

Bounds on the minimum distance of the duals of BCH codes

Daniel Augot, Françoise Levy-dit-Vehel

INRIA, Domaine de Voluceau, BP 105, 78150 Le Chesnay Cedex, France

Abstract — We consider duals of BCH codes of length $p^m - 1$ over $GF(p)$. A lower bound on their minimum distance is found via the adaptation of the Weil bound to cyclic codes. However, this bound is of no significance for roughly half of these codes.

We partially fill this gap by giving a lower bound for an infinite class of duals of BCH codes.

In the second part we present a lower bound obtained with an algorithm due to Massey and Schaub. In the case of binary codes of length 127 and 255, the results are surprisingly higher than all previously known bounds.

I. NOTATIONS AND DEFINITION OF THE CLASS

We consider cyclic codes of length $n = p^m - 1$ over $GF(p)$. A defining-set of a code C is a set $T \subset [0, n]$, such that $\{\alpha^j, j \in T\}$ are the zeroes of the generator polynomial of C , where α is a primitive element in $GF(p^m)$. We call check-set of C a subset J of $[0, n]$, such that the defining-set T^\perp of the dual C^\perp of C is the union of the cyclotomic cosets of the elements of J .

The Mattson-Solomon polynomial of $a \in GF(p)^n$, is the polynomial: $MS_a(Z) = \sum_{i=1}^n A_i Z^{n-i}$, where $A_i = a(\alpha^i)$, $1 \leq i \leq n$.

Definition 1 Let $1 \leq t \leq m$, and $0 \leq i < p - 1$. We define the code $C(t, i)$ to be the dual of the BCH code of length $p^m - 1$ over $GF(p)$, with designed distance $d(t, i) = \sum_{j=1}^a (i+1)p^{m-j} + (1 - \delta_{r,0})$, with $m = at + r$, $0 \leq r < t$, and δ is the Kronecker symbol.

For these duals we shall give an explicit formula for the Weil bound and apply the Roos bound.

II. THE THEORETICAL BOUNDS

For the codes introduced in section 1, the Weil bound adapted by Wolfmann [1] turns into an explicit formula. It is given in assertion 4 of theorem 1 in the binary case, and in assertion 5 of theorem 2 for $p \neq 2$. The other statements come from applying the Roos [Ro] bound, except the third of theorem 1, which is derived from the inclusion in a Reed-Muller code.

Theorem 1 We assume $p = 2$, and we denote by $\delta(t)$, the minimum distance of $C(t, 0)$.

1. for $2 \leq t \leq \frac{m-3}{2}$ (so $m \geq 7$), $\delta(t) \geq 2^{t+1} + 2^t - 4$,
2. for $m \geq 6$, $\delta(\frac{m}{2} - 1) \geq 2^{\frac{m}{2}} - 2$,
3. for $t = \lfloor \frac{m}{2} \rfloor$, $\delta(t) \geq 2^{t+1} - 2^{t-1}$,
4. and for $\frac{m}{2} < t \leq m - 1$, $\delta(t) \geq 2^{m-1} - \frac{2^{m-t}-2}{4} \lfloor 2^{\frac{m-t}{2}} + 1 \rfloor$.

Theorem 2 We assume $p \neq 2$ and $m \geq 4$.

1. For $t = 1$, $\delta(1, i) \geq (z + 2)(p - 1 - i)$, where $z = 0$ if $i \geq \frac{p}{2} - 1$, and z is the largest integer strictly less than $\frac{p}{i+1} - 1$ otherwise.
2. for $2 \leq t < \frac{m-1}{2}$, (so $m \geq 6$),

$$\delta(t, i) \geq (p - i)(p^t - 1 - i)$$
3. for $t = \frac{m-1}{2}$ and $i = 0$, or for $t = \frac{m}{2}$, or $t = \frac{m+1}{2}$ and $i > 0$,

$$\delta(t, i) \geq (p - 1)^2 p^{m-t-2} + p^t - 1 - i$$
4. for $t = \frac{m-1}{2}$ and $0 < i < p - 1$, ($m \geq 5$),

$$\delta(\frac{m-1}{2}, i) \geq (p - 1 - i)p^{\frac{m-3}{2}} + p^{\frac{m-1}{2}} - 1 - i$$
5. for $\frac{m+1}{2} < t \leq m$ or for $t = \frac{m+1}{2}$ and $i = 0$,

$$\delta(t, i) \geq p^{m-1}(p - 1) - \frac{((i+1)p^{m-t}-2)(p-1)}{2p} \lfloor 2p^{\frac{m-t}{2}} \rfloor$$

III. THE ALGORITHMIC METHOD

In order to have a bound for other duals, we use an algorithmic method due to T. Schaub [2] and J. L. Massey for finding a lower bound on the minimum distance of a cyclic code.

Theorem 3 Let $c \in GF(p)^n$, let A_1, \dots, A_n be the Mattson-Solomon coefficients of c . Then the weight of c is equal to the rank of the circulant matrix

$$C_c = \begin{pmatrix} A_1 & \dots & A_n \\ \vdots & \ddots & \vdots \\ A_n & \dots & A_{n-1} \end{pmatrix}. \quad (1)$$

Thus the minimum distance of a code C is equal to the minimum rank of the matrices C_c , for $c \in C$. To find a lower bound on the minimum distance of a cyclic code with defining-set $I(C)$, the idea of Schaub-Massey is to compute a lower bound for generic matrices of the form C_c , such that $A_i = 0$, $i \in I(C)$, while the other coefficients have no fixed value. We shall not describe this "rank-bounding" algorithm in details, which can be seen as a Gaussian algorithm that guesses which rows are independent in a generic matrix C_{gen} .

We have applied this algorithm for duals of binary BCH codes, of length 127 and 255. We give a few examples of the results, and a complete table has been compiled.

REFERENCES

- [1] J. Wolfmann, "New bounds on cyclic codes from algebraic curves." Lecture Notes in Computer Science, vol.388, p.47-62, Springer 1989.
- [2] T. Schaub, *A Linear Complexity Approach to Cyclic Codes*, Swiss Federal Institute of Technology dissertation, Zuerich, 1988.

