at most n variables. The same holds for solving the equation $s_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{w})$. One has to locate zeros of a vector and one has to compute the weight of a vector. All these subroutines have complexity at most $O(n^3)$, see [?].

Questions.

1) Does any code C have a $\lfloor \frac{1}{2}(d-1) \rfloor$ error correcting pair? Or is there an a priori bound on t in terms of the parameters of the code, such that C has a t-error correcting pair.
2) Does any MDS code C have a $\lfloor \frac{1}{2}(d-1) \rfloor$ error correcting pair?

§3. Decoding algebraic geometric codes

In this section we show that an algebraic geometric code on a curve of genus g has a t-error correcting pair with $t = \lfloor \frac{1}{2}(d-1-g) \rfloor$, where g is the genus of the curve. Altough the proof is trivial now one must realize that the idea of an error correcting pair and its properties are hidden in the papers of Skorobogatov and Vlădut [15], Justesen et all [12] back to the papers on decoding BCH codes.

For the theory of algebraic geometric codes we refer to [3], [6], [7], [8], [9], [13]. We follow the notations of [6].

Let X be an absolutely irreducible non singular projective curve defined over $\mathbb{F}$ of genus g. Let $P_1, \cdots, P_n$ be points of X which are rational over $\mathbb{F}$. Let D be the divisor defined by $D = P_1 + \cdots + P_n$. Suppose supp $G \cap$ supp $D = \emptyset$.
Consider the map

$$\alpha^* : \Omega(G - D) \rightarrow \mathbb{F}^n$$

$$w \mapsto (\mathrm{res}_{P_1}(w), \cdots, \mathrm{res}_{P_n}(w)).$$

The code $C^*(D, G)$ is by definition the image of α^* and its dimension we denote by k^*. If $m > 2g-2$ then α^* is injective and $k^* = \dim \Omega(G-D)$, which is at least $n-m+g-1$, equality holds if moreover $m < n$. The minimum distance is at least $m-2g+2$ and we call if the designed minimum distance and denote if by d^*.
By the residue theorem, the dual code $C(D, G)$ of $C^*(D, G)$ is obtained as the image of the map

$$\alpha : L(G) \to \mathbb{F}^n$$

$$f \mapsto (f(P_1), \cdots, f(P_n)).$$

If $m < n$ then α is injective and the dimension of $C(D, G)$ is equal to $\dim L(G)$, which is at least $m+1-g$, equality holds if $m > 2g-2$. The minimum distance is at least $n-m$.

The assumption that $\mathrm{supp}\, G \cap \mathrm{supp}\, D = \emptyset$ is not realy necessary, if one uses the sheaf construction, but then the code is only defined up to generalized equivalence. Two codes A and B in $\mathbb{F}^n$ are called generalized equivalent or isometric, if there exists a permutation $\sigma \in S_n$ and $\lambda_1, \cdots, \lambda_n \in \mathbb{F}^n$ such that $B = \{(\lambda_1 c_{\sigma(1)}, \cdots, \lambda_n c_{\sigma(n)}) \mid c \in A\}$.

For every code $C^*(D, G)$ there exist a rational form ω with simple poles at P_i and residue 1 at all P_i such that $C^*(D, G) = C(D, K+D-G)$ with K the divisor of ω, by Lemma (3.5) of [6]. Hence it is enough to consider only the codes of the form $C^*(D, G)$.

(3.1) **Theorem.** Let F be a divisor with support disjoint from D. Let $A = C(D, F)$, $B = C(D, G-F)$ and $C = C^*(D, G)$. Then

1) $A * B \subseteq C^{\perp}$.
2) If $t + g \leq \deg F < n$ then $k(A) > t$.
3) If $\deg(G-F) > t + 2g - 2$ then $d(B^{\perp}) > t$ and $n < d(A) + d(C)$.

(3.2) **Corollary.** If F is a divisor with support disjoint from D such that $t + g \leq \deg F < n$ and $\deg(G-F) > t + 2g - 2$ then $(C(D, F), C(D, G-F))$ is a t-error correcting pair for $C^*(D, G)$.

Proof of Theorem (3.1).

1) If $\mathbf{a} \in A$ and $\mathbf{b} \in B$ then there exist $f \in L(F)$ and $g \in L(G-F)$ such that $a_i = f(P_i)$ and $b_i = g(P_i)$ for all $i = 1, \cdots, n$. Thus $\mathbf{a}_i \mathbf{b}_i = fg(P_i)$. But $f \in L(F)$ and $g \in L(G-F)$ implies $fg \in L(G)$. Thus $a * b \in C(D, G)$ and $C(D, G)$ is the dual of $C^*(D, G)$.
2) If $t + g \leq \deg F < n$ then $k(A) = \dim L(F) \geq t + 1$ by Riemann-Roch.

3) Now $B^{\perp} = C^*(D, G-F)$ and $\deg(G-F) > t+2g-2$, hence $d(B^{\perp}) \geq \deg(G-F) - 2g + 2 > t$.

Further

$$d(A) + d(C) \geq (n - \deg F) + (m - 2g + 2)$$

$$= n + \deg(G-F) - 2g + 2 > n + t \geq n.$$

This proves the theorem.

(3.3) **Theorem.** Every algebraic geometric code $C^*(D, G)$ of designed minimum distance d^* on a curve of genus g has a t-error correcting pair with $t = \lfloor \frac{1}{2}(d-1-g) \rfloor$ if $2g-2 < m \leq n+2g-2$.

Proof. Let $F_1 = (t+g)P_1$. There exists a rational function f such that $v_{P_1}(f) = t+g$ and $v_{P_i}(f) = 0$ for all $i = 2, \cdots, n$, [2]. Let $F = F_1 - (f)$ then $\deg F = \deg F_1 = t+g$ and $v_{P_i}(F) = 0$ for all $i = 1, \cdots, n$. That is to say F is a divisor of degree $t+g$ with support disjoint from D. Now $t = \lfloor \frac{1}{2}(d^*-1-g) \rfloor$ and $d^* = m - 2g + 2$. Further $\deg(G-F) = m - (t+g) > t + 2g - 2$. Moreover $m \leq n + 2g - 2$ hence $n > t + g$. Thus there exists a divisor with the properties we need in order to apply Corollary (3.2). Therefore there exists a t-error correcting pair for $C^*(D, G)$.

§4. Decoding subfield subcodes

In this section we investigate how we can use a t-error locating pair for C for decoding a subfield subcode of C.

Let $\mathbb{F}$ be a finite field and $\mathbb{F}_0$ a subfield of $\mathbb{F}$. Let C be a linear code in $\mathbb{F}^n$. We denote the subfield subcode $C \cap \mathbb{F}_0^n$ by C_0.

Let $s^0 : \mathbb{F}_0^n \to ((C_0)^{\perp})^{\vee}$ be the syndrome map of C_0. Let $i_{\mathbf{a}}^0 : \mathbb{F}_0^r \to \mathbb{F}_0^n$ and $\pi_{\mathbf{a}}^0 : \mathbb{F}_0^n \to \mathbb{F}_0^r$ be the restriction of $i_{\mathbf{a}}$ and $\pi_{\mathbf{a}}$ to $\mathbb{F}_0^r$ and $\mathbb{F}_0^n$ respectively for an element $\mathbf{a}$ of $\mathbb{F}^n$ with r zeros. Let $s_a^0 = s^0 \circ i_a^0$.

(4.1) **Proposition.** Let A and C be linear codes in $\mathbb{F}^n$. Let $\mathbf{w} \in \mathbb{F}_0^n$. Suppose $\mathbf{w} = \mathbf{c} + \mathbf{e}$ and $\mathbf{c} \in C_0$ and $wt(\mathbf{e}) = d(\mathbf{w}, C_0)$. Let $\mathbf{a}$ be an element of A. If $\mathrm{supp}(\mathbf{e}) \subseteq z(\mathbf{a})$ then the equation $s_{\mathbf{a}}^0(\mathbf{x}) = s^0(\mathbf{w})$ has a solution $\pi_{\mathbf{a}}^0(\mathbf{e})$. If moreover $n < d(A) + d(C_0)$ then this solution is unique.

The proof is verbatim the same as the proof of Proposition (2.10) if we replace s, $s_{\mathbf{a}}$, $i_{\mathbf{a}}$ and $\pi_{\mathbf{a}}$ by s^0, $s_{\mathbf{a}}^0$, $i_{\mathbf{a}}^0$ and $\pi_{\mathbf{a}}^0$ respectively.

(4.2) **Definition.** Let A, B and C be linear codes in $\mathbb{F}^n$. We call (A, B) a t-error correcting pair

for C_0 if $(A\ ,\ B)$ is a t-error locating pair for C and if moreover $n < d(A) + d(C_0)$.

(4.3) **Remark.** If $(A\ ,\ B)$ is a t-error correcting pair for C then it is also a t-error correcting pair for every subfield subcode C_0 of C.

(4.4) **Algorithm.**

0. Begin

1.1. Compute Ker $E_{\mathbf{w}}$.

1.2. If Ker $E_{\mathbf{w}} \neq 0$ then choose a non zero element $\mathbf{a}$ of Ker $E_{\mathbf{w}}$.

2.1. Computation of a solution of $s^0_{\mathbf{a}}(\mathbf{x}) = s^0(\mathbf{w})$.

2.2. If $s^0_{\mathbf{a}}(\mathbf{x}) = s^0(\mathbf{w})$ has no or more than one solution then goto 3.2.

2.3. If $s^0_{\mathbf{a}}(\mathbf{x}) = s^0(\mathbf{w})$ has the unique solution $\mathbf{x}_0$ then compute $wt(\mathbf{x}_0)$.

2.4. If $wt(\mathbf{x}_0) > t$ then goto 3.2.

3.1. Print: "The received word is decoded by";
Print: $\mathbf{w} - i^0_a(\mathbf{x}_0)$; goto 4.

3.2. Print: "The received word has more than t errors".

4. End.

(4.5) **Theorem.** If $(A\ ,\ B)$ is a t-error correcting pair for C_0 and $t \leq \frac{1}{2}(d(C_0) - 1)$ then Algorithm (4.4) corrects t errors with complexity $O(n^3)$.

The proof is the same as the proof of Theorem (2.13).

§5. Decoding cyclic codes beyond the designed error capability

Let $\mathbf{A}$ and $\mathbf{B}$ be two matrices of sizes $(k \times n)$ and $(l \times n)$ respectively. Let $\mathbf{A} * \mathbf{B}$ be the $(kl \times n)$ matrix with rows $\mathbf{a}_i * \mathbf{b}_j$ where $\mathbf{a}_i$, $1 \leq i \leq k$ and $\mathbf{b}_j$, $1 \leq j \leq l$ are the rows of $\mathbf{A}$ and $\mathbf{B}$ respectively.

(5.1) **Lemma.** Let A and B be two linear codes in $\mathbb{F}^n$ with generator matrices $\mathbf{A}$ and $\mathbf{B}$ respectively. Then $A * B \subseteq C^{\perp}$ if and only if $\mathbf{A} * \mathbf{B}$ is part of a parity check matrix of C.

Proof. Trivial.

Let $\mathbb{F}_0 = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_{q^n}$ and β a primitive n^{th} root of unity

(5.2) **Notation.** Let V and W be subsets of $\{1\ ,\ \beta\ ,\ \cdots\ ,\ \beta^{n-1}\}$. Define

$$VW = \{vw \mid v \in V \text{ and } w \in W\}.$$

(5.3) **Notation.** Define the matrix $\mathbf{M}(V)$ by

$$\mathbf{M}(V) = \begin{pmatrix} 1 & \beta^{i_1} & \cdots & \beta^{(n-1)i_1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{i_k} & \cdots & \beta^{(n-1)i_k} \end{pmatrix},$$

where $V = \{\beta^{i_1}, \cdots, \beta^{i_k}\}$ and $0 \le i_1 < \cdots < i_k \le n-1$.

(5.4) **Lemma.** Let A and B be linear codes in $\mathbb{F}^n$ with generator matrices $\mathbf{M}(V)$ and $\mathbf{M}(W)$ respectively for subsets V and W of $\{1, \beta, \cdots, \beta^{n-1}\}$. Let C be the linear code in $\mathbb{F}^n$ with parity check matrix $\mathbf{M}(VW)$. Then $A * B \subseteq C^{\perp}$.

Proof. $\mathbf{M}(V) * \mathbf{M}(W)$ is also a parity check matrix for C. Hence $A * B \subseteq C^{\perp}$ by Lemma (5.1).

Let C_0 be a cyclic code of length n over $\mathbb{F}_0$.
$V \subseteq \{1, \beta, \cdots, \beta^{n-1}\}$ is called a defining set of C_0 if

$$C_0 = \{\mathbf{c} \in \mathbb{F}_0^n \mid \sum_{i=0}^{n-1} \mathbf{c}_i v^i = 0 \text{ for all } v \in V\}.$$

(5.5) **Theorem (BCH).** Let C_0 be a cyclic code with defining set V containing $\{\beta^{i+1}, \cdots, \beta^{i+\delta-1}\}$. Then $d(C_0) \ge \delta$.

(5.6) **Theorem (Hartmann-Tzeng).** Let C_0 be a cyclic code with defining set V containing $\{\beta^{i+jl+la} \mid 1 \le j \le \delta-1, 0 \le l \le s\}$, where $gcd(a, n) = 1$. Then $d(C_0) \ge \delta + s$.

(5.7) **Notation.** Let $V = \{\beta^{i}, \cdots, \beta^{i_k}\}$, where $0 \le i_1 < \cdots < i_k \le n-1$. Then

$$\overline{V} = \{\beta^{i} \mid i_1 \le i \le i_k\}.$$

(5.8) **Theorem (Roos).** Let V be a defining set of a cyclic code with minimum distance d_V. Let W be a set of n^{th} roots of unity such that $|\overline{W}| \le |W| + d_V - 2$. Then the cyclic code C_0 with defining set containing VW has minimum distance $d(C_0) \ge |W| + d_V - 1$.

The BCH, Hartmann-Tzeng and Roos bound can be proved by looking at the rank of $(\mathbf{M}(V) * \mathbf{M}(W))_I$, see Van Lint and Wilson [14].

(5.9) **Theorem.** Let V be the defining set of a cyclic code containing $\delta - 1$ consecutive elements. Let W be a set of roots of unity. Let e be a natural number such that $e < \delta - 1$, $|\overline{W}| \le |W| + \delta - e - 2$ and $e \le \frac{1}{2}(|W| + \delta - 2)$. Then the cyclic code C_0 with defining set containing VW has minimum distance $d(C_0) \ge |W| + \delta - 1$ and C_0 has an e-error correcting

pair.

Proof. The statement about the minimum distance is the content of Roos' Theorem. V contains the set $\{\beta^{i+1}, \cdots, \beta^{i+\delta-1}\}$. Let $V_A = \{\beta^{i+1}, \cdots, \beta^{i+e+1}\}$ and let A be the linear code in $\mathbb{F}^n$ with generator matrix $\mathbf{M}(V_A)$, then $d(A^\perp) \geq e+2$ by the BCH bound and $k(A^\perp) = n-(e+1)$, hence $A^\perp$ is an MDS code with parameters $[n, n-(e+1), e+2]$, by the Singleton bound. Thus A is an MDS code with parmeters $[n, e+1, n-e]$. In particular $k(A) = e+1$.
Let $V_B = \{\beta^j \mid 0 \leq j \leq \delta-e-2\}$. Furthermore $|\overline{W}| \leq |W| + \delta - e - 2$. Let B be the linear code in $\mathbb{F}^n$ with generator matrix $\mathbf{M}(V_B W)$ then $\mathbf{M}(V_B W)$ is a parity check matrix for $B^\perp$, hence $d(B^\perp) \geq |W| + \delta - e - 2$, by the Roos' bound (5.8).
Now $V_A V_B W \subseteq V W$ is contained in the defining set of C and $\mathbf{M}(V_A)$ and $\mathbf{M}(V_B W)$ are the generator matrices of A and B respectively. Hence $A * B \subseteq C^\perp$, by Lemma (5.4).
Finally $d(A) + d(C_0) \geq n - e + |W| + \delta - 1 > n - e + 2e \geq n$. Thus (A, B) is an e-error correcting pair for C_0. This proves the theorem.

(5.11) **Remark.** Feng and Tzeng [5] give a decoding algorithm in the situation of Theorem (5.10), but with the weaker assumption $|\overline{W}| \leq W + \delta - 2$ instead of $|\overline{W}| \leq |W| + \delta - e - 2$. Elia [4] and Janssen and Van Tilborg [10] [11] found more decoding procedures bases on error location which decode beyond the designed error capability.

References

[1] E.R. Berlekamp, R.J. Mc Eliece, H.C.A. van Tilborg: On the inherent intracibility of certain coding problems, IEEE vol IT-**24** (3) 1978, 384-386.

[2] C. Chevalley: Introduction to the theory of algebraic functions of one variable, Math. Surveys vol VI, Am. Math. Soc., 1951.

[3] Y. Driencourt and J.F. Michon: Rapport sur les codes géométriques, oktober 1986.

[4] M. Elia: Algebraic decoding of the (23, 12, 7) Golay code, IEEE Transactions vol IT-**33** (1) 1987,

[5] G.L. Feng and K.K. Tzeng: A generalized iterative algorithm for decoding cyclic codes beyond the BCH bound, IEEE Int. Symp. on Information Theory, Quebec, Canada 1983.

[6] G. van der Geer and J.H. van Lint: Introduction to coding theory and algebraic geometry, Birkhäuser, 1988.

[7] V.D. Goppa: Codes associated with divisors, Problemy Peredachi Informatsii, vol **13** (1) (1977), 33-39.

[8] V.D. Goppa: Codes on algebraic curves, Soviet Math. Dokl. **24** (1) (1983), 75-91.

[10] J.C.M. Janssen: Decoding linear cyclic codes beyond the BCH bound, Master's Thesis, University of Technology, Eindhoven, april 1988.

[11] J.C.M. Janssen and H.C.A. van Tilborg: Algebraic decoding e_{BCH} of some binary cyclic codes, when $e > e_{BCH}$, preprint TUE, 1988.

[12] J. Justesen, K.J. Larsen, H.E. Jensen, A. Havemose, T. Hϕholdt: Construction and decoding of a class of algebraic geometry codes, preprint Techn. Un. Kopenhagen 1988.

[13] G. Lachaud: Les codes géométriques de Goppa, Séminaire Bourbaki, no. **641** (1985).

[14] J.H. van Lint and R.M. Wilson: On the minimum distance of cyclic codes, IEEE vol IT-**32** (1) (1986), 23-40.

[15] A.N. Skorobogatov and S.G. Vlădut: On the decoding of algebraic geometric codes, Inst. for Problems of Information Transmission (1988).