Cyclic and BCH Codes whose Minimum Distance Equals their Maximum BCH bound

José Joaquín Bernal*, Diana H. Bueno-Carreño† and Juan Jacobo Simón*.
*Departamento de Matemáticas
Universidad de Murcia, 30100 Murcia, Spain.
Email: {josejoaquin.bernal, jsimon}@um.es
†Departamento de Ciencias Naturales y Matemáticas
Pontificia Universidad Javeriana, Cali, Colombia
Email: dhbueno@javerianacali.edu.co

Abstract

In this paper we study the family of cyclic codes such that its minimum distance reaches the maximum of its BCH bounds. We also show a way to construct cyclic codes with that property by means of computations of some 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 minimum distance $d(C)=\delta$. Finally, we present some examples of new binary BCH codes satisfying that condition. 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.

I. Introduction

The computation of the minimum distance of a cyclic code, or a lower bound for it, is one of the main problems on abelian codes (see, for example, [3], [6], [7]). The oldest lower bound for the minimum distance of a cyclic code is the BCH bound [5, 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. In particular, an interesting problem is to determine when the maximum of the BCH bounds of a given cyclic code equals its minimum distance (see [2], [6]). This is our interest.

In this paper we deal with three problems related to the study of the BCH bound. The first one is how to give necessary and sufficient conditions for a cyclic code to insure that the maximum of its BCH bounds equals its minimum distance. The second problem is how to construct such cyclic codes. Our third problem is related to construction techniques of BCH codes for which its designed distance, its maximum BCH bound and its minimum distance coincide.

To solve our first problem, 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 in [1]. These tools and the notation needed 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 (problem 1). Then we study how to construct cyclic codes with that property by means of computations of divisors of a polynomial of the form x^n-1 (problem 2). Section 4 is devoted to solve our third problem. We apply our results to the study of those BCH codes C, with designed distance δ, that have minimum distance $d(C)=\delta$ (see [6, Section 9.2]). In this paper, some examples of construction techniques and examples of new binary BCH codes whose minimum distance equals its designed distance are presented. We point out that all computations were done by using the GAP4r7 program [4] with the cooperation of Alexander Konovalov. The authors are indebted to him.

II. Notation and preliminaries

We will use standard terminology from coding theory (see for example [6, Chapter 7] or [2, Section 2]). We denote by q a power of the prime number p and by $\mathbb{F}_q$ the field of q elements. Let n be a positive integer which is coprime to q. We denote by R_n the set of n-th roots of unity and by U_n the set of *primitive* n-th roots of unity.

We denote by $\mathbb{F}_q[x]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. For any $g=g(x)\in\mathbb{F}_q[x]$ we denote by $\deg(g)$ its degree, by $supp(g)$ its support and by $\omega(g)=|supp(g)|$ its weight. For any positive integer n, we consider the quotient ring $\mathbb{F}_q[x]/(x^n-1)$ which will be denoted by $\mathbb{F}_q(n)$. As usual, we identify the elements $g\in\mathbb{F}_q(n)$ with polynomials; so we may take $g\in\mathbb{F}_q(n)$ and then write $g\in\mathbb{F}_q[x]$ (where $\deg(g)<n$). For any $f\in\mathbb{F}_q[x]$ we denote by $\overline{f}$ its image under the canonical projection onto $\mathbb{F}_q(n)$.

As in [7], a cyclic code C of length n in the alphabet $\mathbb{F}_q$ will be identified with the corresponding ideal in $\mathbb{F}_q(n)$ (up to permutation equivalence). Then, by a cyclic code we mean an ideal of $\mathbb{F}_q(n)$. It is well known that if $\gcd(n,q)=1$ then the

This work was partially supported by MINECO (Ministerio de Economía y Competitividad), (Fondo Europeo de Desarrollo Regional) project MTM2012-35240, Programa Hispano Brasileño de Cooperación Universitaria PHB2012-0135, and Fundación Séneca of Murcia. The second author has been supported by Departamento Administrativo de Ciencia, Tecnología e Innovación de la República de Colombia

quotient ring $\mathbb{F}_q(n)$ is semisimple and then every cyclic code has a unique monic generator polynomial [6, Theorem 7.1] and a unique idempotent generator [6, Theorem 8.1]. We always assume that $\gcd(n,q)=1$.

We denote by $\mathbb{Z}_n$ the integers modulo n and we identify any class in $\mathbb{Z}_n$ with its canonical representative. It is well-known that every cyclic code C in $\mathbb{F}_q(n)$ is totally determined by its set of zeros (or its root set), which is defined as $Z(C)=\{\alpha\in R_n \mid c(\alpha)=0, \text{ for all } c\in C\}$; thus, for any polynomial $f\in\mathbb{F}_q(n)$, we have that $f\in C$ if and only if $f(\alpha)=0$ for all $\alpha\in Z(C)$. Fixed $\alpha\in U_n$, we denote the defining set of C with respect to α as $D_\alpha(C)=\left\{i\in\mathbb{Z}_n \mid \alpha^i\in Z(C)\right\}$ (see [6, p. 199]). It is well-known that, when $\gcd(n,q)=1$, defining sets are partitioned in q-cyclotomic cosets modulo n [6, p. 104], which are defined as follows: given any element $a\in\mathbb{Z}_n$, the q-cyclotomic coset of a modulo n is the set $C_q(a)=\{a,qa,\dots,q^{n_a-1}a\}(\mod n)$, 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 $\mathbb{F}_q(n)$ in the obvious way.

For any code C, we denote its minimum distance by $d(C)$. The BCH bound states that for any cyclic code in $\mathbb{F}_q(n)$ that has a string of $\delta-1$ consecutive powers of some $\alpha\in U_n$ as zeros, the minimum distance of the code is at least δ [6, Theorem 7.8]. In terms of defining sets, if there is a string of $\delta-1$ consecutive integers modulo n in $D_\alpha(C)$, for some $\alpha\in U_n$, then $d(C)\geq\delta$. Note that different roots of unity may yield different defining sets and consequently different lower bounds. For any cyclic code C the maximum of its BCH bounds will be denoted by $\Delta(C)$. Sometimes it is called *the* BCH (lower) bound of the code (see [1, p. 22] and [2, p. 984]).

The following Remark shows that in order to compute the maximum $\Delta(C)$ we do not need to consider all the elements in U_n. This fact will be used later.

Remark 1. *Let $C_q(a_1),\dots,C_q(a_h)$ be the q-cyclotomic cosets modulo n and fix a complete set of representatives $\{a_1,\dots,a_h\}$. Suppose we have chosen $\alpha\in U_n$ to get a defining set $D_\alpha(C)$. We want to identify the elements $\beta\in U_n$ satisfying that $D_\beta(C)\neq D_\alpha(C)$. Then, β must satisfy the equality $\beta^{a_iq^j}=\alpha$ for some representative a_i with $\gcd(n,a_i)=1$ and $j\in\mathbb{Z}$. In this case $D_\beta(C)=a_i\cdot D_\alpha(C)$, where the multiplication has the obvious meaning. We define*

$$A(n)=\{a_i \mid \gcd(a_i,n)=1\}. \tag{1}$$

It is easy to see that $O_n(q)=|C_q(a_i)|$ for any $a_i\in A(n)$. In addition, since $D_{\beta^{a_i}}(C)=D_{\beta^{a_iq^j}}(C)=D_{\beta^{a_iq^{j'}}}(C)$ $(j,j'\in\mathbb{Z})$, we conclude that we have to consider at most $\frac{\phi(n)}{O_n(q)}$ distinct defining sets or elements in U_n to get $\Delta(C)$.

For example, set $n=41$ and $q=2$. The 2-cyclotomic cosets are $C_2(0)$, $C_2(1)$ and $C_2(3)$. So $A(41)=\{1,3\}$. Fixed $\alpha\in U_{41}$, let C be the cyclic code with defining set $D_\alpha(C)=C_2(1)$. Some BCH bounds for C with respect to α are $\delta_1=3$ by considering $\{1,2\}\subset D_\alpha(C)$, and $\delta_2=4$ by considering $\{8,9,10\}\subset D_\alpha(C)$. Now we also have to consider $D_\beta(C)=3\cdot D_\alpha(C)=C_2(3)$ and compute the corresponding BCH bounds. We find $\delta_3=6$ by considering $\{11,12,13,14,15\}\subset D_\beta(C)$. In this case, $\Delta(C)=6$. It is worth to mention that in the binary and ternary cases for $n\leq70$ we have that $\frac{\phi(n)}{O_n(q)}\leq6$ and for $n\leq90$ we have that $\frac{\phi(n)}{O_n(q)}\leq8$.

A cyclic code C in $\mathbb{F}_q(n)$, with generator polynomial $g(x)$, is a BCH code of designed distance δ if there exists $\alpha\in U_n$ and $b\in\{0,\dots,n-1\}$ such that $g(x)$ is the polynomial with the lowest degree over $\mathbb{F}_q$ such that $\left\{\alpha^{b+j} \mid j=0,\dots,\delta-2\right\}\subseteq Z(C)$ (see [6, p. 202]). Equivalently, C is a BCH code if for any cyclotomic coset $Q\subseteq D_\alpha(C)$ we have that $Q\cap\{b+j \mid j=0,\dots,\delta-2\}\neq\emptyset$. As it is known, this implies that C is the cyclic code with highest dimension such that its set of zeros satisfies the inclusion mentioned above. We denote such a code by $B_q(\alpha,\delta,b)$. The Bose distance of a BCH code $C=B_q(\alpha,\delta,b)$ is defined as the largest δ' such that $C=B_q(\alpha',\delta',b')$, for some $b'\in\{0,\dots,n-1\}$ and some $\alpha'\in U_n$. We note that for a BCH code it may happen that its Bose distance is less than $\Delta(B_q(\alpha,\delta,b))$, as we shall see in the next example.

Let $\mathbb{L}|\mathbb{F}_q$ be an extension field. For any element $a\in\mathbb{L}$ we denote by $\min_q(a)$ the minimal polynomial of a in $\mathbb{F}_q[x]$. In the case $q=2$ we only write $\min(a)$.

Example 2. Set $q=2$, $n=21$ and fix $\alpha\in U_{21}$ such that $\min(\alpha)=x^6+x^5+x^4+x^2+1$. Let $C=B_2(\alpha,4,6)$ be the BCH code generated by $\operatorname{lcm}\{\min(\alpha),\min(\alpha^3),\min(\alpha^7)\}$. Consider the 2-cyclotomic cosets modulo 21, $C_2(0)=\{0\}$, $C_2(1)=\{1,2,4,8,11,16\}$, $C_2(3)=\{3,6,12\}$, $C_2(5)=\{5,10,13,17,19,20\}$, $C_2(7)=\{7,14\}$ and $C_2(9)=\{9,15,18\}$. One may check that the defining set of the code C with respect to α is $D_\alpha(C)=C_2(1)\cup C_2(3)\cup C_2(7)=C_2(6)\cup C_2(7)\cup C_2(8)$. In this case $A(21)=\{1,5\}$ so we also have to consider the element $\beta\in U_{21}$ such that $\beta^5=\alpha$. Then $D_\beta(C)=5\cdot D_\alpha(C)=C_2(5)\cup C_2(7)\cup C_2(9)$. One may see that the Bose distance is $\delta=4$, given by considering $\{6,7,8\}\subset D_\alpha(C)$ and $\{13,14,15\}\subset D_\beta(C)$. However $\Delta(C)=5$, because $\{1,2,3,4\}\subset D_\alpha(C)$ and $\{17,18,19,20\}\subset D_\beta(C)$. But $\{1,2,3,4\}\subset C_2(1)\cup C_2(3)$ and $\{17,18,19,20\}\subset C_2(5)\cup C_2(9)$, 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 $\mathbb{L}|\mathbb{F}_q$ be an extension field such that $U_n\subseteq\mathbb{L}$ and fix $\alpha\in U_n$. The *(discrete) Fourier transform* of a polynomial

$f \in \mathbb{F}_q(n)$ with respect to α (also called Mattson-Solomon polynomial), that we denote by $\varphi_{\alpha,f}$ is defined as

$$\varphi_{\alpha,f}(x) = \sum_{j=0}^{n-1} f(\alpha^j)x^j.$$

Clearly, $\varphi_{\alpha,f} \in \mathbb{L}(n)$; moreover, the function Fourier transform may be viewed as an isomorphism of algebras $\varphi_\alpha : \mathbb{L}(n) \longrightarrow (\mathbb{L}^n, \star)$, where the multiplication "$\star$" in $\mathbb{L}^n$ is defined coordinatewise (see [1, Section 2.2] or [6, § 8.6]). Then we may see $\varphi_{\alpha,f}$ as a vector in $\mathbb{L}^n$ or as a polynomial in $\mathbb{L}(n)$. The inverse of the Fourier transform is given by $\varphi_{\alpha,g}^{-1}(x) = \frac{1}{n}\sum_{i=0}^{n-1} g(\alpha^{-i})x^i$, where $g \in \mathbb{L}(n)$ (see for example [1], [2], [6]). For any $i \in \{0,\dots,n-1\}$ we denote $\varphi_{\alpha,f}[i] = f(\alpha^i)$, the coefficient (or coordinate) corresponding to x^i.

Remark 3. *For any $\alpha \in U_n$, $f \in \mathbb{F}_q(n)$ and $g \in \mathbb{L}(n)$ we have that:*

1) *$supp\left(\varphi_{\alpha,f}\right) = \left\{i \in \{0,\dots,n-1\} \mid f\left(\alpha^i\right) \neq 0\right\}$ and hence $\mathbb{Z}_n \setminus supp\left(\varphi_{\alpha,f}\right) = D_\alpha(f)$, the defining set of f.*
2) *Since $f = \varphi_{\alpha,\varphi_{\alpha,f}}^{-1}(x)$ then $supp(f) = \left\{i \in \{0,\dots,n-1\} \mid \varphi_{\alpha,f}\left(\alpha^{-i}\right) \neq 0\right\}$, so that $|supp(f)| = n - \left|Z\left(\varphi_{\alpha,f}\right)\right|$.*
3) *$\varphi_{\alpha,g}^{-1} \in \mathbb{F}_q(n)$ if and only if $\left(g\left(\alpha^j\right)\right)^q = g\left(\alpha^j\right)$ for any $j \in \{0,\dots,n-1\}$.*
4) *$\varphi_{\alpha,g}^{-1} \in \mathbb{F}_q(n)$ if and only if $\varphi_{\beta,g}^{-1} \in \mathbb{F}_q(n)$ for all $\beta \in U_n$.*

The first two assertions come directly from the definition of the discrete Fourier transform together with the fact that it is an isomorphism. The third one comes directly from the well-known property that an element $a \in \mathbb{L}$ satisfies that $a \in \mathbb{F}_q$ if and only if $a^q = a$. Finally to see the last assertion observe that if we take another primitive root of unity $\beta \neq \alpha$ the coefficients of $\varphi_{\beta,g}^{-1}$ are obtained by permuting those of $\varphi_{\alpha,g}^{-1}$.

The following lemma, related with the discrete Fourier transform, will play an important role later.

Lemma 4. *Let $g \in \mathbb{L}(n)$. If $\varphi_{\alpha,g}^{-1} \in \mathbb{F}_q(n)$ for any $\alpha \in U_n$ then supp(g) is a union of cyclotomic cosets. If g is an idempotent in $(\mathbb{L}^n, \star)$ the converse holds; that is, if supp(g) is union of q-cyclotomic cosets then $\varphi_{\alpha,g}^{-1} \in \mathbb{F}_q(n)$.*

Proof. First, suppose that $\varphi_{\alpha,g}^{-1} \in \mathbb{F}_q(n)$. Observe that for any $f(x) \in \mathbb{F}_q(n)$, $\varphi_{\beta,f}^q(x) = \sum_{j=0}^{n-1}\left(f\left(\beta^j\right)\right)^q x^j = \sum_{j=0}^{n-1}\left(f\left(\beta^q\right)\right)^j x^j = \varphi_{\beta^q,f}(x)$. So the defining set of $\varphi_{\alpha,g}^{-1}$ is a union of cyclotomic cosets. Since $supp(g) = \mathbb{Z}_n \setminus D_\alpha(\varphi_{\alpha,g}^{-1})$ we are done.

We first note that any idempotent in $(\mathbb{L}^n, \star)$ verifies that its coordinates (or coefficients) are only 1 or 0. Now, suppose that $g \in (\mathbb{L}^n, \star)$ is an idempotent and $supp(g)$ is a union of q-cyclotomic cosets. Then there exists an idempotent $e \in \mathbb{F}_q(n)$ such that $D_\alpha(e) = \mathbb{Z}_n \setminus supp(g)$; in fact, e is the idempotent generator of the code over $\mathbb{F}_q$ with defining set $\mathbb{Z}_n \setminus supp(g)$ with respect to α. Since e is an idempotent in $\mathbb{F}_q(n)$ we have that $\varphi_{\alpha,e}$ is an idempotent in $(\mathbb{L}^n, \star)$ and also $supp(\varphi_{\alpha,e}) = supp(g)$. Then $\varphi_{\alpha,e} = g$ and hence $\varphi_{\alpha,g}^{-1} \in \mathbb{F}_q(n)$. □

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. We only need the univariate polynomials version.

Definition 5. *Let $\mathbb{L}$ be a field. For any element $g \in \mathbb{L}(n)$ we define the apparent distance of g, that we denote by $d^*(g)$, as follows*

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

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

It is easy to see that one may compute the apparent distance of a polynomial $0 \neq g \in \mathbb{L}(n)$ as follows. Suppose that $g = \sum a_i x^i$. If we associate to the polynomial its coefficient vector $M(g) = (a_0,\dots,a_{n-1})$ then the apparent distance $d^*(g)$ is the length of the biggest chain of consecutive zeros (modulo n) in $M(g)$ plus 1.

Example 6. Let $f = 1+x+x^4 \in \mathbb{F}_2(5)$. Compute $\overline{x^0 f} = 1+x+x^4$, $\overline{xf} = 1+x+x^2$; $\overline{x^2 f} = x+x^2+x^3$; $\overline{x^3 f} = x^2+x^3+x^4$; $\overline{x^4 f} = 1+x^3+x^4$. Then $d^*(f) = 5 - \deg(\overline{xf}) = 3$.

If we take $M(f) = (1\ 1\ 0\ 0\ 1)$ then $d^*(f) = 2+1 = 3$.

Let $f \in \mathbb{L}(n)$. It is clear that the polynomials f and $\overline{x^h f}$ have the same set of zeros (or root set). Hence, $\deg\left(\overline{x^h f}\right) \geq |D_\alpha(f)|$, for any $\alpha \in U_n$, where $D_\alpha(f)$ denotes the defining set of f. Therefore $d^*(f) \leq n - |D_\alpha(f)|$ for any $\alpha \in U_n$.

Now, by the definition of the inverse Fourier transform (see Remark 3), we have that

$$\omega(f) = n - |D_\alpha(\varphi_{\alpha,f})|. \tag{2}$$

Hence,

$$d^*(\varphi_{\alpha,f}) \leq n - |D_\alpha(\varphi_{\alpha,f})| = \omega(f), \quad \text{for all} \quad f \in \mathbb{F}_q(n) \quad \text{and} \quad \alpha \in U_n. \tag{3}$$

This implies that the minimum of the apparent distances of the images of the nonzero codewords of a cyclic code is a lower bound for its minimum distance. Camion's definition of apparent distance of an abelian code comes from these ideas. In our case, we present that definition as follows.

Definition 7. *Let C be a cyclic code in $\mathbb{F}_q(n)$ and consider $\alpha \in U_n$. The apparent distance of C with respect to α is $d^*_\alpha(C) = \min_{c\in C,\, c\neq 0}\{d^*(\varphi_{\alpha,c})\}$ and the apparent distance of C is*

$$d^*(C) = \max_{\alpha\in U_n}\{d^*_\alpha(C)\}.$$

We also define the set of optimal roots of C as

$$\mathcal{R}(C) = \left\{\beta \in U_n \;\mid\; d^*_\beta(C) = d^*(C)\right\}.$$

For the paragraph prior Definition 7 we have that $d^*(C) \leq d(C)$ for any cyclic code C. In [1, p. 22] Camion shows that for any cyclic code C the equality $d^*(C) = \Delta(C)$ holds.

Note that the value $d^*(\varphi_{\alpha,c})$ depends on the support of $\varphi_{\alpha,c}$; that is, it depends on the *distribution* of the zeros of c with respect to α; so, the minimum $d^*_\alpha(C)$ depends on the *distribution* of $D_\alpha(C)$. Hence, in order to compute the maximum $d^*(C)$ we need to look at the different defining sets of C, for each $\alpha \in U_n$. As we have seen in Remark 1, if we fix $\alpha \in U_n$ and $\{a_1, \ldots, a_h\}$, a complete set of representatives of the q-cyclotomic cosets modulo n, to consider the different defining sets of C we only need to consider the roots $\beta \in U_n$ such that $\beta^{a_i} = \alpha$ for some a_i coprime with n. Then, for any $\alpha \in U_n$ we define the set

$$\mathcal{R}_\alpha = \{\beta \in U_n \;\mid\; \beta^a = \alpha,\; a \in A(n)\}. \tag{4}$$

where $A(n)$ was defined in (1).

Therefore, in practice, to compute the apparent distance of a cyclic code C in $\mathbb{F}_q(n)$ it is enough to fix $\alpha \in U_n$ and compute $d^*(C) = \max\{d^*_\beta(C) \;\mid\; \beta \in \mathcal{R}_\alpha\}$.

Let $e, g \in C$ be the idempotent generator and the generator polynomial of C, respectively. If $f, h \in \mathbb{F}_q(n)$ then $supp\,(\varphi_{\beta,fh}) \subseteq supp\,(\varphi_{\beta,f})$ because $\varphi_{\beta,fh} = \varphi_{\beta,f} \star \varphi_{\beta,h}$, and then, for any $c \in C$, and any $\beta \in U_n$, we have that $supp\,(\varphi_{\beta,c}) \subseteq supp\,(\varphi_{\beta,g}) = supp\,(\varphi_{\beta,e})$; so that, $d^*\,(\varphi_{\beta,g}) = d^*\,(\varphi_{\beta,e}) \leq d^*\,(\varphi_{\beta,c})$. Hence, $d^*_\beta(C) = d^*\,(\varphi_{\beta,e})$ and

$$\Delta(C) = d^*(C) = d^*\,(\varphi_{\beta,e}) = d^*\,(\varphi_{\beta,g}) \leq d(C), \quad \forall \beta \in \mathcal{R}(C). \tag{5}$$

(see [1, p. 22]).

Example 8. Set $q = 2$, $n = 17$ and take $a_1 = 0, a_2 = 1, a_3 = 3$ as representatives of the 2-cyclotomic cosets in $\mathbb{Z}_{17}$. Then $A(17) = \{1, 3\}$. Let C be the cyclic code with defining set $D_\alpha(C) = C_2(1) = \{1, 2, 4, 8, 9, 13, 15, 16\}$ with respect to $\alpha \in U_{17}$, such that $\min(\alpha) = x^8+x^7+x^6+x^4+x^2+x+1$. The reader may check that $e = x^{16}+x^{15}+x^{13}+x^9+x^8+x^4+x^2+x+1$ is the idempotent generator of C, and $M(\varphi_{\alpha,e}) = (1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0)$. Then $d^*\,(\varphi_{\alpha,e}) = 3$. Taking β such that $\beta^3 = \alpha$, one may check that $d^*\,(\varphi_{\beta,e}) = 4$. Hence $\Delta(C) = d^*(C) = d^*\,(\varphi_{\beta,e}) = 4$.

As an immediate consequence of (5) we have the following corollary.

Corollary 9. *Let C be a cyclic code in $\mathbb{F}_q(n)$ and let $e, g \in C$ be the idempotent generator and the generator polynomial of C, respectively. For $f \in \{e, g\}$ we have that if $d^*(\varphi_{\alpha,f}) = \omega(f)$ for some $\alpha \in U_n$ then $d(C) = \Delta(C)$ and $\alpha \in \mathcal{R}(C)$.*

Proof. By hypothesis, $d^*(\varphi_{\alpha,f}) = \omega(f) \geq d(C)$. Now, if $\beta \in \mathcal{R}(C)$ then $d^*(\varphi_{\alpha,f}) \leq d^*(\varphi_{\beta,f})$ and so (5) get us the result. □

In the following table we list non trivial cyclic codes of lenght at most 31, satifying the conditions of the corollary above; that is, $d^*\varphi_{\alpha,f} = \omega(f)$ for some $\alpha \in U_n$. Here, $\overline{D(C)} = \mathbb{Z}_n \setminus D(C)$. Computations were done by using GAP4r7.

Lenght	$\overline{D(C)}$	$\dim_{\mathbb{F}}(C)$	$d(C)$
7	$C_2(3)$	3	4
	$C_2(1)$	3	4
	$C_2(0) \cup C_2(3)$	4	3
	$C_2(0) \cup C_2(1)$	4	3
9	$C_2(3)$	2	6
	$C_2(0) \cup C_2(3)$	3	3
	$C_2(1)$	6	2

Lenght	$\overline{D(C)}$	$\dim_{\mathbb{F}}(C)$	$d(C)$
15	$C_2(5)$	2	10
	$C_2(0) \cup C_2(5)$	3	5
	$C_2(1)$	4	8
	$C_2(7)$	4	8
	$C_2(0) \cup C_2(3)$	5	3
	$C_2(0) \cup C_2(7)$	5	7
	$C_2(0) \cup C_2(1)$	5	7
	$C_2(3) \cup C_2(5)$	6	6
	$C_2(0) \cup C_2(5) \cup C_2(7)$	7	5
	$C_2(1) \cup C_2(3)$	8	4
	$C_2(3) \cup C_2(7)$	8	4
	$C_2(3) \cup C_2(7)$	8	4
	$C_2(1) \cup C_2(5) \cup C_2(7)$	10	2
21	$C_2(7)$	2	14
	$C_2(3)$	3	12
	$C_2(9)$	3	12
	$C_2(0) \cup C_2(7)$	3	7
	$C_2(0) \cup C_2(3)$	4	9
	$C_2(0) \cup C_2(9)$	4	9
	$C_2(3) \cup C_2(7)$	5	10
	$C_2(7) \cup C_2(9)$	5	10
	$C_2(0) \cup C_2(3) \cup C_2(9)$	7	3
	$C_2(1) \cup C_2(7)$	8	6
	$C_2(5) \cup C_2(7)$	8	6
	$C_2(1) \cup C_2(9)$	9	4
	$C_2(3) \cup C_2(5)$	9	4
	$C_2(0) \cup C_2(5) \cup C_2(9)$	10	5
	$C_2(0) \cup C_2(1) \cup C_2(3)$	10	5
	$C_2(5) \cup C_2(7) \cup C_2(9)$	11	6
	$C_2(0) \cup C_2(1) \cup C_2(7) \cup C_2(9)$	12	3
25	$C_2(3) \cup C_2(5)$	5	5
27	$C_2(9)$	2	18
	$C_2(3)$	5	6
	$C_2(1)$	18	2
	$C_2(0) \cup C_2(9)$	3	9
31	$C_2(1)$	5	16
	$C_2(5)$	5	16
	$C_2(15)$	5	16
	$C_2(0) \cup C_2(1)$	6	15
	$C_2(0) \cup C_2(15)$	6	15
	$C_2(3) \cup C_2(7)$	10	6
	$C_2(5) \cup C_2(11)$	10	10
	$C_2(1) \cup C_2(3) \cup C_2(15)$	15	6
	$C_2(1) \cup C_2(5) \cup C_2(11)$	15	6
	$C_2(1) \cup C_2(7) \cup C_2(15)$	15	6
	$C_2(5) \cup C_2(9) \cup C_2(15)$	15	6
	$C_2(0) \cup C_2(1) \cup C_2(3) \cup C_2(7)$	16	5
	$C_2(0) \cup C_2(1) \cup C_2(11) \cup C_2(15)$	16	5
	$C_2(0) \cup C_2(1) \cup C_2(5) \cup C_2(15)$	16	5
	$C_2(0) \cup C_2(3) \cup C_2(5) \cup C_2(11)$	16	5
	$C_2(0) \cup C_2(5) \cup C_2(7) \cup C_2(11)$	16	5
	$C_2(0) \cup C_2(3) \cup C_2(5) \cup C_2(11)$	16	5

Let us comment how these results allow us to construct cyclic codes and to compute its apparent distance (or the BCH bound). First, let us observe that for any cyclic code C generated by $e = e^2 \in \mathbb{F}_q(n)$ one has that $\varphi_{\alpha,e}$ is an idempotent in

$(\mathbb{L}, \star)$. So, $\varphi_{\alpha,e}[i] = e(\alpha^i) = 0$ if $i \in D_\alpha(C)$ and 1 otherwise.

Now, let $\{a_1, \ldots, a_h\}$ be a complete set of represantives of the q-cyclotomic cosets modulo n. For each choice $D = \cup_{j=1}^t C_q(a_{i_j})$, with $i_j \in \{1, \ldots, h\}$ and $1 \leq t \leq h$, we denote by $F_D \in \mathbb{F}_q^n$ the vector such that $F_D[i] = 0$ if $i \in D$ and 1 otherwise. Then F_D may be viewed as the image under the Fourier transform of the idempotent generator of a cyclic code C in $\mathbb{F}_q(n)$ such that $D = D_\alpha(C)$ with respect to some $\alpha \in U_n$. That is, if C is the cyclic code with defining set $D_\alpha(C) = D$, with respecct to $\alpha \in U_n$, and $e^2 = e$ is its idempotent generator then we have that $F_D = \varphi_{\alpha,e} \in \mathbb{F}_q^n$. To compute the apparent distance $d^*(C)$ we first consider the set $A(n) = \{a_{i_1}, \ldots, a_{i_k}\} \subseteq \{a_1, \ldots, a_h\}$. Then, for every $j = 1, \ldots, k$, let $\beta_j \in U_n$ be such that $\beta_j^{a_{i_j}} = \alpha$; recall that this implies $D_{\beta_j}(C) = a_{i_j} \cdot D_\alpha(C)$. The apparent distance of $\varphi_{\beta_j,e}$ is the length of the biggest chain of consecutive zeros (modulo n) in $F_{D_{\beta_j}(C)}$ plus 1. So, $d^*(C) = \max\limits_{j=1,\ldots,k} d^*(F_{D_{\beta_j}(C)})$.

Example 10. Set $n = 21$, $q = 2$ and $A(21) = \{1, 5\}$. Consider the 2-cyclotomic cosets: $C_2(0)$, $C_2(1)$, $C_2(3)$, $C_2(5)$, $C_2(7)$, $C_2(9)$ listed in Example 2. Choose $D = C_2(1) \cup C_2(3) \cup C_2(7)$. Then

$$F_D \;=\; (1\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1)\,.$$

Let $C = \langle e \rangle$ be the cyclic code such that $D_\alpha(C) = D$ for some $\alpha \in U_{21}$. Then $d^*(\varphi_{\alpha,e}) = 5$. We only need to consider $\beta \in U_{21}$ such that $\beta^5 = \alpha$. In that case, $D_\beta(C) = 5 \cdot D_\alpha(C) = C_2(5) \cup C_2(9) \cup C_2(7)$. Then

$$F_{D_\beta(C)} \;=\; (1\,1\,1\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,0)\,.$$

So $d^*(F_{D_\beta(C)}) = 5$ too. Hence $d^*(C) = 5$ and $\mathcal{R}(C) = \{\beta, \beta^5\}$. The reader may check that C has four BCH bounds, $\delta = 2, 3, 4, 5$.

III. The minimum distance and the BCH bound

For an arbitrary element $g \in \mathbb{L}(n)$, which we may view as a polynomial with $\deg(g) \leq n - 1$, it is easy to see that the equality $\gcd(g, x^n - 1) = \gcd(x^h g, x^n - 1)$ holds for any $h \in \{0, \ldots, n-1\}$ as x^h and $x^n - 1$ are relatively prime polynomials; so, we may write

$$m_g = \gcd(x^h g, x^n - 1) \tag{6}$$

as m_g does not depend on h. For any $h \in \{0, \ldots, n-1\}$ we also write

$$x^h g = (x^n - 1) f_{g,h} + \overline{x^h g} \tag{7}$$

where $0 \leq \deg(\overline{x^h g}) < n$. 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 [6, Theorem 8.6.31]) we obtain the following result.

Lemma 11. *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 $d^*(g) = n - \deg(g)$.*

Proof. *(1)* It comes from the fact that $m_g \mid \overline{x^h g}$ for any $0 \leq h \leq n - 1$, and from Definition 5. *(2)* By the definition of $d^*(g)$ we have that $d^*(g) \geq n - \deg(g)$. To get the converse inequality note that $g = s m_g$, for some $s \in \mathbb{F}_q$, and apply *(1)*. □

Now let C be a cylic code in $\mathbb{F}_q(n)$ and let $c \in C$ be any codeword. By (3) we have that $d^*(\varphi_{\alpha,c}) \leq \omega(c)$. We wonder if the equality may occur. Next result will be helpful to find an answer (see [1, Theorem 4.1] and [3, Theorem 2]).

Lemma 12. *Let C be a cyclic code in $\mathbb{F}_q(n)$ and $c \in C$. Then $n - \deg\left(m_{\varphi_{\alpha,c}}\right) = \omega(c)$, for all $\alpha \in U_n$.*

Proof. We have that $n - \deg\left(m_{\varphi_{\alpha,c}}\right) = |\{\alpha^j \mid \varphi_{\alpha,c}(\alpha^j) \neq 0\}|$. By Remark 3 and (2) we are done. □

Note that by Lemma 11 we have that 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 holds.

Proposition 13. *Consider $f \in \mathbb{L}(n)$ and let m_f be as in (6). 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 $\mathbb{L}[x]$).*

Proof. Suppose first that the equality holds. By definition of apparent distance we know that there exists $h \in \{0, \ldots, n-1\}$ such that $d^*(f) = n - \deg\left(\overline{x^h f}\right)$. Hence $\deg\left(\overline{x^h f}\right) = \deg(m_f)$. By (6) and (7) we have that m_f and $\overline{x^h f}$ have exactly the same set of zeros and hence they are associated polynomials, or equivalently, $\overline{x^h f} \mid x^n - 1$.

Conversely, suppose that there exists $h \in \{0, \ldots, n-1\}$ such that $\overline{x^h f} \mid x^n - 1$. Again by (7) and (6), $\overline{x^h f}$ and m_f must be associated polynomials. By definition of apparent distance we have that $d^*(f) = d^*\left(\overline{x^h f}\right)$ and by Lemma 11*(2)*, $d^*\left(\overline{x^h f}\right) = n - \deg\left(\overline{x^h f}\right)$. The result follows immediately. □

Now we deal with our first problem. We are going to present some results that give theoretical characterizations for a given cyclic code to satisfy the equality $d(C) = \Delta(C)$.

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 $\mathbb{F}_q$ and an extension $\mathbb{L}|\mathbb{F}_q$ such that $U_n \subseteq \mathbb{L}$. Let C be a cyclic code in $\mathbb{F}_q(n)$. 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) $\varphi_{\alpha,f}^{-1} \in C$, for some $\alpha \in \mathcal{R}(C)$.

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

Proof. First, suppose that $d(C) = \Delta(C)$. Then we have that $d(C) = d^*(C)$. Let $c \in C$ such that $\omega(c) = d(C)$, consider $\alpha \in \mathcal{R}(C)$ and set, as in (6), $m_{\varphi_{\alpha,c}} = \gcd(\varphi_{\alpha,c}, x^n - 1)$. By definition of apparent distance and by applying results above, we have that

$$\omega(c) \geq d^*(\varphi_{\alpha,c}) \geq d^*_\alpha(C) = d^*(C) = d(C) = \omega(c) = n - \deg\left(m_{\varphi_{\alpha,c}}\right).$$

Hence $d^*(\varphi_{\alpha,c}) = d^*(C)$, since $d^*\left(\varphi_{\alpha,c}\right) = n - \deg\left(m_{\varphi_{\alpha,c}}\right)$. So, $f = \varphi_{\alpha,c}$ satisfies all required conditions.

Conversely, suppose there exists $f \in \mathbb{L}(n)$ satisfying conditions *(1 – 3)* of the statement. By Lemma 12 and the definition of minimum distance, we have that $d^*(f) = \omega(\varphi_{\alpha,f}^{-1}) \geq d(C)$. Then by Condition *(1)*, $d^*(C) \geq d(C)$, and hence by (5), $\Delta(C) = d(C)$.

The final assertion follows directly from Proposition 13. □

So, to check if a code satisfies the conditions in the theorem above, Proposition 13 shows us that we have to focus on properties of some divisors of $x^n - 1$. After Corollary 16 we will make some comments about complexity in order to consider those divisors.

Corollary 15. *Let C be a cyclic code in $\mathbb{F}_q(n)$. Then $d(C) = \Delta(C)$ if and only if there exist $k \in \{0, \dots, n-1\}$ 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) $d^*(f) = d^*(C)$.
2) $\varphi_{\alpha,f}^{-1} \in C$, for some $\alpha \in \mathcal{R}(C)$.

Proof. Set $h = n - k$. Then $g = \overline{x^h f}$ and the result follows from Proposition 13 and the theorem above. □

We note that, in the setting of the previous corollary, it may happen that there exist $\alpha, \beta \in U_n$ such that $\varphi_{\alpha,f}^{-1} \in C$ but $\varphi_{\beta,f}^{-1} \notin C$.

We may rewrite the condition *(3)* in Theorem 14 or *(2)* in Corollary 15, as follows.

Corollary 16. *Let C be a cyclic code in $\mathbb{F}_q(n)$. Then $d(C) = \Delta(C)$ if and only if there exist $k \in \{0, \dots, n-1\}$ 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$(f) \subseteq \mathbb{Z}_n \setminus D_\alpha(C)$, for some $\alpha \in \mathcal{R}(C)$,
3) $(f(\alpha^j))^q = f(\alpha^j)$, for any $j \in \{0, \dots, n-1\}$.

Proof. From Remark 3, it comes immediately that condition *(2)* in Corollary 15 holds if and only if conditions *(2)+(3)* of this corollary hold. □

Given a linear code C of length n, we wonder about how difficult is to check the equality $\Delta(C) = d(C)$; in other words, using our previous results, how difficult is to find a polynomial satisfying the required conditions?

To apply any of the corollaries above we have to compute the divisors $g \mid x^n - 1$ in $\mathbb{L}[x]$ with $\deg(g) = n - \Delta(C)$. This means that we have to check at most $h \cdot \binom{n}{n-\Delta(C)}$ polynomials, where $h = |A(n)|$. Clearly, if $\Delta(C)$ is not a "big" number we may check all divisors in $\mathbb{L}[x]$. In case that $\Delta(C)$ was a "big" number, we could reduce it by taking an intermediate field, $\mathbb{F}_q \subset \mathbb{K} \subset \mathbb{L}$, where the number of divisors of $x^n - 1$ (in $\mathbb{K}[x]$) is smaller. However, in that case, our searching of codes would not be exhaustive.

For example, consider the binary cyclic code C of length 45 with $D_\alpha(C) = C_2(3) \cup C_2(5)$, for some $\alpha \in U_{45}$. One may see that $\Delta(C) = 3$ and $\dim(C) = 35$. Consider $A(45) = \{1, 7\}$. To check any of our corollaries above we have to consider $2\binom{45}{42}$-polynomials (note that $2^{14} < 2\binom{45}{42} < 2^{15}$) so our method works. On the other hand, for codes with apparent distance greater than 5, we might choose to consider the factors of $x^{45} - 1$ in an intermediate ring. For example, in $\mathbb{F}_{2^4}[x]$ there are 15 factors of degree 1 and 10 factors of degree 3. No more than 50 computations. Essentially the same happens in $\mathbb{F}_{2^6}[x]$.

Now we give another sufficient condition to characterize cyclic codes whose apparent distance reaches its minimum distance.

Corollary 17. *Let C be a cyclic code in $\mathbb{F}_q(n)$ with generator idempotent $e \in C$. If there exist $h \in \{0, \dots, n-1\}$ and $\alpha \in U_n$ such that $\overline{x^h \varphi_{\alpha,e}} \mid x^n - 1$ then $d(C) = \Delta(C)$ and $\alpha \in \mathcal{R}(C)$.*

Proof. From Proposition 13 and Lemma 12 we may deduce that $d^*\left(\varphi_{\alpha,e}\right) = n - \deg\left(m_{\varphi_{\alpha,e}}\right) = \omega(e)$. So, the result follows directly from Corollary 9. □

The previous results give us conditions for a cyclic code C to satisfy the equality $d(C) = \Delta(C)$. Now we deal with our second problem, that is, the construction of such kind of codes.

Corollary 18. *Consider an intermediate field $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \mathbb{L}$, let $g \in \mathbb{K}[x]$ be a divisor of $x^n - 1$ and $\beta \in U_n$. If $\varphi^{-1}_{\beta,\overline{x^k g}}$ belongs to $\mathbb{F}_q(n)$, for some $k \in \{0, \ldots, n-1\}$, then the family of permutation equivalent cyclic codes $\left\{C_\alpha = \left(\varphi^{-1}_{\alpha,\overline{x^k g}}\right) \mid \alpha \in U_n\right\}$ satisfies $\Delta(C_\alpha) = d(C_\alpha)$ for all $\alpha \in U_n$. Moreover, in this case, $\dim_{\mathbb{F}_q}(C_\alpha) = |supp(g)|$, for all $\alpha \in U_n$.*

Proof. Fix $\alpha \in U_n$. Set $f = \overline{x^k g}$ and let $e \in \mathbb{F}_q(n)$ be the idempotent generator of the ideal $C = \left(\varphi^{-1}_{\alpha,f}\right)$ in $\mathbb{F}_q(n)$ (see Remark 3(4)). It is easy to check that $supp(\varphi_{\alpha,e}) = supp(f) = \mathbb{Z}_n \setminus D_\alpha(C)$ and hence, $d^*(\varphi_{\alpha,e}) = d^*(f)$. On the one hand, by Proposition 13 and Lemma 12 one has that $d^* f = n - deg(m_f) = \omega\left(\varphi^{-1}_{\beta,f}\right) \geq d(C)$. On the other hand, by (5), $d^* f = d^*\left(\varphi_{\alpha,e}\right) \leq d^*_\alpha(C) \leq d^*(C) \leq d(C)$. So we are done. □

Then, in order to construct codes with the desired property we need to find a divisor g of $x^n - 1$ satisfying the condition *(2)* in Corollary 15. However, in the case $\mathbb{K} = \mathbb{F}_2$, it is clear that $g \in (\mathbb{F}_2^n, \star)$ is always an idempotent, and so, we only have to check that $supp(g)$ is union of 2-cyclotomic cosets (see Lemma 4).

Let us show by an example how the combination of Corollary 16 and Corollay 18 works.

Example 19. Set $q = 2$, $n = 45$. In this case $A(45) = \{1, 7\}$. Take $g = x^{40} + x^{39} + x^{38} + x^{36} + x^{35} + x^{32} + x^{30} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{17} + x^{15} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$. One may check that $g \mid x^{45} - 1$ in $\mathbb{F}_2[x]$ (so that $\mathbb{K} = \mathbb{F}_2$). To find the parameter k mentioned in the corollary above, we may analize the vector $M(g)$ or we may fix $\beta \in U_{45}$ (as instance, such that $\min(\beta) = x^{12} + x^3 + 1$) and compute $g(1)$ and $g(\beta^3)$, because $D_\beta(g) = \mathbb{Z}_{45} \setminus (C_2(0) \cup C_2(3))$. Let us choose the last alternative. Since $g(1) = 1$ and $g(\beta^3) = \beta^{30}$ then $k = 5$ will work because setting $f = x^5 g$ we have that $f(1) = 1$, $f\left(\beta^3\right) = (\beta^3)^5 \beta^{30} = \beta^{45} = 1$ and then $f\left(\beta^6\right) = f\left(\beta^{12}\right) = f\left(\beta^{24}\right) = 1$, as $C_2(3) = \{3, 6, 12, 24\}$. So that, $\varphi^{-1}_{\alpha,f} \in \mathbb{F}(45)$, for all $\alpha \in U_{45}$. Now set $C = (\varphi^{-1}_{\beta,f})$. Then $D_\beta(C) = C_2(1) \cup C_2(3) \cup C_2(9) \cup C_2(21) = \mathbb{Z}_{45} \setminus supp(M(f))$ and, by analizing $M(g)$ or $M(f) = F_{D_\beta(C)}$ as in Example 10, we have that $5 = d(C) = \Delta(C)$ and $\dim(C) = 21$.

As $supp(x^5 g) = \mathbb{Z}_{45} \setminus D_\beta(C)$, one may see that there are three subsets that determines $d^*(C)$; to wit, $\{1, 2, 3, 4\}$, $\{16, 17, 18, 19\}$ and $\{31, 32, 33, 34\}$. We choose $\{1, 2, 3, 4\} \subset D_\beta(C)$ and construct the code C' such that $D_\beta(C') = D_\beta(C) \setminus C_2(21)$. Note that C is a subcode of C', because $D_\beta(C') \subset D_\beta(C)$. Now one has that C' satisfies the conditions in Corollary 15, because $d^*(C) = 5 = d^*(f)$ and $\varphi^{-1}_{\alpha,f} \in C \subset C'$, so that $5 = d(C') = \Delta(C')$ and $\dim(C') = 25$, that is, C' has better parameters than C.

In the next section (see, as instance, Example 25) we will refine this type of construction to obtain BCH codes C such that $\Delta(C) = d(C)$. Now we continue with the construction of codes C satisfying that $\Delta(C) = d(C)$.

Corollary 20. *Consider an intermediate field $\mathbb{F}_q \subseteq \mathbb{F}_{q'} \subseteq \mathbb{L}$, let h be an irreducible factor of $x^n - 1$ in $\mathbb{F}_{q'}[x]$ with defining set $D_\alpha(h)$ for some $\alpha \in U_n$. Set $g = (x^n - 1)/h$. If there are positive integers j, t such that $g(\alpha^j) = \alpha^t$ and $\gcd\left(j, \frac{n}{\gcd(q-1,n)}\right) \mid t$ then there exists a q-ary code of length n whose BCH bound equals its minimum distance.*

Proof. By hypothesis, the congruence (in X),

$$\frac{q-1}{\gcd(q-1,n)} jX \equiv -\frac{q-1}{\gcd(q-1,n)} t \mod \frac{n}{\gcd(q-1,n)}$$

has a solution $X = k$, with $0 \leq k \leq \frac{n}{\gcd(q-1,n)}$. Then $(q-1)(jk+t) \equiv 0 \mod n$, which means that $q(jk+t) \equiv jt + k \mod n$, and hence $\overline{x^k g}(\alpha^j) = \alpha^{jk+t} \in \mathbb{F}_q$. Clearly, for any $jq'^a \in D_\alpha(h)$ we have $jq'^a k + tq'^a \equiv q'^a(jk+t) \equiv jk + t \mod n$, so that $\overline{x^k g}(\alpha^{jq'^a}) \in \mathbb{F}_q$. As $\overline{x^k g}(\alpha^i) = 0$ for all $i \in \mathbb{Z}_n \setminus D_\alpha(h)$, we may apply Corollary 18 to get the desired result. More precisely, the code $C = \left(\varphi^{-1}_{\alpha,\overline{x^k g}}\right) \subseteq \mathbb{F}_q(n)$ satisfies the required conditions. □

Corollary 21. *Let $n = 2^m - 1$, for some $m \in \mathbb{N}$. There exist at least $\frac{\phi(n)}{m}$ binary codes of length n whose BCH bound equals its minimum distance.*

Proof. We are going to apply the corollary above with $2 = q = q'$. Take $\mathbb{L} = \mathbb{F}_{2^m}$. For each $0 < j < n$, coprime with n, we consider the 2-cyclotomic coset $C_2(j)$, which has exactly m elements. Consider $\alpha \in U_n$. Let $h | x^n - 1$ be the polynomial in $\mathbb{F}_q[x]$, such that $D_\alpha(h) = C_2(j)$ and $g_j = (x^n - 1)/h$. By hypothesis, α is a primitive element for $\mathbb{L}$, so that $g_j(\alpha^j) = \alpha^k$ for some $k \in \mathbb{Z}_n$. The condition $\gcd(j, n) \mid k$ holds obviously. So that there exists a binary code of length n whose BCH bound equals its minimum distance. Moreover, by Corollary 18 the family of codes $\{C_j = \left(\varphi^{-1}_{\alpha,\overline{x^k g_j}}\right) \mid \gcd(j, n) = 1\}$ satisfies that $d(C_j) = \Delta(C_j)$ for any j. To compute the number of different codes in that family we consider the set

$B = \{C_2(j) \mid j \in \mathbb{Z}_n, \gcd(j,n) = 1\}$. One may check that $|B| = \frac{\phi(n)}{m}$. Let $C_q(j) \neq C_q(j') \in B$. If $\alpha \in U_n$ and h, h' are the divisors of $x^n - 1$ with $D_\alpha(h) = C_q(j)$ and $D_\alpha(h') = C_q(j')$ then $g_j = (x^n - 1)/h$ and $g_{j'} = (x^n - 1)/h'$ have the same degree, and hence $supp(g_j) \neq supp(g_{j'})$ because they are binary polynomials. Since $D(C_j) = supp(\overline{x^k g_j})$ the result comes immediately. □

Example 22. Set $q = 2$, $n = 15$. Then $A(15) = \{1, 7\}$. By Corollary 21 there exist at least two codes such that its BCH bound equals its minimum distance (they will be determined by the polynomials g_3 and g_4 defined below). Denote the irreducible factors of $x^{15} - 1$ in $\mathbb{F}_2[x]$, by $h_1 = \Phi_2$, $h_2 = \Phi_3$, $h_3 = x^4 + x + 1$, $h_4 = x^4 + x^3 + 1$ and $h_5 = \Phi_5$, where Φ_j denotes the j-th cyclotomic polynomial. Setting $g_i = \frac{x^n - 1}{h_i}$, $i = 1, \ldots, 5$, we apply the corollaries above (with $\mathbb{K} = \mathbb{F}_2$) as follows.

Consider the factor g_2. Then one may check that in this case $\varphi^{-1}_{\alpha,\overline{xg_2}} = x^{10} + x^5 \in \mathbb{F}_2(15)$, for all $\alpha \in U_{15}$. The cyclic code C generated by $x^{10} + x^5$ satisfies $\dim(C) = 10$ and $\Delta(C) = 2 = d(C)$. Now let us fix $\alpha \in U_{15}$ such that $h_3 = \min(\alpha)$ and $h_4 = \min(\alpha^{13})$, where $\min(\alpha^t)$ denotes the minimal polynomial of α^t in $\mathbb{F}_2[x]$. Then $\varphi^{-1}_{\alpha,\overline{xg_3}} = x^{14} + x^{13} + x^{11} + x^7 \in \mathbb{F}_2(15)$ and $\varphi^{-1}_{\alpha,\overline{x^3 g_4}} = x^8 + x^4 + x^2 + x \in \mathbb{F}_2(15)$. This gives us the table

Generator	Dimension	$\Delta = d$
$\varphi^{-1}_{\alpha,\overline{xg_2}}$	10	2
$\varphi^{-1}_{\alpha,\overline{xg_3}}$	8	4
$\varphi^{-1}_{\alpha,\overline{x^3 g_4}}$	8	4

The polynomial g_1 gets an improper code. In the case of g_5, as $D_\alpha(g_5) = \mathbb{Z}_{15} \setminus C_2(3)$, it happens that, $g_5\left(\alpha^3\right) = \alpha^{14}$, so the conditions of Corollary 20 are not satisfied.

After inspecting the divisors of $x^{15} - 1$ in $\mathbb{F}_2[x]$ we find more interesting codes. For instance, one may check that the polynomial $h_2 h_3 h_5$ satisfies the conditions of Corollary 18, with $k = 0$, and hence it yields a code, say C', such that $\Delta(C') = d(C') = 5$ and $\dim(C') = 7$.

Example 23. Set $q = 2$ and $n = 21$. Denote the irreducible factors of $x^{21} - 1$ in $\mathbb{F}_2[x]$ by $h_1 = \Phi_2$, $h_2 = \Phi_3$, $h_3 = x^3 + x + 1$, $h_4 = x^3 + x^2 + 1$, $h_5 = x^6 + x^4 + x^2 + x + 1$ and $h_6 = x^6 + x^5 + x^4 + x^2 + 1$.

Set $g_i = \frac{x^n - 1}{h_i}$, $i = 1, \ldots, 6$, and fix $\alpha \in U_{21}$ such that $\min(\alpha) = h_6$. We apply Corollary 20 as above (with $\mathbb{K} = \mathbb{F}_2$) to get the following table of binary codes of length 21 whose BCH bound equals its minimum distance. We complete with another one satisfying the conditions of Corollary 18.

Generator	Dimension	$\Delta = d$
$\varphi^{-1}_{\alpha,\overline{xg_2}}$	14	2
$\varphi^{-1}_{\alpha,g_3}$	12	3
$\varphi^{-1}_{\alpha,\overline{x^3 g_4}}$	12	3
$\varphi^{-1}_{\alpha,\overline{xg_5}}$	8	6
$\varphi^{-1}_{\alpha,\overline{x^5 g_6}}$	8	6
$\varphi^{-1}_{\alpha,\overline{h_1 h_3 h_5 h_6}}$	10	5

IV. Applications: Constructing BCH codes whose minimum distance equals their apparent distance

The following result allows us to construct BCH codes $B_q(\alpha, \delta, b)$ for which $d(B_q(\alpha, \delta, b)) = \Delta(B_q(\alpha, \delta, b)) = \delta$. We recall that the ideal generated by a polynomial $g \in \mathbb{F}_q(n)$ is denoted by (g).

Theorem 24. *Let n be a positive integer, p a prime number, q a power of p and U_n the set of primitive n-th roots of unity. Assume that $\gcd(n, q) = 1$. Consider the fields $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \mathbb{L}$ such that $U_n \subset \mathbb{L}$. Let $g \in \mathbb{K}[x]$ be a divisor of $x^n - 1$. If there exist $k \in \{0, \ldots, n-1\}$ and $\beta \in U_n$ such that $\varphi^{-1}_{\beta,\overline{x^k g}} \in \mathbb{F}_q(n)$ then there exists a family of permutation equivalent BCH codes $\{C_\alpha = B_q(\alpha, \delta, b) \mid \alpha \in U_n\}$ with $\delta = n - \deg(g)$ and $b \in \mathbb{Z}_n$, such that $\delta = \Delta(C_\alpha) = d(C_\alpha)$ and $\varphi^{-1}_{\alpha,\overline{x^k g}} \in C_\alpha$.*

Proof. Set $g = \sum_{i=0}^{n-1} a_i x^i$ and suppose that there there exist $k \in \{0, \ldots, n-1\}$ and $\beta \in U_n$ such that $\varphi^{-1}_{\beta,\overline{x^k g}} \in \mathbb{F}_q(n)$. Let $f = \overline{x^k g}$ and consider $\alpha \in U_n$. By Lemma 11, $d^*(g) = n - \deg(g)$. Clearly $m_f = g$ and $d^*(f) = d^*(g)$. We collect $T = \bigcup_{j=\deg(g)+k+1}^{n+k-1} C_q(\overline{j})$, where $\overline{j}$ is the canonical representative of j module n, and $\varepsilon = \sum_{i=0}^{n-1} r_i x^i$ such that $r_i = 0$ if $i \in T$ and 1, otherwise.

We claim that $d^*(g) = d^*(\varepsilon)$. From the definition of ϵ one has that $d^*(g) \leq d^*(\varepsilon)$. We are going to see the reverse inequality. By Remark 3(3), as $\varphi^{-1}_{\beta,f} \in \mathbb{F}_q(n)$ we have that $supp\,(f)$ is union of q-cyclotomic cosets modulo n. So, for any $j \in \{\deg(g) + k + 1, \ldots, n + k - 1\}$ we have that $C_q(\overline{j}) \cap supp\,(f) = \emptyset$ and hence $T \subseteq \mathbb{Z}_n \setminus supp\,(f)$, which means that $supp\,(f) \subseteq supp\,(\varepsilon)$ and hence $d^*(g) = d^*(f) \geq d^*(\varepsilon)$.

By construction, $supp(\varepsilon)$ is union of q-cyclotomic cosets, so $\varphi^{-1}_{\alpha,\varepsilon} \in \mathbb{F}_q(n)$ (see Lemma 4). We set $C = \left(\varphi^{-1}_{\alpha,\varepsilon}\right)$ in $\mathbb{F}_q(n)$. We are going to see that C satisfies the conditions *(1)* and *(2)* of Corollary 15.

(1) We have already seen that $d^*(f) = d^*(g) = d^*(\varepsilon)$. Now, by Proposition 13 and Lemma 12 one has that $d^* f = n - deg(m_f) = \omega\left(\varphi_{\alpha,f}^{-1}\right) \geq d(C)$. On the other hand, by (5), $d^* f = d^*(\epsilon) = d^*\left(\varphi_{\alpha,\varphi_{\alpha,\epsilon}^{-1}}\right) \leq d_\alpha^*(C) \leq d^*(C) \leq d(C)$.Therefore $d^*(C) = d^*(f)$.

(2) Since $supp(f) \subseteq supp(\varepsilon)$, we have that $f \star \varepsilon = f$, and then $\varphi_{\alpha,f}^{-1} \cdot \varphi_{\alpha,\varepsilon}^{-1} = \varphi_{\alpha,f}^{-1}$, which means that $\varphi_{\alpha,f}^{-1} \in (\varphi_{\alpha,\varepsilon}^{-1}) = C$ (see also Remark 3(4)). So that, conditions of Corollary 15 are satisfied, and hence $d(C) = \Delta(C)$.

Finally, to see that C is a BCH code with designed distance $\delta = \Delta(C)$, we note that, any q-cyclotomic coset $Q \subseteq supp(\varepsilon) = D_\alpha(C)$ verifies that $Q \cap \{deg(g) + k + 1, \ldots, n + k - 1\} \neq \emptyset$. So, as we mentioned in Section II, this means that C is a BCH code with $b = deg(g) + k + 1$ and designed distance $\delta = \Delta(C) = n - deg(g)$. □

The theorem above gives us a method to transform a given cyclic code $C = (g)$, with $d(C) = \Delta(C)$ into another code with higher dimension; in fact, we can get a new BCH code. The key idea is to consider as generator ε instead of g via the definition of T. This definition may be done in different ways that can drives us to different BCH codes. All these ideas are shown in the next example.

Example 25. We continue with the code C showed in Example 19. Recall that $q = 2$, $n = 45$ and C is the cyclic code with $D_\beta(C) = C_2(1) \cup C_2(3) \cup C_2(9) \cup C_2(21)$, where $\beta \in U_{45}$ is such that $\min(\beta) = x^{12} + x^3 + 1$. Following the proof of the previous theorem we have that $T = C_2(1) \cup C_2(3)$ and set $\varepsilon = \sum_{i \notin T} x^i$. Then $C'' = \left(\varphi_{\beta,\varepsilon}^{-1}\right)$ has $D_\beta(C'') = C_2(1) \cup C_2(3)$; so that it is the BCH code $B_2(\beta, 5, 1)$ of dimension 29 such that $d(C'') = \Delta(C'') = 5$. This code has even better parameters than C' (see Example 19).

It is also possible to obtain, from the code C', the BCH code $B_2(\beta, 5, 16)$ with $d(B_2(\beta, 5, 16)) = \Delta(B_2(\beta, 5, 16)) = 5$ and dimension 29, by taking $T' = C_2(1) \cup C_2(9)$.

The following theorem is a classical result on the theory of BCH codes.

Theorem 26 ([6]). *Let $h, m \in \mathbb{N}$. A BCH code C of length $n = q^m - 1$ and designed distance $\delta = q^h - 1$ over $\mathbb{F}_q$ satisfies that $d(C) = \Delta(C)$.*

Now let us show some examples of construction of new BCH codes.

Example 27. Set $q = 2$ and $n = 15$. Consider the polynomial $g = g_3$ in Example 22; that is $g = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$. Then, its coefficient vector is

$$M(g) = (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$$

and we may check that $d^*(g) = 4$. We know that $\varphi_{\alpha,g}^{-1} \notin \mathbb{F}_2(n)$ for all $\alpha \in U_{15}$, because $C_2(7)$ is not contained in $supp(g)$ (see Lemma 4). However, the polynomial $\overline{xg}$ with coefficient vector

$$M(\overline{xg}) = (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$$

satisfies that $\varphi_{\alpha,\overline{xg}}^{-1} \in \mathbb{F}_2(n)$ for all $\alpha \in U_{15}$. Let us fix $\alpha \in U_{15}$. Then $C = (\varphi_{\alpha,\overline{xg}}^{-1})$ is a binary code with $d(C) = d^*(C) = 4$ and $\dim_{\mathbb{F}_2}(C) = 8$ (see Corollary 18). But, C is not a BCH code. Following the ideas in Theorem 24 we may replace 0's by 1's in the suitable places to get the vector

$$M(\varepsilon) = (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$$

such that $C' = \left(\varphi_{\alpha,\varepsilon}^{-1}\right)$ is a BCH code in $\mathbb{F}_2(n)$, with $d(C') = d^*(C') = \delta = 4$ and $\dim_{\mathbb{F}_2}(C') = 10$. Clearly, this code cannot be considered in Theorem 26.

We finish by extending Corollary 20 to BCH codes.

Corollary 28. *Consider an intermediate field $\mathbb{F}_q \subseteq \mathbb{F}_{q'} \subseteq \mathbb{L}$, let h be an irreducible factor of $x^n - 1$ in $\mathbb{F}_{q'}[x]$ with defining set $D_\alpha(h)$ for some $\alpha \in U_n$ and $g = (x^n - 1)/h$. If there are positive integers j, t such that $g(\alpha^j) = \alpha^t$ and $\gcd\left(j, \frac{n}{\gcd(q-1,n)}\right) \mid t$ then there exists a BCH code of designed distance δ, $C = B_q(\alpha, \delta, b)$, such that $\delta = \Delta(C) = d(C) = \deg(h)$, for certain $b \in \mathbb{Z}_n$.*

Proof. Comes immediately from Corollary 20 together with Theorem 24. □

Example 29. We continue with the codes determined by the polynomials g_2, g_3 and g_4 in Example 22. Recall that in this case $\alpha \in U_{15}$ satisfies that $\min(\alpha) = h_3$. By applying the ideas contained in the proof of Theorem 24, one may obtain the following BCH codes whose minimum distance equals the maximum of their BCH bounds.

It is possible to modify the defining set, w.r.t. α, of a cyclic code in order to obtain a defining set for a new code with higher dimension. In this case we will say that the original one was dimensional-extended to the new one. For example, $\left(\varphi_{\alpha,\overline{xg_2}}^{-1}\right)$ in $\mathbb{F}_q(15)$ has dimension 10 and it can be dimensional-extended to the codes $B_2(\alpha, 2, 0)$ of dimension 14 and $B_2(\alpha, 2, 3t)$ of dimension 11, for $t = 1, 2, 3$. The cyclic code determined by g_3, that is $\left(\varphi_{\alpha,\overline{xg_3}}^{-1}\right)$ in $\mathbb{F}_q(15)$, has dimension 8 and it may be dimensional-extended to $B_2(\alpha, 4, 13)$ of dimension 10. Finally, from $\left(\varphi^{-1}_{\alpha,\overline{x^3 g_4}}\right)$, with dimension 8, we get $B_2(\alpha, 4, 0)$ of dimension 10.

Note that the dimensional-extended BCH codes associated to g_2, g_3 and g_4 are not considered in the classical result 26. There is another interesting code which has not been considered: the code $\left(\varphi^{-1}_{\alpha,\overline{h_1 h_2 h_3 h_5}}\right)$, where h_1, h_2, h_3, h_5 were defined in Example 22, is the code $B_2(\alpha, 5, 11)$ of dimension 10.

Example 30. We also also show how to *extend the dimension* of the codes in Example 23. We recall that $q = 2$, $n = 21$ and α satisfies that $\min(\alpha) = h_6$. In this case, we have the following BCH codes whose minimum distance and apparent distance coincide.

It is possible to modify the set $D_\alpha\left(\varphi^{-1}_{\alpha,\overline{x g_2}}\right)$ in three different ways. The biggest dimensional-extended code that we can obtain is $B_2(\alpha, 2, 0)$ of dimension 20. In the case of $\left(\varphi^{-1}_{\alpha,g_3}\right)$, it determines two BCH codes. The first one is $B_2(\alpha, 3, 19)$ of dimension 15 and the second one is $B_2(\alpha, 3, 12)$ of dimension 12. The code $\left(\varphi^{-1}_{\alpha,\overline{x^3 g_4}}\right)$ may be dimensional-extended to $B_2(\alpha, 3, 15)$ of dimension 12, and $B_2(\alpha, 3, 1)$ of dimension 15. The code $\left(\varphi^{-1}_{\alpha,\overline{x g_5}}\right)$ may be dimensional-extended to $B_2(\alpha, 6, 17)$ of dimension 11. In the case of $\left(\varphi^{-1}_{\alpha,\overline{x^5 g_6}}\right)$, we obtain $B_2(\alpha, 6, 0)$ of dimension 11. Finally, $\left(\varphi^{-1}_{\alpha,\overline{h_1 h_3 h_5 h_6}}\right)$ is the BCH code $B_2(\alpha, 10, 17)$ of dimension 10.

We finish with an example of a binary BCH code of length 33 whose minimum distance equals the maximum of their BCH bounds. We have not found in the literature any binary BCH code satisfying that condition and having this length and dimension.

Example 31. Set $q = 2$, $n = 33$ and $\alpha \in U_{33}$ such that $\min(\alpha) = x^{10} + x^7 + x^5 + x^3 + 1$ and $g = \min(\alpha)\min(\alpha^3)\min(\alpha^5)$. One may check that g verifies the conditions of Theorem 24 with $k = 0$ and $T = C_2(1)$; in fact $\varphi^{-1}_{\alpha,g} = x^{22} + x^{11} + 1$. Hence, it determines $B_2(\alpha, 3, 31)$ of dimension 23.

Acknowledgement. The authors are grateful to the referees for many suggestions which contributed to improve this paper.

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] GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra. http://www.gap-system.org/

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

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

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

Received xxxx 20xx; revised xxxx 20xx.