On the Weight Distribution of the Dual of some Cyclic Codes with Two Non Conjugated Zeros✧

C.A. Vázquez-Fernández*[1], G. Vega-Hernández[2]

[1] Posgrado en Ciencia e Ingeniería de la Computación,
Universidad Nacional Autónoma de México,
04510 México D.F., México
* cvazquez@uxmcc2.iimas.unam.mx
[2] Dirección General de Cómputo y de Tecnologías de Información y Comunicación,
Universidad Nacional Autónoma de México, 04510 México D.F., México
gerardov@servidor.unam.mx

ABSTRACT
An important family of codes for error control in digital communications are the so-called cyclic codes; therefore, finding the weight distribution of a *q*-ary cyclic code *C* is not only a problem of theoretical interest, but also of practical importance. Typically, when the finite field $\mathbb{F}_q$ is a prime field, the problem is handled by expressing the Hamming weight of each codeword in *C* by means of certain combination of exponential sums. In this work, we will present a new method for computing the weight distribution of the dual of some cyclic codes with two non conjugated zeros. As we will see, such distribution is also given by means of the evaluation of certain exponential sums, however, such evaluation is only needed to be done over a subset. Moreover, this method has the advantage of flexibility, in the sense that it can also be applied to cyclic codes over finite fields of non prime order.

Keywords: Coding theory, cyclic codes, weight distribution, linear recurring sequences, exponential sums.

RESUMEN
Una familia importante de códigos para el control de errores en comunicaciones digitales son los llamados códigos cíclicos; por lo tanto, encontrar la distribución de pesos de un código cíclico *q*-ario *C*, no sólo es un problema de interés teórico sino también tiene una importancia práctica. Típicamente, cuando el campo finito $\mathbb{F}_q$ es un campo primo, el problema es manejado expresando el peso de Hamming de cada palabra de código en *C* por medio de cierta combinación de sumas exponenciales. En este trabajo, presentaremos un nuevo método para calcular la distribución de pesos del dual de algunos códigos cíclicos con dos ceros no conjugados. Como veremos, tal distribución esta dada también en términos de la evaluación de ciertas sumas exponenciales, sin embargo, tal evaluación será solamente necesaria sobre un subconjunto. Por otra parte, este método tiene la ventaja de la flexibilidad, en el sentido que puede también ser aplicado a códigos cíclicos sobre campos finitos de orden no primo.

1. Introduction

Let $q = p^m$ where p is a prime number and *m* is a positive integer. For some positive integer *k*, let γ be a primitive element of $\mathbb{F}_{q^k}$. Let C be the cyclic code over $\mathbb{F}_q$ of length $n = q^k - 1$. Finding the weight distribution of *C* is a problem of theoretical and practical interest. Typically, when the finite field $\mathbb{F}_q$ is a prime field, the problem is handled by expressing the Hamming weight of each codeword in *C* by means of certain combination of exponential sums. More precisely speaking, if *C* is a reducible cyclic code with parity-check polynomial $h(x) = h_1(x)h_2(x)\cdots h_t(x) \quad (t > 1)$, where $h_i(x)$ $(1 \le i \le t)$ are distinct irreducible polynomials over $\mathbb{F}_p[x]$ with the same degree k, and if γ^{-a_i} is a zero of $h_i(x)$ $(1 \le i \le t)$, then the weight distribution of cyclic code *C* can be derived from the value distribution of the exponential sum (see for example [1, 2])

✧ Partially supported by PAPIIT-UNAM IN105611

$$\sum_{c\in\mathbb{F}_{q^k}} \chi(d_1c^{a_1} + d_2c^{a_2} + \cdots + d_tc^{a_t}), \qquad (1)$$

where χ is the canonical additive character of $\mathbb{F}_{p^k}$, and $d_1, d_2, \cdots, d_t \in \mathbb{F}_{p^k}$.

In this work, we will present a new method for computing the weight distribution of some cyclic codes whose dual code has two non conjugated zeros; that is, we will show that if *C* is a cyclic code over $\mathbb{F}_q$, whose dual code has zero γ^{a_1} and γ^{a_2}, where the integers a_1 and a_2 satisfy $a_1q^i \not\equiv a_2 \pmod{q^k-1}$, for all $i \geq 0$ and

$$\gcd(a_1, (q^k-1)/(q-1)) = \gcd(a_2, (q^k-1)/(q-1)) = 1, \qquad (2)$$

then it is always possible to find an integer ω in such a way that the weight distribution of *C* can be fully obtained by means of the distribution of the values

$$\sum_{c\in\mathbb{F}_{q^k}} \chi(dc^{\omega} - c), \qquad (3)$$

where ; however, as we will see, the computation of such values is only needed to be done over a subset of $\mathbb{F}_{q^k}^*$. In addition, this alternative method has the advantage of flexibility in the sense that it can also be applied to cyclic codes over finite fields of non prime order.

In order to achieve our goal, we will use several results related to linear recurring sequences and exponential sums. These results can be found in [3].

This work is organized as follows: in Section 2, we recall the connection between linear cyclic codes and linear recurring sequences. In Section 3, we use some characterizations for the one-weight irreducible cyclic codes in order to obtain some preliminary results. Section 4, is also devoted to presenting some preliminary results, but now related to exponential and Gaussian sums. The new method for computing the weight distribution is presented in Section 5. In Section 6, some examples are shown, whereas in Section 7, the conclusion is presented.

2. Linear Recurring Sequences and Cyclic Codes

First of all, we set, for this section and for the rest of this work, the following:

Notation: By using *p*, *q* and *k*, we will denote positive integers, such that *p* is a prime number and *q* is a positive power of *p*. We will fix $n = q^k - 1$ and $\Delta = (q^k-1)/(q-1)$. For now on, γ will denote a fixed primitive element of $\mathbb{F}_{q^k}$. As usual, wt(*c*(*x*)), will mean the *Hamming weight* of the polynomial *c*(*x*) in the ring $\mathbb{F}_q[x]/(x^n-1)$. Also, we will denote by "Tr", the *absolute trace mapping* from $\mathbb{F}_{q^k}$ to the prime field $\mathbb{F}_p$, and by "$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$" the *trace mapping* from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Finally, we will denote by $\mathcal{C}_b$ the *cyclotomic coset modulo n* over the prime field $\mathbb{F}_p$ which contains *b*, where $0 \leq b < n$. The subscript b is called the *coset representative modulo n* (see for example [4, p. 197]).

Let $h(x)$ and $g(x)$ be monic polynomials over $\mathbb{F}_q$, such that $h(x)$ is irreducible, $\deg(h(x)) = k$ and $h(x)g(x) = x^n - 1$. Without loss of generality, we may suppose that

$$h(x) = x^k - h_{k-1}x^{k-1} - h_{k-2}x^{k-2} - \cdots - h_0. \qquad (4)$$

Since the coefficients of the polynomial $g(x)$, can be obtained through the synthetic division of polynomials $x^n - 1$ and $h(x)$, then, if

$$g(x) = g_0x^{n-1} + g_1x^{n-2} + \cdots + g_{k-1}x^{n-k} + g_kx^{n-k-1} + \cdots + g_{n-1}, \qquad (5)$$

we have $g_i = 0$ for all $0 \le i < k-1$, $g_{k-1} = 1$ and

$$g_{m+k} = h_{k-1}g_{m+k-1} + h_{k-2}g_{m+k-2} + \cdots + h_0 g_m, \qquad (6)$$

With $0 \le m < n-k$ That is, the n coefficients of $g(x)$ in (5) are the first n terms of the *kth-order impulse response sequence* (see [3, p. 402]), given by

$$g_{m+k} = h_{k-1}g_{m+k-1} + h_{k-2}g_{m+k-2} + \cdots + h_0 g_m \quad \text{for } m = 0,1,2,\cdots. \qquad (7)$$

In agreement with Theorem 8.27 in [3, p. 408], the previous sequence is *periodic* (in the sense of Definition 8.5 in [3, p. 398]), where such period, r, is equal to the order of $h(x)$ (see for example Definition 3.2 in [3, p. 84]), that is, $r = \text{ord}(h(x))$.

We will use the same notation introduced in [3, Ch. 8, Secc. 5, p. 423]. Thus, $S(h(x))$ will denote the set of all *homogeneous linear recurring* sequences in $\mathbb{F}_q$ with characteristic polynomial $h(x)$. Particularly, we will denote by σ the unique element in $S(h(x))$, which corresponds to the kth-order impulse response sequence whose characteristic polynomial is $h(x)$. That is, in the context of (7), we see that $\sigma = g_0, g_1, g_2, \cdots$. For any sequence $\tau = t_0, t_1, t_2, \cdots$ in $\mathbb{F}_q$, for any integer $s \ge 0$ and for any finite field element $d \in \mathbb{F}_q$, we denote by $d\tau^{(s)}$ the shifted and weighted sequence $dt_s, dt_{s+1}, dt_{s+2}, \cdots$. Since the period r, of σ, divides the length n, then the n coefficients of the polynomial $dx^s g(x)$, in the ring $\mathbb{F}_q[x]/(x^n - 1)$, are the first n terms of the shifted and weighted sequence $d\sigma^{(s)}$.

Let $\tau = t_0, t_1, t_2, \cdots$ be any sequence in $\mathbb{F}_q$. Additionally, let $e \in \mathbb{F}_q$ and let N be a positive integer. Then, we will denote by $Z(\tau, e, N)$ the number of i, $0 \le i < N$, with $t_i = e$ (this notation is similar to that introduced in [3, p. 453]). Since $r \mid n$ then, for the particular case of the sequence σ, we have (see equation 8).

$$Z(d\sigma^{(s)}, 0, n) = Z(\sigma, 0, n), \text{ for all } d \in \mathbb{F}_q^* \text{ and for any integer } s \ge 0. \qquad (8)$$

We end this section by recalling that the kth-order impulse response sequence σ, can be given by means of the trace function; that is, if α is a root of $h(x)$, then by virtue of Theorem 8.24 of [3, p. 406], we know that there exists $\theta \in \mathbb{F}_{q^k}$ in such a way that the elements of the sequence σ are given by

$$g_m = \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\theta\alpha^m) \quad \text{for } m = 0,1,2,\cdots. \qquad (9)$$

An explicit formula for θ is presented in [5, Lemma 3].

3. One-weight Irreducible Cyclic Codes and Some of its Consequences

The following definition could be considered as an extension of the order, ord(f), of a polynomial $f(x) \in \mathbb{F}_q[x]$.

Definition 1 *Let $h(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree with $h(0) \neq 0$. The least positive integer ρ for which x^ρ is congruent modulo $h(x)$, to some element of $\mathbb{F}_q$, is called the quasi-order of $h(x)$ and it will be denoted by qord($h(x)$).*

The following set of characterizations for the one-weight cyclic codes, that was introduced in [6], will be the main tool of this work.

Theorem 1 *Let q, k, n, Δ and γ be as before. For a positive integer* a, *let $h_a(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of γ^a. Set $\rho = \text{qord}(h_a(x))$ and $g_a(x) = (x^n - 1)/h_a(x)$. Then, the following five statements are equivalent:*

A) $\gcd(a, \Delta) = 1$.

B) $\deg(h_a(x)) = k$ and $\rho = \Delta$.

C) $\deg(h_a(x)) = k$ and $\mathrm{wt}(g_a(x)) = (q-1)q^{k-1}$.
D) $\deg(h_a(x)) = k$ *and, if* σ *is the kth-order impulse response sequence with characteristic polynomial* $h_a(x)$, *then for any nonzero codeword* $c(x)$ *in the cyclic code* $< g_a(x) >$ *there exists a uniquely determined integer s,* $0 \le s < \Delta$, *and a uniquely determined field element* $d \in \mathbb{F}_q$, *such that the n coefficients of* $c(x)$ *are the first n terms of the sequence* $\tau = d\sigma^{(s)}$.
E) $h_a(x)$ *is the parity-check polynomial for a one-weight cyclic code over* $\mathbb{F}_q$ *, of length n and dimension k.*

With the same notation we present the following:

Remark 1 *Observe that if* a *satisfies Statement (A) then, by Statement (B) and Definition 1,* Δ *is the least positive integer for which* $(\gamma^a)^{\Delta} \in \mathbb{F}_q^*$.

Remark 2 *Observe that if* a *satisfies Statement (A) then, by Statement (B) and Definition 1, there exists a uniquely determined field element* $d_a \in \mathbb{F}_q^*$ *such that* $x^{\Delta} g_a(x) = d_a g_a(x)$ *in the ring* $\mathbb{F}_q[x]/(x^n - 1)$, *which in turn implies that* $\sigma^{(\Delta+m)} = d_a \sigma^{(m)}$ *for any integer* $m \ge 0$.

Keeping in mind the previous remarks, we present the following lemmas.

Lemma 1 *Assume the same notation as in the previous theorem. Also assume that* integer a satisfies Statement (A) and set $\alpha = \gamma^a$. Then

$$\left\{ d\alpha^s : d \in \mathbb{F}_q^* \text{ and } 0 \le s < \Delta \right\} = \mathbb{F}_{q^k}^* . \quad (10)$$

Proof: It will suffice to prove that $\left|\left\{ d\alpha^s : d \in \mathbb{F}_q^* \text{ and } 0 \le s < \Delta \right\}\right| = q^k - 1$Therefore, suppose the existence of finite field elements $d_1, d_2 \in \mathbb{F}_q^*$ and integers $0 \le s_1, s_2 < \Delta$ such that $d_1\alpha^{s_1} = d_2\alpha^{s_2}$. Without loss of generality, we may assume $s_1 \ge s_2$, thus $d_1 d_2^{-1} \alpha^{s_1 - s_2} = 1$, which implies that $\alpha^{s_1 - s_2} \in \mathbb{F}_q^*$. But $0 \le s_1 - s_2 < \Delta$ thus, by Remark 1, we get $s_1 = s_2$, and, in consequence, $d_1 = d_2$.

Lemma 2 *With the same notation, let* a_1 *and* a_2 *be two integers such that* $\gcd(a_1, \Delta) = \gcd(a_2, \Delta) = 1$ *and* $a_1 q^i \not\equiv a_2 \pmod{q^k - 1}$ *, for all* $i \ge 0$ *. Let C be the cyclic code over* $\mathbb{F}_q$ *of length n, whose parity-check polynomial is given by* $h_{a_1}(x) h_{a_2}(x)$. *Let* σ_1 *and* σ_2 *be, respectively, the kth-order impulse response sequences whose characteristic polynomials are, respectively,* $h_{a_1}(x)$ *and* $h_{a_2}(x)$. *As usual, let* A_i *be the number of codewords in C, of Hamming weight i. If we take the following set of sequences*

$$\mathcal{S} = \{ d\sigma_1^{(s)} - \sigma_2 : d \in \mathbb{F}_q^* \text{ and } 0 \le s < \Delta \},$$

(11)

then $|\mathcal{S}| = q^k - 1$, *and if we set*

$$\mathcal{W} = \{ n - Z(\tau, 0, n) : \tau \in \mathcal{S} \} \cup \{ (q-1)q^{k-1} \}$$

(12)

and

$$F_i = \left| \{ \tau \in \mathcal{S} : i \in \mathcal{W} \text{ and } n - Z(\tau, 0, n) = i \} \right|,$$

(13)

then C is a $|\mathcal{W}|-$ *weight cyclic code of dimension* $2k$ *whose weight distribution is as follows:*

$$A_i = \begin{cases} 1 & \text{if } i = 0 \\ 0 & \text{if } i \ne 0 \text{ and } i \notin \mathcal{W} \\ (q^k - 1)(F_i + 2) & \text{if } i = (q-1)q^{k-1} \\ (q^k - 1)F_i & \text{if } i \ne (q-1)q^{k-1} \text{ and } i \in \mathcal{W} \end{cases} . \quad (14)$$

Proof: Let $g_{a_i}(x) = (x^n - 1)/h_{a_i}(x)$ and $C_i = < g_{a_i}(x) >$, with *i*=1,2. Since $h_{a_1}(x) \ne h_{a_2}(x)$

then, by Theorem 1, we know that $|C_1| = |C_2| = q^k$ and $C_1 \cap C_2 = \overline{0}$, hence the dimension of C is 2k. In addition, by Statement (D), we conclude that $|\mathcal{S}| = q^k - 1$.

We are going to show that if $c(x)$ is a nonzero codeword in C then $\mathrm{wt}(c(x)) \in \mathcal{W}$. Any codeword $c(x) \in C$ is of the form $c(x) = c_1(x) - c_2(x)$, for some codewords $c_1(x) \in C_1$ and $c_2(x) \in C_2$. The codeword $c(x)$ will be trivial if at least one of the codewords $c_1(x)$ or $c_2(x)$ is zero and nontrivial if the two codewords $c_1(x)$ and $c_2(x)$ are different from zero. Again, by Theorem 1, we know that C_1 and C_2 are both one-weight cyclic codes with nonzero weight equal to $(q-1)q^{k-1}$, thus if $c(x)$ is a nonzero trivial codeword we see that $\mathrm{wt}(c(x)) = (q-1)q^{k-1} \in \mathcal{W}$. Now, suppose that $c(x)$ is nontrivial; thus by Statement (D), there exist uniquely determined integers s_1 and s_2, $0 \le s_1, s_2 < \Delta$, and uniquely determined field elements $d_1, d_2 \in \mathbb{F}_q^*$, such that the n coefficients of $c(x)$ are the first n terms of the sequence $\tau_0 = d_1\sigma_1^{(s_1)} - d_2\sigma_2^{(s_2)}$. Let s and ϵ be two integers in such a way that $s + s_2 = \epsilon\Delta + s_1$, where $0 \le s < \Delta$ and $\epsilon = 0$ or 1. Now, by Remark 2, there exists a field element $d_{a_1} \in \mathbb{F}_q^*$ such that $\sigma_1^{(\Delta+m)} = d_{a_1}\sigma_1^{(m)}$ for any integer $m \ge 0$. Thus, let d be the field element in $\mathbb{F}_q^*$ in such a way that $d_1 = dd_2$ if $\epsilon = 0$ and $d_1 = dd_2d_{a_1}$ if $\epsilon = 1$. Clearly $\tau = d\sigma_1^{(s)} - \sigma_2 \in \mathcal{S}$ and, owing to our choice of d and s, we have $d_2\tau^{(s_2)} = \tau_0$ which implies, by (8), that $Z(\tau_0,0,n) = Z(\tau,0,n)$, therefore $\mathrm{wt}(c(x)) \in \mathcal{W}$.

Finally, the weight distribution of C comes from the fact that the number of nonzero trivial codewords in C is equal to $2(q^k - 1)$ (all of them having weight $(q-1)q^{k-1}$), and the fact that for each sequence $\tau \in \mathcal{S}$, there are exactly $q^k - 1$ different pairs (d_2, s_2), in such a way that the first n terms of the sequence $d_2\tau^{(s_2)}$ are the n coefficients of some nontrivial codeword $c(x) \in C$.

4. Some Results on Exponential and Gaussian Sums

We begin this section by recalling some notations on character and Gaussian sums. Thus, by keeping our current notation, we define the *canonical additive character* χ of $\mathbb{F}_{q^k}$:

$$\chi(c) := e^{2\pi i \,\mathrm{Tr}(c)/p}, \quad \text{for all } c \in \mathbb{F}_{q^k}. \qquad (15)$$

On the other hand, any *multiplicative character* of $\mathbb{F}_{q^k}$ is defined by

$$\psi_j(\gamma^l) := e^{2\pi ijl/(q^k-1)}, \quad \text{for } j,l = 0,1,\cdots,q^k - 2.$$

16)

For any multiplicative character ψ of $\mathbb{F}_{q^k}$ and for the canonical additive character χ of $\mathbb{F}_{q^k}$, the *Gaussian sum* $G(\psi,\chi)$ is defined by

$$G(\psi,\chi) := \sum_{c \in \mathbb{F}_{q^k}^*} \psi(c)\chi(c). \qquad (17)$$

For any two integers ω and i, we define the following exponential sum:

$$\mathrm{E}_{q^k}^{(\omega)}(i) := \sum_{c \in \mathbb{F}_{q^k}} \chi(\gamma^i c^\omega - c). \qquad (18)$$

The following two lemmas are properties of $\mathrm{E}_{q^k}^{(\omega)}(i)$:

Lemma 3 *Let ω and i be two integers, then*

$$\mathrm{E}_{q^k}^{(\omega p)}(i) = \mathrm{E}_{q^k}^{(\omega)}(i) \quad \textit{and} \quad \mathrm{E}_{q^k}^{(\omega)}(ip) = \mathrm{E}_{q^k}^{(\omega)}(i).$$

(19)

Proof: First of all, observe that

$$\mathrm{E}_{q^k}^{(\omega)}(i) = 1+\sum_{b}\overline{\chi}(\gamma^b)\sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{j\omega}), \tag{20}$$

Where *b* runs through a set of coset representatives modulo *n*. Thus, the result follows from the following identities:

$$\begin{aligned}\sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{jp\omega}) &= \sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{j\omega})\\ \sum_{j\in\mathcal{C}_b}\chi(\gamma^{ip}\gamma^{j\omega}) = \sum_{j\in\mathcal{C}_b}\chi(\gamma^{ip}\gamma^{jp\omega}) &= \sum_{j\in\mathcal{C}_b}\chi((\gamma^i\gamma^{j\omega})^p) = \sum_{j\in\mathcal{C}_b}\chi(\gamma^i\gamma^{j\omega}).\end{aligned} \tag{21}$$

Lemma 4 *Let ω and i be two integers, then*

$$\sum_{i=0}^{q^k-2}\mathrm{E}_{q^k}^{(\omega)}(i) = q^k. \tag{22}$$

Proof: Since $\chi(0)=1$ we have

$$\sum_{i=0}^{q^k-2}\sum_{c\in\mathbb{F}_{q^k}}\chi(\gamma^i c^\omega - c) = q^k - 1 + \sum_{c\in\mathbb{F}_{q^k}^*}\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega - c). \tag{23}$$

But $\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega - c) = \chi(-c)\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega)$ and since, for all $c\neq 0$, we know that $\sum_{i=0}^{q^k-2}\chi(\gamma^i c^\omega) = \sum_{i=0}^{q^k-2}\chi(\gamma^i) = -1$, thus we conclude

$$\sum_{i=0}^{q^k-2}\sum_{c\in\mathbb{F}_{q^k}}\chi(\gamma^i c^\omega - c) = q^k - 1 - \sum_{c\in\mathbb{F}_{q^k}^*}\chi(-c) = q^k - 1 - \sum_{i=0}^{q^k-2}\chi(\gamma^i) = q^k. \tag{24}$$

Lemma 5 *Let ν and ζ be two integers in such a way that $\nu\zeta = (q-1)$. Then, for any integers ω and y, we have*

$$\sum_{t=1}^{\Delta\nu-1}\psi_{\zeta t}(\gamma^y)G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) = -q^k + \Delta\nu\sum_{j=0}^{\zeta-1}\mathrm{E}_{q^k}^{(\omega)}(y+j\Delta\nu). \tag{25}$$

Proof: By using the definition of Gaussian sum, one obtains

$$\begin{aligned}G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) &= \sum_{c_1\in\mathbb{F}_{q^k}^*}\sum_{c\in\mathbb{F}_{q^k}^*}\overline{\psi_{\zeta t}}(c_1)\chi(c_1)\psi_{\zeta t}^{\omega}(c)\overline{\chi}(c)\\ &= \sum_{c\in\mathbb{F}_{q^k}^*}\sum_{c_1\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(c^\omega c_1^{-1})\chi(c_1 - c).\end{aligned} \tag{26}$$

In the inner sum we substitute $d^{-1} = c^{\omega}c_1^{-1}$. Then

$$\begin{aligned} G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) &= \sum_{c\in\mathbb{F}_{q^k}^*}\sum_{d\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(d^{-1})\chi(dc^{\omega}-c) \\ &= \sum_{d\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(d^{-1})\Big(\sum_{c\in\mathbb{F}_{q^k}}\chi(dc^{\omega}-c)-\chi(0)\Big) \\ &= \sum_{d\in\mathbb{F}_{q^k}^*}\psi_{\zeta t}(d^{-1})\sum_{c\in\mathbb{F}_{q^k}}\chi(dc^{\omega}-c) \\ &= \sum_{i=0}^{q^k-2}\psi_{\zeta t}(\gamma^{-i})\mathsf{E}_{q^k}^{(\omega)}(i), \end{aligned} \tag{27}$$

therefore,

$$\begin{aligned} \sum_{t=1}^{\Delta\nu-1}\psi_{\zeta t}(\gamma^{y})G(\overline{\psi_{\zeta t}},\chi)G(\psi_{\zeta t}^{\omega},\overline{\chi}) &= \sum_{i=0}^{q^k-2}\mathsf{E}_{q^k}^{(\omega)}(i)\sum_{t=1}^{\Delta\nu-1}\psi_{\zeta}(\gamma^{t(y-i)}) \\ &= -\sum_{i=0}^{q^k-2}\mathsf{E}_{q^k}^{(\omega)}(i)+\Delta\nu\sum_{j=0}^{\zeta-1}\mathsf{E}_{q^k}^{(\omega)}(y+j\Delta\nu), \end{aligned} \tag{28}$$

since ψ_{ζ} has order $\Delta\nu$. The result now follows by Lemma 4.,

We end this section with the following:

Lemma 6 *Let a_1 and a_2 be two integers and set $\nu = \gcd(a_1-a_2, q-1)$, $\zeta = (q-1)/\nu$, and $\alpha_2 = \gamma^{a_2}$. Assume that a_2 is a unit in the ring $\mathbb{Z}_{\Delta}$, where $\tilde{a}_2$ is its inverse in such ring. Let $\omega = 1+\tilde{a}_2(a_1-a_2)$, where the arithmetic operations in the definition of ω are taken in $\mathbb{Z}$. Let B be a set of pairs of multiplicative characters of $\mathbb{F}_{q^k}$. For $d,\theta_1,\theta_2 \in \mathbb{F}_{q^k}^*$ we set*

$$\mathcal{F}(d) = \sum_{(\psi,\varphi)\in B}\psi(\theta_1)G(\overline{\psi},\chi)\varphi(\theta_2)\mathrm{G}(\overline{\varphi},\overline{\chi})\psi(d)\sum_{m=0}^{n-1}\psi(\alpha_1)^m\varphi(\alpha_2)^m. \tag{29}$$

If $B = \left\{\left(\psi_{u_1},\psi_{u_2(q-1)-u_1}\right) \mid 0 \le u_1 < q^k-1,\ 0 \le u_2 < \Delta\right\}$ then, for any integer y, we have

$$\mathcal{F}(\theta_1^{-1}\theta_2^{\omega}\gamma^{y}) = -n^2+\frac{n^2}{\zeta}\sum_{j=0}^{\zeta-1}\mathsf{E}_{q^k}^{(\omega)}(y+j\Delta\nu). \tag{30}$$

Proof: By using *B* we have

$$\begin{aligned} \mathcal{F}(d) &= \sum_{u_1=0}^{q^k-2}\psi_{u_1}(\theta_1)G(\overline{\psi}_{u_1},\chi)\sum_{u_2=0}^{\Delta-1}\psi_{u_2(q-1)-u_1}(\theta_2)G(\overline{\psi}_{u_2(q-1)-u_1},\overline{\chi})\psi_{u_1}(d) \\ &\quad\times\sum_{m=0}^{n-1}\psi_{u_1}(\alpha_1)^m\psi_{u_2(q-1)-u_1}(\alpha_2)^m. \end{aligned} \tag{31}$$

The inner sum in the last expression is a finite geometric series that vanishes if

$$\psi_{u_1}(\alpha_1)\psi_{u_2(q-1)-u_1}(\alpha_2) \neq 1, \text{ because of}$$

$$\psi_{u_1}(\alpha_1)^n \psi_{u_2(q-1)-u_1}(\alpha_2)^n = \psi_{u_1}(\alpha_1^n)\psi_{u_2(q-1)-u_1}(\alpha_2^n) = \psi_{u_1}(1)\psi_{u_2(q-1)-u_1}(1) = 1. \tag{32}$$

On the other hand,

$$\psi_{u_1}(\alpha_1)\psi_{u_2(q-1)-u_1}(\alpha_2) = 1 \iff \psi_1(\gamma^{a_1u_1+a_2(u_2(q-1)-u_1)}) = 1, \tag{33}$$

and clearly

$$\psi_1(\gamma^{a_1u_1+a_2(u_2(q-1)-u_1)}) = 1 \Leftrightarrow a_2u_2(q-1) \equiv (a_2-a_1)u_1 \pmod{q^k-1}, \tag{34}$$

but the last congruence implies that $(q-1) \mid (a_2-a_1)u_1$, and since $\gcd(a_1-a_2, q-1) = \nu$, therefore $u_1 = \zeta t$ for $t = 0,1,\cdots,\Delta\nu-1$. Now, also from the previous congruence, we have

$$\tilde{a}_2a_2u_2(q-1) \equiv \tilde{a}_2(a_2-a_1)u_1 \pmod{q^k-1}, \tag{35}$$

but $\tilde{a}_2a_2 = 1+\ell\Delta$ for some integer ℓ, thus

$$u_2(q-1) \equiv \tilde{a}_2(a_2-a_1)u_1 \pmod{q^k-1}, \tag{36}$$

and hence, for each t, there exists a uniquely $0 \leq u_2 < \Delta$ such that $u_2 \equiv \tilde{a}_2bt \pmod{\Delta}$, where $b = (a_2-a_1)/\nu$. With this we conclude that $\psi_{u_1} = \psi_{\zeta t}$ and $\psi_{u_2(q-1)-u_1} = \psi_{\tilde{a}_2(a_2-a_1)\zeta t-\zeta t} = \overline{\psi^{\omega}_{\zeta t}}$. Thus

$$\mathcal{F}(\theta_1^{-1}\theta_2^{\omega}\gamma^y) = n + n\sum_{t=1}^{\Delta\nu-1}\psi_{\zeta t}(\theta_1)G(\overline{\psi_{\zeta t}},\chi)\overline{\psi^{\omega}_{\zeta t}}(\theta_2)G(\psi^{\omega}_{\zeta t},\overline{\chi})\psi_{\zeta t}(\theta_1^{-1}\theta_2^{\omega}\gamma^y). \tag{37}$$

But $\psi_{\zeta t}(\theta_1)\overline{\psi^{\omega}_{\zeta t}}(\theta_2)\psi_{\zeta t}(\theta_1^{-1}\theta_2^{\omega}) = 1$, and since $\Delta\nu = n/\zeta$ then, by means of previous lemma, we obtain the desired result.

5. The Weight Distribution of some Cyclic Codes whose Dual Code has Two Non Conjugated Zeros

The following result shows that for some cyclic codes *C* whose dual code has two non conjugated zeros, it is always possible to find an integer ω in such a way that the weight distribution of *C* can be fully obtained by means of the distribution of the values $\sum_{c\in\mathbb{F}_{q^k}}\chi(dc^{\omega}-c)$, where $d\in\mathbb{F}_{q^k}^{*}$.

Theorem 2 *For a positive integer a, let* $h_a(x)\in\mathbb{F}_q[x]$ *be the minimal polynomial of* γ^a. *Let* a_1 *and* a_2 *be two integers such that* $\gcd(a_1,\Delta)=\gcd(a_2,\Delta)=1$ *and* $a_1q^i\not\equiv a_2 \pmod{q^k-1}$, *for all* $i\geq 0$. *Let* α_1, α_2, ν, ζ, $\tilde{a}_2$ *and* ω *be as in Lemma 6. Let C be the cyclic code over* $\mathbb{F}_q$ *of length n, whose parity-check polynomial is given by* $h_{a_1}(x)h_{a_2}(x)$. *As usual, let* A_i *be the number of codewords in C, of Hamming weight i. Let*

$$\mathcal{Y}=\{0,1,2,\cdots,q^k-2\}, \tag{38}$$

and if we set

$$\mathcal{W}'=\{(q-1)q^{k-1}-\frac{\nu}{q}\sum_{j=0}^{\zeta-1}\mathrm{E}_{q^k}^{(\omega)}(y+j\Delta\nu): y\in\mathcal{Y}\}\cup\{(q-1)q^{k-1}\} \tag{39}$$

and

$$F_i'=|\{y\in\mathcal{Y}: i\in\mathcal{W}' \text{ and } (q-1)q^{k-1}-\frac{\nu}{q}\sum_{j=0}^{\zeta-1}\mathrm{E}_{q^k}^{(\omega)}(y+j\Delta\nu)=i\}|, \tag{40}$$

then C is a $|\mathcal{W}'|-$ *weight cyclic code of dimension 2k whose weight distribution is as follows:*

$$A_i=\begin{cases}1 & \text{if } i=0\\ 0 & \text{if } i\neq 0 \text{ and } i\notin\mathcal{W}'\\ (q^k-1)(F_i'+2) & \text{if } i=(q-1)q^{k-1}\\ (q^k-1)F_i' & \text{if } i\neq(q-1)q^{k-1} \text{ and } i\in\mathcal{W}'\end{cases}. \tag{41}$$

Proof: Let σ_1 and σ_2 be, respectively, the *k*th-order impulse response sequences whose characteristic polynomials are, respectively, $h_{a_1}(x)$ and $h_{a_2}(x)$. Let $\mathcal{S}$, $\mathcal{W}$ and F_i be as in Lemma 2. Thus, in the context of the proof of Lemma 2, it will suffice to prove the existence of a bijection Φ, from $\mathcal{S}$ onto $\mathcal{Y}$, in such a way that if $\Phi(\tau)=y$ then

$$(q-1)q^{k-1}-\frac{\nu}{q}\sum_{j=0}^{\zeta-1}\mathrm{E}_{q^k}^{(\omega)}(y+j\Delta\nu)=n-Z(\tau,0,n). \tag{42}$$

For this, we assume that $\sigma_i = g_0^{(i)}, g_1^{(i)}, g_2^{(i)}, \ldots$, for $i = 1,2$. Additionally, by using (9), we take θ_i such that $g_m^{(i)} = \mathrm{Tr}_{F/K}(\theta_i \alpha_i^m)$, for $i = 1,2$ and $m = 0,1,2,\cdots$. Since $h_{a_i}(x) \neq 1$, for $i = 1,2$, we have $\theta_1^{-1}\theta_2^{\omega} \neq 0$. With this, we now use Lemma 1 in order to define the bijection Φ in the following way

$$\Phi(\tau = d\sigma_1^{(s)} - \sigma_2) = y - d\alpha_1^s = \theta_1^{-1}\theta_2^{\omega}\gamma^y. \tag{43}$$

So, it only remains to compute $Z(\tau,0,n)$. For this, let χ' be the canonical additive character of $\mathbb{F}_q$, then, by the orthogonal property of χ', we have

$$\frac{1}{q}\sum_{c\in\mathbb{F}_q}\chi'(c(dg_{m+s}^{(1)} - g_m^{(2)})) = \begin{cases} 1 & \text{if } dg_{m+s}^{(1)} = g_m^{(2)} \\ 0 & \text{otherwise} \end{cases}. \tag{44}$$

Thus,

$$Z(\tau,0,n) = \frac{1}{q}\sum_{m=0}^{n-1}\sum_{c\in\mathbb{F}_q}\chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(dc\,\theta_1\alpha_1^{m+s}))\chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(-c\,\theta_2\,\alpha_2^m)). \tag{45}$$

If χ denotes the canonical additive character of $\mathbb{F}_{q^k}$, then χ' and χ are related by $\chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\beta)) = \chi(\beta)$ for all $\beta \in \mathbb{F}_{q^k}$. Therefore,

$$\begin{aligned} Z(\tau,0,n) &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{m=0}^{n-1}\chi(dc\,\theta_1\alpha_1^{m+s})\overline{\chi}(c\,\theta_2\,\alpha_2^m) \\ &= \frac{n}{q} + \frac{1}{q}\sum_{c\in\mathbb{F}_q^*}\sum_{m=0}^{n-1}\chi(dc\,\theta_1\alpha_1^{m+s})\overline{\chi}(c\,\theta_2\,\alpha_2^m). \end{aligned} \tag{46}$$

Now, by means of the expansion of the restriction of χ to $\mathbb{F}_{q^k}^*$ in terms of the multiplicative characters of $\mathbb{F}_{q^k}$, with Gaussian sums as Fourier coefficients (see for example [3, p. 195]), we know that $\chi(dc\,\theta_1\alpha_1^{m+s})\overline{\chi}(c\,\theta_2\,\alpha_2^m)$ is equal to

$$\frac{1}{(q^k-1)^2}\sum_{\psi}\sum_{\varphi}\psi(dc\,\theta_1\alpha_1^{m+s})G(\overline{\psi},\chi)\varphi(c\,\theta_2\,\alpha_2^m)G(\overline{\varphi},\overline{\chi}), \tag{47}$$

where the sums are extended over all multiplicative characters ψ and φ of $\mathbb{F}_{q^k}$. Since $n = q^k - 1$ then, by substituting the last expression into (46), we obtain

$$\begin{aligned} Z(\tau,0,\mathrm{n}) = \frac{n}{q} + \frac{1}{qn^2}&\sum_{\psi}\psi(\theta_1)G(\overline{\psi},\chi)\sum_{\varphi}\varphi(\theta_2)G(\overline{\varphi},\overline{\chi})\psi(d\alpha_1^s) \\ &\times\sum_{m=0}^{n-1}\psi(\alpha_1)^m\varphi(\alpha_2)^m\sum_{c\in\mathbb{F}_q^*}(\psi\varphi)(c). \end{aligned} \tag{48}$$

If the restriction of $\psi\varphi$ to $\mathbb{F}_q^*$ is nontrivial, then, by the orthogonal property of $\psi\varphi$, we have $\sum_{c\in\mathbb{F}_q^*}(\psi\varphi)(c)=0$. Consequently, it suffices to extend the previous sum over the set B of pairs of characters ψ and φ for which $\psi\varphi$ is trivial in $\mathbb{F}_q^*$, so that $Z(\tau,0,n)$ is equal to

$$\frac{n}{q}+\frac{q-1}{qn^2}\sum_{(\psi,\varphi)\in B}\psi(\theta_1)G(\overline{\psi},\chi)\varphi(\theta_2)G(\overline{\varphi},\overline{\chi})\psi(d\alpha_1^s)\sum_{m=0}^{n-1}\psi(\alpha_1)^m\varphi(\alpha_2)^m. \qquad (49)$$

Since $\mathbb{F}_q^* = \{\gamma^{s\Delta} \mid 0 \le s < (q-1)\}$, then

$$B = \left\{\left(\psi_{u_1},\psi_{u_2(q-1)-u_1}\right) \,\middle|\, 0 \le u_1 < q^k-1,\ 0 \le u_2 < \Delta\right\}. \qquad (50)$$

But, by bijection Φ, we know that $d\alpha_1^s = \theta_1^{-1}\theta_2^{\omega}\gamma^y$, thus a direct application of Lemma 6 proves (42).

6. Some Examples

The main key for the determination of the weight distribution, in the context of Theorem 2 is the evaluation of the exponential sums $\mathrm{E}_{q^k}^{(\omega)}(i)$, for a fixed ω, and for $i = 0,1,\cdots,q^k-2$. However, thanks to the second equality in Lemma 3, such evaluation is only needed to be done for a set of coset representatives modulo q^k-1. Taking this into consideration, and by using our current notation, we present the following examples.

1) Let $q=4$, $k=2$, $a_1=6$ and $a_2=3$, then $\Delta=5$, $\nu=3$, $\zeta=1$, $\tilde{a}_2=2$ and $\omega=7$. If we choose $\mathbb{F}_{16}=\mathbb{F}_2(\gamma)$, with $\gamma^4+\gamma+1=0$, we find that $\mathrm{E}_{16}^{(7)}(0)=\mathrm{E}_{16}^{(7)}(1)=0$, $\mathrm{E}_{16}^{(7)}(3)=4$, $\mathrm{E}_{16}^{(7)}(5)=8$ and $\mathrm{E}_{16}^{(7)}(7)=-4$. Since $|\mathcal{C}_b|=4$ for b = 1,3,7, $|\mathcal{C}_5|=2$ and $|\mathcal{C}_0|=1$ then, by Theorem 2 we have $\mathcal{W}'=\{12,9,6,15\}$, $F'_{12}=5$, $F'_9=F'_{15}=4$ and $F'_6=2$. Therefore $h_6(x)h_3(x)\in\mathbb{F}_4[x]$, is the parity-check polynomial for a four-weight cyclic code over $\mathbb{F}_4$, of length 15, dimension 4 and weight enumerator polynomial:
$A(z) = 1+30z^6+60z^9+105z^{12}+60z^{15}$.

2) Let $q=4$, $k=2$, $a_1=6$ and $a_2=2$, then $\Delta=5$, $\nu=1$, $\zeta=3$, $\tilde{a}_2=3$ and $\omega=13$. Due to the first equality in Lemma 3, we have $\mathrm{E}_{16}^{(13)}(i)=\mathrm{E}_{16}^{(7)}(i)$ for all i $(0\le i<15)$. Thus, by using the previous example, we have

$$\sum_{j=0}^{2}\mathrm{E}_{16}^{(13)}(y+5j) = \begin{cases}16 & \text{if } y\in\mathcal{C}_0\cup\mathcal{C}_5\\ 0 & \text{otherwise}\end{cases},$$

implying that $\mathcal{W}'=\{8,12\}$, $F'_8=3$ and $F'_{12}=12$. Therefore $h_6(x)h_2(x)\in\mathbb{F}_4[x]$, is the parity-check polynomial for a two-weight cyclic code over $\mathbb{F}_4$, of length 15, dimension 4 and weight enumerator polynomial:
$A(z) = 1+45z^8+210z^{12}$.

3) Let $q=2$, $k=4$, $a_1=7$ and $a_2=1$, then $\Delta=15$, $\nu=\zeta=1$, $\tilde{a}_2=1$ and $\omega=7$. Thus, by using Example 1), we have $\mathcal{W}'=\{8,6,4,10\}$, $F'_8=5$, $F'_6=F'_{10}=4$ and $F'_4=2$. Therefore $h_1(x)h_7(x)\in\mathbb{F}_2[x]$, is the parity-check polynomial

for a four-weight binary cyclic code of length 15, dimension 8 and weight enumerator polynomial:
$A(z) = 1+30z^4+60z^6+105z^8+60z^{10}$.

4) Let $q=3$, $k=3$, $a_1=4$ and $a_2=2$, then $\Delta=13$, $\nu=2$, $\zeta=1$, $\tilde{a}_2=7$ and $\omega=15$. If we choose $\mathbb{F}_{27}=\mathbb{F}_3(\gamma)$, with $\gamma^3+2\gamma+1=0$, we find that for $i\in\{0,2,4,7,13,14,17\}$, $E_{27}^{(15)}(i)=0$, $E_{27}^{(15)}(1)=E_{27}^{(15)}(8)=9$ and $E_{27}^{(15)}(5)=-9$. Since $|\mathcal{C}_b|=3$ for b = 1,2,4,5,7,8,14,17 and $|\mathcal{C}_b|=1$ for b = 0,13 then, by Theorem 2 we have $\mathcal{W}'=\{18,12,24\}$, $F'_{18}=17$, $F'_{12}=6$ and $F'_{24}=3$. Therefore $h_4(x)h_2(x)\in\mathbb{F}_3[x]$, is the parity-check polynomial for a three-weight cyclic code over $\mathbb{F}_3$, of length 26, dimension 6 and weight enumerator polynomial:
$A(z) = 1+156z^{12}+494z^{18}+78z^{24}$.

7. Conclusion

In general, the problem of determining the weight distribution of a cyclic code over a finite field seems to be difficult. Typically, when the finite field is a prime field, the problem is handled by expressing the Hamming weight of each codeword by means of certain combination of exponential sums. In this work, we presented an alternative method for computing the weight distribution of some cyclic codes whose dual code has two non conjugated zeros (Theorem 2). This method also needs the evaluation of some exponential sums, however, as we saw in the previous section, such evaluation is only needed to be done over a set of coset representatives modulo n. Additionally, this method has the advantage of flexibility, in the sense that it can also be applied to cyclic codes over finite fields of non prime order.

References

[1] Moisio, M.J., Exponential sums, Gauss sums and cyclic codes, Dissertation, Acta Univ.Oul. A 306, 1998, pp. 33.

[2] Feng, K. & Luo J., Weight distribution of some reducible cyclic codes, Finite Fields and Their Applications, Vol. 14, No. 2, 2008, pp. 390-409.

[3] Lidl, R. & Niederreiter, H., Finite Fields, Cambridge Univ. Press, Cambridge, 1983, pp. 755.

[4] MacWilliams, F.J. & Sloane, N.J.A., The Theory of Error-Correcting Codes, Amsterdam. North-Holland, The Netherlands, 1977, pp. 762.

[5] Vega, G., Two-weight cyclic codes constructed as the direct sum of two one-weight cyclic codes, Finite Fields and Their Applications, Vol. 14, No. 3, 2008, pp. 785-797.

[6] Vega, G., Determining the Number of One-weight Cyclic Codes when Length and Dimension are Given, International Workshop on the Arithmetic of Finite Fields 2007, Lecture Notes in Computer Science, vol. 4547, 2007, pp. 284-293.

Authors´ Biographies

Gerardo VEGA-HERNÁNDEZ

Dr. Vega holds Level 2 in the National System of Researchers (SNI-SEP), Mexico (DGTIC-UNAM). Also, he is a professor at Doctoral level, at PCIC-UNAM. His research fields are cryptography and coding theory.

Carlos Alberto VÁZQUEZ FERNÁNDEZ

He received the M.Sc. degree from the PCIC-UNAM, Mexico in 2009. Currently, Mr. Vazquez is pursuing his doctoral studies, in the above institution, in the research field of coding theory.