J. Algebra Comb. Discrete Appl.
4(3) • 281–290

Received: 12 August 2016
Accepted: 17 April 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

A class of cyclic codes constructed via semiprimitive two-weight irreducible cyclic codes*

Research Article

Jesús E. Cuén-Ramos, Gerardo Vega

Abstract: We present a family of reducible cyclic codes constructed as a direct sum (as vector spaces) of two different semiprimitive two-weight irreducible cyclic codes. This family generalizes the class of reducible cyclic codes that was reported in the main result of [10]. Moreover, despite of what was stated therein, we show that, at least for the codes studied here, it is still possible to compute the frequencies of their weight distributions through the cyclotomic numbers in an easy way.

2010 MSC: 94B15, 11T71

Keywords: Weight distribution, Reducible cyclic codes, Semiprimitive cyclic codes, Cyclotomic numbers

1. Introduction

It is said that a cyclic code is reducible if its parity-check polynomial is factorizable in two or more irreducible factors. Each one of these irreducible factors can be seen as the parity-check polynomial of an irreducible cyclic code. Therefore, a reducible cyclic code is, basically, a direct sum (as vector spaces) of these irreducible cyclic codes. Reducible cyclic codes whose parity-check polynomials are factorizable in exactly two different irreducible factors have been extensively studied (see, for example, [10], [3], [11], [6], [5], [2], [12] and [8]). A very interesting problem regarding this kind of reducible cyclic codes is to obtain their full weight distributions. In particular, [10] employed an elaborate procedure that uses some sort of elliptic curves in order to obtain the weight distribution of a class of reducible cyclic codes. We present here a family of reducible cyclic codes constructed as a direct sum of two different semiprimitive two-weight irreducible cyclic codes, that generalizes such class of reducible cyclic codes. Moreover, we show that, contrary to what was stated in [10, p. 7254], it is still possible, at least for the codes in this

* *This work was partially supported by PAPIIT-UNAM IN107515.*
Jesús E. Cuén-Ramos (Corresponding Author); Posgrado en Ciencias Matemáticas, Universidad Nacional Autónoma de México, 04530 Ciudad de México, Mexico (email: elisandro@ciencias.unam.mx).
Gerardo Vega; Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, Mexico (email: gerardov@unam.mx).

Table 1. **Weight distribution of $\mathcal{C}_{(a_i)}$, $i = 1, 2$.**

Weight	Frequency
0	1
$\frac{(q-1)}{d}(q^{k-1} - q^{(k-2)/2})$	$\frac{(q^k-1)}{2}$
$\frac{(q-1)}{d}(q^{k-1} + q^{(k-2)/2})$	$\frac{(q^k-1)}{2}$

Table 2. **Weight distribution of $\mathcal{C}_{(a_1,a_2)}$.**

Weight	Frequency
0	1
$\frac{2(q-1)}{3d}(q^{k-1} - q^{(k-2)/2})$	$\frac{3(q^k-1)}{2}$
$\frac{2(q-1)}{3d}(q^{k-1} + q^{(k-2)/2})$	$\frac{3(q^k-1)}{2}$
$\frac{q-1}{d}(q^{k-1} - q^{(k-2)/2})$	$\frac{(q^k-1)(q^k-5)}{8}$
$\frac{q-1}{3d}(3q^{k-1} - q^{(k-2)/2})$	$\frac{3(q^k-1)^2}{8}$
$\frac{q-1}{3d}(3q^{k-1} + q^{(k-2)/2})$	$\frac{3(q^k-1)^2}{8}$
$\frac{q-1}{d}(q^{k-1} + q^{(k-2)/2})$	$\frac{(q^k-1)(q^k-5)}{8}$

family, to compute the frequencies of their weight distributions through the cyclotomic numbers in an easy way.

In order to give a detailed explanation of what is the main result of this work, let p, t, q, k and Δ be integers, such that p is a prime, $q = p^t$ and $\Delta = (q^k - 1)/(q - 1)$. In addition, let γ be a fixed primitive element of $\mathbb{F}_{q^k}$ and, for any integer a, denote by $h_a(x) \in \mathbb{F}_q[x]$ the minimal polynomial of γ^{-a}. Also, for any integers $a_1, a_2, a_3, \ldots, a_t$, let $\mathcal{C}_{(a_1,a_2,a_3,\ldots,a_t)}$ be the cyclic code with parity-check polynomial $\prod_{i=1}^{t} h_{a_i}(x)$. With this notation, the following result gives a description for the weight distribution of a family of reducible cyclic codes:

Theorem 1.1. *Suppose that* $3|(q^k - 1)$. *Let* a_1, a_2, d *and* n *be any integers such that* $a_1 - a_2 = \pm\frac{q^k-1}{3}$, $d = \gcd(q^k - 1, a_1, a_2)$ *and* $n = \frac{q^k-1}{d}$. *If* $\gcd(\Delta, 3a_1) = 2$ *then*

(A) $\mathcal{C}_{(a_1)}$ *and* $\mathcal{C}_{(a_2)}$ *are two different semiprimitive two-weight irreducible cyclic codes of length* n *and dimension* k *over* $\mathbb{F}_q$. *In addition, these codes have the same weight distribution which is given in Table 1.*

(B) $\mathcal{C}_{(a_1,a_2)}$ *is an* $[n, 2k]$ *cyclic code over* $\mathbb{F}_q$, *with the weight distribution given in Table 2.*

Recently, in [8] was given a unified explanation for the weight distribution of several families of codes whose parity-check polynomials are given by the products of the form $h_a(x)h_{a\pm\frac{q^k-1}{2}}(x)$, where $h_a(x) \neq h_{a\pm\frac{q^k-1}{2}}(x)$. From this perspective, therefore, it is important to keep in mind that the parity-check polynomials of the kind of codes studied in [10], and those studied by Theorem 1.1, are now given by the products of the form $h_a(x)h_{a\pm\frac{q^k-1}{3}}(x)$.

This work is organized as follows: In Section 2 we establish some notations, recall some definitions and establish our main assumption. Section 3 is devoted to presenting some preliminaries and general results. In Section 4 we use these results in order to present a formal proof of Theorem 1.1. In Section 5 we show some applications of Theorem 1.1. Finally, Section 6 is devoted to conclusions.

2. Definitions, notations, preliminaries and main assumption

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

Notation. By using p, t, q, k and Δ, we will denote five positive integers such that p is a prime number, $q = p^t$ and $\Delta = (q^k - 1)/(q - 1)$. From now on, γ will denote a fixed primitive element of $\mathbb{F}_{q^k}$. For any integer a, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial of γ^{-a}. Furthermore, 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 $\mathbb{F}_q$. For any positive divisor m of $q^k - 1$ and for any $0 \leq i \leq m-1$, we define $\mathcal{D}_i^{(m)} := \gamma^i \langle \gamma^m \rangle$, where $\langle \gamma^m \rangle$ denotes the subgroup of $\mathbb{F}_{q^k}^*$ generated by γ^m. The cosets $\mathcal{D}_i^{(m)}$ are called *cyclotomic classes* of order m in $\mathbb{F}_{q^k}$. In connection with these cyclotomic classes, we have the *cyclotomic numbers* of order m:

$$(i,j)^{(m,q^k)} := |(\mathcal{D}_i^{(m)} + 1) \cap \mathcal{D}_j^{(m)}| \, ,$$

where $(\mathcal{D}_i^{(m)} + 1) = \{x + 1 \mid x \in \mathcal{D}_i^{(m)}\}$, and $0 \leq i, j \leq m-1$. Finally, the canonical additive character χ, of $\mathbb{F}_{q^k}$, is:

$$\chi(y) = \zeta_p^{\mathrm{Tr}(y)} \, , \qquad \text{for all } y \in \mathbb{F}_{q^k} \, ,$$

where $\zeta_p = \exp(\frac{2\pi\sqrt{-1}}{p})$.

The following definition is a proper generalization of the idea of a semiprimitive irreducible cyclic code that was introduced recently in [9].

Definition 2.1. Let p, q, k and Δ be as before, and for any integer a let $u = \gcd(\Delta, a)$. Then an irreducible cyclic code with parity-check polynomial $h_a(x)$, of degree k, is called a *semiprimitive code* if $u \geq 2$, and if -1 is a power of p modulo u (that is, if the prime p is *semiprimitive modulo* u).

Now, we also set for the rest of this work the following:

Main assumption. From now on, we are going to suppose that $3|(q^k - 1)$, $2|\Delta$ and $3 \nmid \Delta$. Also, in what follows, we will reserve the Greek letter τ in order to fix $\tau = \gamma^{\frac{q^k-1}{3}}$.

Remark 2.2. *As a consequence of our main assumption, note that k should be an even integer, whereas q must be an odd integer greater than 5, and necessarily $3|(q-1)$ and $4|(q^k-1)$. In addition, observe that $\mathbb{F}_q^* \subset \mathcal{D}_0^{(2)}$, $\tau \in \mathcal{D}_0^{(2)}$, and also that the finite field element τ is a primitive three-root of unity satisfying $\tau^2 + \tau + 1 = 0$.*

The following is a well known result ([5, Lemma 4]):

Lemma 2.3. *Define*

$$\eta_i = \sum_{x \in \mathcal{D}_i^{(2)}} \chi(x) \, , \quad i = 0, 1 \, .$$

Then $\eta_1 = -1 - \eta_0$, and

$$\eta_0 = \begin{cases} \frac{-1+(-1)^{tk-1}q^{k/2}}{2} & \text{if } p \equiv 1 \pmod 4, \\ \frac{-1+(-1)^{tk-1}(\sqrt{-1})^{tk}q^{k/2}}{2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The exponential sums η_0 and η_1 are known as the *Gaussian periods* of order 2. Since we will be dealing with the Gaussian period of order 2, we also need the cyclotomic numbers of order 2. The following result is on that direction ([5]).

Lemma 2.4. *Suppose that $4|(q^k - 1)$, then*

$$\begin{aligned} (0,0)^{(2,q^k)} &= \tfrac{q^k-5}{4} \, , \\ (0,1)^{(2,q^k)} = (1,0)^{(2,q^k)} = (1,1)^{(2,q^k)} &= \tfrac{q^k-1}{4} \, . \end{aligned}$$

3. Some preliminaries and general results

With our current notation and main assumption in mind we present the following results.

Lemma 3.1. *Let a_1, a_2 and d be integers such that $a_2 = a_1 \pm \frac{q^k-1}{3}$ and $d = \gcd(q^k-1, a_1, a_2) \neq 0$. Then $3|\frac{q^k-1}{d}$ and $d = \gcd(q^k-1, a_1)$ or $d = \gcd(q^k-1, a_2)$.*

Proof. Since d divides both a_1 and a_2, we have that $d|\frac{q^k-1}{3}$. Therefore the first assertion is true. Let $d_i = \gcd(q^k-1, a_i)$ for $i = 1, 2$. Without loss of generality, suppose that $d_1 \leq d_2$. Observe that $d = \gcd(\frac{q^k-1}{3}, a_i)$ for $i = 1, 2$, and therefore either d_i is d or $3d$. Now, if $d_1 = 3d$, then $d_2 = 3d$, which implies that $3d|q^k-1, a_1, a_2$. But this last condition is impossible, thus $d_1 = d$. □

Lemma 3.2. *If $3d$ is a divisor of q^k-1 and $\gcd(\Delta, 3d) = 2$, then for any integer i*

$$\{xy \mid x \in \mathcal{D}_i^{(3d)} \text{ and } y \in \mathbb{F}_q^*\} = \frac{2(q-1)}{3d} * \mathcal{D}_i^{(2)},$$

where $\frac{2(q-1)}{3d} * \mathcal{D}_i^{(2)}$ is the multiset in which each element of $\mathcal{D}_i^{(2)}$ appears with multiplicity $\frac{2(q-1)}{3d}$.

Proof. Since $2|\Delta$ and $2|3d$, $\mathbb{F}_q^* \subset \mathcal{D}_0^{(2)}$ and $\mathcal{D}_0^{(3d)} \subset \mathcal{D}_0^{(2)}$. But $\gcd(\Delta, 3d) = 2$, therefore the result comes from the fact that $|\mathcal{D}_0^{(3d)}|\,|\mathbb{F}_q^*|/|\mathcal{D}_0^{(2)}| = 2(q-1)/3d$, and $\mathcal{D}_i^{(2)} = \gamma^i \mathcal{D}_0^{(2)}$ for any integer i. □

By using τ, and the cyclotomic classes of order 2, we define the following sets:

$$\begin{aligned} \mathcal{G} &:= \{(\alpha, -\beta) \in \mathbb{F}_{q^k}^2 \mid (\alpha - \beta\tau^i) \neq 0,\ 0 \leq i < 3\}, \text{ and} \\ \mathcal{E}_{i,j} &:= \{(\alpha, -\alpha\tau^i) \in \mathbb{F}_{q^k}^2 \mid (\alpha - \alpha\tau) \in \mathcal{D}_j^{(2)}\} \text{ for } i = 0, 1, 2, \text{ and } j = 0, 1. \end{aligned}$$

Remark 3.3. *Through a direct inspection it is easy to see that the above seven sets are pairwise disjoint and their union is equal to $\mathbb{F}_{q^k}^2 \setminus (0,0)$. In addition, clearly $|\mathcal{E}_{i,j}| = |\mathcal{D}_0^{(2)}| = \frac{q^k-1}{2}$, $|\mathcal{G}| = q^{2k} - 1 - 6|\mathcal{E}_{0,0}| = (q^k-1)(q^k-2)$ and, due to Remark 2.2, we have that if $(\alpha - \alpha\tau) \in \mathcal{D}_j^{(2)}$, for some integer $j = 0, 1$, then necessarily $(\alpha - \alpha\tau^2) = -\tau^2(\alpha - \alpha\tau) \in \mathcal{D}_j^{(2)}$.*

Now, for each $(\alpha, -\beta) \in \mathcal{G}$, we define the function $f_{\alpha,\beta} : \{0,1,2\} \to \{0,1\}$, given by the rule $f_{\alpha,\beta}(i) = j$ if and only if $(\alpha - \beta\tau^i) \in \mathcal{D}_j^{(2)}$. With the help of these functions we induce a partition of the set $\mathcal{G}$ into the following disjoint subsets:

$$\mathcal{S}_l := \{(\alpha, -\beta) \in \mathcal{G} \mid W_H(f_{\alpha,\beta}(0), f_{\alpha,\beta}(1), f_{\alpha,\beta}(2)) = l\},$$

for $l = 0, 1, 2, 3$, where $W_H(\cdot)$ stands for the usual Hamming weight function.

Remark 3.4. *For any $\alpha, \beta \in \mathbb{F}_{q^k}$, we define $u_i = (\alpha - \beta\tau^i)$, for $i = 0, 1, 2$. It is not difficult to see that these u values satisfy $u_0 + u_1\tau + u_2\tau^2 = 0$. Furthermore, observe that if we arbitrarily choose the values of, say, u_0 and u_2 then there must exist a unique vector $(\alpha, \beta) \in \mathbb{F}_{q^k}^2$, such that $u_0 = (\alpha - \beta)$, $u_2 = (\alpha - \beta\tau^2)$ and $u_1 = -\tau^{-1}(u_0 + u_2\tau^2)$. Therefore, if we want to calculate, for example, $|\mathcal{S}_0|$ then we can assume, without loss of generality, that u_2 can take any value in $\mathcal{D}_0^{(2)}$. This leads us to $\frac{q^k-1}{2}$ possible choices for u_2. But $u_1 = -u_2\tau(\frac{u_0}{u_2}\tau^{-2} + 1)$ and $-1, \tau \in \mathcal{D}_0^{(2)}$ (see Remark 2.2), thus, in order that u_1 and u_0 also belong to $\mathcal{D}_0^{(2)}$ it is necessary that $(\frac{u_0}{u_2}\tau^{-2} + 1) \in \mathcal{D}_0^{(2)}$. Hence, the number of such instances is given by the cyclotomic number $(0,0)^{(2,q^k)}$. Consequently, we have $|\mathcal{S}_0| = \frac{q^k-1}{2}(0,0)^{(2,q^k)}$. In a quite similar way, one can obtain $|\mathcal{S}_1|$, $|\mathcal{S}_2|$ and $|\mathcal{S}_3|$.*

Table 3. **Value distribution of** $\sum_{z\in\mathcal{D}_0^{(2)}}\sum_{i=0}^{2}\chi(z(\alpha+\beta\tau^i))$.

Value	Frequency
$\frac{3(q^k-1)}{2}$	1
$\frac{q^k-1}{2}+2\eta_0$	$\frac{3(q^k-1)}{2}$
$\frac{q^k-1}{2}+2\eta_1$	$\frac{3(q^k-1)}{2}$
$3\eta_0$	$\frac{(q^k-1)(q^k-5)}{8}$
$-1+\eta_0$	$\frac{3(q^k-1)^2}{8}$
$-1+\eta_1$	$\frac{3(q^k-1)^2}{8}$
$3\eta_1$	$\frac{(q^k-1)(q^k-5)}{8}$

Keeping in mind the previous definitions and observations we now present the following result, which will be important in order to determine the weight distribution of the class of reducible cyclic codes that we are interested in.

Lemma 3.5. *With our notation and main assumption, we have*

$$\begin{aligned}
|\mathcal{S}_0| &= \frac{q^k-1}{2}(0,0)^{(2,q^k)},\\
|\mathcal{S}_1| &= \frac{3(q^k-1)}{2}(0,1)^{(2,q^k)},\\
|\mathcal{S}_2| &= \frac{3(q^k-1)}{2}(1,1)^{(2,q^k)},\\
|\mathcal{S}_3| &= (q^k-1)(q^k-2)-(|\mathcal{S}_0|+|\mathcal{S}_1|+|\mathcal{S}_2|).
\end{aligned}$$

Furthermore, if χ denotes the canonical additive character of $\mathbb{F}_{q^k}$, and if η_0 and η_1 are as in Lemma 2.3, then, for any $\alpha,\beta\in\mathbb{F}_{q^k}$, we also have

$$\sum_{z\in\mathcal{D}_0^{(2)}}\sum_{i=0}^{2}\chi(z(\alpha+\beta\tau^i))=\begin{cases}
\frac{3(q^k-1)}{2} & \text{if } (\alpha,\beta)=(0,0),\\
\frac{q^k-1}{2}+2\eta_0 & \text{if } (\alpha,\beta)\in\cup_{i=0}^{2}\mathcal{E}_{i,0},\\
\frac{q^k-1}{2}+2\eta_1 & \text{if } (\alpha,\beta)\in\cup_{i=0}^{2}\mathcal{E}_{i,1},\\
3\eta_0 & \text{if } (\alpha,\beta)\in\mathcal{S}_0,\\
-1+\eta_0 & \text{if } (\alpha,\beta)\in\mathcal{S}_1,\\
-1+\eta_1 & \text{if } (\alpha,\beta)\in\mathcal{S}_2,\\
3\eta_1 & \text{if } (\alpha,\beta)\in\mathcal{S}_3.
\end{cases}$$

Proof. The first assertion comes from Remark 3.4. Since $\sum_{z\in\mathcal{D}_0^{(2)}}\chi(0)=|\mathcal{D}_0^{(2)}|=\frac{q^k-1}{2}$, the second assertion comes from Lemma 2.3, Remark 3.3, and from the definitions of the sets $\mathcal{E}_{i,j}$ and $\mathcal{S}_l$, with $i=0,1,2$, $j=0,1$, and $l=0,1,2,3$. □

Considering the actual values of the cyclotomic numbers in Lemma 2.4, the following result is an important consequence.

Corollary 3.6. *Consider the same hypotheses as in the previous lemma. Then the value distribution of the character sum $\sum_{z\in\mathcal{D}_0^{(2)}}\sum_{i=0}^{2}\chi(z(\alpha+\beta\tau^i))$ is given in Table 3.*

4. Proof of Theorem 1.1

Proof. Part (A): First note that $\gcd(\Delta, 3a_1) = \gcd(\Delta, 3a_2) = 2$, in consequence $\gcd(\Delta, a_i) = 2$ for i=1,2.

Let v_i be an integer such that $1 \leq v_i < k$ and $a_i q^{v_i} \equiv a_i \pmod{q^k - 1}$. Then $\frac{q^k-1}{q-1} | a_i \frac{q^{v_i}-1}{q-1}$, but $\gcd(\Delta, a_i) = 2$, thus $(q^k - 1) | 2(q^{v_i} - 1)$ for i=1,2. However, this last condition is impossible if $1 \leq v_i < k$ and $q \geq 7$ (recall Remark 2.2). Hence $\deg(h_{a_i}(x)) = k$.

Now, suppose that $h_{a_1}(x) = h_{a_2}(x)$. Then, there exists an integer $0 \leq v < k$ such that $a_1 q^v \equiv a_2 \pmod{q^k - 1}$. But $a_2 = a_1 \pm \frac{q^k-1}{3}$, thus the last congruence implies that $a_1(q^v - 1) \equiv \pm\frac{q^k-1}{3} \pmod{q^k - 1}$ and $v \geq 1$. Then $3a_1(q^v - 1) \equiv 0 \pmod{q^k - 1}$ with $1 \leq v < k$. That is $\frac{q^k-1}{q-1} | 3a_1 \frac{q^{v_i}-1}{q-1}$. But $\gcd(\Delta, 3a_1) = 2$, thus $(q^k - 1) | 2(q^{v_i} - 1)$. However, this last condition is impossible if $1 \leq v_i < k$ and $q \geq 7$. Hence $h_{a_1}(x) \neq h_{a_2}(x)$.

On the other hand, note that $\mathcal{C}_{(a_1)}$ and $\mathcal{C}_{(a_2)}$ have the same length $n = \frac{q^k-1}{d}$, and owing to Lemma 3.1, we have that $3|n$.

Since $\gcd(\Delta, a_1) = \gcd(\Delta, a_2) = 2$, clearly, in accordance with Definition 2.1, $\mathcal{C}_{(a_1)}$ and $\mathcal{C}_{(a_2)}$ are two different semiprimitive two-weight irreducible cyclic codes. Thus, by means of the characterization for this kind of codes in [9, Theorem 7], we can see that their weight distributions are as is shown in Table 1.

Part (B): By Lemma 3.1 and since $\mathcal{C}_{(a_2,a_1)} = \mathcal{C}_{(a_1,a_2)}$, we can assume without loss of generality that $d = \gcd(q^k - 1, a_1)$.

Clearly, the cyclic code $\mathcal{C}_{(a_1,a_2)}$ has length n and its dimension is $2k$ due to Part (A).

Now, for each $\alpha, \beta \in \mathbb{F}_{q^k}$, we define $c(n, a_1, a_2, \alpha, \beta)$ as the vector of length n over $\mathbb{F}_q$, which is given by:

$$(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^i + \beta(\gamma^{a_2})^i))_{i=0}^{n-1} .$$

Thanks to Delsarte's Theorem ([1]), it is well known that

$$\mathcal{C}_{(a_1,a_2)} = \{c(n, a_1, a_2, \alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_{q^k}\} .$$

Thus the Hamming weight of any codeword $c(n, a_1, a_2, \alpha, \beta)$ is equal to $n - Z(\alpha, \beta)$, where

$$Z(\alpha, \beta) = \sharp\{\, i \mid \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha\gamma^{a_1 i} + \beta\gamma^{a_2 i}) = 0,\ 0 \leq i < n\} .$$

Now, if χ' is the canonical additive character of $\mathbb{F}_q$, then, by the orthogonal property of χ' (see, for example, [4, p. 192]), we know that for each $c \in \mathbb{F}_q$ we have

$$\sum_{y \in \mathbb{F}_q} \chi'(yc) = \begin{cases} q & \text{if } c = 0, \\ 0 & \text{if } c \neq 0, \end{cases}$$

thus

$$Z(\alpha, \beta) = \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q} \chi'(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(y(\alpha\gamma^{a_1 i} + \beta\gamma^{a_2 i}))) .$$

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

$$\begin{aligned} Z(\alpha, \beta) &= \frac{n}{q} + \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \chi(y(\alpha\gamma^{a_1 i} + \beta\gamma^{a_2 i})) \\ &= \frac{n}{q} + \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \chi(\gamma^{a_1 i} y(\alpha + \beta\tau^{\epsilon i})) , \end{aligned}$$

where the last equality arises because $a_2 - a_1 = \epsilon\frac{q^k-1}{3}$ for some integer ϵ equal to 1 or -1. On the other hand, since $d|(a_2 - a_1)$ and $d = \gcd(q^k - 1, a_1)$, there must exist integers l, r and s, in such way that $\tau^\epsilon = \gamma^{dl}$, $d = r(q^k - 1) + sa_1$ and $\tau^{\epsilon i} = (\gamma^{a_1 i})^{ls}$. Therefore

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{1}{q}\sum_{i=0}^{n-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{di}y(\alpha+\beta\tau^{si}))\ .$$

But $3|n$. Then

$$\{\gamma^{di} \mid 0 \le i < n\} = \mathcal{D}_0^{(d)} = \mathcal{D}_0^{(3d)} \cup \mathcal{D}_d^{(3d)} \cup \mathcal{D}_{2d}^{(3d)}.$$

Therefore,

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{1}{q}\sum_{i=0}^{2}\sum_{x\in\mathcal{D}_{di}^{(3d)}}\sum_{y\in\mathbb{F}_q^*}\chi(xy(\alpha+\beta\tau^{si}))\ .$$

Now, since $d = \gcd(\frac{q^k-1}{3}, a_1)$ (see proof of Lemma 3.1) and $\gcd(\Delta, 3(\frac{q^k-1}{3}), 3a_1) = \gcd(\Delta, 3a_1)$, we have $\gcd(\Delta, 3d) = 2$. Thus, by Lemma 3.2, we obtain

$$\begin{aligned} Z(\alpha,\beta) &= \frac{n}{q} + \frac{2(q-1)}{3dq}\sum_{i=0}^{2}\sum_{z\in\mathcal{D}_{di}^{(2)}}\chi(z(\alpha+\beta\tau^{si})) \\ &= \frac{n}{q} + \frac{2(q-1)}{3dq}\sum_{z\in\mathcal{D}_0^{(2)}}\sum_{i=0}^{2}\chi(z(\alpha+\beta\tau^{si}))\ , \end{aligned}$$

where the last equality follows from the fact that $2|d$ (recall that $\gcd(\Delta, 3d) = 2$). Now, by Lemma 3.1, we have that $3d|q^k - 1$. Therefore, note that $3 \nmid s$, and this is so because if $3|s$, $3d|sa_1$, but recall that $d = r(q^k - 1) + sa_1$, then $3d|d$, and clearly this is a contradiction. Then

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2(q-1)}{3dq}\sum_{z\in\mathcal{D}_0^{(2)}}\sum_{i=0}^{2}\chi(z(\alpha+\beta\tau^{i}))\ .$$

Therefore the result comes from Corollary 3.6 because the Hamming weight of any codeword of the form $c(n, a_1, a_2, \alpha, \beta)$ in $\mathcal{C}_{(a_1,a_2)}$ is equal to $n - Z(\alpha,\beta)$. □

5. Some applications of Theorem 1.1

As we saw, through this work we deals with the kind of reducible cyclic codes whose parity check polynomials are given by the products of the form $h_a(x)h_{a\pm\frac{q^k-1}{3}}(x)$, where a is any integer and $h_a(x) \neq h_{a\pm\frac{q^k-1}{3}}(x)$. The following result, which is the main result in [10, Theorem 3.6], also deals with this kind of reducible cyclic codes:

Theorem 5.1. *Let h be a positive factor of $q-1$, and assume that 3 divides h. If $\gcd(k, 3(q-1)/h) = 2$, then $\mathcal{C}_{(\frac{q-1}{h}, \frac{q-1}{h}+\frac{q^k-1}{3})}$ is an $[h\Delta, 2k]$ code with the weight distribution in Table 4.*

The following result shows that the family of codes in Theorem 5.1, is included in Theorem 1.1.

Theorem 5.2. *Conditions in Theorem 5.1 imply conditions in Theorem 1.1.*

Table 4. **Weight distribution of $\mathcal{C}_{(\frac{q-1}{h},\frac{q-1}{h}+\frac{q^k-1}{3})}$.**

Weight	Frequency
0	1
$\frac{2h}{3}(q^{k-1}-q^{(k-2)/2})$	$\frac{3(q^k-1)}{2}$
$\frac{2h}{3}(q^{k-1}+q^{(k-2)/2})$	$\frac{3(q^k-1)}{2}$
$h(q^{k-1}-q^{(k-2)/2})$	$\frac{(q^k-1)(q^k-5)}{8}$
$h(q^{k-1}+q^{(k-2)/2})$	$\frac{(q^k-1)(q^k-5)}{8}$
$\frac{h}{3}(3q^{k-1}-q^{(k-2)/2})$	$\frac{3(q^k-1)^2}{8}$
$\frac{h}{3}(3q^{k-1}+q^{(k-2)/2})$	$\frac{3(q^k-1)^2}{8}$

Table 5. **Weight distribution of $\mathcal{C}_{(a_1,a_2,a_3)}$.**

Weight	Frequency $(\sum_{i=0}^{2} u_i = 3)$
$\frac{q-1}{3\delta q}(u_1(q^k+q^{k/2})+u_2(q^k-q^{k/2}))$	$(\frac{3!}{u_0!u_1!u_2!})(\frac{q^k-1}{2})^{u_1+u_2}$

Proof. Clearly $3|(q^k-1)$, and because $\gcd(\Delta,\rho)=\gcd(k,\rho)$ for all $\rho|(q-1)$ (see, for example [7, Remark 3]), we have $\gcd(\Delta,3(q-1)/h)=2$. Thus, by taking $a_1=(q-1)/h$ in Theorem 1.1, the result follows directly. □

As was mentioned before, Theorem 1.1 deals with the weight distribution of cyclic codes, $\mathcal{C}_{(a,a\pm\frac{q^k-1}{3})}$, under the condition $\gcd(\Delta,3a)=2$, but we also believe that is interesting the weight distribution of the cyclic codes, $\mathcal{C}_{(a,a-\frac{q^k-1}{3},a+\frac{q^k-1}{3})}$, under the same condition, because their parity-check polynomials differ by one irreducible factor. However, that kind of codes was treated in [13, Corollary 10]. Thus, we recall part of that result with our notation in the following:

Corollary 5.3. *With our notation and main assumption, suppose that a_1, a_2, a_3 and δ be integers such that $\delta=\gcd(q^k-1,a_1,a_2,a_3)$, $a_2=a_1+\frac{q^k-1}{3}$, $a_3=a_1-\frac{q^k-1}{3}$ and $\gcd(\Delta,3a_1)=2$. Then $\mathcal{C}_{(a_1,a_2,a_2)}$ is a $[(q^k-1)/\delta,3k]$ cyclic code over $\mathbb{F}_q$ with weight distribution in Table 5.*

The following are direct applications of Theorem 1.1.

Example 5.4. *With our notation, let $q=13$, $k=2$, $a_1=8$, $a_2=a_1+\frac{q^k-1}{3}=64$ and $a_3=a_1-\frac{q^k-1}{3}=-48$. Then $\Delta=14$, $d=\delta=8$ and $n=21$. Clearly $3|(q^k-1)$ and $\gcd(\Delta,3a_1)=2$. By Theorem 1.1, $\mathcal{C}_{(8)}$ and $\mathcal{C}_{(64)}$ are two different semiprimitive two-weight irreducible cyclic codes of length 21, dimension 2 and weight enumerator polynomial $A(z)=1+84z^{18}+84z^{21}$. In addition, $\mathcal{C}_{(8,64)}$ is a cyclic code of length 21, dimension 4 and weight enumerator polynomial*

$$\begin{aligned}A(z) &= 1+252z^{12}+252z^{14}+3444z^{18}\\ &\quad +10584z^{19}+10584z^{20}+3444z^{21}\,.\end{aligned}$$

On the other hand, by Corollary 5.3, $\mathcal{C}_{(8,64,-48)}$ is a cyclic code of length 21, dimension 6 and weight enumerator polynomial

$$\begin{aligned}A(z) &= 1+252z^{6}+252z^{7}+21168z^{12}+42336z^{13}+21168z^{14}\\ &\quad +592704z^{18}+1778112z^{19}+1778112z^{20}+592704z^{21}\,.\end{aligned}$$

Remark 5.5. *Since $2|\Delta$, clearly the length of all codes in Theorem 5.1 must be an even number. Therefore, the code in the previous example does not belong to the class of codes in Theorem 5.1.*

Example 5.6. *Now, let* $q = 7$, $k = 2$, $a_1 = 2$, $a_2 = a_1 - \frac{q^k-1}{3} = -14$, *and* $a_3 = a_1 + \frac{q^k-1}{3} = 18$. *Then* $\Delta = 8$, $d = \delta = 2$ *and* $n = 24$. *Clearly* $3|(q^k - 1)$ *and* $\gcd(\Delta, 3a_1) = 2$. *By Theorem 1.1,* $\mathcal{C}_{(2)}$ *and* $\mathcal{C}_{(-14)}$ *are two different semiprimitive two-weight irreducible cyclic codes of length* 24, *dimension* 2 *and weight enumerator polynomial* $A(z) = 1 + 24z^{18} + 24z^{24}$. *In addition,* $\mathcal{C}_{(2,-14)}$ *is a cyclic code of length* 24, *dimension* 4 *and weight enumerator polynomial*

$$\begin{aligned} A(z) &= 1 + 72z^{12} + 72z^{16} + 264z^{18} \\ &\quad +864z^{20} + 864z^{22} + 264z^{24} . \end{aligned} \tag{1}$$

On the other hand, by Corollary 5.3, $\mathcal{C}_{(2,-14,18)}$ *is a cyclic code of length* 24, *dimension* 6 *and weight enumerator polynomial*

$$\begin{aligned} A(z) &= 1 + 72z^{6} + 72z^{8} + 1728z^{12} + 3456z^{14} + 1728z^{16} \\ &\quad +13824z^{18} + 41472z^{20} + 41472z^{22} + 13824z^{24} . \end{aligned}$$

Remark 5.7. *Suppose again that* $q = 7$ *and* $k = 2$. *Then* $h_{-14}(x) = h_{34}(x) \neq h_{18}(x)$, *and consequently note that despite that the weight enumerator polynomial in the previous example is exactly the same as weight enumerator polynomial in the example of [10, page 7257], the cyclic codes* $\mathcal{C}_{(2,-14)}$ *and* $\mathcal{C}_{(2,18)}$ *are different. In addition, also note that the cyclic code* $\mathcal{C}_{(2,-14)} = \mathcal{C}_{(2,34)}$ *does not belong to the class of codes in Theorem 5.1.*

Remark 5.8. *Through a direct inspection, it is not difficult to see that all different reducible cyclic codes over* $\mathbb{F}_7$ *of length* 24, *dimension* 4 *and weight enumerator polynomial, as in (1), are* $\mathcal{C}_{(2,18)}$, $\mathcal{C}_{(2,34)}$, $\mathcal{C}_{(18,34)}$, $\mathcal{C}_{(6,10)}$, $\mathcal{C}_{(6,26)}$ *and* $\mathcal{C}_{(10,26)}$. *All these reducible cyclic codes belong to the class of codes in Theorem 1.1.*

Remark 5.9. *Under our main assumption, note that if* $\gcd(\Delta, 3a) = 2$, *then* $\gcd(\Delta, 3(a \pm \frac{q^k-1}{3})) = 2$. *Therefore, a reducible cyclic code,* $\mathcal{C}_{(a,a\pm\frac{q^k-1}{3})}$, *will belong to the family of codes in Theorem 1.1, if and only if* $\gcd(\Delta, a) = 2$. *This condition, which is easy to verify, allows us to identify all the reducible cyclic codes that satisfy conditions in Theorem 1.1. In fact, if* $N_{(q,k)}$ *is the number of different reducible cyclic codes,* $\mathcal{C}_{(a_1,a_2)}$, *that satisfy such conditions, then it is not difficult to see that*

$$N_{(q,k)} = \frac{\phi(\frac{\Delta}{2})(q-1)}{k} ,$$

where ϕ *is the usual Euler* ϕ*-function. What is interesting here is that it seems that* $N_{(q,k)}$ *is also the total number of reducible cyclic codes whose weight distribution is given in Table 2.*

6. Conclusion

In this work we found the sufficient numerical conditions in order to obtain the full weight distribution of a family of codes that belongs to the kind of reducible cyclic codes whose parity-check polynomials are given by the products of the form $h_a(x)h_{a\pm\frac{q^k-1}{3}}(x)$. By means of the characterization of all semiprimitive two-weight irreducible cyclic codes that was presented in [9, Theorem 7], we were able to identify that the codes in this family are constructed as a direct sum (as vector spaces) of two different semiprimitive two-weight irreducible cyclic codes. In addition, we also showed that the class of codes recently studied in [10] is included in this family. Moreover, despite of what was stated in [10], we showed that, at least for the codes in this family, it is still possible to compute the frequencies of their weight distributions through the cyclotomic numbers in an easy way.

Finally, we believe that perhaps, following the same idea as in [8], it could be possible to develop a more general theory that allows us to present a unified explanation for an enlarged family of reducible cyclic codes of this kind.

References

[1] P. Delsarte, On subfield subcodes of Reed–Solomon codes, IEEE Trans. Inform. Theory 21(5) (1975) 575–576.
[2] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inform. Theory 57(12) (2011) 8000–8006.
[3] T. Helleseth, Some two–weight codes with composite parity–check polynomials, IEEE Trans. Inform. Theory 22(5) (1976) 631–632.
[4] R. Lidl, H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge 1983.
[5] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, IEEE Trans. Inform. Theory 57(1) (2011) 397–402.
[6] G. Vega, Two–weight cyclic codes constructed as the direct sum of two one–weight cyclic codes, Finite Fields Appl. 14(3) (2008) 785–797.
[7] G. Vega, The weight distribution of an extended class of reducible cyclic codes, IEEE Trans. Inform. Theory 58(7) (2012) 4862–4869.
[8] G. Vega, L. B. Morales, A general description for the weight distribution of some reducible cyclic codes, IEEE Trans. Inform. Theory 59(9) (2013) 5994–6001.
[9] G. Vega, A critical review and some remarks about one– and two–weight irreducible cyclic codes, Finite Fields Appl. 33 (2015) 1–13.
[10] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of cyclic codes and elliptic curves, IEEE Trans. Inform. Theory 58(12) (2012) 7253–7259.
[11] J. Wolfmann, Are 2−weight projective cyclic codes irreducible?, IEEE Trans. Inform. Theory 51(2) (2005) 733–737.
[12] M. Xiong, The weight distributions of a class of cyclic codes, Finite Fields Appl. 18(5) (2012) 933–945.
[13] J. Yang, M. Xiong, C. Ding, J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory 59(9) (2013) 5985–5993.