Bounds on the minimum distance of the duals of BCH codes

Daniel Augot*, Françoise Levy-dit-Vehel *

Abstract

We consider primitive cyclic codes of length $p^m - 1$ over $\mathbf{F}_p$. The codes of interest here are duals of BCH codes. For these codes, a lower bound on their minimum distance can be found via the adaptation of the Weil bound to cyclic codes (see [10]). However, this bound is of no significance for roughly half of these codes.

We shall fill this gap by giving, in the first part of the paper, a lower bound for an infinite class of duals of BCH codes. Since this family is a filtration of the duals of BCH codes, the bound obtained for it induces a bound for all duals.

In the second part we present a lower bound obtained by implementing an algorithmic method due to Massey and Schaub (the rank-bounding algorithm). The numerical results are surprisingly higher than all previously known bounds.

Index terms : BCH codes, Duals, Roos and Weil bounds, Rank-bounding algorithm.

I. Introduction

A. Preliminaries

We consider cyclic codes of length $n = p^m - 1$ over $\mathbf{F}_p$, that is, ideals of the ring $\mathbf{F}_p[X]/(X^n - 1)$, for $m \in \mathbf{N}^*$. A defining-set of a code C is a set $T \subset [0, n-1]$, such that $\{\alpha^j,\ j \in T\}$ is the zero-set of the generator polynomial of C, where α is a primitive element in $\mathbf{F}_{p^m}$. Then, the narrow-sense BCH code of designed distance d is the code with defining-set $T = \cup_{1 \leq s < d} cl(s)$, where $cl(s)$ is the cyclotomic coset of p modulo n whose smallest element is s.

The dual $C^\perp$ of a code C is the set of vectors which are orthogonal (with respect to the inner product of $\mathbf{F}_p^n$) to all codewords of C. If C is cyclic, then so is $C^\perp$. Then we call check-set of C a subset J of $[0, n]$, such that the defining-set $T^\perp$ of $C^\perp$ can be written as the union of the cyclotomic cosets of the elements of J. Also, we recall that the Mattson-Solomon polynomial of an element $a = (a_0, \ldots, a_{n-1})$ of $\mathbf{F}_p^n$, is the following polynomial of $\mathbf{F}_{p^m}[Z]$:

*Institut National de Recherche en Informatique et Automatique (INRIA) Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex FRANCE

$MS_a(Z) = \sum_{i=1}^n A_i Z^{n-i}$, where $A_i = a(\alpha^i)$, $1 \le i \le n$ (identifying a with a polynomial of $\mathbf{F}_p[X]/(X^n-1)$).

We shall need the following result, that we call "Weil bound" for short. It is in fact a bound that comes from the results of Weil and Serre on the number of rational points of algebraic curves, adapted by Wolfmann to the case of cyclic codes.

Theorem 1 *[10] Let C be a cyclic code of length p^m-1 over $\mathbf{F}_p$, with generator polynomial $g(z)$ and check-set J. Let $\theta = \sup J$. If every element of J is prime to p, the non-zero weights of C satisfy :*

$$p^{m-1}(p-1) - \frac{(\theta-1)(p-1)}{2p}\lfloor 2p^{\frac{m}{2}}\rfloor \le w \le p^{m-1}(p-1) + \frac{(\theta-1)(p-1)}{2p}\lfloor 2p^{\frac{m}{2}}\rfloor, \quad \text{if } g(1)=0,$$

$$p^{m-1}(p-1)-1 - \frac{(\theta-1)(p-1)}{2p}\lfloor 2p^{\frac{m}{2}}\rfloor \le w \le p^{m-1}(p-1)-1 + \frac{(\theta-1)(p-1)}{2p}\lfloor 2p^{\frac{m}{2}}\rfloor, \ \text{if } g(1)\neq 0.$$

Remark 1 If C is the dual of the BCH code of designed distance d, then theorem 1 applies with θ being the largest designed distance strictly less than d, that is, the largest integer less than d, which is at the same time the smallest element of its cyclotomic coset.

There exists a value of θ, say θ_0, such that for $\theta \ge \theta_0$, the lower bound given by the above theorem is negative. In the following lemma, we precize the value of θ_0, in the case where 1 is a zero of the generator polynomial of the code (it is the only case of interest here, because 0 belongs to the defining-set of any dual of BCH code). The proof can be found in [4].

Lemma 1 *With the notations of theorem 1, for the cyclic codes admitting 1 as zero, the Weil bound is negative for $\theta \ge \theta_0$, with :*

- *if m is even, $\theta_0 = p^{\frac{m}{2}}+1$,*
- *if m is odd, θ_0 is the smallest element greater than or equal to $\lceil \frac{2p^m}{\lfloor 2p^{\frac{m}{2}}\rfloor}\rceil + 1$, which is at the same time the smallest element of its cyclotomic coset. Let $\Lambda = \lceil \frac{2p^m}{\lfloor 2p^{\frac{m}{2}}\rfloor}\rceil$. We get : For $p=2$ and $m \ge 5$, or for $p>2$ and $m\ge 3$, $\theta_0 = \Lambda+1$ if $p \not| \Lambda+1$, and $\theta_0 = \Lambda+2$ otherwise.*

Note : In many cases, we have $\Lambda = \lceil p^{\frac{m}{2}}\rceil$.

Another result of interest for us is the Roos bound. To recall it, we need to introduce two notations : For a subset A of $\mathbf{F}_{p^m}$, say $A = \{\alpha^{j_1},\ldots,\alpha^{j_k}\}$, we shall denote by $\tilde{A}$, the subset : $\tilde{A} = \{\alpha^s,\ s \in \cup_{l=1}^k cl(j_l)\}$; that is, if $\alpha^j \in A$, then $\alpha^{jp^i \bmod n} \in \tilde{A}$ for all i, $0 \le i \le m-1$. This notation follows from the fact that if A is a zero-set of a cyclic code C over $\mathbf{F}_{p^m}$, then $\tilde{A}$ is a zero-set of a cyclic code over $\mathbf{F}_p$, namely the subfield subcode of C.

If A and B are two subsets of a field F, the *product-set* AB is the set $\{ab,\ a\in A,\ b \in B\}$.

Theorem 2 *[9] Let $\mathcal{D}$ be a cyclic code of length n over $\mathbf{F}_{p^m}$, and let T_1 be its zero-set. Assume $d_{min}\mathcal{D} \ge \delta$. Let β be a primitive n-th root of unity in $\mathbf{F}_{p^m}$, and $T_2 = \{\beta^{i_1},\ldots,\beta^{i_k}\}$, where $0 \le i_1 < i_2 < \ldots < i_k \le n-1$. If the number of "missing powers" in T_2, namely $i_k - i_1 - k + 1$, is strictly less than $\delta - 1$, then the cyclic code of length n over $\mathbf{F}_p$ whose zero-set is $\widetilde{T_1 T_2}$ has minimum weight at least $\delta + k - 1$.*

Note that the true minimum distance of the duals of some cyclic codes can be found from the minimum distance of the duals of BCH codes. This has been shown by Moreno, Zinoviev and Kumar [7].

B. A particular class of duals of BCH codes

In order to derive a bound on the minimum distance of the duals of BCH codes, we first isolate a particular class of them. This class was chosen for combinatorial reasons. Indeed, for a code of this class, the particular form of its defining-set settles a fully adapted context to apply the Roos and Weil bounds.

Definition 1 *Let $1 \leq t \leq m$, and $0 \leq i < p-1$. We define the code $B^{\perp}(t,i)$ as the dual of the BCH code of length p^m-1 over $\mathbf{F}_p$, with designed distance $d(t,i) = \sum_{j=1}^{a}(i+1)p^{m-jt}+(1-\delta_{r,0})$, with $m = at+r$, $0 \leq r < t$, and δ is the Kronecker symbol.*

In the following, we identify an element s in $[0,n[$ with its p-ary expansion, namely $s = \sum_{i=0}^{m-1} s_i p^i = (s_0 \ldots s_{m-1})$.

Proposition 1 *The defining-set of $B^{\perp}(t,i)$ is $T(t,i) = \{v \in [0,n]$, the p-ary expansion of v has no pattern of the form $j\underbrace{p-1\ldots p-1}_{t-1}$, with $p-1-i \leq j \leq p-1\}$.*

Remark 2 We have the following inclusions on $B^{\perp}(t,i)$ codes :

$$\ldots B^{\perp}(t,i) \subset B^{\perp}(t,i+1)\ldots B^{\perp}(t,p-2) \subset B^{\perp}(t-1,0)\ldots$$

II. The theoretical bounds

A. A bound on the minimum distance of $B^{\perp}(t,i)$

The idea is to use the property that the defining-set of $B^{\perp}(t,i)$ contains regularly distributed patterns of consecutive roots. This is exactly what is needed to use the Roos bound in an efficient way. Let us first treat an example to show how the Roos bound can be applied to these codes.

Example

- Suppose $p = 2$, $m = 9$ and $t = 3$. We use the notations of theorem 2. Take $\mathcal{D}$ to be the cyclic code of length 511 over $\mathbf{F}_{512}$, with zero-set $T_1 = \{\alpha^r,\ 0 \leq r \leq v-1\}$, where $v = p^t - 1 = 7$ and α is a primitive 511-th root of unity in $\mathbf{F}_{512}$. By the BCH bound, $d_{min}\mathcal{D} \geq 8$. We choose $\beta = \alpha^a$, with $a = 2^{t+1} = 16$, and $i_j = j-1$ for $1 \leq j \leq 2^t - 1 = 7$, $i_j = j$, for $j = 2^t + l$, $0 \leq l \leq 2^t - 3 = 5$; (with the notations of the theorem, $k = 13$). The product-set T_1T_2 is exactly

$$\{\alpha^{ai_j+r},\ 1 \leq j \leq 13,\ 0 \leq r \leq v-1 = 6\},$$

and, by proposition 1, it is easy to see that the defining-set of $B^{\perp}(3,0)$ contains $\widetilde{T_1T_2}$, so that $B^{\perp}(3,0)$ is a subcode of the code, say $\mathcal{E}$, with defining-set $\widetilde{T_1T_2}$. As $i_{13} - i_1 - 12 = 1 < 7$, we get $d_{min}B^{\perp}(3,0) \geq d_{min}\mathcal{E} \geq 8 + 13 - 1 = 20$, while the BCH bound applied to any of these two codes gives 8.

- Suppose now $p = 3$, and consider the code $B^{\perp}(3,0)$ in the length 2186. We take $T_1 = \{\alpha^l,\ 0 \le l \le v-1\}$, where now $v = p^t - 1 = 26$ and α is a primitive 2186-th root in $\mathbf{F}_{2187}$. Here $\delta = 27$. We set $\beta = \alpha^a$, with $a = p^t = 27$. For $j \in [0,35]$, let r be the quotient of j divided by $p-1$. Then, set $i_j = j + r$ (as i_1 can be equal to 0 in theorem 2, we can, for convenience, start the index j from 0). Again, the set $\widetilde{T_1T_2}$ where

$$T_1T_2 = \{\alpha^{ai_j+l},\ 0 \le j \le 35,\ 0 \le l \le 25\},$$

  is included in $T(3,0)$. Here $k = 36$, and the number of "missing powers" in T_2 is $i_{35} - i_0 - 35 = 52 - 35 = 17 < 26$, so that $d_{min}B^{\perp}(3,0) \ge 27 + 36 - 1 = 62$, while the BCH bound gives 27.

The following two theorems are derived from the Roos (as shown in the example) and Weil bounds. For a proof, see [3]. Note that, for $p = 2$, the $B^{\perp}(t,i)$s identify with the $B^{\perp}(t,0)$s.

Theorem 3 *We assume $p = 2$, and we denote by $\delta(t)$, the minimum distance of $B^{\perp}(t,0)$.*

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

   $\delta(t) \ge 2^{m-1} - \frac{2^{m-t-2}}{4}\lfloor 2^{\frac{m}{2}+1} \rfloor$.

Theorem 4 *We assume $p \ne 2$, and we denote by $\delta(t,i)$, the minimum distance of $B^{\perp}(t,i)$.*

1. *for $t = 1$, $\delta(1,i) \ge (z+2)(p-1-i)$, where $z = 0$ if $i \ge \frac{p}{2} - 1$, and z is the largest integer strictly less than $\frac{p}{i+1} - 1$ otherwise.*
2. *for $2 \le t < \frac{m-1}{2}$ (so $m \ge 6$), $\delta(t,i) \ge (p-i)(p^t - 1 - i)$,*
3. *for $t = \frac{m-1}{2}$ and $i = 0$, or for $t = \frac{m}{2}$, or $t = \frac{m+1}{2}$ and $i > 0$,*

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

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

B. A bound for all duals of BCH codes

We shall here give an estimate on the minimum distance of all duals of BCH codes. This estimate is derived from theorems 3 and 4, and by the fact that the $B^{\perp}(t,i)$s realize a filtration of the duals of BCH codes, in the sense that every dual of BCH code can be located between two consecutive $B^{\perp}(t,i)$s. Indeed, let $d \in [0,n[$. Then there exists t and i such that $d(t,i) \leq d < d(t,i+1)$ or, if $i = p-2$, $d(t,p-2) \leq d < d(t-1,0)$. But then, for the dual say $B^{\perp}(d)$ of the BCH code of designed distance d, we have

$$B^{\perp}(t,i) \subseteq B^{\perp}(d) \subset B^{\perp}(t,i+1),$$

(or $B^{\perp}(t,p-2) \subseteq B^{\perp}(d) \subset B^{\perp}(t-1,0)$).
The results of the following three theorems do not all come from including $B^{\perp}(d)$ in a $B^{\perp}(t,i)$ code. Some are also derived by applying the Weil bound directly to $B^{\perp}(d)$ (see remark 1), or by applying the Hartmann-Tzeng bound [2] to $B^{\perp}(d)$ and then including this code in a Reed-Muller code. The proofs, being quite long, are omitted here and are to be found in [4].

We denote by $\delta(d)$, the minimum distance of $B^{\perp}(d)$. The next theorem treats the case $p = 2$.

Theorem 5 *Let $d \geq 3$, and $l = l(d)$, such that*

$$2^{l} + 1 \leq d < 2^{l+1} + 1. \tag{1}$$

Set $t = m - l$.

1. *If $d = d(t,0)$, a bound on $\delta(d)$ is given by theorem 3.*
2. *We assume $d \neq d(t,0)$. Then we have the following lower bound on $\delta(d)$.*
   (a) $l < \lfloor \frac{m}{2} \rfloor$
   $\delta(d) \geq weil(d)$, *where $weil(d)$ is the Weil bound for $B^{\perp}(d)$, as given in theorem 1.*
   (b) $l = \lfloor \frac{m}{2} \rfloor$,
   If m is even,
   - $d < 2^{\frac{m}{2}+1} - 3 \;\Rightarrow\; \delta(d) \geq 2^{\frac{m}{2}+1} - 2^{\frac{m}{2}-1}$,
   - $d = 2^{\frac{m}{2}+1} - 3$ *or* $d = 2^{\frac{m}{2}+1} - 1 \;\Rightarrow\; \delta(d) \geq 2^{\frac{m}{2}}$.

   If m is odd,
   Let θ_0 be defined as in lemma 1. Then
   - $d < \theta_0 \;\Rightarrow\; \delta(d) \geq sup(2^{\frac{m+3}{2}} - 2^{\frac{m-1}{2}}, weil(d))$,
   - $\theta_0 \leq d < 2^{\frac{m+1}{2}} - 3 \;\Rightarrow\; \delta(d) \geq 2^{\frac{m+3}{2}} - 2^{\frac{m-1}{2}}$,
   - $d = 2^{\frac{m+1}{2}} - 3$ *or* $d = 2^{\frac{m+1}{2}} - 1 \;\Rightarrow\; \delta(d) \geq 2^{\frac{m+1}{2}}$.

(c) $\frac{m}{2} < l < m-2$,

- $d < 2^{l+1} - 3 \;\Rightarrow\; \delta(d) \geq 2^{t+1} - 2^{t-1}$,
- $d = 2^{l+1} - 3$ *or* $d = 2^{l+1} - 1 \;\Rightarrow\; \delta(d) \geq 2^t + 2^{t-1} - 4$,

(d) $l = m-2$ *and* $m \geq 4$

$\delta(d) \geq 6$, except for $d = 2^{m-1} - 1$ and $d = 2^{m-1} - 2^{\frac{m}{2}-1} - 1$, in which cases we only have $\delta(d) \geq 4$.

The next two theorems concern the non-binary case.

Theorem 6 *Let $1 \leq t \leq m$ and d such that*

$$d(t,i) \leq d < d(t,i+1), \quad i < p-2.$$

1. *If $d = d(t,i)$, a bound on $\delta(d)$ is given by theorem 4.*
2. *We assume $d \neq d(t,i)$. Then we have the following lower bound on $\delta(d)$:*

   (a) $t = 1$,

   - $\delta(d) \geq 2(p-2-i)$ *if* $i < p-4$, $\delta(d) \geq p-i$ *otherwise.*

   (b) $2 \leq t < \frac{m+1}{2}$,

   - $2 \leq t < \frac{m-1}{2}$, $\delta(d) \geq (p-1-i)(p^t-2-i)$,
   - $t = \frac{m-1}{2}$ *(m odd)*, $\delta(d) \geq (p-2-i)p^{\frac{m-3}{2}} + p^{\frac{m-1}{2}} - 2 - i$,
   - $t = \frac{m}{2}$ *(m even)*, $\delta(d) \geq (p-1)^2 p^{\frac{m}{2}-2} + p^{\frac{m}{2}} - 2 - i$,

   (c) $t = \frac{m+1}{2}$, *(m odd, $m \geq 5$). Let θ_0 be defined as in lemma 1.*

   - $d \leq \theta_0 \;\Rightarrow\; \delta(d) \geq sup((p-1)^2 p^{\frac{m-5}{2}} + p^{\frac{m+1}{2}} - 2 - i, weil(d))$, *where $weil(d)$ is the Weil bound for $\bar{B}^{\perp}(d)$, as given in theorem 1.*
   - $\theta_0 < d \;\Rightarrow\; \delta(d) \geq (p-1)^2 p^{\frac{m-5}{2}} + p^{\frac{m+1}{2}} - 2 - i$,

   (d) $\frac{m+1}{2} < t \leq m$, $\delta(d) \geq weil(d)$.

Theorem 7 *Let $2 \leq t \leq m-1$, and d such that*

$$d(t,p-2) \leq d < d(t-1,0).$$

1. *If $d = d(t,p-2)$, a bound on $\delta(d)$ is given by theorem 4.*
2. *We assume $d \neq d(t,p-2)$. We then have the following bound on $\delta(d)$:*

   (a) $2 \leq t < \frac{m+1}{2}$, $\delta(d) \geq p^t - p + 2$, *except for* $d = p^{m-t+1} - 1$, *in which case* $\delta(d) \geq p^t - p$.

   (b) $t = \frac{m+1}{2}$ *(m odd)*, $\delta(d) \geq p^{\frac{m+1}{2}} - p + 2$, *except for* $d = p^{\frac{m+1}{2}} - 1$, *in which case* $\delta(d) \geq (p-1)^2 p^{\frac{m-3}{2}} + p^{\frac{m-1}{2}} - 1$.

   (c) $\lceil \frac{m}{2} \rceil + 1 \leq t \leq m-1$, *$\delta(d)$ is bounded from below by the Weil bound (theorem 1).*

III. The algorithmic approach

We use an algorithmic approach to compute a lower bound on the minimum disatnce of the duals of BCH codes. The algorithmic method used here is due to T. Schaub and J. L. Massey, and is quite general to find a lower bound on the minimum distance of any cyclic code. We have implemented this method using the C language. We present the main ideas of the algorithm. It is based on the following theorem, see for instance [8].

Theorem 8 *Let $c \in \mathbf{F}_p^n$, let $A_1, \ldots, A_n$ be the Mattson-Solomon coefficients of c. Then the weight of c is equal to the rank of the circulant matrix*

$$C_c = \begin{pmatrix} A_0 & A_1 & \ldots & A_{n-1} \\ A_1 & A_2 & \ldots & A_0 \\ \vdots & \vdots & & \vdots \\ A_{n-1} & A_0 & \ldots & A_{n-2} \end{pmatrix}. \tag{2}$$

Thus finding a lower bound on the minimum distance of a code C can be done by finding the minimum rank of the matrices C_c, for all the codewords $c \in C$. Since it is not feasible to compute the rank of all these matrices, the algorithm compute a lower bound for the rank of a *generic matrix* C_{gen}, which is as follows.

Let $I(C)$ be the defining set of a cyclic code C. Then the Mattson-Solomon coefficients of the codewords of c satisfy

$$\forall\, i \in I(C), \quad A_i = 0.$$

The *generic matrix* of the code C is the matrix C_{gen}, corresponding to the matrix C_c, with zero's in the position of the A_i's, $i \in I(C)$, and the symbol Δ^+ in the other positions. The symbol Δ^+ means "certainly non zero".

As an example, consider the following matrix

$$\begin{pmatrix} \Delta^+ & 0 & \Delta^+ \\ \Delta^+ & \Delta^+ & 0 \\ 0 & \Delta^+ & \Delta^+ \end{pmatrix}.$$

The rank of such a matrix is easily seen to be greater than or equal to 2 for any non zero values which can be given to the symbols Δ^+.

The rank-bounding algorithm, designed by T. Schaub, finds a set of necessarily independant columns in such a matrix, for all non zero values given to the Δ^+. The lower bound returned for the rank is the number of these lines.

The algorithm works by inspecting each line after another, trying to express the current line in terms of previous lines. If this is impossible, the algorithm add the current line to the set of independant lines. If not, it skips to the next line. The techniques for establishing the independance of a line are too intricated to be described here, and are fully explicited in [8]. The rank-bounding algorithm works with complexity $O(n^3)$ for a matrix of size n. No arithmetical operations are needed.

The algorithm computes a lower bound for codewords that do not belong to any other subcode, for it assume that the A_i's not belonging to the defining set are non-zero. It must be recursively applied to all cyclic subcodes, or to a portion of these. In the cases where the code has too many subcodes, the complexity is large.

IV. Numerical results

We shall now present numerical tables illustrating the theoretical bound (theorems 5, 6 and 7) and Schaub's method.

In the first column of the tables, we quote the designed distance d of the BCH-code. The dagger means that the code corresponds to a $B^{\perp}(t,i)$ code ($\bar{B}^{\perp}(t,0)$ in the binary case). The star in the Schaub's bound column means that the value is the actual minimum distance.

The first example is in the binary case, in the length 127 (table I). We can see that Schaub's algorithm gives very high values, e.g. for $d = 9$ to 21. For $d = 11$ (respectively 15, 19), we proved by the algorithmic method that the minimum distance of $\bar{B}^{\perp}(d)$ is at least 32 (respectively 28, 22), and some other considerations (see [1]) lead to prove that it actually is the minimum distance.

For large designed distances, the gap between the two method is not so obvious. The next example also concerns the binary case (table II, length 255). The "?" means that the algorithm couldn't stop because there were too many subcodes.

Note that, for the dual of the BCH code with designed distance 9, Schaub's algorithm gives 86, and, as the code is 4-divisible (see e.g. [3]), we get 88.

The last table concerns the ternary case (table III). It is worth to notice here that the theoretical bound is better for the first values of the designed distance (till $d = 10$).

As for $p = 2$, there are cases where the algorithm couldn't stop.

References

[1] D. Augot, "Etude algébrique des mots de poids minimum des codes cycliques, méthodes d'algèbre linéaire sur les corps finis", Thèse de doctorat, Paris VI, 1993.

[2] C.R.P Hartmann and K.K. Tzeng, "Generalizations of the BCH bound", Info. and Control vol.20, p.489-498, 1972.

[3] F. Levy-dit-Vehel, "Bounds on the minimum distance of the duals of extended BCH codes", Applicable Algebra in Engineering Communication and Computing (AAECC) vol.6 n^0 3, pp.175-190, Springer-Verlag 1995.

[4] F. Levy-dit-Vehel, "Divibilité des codes cycliques : Applications et prolongements", Thèse de doctorat, Paris VI, 1994.

[5] J.L. Massey, T. Schaub, "Linear complexity in coding theory", in *Coding theory and Applications*, Lecture Notes in Computer Science vol.311, Springer-Verlag 1988.

[6] O. Moreno and V. Kumar, "Minimum Distance Bounds for Cyclic Codes and Deligne's Theorem", IEEE Trans. on Info. Theory, vol. IT 39 no 5, pp. 1524-1534, September 93.

[7] O. Moreno, V. Zinoviev and V. Kumar, "The Exact Minimum Distance of Some Cyclic Codes", in *Proceedings of AGCT4'94*, Novgorod, Russia.

[8] T. Schaub, "A linear complexity approach to cyclic codes", Dissertation, Swiss Federal Institute of Technology, Zuerich 1988.

[9] C. Roos, "A new lower bound for the minimum distance of a cyclic code", IEEE Trans. on Info. Theory, vol. IT 29 no 3, May 1983.

[10] J. Wolfmann, "New bounds on cyclic codes from algebraic curves", in *Lecture Notes in Computer Science*, vol.388,p.47-62, Springer-Verlag 1989.

d	theoretical bound	Schaub's bound
3 †	64	64*
5 †	56	56*
7	48	48*
9 †	32	40
11	24	32*
13	16	30
15	16	28*
19 †	12	22*
21	12	20
23	12	16
27	12	14
29	8	14
31	8	12
43 †	8	8
47	6	8
55	6	6
63	4	4

TABLE I: Bounds for duals of BCH codes, $p = 2$, length 127.

d	theoretical bound	Schaub's bound
3 †	128	128*
5 †	112	112*
7	96	96*
9 †	80	88
11	64	64
13	48	64
15	32	60
17 †, 19	24	42
21	24	40
23, 25, 27	24	32
29	16	28
31	16	26
37 †	14	22
39	12	22
43, 45	12	20
47, 51, 53	12	16
55, 59	12	?
61, 63, 85 †	8	?
87, 91, 95, 111	6	?
119, 127	4	?

TABLE II : Bounds for duals of BCH codes, $p = 2$, length 255.

d	theoretical bound	Schaub's bound
2 †	162	162
4 †	153	121
5	135	114
7 †	122	80
8	102	80
10 †	90	80
11	51	79
13	51	72
14	51	65
16	51	56
17	51	53
19 †	29	51
20	26	48
22	26	38
23	26	35
25	26	26
26, 31 †	20	26
32, 34, 35	10	26
38	10	25
40, 41	10	23
43, 44	10	22
47,49	10	19
50 to 61 †	10	?
62 to 79	8	?
80, 121 †	6	?
122 to 161	2	?

TABLE III: Bounds for duals of BCH codes, $p = 3$, length 242.

TABLE I: Bounds for duals of BCH codes, $p = 2$, length 127.

TABLE II : Bounds for duals of BCH codes, $p = 2$, length 255.

TABLE III: Bounds for duals of BCH codes, $p = 3$, length 242.