

Decoding Linear Codes

Iwan M. Duursma
Eindhoven University of Technology *

March, 1994

Abstract

We mention four recent results, none of which has appeared yet. They come from different sources. The purpose of these notes is to present them in a short way. Two results concern the generalization of the Roos-bound from cyclic codes to more general linear codes. Two others concern the use of majority coset decoding to the decoding of cyclic codes.

*Supported by NWO, The Netherlands. Prepared for a visit to INRIA, Paris, March 18-22. Current address: LMD Equipe ATI, Case 930, 13288 MARSEILLE CEDEX 9. E-mail: duursma@lmd.univ-mrs.fr.

Introduction

(0.1) Needless to say that there has been much progress over the past few years on the decoding of linear codes. For both cyclic codes and geometric Goppa codes, this yielded better bounds on the minimum distance and improved decoding algorithms. Often the methods split according to two basic ideas. In the words of vanLint and Wilson these are the AB-method and the Shifting-method [5]. In the words of Pellikaan these are error-correcting pairs and error-correcting arrays [6, 7].

The Roos-bound for cyclic codes is an example of the first idea. We give two different generalizations to more general linear codes. They are due to Pellikaan [8] and Duursma respectively.

Majority Coset Decoding is an example of the second idea. Introduced by Feng and Rao, it applies to geometric Goppa codes [3, 1]. In a yet to appear article, Feng and Tzeng show the application to cyclic codes [4]. We discuss their method. We mention two subclasses of cyclic codes defined by Duursma and Kötter [2] to which the method is immediately applicable.

(0.2) The following notation and terminology applies throughout. A code C is a linear subspace of the space of n -tuples over a field F . For a word $\mathbf{c} \in C$, let

$\text{wt}(\mathbf{c})$, Hamming weight of \mathbf{c} .

For a code C , let

$n(C)$, length.
 $k(C)$, dimension.
 $d(C)$, minimum distance.
 $g(C)$, = $n(C) + 1 - k(C) - d(C)$, genus.

For two vectors \mathbf{a} and \mathbf{b} of the same length, let

$\mathbf{a} * \mathbf{b}$, componentwise product.

For two codes A and B of the same length, let

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

For n with $\gcd(n, \text{char } F) = 1$, let

α , primitive n -th root of unity in an extension of F .
 $\alpha(i)$, = $(1, \alpha^i, \alpha^{2i}, \dots, \alpha^{(n-1)i})$.

On the Roos-bound

(1.1) We formulate the original Roos bound [9]. Let the codes A and B be defined as follows, for $i_1 < i_2 < \dots < i_{s+1}$,

$$\begin{aligned} A &= \langle \alpha(i_1), \alpha(i_2), \dots, \alpha(i_{s+1}) \rangle, \\ B &= \langle \alpha(1), \alpha(2), \dots, \alpha(d-1) \rangle. \end{aligned}$$

Let $i_{s+1} - i_1 - s < d - 1$. Then, a code C with $C \perp A * B$ has minimum distance $d(C) \geq d + s$. We claim that the following symmetric version of the

Roos bound holds. Thus, for $i_1 < i_2 < \dots < i_{s+1}$, and $j_1 < j_2 < \dots < j_{r+1}$, let

$$\begin{aligned} A &= \langle \alpha(i_1), \alpha(i_2), \dots, \alpha(i_{s+1}) \rangle, \\ B &= \langle \alpha(j_1), \alpha(j_2), \dots, \alpha(j_{r+1}) \rangle. \end{aligned}$$

Let $i_{s+1} - i_1 - s < r + 1$ and $j_{r+1} - j_1 - r < s + 1$. Then, a word \mathbf{c} with $\mathbf{c} \perp A * B$ has weight $\text{wt}(\mathbf{c}) \leq i_{s+1} - i_1 - s + j_{r+1} - j_1 - r$, or $\text{wt}(\mathbf{c}) \geq r + s + 2$. This version can be obtained with the AB-method for cyclic codes [5]. We include proofs of both claims for the case of general linear codes.

(1.2) We first give a generalization of the asymmetric version, due to Pelikaan [8]. Let $C \perp A * B$, and let

- (0) A is non-degenerate
- (1) $k(A) > a$
- (2) $d(B^\perp) > b$
- (3) $d(A) > n - a - b$

Then $d(C) > a + b$.

(If the conditions hold with $a = b = t$, then t errors can be corrected effectively for the code C . The pair (A, B) is then called a t -error-correcting pair [6])

Proof. Note that $C * A \perp B$. First, assume $\text{wt}(\mathbf{c}) \leq b$. With (0), we obtain a nontrivial word $\mathbf{c} * \mathbf{a} \in B^\perp$ of weight $\text{wt}(\mathbf{c} * \mathbf{a}) \leq b$. A contradiction with (2). Next, assume $b < \text{wt}(\mathbf{c}) \leq a + b$. Let $I^- \subset \text{support}(\mathbf{c}) \subset I^+$, with $\text{card}(I^-) = b$, and $\text{card}(I^+) = a + b$. With (1), we obtain a word \mathbf{a} with zeros at $I^+ \setminus I^-$. For this \mathbf{a} , the vector $\mathbf{c} * \mathbf{a} \in B^\perp$ has support in I^- . By (3), it is non-trivial. A contradiction with (2). \square

(1.3) We next prove a generalization of the symmetric version. Let $\mathbf{c} \perp A * B$, and let $k(A) > g(B)$ and $k(B) > g(A)$. Then

$$\text{wt}(\mathbf{c}) \leq g(A) + g(B), \quad \text{or} \quad \text{wt}(\mathbf{c}) \geq k(A) + k(B).$$

Proof. We combine the inequalities to be proved in (1.4) and (1.5) to obtain

$$\text{wt}(\mathbf{c}) \geq \min\{\text{wt}(\mathbf{c}) - g(A), k(A)\} + \min\{\text{wt}(\mathbf{c}) - g(B), k(B)\}.$$

For the right hand side, four possibilities may occur. Two of these are ruled out by the assumptions and the two given possibilities remain. \square

(1.4) Following vanLint and Wilson [5], the weight of a vector \mathbf{c} with $\mathbf{c} \perp A * B$ is bounded below by

$$\text{wt}(\mathbf{c}) \geq k(\mathbf{c} * A) + k(\mathbf{c} * B).$$

Proof. One constructs mutually orthogonal codes A' and B' of length $\text{wt}(\mathbf{c})$, such that $k(A') = k(\mathbf{c} * A)$ and $k(B') = k(\mathbf{c} * B)$. The sum of the dimensions of orthogonal spaces is at most the dimension of the ambient space. \square

(1.5) The dimension of $\mathbf{c} * A$ is bounded below by

$$k(\mathbf{c} * A) \geq \min\{\text{wt}(\mathbf{c}) - g(A), k(A)\}.$$

Proof. Assume $k(\mathbf{c} * A) < k(A)$. There exists a non-trivial word in A with zeros at the support of \mathbf{c} , and zeros at $k(A) - k(\mathbf{c} * A) - 1$ other coordinates. Thus

$$d(A) \leq n - \text{wt}(\mathbf{c}) - (k(A) - k(\mathbf{c} * A) - 1).$$

Or $k(\mathbf{c} * A) \geq \text{wt}(\mathbf{c}) - g(A)$. \square

(1.6) Consider codes of length $n = q^2 - 1$ over the field $F = GF(q)$. Let the code C be defined by

$$C^\perp = \langle \alpha(0), \alpha(1), \alpha(2), \alpha(q), \alpha(q+1), \alpha(q+2), \alpha(2q), \alpha(2q+1), \alpha(2q+2) \rangle$$

The code C is non-trivial for $q \geq 4$. For words with support among the $q+1$ -roots of unity, the parity checks reduce to

$$\langle \alpha(0), \alpha(1), \alpha(2), \alpha(-1), \alpha(0), \alpha(1), \alpha(-2), \alpha(-1), \alpha(0) \rangle.$$

So, for $q \geq 5$, the code C has an MDS subcode of type $[q+1, q-4, 6]$, and $d(C) \leq 6$. For $q = 4$, an equivalent code is obtained with the dual code

$$C^\perp = \langle \alpha(0), \alpha(2), \alpha(4), \alpha(8), \alpha(10), \alpha(12), \alpha(1), \alpha(3), \alpha(5) \rangle.$$

So, for $q = 4$, we have $d(C) \geq 7$.

(1.7) We apply the results of this section to the code C of (1.6). With

$$\begin{aligned} A &= \langle \alpha(0), \alpha(1), \alpha(2) \rangle, \\ B &= \langle \alpha(0), \alpha(q), \alpha(2q) \rangle, \end{aligned}$$

the bounds (1.2) and (1.3) yield $d(C) > 2 + 3$ and $d(C) \geq 3 + 3$ respectively. Next, let

$$A = B = \langle \alpha(0), \alpha(1), \alpha(q), \alpha(q+1) \rangle.$$

For $q + 1 < 3 + 3$, the bound (1.2) yields $d(C) > 3 + 3$. For $q - 2 < 4$, the bound (1.3) yields $\text{wt}(\mathbf{c}) \leq 2(q - 2)$ or $\text{wt}(\mathbf{c}) \geq 8$. We conclude that,

$$\begin{aligned} q = 4 : & \quad d(C) \geq 8. \\ q = 5 : & \quad d(C) = 6, \text{ and no words of weight seven.} \\ q \geq 7 : & \quad d(C) = 6. \end{aligned}$$

Majority coset decoding of cyclic codes

(2.1) Let A and B be linear codes of dimension d with an ordered basis,

$$\begin{aligned} A &= \langle \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_d \rangle, \\ B &= \langle \mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_d \rangle. \end{aligned}$$

For a vector \mathbf{c} , let

$$S(\mathbf{c}) = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_d \end{pmatrix} \text{diag}(\mathbf{c}) \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_d \end{pmatrix}^T$$

For a given code C , let A and B , and the ordering of their bases, be such that for each $\mathbf{c} \in C$ the entries of $S(\mathbf{c})$ are zero above the back-diagonal. Also, let the entries on the back-diagonal be such that they can all be obtained from any given entry among them.

(2.2) A non-trivial example is obtained with the binary cyclic code C of type $[21, 9, 8]$ that is defined with

$$C^\perp \supset \langle \alpha(0), \alpha(1), \alpha(3), \alpha(7) \rangle.$$

We may choose for A and B

$$\begin{aligned} A &= \langle \alpha(0), \alpha(7), \alpha(11), \alpha(8), \alpha(2), \alpha(1), \alpha(9) \rangle. \\ B &= \langle \alpha(0), \alpha(14), \alpha(16), \alpha(1), \alpha(4), \alpha(11), \alpha(9) \rangle. \end{aligned}$$

With $S_i = \alpha(i) \mathbf{c}^T$, we have

$$S(\mathbf{c}) = \begin{pmatrix} S_0 & S_7 & S_{11} & S_8 & S_2 & S_1 & S_9 \\ S_{14} & S_0 & S_4 & S_1 & S_{16} & S_{15} & - \\ S_{16} & S_2 & S_6 & S_3 & S_{18} & - & - \\ S_1 & S_8 & S_{12} & S_9 & - & - & - \\ S_4 & S_{11} & S_{15} & - & - & - & - \\ S_{11} & S_{18} & - & - & - & - & - \\ S_9 & - & - & - & - & - & - \end{pmatrix}$$

The irrelevant entries are omitted. See (2.6) for two families of examples.

(2.3) For a matrix M , the rank is defined as the dimension of the column space. Ordering the columns from left to right, we may define the rank equivalently as the number of columns that cannot be expressed as a linear combination of previous columns.

As a way to study the rank of a matrix M with unknown entries, we first order and then partition the columns. For the j -th column, let x_j denote the first unknown entry. We assume that the x_j occur in different rows and that the columns are ordered such that $\text{row}(x_j)$ decreases with j . Then, let

- C_0 , the set of columns j that are independent of previous columns.
- C_1 , the set of columns j that are dependent of previous columns for a proper x_j .
- C_∞ , the set of columns j that are dependent of previous columns for any x_j .

Denote the cardinalities of the sets by c_0, c_1 and c_∞ respectively. We have $c_\infty \leq c_0$.

Proof. For the columns C_∞ , we can choose the x_j such that the columns are mutually independent. Still, they are in the span of the columns C_0 . \square

(2.4) We consider the partition of the columns for the matrix $M = S(\mathbf{e})$ in (2.2), for $S_0 = 1, S_1 = 0, S_3 = 1, S_7 = 1$,

$$S(\mathbf{e}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & x_7 \\ 1 & 1 & 0 & 0 & 0 & x_6 & - \\ 0 & 0 & 1 & 1 & x_5 & - & - \\ 0 & 0 & 1 & x_4 & - & - & - \\ 0 & 0 & x_3 & - & - & - & - \\ 0 & x_2 & - & - & - & - & - \\ x_1 & - & - & - & - & - & - \end{pmatrix}$$

We find $C_0 = \{1, 3\}, C_1 = \{2, 4, 6\}, C_\infty = \{5, 7\}$. The proper choices are $x_2 = 0, x_4 = 1$ and $x_6 = 0$. It follows that

$$\begin{aligned} \text{rank } S(\mathbf{e}) &\geq 3, & \text{for } S_9 = 0. \\ \text{rank } S(\mathbf{e}) &\geq 4, & \text{for } S_9 = 1. \\ \text{rank } S(\mathbf{e}) &\geq 5, & \text{for } S_9 \neq 0, 1. \end{aligned}$$

Thus $S_9 = 0$, for $\text{wt}(\mathbf{e}) \leq 3$.

(2.5) For a matrix $M = S(\mathbf{e})$ in general, we partition the columns C_1 into

C_1^+ , the choice for x_j coincides with the actual value of the entry.

C_1^- , the choice for x_j differs from the actual value of the entry.

Let the cardinalities be denoted by c_1^+ and c_1^- respectively. Then, $c_1^+ - c_1^- \geq d - 2\text{wt}(\mathbf{e})$. And, for \mathbf{e} of small weight, the unknown entries on the back-diagonal can be obtained with a majority decision.

Proof. We have $d = c_0 + c_1^+ + c_1^- + c_\infty$, and $\text{rank } S(\mathbf{e}) \geq c_0 + c_1^-$. Combination with $\text{rank } S(\mathbf{e}) \leq \text{wt}(\mathbf{e})$, and $c_\infty \leq c_0$ (2.3) yields

$$d - 2\text{wt}(\mathbf{e}) \leq d - 2\text{rank } S(\mathbf{e}) \leq c_1^+ - c_1^- + c_\infty - c_0 \leq c_1^+ - c_1^-.$$

\square

(2.6) We mention two subclasses of cyclic codes, defined by Duursma and Kötter [2]. Let F be a finite field of characteristic p , and let n be an integer coprime with p . The codes are of length n and defined over the field F . For a power q of p , the classes are defined by

$$C_1(F, n, q, t)^\perp \supset \langle \alpha(1), \alpha(2), \alpha(q+1), \alpha(q^2+1), \dots, \alpha(q^{t-1}+1) \rangle,$$

and

$$C_2(F, n, q, t)^\perp \supset \langle \alpha(0), \alpha(1), \alpha(q+1), \alpha(q^3+1), \dots, \alpha(q^{2t-3}+1) \rangle.$$

Fixing F , n and q , the minimum distance of the codes satisfies

$$d(C_i(t)) \geq \min\{2t+1, d(C_i(\infty))\},$$

for $i = 1, 2$, where ∞ denotes an arbitrary large integer.

Proof. For the first class, let $\mathbf{c} \in C_1(t)$. The matrix $S(\mathbf{c})$ is of the type (2.1), with $d = 2t + 1$, for

$$\begin{aligned} A_1(t) &= \langle \alpha(q^t), \alpha(q^{t-1}), \alpha(q^{t-2}), \dots, \alpha(q^{-t+2}), \alpha(q^{-t+1}), \alpha(1+q^{-t}) \rangle \\ B_1(t) &= \langle \alpha(0), \alpha(q), \alpha(q^2), \dots, \alpha(q^{2t-1}), \alpha(q^{2t}) \rangle \end{aligned}$$

The $2t+1$ syndromes on the back-diagonal are all conjugates of the syndrome $S_{q^{t+1}}$. Either $S_{q^{t+1}} \neq 0$, and $\text{wt}(\mathbf{c}) \geq 2t+1$, or $S_{q^{t+1}} = 0$, and $\mathbf{c} \in C_1(t+1)$. For the second class, let $\mathbf{c} \in C_2(t)$. The matrix $S(\mathbf{c})$ is of the type (2.1), with $d = 2t + 1$, for

$$\begin{aligned} A_2(t) &= \langle \alpha(0), \alpha(q^{2t-2}), \alpha(q^{2t-4}), \dots, \alpha(q^{-2t+4}), \alpha(q^{-2t+2}), \alpha(q^{-1}+q^{-2t}) \rangle \\ B_2(t) &= \langle \alpha(0), \alpha(q), \alpha(q^3), \dots, \alpha(q^{4t-5}), \alpha(q^{4t-3}), \alpha(q^{4t-1}+q^{2t}) \rangle \end{aligned}$$

The $2t+1$ syndromes on the back-diagonal are all conjugates of the syndrome $S_{q^{2t-1+1}}$. Either $S_{q^{2t-1+1}} \neq 0$, and $\text{wt}(\mathbf{c}) \geq 2t+1$, or $S_{q^{2t-1+1}} = 0$, and $\mathbf{c} \in C_2(t+1)$. In both cases the claim on the distance follows with induction. \square

(2.7) As an example, consider the even-weight subcode of the binary Golay code C . It is of the second type with $q = 2$ and $t = 3$, since

$$C^\perp \supset \langle \alpha(0), \alpha(1), \alpha(3), \alpha(9) \rangle$$

The matrix $S(\mathbf{c})$ is defined with

$$\begin{aligned} A &= \langle \alpha(0), \alpha(16), \alpha(4), \alpha(1), \alpha(6), \alpha(13), \alpha(21) \rangle, \\ B &= \langle \alpha(0), \alpha(2), \alpha(8), \alpha(9), \alpha(13), \alpha(6), \alpha(9) \rangle. \end{aligned}$$

And

$$S(\mathbf{c}) = \begin{pmatrix} S_0 & S_{16} & S_4 & S_1 & S_6 & S_{13} & S_{21} \\ S_2 & S_{18} & S_6 & S_3 & S_8 & S_{15} & - \\ S_8 & S_1 & S_{12} & S_9 & S_{14} & - & - \\ S_9 & S_2 & S_{13} & S_{10} & - & - & - \\ S_{13} & S_6 & S_{17} & - & - & - & - \\ S_6 & S_{22} & - & - & - & - & - \\ S_{19} & - & - & - & - & - & - \end{pmatrix}$$

For $S_{33} = S_{10} \neq 0$, the word has distance at least seven. For $S_{10} = 0$, the word is trivial. Three errors can be corrected for the code by using majority coset decoding, similar to (2.4). But in fact the majority decision is superfluous, as it is shown in [2] that $4 \in C_1^+$, for $\text{wt}(\mathbf{e}) \leq 3$.

References

- [1] I.M. Duursma, "Majority coset decoding," *IEEE Trans. Inform. Theory*, vol.IT-39, May 1993.
- [2] I.M. Duursma, and R. Kötter, *Error-locating pairs for cyclic codes*. Eindhoven, Linköping: preprint, 1993.
- [3] G.L. Feng and T.R.N.Rao, "Decoding algebraic geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol.IT-39, January 1993.
- [4] G.L. Feng and K.K. Tzeng, *A new procedure for decoding cyclic and BCH codes up to actual minimum distance*. Lafayette, Bethlehem: preprint, 1993.
- [5] J.H. van Lint and R.M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol.IT-32, pp.23-40, 1986.
- [6] R. Pellikaan, "On decoding by error location and dependent sets of error positions," *Discrete Mathematics*, vol.106-107, pp.369-381, 1992.

- [7] R. Pellikaan, "On the efficient decoding of algebraic-geometric codes," *Eurocode 92*, CISM 339, Springer, pp.231-253, 1993.
- [8] R. Pellikaan, *On the existence of error-correcting pairs*. Eindhoven: preprint, 1994.
- [9] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. Inform. Theory*, vol.IT-29, pp.330-332, 1983.