Idempotent and BCH bound

Daniel Augot * Nicolas Sendrier †

Abstract

Using the characterization of the idempotents of a narrow-sense primitive binary BCH code, we are able to give classes of such codes whose minimum distance reaches the BCH bound.

Let α be a primitive element of $GF(2^m)$. We denote $R_n = GF(2)[x]/(x^n - 1)$, $n = 2^m - 1$.

1 Binary BCH codes and locator polynomials

1.1 Primitive binary BCH codes

For our purpose we only need to define a particular class of BCH codes: the primitive narrow-sense BCH codes.

Definition 1 *The* primitive narrow-sense binary BCH code of length n and designed distance δ, *denoted $B(n, \delta)$ if it exists, is the set S of polynomials of R_n such that:*

1. *For all $c(x)$ in S and for all i, $1 \leq i < \delta$, $c(\alpha^i) = 0$.*
2. *There exists $g(x)$ in S such that $g(\alpha^\delta) \neq 0$.*

Remark 1

1. A code may verify the first condition of Definition 1 but not the second. This happens if there is a conjugate α^j of α^δ in $GF(2^m)$ such that $1 \leq j < \delta$. In this case the code is equal to $B(n, \delta')$ for some $\delta' > \delta$ and $B(n, \delta)$ does not exist.
2. A necessary and sufficient condition for $B(n, \delta)$ to exist is that δ is the smallest element of its cyclotomic class modulo n. In particular δ must be odd.
3. The definition of $B(n, \delta)$ depends on the choice of a primitive element in $GF(2^m)$, although it leads to an equivalent code. To get rid this problem, we consider that, once for all, we have chosen a primitive element for each extension of $GF(2)$. Thus speaking of THE code $B(2^s - 1, \delta)$ for all s and any suitable δ is sound.

*Université Paris 6, LITP, 2 pl. Jussieu, 75251 Paris CEDEX 05, FRANCE
†INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay CEDEX, FRANCE

1.2 Locator polynomials

For this section, all details can be found in [2, Ch. 8. §6 and Ch. 9. §2].

Definition 2 *Let $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^n$ be an element of R_n of Hamming weight w. The locators of $c(x)$ are the elements $X_1 = \alpha^{j_1}, \ldots, X_w = \alpha^{j_w}$ of $GF(2^m)$ where $c_{j_1}, \ldots, c_{j_w}$ are the non-zero coefficients of $c(x)$.*

The locator polynomial of $c(x)$ is the following polynomial of $GF(2^m)[z]$

$$\sigma(z) = \prod_{i=1}^{w} (1 - zX_i).$$

Proposition 1 *Let δ be an odd integer and let $\sigma(z) = \sigma_0 + \ldots + \sigma_w x^w$ be the locator polynomial of an element $c(x)$ of R_n of weigth $w \geq \delta$.*

1. *We have*
$$c(\alpha) = \ldots = c(\alpha^{\delta-1}) = 0 \Leftrightarrow \sigma_i = 0 \text{ for all odd } i,\ 1 \leq i < \delta. \tag{1}$$
2. *Furthermore, if $w = \delta$ or $w = \delta + 1$ and $c(x)$ verifies either side of equivalence (1) then $B(n, \delta)$ exists and has minimum distance δ.*

proof :

1. For all integer $j \geq 0$, let $A_j = c(\alpha^j)$. The first w Newton identities for $c(x)$ are:
$$\left\{ \begin{array}{lcl} I_1 & : & A_1 + \sigma_1 = 0 \\ I_2 & : & A_2 + A_1\sigma_1 + 2\sigma_2 = 0 \\ \vdots & & \qquad\qquad \vdots \\ I_r & : & A_r + \sum_{i=1}^{r-1} A_{r-i}\sigma_i + r\sigma_r = 0 \\ \vdots & & \qquad\qquad \vdots \\ I_w & : & A_w + \sum_{i=1}^{w-1} A_{w-i}\sigma_i + w\sigma_w = 0 \end{array} \right.$$
   (a) Suppose we have $A_1 = \ldots = A_{\delta-1} = 0$. Since $w \geq \delta$, for all odd $r < \delta$, we have $\sigma_r = 0$ from I_r.
   (b) Suppose $\sigma_r = 0$ for all odd $r < \delta$. We prove by induction on r that $A_r = 0$ for $r < w$.
      i. From I_1 we have $A_1 = 0$.
      ii. Let $r < \delta$ and suppose $A_1 = \ldots = A_{r-1} = 0$. The identity I_r gives $A_r = 0$ for both odd and even r.
2. We suppose that $c(x)$ verifies (1) and has weigth $w = \delta$ or $w = \delta + 1$.

   From Remark 1, $c(x)$ is in the code $B(n, \delta')$ for some $\delta' \geq \delta$. Let d be the minimum distance d of $B(n, \delta')$. From the BCH bound and the definition of the minimum distance, we have $w \geq d \geq \delta'$, so $\delta + 1 \geq d \geq \delta'$. Since δ and δ' are both odd, this inequality implies $\delta \geq \delta'$, thus $\delta = \delta'$.

$\square$

2 Characterization of an idempotent of $B(n, \delta)$

Definition 3 *An idempotent $p(x)$ of R_n is a polynomial such that $p(x)^2 = p(x)$.*

Proposition 2 [1, Lemma 2] *Let $\sigma(z)$ be the locator polynomial of $c(x)$ in R_n. Then $c(x)$ is an idempotent if and only if $\sigma(z)$ has all its coefficients in $GF(2)$.*

Definition 4 *The* splitting field *of a polynomial $p(x)$ of $GF(q)[x]$ is the smallest extension of $GF(q)$ containing all the roots of $p(x)$.*

Theorem 1 *Let δ be an odd integer and $\sigma(z) = \sigma_0 + \ldots + \sigma_w x^w$ be a polynomial of $GF(2)[z]$ of degree δ or $\delta + 1$ such that $\sigma_\delta = \sigma_0 = 1$ and $\sigma_i = 0$ for all odd i, $1 \leq i < \delta$.*

If $GF(2^m)$ is the splitting field of $\sigma(z)$ then the code $B(n = 2^m - 1, \delta)$ exists and its minimum distance is equal to δ.

proof :

1. Since $\sigma'(z) = \frac{d}{dz}\sigma(z) = z^{\delta-1}$ we have $\gcd(\sigma'(z), \sigma(z)) = 1$, so $\sigma(z)$ has no multiple roots.

2. $\sigma_0 = 1$, so zero is not a root of $\sigma(z)$. Since $\sigma(z)$ splits in $GF(2^m)$, it is the locator polynomial of some element $c(x)$ of R_n.

3. From Proposition 1, it follows that $B(n, \delta)$ exists and has minimum distance δ.

□

Corollary 1 *If a polynomial $\sigma(z)$ verifies the assumptions of Theorem 1, then $B(n, \delta)$ exists and contains an idempotent codeword of weight δ or $\delta + 1$. This codeword is precisely the element of R_n whose locator polynomial is $\sigma(z)$.*

Corollary 2 *If there exists no polynomial verifying the assumptions of Theorem 1, then if $B(n, \delta)$ exists, it contains no idempotent of weight δ or $\delta + 1$.*

Remark 2 A polynomial $\sigma(z)$ of $GF(2)[z]$ verifies the assumptions of Theorem 1 if and only if it is equal to $1 + (zp(z))^2 + z^\delta$ for some polynomial $p(z)$ in $GF(2)[z]$ of degree lower or equal to $(\delta + 1)/2$.

3 Binary codes with minimum weight idempotents

3.1 Finding the splitting field of a polynomial of $GF(2)[z]$

We present here an algorithm that computes the splitting field of a polynomial $\sigma(z)$ of $GF(2)[z]$.

Algorithm 1

INPUT: *a polynomial* $\sigma(z)$ *in* $GF(2)[z]$

1. $s_0(z) = \sigma(z)$, $p_0(z) = z$

2. *for all* $i \geq 0$, *while* $s_i(z) \neq 1$, $\begin{cases} p_{i+1}(z) &= p_i(z)^2 \mod s_i(z) \\ r_{i+1}(z) &= \gcd(s_i(z), p_{i+1}(z) - z) \\ s_{i+1}(z) &= \dfrac{s_i(z)}{r_{i+1}(z)} \end{cases}$

3. *let* $I = \{i, 1 \leq i \leq i_0 \mid r_i(z) \neq 1\}$, *where* i_0 *is the smallest index such that* $s_{i_0}(z) = 1$.

OUTPUT: $\operatorname{lcm} I$ *(lowest common multiple)*

Lemma 1 *For all* i, $1 \leq i \leq i_0$, *we have*

$$p_i(z) = z^{2^i} \mod s_{i-1}(z). \tag{2}$$

proof :

1. For $i = 1$, $p_1(z) = p_0(z)^2 \mod s_0(z) = z^2 \mod s_0(z)$.
2. For $i \geq 1$, we suppose we have $p_i(z) = z^{2^i} \mod s_{i-1}(z) = z^{2^i} + \lambda(z)s_{i-1}(z)$, then

$$\begin{aligned} p_{i+1}(z) &= p_i(z)^2 \mod s_i(z) \\ &= (z^{2^i} + \lambda(z)s_{i-1}(z))^2 \mod s_i(z) \\ &= (z^{2^i} + \lambda(z)r_i(z)s_i(z))^2 \mod s_i(z) \\ &= z^{2^{i+1}} \mod s_i(z) \end{aligned}$$

□

Lemma 2 *For all* i, $1 \leq i \leq i_0$, $s_i(z)$ *is the product all irreducible factors of* $\sigma(z)$ *of degree* $> i$.

proof : We prove the result by induction on i.

1. For $i = 1$, we have $r_1(z) = \gcd(z^2 - z, \sigma(z))$, and $s_1(z) = \sigma(z)/r_1(z)$, so the result holds for $s_1(z)$.
2. For $i > 1$, we have $s_i(z) = s_{i-1}(z)/r_i(z)$, where $r_i(z) = \gcd(s_{i-1}(z), z^{2^i} - z)$. All irreducible polynomials of degree i are factors of $z^{2^i} - z$, thus the irreducible factors of $s_i(z)$ are exactly the factors of $s_{i-1}(z)$ except those of degree i.

□

Lemma 3 *For all i, $1 \leq i \leq i_0$, $r_i(z)$ is the product of the irreducible factors of $\sigma(z)$ of degree i.*

proof : This result is a consequence of Lemma 2 and of the relation $r_i(z) = s_{i-1}(z)/s_i(z)$. $\square$

Proposition 3 *Algorithm 1 always ends, and the integer it returns for the input $\sigma(z)$ is the extension degree of the splitting field of $\sigma(z)$.*

proof : Let m_σ be the extension degree of $\sigma(z)$. We have

- From definition of m_σ, $\sigma(z) \mid z^{2^{m_\sigma}} - z$.
- By Lemma 2, $s_{m_\sigma - 1}(z) \mid \sigma(z)$ and thus $s_{m_\sigma-1}(z) \mid z^{2^{m_\sigma}} - z$.
- By Lemma 1, $r_{m_\sigma}(z) = \gcd(s_{m_\sigma-1}(z), z^{2^{m_\sigma}} - z) = s_{m_\sigma-1}(z)$ and thus $s_{m_\sigma}(z) = 1$.

So $i_0 < \infty$ and the algorithm ends.

From the construction of the $r_i(z)$, we have

$$\sigma(z) = \prod_{i=1}^{i_0} r_i(z),$$

so the smallest field containing all the roots of $\sigma(z)$ is the smallest field containing all the roots of the $r_i(z)$'s.

By Lemma 3 the smallest field containing the roots of $r_i(z) \neq 1$ is $GF(2^i)$. Thus if $I = \{i, 1 \leq i \leq i_0 \mid r_i(z) \neq 1\}$, the splitting field of $\sigma(z)$ is the smallest field containing $GF(2^i)$ for all i in I, that is $GF(2^m)$ where $m = \operatorname{lcm} I$. $\square$

3.2 A table of primitive BCH codes who reach the BCH bound

For any given δ, using Algorithm 1 we compute the extension degree of the splitting field of the polynomials $\sigma(z) = 1 + (zp(z))^2 + z^\delta$ for all $p(z) \in GF(2)[z]$ of degree $\leq (\delta - 1)/2$. Let M_δ be the set of all the integer obtained. From Theorem 1, for all m in M_δ the code $B(2^m - 1, \delta)$ exists and has minimum distance δ.

In Table 1 we give the values of all $m \in M_\delta$ for all odd δ between 3 and 49. We thus have a list a binary primitive narrow-sense BCH codes that reach the BCH bound.

Remark 3 If m' is in M_δ, then for any multiple m of m', $B(2^m - 1, \delta)$ exists and has minimum distance δ.

δ	m
3	2, 3
5	4, 5, 6
7	3, 4, 7, 10
9	6, 8, 9, 10, 14, 15, 21
11	5, 6, 8, 11, 21, 28
13	8, 9, 10, 12, 13, 14, 21, 22, 33, 35
15	4, 5, 6, 7, 9, 26, 33, 39
17	8, 9, 10, 12, 14, 15, 17, 21, 35, 39, 44, 52, 55, 65, 66, 77
19	8, 9, 10, 12, 15, 19, 21, 28, 34, 35, 39, 51, 52, 65, 66, 77, 91
21	6, 7, 8, 9, 10, 11, 15, 38, 51, 57, 68, 85
23	6, 8, 10, 11, 14, 15, 21, 23, 35, 51, 52, 57, 65, 68, 76, 85, 95, 117, 119
25	8, 10, 12, 13, 15, 18, 21, 22, 25, 28, 33, 46, 57, 68, 69, 76, 77, 95, 102, 119, 133, 153
27	6, 7, 8, 9, 10, 13, 15, 33, 44, 55, 68, 69, 76, 85, 92, 115, 187
29	10, 12, 14, 15, 16, 18, 21, 25, 26, 27, 29, 35, 39, 44, 66, 68, 69, 76, 77, 92, 95, 99, 102, 114, 115, 153, 161, 171, 187, 209, 221, 715
31	5, 6, 8, 9, 14, 21, 31, 39, 44, 52, 58, 77, 87, 92, 119, 161, 209, 221, 247, 374, 561
33	10, 11, 12, 15, 16, 17, 18, 21, 27, 28, 39, 52, 62, 76, 87, 91, 92, 93, 95, 114, 115, 116, 133, 138, 145, 171, 175, 207, 247, 322
35	9, 10, 12, 14, 15, 16, 17, 21, 22, 25, 33, 35, 52, 65, 77, 78, 87, 91, 92, 93, 95, 114, 116, 124, 138, 143, 145, 152, 155, 203, 253, 299, 494, 741
37	8, 10, 12, 14, 15, 18, 19, 21, 27, 33, 34, 37, 44, 51, 52, 55, 65, 77, 78, 92, 93, 115, 116, 117, 119, 124, 138, 143, 155, 161, 174, 175, 203, 207, 217, 261, 299, 506
39	8, 9, 10, 12, 13, 15, 19, 21, 25, 28, 33, 35, 44, 51, 55, 68, 74, 77, 85, 111, 115, 116, 119, 124, 138, 145, 174, 186, 187, 217, 319, 322, 391, 406
41	10, 12, 14, 15, 16, 18, 21, 25, 26, 27, 35, 38, 39, 41, 44, 51, 57, 65, 66, 68, 77, 91, 99, 111, 116, 119, 124, 133, 138, 148, 155, 174, 184, 185, 186, 207, 209, 261, 279, 319, 341, 374, 377, 391, 437, 759, 1615, 2431
43	7, 8, 11, 12, 15, 18, 20, 27, 39, 43, 50, 52, 57, 65, 68, 76, 82, 85, 95, 102, 111, 115, 116, 123, 124, 138, 145, 148, 153, 174, 185, 186, 207, 221, 261, 279, 310, 377, 403, 437, 782, 1173
45	8, 9, 10, 11, 12, 14, 15, 21, 23, 25, 35, 39, 52, 57, 65, 68, 76, 85, 86, 91, 102, 119, 123, 124, 129, 133, 145, 148, 155, 164, 174, 186, 205, 217, 222, 247, 259, 403, 442, 493, 754
47	8, 9, 10, 12, 15, 21, 22, 23, 28, 33, 35, 47, 52, 55, 68, 76, 77, 78, 91, 95, 102, 114, 119, 123, 129, 133, 143, 148, 155, 164, 172, 174, 185, 186, 205, 215, 221, 222, 287, 325, 407, 425, 434, 493, 494, 518, 527, 551, 741, 806, 1131, 1209, 1885, 3553
49	10, 12, 14, 15, 16, 18, 21, 25, 27, 33, 35, 44, 46, 49, 52, 55, 65, 68, 69, 76, 78, 85, 94, 95, 102, 114, 117, 119, 129, 141, 143, 145, 148, 153, 164, 171, 172, 174, 186, 187, 203, 209, 215, 222, 232, 246, 248, 261, 279, 287, 299, 301, 333, 369, 407, 442, 481, 527, 551, 589, 663, 741, 986, 1131, 1209, 1479, 1771, 2387, 3059, 4199

Table 1: Some $B(2^m - 1, \delta)$ codes with true minimum distance δ.

Thus the values of $m \in M_\delta$ for which we already had an integer $m' < m$, $m' \mid m$ and $m' \in M_\delta$ were discarded from Table 1,

References

[1] D. Augot, P. Charpin, and N. Sendrier. Studying the locator polynomials of minimum weight codewords of BCH codes. *IEEE Transactions on Information Theory*, 38(3):960–973, May 1992.

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