Determining the Complete Weight Distributions of Some Families of Cyclic Codes

Gerardo Vega and Félix Hernández

July 1, 2024

Determining the complete weight distributions of some families of cyclic codes*

Gerardo Vega[1[0000−0002−4957−6575]] and Félix Hernández[2[0000−0002−4791−485X]]

[1] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, MEXICO
gerardov@unam.mx

[2] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, MEXICO
felixhdz@ciencias.unam.mx

Abstract. Obtaining the complete weight distributions for nonbinary codes is an even harder problem than obtaining their Hamming weight distributions. In fact, obtaining these distributions is a problem that usually involves the evaluation of sophisticated exponential sums, which leaves this problem open for most of the linear codes. In this work we present a method that uses the known complete weight distribution of a given cyclic code, to determine the complete weight distributions of other cyclic codes. In addition we also obtain the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes, and use these distributions and the method, in order to determine the complete weight distributions of infinite families of cyclic codes. As an example, and as a particular instance of our results, we determine in a simple way the complete weight distribution for one of the two families of reducible cyclic codes studied by Bae, Li and Yue [Discrete Mathematics, 338 (2015) 2275–2287].

Keywords: Complete weight enumerator · Weight distribution · One- and two-weight irreducible cyclic codes · Cyclic codes · Gauss sums.

1 Introduction

The complete weight distribution of a code enumerates the codewords by the number of symbols of each kind contained in each codeword. Therefore, the complete weight distribution of a code contains much more information than the Hamming weight distribution. In fact, the complete weight distribution has a wide range of applications in many research fields as the information it contains is of vital use in practical applications. For example, as pointed out in [2] the complete weight distribution of Reed-Solomon codes could be helpful in soft decision decoding. As another example, the complete weight distribution is useful in the computation of the Walsh transform of monomial functions over

* This manuscript is partially supported by PAPIIT-UNAM IN107423. The second author has also received research support from CONAHCyT, México.

finite fields [6]. Unfortunately, determining the complete weight distribution is an even harder problem than obtaining the Hamming weight distribution. As a consequence, the complete weight distribution is unknown for most codes.

For this reason, determining the complete weight distributions of either linear codes or cyclic codes over finite fields has received a great deal of attention in recent years (see for example [1, 3, 10, 11, 16–19]). In this work we present a method that uses the known complete weight distribution of a given cyclic code, to determine the complete weight distribution of other cyclic codes. In addition we also obtain the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes, and use these distributions and the method, in order to determine the complete weight distribution of infinite families of cyclic codes. As an example, and as a particular instance of our results, we determine in a simple way the complete weight distribution for one of the two families of reducible cyclic codes studied in [1]. As another example we also determine the complete weight distributions for another family of cyclic codes which, as we shall see later, can be obtained in terms of the complete weight distribution of the subclass of optimal three-weight cyclic codes recently reported in [15].

This work is organized as follows: In Section 2 we establish the notation, give some definitions, and recall some known results. Particularly, we recall a result that determines the Hamming weight distributions of all one- and two-weight semiprimitive irreducible cyclic codes. By using such result, the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes is determined in Section 3. A method for determining new complete weight distributions, in terms of known ones, is presented in Section 4. In Section 5, we use the complete weight distributions obtained in Section 3, and the method in Section 4, in order to determine the complete weight distributions of infinite families of cyclic codes. As examples, and as particular instances of our results, two of these families are presented in this section. Finally, Section 6 is devoted to conclusions.

2 Notation, definitions and known results

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

Notation. Let p, t, q, m, and Δ, denote positive integers such that p is a prime number, $q = p^t$ and $\Delta = \frac{q^m-1}{q-1}$. From now on, γ will denote a fixed primitive element of $\mathbb{F}_{q^m}$. Let u be an integer such that $u|(q^m-1)$. For $i = 0, 1, \cdots, u-1$, we define $\mathcal{C}_i^{(u,q^m)} := \gamma^i \langle \gamma^u \rangle$, where $\langle \gamma^u \rangle$ denotes the subgroup of $\mathbb{F}_{q^m}^*$ generated by γ^u. The cosets $\mathcal{C}_i^{(u,q^m)}$ are called the *cyclotomic classes* of order u in $\mathbb{F}_{q^m}$. For an integer u, such that $\gcd(p, u) = 1$, p is said to be *semiprimitive modulo* u if there exists a positive integer d such that $u|(p^d + 1)$. We will denote by "Tr", the *absolute trace mapping* from either $\mathbb{F}_{q^m}$ or $\mathbb{F}_q$ to the prime field $\mathbb{F}_p$, and by "$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$" the *trace mapping* from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Let $s \in \mathbb{F}_q$, and let $V = (v_0, v_1, \cdots, v_{n-1})$ be a vector of length n over $\mathbb{F}_q$. We define *the number* *of occurrences of the symbol s in V*, $\mathscr{N}(s,V)$, as the number of times that s appears as an entry in the vector V. That is:

$$\mathscr{N}(s,V=(v_0,v_1,\cdots,v_{n-1})) := |\{i \mid s=v_i,\ 0 \le i < n\}| \ .$$

An $[n,l,d]$ linear code, $\mathscr{C}$, over $\mathbb{F}_q$ is an l-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d, and the vectors of $\mathscr{C}$ are called *codewords*. A code $\mathscr{C}$ is *cyclic* if it is linear and if $(c_0,c_1,\ldots,c_{n-1}) \in \mathscr{C}$ implies $(c_{n-1},c_0,\ldots,c_{n-2}) \in \mathscr{C}$. A cyclic code is irreducible (reducible) if its *parity-check polynomial* (see for example [13, p. 194]) is irreducible (reducible). Let A_i be the number of codewords with Hamming weight i in $\mathscr{C}$ (recall that the *Hamming weight* of a codeword $\mathbf{c}$ is the number of nonzero coordinates in $\mathbf{c}$). Then, the sequence 1, A_1, $\ldots$, A_n is called the *Hamming weight distribution* of the linear code $\mathscr{C}$, and the polynomial $1+A_1T+\ldots+A_nT^n$ is called the *Hamming weight enumerator* of $\mathscr{C}$. If $\sharp\{1 \le i \le n : A_i \neq 0\} = M$, then $\mathscr{C}$ is called an *M-weight* code.

In a similar way let $\mathscr{C}$ be a code of length n over $\mathbb{F}_q$. Denote the q elements of $\mathbb{F}_q$ by $u_0=0$, $u_1,\cdots,u_{q-1}$ in some fixed order. By denoting $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, we define the *complete weight* of a vector $\mathbf{v}=(v_0,v_1,\cdots,v_{n-1}) \in \mathbb{F}_q^n$, as the vector $w_{\rm cplt}(\mathbf{v}) := (f_1,f_2,\cdots,f_{q-1}) \in \mathbb{N}_0^{q-1}$, where f_l $(1 \le l < q)$ is the number of components v_j $(0 \le j < n)$ of $\mathbf{v}$ that are equal to u_l. In addition, for a vector $\boldsymbol{f}=(f_1,f_2,\cdots,f_{q-1}) \in \mathbb{N}_0^{q-1}$ we denote by $Z^{\boldsymbol{f}}$ the monomial in the $q-1$ variables $(z_1,z_2,\cdots,z_{q-1})$ given by

$$Z^{\boldsymbol{f}} := z_1^{f_1} z_2^{f_2} \cdots z_{q-1}^{f_{q-1}} \ ,$$

Now, for a linear code $\mathscr{C}$ of length n over $\mathbb{F}_q$, we define the *set of complete nonzero weights* of $\mathscr{C}$, $W_{\mathscr{C}}$, by the set:

$$W_{\mathscr{C}} := \{w_{\rm cplt}(\mathbf{c}) \mid \mathbf{c} \text{ is a nonzero codeword in } \mathscr{C}\} \ ,$$

and for each complete nonzero weight $\boldsymbol{w} \in W_{\mathscr{C}}$, we define its frequency, $A_{\boldsymbol{w}}$, as:

$$A_{\boldsymbol{w}} := \sharp\{\ \mathbf{c} \in \mathscr{C} \mid w_{\rm cplt}(\mathbf{c}) = \boldsymbol{w}\ \} \ .$$

The sequence $1, \{A_{\boldsymbol{w}}\}_{\boldsymbol{w} \in W_{\mathscr{C}}}$ is called the *complete weight distribution* of the linear code $\mathscr{C}$, whereas the polynomial

$$\mathrm{CWE}_{\mathscr{C}}(Z) := 1 + \sum_{\boldsymbol{w} \in W_{\mathscr{C}}} A_{\boldsymbol{w}}\, Z^{\boldsymbol{w}} \ , \tag{1}$$

is called its *complete weight enumerator*.

Remark 1. Let n be as before, and let $f_0 : \mathbb{N}_0^{q-1} \to \mathbb{N}_0$ be the function given by

$$f_0(f_1,f_2,\cdots,f_{q-1}) = n - \sum_{i=1}^{q-1} f_i \ .$$

Thus, it is important to observe that a quite common definition for the complete weight enumerator (see for example [13, p. 141]) is:

$$\mathrm{CWE}_{\mathscr{C}}(Z) := z_0^n + \sum_{\boldsymbol{w} \in W_{\mathscr{C}}} A_{\boldsymbol{w}}\, z_0^{f_0(\boldsymbol{w})} Z^{\boldsymbol{w}} \ .$$

For linear codes these two definitions are equivalent and, for the convenience of this work, we are going to use (1). In addition, observe also that (1) coincides with the Hamming weight enumerator when $q = 2$ and contains much more information if $q > 2$.

The following gives an explicit description of an irreducible cyclic code of length n and dimension $\mathrm{ord}_n(q)$ (the order of q modulo n; the smallest integer $m > 0$ for which $q^m \equiv 1 \pmod{n}$) over $\mathbb{F}_q$.

Definition 1. *Let n, N and N' be integers such that $N = \gcd(q^m - 1, N')$ and $nN = q^m - 1$. Then the set*

$$\mathcal{I}_{N'} := \{\mathbf{c}(a) \mid a \in \mathbb{F}_{q^m}\} \ ,$$

where

$$\mathbf{c}(a) := (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{N'i}))_{i=0}^{n-1} \ ,$$

is an irreducible cyclic code *of length n and dimension* $\mathrm{ord}_n(q)$ *over* $\mathbb{F}_q$.

Remark 2. Note that $\mathcal{I}_N$ and $\mathcal{I}_{N'}$ are in general two different irreducible cyclic codes, however they are equivalent in the sense that both share the same length $n = \frac{q^m-1}{N}$, the same dimension $\mathrm{ord}_n(q)$, and the same Hamming and complete weight distribution.

Main assumption. From now on, we use n and N as integers in such a way that $nN = q^m - 1$, assuming that $m = \mathrm{ord}_n(q)$. Under these circumstances, note that if $h_N(x) \in \mathbb{F}_q[x]$ is the *minimal polynomial* of γ^{-N} (see for example [13, p. 99]), then, due to Delsarte's Theorem [5], $h_N(x)$ is the parity-check polynomial of an irreducible cyclic code of length n and dimension m over $\mathbb{F}_q$.

The *canonical additive character* of $\mathbb{F}_q$ is defined as follows:

$$\chi(x) := e^{2\pi\sqrt{-1}\,\mathrm{Tr}(x)/p} \ , \qquad \text{for all } x \in \mathbb{F}_q \ .$$

Let $a \in \mathbb{F}_q$, then the orthogonality relation for χ is

$$\sum_{x \in \mathbb{F}_q} \chi(xa) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

This property plays an important role in numerous applications of finite fields. Among them, this property is useful for determining the number of zero entries in a given vector; for example, if $\mathbf{v} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, then

$$\mathscr{N}(0, \mathbf{v}) = \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q} \chi(y a_i) \ . \tag{2}$$

If $\langle \lambda \rangle = \mathbb{F}_q^*$, then any *multiplicative character* of $\mathbb{F}_q$ is defined by

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

If q is odd, an important multiplicative character of $\mathbb{F}_q$ is the so-called *quadratic character* which is denoted by η and defined by: $\eta(x) = 1$ if x is the square of an element of $\mathbb{F}_q^*$ and $\eta(x) = -1$ otherwise.

Let ψ be a multiplicative and χ an additive character of a finite field F. Then the *Gaussian sum*, $G_F(\psi, \chi)$, of ψ and χ over the finite field F is defined by

$$G_F(\psi, \chi) := \sum_{x \in F^*} \psi(x)\chi(x) \ .$$

Determining the value of a Gaussian sum is, in general, a difficult task. However, for the canonical additive character and the quadratic character of a finite field, we have the following result:

Theorem 1. *[12, Theorem 5.15, p. 199] With our notation, let η be the quadratic character of $\mathbb{F}_q$ and let χ be the canonical additive character of $\mathbb{F}_q$. Assume that $q = p^t$ is odd. Then*

$$G_{\mathbb{F}_q}(\eta, \chi) = \begin{cases} (-1)^{t-1} q^{1/2} & \textit{if } p \equiv 1 \pmod 4 \ , \\ (-1)^{t-1}(\sqrt{-1})^t q^{1/2} & \textit{if } p \equiv 3 \pmod 4 \ . \end{cases}$$

The following known result gives a full description for all one-weight and semiprimitive two-weight irreducible cyclic codes over any finite field.

Theorem 2. *[14, Theorem 2] Let n, N, and $\mathcal{I}_N$ be as in Definition 1. Fix $u = \gcd(\varDelta, N)$. Assume that $u = 1$ or p is semiprimitive modulo u. Let d be the smallest positive integer such that $u|(p^d + 1)$ and let $s = 1$ if $u = 1$ and $s = (mt)/(2d)$ if $u > 1$. Let $\mathbf{c}(a) \in \mathcal{I}_N$ and fix*

$$W_A = \frac{nq^{m/2-1}}{\varDelta}(q^{m/2} - (-1)^{s-1}(u-1)) \ , \quad W_B = \frac{nq^{m/2-1}}{\varDelta}(q^{m/2} - (-1)^s) \ ,$$

and

$$\delta := \begin{cases} 0 & \begin{array}{l} \textit{if } u = 1; \textit{ or } p = 2; \textit{ or } p > 2 \textit{ and } 2|s; \\ \textit{or } p > 2,\ 2 \nmid s, \textit{ and } 2|\frac{p^d+1}{u} \end{array} \\ \frac{u}{2} & \textit{if } p > 2,\ 2 \nmid s \textit{ and } 2 \nmid \frac{p^d+1}{u} \ . \end{cases} ,$$

Then,

$$w_H(\mathbf{c}(a)) = \begin{cases} 0 & \textit{if } a = 0 \ , \\ W_A & \textit{if } a \in \mathcal{C}_\delta^{(u,q^m)} \ , \\ W_B & \textit{if } a \in \mathbb{F}_{q^m}^* \setminus \mathcal{C}_\delta^{(u,q^m)} \end{cases} , \tag{3}$$

where $w_H(\cdot)$ *stands for the usual Hamming weight function. Therefore, since* $|\mathcal{C}_\delta^{(u,q^m)}| = \frac{q^m-1}{u}$, $\mathcal{I}_N$ *is either a one-weight* ($u=1$) *or a two-weight* ($u>1$) $[n,m]$ *irreducible cyclic code whose Hamming weight enumerator is*

$$1+\frac{q^m-1}{u}T^{W_A}+\frac{(q^m-1)(u-1)}{u}T^{W_B} \ . \tag{4}$$

Some desirable properties of a linear code are that it is optimal and that it has few nonzero weights (see for example [4]). The complete weight enumerator of a subclass of optimal three-weight cyclic codes was recently presented. We now recall such result by means of the following:

Theorem 3. *[15, Theorem 1] Let* e_2 *and* e_3 *be integers. If* $\gcd(e_3,q^2-1)=1$ *and* $e_3 \equiv e_2 \pmod{q-1}$*, then* $h(x) := h_{(q+1)e_2}(x)h_{e_3}(x)$ *is the parity-check polynomial of an optimal three-weight* $[q^2-1,3,q(q-1)-1]$ *cyclic code,* $\mathscr{C}$*, whose complete weight enumerator,* $\mathrm{CWE}_{\mathscr{C}}(Z)$*, is*

$$\mathrm{CWE}_{\mathscr{C}}(Z)=1+(q-1)\prod_{i=1}^{q-1} z_i^{q+1}+(q^2-1)\left(\prod_{i=1}^{q-1} z_i^{q}+\sum_{j=1}^{q-1} z_j \prod_{i=1, i\neq j}^{q-1} z_i^{q+1}\right) .$$

3 Some preliminary results

Through the following result, we determine the complete weight distribution for a particular kind of one- or two-weight irreducible cyclic codes in Theorem 2.

Proposition 1. *Consider the same notation and assumption as in Theorem 2. In addition, assume also that* N *is a proper divisor of* Δ*. Then* $\mathcal{I}_N$ *is either a one- or two-weight irreducible cyclic code whose complete weight enumerator is*

$$\mathrm{CWE}_{\mathcal{I}_N}(Z)=1+\frac{q^m-1}{N}\prod_{i=1}^{q-1} z_i^{\epsilon_1}+\frac{(q^m-1)(N-1)}{N}\prod_{i=1}^{q-1} z_i^{\epsilon_2} \ , \tag{5}$$

where

$$\epsilon_1 := \frac{W_A}{q-1} \quad \textit{and} \quad \epsilon_2 := \frac{W_B}{q-1} \ .$$

Proof. In the light of Theorem 2, it is sufficient to determine the complete weight enumerator of $\mathcal{I}_N$. Since $u=\gcd(\Delta,N)$ and $N|\Delta$, $u=N$ and $n=\frac{q^m-1}{u}$. Let $\mathbf{c}(a)\in\mathcal{I}_N$, $\tau=\frac{\Delta}{u}$ and consider the $\frac{n}{\tau}=q-1$ vectors, V_j, given by:

$$V_j := (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{u(\tau j+i)}))_{i=0}^{\tau-1}, \text{ for } j=0,1,\cdots,q-2 \ .$$

Thus, note that $\mathbf{c}(a)=V_0|V_1|\cdots|V_{q-2}$, where the operator "|" stands for the vector concatenation. On the other hand, recall that $\langle\gamma^\Delta\rangle=\mathbb{F}_q^*$ and note that the length of the vector V_j is $\tau=\frac{\Delta}{u}$. Therefore,

$$V_j = (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{\Delta j+ui}))_{i=0}^{\tau-1} = \gamma^{\Delta j}(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{ui}))_{i=0}^{\tau-1} = \gamma^{\Delta j}V_0 \ ,$$

for $j = 0, 1, \cdots, q-2$. This means that, if $x := \mathscr{N}(1, \mathbf{c}(a))$, then $\mathscr{N}(s, \mathbf{c}(a)) = x$ for all $s \in \mathbb{F}_q^*$. In consequence, the result now follows from (3), (4), and the fact that $|\mathbb{F}_q^*| = q-1$. □

Remark 3. In the previous proposition if q is odd and $N = 2$, then, without loss of generality, $\epsilon_1 = \frac{q^{m-1}+q^{m/2-1}}{2}$ and $\epsilon_2 = \frac{q^{m-1}-q^{m/2-1}}{2}$, and note that $\epsilon_1 + \epsilon_2 = q^{m-1}$.

When q and m are odd integers, we can also determine the complete weight distribution for some of the one-weight irreducible cyclic codes in Theorem 2.

Proposition 2. *With our current notation, suppose that q and m are odd. Let N be an integer such that $\gcd(N, q^m-1) = 2$ and let $\mathcal{I}_N$ be as in Definition 1. Let $\lambda = \gamma^{\Delta}$ and fix the elements of $\mathbb{F}_q$ as $u_0 = 0$, $u_i = \lambda^{i-2\lfloor \frac{i}{2} \rfloor}\lambda^{2\lfloor \frac{i}{2} \rfloor}$, for $i = 1, 2, \cdots, q-1$ (observe that $u_{q-1} = 1$). Let $\mathcal{O}$ be the subset of odd integers in $\{1, 2, \cdots, q-1\}$, that is $\mathcal{O} := \{1, 3, \cdots, q-2\}$. Then $\mathcal{I}_N$ is a $[\frac{q^m-1}{2}, m, \frac{q^{m-1}(q-1)}{2}]$ one-weight irreducible cyclic code whose complete weight enumerator is*

$$\mathrm{CWE}_{\mathcal{I}_N}(Z) = 1 + \frac{q^m-1}{2}\left(\prod_{i \in \mathcal{O}} z_i^{\varepsilon_1} z_{i+1}^{\varepsilon_2} + \prod_{i \in \mathcal{O}} z_i^{\varepsilon_2} z_{i+1}^{\varepsilon_1}\right) \ , \tag{6}$$

where

$$\varepsilon_1 := \frac{q^{m-1}+q^{\frac{m-1}{2}}}{2} \quad \text{and} \quad \varepsilon_2 := \frac{q^{m-1}-q^{\frac{m-1}{2}}}{2} \ .$$

Proof. Due to Remark 2 we can assume, without loss of generality, that $N = 2$. By Theorem 2, and since m is odd, $\mathcal{I}_N$ is a $[\frac{q^m-1}{2}, m, \frac{q^{m-1}(q-1)}{2}]$ one-weight irreducible cyclic code whose weight enumerator is $1 + (q^m-1)T^{\frac{q^{m-1}(q-1)}{2}}$. We now determine the complete weight enumerator for $\mathcal{I}_N$. Let $c \in \mathbb{F}_q^*$ and $a, c' \in \mathbb{F}_{q^m}^*$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c') = c$. Then

$$\begin{aligned}\mathscr{N}(c, \mathbf{c}(a)) &= \sharp\{0 \le i < \frac{q^m-1}{2} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{2i}) - c = 0\} \ ,\\ &= \sharp\{0 \le i < q^m-1 \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{2i} - c') = 0\}/2 \ .\end{aligned}$$

If χ' and χ are the canonical additive characters of $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$, respectively, then, due to (2) and since $\chi' = \chi \circ \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, we have

$$\begin{aligned}2\mathscr{N}(c, \mathbf{c}(a)) &= \sum_{i=0}^{q^m-2} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \chi(y\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a\gamma^{2i} - c')) \ ,\\ &= \frac{q^m-1}{q} + \frac{1}{q}\sum_{y \in \mathbb{F}_q^*}\sum_{x \in \mathbb{F}_{q^m}^*} \chi'(y(ax^2 - c')) \ .\end{aligned}$$

Therefore, by [12, Theorem 5.30, p. 217], we have

$$2\mathscr{N}(c,\mathbf{c}(a)) = \frac{q^m-1}{q} + \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}(\chi'(-yc')\eta(ya)G_{\mathbb{F}_{q^m}}(\eta,\chi') - \chi'(-yc'))\ ,$$

where η is the quadratic character of $\mathbb{F}_{q^m}$. Now because m is odd, η is also the quadratic character of $\mathbb{F}_q$. Thus, since $\chi'(-yc') = \chi(-yc)$ and $c \neq 0$,

$$\begin{aligned}
2\mathscr{N}(c,\mathbf{c}(a)) &= \frac{q^m-1}{q} + \frac{1}{q}(G_{\mathbb{F}_{q^m}}(\eta,\chi')\sum_{y\in\mathbb{F}_q^*}\chi(-yc)\eta(ya) - \sum_{y\in\mathbb{F}_q^*}\chi(-yc))\ ,\\
&= q^{m-1} + \frac{1}{q}\eta(a)G_{\mathbb{F}_{q^m}}(\eta,\chi')\sum_{y\in\mathbb{F}_q^*}\chi(-yc)\eta(y)\ ,\\
&= q^{m-1} + \frac{1}{q}\eta(a)\eta(-c)G_{\mathbb{F}_{q^m}}(\eta,\chi')\sum_{y\in\mathbb{F}_q^*}\chi(-yc)\eta(-yc)\ ,\\
&= q^{m-1} + \frac{1}{q}\eta(a)\eta(-c)G_{\mathbb{F}_{q^m}}(\eta,\chi')G_{\mathbb{F}_q}(\eta,\chi)\ ,
\end{aligned}$$

where the second equality holds because $\sum_{y\in\mathbb{F}_q^*}\chi(-yc) = -1$. Let $l=1$ if $p\equiv 3 \pmod 4$ and $\frac{t(m+1)}{2}$ is odd, and $l=0$ otherwise. Then, by Theorem 1, we have

$$\begin{aligned}
2\mathscr{N}(c,\mathbf{c}(a)) &= q^{m-1} + \frac{1}{q}\eta(a)\eta(-c)(-1)^{t-1}q^{1/2}(-1)^{mt-1}(-1)^l q^{m/2}\ ,\\
&= q^{m-1} + \eta(-a)\eta(c)(-1)^l q^{\frac{m-1}{2}}\ ,
\end{aligned}$$

therefore,

$$\mathscr{N}(c,\mathbf{c}(a)) = \begin{cases} \varepsilon_1 & \text{if } \eta(-a)(-1)^l = \eta(c)\ ,\\ \varepsilon_2 & \text{if } \eta(-a)(-1)^l \neq \eta(c)\ ,\end{cases}$$

and observe that if $\eta(c)=1$ ($\eta(c)=-1$) then there must exists an even (odd) integer $1\le i\le q-1$ such that $u_i = c$. Finally, since $\sharp\{a\in\mathbb{F}_{q^m}^* \mid \eta(-a)(-1)^l = 1\} = \frac{q^m-1}{2}$, both values ε_1 and ε_2 occur $\frac{q^m-1}{2}$ times. □

The Multinomial Theorem (see for example [8]) is a generalization of the Binomial Theorem, and therefore, it describes how to expand the power of a sum of more than two terms. We now recall such result by means of the following:

Theorem 4. *For a positive integer k and a non-negative integer r,*

$$(y_1+y_2+\cdots+y_k)^r = \sum_{e_1+e_2+\cdots+e_k=r}\binom{r}{e_1,e_2,\ldots,e_k}\prod_{j=1}^{k}y_j^{e_j}\ ,$$

where $e_1, \cdots, e_k$ *are non-negative integers, and*

$$\binom{r}{e_1, e_2, ..., e_k} := \frac{r!}{e_1! e_2! \cdots e_k!} .$$

As an almost direct consequence of the previous theorem we have:

Lemma 1. *Let* k *and* r *be as before. Then*

$$(1 + y_1 + y_2 + \cdots + y_k)^r = 1 + \sum_{i=1}^{r} \sum_{e_1+e_2+\cdots+e_k=i} \binom{r}{e_1, e_2, ..., e_k, r-i} \prod_{j=1}^{k} y_j^{e_j} .$$

Proof. Clearly, $(1+y)^r = 1 + \sum_{i=1}^r \binom{r}{i} y^i$, and if $y = y_1 + y_2 + \cdots + y_k$, then, by the previous theorem, we have

$$(1+y)^r = 1 + \sum_{i=1}^{r} \binom{r}{i} \sum_{e_1+e_2+\cdots+e_k=i} \binom{i}{e_1, e_2, ..., e_k} \prod_{j=1}^{k} y_j^{e_j} .$$

The result now follows from the fact that

$$\binom{r}{i} \binom{i}{e_1, e_2, ..., e_k} = \binom{r}{e_1, e_2, ..., e_k, r-i} .$$

□

4 Determining new complete weight distributions in terms of known ones

Given a cyclic code, $\mathscr{C}$, whose Hamming weight enumerator is known, it is possible to determine the Hamming weight enumerator of another cyclic code, $\mathscr{C}'$, in terms of a power of the Hamming weight enumerator of $\mathscr{C}$. A first version of this result was presented in [7,9] (see particularly Lemma 4.5 and Theorem 5.1 in [7]). An equivalent result for the complete weight enumerator is as follows:

Theorem 5. *For suitable integers* n, m *and* d, *let* $\mathscr{C}$ *be an* $[n, m, d]$ *cyclic code, over* $\mathbb{F}_q$, *with parity-check polynomial* $h(x)$, *and whose complete weight enumerator is* $\mathrm{CWE}_{\mathscr{C}}(Z)$. *Let also* r *be any positive integer, such that* $\gcd(q, r) = 1$. *Then, the polynomial* $h(x^r)$ *is the parity-check polynomial of an* $[nr, mr, d]$ *cyclic code,* $\mathscr{C}'$, *whose complete weight enumerator,* $\mathrm{CWE}_{\mathscr{C}'}(Z)$, *is* $\mathrm{CWE}_{\mathscr{C}'}(Z) = \mathrm{CWE}_{\mathscr{C}}(Z)^r$.

Proof. Clearly, $h(x^r) | (x^{nr} - 1)$ and $\deg(h(x)) = m$. Therefore, since $\gcd(q, nr) = 1$, we have that $h'(x) := h(x^r)$ is the parity-check polynomial of an $[nr, mr]$ cyclic code, $\mathscr{C}'$, over $\mathbb{F}_q$. Suppose that $W_{\mathscr{C}} = \{\boldsymbol{w}_1, \boldsymbol{w}_2, \cdots, \boldsymbol{w}_k\}$ is the set of complete nonzero weights of $\mathscr{C}$, and, for $1 \le j \le k$, let $A_{\boldsymbol{w}_j}$ be the number of codewords in $\mathscr{C}$ whose complete weight is equal to $\boldsymbol{w}_j$. In a similar way, suppose that

$W_{\mathscr{C}'} = \{\boldsymbol{w}'_1, \boldsymbol{w}'_2, \cdots, \boldsymbol{w}'_{k'}\}$ is the set of complete nonzero weights of $\mathscr{C}'$, and, for $1 \leq j \leq k'$, let $A'_{\boldsymbol{w}'_j}$ be the number of codewords in $\mathscr{C}'$ whose complete weight is equal to $\boldsymbol{w}'_j$. Then $\mathrm{CWE}_{\mathscr{C}}(Z) = 1 + \sum_{j=1}^{k} A_{\boldsymbol{w}_j} z^{\boldsymbol{w}_j}$ and $\mathrm{CWE}_{\mathscr{C}'}(Z) = 1+\sum_{j=1}^{k'} A'_{\boldsymbol{w}'_j} z^{\boldsymbol{w}'_j}$ are the complete weight enumerators of $\mathscr{C}$ and $\mathscr{C}'$, respectively.

Through the correspondence

$$\pi : \mathbb{F}_q^{nr} \to \mathcal{R}_{nr} := \mathbb{F}_q[x]/(x^{nr} - 1) \;,$$

with

$$\pi(a_0, a_1, ..., a_{nr-1}) := a_0 + a_1 x + \cdots + a_{nr-1}x^{nr-1} \;,$$

we can view the cyclic code $\mathscr{C}'$ as an ideal in the ring $\mathcal{R}_{nr}$, whose generator polynomial is $g'(x) = (x^{nr} - 1)/h'(x)$. By considering this, let us define, for $i = 1, \cdots, r$,

$$o_i := \{\pi^{-1}(x^{i-1}g'(x)), \pi^{-1}(x^{i-1+r}g'(x)), \cdots, \pi^{-1}(x^{i-1+(m-1)r}g'(x))\} \subset \mathbb{F}_q^{nr} \;.$$

Observe that if $\mathcal{S}_i \subset \mathbb{F}_q^{nr}$ $(i = 1, \cdots, r)$ is the linear span of o_i (that is $\mathcal{S}_i = \langle o_i \rangle$), then we have for sure the following three facts:

(i) $\mathscr{C}' = \displaystyle\bigoplus_{i=1}^{r} \mathcal{S}_i$ (where $\bigoplus$ denotes direct sum of subspaces), and $\mathcal{S}_i \cap \mathcal{S}_l = \{\mathbf{0}\}$ (the zero codeword in $\mathscr{C}'$) if and only if $1 \leq i \neq l \leq r$. That is, any subspace $\mathcal{S}_i$ $(i = 1, \cdots, r)$ is independent of all other subspaces $\mathcal{S}_l$ in the sense that there does not exist any nonzero codeword in $\mathcal{S}_i$ which is a linear combination of codewords in the other subspaces. Therefore, for each $c' \in \mathscr{C}'$ there must exist unique codewords $c_1, \cdots, c_r$, with $c_i \in \mathcal{S}_i$ and $1 \leq i \leq r$, such that $c' = c_1 + \cdots + c_r$.

(ii) For each pair of codewords a and b, such that $a \in \mathcal{S}_i$ and $b \in \mathcal{S}_l$, with $1 \leq i \neq l \leq r$, we have that $w_{\mathrm{cplt}}(a + b) = w_{\mathrm{cplt}}(a) + w_{\mathrm{cplt}}(b)$.

(iii) Each $\mathcal{S}_i$ is an $[nr, m, d]$ linear code (not necessarily cyclic), whose complete weight enumerator is given by $\mathrm{CWE}_{\mathscr{C}}(Z)$.

With the idea of clarifying the previous facts we briefly interrupt this proof in order to present the following:

Example 1. Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, with $\alpha^2 + \alpha + 1 = 0$, and we denote the elements of $\mathbb{F}_4$ as: $u_0 = 0$, $u_1 = 1$, $u_2 = \alpha$ and $u_3 = \alpha + 1$. Let $n = 5$, $h(x) = 1 + \alpha x + x^2$, and $r = 3$. Then $g(x) := \frac{x^5-1}{h(x)} = 1 + \alpha x + \alpha x^2 + x^3$, and $g'(x) := g(x^3)$. Under these conditions, it is not difficult to see that the cyclic code $\mathscr{C}$ is a $[5, 2, 4]$ one-weight irreducible cyclic code over $\mathbb{F}_4$, whose complete weight enumerator is $\mathrm{CWE}_{\mathscr{C}}(Z) = 1 + 5z_1^2z_2^2z_3^0 + 5z_1^2z_2^0z_3^2 + 5z_1^0z_2^2z_3^2$. Therefore note that $W_{\mathscr{C}} = \{(2, 2, 0), (2, 0, 2), (0, 2, 2)\}$. The generator matrices for the cyclic codes $\mathscr{C}$ and $\mathscr{C}'$ are, respectively,

$$G = \begin{bmatrix} 1 & \alpha & \alpha & 1 & 0 \\ 0 & 1 & \alpha & \alpha & 1 \end{bmatrix} ,$$

and

$$G' = \begin{bmatrix} 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 \end{bmatrix} .$$

Therefore

$$o_1 = \left\{ \begin{matrix} (1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0), \\ (0 & 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0) \end{matrix} \right\} ,$$

$$o_2 = \left\{ \begin{matrix} (0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 0 & 0), \\ (0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0) \end{matrix} \right\} ,$$

and

$$o_3 = \left\{ \begin{matrix} (0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 0), \\ (0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha & 0 & 0 & \alpha & 0 & 0 & 1) \end{matrix} \right\} .$$

In this way, note that $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$ are $[15, 2, 4]$ linear codes (they are not cyclic), whose complete weight enumerator is $\mathrm{CWE}_{\mathscr{C}}(Z)$, and clearly $\mathscr{C}' = \mathcal{S}_1 \bigoplus \mathcal{S}_2 \bigoplus \mathcal{S}_3$ and $\mathcal{S}_i \cap \mathcal{S}_j = \{\mathbf{0}\}$, $1 \leq i \neq j \leq 3$.

Continuing with the proof, we now define $\mathcal{U} := \{\mathcal{S}_1, \cdots, \mathcal{S}_r\}$ and recall that $W_{\mathscr{C}} = \{\boldsymbol{w}_1, \boldsymbol{w}_2, \cdots, \boldsymbol{w}_k\} \subset \mathbb{N}_0^{q-1}$. Thus, as a consequence of the previous facts, note that for each codeword $c' \in \mathscr{C}'$, with $w_{\mathrm{cplt}}(c') = \boldsymbol{w}' \in W_{\mathscr{C}'}$, there must exist an integer i; k non-negative integers, $e_1, \cdots, e_k$; k disjoint subsets, $\mathcal{V}_1, \cdots, \mathcal{V}_k$, of the set $\mathcal{U}$; and k codewords, $a_1, \cdots, a_k$, of $\mathscr{C}'$, in such a way that the following conditions are met:

(1) $1 \leq i \leq r$, $i = e_1 + \cdots + e_k$ and $c' = a_1 + \cdots + a_k$.
(2) $|\mathcal{V}_j| = e_j$, $a_j \in \bigoplus_{\mathcal{S} \in \mathcal{V}_j} \mathcal{S}$ and $w_{\mathrm{cplt}}(a_j) = e_j \boldsymbol{w}_j$, for $j = 1, \cdots, k$.
(3) The complete nonzero weight $\boldsymbol{w}'$, can be expressed as $\boldsymbol{w}' = w_{\mathrm{cplt}}(a_1 + \cdots + a_k) = w_{\mathrm{cplt}}(a_1) + \cdots + w_{\mathrm{cplt}}(a_k) = e_1 \boldsymbol{w}_1 + \cdots + e_k \boldsymbol{w}_k$, where the penultimate equality holds because the subsets $\mathcal{V}_j$ are disjoint.

Then, we can summarize all the above by saying that for each $\boldsymbol{w}' \in W_{\mathscr{C}'}$, there must exist at least one $(k+1)$-tuple of non-negative integers $(i, e_1, \cdots, e_k)$, that satisfies $1 \leq i \leq r$, $i = e_1 + \cdots + e_k$ and $\boldsymbol{w}' = e_1 \boldsymbol{w}_1 + \cdots + e_k \boldsymbol{w}_k$. In consequence, if we construct, for each $\boldsymbol{w}' \in W_{\mathscr{C}'}$, the set

$$\begin{aligned}\mathcal{T}_{\boldsymbol{w}'} := \{\ \tau \mid \tau &\text{ is an } (k+1)\text{-tuple of non-negative integers of the form}\\ &(i, e_1, \cdots, e_k) \text{ that satisfies, } 1 \leq i \leq r,\ i = e_1 + \cdots + e_k \text{ and}\\ &\boldsymbol{w}' = e_1\boldsymbol{w}_1 + \cdots + e_k\boldsymbol{w}_k\ \}\ ,\end{aligned}$$

then it is clear that $|\mathcal{T}_{\boldsymbol{w}'}| \neq 0$. Now, by taking a fixed $(i, e_1, \cdots, e_k) \in \mathcal{T}_{\boldsymbol{w}'}$, we have that there are

$$\binom{r}{e_1}\binom{r-e_1}{e_2}\cdots\binom{r-(e_1+\cdots+e_{k-1})}{e_k} = \binom{r}{e_1, e_2, ..., e_k, r-i}$$

possible choices for the construction of the disjoint subsets: $\mathcal{V}_1, \cdots, \mathcal{V}_k$. But recall that all the $\mathbb{F}_q$-linear subspaces $\mathcal{S}_i$, have the same complete weight enumerator $\mathrm{CWE}_{\mathscr{C}}(Z)$. Therefore, for all these $\mathbb{F}_q$-linear subspaces $\mathcal{S}_i$, the integer value $A_{\boldsymbol{w}_j}$ (for $j = 1, \cdots, k$) is the frequency of occurrence of the complete nonzero weight $\boldsymbol{w}_j$. Consequently we have

$$A'_{\boldsymbol{w}'} = \sum_{(i,e_1,+\cdots+e_k)\in\mathcal{T}_{\boldsymbol{w}'}} \binom{r}{e_1, e_2, ..., e_k, r-i} \prod_{j=1}^{k} A_{\boldsymbol{w}_j}^{e_j}\ ,$$

but, since $\boldsymbol{w}' = e_1\boldsymbol{w}_1 + \cdots + e_k\boldsymbol{w}_k$ and $A_{\boldsymbol{w}_j}^{e_j} Z^{e_j\boldsymbol{w}_j} = (A_{\boldsymbol{w}_j} Z^{\boldsymbol{w}_j})^{e_j}$,

$$A'_{\boldsymbol{w}'} Z^{\boldsymbol{w}'} = \sum_{(i,e_1,+\cdots+e_k)\in\mathcal{T}_{\boldsymbol{w}'}} \binom{r}{e_1, e_2, ..., e_k, r-i} \prod_{j=1}^{k} (A_{\boldsymbol{w}_j} Z^{\boldsymbol{w}_j})^{e_j}\ .$$

Conversely, note that for each $(k+1)$-tuple of non-negative integers of the form $(i, e_1, \cdots, e_k)$, that satisfies $1 \leq i \leq r$ and $i = e_1 + \cdots + e_k$, there must exist a unique $\boldsymbol{w}' \in W_{\mathscr{C}'}$ such that $\boldsymbol{w}' = e_1\boldsymbol{w}_1 + \cdots + e_k\boldsymbol{w}_k$. Therefore,

$$\mathrm{CWE}_{\mathscr{C}'}(Z) = 1 + \sum_{i=1}^{r} \sum_{e_1+e_2+\cdots+e_k=i} \binom{r}{e_1, e_2, ..., e_k, r-i} \prod_{j=1}^{k} (A_{\boldsymbol{w}_j} Z^{\boldsymbol{w}_j})^{e_j}\ ,$$

and, by Lemma 1, we conclude that $\mathrm{CWE}_{\mathscr{C}'}(Z) = \mathrm{CWE}_{\mathscr{C}}(Z)^r$. Finally, both $\mathscr{C}$ and $\mathscr{C}'$ have the same minimum Hamming distance, d, because $W_{\mathscr{C}} \subseteq W_{\mathscr{C}'}$. $\square$

Example 2. Let $\mathscr{C}$ and $\mathscr{C}'$ be as in Example 1. Thus, due to Theorem 5, $\mathscr{C}'$ is a $[15, 6, 4]$ cyclic code over $\mathbb{F}_4$, whose complete weight enumerator is:

$$\begin{aligned}\mathrm{CWE}_{\mathscr{C}'}(Z) = \mathrm{CWE}_{\mathscr{C}}(Z)^3 &= (1 + 5z_1^2z_2^2z_3^0 + 5z_1^2z_2^0z_3^2 + 5z_1^0z_2^2z_3^2)^3\\ &= 1 + 15(z_1^2z_2^2z_3^0 + z_1^2z_2^0z_3^2 + z_1^0z_2^2z_3^2) + 75(z_1^4z_2^4z_3^0 + z_1^4z_2^0z_3^4 + z_1^0z_2^4z_3^4)\\ &\quad +125(z_1^6z_2^6z_3^0 + z_1^6z_2^0z_3^6 + z_1^0z_2^6z_3^6) + 150(z_1^2z_2^2z_3^4 + z_1^2z_2^4z_3^2 + z_1^4z_2^2z_3^2)\\ &\quad +375(z_1^2z_2^4z_3^6 + z_1^2z_2^6z_3^4 + z_1^4z_2^2z_3^6 + z_1^4z_2^6z_3^2 + z_1^6z_2^2z_3^4 + z_1^6z_2^4z_3^2)\\ &\quad +750z_1^4z_2^4z_3^4\ .\end{aligned}$$

By using directly the cyclic code $\mathscr{C}'$, the previous numerical result was verified by a computer program.

5 Complete weight distribution of families of cyclic codes

In order to observe the usefulness of Theorem 5, we now determine in a simple way the complete weight distribution for one of the two families of reducible cyclic codes studied in [1].

Theorem 6. *[1, Theorem 3.1] With the notation of Propositions 1 and 2, suppose that q is odd and let $\mathscr{C}'$ be the $[q^m-1, 2m]$ reducible cyclic code with parity-check polynomial $h'(x) := h_1(x)h_{\frac{q^m-1}{2}+1}(x)$. Then the complete weight enumerator of $\mathscr{C}'$ is*

$$\begin{aligned}
\mathrm{CWE}_{\mathscr{C}'}(Z) &= \left[1+\frac{q^m-1}{2}\left(\prod_{i=1}^{q-1} z_i^{\epsilon_1} + \prod_{i=1}^{q-1} z_i^{\epsilon_2}\right)\right]^2 \\
&= 1+(q^m-1)\left(\prod_{i=1}^{q-1} z_i^{\epsilon_1} + \prod_{i=1}^{q-1} z_i^{\epsilon_2}\right) + \frac{(q^m-1)^2}{2}\prod_{i=1}^{q-1} z_i^{q^{m-1}} \\
&\quad + \frac{(q^m-1)^2}{4}\left(\prod_{i=1}^{q-1} z_i^{2\epsilon_1} + \prod_{i=1}^{q-1} z_i^{2\epsilon_2}\right) ,
\end{aligned} \tag{7}$$

if m is even and

$$\begin{aligned}
\mathrm{CWE}_{\mathscr{C}'}(Z) &= \left[1+\frac{q^m-1}{2}\left(\prod_{i\in\mathcal{O}} z_i^{\varepsilon_1} z_{i+1}^{\varepsilon_2} + \prod_{i\in\mathcal{O}} z_i^{\varepsilon_2} z_{i+1}^{\varepsilon_1}\right)\right]^2 \\
&= 1+(q^m-1)\left(\prod_{i\in\mathcal{O}} z_i^{\varepsilon_1} z_{i+1}^{\varepsilon_2} + \prod_{i\in\mathcal{O}} z_i^{\varepsilon_2} z_{i+1}^{\varepsilon_1}\right) + \frac{(q^m-1)^2}{2}\prod_{i=1}^{q-1} z_i^{q^{m-1}} \\
&\quad + \frac{(q^m-1)^2}{4}\left(\prod_{i\in\mathcal{O}} z_i^{2\varepsilon_1} z_{i+1}^{2\varepsilon_2} + \prod_{i\in\mathcal{O}} z_i^{2\varepsilon_2} z_{i+1}^{2\varepsilon_1}\right) ,
\end{aligned} \tag{8}$$

if m is odd.

Proof. Let $h_2(x)$ be the minimal polynomial of γ^{-2}. Since q is odd, $\deg(h_2(x)) = \deg(h_1(x)) = \deg(h_{\frac{q^m-1}{2}+1}(x)) = m$. Additionally, since γ^{-2} is a root of $h_2(x)$, and because $\gamma^{-\frac{q^m-1}{2}-1} = -\gamma^{-1}$, we see that γ^{-1} and $\gamma^{-\frac{q^m-1}{2}-1}$ are both roots of $h_2(x^2)$. Thus, $h_2(x^2) = h_1(x)h_{\frac{q^m-1}{2}+1}(x)$ and, by Definition 1 and Propositions 1 and 2, $h(x) := h_2(x)$ is the parity-check polynomial of a $[\frac{q^m-1}{2}, m]$ irreducible cyclic code, $\mathcal{I}_N$, whose complete weight enumerator is given by (5) if m is even and (6) if m is odd, where $N = 2$ for these two equations. Clearly $\gcd(q, 2) = 1$, thus, by Theorem 5 and Remark 3, $\mathscr{C}'$ is a $[q^m-1, 2m]$ reducible cyclic code whose complete weight enumerator is given by (7) if m is even and by (8) if m is odd. Finally, note that (7) and (8) coincide with Tables 1 and 2 in [1], respectively. □

Example 3. (A) Let $q = 3$ and $m = 2$. Then by Theorem 6 $\epsilon_1 = 2$, $\epsilon_2 = 1$, and $h'(x) = h_1(x)h_5(x)$ is the parity-check polynomial of an $[8, 4]$ reducible cyclic code, $\mathscr{C}'$, whose complete weight enumerator is

$$\mathrm{CWE}_{\mathscr{C}'}(Z) = (1 + 4(z_1^2 z_2^2 + z_1 z_2))^2 = 1 + 32 z_1^3 z_2^3 + 16 z_1^4 z_2^4 + 24 z_1^2 z_2^2 + 8 z_1 z_2 \ ,$$

which coincides with Example 3.2(1) in [1] (take into consideration Remark 1).

(B) Let $q = 5$ and $m = 2$. Then by Theorem 6 $\epsilon_1 = 2$, $\epsilon_2 = 3$, and $h'(x) = h_1(x)h_{13}(x)$ is the parity-check polynomial of a $[24, 4]$ reducible cyclic code, $\mathscr{C}'$, whose complete weight enumerator is

$$\begin{aligned}\mathrm{CWE}_{\mathscr{C}'}(Z) &= (1 + 12(z_1^2 z_2^2 z_3^2 z_4^2 + z_1^3 z_2^3 z_3^3 z_4^3))^2 \\ &= 1 + 288 z_1^5 z_2^5 z_3^5 z_4^5 + 144(z_1^4 z_2^4 z_3^4 z_4^4 + z_1^6 z_2^6 z_3^6 z_4^6) \\ &\quad + 24(z_1^2 z_2^2 z_3^2 z_4^2 + z_1^3 z_2^3 z_3^3 z_4^3) \ ,\end{aligned}$$

which coincides with Example 3.2(2) in [1].

(C) Let $q = 3$ and $m = 3$. Then by Theorem 6 $\varepsilon_1 = 3$, $\varepsilon_2 = 6$, and $h'(x) = h_1(x)h_{14}(x)$ is the parity-check polynomial of a $[26, 6]$ reducible cyclic code, $\mathscr{C}'$, whose complete weight enumerator is

$$\begin{aligned}\mathrm{CWE}_{\mathscr{C}'}(Z) &= (1 + 13(z_1^3 z_2^6 + z_1^6 z_2^3))^2 \\ &= 1 + 338 z_1^9 z_2^9 + 169(z_1^{12} z_2^6 + z_1^6 z_2^{12}) + 26(z_1^3 z_2^6 + z_1^6 z_2^3) \ ,\end{aligned}$$

which coincides with Example 3.2(3) in [1].

(D) Let $q = 5$ and $m = 3$. Then by Theorem 6 $\varepsilon_1 = 10$, $\varepsilon_2 = 15$, and $h'(x) = h_1(x)h_{63}(x)$ is the parity-check polynomial of a $[124, 6]$ reducible cyclic code, $\mathscr{C}'$, whose complete weight enumerator is

$$\begin{aligned}\mathrm{CWE}_{\mathscr{C}'}(Z) &= (1 + 62(z_1^{10} z_2^{15} z_3^{10} z_4^{15} + z_1^{15} z_2^{10} z_3^{15} z_4^{10}))^2 \\ &= 1 + 7688 z_1^{25} z_2^{25} z_3^{25} z_4^{25} + 3844(z_1^{20} z_2^{30} z_3^{20} z_4^{30} + z_1^{30} z_2^{20} z_3^{30} z_4^{20}) \\ &\quad + 124(z_1^{10} z_2^{15} z_3^{10} z_4^{15} + z_1^{15} z_2^{10} z_3^{15} z_4^{10}) \ ,\end{aligned}$$

which coincides with Example 3.2(4) in [1] (be careful, for this last example the authors of [1] choose a different order for the elements in $\mathbb{F}_5$).

As another instance of Theorem 5, we can now determine the complete weight distributions for another family of cyclic codes which, as we shall see below, can be obtained in terms of the complete weight distribution of the subclass of optimal three-weight cyclic codes given in Theorem 3:

Theorem 7. *Consider the same notation and assumption as in Theorem 3. Let r be any positive integer, such that $\gcd(q, r) = 1$. Then $h(x^r)$ is the parity-check* *polynomial of a* $[(q^2-1)r, 3r, q(q-1)-1]$ *cyclic code,* $\mathscr{C}'$*, whose complete weight enumerator,* $\mathrm{CWE}_{\mathscr{C}'}(Z)$*, is*

$$\mathrm{CWE}_{\mathscr{C}'}(Z) = \left[1 + (q-1)\prod_{i=1}^{q-1} z_i^{q+1} + (q^2-1)\left(\prod_{i=1}^{q-1} z_i^q + \sum_{j=1}^{q-1} z_j \prod_{i=1, i\neq j}^{q-1} z_i^{q+1} \right) \right]^r .$$

Proof. Direct from Theorems 5 and 3. □

Example 4. Let $(q, e_2, e_3, r) = (4, 1, 1, 3)$. Thus, due to Theorem 3 and [15, Example 1], $h(x) = h_5(x)h_1(x)$ is the parity-check polynomial of an optimal three-weight $[15, 3, 11]$ cyclic code, $\mathscr{C}$, over $\mathbb{F}_4$, whose complete weight enumerator is $\mathrm{CWE}_{\mathscr{C}}(Z) = 1+3A+15(B+C+D+E)$, where $A = (z_1z_2z_3)^5$, $B = (z_1z_2z_3)^4$, $C = z_1z_2^5z_3^5$, $D = z_1^5z_2z_3^5$, and $E = z_1^5z_2^5z_3$. On the other hand, by Theorem 7, $h(x^3)$ is the parity-check polynomial of a $[45, 9, 11]$ cyclic code, $\mathscr{C}'$, whose complete weight enumerator, $\mathrm{CWE}_{\mathscr{C}'}(Z)$, is

$$\begin{aligned}
\mathrm{CWE}_{\mathscr{C}'}(Z) &= \mathrm{CWE}_{\mathscr{C}}(Z)^3 \\
&= 1 + 9A + 27(A^2 + A^3) + (45 + 270A + 405A^2)(B + C + D + E) \\
&\quad + (4050AB + 1350B + 10125B^2)(C + D + E) \\
&\quad + (675 + 2025A)(B^2 + C^2 + D^2 + E^2) \\
&\quad + 3375(B^3 + C^3 + D^3 + E^3) \\
&\quad + (1350 + 4050A + 20250B)(CD + CE + DE) + 20250CDE \\
&\quad + 10125(B(C^2 + D^2 + E^2) + C^2(D + E) \\
&\qquad\qquad + D^2(C + E) + E^2(C + D)) .
\end{aligned}$$

By using directly the cyclic code $\mathscr{C}'$, the previous numerical result was verified by a computer program.

6 Conclusions

In this work we determined the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes (Propositions 1 and 2). After this, a method that determines new complete weight distributions in terms of known ones was presented (Theorem 5). Then, we used such method in order to determine the complete weight distribution of infinite families of cyclic codes (Section 5). As an example of such families, the complete weight distribution for one of the two families of reducible cyclic codes studied in [1] was determined in a simple way (Theorem 6). As another example, the complete weight distribution for another family of cyclic codes was also determined which, as shown earlier, can be obtained in terms of the complete weight distribution of the subclass of optimal three-weight cyclic codes presented recently in [15] (Theorem 7).

As it is known, Theorem 2 gives us the Hamming weight distributions for all one-weight and semiprimitive two-weight irreducible cyclic codes over any finite field. On the other hand, by means of Propositions 1 and 2, the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes were determined. Thus, as a complement of this work, we believe that it would be interesting to determine the complete weight distributions of the remaining part of the family of one- and semiprimitive two-weight irreducible cyclic codes in Theorem 2.

References

1. Bae, S., Li, C., Yue, Q.: On the complete weight enumerator of some reducible cyclic codes. Discret. Math. **338**, 2275–2287 (2015)
2. Blake, I.F., Kith, K.: On the complete weight enumerator of Reed-Solomon codes. SIAM J. Discret. Math. **4**(2), 164–171 (1991)
3. Chan, C.H., Xiong, M.: On the complete weight distribution of subfield subcodes of algebraic-geometric codes. IEEE Trans. Inf. Theory **65**(11), 7079–7086 (2019)
4. Cheng, Y., Cao, X., Luo, G.: Three new constructions of optimal linear codes with few weights. Comp. Appl. Math. **42**(321) (2023)
5. Delsarte, P.: On subfield subcodes of Reed-Solomon codes. IEEE Trans. Inf. Theory **21**(5), 575–576 (1975)
6. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**, 2018–2032 (2006)
7. Helleseth, T., Kløve, T., Mykkeltveit, J.: The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)n)$. Discrete Mathematics **18**(2), 179–211 (1977)
8. Hilliker, D.L.: On the multinomial theorem. Fibonacci Quarterly **15**(1), 22–24 (1977)
9. Kløve, T.: The weight distribution for a class of irreducible cyclic codes. Discrete Mathematics **20**, 87–90 (1977)
10. Li, C., Bae, S., Ahn, J., Yang, S., Yao, Z.A.: Complete weight enumerators of some linear codes and their applications. Designs, Codes Cryptogr. **81**, 153–168 (2016)
11. Li, C., Yue, Q., Fu, F.W.: Complete weight enumerators of some cyclic codes. Designs, Codes Cryptogr. **80**, 295–315 (2015)
12. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge Univ. Press, Cambridge, U.K. (1983)
13. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland, Amsterdam, The Netherlands (1977)
14. Vega, G.: The b-symbol weight distributions of all semiprimitive irreducible cyclic codes. Des. Codes Cryptogr. **91**, 2213–2221 (2023)
15. Vega, G., Hernández, F.: The complete weight distribution of a subclass of optimal three-weight cyclic codes. Cryptogr. Commun. **15**(2), 317–330 (2023)
16. Yang, S.: Complete weight enumerators of a class of linear codes from weil sums. In IEEE Access **8**, 194631–194639 (2020)
17. Yang, S., Yao, Z.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Cryptogr. **82**, 663–674 (2017)
18. Yang, S., Yao, Z.A.: Complete weight enumerators of a class of linear codes. Discret. Math. **340**(4), 729–739 (2017)
19. Yang, S., Yao, Z.A., Zhao, C.A.: A class of three-weight linear codes and their complete weight enumerators. Cryptogr. Commun. **9**, 133–149 (2017)