

A symmetric Roos-bound for general linear codes

Iwan M. Duursma

February 1994

Abstract

We give bounds for the weights of a linear code, by using the generalization to linear codes of the AB -bound for cyclic codes. The latter bound in turn generalizes the Roos-bound for cyclic codes. The bounds are compared with a different generalization of the Roos-bound due to Pellikaan.

Notation 1 For a linear code C , let $n(C)$, $k(C)$, $d(C)$ and $g(C)$ denote its length, dimension, minimum distance and genus respectively. We define the genus ad hoc as $g(C) = n(C) + 1 - k(C) - d(C)$. Thus it is a non-negative integer. When computing weight distributions, a different definition may be preferred. For a word $\mathbf{c} \in C$, let $wt(\mathbf{c})$ denote the Hamming weight of \mathbf{c} . For linear codes A and B of the same length, let $A * B = \{\mathbf{a} * \mathbf{b} : \mathbf{a} \in A, \mathbf{b} \in B\}$, with $\mathbf{a} * \mathbf{b}$ the componentwise product of \mathbf{a} and \mathbf{b} .

The following theorem is the main tool in the AB -method, due to vanLint and Wilson, for proving the minimum distance of cyclic codes.

Theorem 2 *Let $\mathbf{c} \perp A * B$. Then*

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

Proof. One constructs mutually orthogonal codes A' and B' of length $wt(\mathbf{c})$, 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

Lemma 3 (main lemma)

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

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

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

Or

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

□

For words \mathbf{c} of sufficiently large weight, at least one of the dimensions $k(\mathbf{c} * A)$ or $k(\mathbf{c} * B)$ is maximal.

Corollary 4 *Let $\mathbf{c} \perp A * B$, and let $wt(\mathbf{c}) > g(A) + g(B)$. Then*

$$k(\mathbf{c} * A) = k(A), \text{ or } k(\mathbf{c} * B) = k(B).$$

Proof. If both $k(\mathbf{c} * A) < k(A)$ and $k(\mathbf{c} * B) < k(B)$, we obtain $wt(\mathbf{c}) \geq wt(\mathbf{c}) - g(A) + wt(\mathbf{c}) - g(B)$. This contradicts the assumption. □

Lemma 5 *Let $\mathbf{c} \perp A * B$. Then*

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

Proof. Combine the theorem and the lemma. □

Theorem 6 (main theorem) *Let $\mathbf{c} \perp A * B$, and let $k(A) > g(B)$ and $k(B) > g(A)$. Then*

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

Proof. In the inequality of the lemma, four possibilities occur for the right hand side. Two of these are ruled out by the assumptions and the two given possibilities remain. □

The Roos-bound is the special case where A , B and C are cyclic, and $g(B) = 0$. The theorem shows that bounds can still be obtained if both A and B have non-zero genus as long as their genus is not too large.

Example 7 For cyclic codes, the theorem excludes weights in a way similar to the combination of Theorem 5 and Corollary 1 in the paper [Van-Lint and Wilson]. In Example 3 [id.], the code C has zeros at $R \supseteq A'B'$, for

$$\begin{aligned} A' &= \{\alpha^i : 83 \leq i \leq 95\} \cup \{\alpha^i : 98 \leq i \leq 111\} \\ B' &= \{\beta^j : j = -7, 0, 1\}, \quad \beta = \alpha^{16}. \end{aligned}$$

With the sets A' and B' we associate codes A and B in the natural way, such that $C \perp A * B$. The codes have $k(A) = 27$, $g(A) \leq 2$, and $k(B) = 3$, $g(B) \leq 6$. The theorem yields: $wt(\mathbf{c}) \leq 2 + 6$, or $wt(\mathbf{c}) \geq 27 + 3$. Clearly $d(C) \geq 30$.

Example 8 With the Klein quartic, one can construct codes A , B and C over $GF(8)$ of type $[24, 3, 20]$, $[24, 4, 19]$ and $[24, 16, 7]$ respectively. These codes improve on the Goppa bound by one. The codes B and C are the only codes, upto equivalence, with dimension in the range $2, 4, \dots, 18$ that improve on the Goppa bound [Duursma, unpublished]. Let Q_1, Q_2 and Q_3 form a "Wendendreiecke" [Klein]. The defining divisors for the codes B and C are equivalent to $2(Q_1 + Q_2 + Q_3)$ and $6(Q_1 + Q_2 + Q_3)$ respectively. The code A has as defining divisor the intersection divisor of a line with the curve. For the proper divisors, we have $C \perp A * B$. With $k(A) = 3$, $g(A) = 2$, and $k(B) = 4$, $g(B) = 2$, the theorem yields: $wt(\mathbf{c}) \leq 4$, or $wt(\mathbf{c}) \geq 7$. Clearly $d(C) \geq 7$.

Remark 9 Over the field $GF(64)$, the extended code \bar{B} has $g(\bar{B}) = 3$, and the code \bar{C} with $\bar{C} \perp \bar{A} * \bar{B}$ has $d(\bar{C}) = 6$. Thus, after the set of points on the curve that defines the coordinates is extended, the distance equals the Goppa distance. In particular, the Feng and Rao distance of C equals the Goppa distance.

Remark 10 Comparison with $d(C) \geq k(A) + d(B^\perp) - 1$ [Pellikaan].

(In the latter example, it yields $d(C) \geq 6$. Still, with a modification of the corresponding decoding procedure, three errors can be corrected effectively -

more later)

(If the code B has $g(B) = 0$, i.e. is maximum distance separable, the bound agrees with $d(C) \geq k(A) + k(B)$. Otherwise, the latter bound will be better. Unlike Pellikaan's generalization, our bound does not tell how to decode errors effectively - more later)

The author is employed by the Dutch Organization for Scientific Research.
Work address for the year 93/94:

Laboratoire de Mathématiques Discrètes
(163, avenue de Luminy)
Case 930
13288 MARSEILLE CEDEX 9
France

E-mail: duursma@lmd.univ-mrs.fr