A characterization of cyclic codes whose minimum distance equals their maximum BCH bound*

José Joaquín Bernal and Juan Jacobo Simón
University of Murcia (Spain)

Diana H. Bueno-Carreño
Pontificia Universidad Javeriana-Cali (Colombia)

(josejoaquin.bernal,jsimon,dianahaidive.bueno)@um.es

Abstract

In this extended abstract we characterize those cyclic codes for which its minimum distance reaches the maximum of its BCH bounds. We also study a constructive point of view by means of computations of divisors of a polynomial of the form $x^n - 1$. We apply our results to the study of those BCH codes C, with designed distance δ that have true minimum distance $d(C) = \delta$. Finally, we present some examples of new binary BCH codes with true minimum distance. To do this, we make use of two related tools: the discrete Fourier transform and the notion of apparent distance of a code, originally defined for multivariate abelian codes.

Keywords
Cyclic codes, BCH bound, apparent distance, true minimum distance

1 Introduction

To compute the minimum distance of cyclic codes, or a lower bound for them, is one of the most studied problems in abelian codes (see, for example, [3, 5, 6]). The oldest lower bound for the minimum distance of a cyclic code is the BCH bound [4, p. 151]. The study of this bound and its generalizations is a classical topic, which includes the study of the very well-known family of BCH codes. Whitin them, an interesting problem is to determine, for a given code, when the maximum of its BCH bounds equals its minimum distance (see [2, 5]). This is our interest.

In this extended abstract we state conditions on a cyclic code for its minimum distance equals the maximum of its BCH bounds. To do this, we make use of two related tools; to witt, the discrete Fourier transform and the notion of apparent distance of a code, originally defined for multivariate abelian codes in [1]. These tools and all notation are given in Section 2. In Section 3, we characterize those cyclic codes for which its minimum distance reaches the maximum of its BCH bounds. Then we study a constructive point of view by means of computations of divisors of a polynomial of the form $x^n - 1$. In Section 4, we apply our results to the study of those BCH codes C, with designed distance δ, that have true minimum distance $d(C) = \delta$ (see [5, Section 9.2]). Finally, some examples of new binary BCH codes with true minimum distance are presented.

2 Notation and preliminaries

We will use standard terminology from coding theory (see, for example [5, Chapter 7] or [2, Section 2]). We denote by q a power of a prime number p and by $\mathbb{F} = \mathbb{F}_q$ the field of q-elements. Let n be a positive integer which is coprime to q and let $\mathbb{L}/\mathbb{F}$ an extension field containing a n-th primitive root of unity, say α, that we fix throughout this note.

*This work was partially supported by MINECO (Ministerio de Economía y Competitividad), (Fondo Europeo de Desarrollo Regional) project MTM2012-35240 and Fundación Séneca of Murcia. The second author has been supported by Departamento Administrativo de Ciencia, Tecnología e Innovación de la República de Colombia

We denote by $\mathbb{F}[x]$ the ring of polynomials with coefficients in $\mathbb{F}$. For any polynomial $g = g(x) \in \mathbb{F}[x]$ we denote by $\deg(g)$ its degree and by $supp(g)$ its support. Instead of working with group rings, we consider the polynomial $x^n - 1 \in \mathbb{F}[x]$ and form the quotient ring $\mathbb{F}[x]/(x^n - 1)$, which we denote by $\mathbb{F}(n)$. As usual, we identify the elements $g \in \mathbb{F}(n)$ with polynomials; so that we may take $g \in \mathbb{F}(n)$ and then write $g \in \mathbb{F}[x]$ (where $\deg(g) < n$). In case we first consider a polynomial $f \in \mathbb{F}[x]$, possibly with $\deg(f) \geq n$, then we denote by $\overline{f}$ its image under the canonical projection onto $\mathbb{F}(n)$.

A cyclic code C of length n in the alphabet $\mathbb{F}$ will be identified with its corresponding ideal in $\mathbb{F}(n)$ (up to permutation equivalence). It is well known that, when $\gcd(n, q) = 1$, the quotient ring $\mathbb{F}(n)$ is semisimple and then every cyclic code has a unique monic generator polynomial [5, Theorem 7.1] and a unique generator idempotent [5, Theorem 8.1]. We always assume that $\gcd(n, q) = 1$.

It is well known that every cyclic code C of $\mathbb{F}(n)$ is totally determined by its root set (or the zeros of the code), which is defined as $Z(C) = \left\{\alpha^i \mid c(\alpha^i) = 0 \text{ for all } c \in C\right\}$; that is, for any polynomial $f \in \mathbb{F}(n)$, we have that $f \in C$ if and only if $f(\beta) = 0$ for all $\beta \in Z(C)$. We denote the defining set of C as $D(C) = \left\{i \in \mathbb{Z}_n \mid \alpha^i \in Z(C)\right\}$ [5, p. 199]. It is well-known that defining sets are partitioned in q-cyclotomic cosets modulo n [5, p.104]; that is, denoting by $\mathbb{Z}_n$, the integers modulo n, and given any element $a \in \mathbb{Z}_n$, the q-cyclotomic coset of a, modulo n is the set $C_q(a) = \{a, qa, \ldots, q^{n_a - 1}a\}$, where n_a is the smallest positive integer such that $q^{n_a}a \equiv a \mod n$. We recall that the notions of set of zeros and defining set are also applied to polynomials in $\mathbb{F}(n)$.

For any code C, we denote its minimum distance by $d(C)$. The BCH bound states that for any cyclic code that has a string of $\delta - 1$ consecutive powers of α as zeros, the minimum distance of the code is at least δ [5, Theorem 7.8]. Clearly, for any cyclic code C there exists the maximum of its BCH bounds, that we denote by $\Delta(C)$. Some times it is called *the* BCH (lower) bound of the code (see [1, p. 22] and [2, p. 984]).

A cyclic code C of $\mathbb{F}(n)$, with polynomial generator $g(x)$, is a BCH code of designed distance δ if $g(x)$ is the polynomial with the lowest degree over $\mathbb{F}$ having $\left\{\alpha^{b+j} \mid j = 0, \ldots, \delta - 2\right\} \subseteq Z(C)$ (see [5, p. 202]) or, equivalently if for any cyclotomic coset $Q \subseteq D(C)$ we have that $Q \cap \{b + j \mid j = 0, \ldots, \delta - 2\} \neq \emptyset$. The Bose distance is defined for a BCH code C of designed distance δ, as the largest δ' such that C is a BCH code of designed distance δ'. Note that for a BCH code C it may happens that its Bose distance being less that $\Delta(C)$, as the following example shows.

Example 1. Set $q = 2$, $n = 31$ and α a 31-th primitive root of unity. Let C be the BCH code generated by $\operatorname{lcm}\{M^{(15)}, M^{(16)}, M^{(17)}\}$, where $M^{(t)}$, denotes the minimal polynomial of α^t in $\mathbb{F}[x]$. Consider the 2-cyclotomic cosets $C_1 = \{1, 2, 4, 8, 16\}$, $C_3 = \{3, 6, 12, 17, 24\}$ and $C_{15} = \{15, 23, 27, 29, 30\}$. Then one may check that the defining set of the code C is $D(C) = C_1 \cup C_3 \cup C_{15}$, and that the Bose distance is $\delta = 4$. However $\Delta(C) = 5$, because $\{1, 2, 3, 4\} \subset D(C)$. But $\{1, 2, 3, 4\} \subset C_1 \cup C_3$, so that C cannot be a BCH code of designed distance $\delta = 5$. Hence the Bose distance is less than the maximum of all possible BCH bounds (or simply, the BCH bound, $\Delta(C)$).

Let $\mathbb{L}/\mathbb{F}$ an extension field that contains a n-th primitive root of unity, α. The (discrete) Fourier transform of a polynomial $f \in \mathbb{F}(n)$ (also called Mattson-Solomon polynomial), that we denote by φ_f is defined as $\varphi_f(x) = \sum_{j=0}^{n-1} f(\alpha^j)X^j$. Clearly, $\varphi_f \in \mathbb{L}(n)$; moreover, the Fourier transform may be viewed as an isomorphism of algebras $\varphi : \mathbb{L}(n) \longrightarrow (\mathbb{L}^n, \star)$, where the multiplication "$\star$" in $\mathbb{L}^n$ is defined coordinatewise (see [1, Section 2.2] or [5, § 8.6]). The inverse of the Fourier transform is given by $\varphi_g^{-1} = \frac{1}{n}\sum_{i=0}^{n-1} g(\alpha^{-i})X^i$ (see for details any of [1, 2, 5]).

Let us recall some definitions in [1, Chapter 3] related to the computation of the BCH bound. The context of these definitions is the study of multivariate polynomials, so, for the sake of simplicity, we present a very simplyfied version only concerning univariate polynomials.

Definition 2. *Let $\mathbb{L}/\mathbb{F}$ an extension field that contains a n-th primitive root of unity, α. For any element $g \in \mathbb{L}(n)$ we define the apparent distance of g, that we denote $d^*(g)$, as follows.*

1. *If $g = 0$ then $d^*(0) = 0$.*
2. *If $g \neq 0$ then*

$$d^*(g) = \max\left\{n - \deg\left(\overline{x^h g}\right) \mid 0 \leq h \leq n - 1\right\}.$$

Now, the apparent distance of a cyclic code C in $\mathbb{F}(n)$ with generator idempotent $e \in C$ is $d^*(C) = d^*(\varphi_e)$ and moreover

$$\Delta(C) = d^*(C) = d^*(\varphi_e) \leq d(C) \tag{1}$$

(see [1, p. 22]). As an immediate consequence we have.

Corollary 3. *Notation as above. Let C be a cyclic code in $\mathbb{F}(n)$ with generator idempotent $e \in C$. If $d^*(\varphi_e) = \omega(e)$ then $d(C) = \Delta(C)$.*

3 The minimum distance and the BCH bound

We keep all notation of the preceding section. For an arbitrary element $g \in \mathbb{L}(n)$, which we may view as a polynomial with $\deg(g) \leq n-1$ and for any $h \in \{0, \ldots, n-1\}$ we write

$$m_g = \gcd(x^h g, x^n - 1) \tag{2}$$

where m_g does not depend on h, because x^h and $x^n - 1$ are relatively prime polynomials. We also write, for any $h \in \{0, \ldots, n-1\}$

$$x^h g = (x^n - 1) f_{g,h} + \overline{x^h g} \tag{3}$$

where $f_{g,h}$ is a suitable quotient from the division algorithm. Note that if $g \neq 0$ then $\overline{x^h g} \neq 0$ because $\deg(g) < n$. By using results in [1] and [3] (see also [5, Theorem 8.6.31]) we may get the following result.

Lemma 4. *Let n, q, $\mathbb{F}$ and $\mathbb{L}$ be as above. Consider $g \in \mathbb{L}(n)$ and let m_g be as above. Then*

1. *$d^*(g) \leq n - \deg(m_g)$.*
2. *If $g \mid x^n - 1$ then $d^*(g) = n - \deg(g)$.*

As a direct consequence we have the following result (see [1, Theorem 4.1] and [3, Theorem 2]).

Corollary 5. *Let C be a cyclic code in $\mathbb{F}(n)$ and $c \in C$. Then*

1. *$d^*(\varphi_c) \leq \omega(c)$.*
2. *$n - \deg(m_{\varphi_c}) = \omega(c)$.*

Then, by lemma above, the apparent distance of any $f \in \mathbb{L}(n)$ is less than or equal to the number of nonzeros of m_f. The following result shows us when the equality is reached.

Proposition 6. *Let n, q, $\mathbb{F}$ and $\mathbb{L}$ be as above. Consider $f \in \mathbb{L}(n)$ and let m_f be as in (2). Then $d^*(f) = n - \deg(m_f)$ if and only if there exists $h \in \{0, \ldots, n-1\}$ such that $\overline{x^h f} \mid x^n - 1$ (equivalently, $\overline{x^h f}$ and m_f are associated polynomials in $\mathbb{L}[x]$).*

Now, our main result.

Theorem 7. *Let n be a positive integer, p a prime number and q a power of p. Assume that $\gcd(n, q) = 1$. Consider the field $\mathbb{F}$ and an extension field $\mathbb{L}/\mathbb{F}$ containing a n-th primitive root of unity α. Let C be a cyclic code in $\mathbb{F}(n)$. Then $d(C) = \Delta(C)$ if and only if there exists a polynomial $f \in \mathbb{L}(n)$, such that*

1. *$d^*(f) = d^*(C)$.*
2. *$d^*(f) = n - \deg(m_f)$*
3. *$\varphi_f^{-1} \in C$.*

Moreover, in this case, there exists $h \in \{0, \ldots, n-1\}$ such that $\overline{x^h f} \mid x^n - 1$.

Under a constructive point of view, the theorem above together with Proposition 6 shows us that we only have to focus on the divisors of $x^n - 1$. Let us state this fact in the following results that we will use in the next section.

Corollary 8. *Hypotheses as in Theorem 7. Let C be a cyclic code in $\mathbb{F}(n)$. Then $d(C) = \Delta(C)$ if and only if there exists $k \in \{0, \ldots, n-1\}$ and a divisor $g \mid x^n - 1$, in $\mathbb{L}[x]$, such that setting $f = \overline{x^k g}$, the following conditions hold.*

1. $d^*(f) = d^*(C)$ *(recall that* $d^*(f) = d^*(g)$*).*

2. $\varphi_f^{-1} \in C$.

Example 9. Set $q = 2$, $n = 45$ and $g = x^{40} + x^{39} + x^{38} + x^{36} + x^{35} + x^{32} + x^{30} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{17} + x^{15} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$. Let α be a 45-th primitve root of unity. To find the parameter k in the corollary above, we have to compute $g(1)$ and $g(\alpha^3)$, because the defining set of the polynomial $(x^{45} - 1)/g$ is $C_2(0) \cup C_2(3)$. Since $g(1) = 1$ and $g(\alpha^3) = \alpha^{30}$ then $k = 15$ works. That is, setting $f = x^{15}g$ we have that $\varphi_f^{-1} \in \mathbb{F}(45)$. Set $C = (\varphi_f^{-1})$ and we have that $5 = d(C) = \Delta(C)$ and $\dim(C) = 21$. In fact, C is a BCH code with $\delta = 5$.

It is well-known that, under our notation, $a \in \mathbb{L}$ verifies that $a \in \mathbb{F}$ if and only if $a^q = a$.

Corollary 10. *Hypotheses as in Theorem 7. Let C be a cyclic code in $\mathbb{F}(n)$. Then $d(C) = \Delta(C)$ if and only if there exists $k \in \{0, \ldots, n-1\}$ and a divisor $g \mid x^n - 1$, in $\mathbb{L}[x]$, such that the following conditions hold.*

1. $d^*(g) = d^*(C)$*, and setting* $f = \overline{x^k g}$*,*

2. $supp(f) \subseteq \mathbb{Z}_n \setminus D(C)$*,*

3. $(f(\alpha^j))^q = f(\alpha^j)$*, for any* $j \in \{0, \ldots, n-1\}$*,*

Now we give a sufficient condition to get BCH codes yielding its true minimum distance.

Corollary 11. *Let C be a cyclic code in $\mathbb{F}(n)$ with generator idempotent $e \in C$. If there exists $h \in \{0, \ldots, n-1\}$ such that $\overline{x^h \varphi_e} \mid x^n - 1$ then $d(C) = \Delta(C)$.*

4 Applications: true minimum distance in BCH codes

We keep all notation. The following result allows us to construct BCH codes $B(\delta)$, for which $d(B(\delta)) = \Delta(B(\delta)) = \delta$. We recall that, for a given polynomial $g \in \mathbb{F}(n)$, it is denoted by (g) the ideal in $\mathbb{F}(n)$ generated by g.

Proposition 12. *Let $g \in \mathbb{L}[x]$ be a divisor of $x^n - 1$. If $\varphi_{\overline{x^k g}}^{-1}$ belongs to $\mathbb{F}[x]$, for some $k \in \{0, \ldots, n-1\}$, then the cyclic code $C = \left(\varphi_{\overline{x^k g}}^{-1}\right)$ verifies that $\Delta(C) = d(C)$.*

Theorem 13. *Let $g \in \mathbb{L}[x]$ be a divisor of $x^n - 1$. If there exists $k \in \{0, \ldots, n-1\}$, such that $\overline{x^k g}(\alpha^j) \in \mathbb{F}$, for all $j = 0, \ldots, n-1$ then there exists a BCH code of designed distance δ, $C = B(\delta)$ (containing $\varphi_{\overline{x^k g}}^{-1}$) such that $\delta = \Delta(C) = d(C) = n - \deg(g)$.*

For any couple of positive integers a, b, we denote by $O_a(b)$ the multiplicative order of b, modulo a. We also denote by $\phi(a)$ the Euler's totient function.

Theorem 14. *Let n be a positive integer, p a prime number and q a power of p. Assume that $\gcd(n, q) = 1$. Consider the field $\mathbb{F}$ and an extension field $\mathbb{L}/\mathbb{F}$ containing a n-th primitive root of unity α. Let h be an irreducible factor of $x^n - 1$ with defining set $D(h)$. We set $g = (x^n - 1)/h$ and pick any $j \in D(h)$. If $g(\alpha^j) = \alpha^k$ then there exists a BCH code of designed distance δ, $C = B(\delta)$ such that $\delta = \Delta(C) = d(C) = \deg(h)$.*

Corollary 15. *Let $n = q^m - 1$, for some $m \in \mathbb{N}$. For each divisor l of n, there exist $\frac{\phi(l)}{O_l(q)}$ BCH codes of designed distance $\delta = O_l(q)$ over $\mathbb{F}$ having true minimum distance δ.*

Example 16. Set $q = 2$ and $n = 15$. Denote the irreducible factors by $h_1 = \Phi_1$, $h_2 = \Phi_3$, $h_3 = x^4 + x + 1$, $h_4 = x^4 + x^3 + 1$ and $h_5 = \Phi_5$.

Setting $g_i = \frac{x^n - 1}{h_i}$ we apply Theorem 14 above to get the following table of BCH codes of length 15 having true minimum distance δ.

Factor	Dimension	$\delta = d$
g_1	15	1
g_2	10	2
g_3	8	4
g_4	8	4
g_5	6	4

Note that the codes associated to $g_2, \ldots, g_5$ are not considered in the classical result [5, Theorem 9.2.5]. There are more nonconsidered codes. The polynomial $g = \Phi_{15}\Phi_5$ verifies the conditions of Theorem 13 with $k = 0$, and hence it determines a BCH code, C_6 having true minimum distance δ, with parameters $\dim(C) = 5$ and $d(C) = 3$. Also $\Phi_5\Phi_3 h_3$ verifies the conditions of Theorem 13 with $k = 0$, and hence it determines a BCH code C_7 having true minimum distance δ, with parameters $\dim(C) = 7$ and $d(C) = 5$.

Example 17. Set $q = 2$ and $n = 21$. Denote the irreducible factors by $h_1 = \Phi_1$, $h_2 = \Phi_3$, $h_3 = x^3 + x + 1$, $h_4 = x^3 + x^2 + 1$, $h_5 = x^6 + x^4 + x^2 + x + 1$ and $h_6 = x^6 + x^5 + x^4 + x^2 + 1$

Setting $g_i = \frac{x^n - 1}{h_i}$ we apply Theorem 14 above to get the following table of binary BCH codes of length 21 having true minimum distance δ. We complete with another one satisfying the conditions of Theorem 13.

Factor	Dimension	$\delta = d$
g_1	21	1
g_2	14	2
g_3	12	3
g_4	12	3
g_5	8	6
g_6	8	6
$\Phi_{21} h_3 h_1$	10	6

We finish with an example of a binary BCH code with true minimum distance δ of length 33. We have not found in the literature any binary BCH code having this length.

Example 18. Set $q = 2$, $n = 33$ and $g = x^{30} + x^{27} + x^{24} + x^{21} + x^{18} + x^{15} + x^{12} + x^9 + x^6 + x^3 + 1$. One may check that g verifies the conditions of Theorem 13 with $k = 0$, and hence it determines a BCH code C having true minimum distance δ, with parameters $\dim(C) = 11$ and $d(C) = 3$.

References

[1] P. Camion, Abelian Codes, MRC Tech. Sum. Rep. 1059, Univ. of Wisconsin, Madison, 1970.

[2] Charpin, P., Open Problems on Cyclic Codes. in V. S. Pless, W. C. Huffman and R. A. Brualdi (editors) *Handbook of Coding Theory* vol. I. North-Holland, Amsterdam, 1998.

[3] R. T. Chien and D. M. Chow, Algebraic Generalization of BCH-Goppa-Helgert Codes, IEEE Trans. Inform. Theory, vol. 21, no. 1, 1975.

[4] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge, 2003.

[5] F.J. Macwilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 1977.

[6] J. H. Van Lint and R. M. Wilson, On the Minimum Distance of Cyclic Codes,IEEE Trans. Inform. Theory, vol. 32, no. 1, 1986.