Upper Bounds on the Dual Distances of EBCH Codes

Carmen-Simona Nedeloaia

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Upper Bounds on the Dual Distances of EBCH Codes

Carmen-Simona Nedeloaia

N° 5477

Janvier 2005

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--5477--FR+ENG

INRIA
ROCQUENCOURT

Upper Bounds on the Dual Distances of EBCH Codes

Carmen-Simona Nedeloaia*

Thème SYM — Systèmes symboliques
Projet CODES

Rapport de recherche n° **5477** — Janvier 2005 — 14 pages

Abstract: We give new upper bounds on the dual distances of extended BCH codes of length 512. First, we apply a probabilistic algorithm due to Canteaut and Chabaud. Secondly, we put these codes in standard bit order and we use the twisted squaring decomposition of affine-invariant codes. We then obtain two subcodes which contain codewords of minimum weights for the duals of BCH codes of length less than or equal to 512. This decomposition also gives new interesting codes of smaller length, which sometimes are found to be Reed-Muller codes.

Key-words: affine-invariant codes, dual distance, minimum-weight word, standard bit order, twisted squaring construction

* Email: carmen.nedeloaia@unilim.fr

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex (France)
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

Bornes supérieures des distances duales des codes EBCH

Résumé : Nous donnons des bornes supérieures nouvelles pour les distances duales des codes BCH étendus de longueur 512. En premier lieu, nous appliquons l'algorithme probabiliste de Canteaut et Chabaud. Deuxièmement, nous mettons ces codes en ordre standard des bits et nous utilisons la décomposition des codes affines-invariants. Nous obtenons ainsi deux sous-codes qui contiennent des mots de poids minimum dans les duaux des codes BCH de longueur inférieure ou égale à 512. De plus, cette décomposition produit des nouveaux codes de longueur plus petite, dont une partie sont des codes de Reed-Muller.

Mots-clés : codes affines-invariants, distance duale, mot de poids minimum, ordre standard de bits, construction carrée modifiée

1 Introduction

In this paper, we treat *primitive* binary BCH codes and our main interest is for the minimum distances of their dual codes. Now, only six minimum distances are still unknown for primitive BCH codes of length up to 512. It is far to be the same for their duals. For $n = 128$, their weight distributions are given in [6]. For $n = 256$, some weight distributions are available (see the link [15]) and recently, an updated table of the minimal weights was published in [13]. Among the duals of the BCH codes of length 256, twelve are such that only an upper bound on their minimal distance is given. Good lower bounds are also known for this length [1]. On the contrary, little is known when $n = 512$, except for BCH codes of small designed distances [12]. Concerning the numerical results, we focus on this length. Two methods are used. First, we apply the minimum-weight algorithm due to Canteaut and Chabaud [4]. Secondly, we use the *linear twisted squaring decomposition* introduced by Forney in [7], which can be applied to any affine-invariant code.

The paper is organized as follows. Main notation, definitions and previously known results are presented in Section 2. We recall here the linear twisted squaring construction (LTSC), as well as the main result of [2] for any affine-invariant code. We also discuss the connection between the component codes and an upper bound of the dual distance (in Remark 1). Our main results are in Section 3. Two subcodes arise from the LTSC decomposition. We begin by giving for one of these subcodes, denoted by B, an upper bound on its dimension (Proposition 4). We later look at the involvement of Reed-Muller codes in the decomposition of the duals of BCH codes. We show that, for several designed distances and for length less than or equal to 512, B is equal to some Reed-Muller code. In Section 4, we focus on the minimum distance of the duals of BCH codes. We used the probabilistic algorithm described in [4] either on the code or on the two subcodes arising from the twisted squaring construction. Then we obtain new upper bounds on the dual distances for codes of length 512. For codes of length 256, we also obtain the same minimum distances and upper bounds as given in [13].

2 Notation and preliminaries

In this section we present the precise notation, definitions and basic results used along this paper. Our main reference for coding theory is [11]. We treat binary linear codes and the distance is always the Hamming distance. For such a code C, its generator matrix is denoted by G_C and its dual code is denoted $C^\perp$. If d is the minimal distance of C then $d^\perp$ is the minimal distance of $C^\perp$, the so-called *dual distance* of C.

For two *arbitrary* binary codes C and D of length n we define:

- The *direct sum* of C and D, as the code of length $2n$:
$$C \oplus D = \{|\mathbf{u}|\mathbf{v}| : \ \mathbf{u} \in C \ \text{ and } \ \mathbf{v} \in D\}.$$
- The *sum* of C and D, as the code of length n:
$$C + D = \{\mathbf{u} + \mathbf{v} : \ \mathbf{u} \in C \ \text{ and } \ \mathbf{v} \in D\}.$$
- If D is a subcode of C, then the *complement code* C/D is a vector space such that $C = D + C/D$. This notation particularly means that C/D is a complete set of coset representatives of D in C.
- The $|u|u + v|$ *construction* of C and D, as the code of words $(\mathbf{u}|\mathbf{u} + \mathbf{v})$ where $\mathbf{u}$ is in C and $\mathbf{v}$ is in D. This code is of length $2n$.

Given a binary linear code C, the *extended code* EC is obtained by adding an overall parity check symbol:

$$\forall \ \mathbf{c} = (c_1, c_2, \ldots, c_n) \in C \Rightarrow E\mathbf{c} = (c_1, c_2, \ldots, c_n, c_\infty) \in EC \ \text{ where } \ c_\infty = \sum_{i=1}^{n} c_i.$$

Conversely, by deleting any coordinate, we obtain a *punctured code*. More generally, given a set $T \subset [1, n]$, we derive the following codes:

- the *punctured code* with respect to T: the linear code of length $n - |T|$ obtained by deleting the coordinates labeled with the elements of T;
- the *shortened code* with respect to T: the linear code of length $n - |T|$ obtained from the codewords of C which are zero on T, by deleting the coordinates in T.

Definition 1 *Let C be a binary code of length 2^m. Thus the coordinates can be indexed by the elements $X \in \mathbb{F}_{2^m}$. The code is said* affine-invariant *if it is invariant under the permutations $X \mapsto \alpha X + \beta$, where $\alpha, \beta \in \mathbb{F}_{2^m}$ and $\alpha \neq 0$.*

In this paper we denote by $\mathrm{BCH}(2^m-1, \delta)$ the narrow-sense primitive BCH code of length 2^m-1 and designed distance δ. Similarly the extended code will be denoted by $\mathrm{EBCH}(2^m, \delta)$ and its dual code by $\mathrm{EBCH}^{\perp}(2^m, \delta)$. The Reed-Muller code of length 2^m and order r is denoted here by $\mathrm{RM}(r, m)$.

We also recall the most important results obtained in [2]. From now on, in this section we consider a binary code C of even length n.

Definition 2 *Let C be a code of length $n = 2t$ and dimension k. Let us denote by F_0 the first t positions and by F_1 the last t positions of any codeword. Assume that C is such that:*

- *the punctured codes on F_0 and on F_1 are equal to a same code A;*
- *the shortened codes on F_0 and on F_1 are equal to a same code B.*

The code C is said to be a linear twisted squaring constructed *(or LTSC) code and is denoted by $C = \|A/B\|^2$.*

Note that A and B are two codes of length t such that B is a subcode of A and $k_A + k_B = k$, where k_A and k_B denotes the dimensions of A and B.

Now let us emphasize that:

1. The generator matrix of $\|A/B\|^2$ can be written

$$\begin{pmatrix} G_{A/B} & \widetilde{G_{A/B}} \\ G_B & 0 \\ 0 & G_B \end{pmatrix}. \tag{1}$$

   Note that the matrices $G_{A/B}$ and $\widetilde{G_{A/B}}$ are different, even if both generate the complement code A/B.

2. With the previous notation, we can write

$$\|A/B\|^2 = (A/B, \widetilde{A/B}) + (B \oplus B),$$

   where $(A/B, \widetilde{A/B})$ denotes the code with generator matrix $(G_{A/B}, \widetilde{G_{A/B}})$. The corresponding relation between the dimensions is

$$k = k_{(A/B,\, \widetilde{A/B})} + 2k_B. \tag{2}$$

3. Each word of $\|A/B\|^2$ is of the form

$$(\mathbf{b}_1 + \mathbf{d},\, \mathbf{b}_2 + \mathbf{d}'), \quad \mathbf{d}, \mathbf{d}' \in A/B, \quad \mathbf{b}_1, \mathbf{b}_2 \in B.$$

   If $\mathbf{d} = \mathbf{d}'$ for all codewords, we obtain the *(1-level) squaring construction*

$$|A/B|^2 = \{(\mathbf{b}_1 + \mathbf{d},\, \mathbf{b}_2 + \mathbf{d}) : \quad \mathbf{d} \in A/B, \quad \mathbf{b}_1, \mathbf{b}_2 \in B\},$$

   which is identical to the $|\mathbf{u}|\mathbf{u}+\mathbf{v}|$ construction, because $B \subseteq A$ (here $\mathbf{u} \in A$, $\mathbf{v} \in B$).

4. The dual of an LTSC code $C = \|A/B\|^2$ is also an LTSC code of the form

$$C^{\perp} = \|B^{\perp}/A^{\perp}\|^2.$$

Definition 3 *A code $C = \|A/B\|^2$ is a recursive LTSC if it is LTSC, the component codes A and B are LTSC, the component codes of A and B are LTSC and so on.*

The following result will be intensely used hereafter.

Theorem 1 *[2, Theorem 4] Affine-invariant codes (and in particular the primitive EBCH codes -and their duals-) are* recursive symmetric reversible *LTSC codes.*

Corresponding to the previous definition and to the proof of the theorem in [2], affine-invariant codes of length 2^m are of degree of decomposition m. Obviously, direct-sum subcodes play a leading role in finding minimum-weight codewords.

In order to obtain this recursive structure, the affine-invariant codes are put *in standard bit order* [2]. Recall that C is a code of length 2^m, so the coordinates can be labeled by using a field element $X \in \mathbb{F}_{2^m}$. Let

$$(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \tag{3}$$

be a basis for the vector space $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Then any element X may be represented by the m-tuple $\psi[X] = (b_0, b_1, \ldots, b_{m-1}) \in \mathbb{F}_2^m$, such that

$$X = \sum_{i=0}^{m-1} b_i \alpha_i.$$

The standard bit order is obtained by *permuting a coordinate labeled by X to position $j+1$ in C such that $\psi[X]$ is the radix-2 representation of j*. Thus we state:

$$\psi[X] = \begin{cases} (b_0, b_1, \ldots, b_{m-2}, 0) & \text{if } X \in F_0 \\ (b_0, b_1, \ldots, b_{m-2}, 1) & \text{if } X \in F_1. \end{cases} \tag{4}$$

Once this permutation determined, we pass to the decomposition of the permuted code, by calculating the shortened code B (so the direct sum $B \oplus B$) and then taking the complement code. This construction is particularly interesting when we work with EBCH codes, because of the construction of their parity-check matrices. The construction of this matrix in standard bit order respects the algorithm given in [2, Appendix].

Remark 1 The code put in this form becomes particularly interesting for finding words of small weight, due to the blocks of zeros. The following bound being obviously

$$d \leq \min\{d_B, d_{(A/B, \widetilde{A/B})}\}, \tag{5}$$

our interest goes towards the study of the codes B, $(A/B, \widetilde{A/B})$ and A. This includes dimensions, minimum distances (or upper bounds) and, not at last, comparisons with known codes. The code B has length a half the length of the code C and a much smaller dimension, so in a majority of cases, for $m \leq 9$, its parameters can be computed by using Magma. As in some cases we obtain Reed-Muller codes, we search for a comparison through a theoretical point of view (see Section 3).

Concerning the code $(A/B, \widetilde{A/B})$, we can obtain a generator matrix such that k_B columns are null, both in $G_{A/B}$ and in $G_{\widetilde{A/B}}$ (more precisely, those columns corresponding to the information set of B). Via Relation (2), *when the dimension of B becomes high, then the dimension and the effective length of the code $(A/B, \widetilde{A/B})$ become small.* This allows us to reduce the effective length of this code in the computation of its minimum distance.

Notice that k_B is related to k_A by the equality $k_A + k_B = k$, so a characterization of the codes A is also important. The codes A can be compared with EBCH$^\perp$ codes; one example is indicated at the end of Section 3. □

Concerning the connections between the EBCH codes and Reed-Muller codes, one can use the definition of the punctured Reed-Muller code [8, p.383] and a simple inclusion between the defining sets, for obtaining the two following well-known results:

Proposition 1 *The inclusion $EBCH(2^m, \delta) \subset RM(r, m)$ is verified for all δ greater than the greatest representative of weight $m - r - 1$ in a cyclotomic coset modulo $(2^m - 1)$.*

Proposition 2 *The binary primitive narrow-sense $BCH(2^m - 1, \delta)$ code contains the punctured Reed-Muller code $RM^*(r, m)$ for all $\delta \leq 2^{m-r} - 1$.*

By passing to dual codes, we can find the greatest integer r_1 and the smallest integer r_2 such that:

$$RM(r_1, m) \subseteq EBCH^\perp(2^m, \delta) \subset RM(r_2, m), \tag{6}$$

for fixed m and δ. Now, as all these codes are in standard bit order, we use their twisted squaring decompositions. By considering their shortened codes on the first 2^{m-1} coordinates, we deduce

$$RM(r_1 - 1, m - 1) \subseteq B(2^m, \delta) \subseteq RM(r_2 - 1, m - 1), \tag{7}$$

where $B(2^m, \delta)$ denotes the code B obtained via the decomposition of EBCH$^\perp(2^m, \delta)$.

3 An Upper Bound on the Dimension of B

In this section we consider primitive cyclic codes as field algebra codes (for more details see [5]). This allows us to do a theoretical study of the code B and to give an upper bound on its dimension, obtained through the LTSC decomposition of affine-invariant codes (see Theorem 1).

We denote by $\mathbf{F}$ the splitting field $\mathbb{F}_{2^m}$ of $X^{2^m-1}-1$ over $\mathbb{F}_2$. Let us denote by $\mathcal{A}$ the algebra of the additive group of $\mathbf{F}$ over $\mathbb{F}_2$, $\mathbb{F}_2[\{\mathbf{F},+\}]$. An element of $\mathcal{A}$ is a formal sum

$$x = \sum_{g\in\mathbf{F}} x_g X^g, \qquad x_g \in \mathbb{F}_2.$$

Addition and scalar multiplication are component-wise and multiplication is given by addition in $\mathbf{F}$ [5, p. 974].

We consider the $\mathbb{F}_2$-linear map of $\mathcal{A}$ into $\mathbf{F}$

$$\phi_s\left(\sum_{g\in\mathbf{F}} x_g X^g\right) = \sum_{g\in\mathbf{F}} x_g g^s, \tag{8}$$

where $0 \le s \le 2^m-1$ and $0^0 = 1$.

Definition 4 *[5, p.974] Let the ambient space be $\mathcal{A} = \mathbb{F}_2[\{\mathbf{F},+\}]$. Let I_{EC} be a subset of $[0,\, 2^m-1]$, containing 0 and invariant under multiplication by 2 mod (2^m-1). The extended cyclic code EC with defining set I_{EC} is defined as follows:*

$$EC = \{x \in \mathcal{A} \mid \phi_s(x) = 0, \quad \forall s \in I_{EC}\}.$$

The code EC is said to be an extended cyclic code in $\mathcal{A}$. *The dual of EC is also an extended cyclic code. Its defining set is the set*

$$I_{EC^\perp} = \{s \in [0,\, 2^m-1] \mid 2^m-1-s \notin I_{EC}\} = [0,\, 2^m-1]\backslash\{-s \mid s \in I_{EC}\}.$$

Therefore, the defining set of EC being known, we can easily calculate the defining set of $\mathrm{EC}^\perp$. For simplicity, *the defining set of $EC^\perp$ will be denoted here by $\mathcal{I}$.* Actually, $0 \in \mathcal{I}$.

In the following, we consider an affine-invariant code EC of length 2^m and we will give an upper bound on the dimension of B. As discussed in Section 2, the dimension of B plays a key role in finding minimum-weight codewords in $EC^\perp$.

We recall that the codes in which we are interested in, $EC^\perp$, are considered in *standard bit order*, so the coordinates are labeled by elements in $\mathbb{F}_{2^m}$, respecting Relation (4). For $x \in \mathrm{EC}^\perp$, $x = \sum\limits_{g\in\mathbf{F}} x_g X^g$, we choose the following notation

$$x_g = \begin{cases} y_g & \text{if } g \in F_0 \\ z_g & \text{if } g \in F_1. \end{cases}$$

For all $g \in F_1$ there exist $b_i \in \mathbb{F}_2$, $0 \le i \le m-2$ such that $g = \sum\limits_{i=0}^{m-2} b_i\alpha_i + \alpha_{m-1}$. Let us denote $g' = \sum\limits_{i=0}^{m-2} b_i\alpha_i$, so $g = g' + \alpha_{m-1}$. The code $B \oplus B$ has dimension $2k_B$. As it is a subcode of $EC^\perp$, its codewords satisfy the relations

$$\sum_{g\in\mathbf{F}} x_g g^s = 0, \quad \forall s \in \mathcal{I}.$$

In order to find other relations which characterize $B \oplus B$, we calculate $\phi_s(x)$ for $s \notin \mathcal{I}$ and $x = (y, z) \in B \oplus B$

$$\begin{aligned}
\sum_{g \in \mathbf{F}} x_g g^s &= \sum_{g \in F_0} y_g g^s + \sum_{g \in F_1} z_g g^s = \sum_{g \in F_0} y_g g^s + \sum_{g' \in F_0} z_{g'+\alpha_{m-1}} (g' + \alpha_{m-1})^s \\
&= \sum_{g \in F_0} y_g g^s + \sum_{g' \in F_0} z_{g'+\alpha_{m-1}} \sum_{i \preceq s} \binom{s}{i} g'^i (\alpha_{m-1})^{s-i} \\
&= \sum_{g \in F_0} y_g g^s + \sum_{g' \in F_0} z_{g'+\alpha_{m-1}} \sum_{i \preceq s} g'^i (\alpha_{m-1})^{s-i} \\
&= \sum_{g \in F_0} y_g g^s + \sum_{i \preceq s} (\alpha_{m-1})^{s-i} \sum_{g \in F_0} z_{g+\alpha_{m-1}} g^i \\
&= \sum_{g \in F_0} y_g g^s + \sum_{g \in F_0} z_{g+\alpha_{m-1}} g^s + \sum_{i \prec s} (\alpha_{m-1})^{s-i} \sum_{g \in F_0} z_{g+\alpha_{m-1}} g^i \\
&= \sum_{g \in F_0} (y_g + z_{g+\alpha_{m-1}}) g^s + \sum_{i \prec s} (\alpha_{m-1})^{s-i} \sum_{g \in F_0} z_{g+\alpha_{m-1}} g^i.
\end{aligned}$$

In the previous equations, $\preceq$ denotes the *partial ordering* defined by

$$(i_0, i_1, \ldots, i_{m-1}) \preceq (s_0, s_1, \ldots, s_{m-1}) \text{ if and only if } i_j \leq s_j, \ \forall j \in [0, m-1],$$

where $(i_0, i_1, \ldots, i_{m-1})$ and $(s_0, s_1, \ldots, s_{m-1})$ are the binary decompositions of i and s. From Lucas' theorem, we have

$$\binom{s}{i} = 1 (\mathrm{mod}\, 2) \quad \text{if and only if} \quad i \preceq s.$$

But $z \in B$ implies $(0, z) \in B \oplus B$, so there exists $y' \in B$ such that $y'_g = z_{g+\alpha_{m-1}}$, $\forall g \in F_0$. We conclude

$$\sum_{g \in \mathbf{F}} x_g g^s = \sum_{g \in F_0} (y_g + z_{g+\alpha_{m-1}}) g^s + \sum_{i \prec s} (\alpha_{m-1})^{s-i} \sum_{g \in F_0} y'_g g^i. \tag{9}$$

Proposition 3 *With the notation*

$$S = \{j \notin \mathcal{I} \mid \forall i \prec j \Rightarrow i \in \mathcal{I}\}, \tag{10}$$

the restriction of ϕ_s to the code $B \oplus B$ is the zero map, for each $s \in \mathcal{I}$ and

$$\phi_s(y, z) = \sum_{g \in F_0} (y_g + z_{g+\alpha_{m-1}}) g^s, \tag{11}$$

for each $s \in S$ and all $y, z \in B$.

Proof. For $s \in S$, Relation (9) can be written

$$\sum_{g \in \mathbf{F}} x_g g^s = \sum_{g \in F_0} (y_g + z_{g+\alpha_{m-1}}) g^s + \sum_{i \prec s,\, i \in \mathcal{I}} (\alpha_{m-1})^{s-i} \sum_{g \in F_0} y'_g g^i.$$

It is also true that $(y', 0) \in \mathrm{EC}^{\perp}$, so $\sum_{g \in F_0} y'_g g^i = 0$, $\forall i \in \mathcal{I}$, and (11) is proved. ◇

Proposition 4 *Let (B, B) denote the code with generator matrix (G_B, G_B). Then the restriction of ϕ_s to (B, B) is the zero map, for each $s \in \mathcal{I} \cup S$. Consequently, the dimension of B, k_B, verifies*

$$k_B = k_{(B,B)} \leq 2^m - (|\mathcal{I}| + |S|).$$

Proof. As (B, B) is a subcode of $B \oplus B$, Relation (11) is true. But $x = (y, z) \in (B, B)$ implies $y_g = z_{g+\alpha_{m-1}}$ for each $g \in F_0$. ◇

Remark 2 Since the relation $k_B < (2^m - |\mathcal{I}|)/2$ is obvious, the previous bound is interesting only if $2^m - (|\mathcal{I}| + |S|) < (2^m - |\mathcal{I}|)/2$, so if $|S| > (2^m - |\mathcal{I}|)/2$. □

Corollary 1 *Assume that for an $s \in S$ there exists only one i ($i \in \mathcal{I}$) such that $i \prec s$. Then, for all $(y, z) \in (B, B)$, we have $y' = y$ in Relation (9) and $\phi_s(y,z) = (\alpha_{m-1})^{s-i} \sum_{g \in F_0} y_g g^i$. More precisely,*

$$\phi_s(y,z) = (\alpha_{m-1})^{s-i} \phi_i(y,0), \quad \forall\, (y,\, z) \in (B,\, B).$$

Now we are interested in the exact computation of the codes B obtained by the LTSC of $\mathrm{EBCH}^{\perp}(2^m, \delta)$, more precisely in finding all the values of δ for which

$$B(2^m, \delta) = RM(r-1,\, m-1). \tag{12}$$

If m is fixed, one method consists in decomposing all the $\mathrm{EBCH}^{\perp}(2^m, \delta)$ and in computing the dimension (and the minimum distance) of B. If we obtain the parameters of a Reed-Muller code, we directly check the equality, as both codes are in standard bit order. The following table presents the parameters for which B is an RM code (also up to one row in the generator matrix), for $m \in \{5, 6, 7, 8, 9\}$.

B	2^m, δ	B	2^m, δ
RM$(0,4)$	32, $\{3,5\}$	RM$(3,6)+[64,1,12]$	128, 47
RM$(1,4)$	32, 7	RM$(4,6)$	128, 63
RM$(2,4)$	32, 15	RM$(0,7)$	256, $\{3,5,7,9\}$
RM$(0,5)$	64, $\{3,5\}$	RM$(1,7)$	256, $\{19,21\}$
RM$(1,5)$	64, 11	RM$(2,7)$	256, 39
RM$(2,5)+[32,1,8]$	64, 23	RM$(4,7)+[128,1,16]$	256, 95
RM$(3,5)$	64, 31	RM$(5,7)$	256, 127
RM$(0,6)$	128, $\{3,5,7,9\}$	RM$(0,8)$	$512, 3 \le \delta \le 17$
RM$(1,6)$	128, $\{11,13\}$	RM$(1,8)$	512, $\{19, 21, 23, 25\}$
RM$(1,6)+[64,1,28]$	128, $\{15,19\}$	RM$(1,8)+[256,1,128]$	512, $\{27, 29, 31, 35\}$
RM$(2,6)$	128, $\{23,27\}$	RM$(6,8)$	512, 255

Remark 3 For fixed r and m, one can easily remark that the smallest δ in the table (if it exists), is the minimum of δ-s greater than the greatest representative of weight r in a cyclotomic coset modulo $(2^m - 1)$ (via Proposition 1). □

Numerical results indicates that in Relation (7), the order $r_1 - 1$ is respected, but the order $r_2 - 1$ can be actually reduced in many cases. This suggests that B is an RM when an inclusion

$$RM(r_1 - 1,\, m-1) \subseteq B(2^m, \delta) \subseteq RM(r_1,\, m-1) \tag{13}$$

is verified. Now, once a δ verifing (12) is found, we have to check the designed distances greater than this value as well, because in many cases the code B can be the same for different $EBCH^{\perp}(2^m, \delta)$ (see our numerical results in Section 4).

Remark 4 Assume that we succeed in proving a relation as

$$(B, B) \subset RM(r, m),$$

for a certain r. So the row space of the matrix (G_B, G_B) is contained in the row space of the matrix

$$\begin{pmatrix} G_{RM}(r, m-1) & G_{RM}(r, m-1) \\ 0 & G_{RM}(r-1, m-1) \end{pmatrix}$$

and finally $B \subseteq RM(r, m-1)$. By passing from (B, B) to B, only the length, and not the order, of the corresponding RM code decreases. □

Now we try to apply the bound given in Proposition 4. In the following examples, (i) denotes the cyclotomic coset of i.

1. for $\delta \in \{3,\, 2^{m-1}\}$ obviously,

$$B(2^m, 3) = RM(0, m-1) \quad \text{and} \quad B(2^m, 2^{m-1} - 1) = RM(m-3, m-1);$$

2. for $\delta = 5$, the defining set of $\mathrm{EBCH}^{\perp}(2^m, 5)$ is $[0, 2^m - 1]\backslash\{(-1) \cup (-3)\}$. But $-1 = (0111\ldots1)$, $-3 = (0011\ldots1)$, so $S = (-3)$. Now (B, B) is a subcode of the code with defining set $[0, 2^m - 1]\backslash(-1)$ which is precisely formed by all integers of weight $< m - 1$, so $\mathrm{RM}(1, m)$. This implies $B \subseteq RM(1, m-1)$. Computation gives $B = RM(0, m-1)$ for $m \geq 5$.

3. for $\delta = 7$, the defining set of $\mathrm{EBCH}^{\perp}(2^m, 7)$ is $[0, 2^m-1]\backslash\{(-1)\cup(-3)\cup(-5)\}$. But $-1 = (0111\ldots1)$, $-3 = (0011\ldots1)$, $-5 = (0101\ldots1)$, so $S = (-3) \cup (-5)$ and therefore (B, B) is a subcode of the code with defining set formed by all integers of weight $< m-1$, so $\mathrm{RM}(1, m)$. Computation gives $B = RM(1, m-1)$ for $m = 5$ and $B = RM(0, m-1)$ for $m \geq 7$.

One case when we find a set S of greater cardinality than in the previous examples is $m = 8$ and $\delta = 19$. The set of non-zeros of the code $\mathrm{EBCH}^{\perp}(256, 19)$ is

$$(15) \cup (31) \cup (47) \cup (61) \cup (63) \cup (95) \cup (111) \cup (119) \cup (127).$$

Binary decomposition gives $15 = (11110000)$, $31 = (11111000)$, $47 = (11110100)$, $61 = (10111100)$, $63 = (11111100)$, $95 = (11111010)$, $111 = (11110110)$, $119 = (11101110)$, $127 = (11111110)$, so $15 \prec 31$, $15 \prec 47$, $15 \prec 63$, $15 \prec 95$, $15 \prec 111$, $15 \prec 127$ and finally

$$S = (15) \cup (61) \cup (119).$$

Now $I \cup S$ contains all the integers of weight ≤ 4 and we deduce $(B, B) \subset RM(8-4-1, 8)$, $B \subset RM(3, 7)$ and in fact $B = RM(1, 7)$ (see the previous table).
Open problem: Find those $\mathrm{EBCH}^{\perp}$ codes for which the component code B is a RM code.

Remark 5 Exactly as the codes B, the codes A are recursive LTSC codes. Then they may be compared to the $\mathrm{EBCH}^{\perp}$ of length equal to the length of A. As an example, if $A(2^m, \delta)$ denotes the code A constructed via the decomposition of $\mathrm{EBCH}^{\perp}(2^m, \delta)$, we obtained that $A(128, 9)$ and $EBCH^{\perp}(64, 11)$ (both in standard bit order) are two $[64, 28, 14]$ *different* codes related by

$$A(128, 9) \cap EBCH^{\perp}(64, 11) = A(128, 7). \quad \square$$

4 Minimal distances and estimations

In this section we list updated results on the dual distances of the $\mathrm{EBCH}^{\perp}$ codes of length 512. For comparison with the results presented in [13], we also give the twisted squaring decomposition of these codes for length 256. The parameters in the tables are as follows:

1. δ denotes the designed distance of the BCH code;

2. k is the dimension of the corresponding $\mathrm{EBCH}^{\perp}$ code;

3. $d^{\perp}_{\max}$ denotes the upper bound on the dual distance (in italic) or the actual dual distance (obtained in all cases by using Magma [9]);

4. A and B are the codes obtained by the LTSC decomposition of the corresponding code $\mathrm{EBCH}^{\perp}(n, \delta)$ *in standard bit order*;

5. $(A/B, \widetilde{A/B})$ is the code obtained by taking the complement of $\mathrm{EBCH}^{\perp}$ by the direct sum $B \oplus B$;

6. the second to last column in our tables indicates the number of null columns in a generator matrix of the code $(A/B, \widetilde{A/B})$. Its importance was discussed in Section 2;

7. the last column in the tables gives the order of the greater Reed-Muller code contained in $\mathrm{EBCH}^{\perp}(n, \delta)$.

We are now going to analyze the numerical results, which we obtain by applying the Canteaut-Chabaud' probabilistic algorithm and the linear twisted squaring decomposition of the duals of BCH codes.

The probabilistic algorithm takes as inputs the length, the dimension and a generator matrix of the code; it searches for a codeword of small weight, close to the conjectured minimum distance, and returns the support of such a codeword. For $n \leq 512$, the parameters of the algorithm [4, p.369] are $p = 1$ and $\sigma = \lceil \log(n)/\log(2) \rceil$.

By applying this algorithm to the EBCH$^\perp$ codes, we obtained for $n = 256$ the same upper bounds as in [13] (see our numerical results at the end of this section). In the case $n = 512$, we obtain new upper bounds on the dual distances. Some problems appear for $n \geq 512$, since for a given length the complexity of the algorithm is maximal when k is close to $n/2$. Let us consider the dual distance as a function of the designed distance of the corresponding BCH code. One can easily prove that this is a *decreasing function*. As soon as, for instance, we found a 64-weight codeword in EBCH$^\perp(512, 37)$, we have proved that there exist codewords of weight less than or equal to 64 in all EBCH$^\perp(512, \delta)$ with $\delta \geq 37$. However, we cannot obtain such a codeword directly in all cases; for example, we only found a 82-weight codeword if $\delta = 57$ or a 66-weight codeword if $\delta = 73$. Nevertheless, we kept the values obtained via this algorithm in our tables, even when they are sharpened by LTSC (using the bound in (5)). *When two values are given for $d^\perp_{max}$, the first (obtained by LTSC), improves the second (obtained via the minimum-weight algorithm).*

There are some codes for which we do not compute $d^\perp_{\max}$ by using directly the probabilistic algorithm. As previously discussed, once a 64-weight codeword is found in EBCH$^\perp(512, 37)$ and in EBCH$^\perp(512, 57)$, therefore for all codes of $37 \leq \delta \leq 57$, the expected value for $d^\perp_{\max}$ is 64, because of the monotonicity

$$\delta_1 < \delta_2 \Rightarrow EBCH^\perp(n, \delta_1) \subset EBCH^\perp(n, \delta_2). \tag{14}$$

By the same argument, the expected value of $d^\perp_{\max}$ when $87 \leq \delta \leq 107$ is 32.

Now consider the LTSC decomposition of the codes involved in (14). These codes are therefore put *in standard bit order* by the same permutation, and the inclusion is still true. One can easily deduce analogous inclusions for the corresponding codes A and B, by using their definitions. Using this monotonicity, we emphasize that all the codes A (resp. B) with identical parameters are *equal*. When these codes are Reed-Muller codes (or up to one row of the generator matrix), they are marked out in our tables by *a star*.

Remark 6 The parameters of the component codes are obtained by using Magma. Only the values in *italic* are upper bounds and not exact minimum distances. Tighter bounds, in second position in the tables, are obtained by applying the probabilistic algorithm to the corresponding component codes (generally B or $(A/B, \widetilde{A/B})$). Concerning the codes $(A/B, \widetilde{A/B})$, no inclusion similar to (14) is expected, so upper bounds for their minimum distances have to be searched for each of them. □

Remark 7 For all codes of length 256 for which only an upper bound is given in [13], we find a word of this weight in the code $(A/B, \widetilde{A/B})$. Also, in all cases for $n = 128$ and almost all cases for $n = 512$, a codeword of weight $d^\perp_{\max}$ is found in one of the codes $B \oplus B$ (or simply B) and $(A/B, \widetilde{A/B})$. Therefore, *these codes are potential minimum-weight subcodes.*

Nevertheless, some exceptions have been found. For EBCH$^\perp(512, 175)$ we cannot find any 14-weight codeword in B, so we conclude that it is to be found in a coset of $B \oplus B$ with respect to the complement code. Two other examples are $\delta = 117$ and $\delta = 123$. On the contrary, for $\delta = 35$, we found a 106-weight codeword in the complement code, improving the value obtained by using the minimum-weight algorithm. □

The order of the RM code in the last columns is obtained via Proposition 1 by passing to the dual codes. Once again, let us remark that a Reed-Muller code in the fifth column has firstly to be searched on the line which corresponds to the increase of the order of RM in the last column.

Parameters of the LTSC construction for codes of length 256

δ	k	$d^{\perp}_{\max}$	A	B	$(A/B, \widetilde{A/B})$	no.null col.	RM
3	9	128	[128,8,64]*	[128,1,128]*	[256,7,128]	2	1
5	17	112	[128,16,48]	[128,1,128]*	[256,15,112]	2	1
7	25	96	[128,24,32]	[128,1,128]*	[256,23,96]	2	1
9	33	96	[128,32,32]	[128,1,128]*	[256,31,96]	2	1
11	41	64	[128,37,*32*]	[128,4,64]	[256,33,64]	8	1
13	49	64	[128,45,*24*]	[128,4,64]	[256,41,64]	8	1
15	57	64	[128,53,*24*]	[128,4,64]	[256,49,64]	8	1
17	65	*60*	[128,61,18]	[128,4,64]	[256,57,*60*]	8	1
19	69	*60*	[128,61,18]	[128,8,64]*	[256,53,*60*]	16	2
21	77	*56*	[128,69,*16*]	[128,8,64]*	[256,61,*56*]	16	2
23	85	*48*	[128,72,*16*]	[128,13,48]	[256,59,*48*]	26	2
25	93	*48*	[128,80,*12*]	[128,13,48]	[256,67,*48*]	26	2
27	101	*48*	[128,80,*12*]	[128,21,48]	[256,59,*48*]	42	2
29	109	*40*	[128,88,8]	[128,21,48]	[256,67,*40*]	42	2
31	117	*36*	[128,96,8]	[128,21,48]	[256,75,*36*]	42	2
37	125	*36*	[128,104,6]	[128,21,48]	[256,83,*36*]	42	2
39	133	*32*	[128,104,6]	[128,29,32]*	[256,75,*32*]	58	3
43	141	*28*	[128,104,6]	[128,37,32]	[256,67,*28*]	74	3
45	149	*26*	[128,107,6]	[128,42,28]	[256,65,*26*]	84	3
47	157	16	[128,107,6]	[128,50,16]	[256,57,24]	100	3
51	165	16	[128,115,4]	[128,50,16]	[256,65,20]	100	3
53	169	16	[128,115,4]	[128,54,16]	[256,61,16]	108	3
55	177	16	[128,115,4]	[128,62,16]	[256,53,16]	124	3
59	185	16	[128,120,4]*	[128,65,16]	[256,55,16]	130	3
61	193	16	[128,120,4]*	[128,73,16]	[256,47,16]	146	3
63	201	12	[128,120,4]*	[128,81,12]	[256,39,12]	162	3
85	209	12	[128,127,2]*	[128,82,12]	[256,45,12]	164	3
87	211	12	[128,127,2]*	[128,84,12]	[256,43,12]	168	4
91	219	10	[128,127,2]*	[128,92,10]	[256,35,10]	184	4
95	227	8	[128,127,2]*	[128,99+1,8]*	[256,27,8]	200	5
111	235	6	[128,127,2]*	[128,108,6]	[256,19,6]	216	5
119	243	4	[128,127,2]*	[128,116,4]	[256,11,4]	232	5
127	247	4	[128,127,2]*	[128,120,4]*	[256,7,4]	240	6

Parameters of the LTSC construction for codes of length 512

δ	k	$d^{\perp}_{\max}$	A	B	$(A/B, \widetilde{A/B})$	no.null col.	RM
3	10	256	[256,9]*	[256,1,256]*	[512,8]	2	1
5	19	240	[256,18]	[256,1,256]*	[512,17]	2	1
7	28	224	[256,27]	[256,1,256]*	[512,26]	2	1
9	37	196	[256,36]	[256,1,256]*	[512,35]	2	1
11	46	192	[256,45]	[256,1,256]*	[512,44,*192*]	2	1
13	55	*184*	[256,54]	[256,1,256]*	[512,53,*184*]	2	1
15	64	*168*	[256,63]	[256,1,256]*	[512,62,*168*]	2	1
17	73	*164*	[256,72]	[256,1,256]*	[512,71,*168(164)*]	2	1

δ	k	$d_{\max}^{\perp}$	A	B	$(A/B, \widetilde{A/B})$	no.null col.	RM
19	82	*128*	[256,73]	[256,9,128]*	[512,64,*128*]	18	2
21	91	*128*	[256,82]	[256,9,128]*	[512,73]	18	2
23	100	*128*	[256,91]	[256,9,128]*	[512,82]	18	2
25	109	*128*	[256,100]	[256,9,128]*	[512,91,*128*]	18	2
27	118	*112*	[256,108]	[256,9+1,112]*	[512,98,*112*]	20	2
29	127	*112*	[256,117]	[256,9+1,112]*	[512,107,*112*]	20	2
31	136	*108*	[256,126]	[256,9+1,112]*	[512,116,*108*]	20	2
35	145	*106(108)*	[256,135]	[256,9+1,112]*	[512,125,*106*]	20	2
37	154	*64*	[256,135]	[256,19,64]	[512,116,*64*]	38	2
39	163	*64*	[256,138]	[256,25,64]	[512,113]	50	2
41	172	*64*	[256,147]	[256,25,64]	[512,122]	50	2
43	181	*64*	[256,147]	[256,34,64]	[512,113]	68	2
45	190	*64*	[256,156]	[256,34,64]	[512,122]	68	2
47	199	*64*	[256,165]	[256,34,64]	[512,131]	68	2
51	208	*64*	[256,174]	[256,34,64]	[512,140]	68	2
53	217	*64*	[256,181]	[256,36,64]	[512,145]	72	2
55	226	*64*	[256,181]	[256,45,64]	[512,136,*64*]	90	2
57	235	*64(82)*	[256,190]	[256,45,64]	[512,145,*64*]	90	2
59	244	*56*	[256,190]	[256,54,56]	[512,136,*56*]	108	2
61	253	*56*	[256,199]	[256,54,56]	[512,145,*56*]	108	2
63	262	*56(70)*	[256,208]	[256,54,56]	[512,154]	108	2
73	271	*56(66)*	[256,217]	[256,54,56]	[512,163]	108	2
75	274	*56(64)*	[256,217]	[256,57,*56*]	[512,160]	114	3
77	283	*56(62)*	[256,217]	[256,66,*56*]	[512,151,*62*]	132	3
79	292	*48*	[256,217]	[256,75,*48*]	[512,142,*48*]	150	3
83	301	*48(54)*	[256,217]	[256,84,*48*]	[512,133,*48*]	168	3
85	310	*48(52)*	[256,217]	[256,93,*48*]	[512,124,*48*]	186	3
87	319	*32*	[256,217]	[256,102,*32*]	[512,115,*32*]	204	4
91	328	*32*	[256,225]	[256,103,*32*]	[512,122,*32*]	206	4
93	337	*32*	[256,228]	[256,109,*32*]	[512,119,*32*]	218	4
95	346	*32*	[256,228]	[256,118,*32*]	[512,110,*32*]	236	4
103	355	*32*	[256,237]	[256,118,*32*]	[512,119,*32*]	236	4
107	364	*32*	[256,237]	[256,127,*32*]	[512,110,*32*]	254	4
109	373	*28*	[256,237]	[256,136,*28*]	[512,101,*28(32)*]	272	4
111	382	*28*	[256,237]	[256,145,*28*]	[512,92,*28*]	290	4
117	391	*26*	[256,246]	[256,145,*28*]	[512,101,*28*]	290	4
119	400	*24*	[256,246]	[256,154,*24*]	[512,92,*24*]	308	4
123	409	*22*	[256,247]*	[256,162,*24*]	[512,85,20-24]	324	4
125	418	*20*	[256,247]*	[256,171,*20*]	[512,76,22-24]	342	4
127	427	*16*	[256,247]*	[256,180,*16*]	[512,67,20]	360	4
171	436	*16*	[256,255]*	[256,181,*16*]	[512,74,20]	362	4
175	445	*14*	[256,255]*	[256,190,*16*]	[512,65,16]	380	5
175	445	*14*	[256,255]*	[256,190,*16*]	[512,65,16]	380	5
183	454	8	[256,255]*	[256,199,8]	[512,56,14]	398	5
187	463	8	[256,255]*	[256,208,8]	[512,47,12]	416	5
191	472	8	[256,255]*	[256,217,8]	[512,38,8]	434	5
219	481	8	[256,255]*	[256,226,8]	[512,29,8]	452	5
223	484	8	[256,255]*	[256,229,8]	[512,26,8]	458	6
239	493	6	[256,255]*	[256,238,6]	[512,17,6]	476	6
255	502	4	[256,255]*	[256,247,4]*	[512,8,4]	494	7

5 Conclusion

In this paper, we determine new upper bounds on the dual distances of binary BCH codes with length 512. It arises that two subcodes are of special importance, as they often contain minimum-weight codewords (up to three cases for $n \leq 512$), which were found with a probabilistic algorithm and even updated in some cases by LTSC. The LTSC decomposition is particularly interesting for greater lengths; notably it can be easily obtained for all EBCH codes and their duals. Therefore we are led to work with codes with reduced length and dimension (see Remark 1 in Section 2). Thereby, we propose several ways for theoretical purpose. Further researches can be concentrated on the characterization of the codes A and B, on their algebraic properties and on their links with other affine-invariant codes.

6 Acknowledgments

The author is very grateful to Pascale Charpin for useful discussions, especially concerning the results in Section 3, and for her careful and patient reading of the manuscript. She also thanks Anne Canteaut for programming help, especially for allowing the use of her minimum-weight searching program, as well as the UMS MEDICIS (FRE 2341) service in computer algebra at the CNRS/Polytechnique for providing computing facilities.

References

[1] D. Augot and F. Levy-dit-Vehel, Bounds on the Minimum Distance of the Duals of the BCH Codes, IEEE Trans. Inform. Theory, vol. 42, no. 4, pp. 1257–1260, July 1996.

[2] Y. Berger and Y. Be'ery, The Twisted Squaring Construction, Trellis Complexity and Generalized Weights of BCH and QR Codes, IEEE Trans. Inform. Theory, vol. 42, no. 6, pp. 1817–1827, Nov. 1996.

[3] W. Bosma and J. Cannon, *Handbook of Magma Functions,* School of Mathematics and Statistics, University of Sydney, Sydney, 1995.

[4] A. Canteaut and F. Chabaud, A New Algorithm for Finding Minimum-Weight Words in a Linear Code: Application to McEliece's Cryptosystem and to Narrow-Sense BCH Codes of Length 511, IEEE Trans. Inform. Theory, vol. 44, no. 1, pp. 367–378, Jan. 1998.

[5] P. Charpin, Open Problems on Cyclic Codes, *Handbook of Coding Theory,* V.S. Pless and W.C. Huffman, Eds., Elsevier Science, North-Holland, 1998.

[6] Y. Desaki, T. Fujiwara and T. Kasami, The Weight Distributions of Extended Binary Primitive BCH Codes of Length 128, IEEE Trans. Inform. Theory, vol. 43, no. 4, pp. 1364–1371, July 1997.

[7] G.D. Forney, Jr., "Coset Codes-Part 2: Binary Lattices and Related Codes", *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1152–1187, Sept. 1988.

[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam, The Nederlands: North-Holland, 1977.

[9] MAGMA web page: http://www.maths.usyd.edu.au:8000/u/magma/

[10] MEDICIS web page: http://www.medicis.polytechnique.fr

[11] V.S. Pless, W.C. Huffman and R.A. Brualdi, An Introduction to Algebraic Codes, *Handbook of Coding Theory*, V.S. Pless, W.C. Huffman, Eds, Elsevier, 1998.

[12] F. Rodier, On the Minimum Distance of the Duals of 4-Error Correcting Extended BCH Codes, IEEE Trans. Inform. Theory, vol. 45, no. 5, pp. 1677–1678, July 1999.

[13] M. Sala, Upper Bounds on the Dual Distance of BCH$(255, k)$, Designs, Codes and Cryptography, vol. 30, pp. 159–168, 2003.

[14] M. Sala and A. Tamponi, A Linear Programming Estimate of the Weight Distribution of BCH$(255, k)$, IEEE Trans. Inform. Theory, vol. 46, no. 6, pp. 2235–2237, Sept. 2000.

[15] Weight Distribution Tables: http://www.logic.cs.hiroshima-cu.ac.jp/wd.

Contents

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399