More on the Covering Radius of BCH Codes

Françoise Levy-Dit-Vehel, Simon Litsyn

▶ To cite this version:

Françoise Levy-Dit-Vehel, Simon Litsyn. More on the Covering Radius of BCH Codes. [Research Report] RR-2656, INRIA. 1995. inria-00074033

HAL Id: inria-00074033
https://inria.hal.science/inria-00074033

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

More on the Covering Radius of BCH Codes

Françoise Lévy-dit-Véhel - Simon Litsyn

N° 2656
Octobre 1995

PROGRAMME 2

Rapport de recherche

Les rapports de recherche de l'INRIA
sont disponibles en format postscript sous
ftp.inria.fr (192.93.2.54)

si vous n'avez pas d'accès ftp
la forme papier peut être commandée par mail :
e-mail : dif.gesdif@inria.fr
(n'oubliez pas de mentionner votre adresse postale).

par courrier :
Centre de Diffusion
INRIA
BP 105 - 78153 Le Chesnay Cedex (FRANCE)

INRIA research reports
are available in postscript format
ftp.inria.fr (192.93.2.54)

if you haven't access by ftp
we recommend ordering them by e-mail :
e-mail : dif.gesdif@inria.fr
(don't forget to mention your postal address).

by mail :
Centre de Diffusion
INRIA
BP 105 - 78153 Le Chesnay Cedex (FRANCE)

Sur le rayon de recouvrement des codes BCH
More on the covering radius of BCH codes *

Françoise Levy-dit-Vehel[1] and Simon Litsyn[2]

Résumé

Nous présentons de nouvelles bornes sur la longueur à partir de laquelle le rayon de recouvrement du code BCH binaire t-correcteur est au plus $2t$.

Mots-clef : rayon de recouvrement, codes BCH, systèmes d'équations sur les corps finis.

Abstract

New lower bounds on the minimum length of t-error correcting BCH codes with covering radius at most $2t$ are derived.

Keywords : covering radius, BCH codes, systems of equations over finite fields.

*To appear in IEEE TRANSACTIONS ON INFORMATION THEORY

[1] Institut National de Recherche en Informatique et Automatique (INRIA), Domaine de Voluceau, Rocquencourt, B.P.105, 78153 Le Chesnay Cedex, FRANCE

[2] Tel Aviv University, Dept. of Electrical Engineering-Systems, P.O.B 39040, Ramat Aviv, Tel Aviv 69978, ISRAEL

More on the covering radius of BCH codes

1 Introduction

Covering radius is an important parameter of error-correcting codes (see e.g. [2, 3]). It characterizes the largest multiplicity of errors that can be corrected by maximum likelihood decoder in BSC. A code is called *maximal* if one can not add a word to it without decreasing its minimum distance. Indeed, maximality can be guaranteed by proving that the covering radius of the code is less than the minimum distance.

Covering radius of BCH codes has gained a great deal of interest. For two- and three- error correcting BCH codes, it was determined in [1, 4, 5, 8]. Further research on the topic was initiated by a paper of T.Helleseth [6]. In [13] A.Tietäväinen proved that the covering radius of $t-$error correcting BCH codes of length $(2^m - 1)/N$ is less than or equal to $2t$ provided

$$2^m \geq ((2t-1)N)^{4t+2}. \qquad (1)$$

A.Skorobogatov and S.Vläduts [15] determined the covering radius of very long primitive BCH codes to be exactly $2t - 1$. Estimates for the lengths from which it is true were given by O.Moreno and C.Moreno [11] and Y.Kaipainen [9]. For t of the form $2^u + 1$ the same result was obtained by A.Tietäväinen [14] for much smaller lengths. For non-primitive BCH codes it was shown in [15] that the covering radius is lowerbounded by $2t$.

In this paper we further improve the estimates on the length of BCH codes starting from which the covering radius is upperestimated by $2t$. It thus gives a new range when primitive BCH-codes are surely maximal, and answers a question of [7]. For the non-primitive case we simplify the proof of [15] that $2t$ is the lower bound. Using a similar technique as in the primitive case we further extend the set of possible lengths for which we know the covering radius exactly.

2 The primitive case

Theorem 1 *The t-error correcting BCH-code of length $2^m - 1$ has covering radius $R \leq 2t$, provided*

1. $m \geq 15$ *for* $t = 4$,

2. $m \geq 20$ *for* $t = 5$,

3. $2^m \geq 4(1+\varepsilon(t))(t-1)^2(t!)^2$, *where* $\varepsilon(t)$ *is a decreasing function of* t *and* $\varepsilon(t) < \frac{e^{2t}}{(t-1)^{2(t-1)}}$ *for* $t \geq 5$.

Proof
Let $BCH(2t+1)$ stand for the t-error correcting BCH code of length $2^m - 1$.

By the form of the parity-check matrix of $BCH(2t+1)$, we have that R is the smallest integer such that, for any $(b_1, \ldots, b_t)$ in $\mathbf{F}_{2^m}^t \setminus \{\mathbf{0}\}$ and for at least one $i \leq R$, the system

$$\left\{ \begin{array}{lcl} x_1 + \ldots + x_i & = & b_1 \\ x_1^3 + \ldots + x_i^3 & = & b_2 \\ \vdots & \vdots & \vdots \\ x_1^{2t-1} + \ldots + x_i^{2t-1} & = & b_t \end{array} \right. \tag{2}$$

has a solution $(x_1, \ldots, x_i) \in (\mathbf{F}_{2^m} \setminus \{0\})^i$, with $x_l \neq x_j$ for $l \neq j$. (Note that, if $(b_1, \ldots, b_t) = \mathbf{0}$, it corresponds to the zero codeword, and, by convention, we assume in this case that $i = 0$).

Using an idea of Tietäväinen [13], we consider the homogeneous system

$$\left\{ \begin{array}{lcl} x_1 + \ldots + x_i & = & b_1 y \\ x_1^3 + \ldots + x_i^3 & = & b_2 y^3 \\ \vdots & \vdots & \vdots \\ x_1^{2t-1} + \ldots + x_i^{2t-1} & = & b_t y^{2t-1} \end{array} \right. \tag{3}$$

If this system has a solution $(x_1, \ldots, x_i, y) = (\xi_1, \ldots, \xi_i, \zeta)$, with $\zeta \in \mathbf{F}_{2^m} \setminus \{0\}$, then the first one has the solution $(\xi_1/\zeta, \ldots, \xi_i/\zeta)$.

A straightforward consequence of the fact that

$$\sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(\alpha x)} = 2^m \delta_{\alpha,0}$$

(Tr being the trace function from $\mathbf{F}_{2^m}$ onto $\mathbf{F}_2$), is that the number of solutions $(x_1, \ldots, x_i, y) \in (\mathbf{F}_{2^m} \setminus \{0\})^{i+1}$ of (3), with $x_i \neq x_j$ for $i \neq j$, is

$$N_i = \frac{1}{2^{mt}} \sum_{0<x_1<\ldots<x_i, y\neq 0}$$

$$\sum_{\alpha_1 \in \mathbf{F}_{2^m}} (-1)^{Tr(\alpha_1(x_1+\ldots+x_i+b_1 y))} \ldots \sum_{\alpha_t \in \mathbf{F}_{2^m}} (-1)^{Tr(\alpha_t(x_1^{2t-1}+\ldots+x_i^{2t-1}+b_t y^{2t-1}))},$$

(after having chosen an order on $\mathbf{F}_{2^m}$).

We have :

$$2^{mt} N_i = \sum_{\alpha_1,\ldots,\alpha_t} \sum_{y \neq 0} (-1)^{Tr(\alpha_1 b_1 y + \ldots + \alpha_t b_t y^{2t-1})}$$

$$\sum_{0<x_1<\ldots<x_i} (-1)^{Tr(\alpha_1 x_1 + \alpha_2 x_1^3 + \ldots + \alpha_t x_1^{2t-1})} \ldots (-1)^{Tr(\alpha_1 x_i + \alpha_2 x_i^3 + \ldots + \alpha_t x_i^{2t-1})}.$$

Let β be a primitive element in $\mathbf{F}_{2^m}$. Denote by $f_{\underline{\alpha}}(z)$, the polynomial $f_{\underline{\alpha}}(z) = \sum_{j=1}^t \alpha_j z^{2j-1}$, where $\underline{\alpha} = (\alpha_1, \ldots, \alpha_t)$.

In the inner sum $S_{\underline{\alpha}} = \sum_{0<x_1<\ldots<x_i} (-1)^{Tr(\alpha_1 x_1 + \alpha_2 x_1^3 + \ldots + \alpha_t x_1^{2t-1})} \ldots (-1)^{Tr(\alpha_1 x_i + \alpha_2 x_i^3 + \ldots + \alpha_t x_i^{2t-1})}$, every choice of $(x_1, \ldots, x_i)$ corresponds to a choice of i distinct positions in the word $c_{\underline{\alpha}} = (Tr(f_{\underline{\alpha}}(\beta^0)), \ldots, Tr(f_{\underline{\alpha}}(\beta^{n-1})))$ of the dual of $BCH(2t+1)$ (see e.g. [10, p.280]).

A typical term in the sum $S_{\underline{\alpha}}$ thus equals 1 if the corresponding positions of $c_{\underline{\alpha}}$ constitute an even sub-vector, and (-1) if they constitute an odd-subvector. Recalling the definition of MacWilliams transform, we get :

$$2^{mt}N_i = \sum_{\alpha_1,\ldots,\alpha_t} P_i(w_{\underline{\alpha}}) \sum_{y\neq 0} (-1)^{Tr(\alpha_1 b_1 y + \ldots + \alpha_t b_t y^{2t-1})}, \qquad (4)$$

where P_i is the i-th Krawtchouk polynomial, and $w_{\underline{\alpha}}$ is the weight of the word $c_{\underline{\alpha}}$:

$$w_{\underline{\alpha}} = \frac{2^m - 1 - \sum_{x\in\mathbf{F}_{2^m}\setminus\{0\}}(-1)^{Tr(\alpha_1 x + \ldots + \alpha_t x^{2t-1})}}{2}.$$

We are interested in showing that, for m large enough, there exists (at least one) $i \leq 2t$, such that $N_i \neq 0$. If, for a non-zero tuple $(a_0, \ldots, a_{2t})$, we have :

$$\sum_{i=0}^{2t} a_i N_i \neq 0,$$

then at least one N_i is non-zero, and thus $R \leq 2t$.
In fact we show here that, for a non-zero $(2t+1)$-tuple $(a_0, \ldots, a_{2t})$ we give explicitly, $\sum_{i=0}^{2t} a_i N_i > 0$ starting from some length. We have :

$$\begin{aligned} 2^{mt}\sum_{i=0}^{2t} a_i N_i &= \sum_{i=0}^{2t} a_i \sum_{\alpha_1,\ldots,\alpha_t} P_i(w_{\underline{\alpha}}) \sum_{y\neq 0}(-1)^{Tr(\alpha_1 b_1 y + \ldots + \alpha_t b_t y^{2t-1})} \\ &= \sum_{\alpha_1,\ldots,\alpha_t} \sum_{y\neq 0}(-1)^{Tr(\alpha_1 b_1 y + \ldots + \alpha_t b_t y^{2t-1})} \sum_{i=0}^{2t} a_i P_i(w_{\underline{\alpha}}). \qquad (5) \end{aligned}$$

The sum $\sum_{i=0}^{2t} a_i P_i(x)$ represents the expansion of a polynomial of degree $2t$ in the basis of Krawtchouk polynomials $(P_0(x), \ldots, P_{2t}(x))$. We denote by $g_{2t}(x)$, the polynomial $g_{2t}(x) = \sum_{i=0}^{2t} a_i P_i(x)$.
We have

$$2^{mt}\sum_{i=0}^{2t} a_i N_i = (2^m - 1)g_{2t}(0) + \sum_{\underline{\alpha}\in\mathbf{F}_{2^m}^t\setminus\{0\}} g_{2t}(w_{\underline{\alpha}}) \sum_{y\neq 0}(-1)^{Tr(\alpha_1 b_1 y + \ldots + \alpha_t b_t y^{2t-1})}.$$

As $w_{\underline{\alpha}}$ is a weight of $BCH^{\perp}(2t+1)$, we have [10, p.280] :

$$d' \leq w_{\underline{\alpha}} \leq 2^m - d',$$

where $d' \geq 2^{m-1} - (t-1)2^{\frac{m}{2}}$.
We choose at this point a polynomial $g_{2t}(x)$, non-negative in $[d', 2^m - d']$, and positive at 0. By the Carlitz-Uchiyama bound [10, p.280] :

$$\sum_{y\neq 0}(-1)^{Tr(\alpha_1 b_1 y + \ldots + \alpha_t b_t y^{2t-1})} \geq -(t-1)2^{\frac{m}{2}+1} - 1,$$

thus
$$2^{mt}\sum_{i=0}^{2t} a_iN_i \ge (2^m-1)g_{2t}(0) - [(t-1)2^{\frac{m}{2}+1}+1]\sum_{\underline{\alpha}\in\mathbf{F}^t_{2^m}\setminus\{\mathbf{0}\}} g_{2t}(w_{\underline{\alpha}}). \tag{6}$$

According to expression (5), we have

$$\sum_{\underline{\alpha}\in\mathbf{F}^t_{2^m}} g_{2t}(w_{\underline{\alpha}}) = 2^{mt}\sum_{i=0}^{2t} a_iN_i^0,$$

where N_i^0 is the number of solutions of system (2) (or system (3)) with RHS zero (i.e. with $(b_1,\ldots,b_t)$ being the zero t-tuple).
N_i^0 is exactly the number of words of weight i in $BCH(2t+1)$. As the minimum distance of this code is at least $2t+1$, it follows that $N_i^0 = 0$ for $1 \le i \le 2t$ (and $N_0^0 = 1$). Thus :

$$\sum_{\underline{\alpha}\in\mathbf{F}^t_{2^m}} g_{2t}(w_{\underline{\alpha}}) = 2^{mt}a_0.$$

Replacing this value in (6), we get :

$$2^{mt}\sum_{i=0}^{2t} a_iN_i \ge (2^m-1)g_{2t}(0) - [(t-1)2^{\frac{m}{2}+1}+1][2^{mt}a_0 - g_{2t}(0)].$$

Thus to show $\sum_{i=0}^{2t} a_iN_i > 0$, it suffices to show

$$[2^m + (t-1)2^{\frac{m}{2}+1}]g_{2t}(0) - [(t-1)2^{\frac{m}{2}+1}+1]2^{mt}a_0 > 0. \tag{7}$$

In order to find the best lower bound for 2^m, we have to choose a polynomial $g_{2t}(x)$, non-negative in $[d', 2^m - d']$, positive in 0 and of degree $2t$, with maximum ratio $\frac{g_{2t}(0)}{a_0}$.
We choose the polynomial

$$g_{2t}(x) = (\sum_{i=0}^{t} P_i(x))^2. \tag{8}$$

In Appendix 4.1, it is shown that this polynomial is optimal in a certain sense.
We then obtain

$$a_0 = \sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix}, \text{ and } g_{2t}(0) = a_0^2.$$

Thus we have to determine the smallest value of m such that

$$[2^{\frac{m}{2}-1} + (t-1)]2^{\frac{m}{2}+1}\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} - [(t-1)2^{\frac{m}{2}+1}+1]2^{mt} > 0 \tag{9}$$

holds. We have

$$\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} > \frac{2^{mt}}{t!}(1 - \frac{e}{(\frac{t-1}{e})^{2(t-1)}}). \tag{10}$$

(see Appendix 4.2 for a proof). Now, to prove inequality (9), it is sufficient to show :

$$[2^{\frac{m}{2}-1} + (t-1)]2^{\frac{m}{2}+1}\frac{2^{mt}}{t!}(1 - \frac{\epsilon}{(\frac{t-1}{\epsilon})^{2(t-1)}}) - [(t-1)2^{\frac{m}{2}+1} + 1]2^{mt} \geq 0.$$

or,

$$2^{\frac{m}{2}} \geq 2(\frac{t!}{(1 - \frac{\epsilon}{(\frac{t-1}{\epsilon})^{2(t-1)}})} - 1)(t-1) + \frac{t!}{(1 - \frac{\epsilon}{(\frac{t-1}{\epsilon})^{2(t-1)}})2^{\frac{m}{2}}}.$$

By the estimate we derived on 2^m, we see that to satisfy the previous inequality, it is sufficient to have

$$2^{\frac{m}{2}} \geq \frac{2(t-1)}{(1 - \frac{\epsilon}{(\frac{t-1}{\epsilon})^{2(t-1)}})}t!$$

The inequality

$$\frac{1}{(1-x)^2} < 1 + \epsilon x$$

is true for $0 < x < 0.182$. As $\frac{\epsilon}{(\frac{t-1}{\epsilon})^{2(t-1)}} < 0.182$ for $t \geq 5$, we obtain the following lower bound :

$$2^m \geq 4(1 + \varepsilon(t))(t-1)^2(t!)^2,$$

with $\varepsilon(t) < \frac{e^{2t}}{(t-1)^{2(t-1)}}$ for $t \geq 5$. The bounds for $t = 4$ and $t = 5$ given in the theorem have been calculated by inequality (9). □

3 The non-primitive case

In the same spirit as in the primitive case, we shall give an upper bound on the covering radius of non-primitive BCH codes.

Theorem 2 *The t-error correcting BCH-code of length $n = \frac{2^m-1}{N}$ has covering radius $R \leq 2t$, provided*

$$2^m \geq (1 + \varepsilon_N(t))((2t-1)N - 1)^2(t!)^2,$$

where $\varepsilon_N(t)$ is a decreasing function of t satisfying, for $N \geq 2$, $\varepsilon_N(4) < 0.347$, $\varepsilon_N(5) < 0.008$, and $\varepsilon_N(t) < \frac{4e^{2t}}{((2t-1)N-1)^2(t-1)^{2(t-2)}}$ for $t \geq 5$.

Proof

It is essentially the same as the one in the primitive case, so that we just outline the main steps.

Instead of system (3), we consider the system

$$\begin{cases} x_1^N + \ldots + x_i^N & = & b_1 y^N \\ x_1^{3N} + \ldots + x_i^{3N} & = & b_2 y^{3N} \\ \vdots & \vdots & \vdots \\ x_1^{(2t-1)N} + \ldots + x_i^{(2t-1)N} & = & b_t y^{(2t-1)N} \end{cases}$$

If N_i denotes the number of distinct non-zero solutions of this system, we have, just like equation (4),

$$2^{mt}N_i = \sum_{\alpha_1,\dots,\alpha_t} P_i(w_{\underline{\alpha}}) \sum_{y\neq 0}(-1)^{Tr(\alpha_1 b_1 y^N+\dots+\alpha_t b_t y^{(2t-1)N})},$$

where now

$$w_{\underline{\alpha}} = \frac{2^m - 1 - \sum_{x\in\mathbf{F}_{2^m}\setminus\{0\}}(-1)^{Tr(\alpha_1 x+\dots+\alpha_t x^{2t-1})}}{2N}.$$

We have

$$d' \leq w_{\underline{\alpha}} \leq \frac{2^m}{N} - d',$$

with

$$d' \geq \frac{1}{N}[2^{m-1} - (D-1)2^{\frac{m}{2}-1}],\ D = (2t-1)N.$$

The Carlitz-Uchiyama bound here gives

$$\sum_{y\neq 0}(-1)^{Tr(\alpha_1 b_1 y^N+\dots+\alpha_t b_t y^{(2t-1)N})} \geq -(D-1)2^{\frac{m}{2}} - 1,$$

so that we get

$$2^{mt}\sum_{i=0}^{2t} a_i N_i \geq (2^m - 1)g_{2t}(0) - [(D-1)2^{\frac{m}{2}} + 1] \sum_{\underline{\alpha}\in\mathbf{F}_{2^m}^t\setminus\{0\}} g_{2t}(w_{\underline{\alpha}}).$$

As $[d', \frac{2^m}{N} - d'] \subset [0, n]$, we can choose the same polynomial

$$g_{2t}(x) = (\sum_{i=0}^{t} P_i(x))^2.$$

thus, instead of inequality (9), we have to determine the smallest value of m such that

$$[2^{\frac{m}{2}} + (D-1)]2^{\frac{m}{2}}\sum_{i=0}^{t}\binom{n}{i} - [(D-1)2^{\frac{m}{2}} + 1]2^{mt} > 0 \tag{11}$$

holds.

A preliminary lower bound on 2^m can be derived from this and we get :

$$2^{\frac{m}{2}} > \frac{D-1}{2}(t-1)!,$$

and, again using $t! > \left(\frac{t}{e}\right)^t$:

$$2^m > \frac{(D-1)^2}{4}\left(\frac{t-1}{e}\right)^{2(t-1)}.$$

This yields :

$$\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} > \frac{2^{mt}}{t!}\left(1-\frac{4e^3}{(D-1)^2\left(\frac{t-1}{e}\right)^{2(t-2)}}\right).$$

Substituting it in (11), we obtain :

$$2^{\frac{m}{2}} > \frac{(D-1)}{\left(1-\frac{4e^3}{(D-1)^2\left(\frac{t-1}{e}\right)^{2(t-2)}}\right)}t!$$

We conclude in the same way as in the primitive case. □

We will now prove that in the non-primitive case the covering radius can not be less than $2t$. It was first shown in [15]. Here, for the sake of completeness, we give a simpler version of their proof.

Theorem 3 *Provided* $2t-2 < 2^{\lceil \frac{m}{2} \rceil}$, *the t-error correcting BCH code of length* $n = \frac{2^m-1}{N}$, $N > 1$, *has covering radius* $R \geq 2t$.

Proof

The assumption on t ensures that the dimension of this code is $n - mt$. We recall that its covering radius is the smallest integer i such that, given $(b_1, \ldots . b_t) \in \mathbf{F}_{2^m}^t \setminus \{\mathbf{0}\}$, the system

$$\left\{\begin{array}{lcl} x_1^N + \ldots + x_i^N & = & b_1 \\ x_1^{3N} + \ldots + x_i^{3N} & = & b_2 \\ \vdots & \vdots & \vdots \\ x_1^{(2t-1)N} + \ldots + x_i^{(2t-1)N} & = & b_t \end{array}\right. , \qquad (12)$$

has a solution $(x_1, \ldots, x_i)$ with $x_k^N \neq x_l^N$ for $k \neq l$.

We prove that there exists RHSs for which this system has no solution in (strictly) less than $2t$ variables.

Consider system (12) with RHS $(b_1, \ldots, b_t)$ where $b_1 \in \mathbf{F}_{2^m} \setminus \{0\}$, and $b_j = b_1^{2j-1}$. Let us denote this system by (S).

Let $(\xi_1, \ldots, \xi_i)$ be a solution of (S), with $\xi_k^N \neq \xi_l^N$ for $k \neq l$. Then the system, say (S'),

$$\left\{\begin{array}{lcl} y_1 + \ldots + y_i & = & b_1 \\ y_1^3 + \ldots + y_i^3 & = & b_1^3 \\ \vdots & \vdots & \vdots \\ y_1^{2t-1} + \ldots + y_i^{2t-1} & = & b_1^{2t-1} \end{array}\right.$$

has the solution $(\zeta_1, \ldots, \zeta_i)$ with $\zeta_k = \xi_k^N$, and the assumption on the ξ_ks gives $\zeta_k \neq \zeta_l$ for $k \neq l$. That means that every solution of (S) gives rise to a solution of (S'). (In fact, the solutions of (S) are exactly those of (S') that are n-th roots of unity in $\mathbf{F}_{2^m}$).

Clearly, a possible solution $(\zeta_1, \ldots, \zeta_i)$ of (S') is the set of locators of a word in a coset of minimum weight 1 of the primitive t-error correcting BCH code. As this code has minimum distance at least $2t+1$, such cosets have weight w with $w = 1$ or $w \geq 2t$. So the only possible solutions of (S') are those in $i = w$ variables. It follows that the possible solutions of system (S) occur only for $i = 1$ and $i \geq 2t$. If $i = 1$, then (S) has no solution if $b_1 \notin \{z^N,\ z \in \mathbf{F}_{2^m} \setminus \{0\}\}$. This proves that the covering radius of the considered code is at least $2t$. □

Combining corollary 2 and theorem 3, we get

Theorem 4 *Let $N > 1$ and $\varepsilon_N(t)$ be as defined in theorem 2. Provided*

$$2^m \geq (1 + \varepsilon_N(t))\left((2t-1)N - 1\right)^2 (t!)^2,$$

the covering radius of the t-error correcting BCH-code of length $n = \frac{2^m-1}{N}$ is exactly $2t$.

4 Appendix

4.1 Optimality of the polynomial defined in (8)

We prove here the following lemma :

Lemma 1 *Let $f(x) = \sum_{i=0}^{2t} a_i P_i(x)$ be the expansion of a polynomial $f(x)$ of degree $2t$ in the basis of Krawtchouk polynomials. A polynomial satisfying $f(x) \geq 0$ on $[0, n]$ that achieves the maximum ratio $\frac{f(0)}{a_0}$, is the polynomial, say $g_{2t}(x)$, given by :*

$$g_{2t}(x) = (\sum_{i=0}^{t} P_i(x))^2.$$

Every polynomial $f(x)$ of degree $2t$, non-negative in $[0, n]$, can be represented as

$$f(x) = A(x)^2 + x(n-x)B(x)^2,$$

with $\deg A \leq t$, and $\deg B \leq t-2$. For this we refer to a theorem of Lukács, expression (1.21.1) in the book of Szegö [12].

As every polynomial can be expanded in the basis of Krawtchouk polynomials, we have that $f(x)$ can be represented as :

$$f(x) = \left(\sum_{i=0}^{t} u_i P_i(x)\right)^2 + x(n-x)\left(\sum_{i=0}^{t-1} v_i P_i(x)\right)^2.$$

The proof will be in two steps.

- The maximum $\frac{f(0)}{a_0}$ is achieved by a polynomial which is a square.

As $P_i(0) = \binom{n}{i}$, we have :

$$f(0) = \left(\sum_{i=0}^{t} u_i \binom{n}{i}\right)^2.$$

On the other hand, the MacWilliams transform [10, chap.5, §2] of f gives

$$a_0 = \frac{1}{2^n}\sum_{l=0}^{n} f(l)\binom{n}{l}$$

$$= \frac{1}{2^n}\sum_{l=0}^{n}\binom{n}{l}\left[\left(\sum_{i=0}^{t} u_i P_i(l)\right)^2 + l(n-l)\left(\sum_{i=0}^{t-2} v_i P_i(l)\right)^2\right].$$

The orthogonality relations for Krawtchouk polynomials [10, chap.5, th. 16] give :

$$a_0 = \sum_{i=0}^{t} u_i^2\binom{n}{i} + \frac{1}{2^n}\sum_{l=0}^{n} l(n-l)\binom{n}{l}\left(\sum_{i=0}^{t-2} v_i P_i(l)\right)^2.$$

As the second term is always non-negative, and by the fact that $f(0)$ does not depend on the v_i's, we get that $\frac{f(0)}{a_0}$ is maximal when all the v_i's are equal to 0.
Thus let $f(x) = \left(\sum_{i=0}^{t} u_i P_i(x)\right)^2$.

- The maximum $\frac{f(0)}{a_0}$ is achieved when all u_i's are equal to 1.

We have :

$$\varphi = \frac{f(0)}{a_0} = \frac{\left(\sum_{i=0}^{t} u_i\binom{n}{i}\right)^2}{\sum_{i=0}^{t} u_i^2\binom{n}{i}},$$

and by the Cauchy-Schwartz inequality :

$$\varphi \leq \frac{\sum_{i=0}^{t} u_i^2\binom{n}{i}\sum_{i=0}^{t}\binom{n}{i}}{\sum_{i=0}^{t} u_i^2\binom{n}{i}} = \sum_{i=0}^{t}\binom{n}{i}.$$

If all u_i's are equal to 1, then $\varphi = \sum_{i=0}^{t}\binom{n}{i}$. Thus φ achieves its maximum for example when all u_i's are equal to 1. □

4.2 Proof of inequality (10)

We have

$$\sum_{i=0}^{t}\binom{n}{i} > \binom{n}{t} + \binom{n}{t-1} = \binom{N}{t},$$

with $N = 2^m$. By Stirling's formula,

$$\sqrt{2\pi}k^{k+\frac{1}{2}}e^{-k+\frac{1}{12k+1}} < k! < \sqrt{2\pi}k^{k+\frac{1}{2}}e^{-k+\frac{1}{12k}},$$

$$\binom{N}{t} > \frac{N^t}{t!e^t}\frac{\exp(\frac{-12t-1}{12(12N+1)(N-t)})}{(1-\frac{t}{N})^{N-t+\frac{1}{2}}}.$$

Using the inequality (true for $0 < x < 1$),

$$\ln(1-x) < \frac{-x}{1-\frac{x}{2}},$$

we get

$$(1-\frac{t}{N})^{N-t+\frac{1}{2}} = e^{(N-t+\frac{1}{2})ln(1-\frac{t}{N})} < e^{-t}e^{\frac{t^2-t}{2N-t}}.$$

Thus,

$$\begin{pmatrix} N \\ t \end{pmatrix} > \frac{N^t}{t!}A,$$

where

$$A = \exp\left(\frac{-12t-1}{12(12N+1)(N-t)} - \frac{t^2-t}{2N-t}\right).$$

We would like to lowerbound A by a constant depending on t. Therefore, we first derive, with the help of inequality (9), a rough lower estimate on 2^m (which would be less than the final one).

Rewriting (9), we get

$$(t-1)2^{\frac{m}{2}+1}[\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} - 2^{mt}] + 2^m\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} - (t-1)2^{\frac{m}{2}+1+mt} > 0.$$

We shall find the value of m starting from which the following weaker inequality holds :

$$(t-1)2^{\frac{m}{2}+1}[\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} - 2^{mt}] + 2^m\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} > 0,$$

or

$$2(t-1)[1 - \frac{2^{mt}}{\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix}}] + 2^{\frac{m}{2}} > 0.$$

That yields

$$2^{\frac{m}{2}} > 2(t-1)[\frac{2^{mt}}{\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix}} - 1],$$

and as $\sum_{i=0}^{t}\begin{pmatrix} n \\ i \end{pmatrix} < \frac{2^{mt}}{(t-1)!}$, we have

$$2^{\frac{m}{2}} > 2(t-1)[(t-1)!-1] > (t-1)!(t-1).$$

Using $t! > \left(\frac{t}{e}\right)^t$, we finally get

$$2^m > e^2\left(\frac{t-1}{e}\right)^{2t}.$$

Assuming this, we get

$$A > e^{-B},$$

where $B = \frac{t^2-t}{2e^2\left(\frac{t-1}{e}\right)^{2t}-t} + \frac{12t+1}{12(12e^2\left(\frac{t-1}{e}\right)^{2t}+1)(e^2\left(\frac{t-1}{e}\right)^{2t}-t)}$.

We have

$$B < \frac{1}{(\frac{t-1}{e})^{2t-1}}.$$

Indeed,

$$B < \frac{t^2-t}{2e^2\left(\frac{t-1}{e}\right)^{2t}-t} + \frac{12t+1}{12\left(e^2\left(\frac{t-1}{e}\right)^{2t}-t\right)^2}$$

$$< \frac{(t^2-t)\left(e^2\left(\frac{t-1}{e}\right)^{2t}-t\right)+t+\frac{1}{12}}{\left(e^2\left(\frac{t-1}{e}\right)^{2t}-t\right)^2} < \frac{(t^2-t)e^2\left(\frac{t-1}{e}\right)^{2t}}{\left(e^2\left(\frac{t-1}{e}\right)^{2t}-t\right)^2}.$$

It is easy to check that

$$e^2\left(\frac{t-1}{e}\right)^{2t} < \sqrt{2}\left(e^2\left(\frac{t-1}{e}\right)^{2t}-t\right),$$

so that

$$B < \frac{2(t^2-t)}{e^2\left(\frac{t-1}{e}\right)^{2t}} = \frac{2t}{e\left(\frac{t-1}{e}\right)^{2t-1}}.$$

Since $\frac{t}{e} < \frac{t-1}{2}$ for $t \geq 4$, we get :

$$B < \frac{t-1}{\left(\frac{t-1}{e}\right)^{2t-1}} = \frac{e}{\left(\frac{t-1}{e}\right)^{2(t-1)}}.$$

Thus,

$$A > \exp\left(-\frac{e}{(\frac{t-1}{e})^{2(t-1)}}\right).$$

As $\exp(-x) > 1-x$ for $0 < x \leq 1$,

$$A > 1 - \frac{e}{(\frac{t-1}{e})^{2(t-1)}},$$

and inequality (10) is proved. □

Acknowledgement

The authors would like to thank Iiro Honkala, Ilia Krasikov, and the anonymous referees for helpful suggestions.

References

[1] E. F. Assmus, Jr., and H. F. Mattson, Jr., "Some 3-error correcting BCH codes have covering radius 5", *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 348–349, 1976.

[2] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, "Covering radius—survey and recent results", *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 328–343, 1985.

[3] G. D. Cohen, S. N. Litsyn, A. C. Lobstein and H. F. Mattson, Jr., "Covering radius 1985-1994", submitted.

[4] D. Gorenstein, W. W. Peterson, and N. Zierler, "Two-error correcting Bose-Chaudhury codes are quasi-perfect", *Information and Control*, vol. 3, pp. 291–294, 1960.

[5] T. Helleseth, "All binary 3-errors correcting BCH codes of length $2^m - 1$ have covering radius 5", *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 257–258, 1978.

[6] T. Helleseth, "On the covering radius of cyclic linear codes and arithmetic codes", *Discrete Applied Mathematics*, vol. 11, pp. 157–173, 1985.

[7] I. S. Honkala and A. Tietäväinen, "Codes and number theory", in *Handbook of Coding Theory*, Eds. R. A. Brualdi, W. C. Huffman, and V. S. Pless, to appear.

[8] J. A. van der Horst and T. Berger, "Complete decoding of triple-error-correcting binary BCH codes", *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 138–147, 1976.

[9] Y. Kapainen, Personal Communication.

[10] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

[11] O. Moreno and C. J. Moreno, "Constructive elementary approach to the covering radius of long BCH codes", 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory, Abstracts of papers, pp. 162–165, Leningrad, 1990.

[12] G. Szegö, *Orthogonal Polynomials*, Amer. Math. Soc. Colloq. Publ., v.23, Providence, RI, 1975.

[13] A. Tietäväinen, "On the covering radius of long binary BCH codes", *Discrete Applied Mathematics*, vol. 16, pp. 75–77, 1987.

[14] A. Tietäväinen, "An asymptotic bound on the covering radii of binary BCH codes", *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 211–213, 1990.

[15] S. G. Vlăduts and A. N. Skorobogatov, "Covering radius for long BCH codes", *Problemy Peredachi Informatsii*, vol. 25, pp. 38–45, 1989. Translated in: *Problems of Inform. Transm.*, vol. 25, No. 1, pp. 28–34, 1989.

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

Unité de recherche INRIA Lorraine - Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 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 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 (France)
Unité de recherche INRIA Sophia Antipolis - 2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

ISSN 0249 - 6399

RR. 2656