THE WEIGHT DISTRIBUTION OF FAMILIES OF REDUCIBLE CYCLIC CODES THROUGH THE WEIGHT DISTRIBUTION OF SOME IRREDUCIBLE CYCLIC CODES

GERARDO VEGA
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
04510 Ciudad de México, Mexico

JESÚS E. CUÉN-RAMOS
Posgrado en Ciencias Matemáticas
Universidad Nacional Autónoma de México
20059 Ciudad de México, Mexico

Abstract. The calculation of the weight distribution for some reducible cyclic codes can be reduced down to the corresponding one of a particular kind of irreducible cyclic codes. This reduction is achieved by means of a known identity (see [3, Theorem 1.1]). In fact, as will be shown here, the weight distribution of some families of reducible cyclic codes, recently reported in several works ([2, 5, 7, 11, 12]), and that of others not previously reported, can be obtained almost directly by means of this identity.

1. Introduction

A cyclic code $C$ is reducible if its parity check polynomial $h(x)$ is at least the product of two irreducible polynomials. Moreover, since cyclic codes are linear, the cyclic code $C$ is the direct sum (as vector spaces) of the irreducible cyclic codes in which their parity check polynomials are the irreducible factors of $h(x)$. Hence, determining the weight distribution (WD, for brevity) of a reducible cyclic code (RCC) is generally more difficult than determining the WD of an irreducible cyclic code (ICC). This work aims to show that the problem of determining the WD of some families of RCCs, recently reported in [2, 5, 7, 11, 12], can be reduced in terms of the WD of some already-studied ICCs, with well-known WDs. In fact, as will be shown later, this reduction can be generalized to a specific family of RCCs, whose WD can always be obtained in terms of the WD of a particular kind of ICC. Furthermore, using this generalization the WD of other RCCs not previously reported is also easily obtained.

In order to give a detailed picture of the above, we need to establish some notation and terminology. Consider the positive integers $p$, $t$, $q$ and $k$ with $p$ prime and $q = p^k$. Let $v$ and $w$ be integers, such that gcd$(v, w) = 1$. Then, the smallest positive integer $i$, such that $w^i \equiv 1 \pmod{v}$, is called the multiplicative order of $w$ modulo $v$, and is denoted by $\text{ord}_v(w)$. $\gamma$ will denote a fixed primitive element of $\mathbb{F}_{q^k}$, and for any integer $a$, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial

2010 Mathematics Subject Classification: Primary: 94B15, 11T71.
Key words and phrases: Weight distribution, irreducible cyclic codes, reducible cyclic codes.
Partially supported by PAPIIT-UNAM IN109818.
* Corresponding author: Gerardo Vega.
† Ph.D. student.

of $\gamma^{-a}$. In addition, $\mathcal{C}_{(a)}$ will denote the ICC whose parity check polynomial is $h_a(x)$. Note that $\mathcal{C}_{(a)}$ is an $[n, l]$ linear code, where $n = \frac{q^k - 1}{\gcd(q^k - 1, a)}$, $l = \deg(h_a(x))$, and note that $l$ must be a divisor of $k$. For integers $a$ and $e$, such that $e > 1$ and $e \mid q^k - 1$, $m_{(a,e)}(x) \in \mathbb{F}_q[x]$ will denote the least common multiple of the $e$ polynomials $h_a(x)$, $h_a+\frac{e-1}{q-1}(x)$, ..., $h_a+\frac{e-1}{q-1}(x)$. 

$\mathfrak{M}(a, e)$ denotes the cyclic code whose parity check polynomial is $m_{(a,e)}(x)$. Since the order of $m_{(a,e)}(x)$ is the least common multiple of the order of its irreducible factors (see [4, Theorem 3.9]), note that the order of $m_{(a,e)}(x)$ divides $e(q^k - 1)/\gcd(q^k - 1, ae)$. Therefore, $\mathfrak{M}(a, e)$ is a linear code of length $e(q^k - 1)/\gcd(q^k - 1, ae)$ and dimension $\deg(m_{(a,e)}(x))$.

In this work we use a known identity among the weight enumerator polynomial of certain cyclic codes ([3, Theorem 1.1]), to show that the problem of determining the WD of the cyclic code $\mathfrak{M}(a, e)$ can always be reduced to the problem of determining the WD of $\mathcal{C}_{(ae)}$ (that is, the ICC whose parity check polynomial is $h_{ae}(x)$). Unfortunately, this reduction is not a solution to the underlying problem (the WD of $\mathfrak{M}(a,e)$) because, in general, it is still a very hard problem to obtain the WD of an ICC ([1]), nevertheless these distributions are well known for some families ([8]). More specifically, it is known that the code $\mathcal{C}_{(ae)}$ corresponds to either a one-weight ICC or a semiprimitive two-weight ICC if and only if $N = 1$ or $2$, or $N > 2$, $f$ is even and $p^{f/2} \equiv -1 \pmod{N}$, where $N = \gcd(\frac{q-1}{ae}, f)$ and $f = \ord_{N}(p)$. The WD of these two kinds of ICCs is also well known; therefore, this knowledge will allow us to not only determine the WD of some hitherto not studied families of cyclic codes with a number of zeros, but will also allow us to almost directly obtain the WD of some RCCs of the form $\mathfrak{M}(a,e)$, that have been recently studied. For example, Cases 1, 2 and 4 of the Concluding Remarks in [2, p. 8005], all cases studied in [5, 7], Case 1 of the Conclusion in [11, p. 5992] (except when $N = 3$), and the family of codes studied in [12], can be solved directly through the WD of either a one-weight ICC or a semiprimitive two-weight ICC (for the analysis of these cases, note that $\gcd(\frac{q-1}{ae}, f) = \gcd(k, ae)$ if $ae \mid (q - 1)$). Now, note that an imposed restriction regarding the aforementioned cases is that the parity check polynomial $m_{(a,e)}(x)$, of $\mathfrak{M}(a,e)$, must be the product of irreducible polynomials of the same degree $k$ (see, for example, Main Assumptions in [11, p. 5985]). A further purpose of this work is to get rid of this restriction by showing that, in spite of $m_{(a,e)}(x)$, it is always possible to obtain the WD of $\mathfrak{M}(a,e)$ in terms of the WD of $\mathcal{C}_{(ae)}$.

Recently [9, Theorem 4], it was shown that it is possible to use the WD of some ICCs in order to obtain the WD of some RCCs whose parity check polynomials have the form $h_{\frac{y^2+1}{p^2}}(x)h_{\frac{y^2+1}{p^2}+\frac{y^2-1}{p^2}}(x)$, where $y$ and $\sigma$ are integers, such that $y > 0$, $\sigma \geq 0$, and $h_{\frac{y^2+1}{p^2}}(x)$, $h_{\frac{y^2+1}{p^2}+\frac{y^2-1}{p^2}}(x)$ are two different irreducible polynomials of the same degree $k$. That is, in that work, the WD of a kind of RCCs of the form $\mathfrak{M}(a,e)$ was obtained when $e = 2$, and when their parity check polynomials, $m_{(a,e)}(x)$, were given as a product of two or more irreducible polynomials ($e \geq 2$ ) that do not necessarily have the same degree.
2. Definitions and known results

Along with the notation and terminology introduced previously, we now present some definitions and recall some already known results.

A subset $\mathcal{C}$ of vectors or words in $\mathbb{F}_q^n$ is called an $[n, l]$ linear code over $\mathbb{F}_q$ if $\mathcal{C}$ is an $l$-dimensional subspace of $\mathbb{F}_q^n$: $n$ is called the length and $l$ is called the dimension of $\mathcal{C}$. In this context, the elements of $\mathcal{C}$ are called code words. Let $A_i$ be the number of code words with Hamming weight $i$ in $\mathcal{C}$ (recall that the Hamming weight of a word $c$ is the number of nonzero coordinates in $c$, [6, p. 8]). Then, the sequence $A_0, A_1, \ldots, A_n$ is called the weight distribution of $\mathcal{C}$, and the polynomial $A_0 + A_1 z + \ldots + A_n z^n$ is called the weight enumerator polynomial of $\mathcal{C}$.

The WD of a code is important because it contains information that determines the capability of error detection and correction of the code.

An $M$-weight code is a code such that the cardinality of the set of nonzero weights is $M$. That is, $M = \{i : A_i \neq 0, i = 1, 2, 3, \ldots, n\}$.

A linear code $\mathcal{C}$ of length $n$ is cyclic if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. Cyclic codes have wide applications in storage and communication systems because, unlike encoding and decoding algorithms for linear codes, encoding/decoding algorithms for cyclic codes can be implemented easily and efficiently by employing shift registers with feedback connections ([6, p. 209]).

By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$, it follows that any linear code $\mathcal{C}$ of length $n$ over $\mathbb{F}_q$ corresponds to a subset of the residue class ring $\mathbb{F}_q[x]/(x^n - 1)$. Moreover, it is well known that the linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$ (see, for example, Theorem 9.36 in [4]).

Now, note that every ideal of $\mathbb{F}_q[x]/(x^n - 1)$ is principal. In consequence, if $\mathcal{C}$ is a cyclic code of length $n$ over $\mathbb{F}_q$, then $\mathcal{C} = \langle g(x) \rangle$, where $g(x)$ is a monic polynomial, such that $g(x) \mid (x^n - 1)$. This polynomial is unique, and it is called the generator polynomial of $\mathcal{C}$ ([6, Theorem 1, p. 190]). On the other hand, the polynomial $h(x) = (x^n - 1)/g(x)$ is referred to as the parity check polynomial of $\mathcal{C}$. In this context, if $l$ is the dimension of $\mathcal{C}$, then $l = \deg(h(x)) = n - \deg(g(x))$.

As usual in cyclic codes, we always assume that the length $n$ of any cyclic code is relatively prime to $q$. Thus, $x^n - 1$ has no repeated factors ([6, p. 196]). Therefore, since $h(x)|(x^n - 1)$, we must keep in mind that the parity check polynomial of any cyclic code has no repeated factors.

A cyclic code over $\mathbb{F}_q$ is called irreducible (reducible) if its parity check polynomial is irreducible (reducible) over $\mathbb{F}_q$.

Let $v$ and $w$ be integers, such that $\gcd(v, w) = 1$. We say that $w$ is semiprimitive modulo $v$, if there exists a positive integer $j$, such that $w^j \equiv -1 \pmod{v}$.

According to Definition 6 in [8], an ICC $\mathcal{C}(a)$ of dimension $k$ over $\mathbb{F}_q$ is called semiprimitive if $u \geq 2$ and $p$ is semiprimitive modulo $u$, where $u = \gcd(q^k - 1, a)$ (recall $q = p^l$).

As already stated, one of the goals of this work is to determine the WD of the cyclic code $\mathfrak{M}(a, e)$ using the WD of the ICC $\mathcal{C}(ae)$. For this reason, it is important to explicitly know the WD of some ICCs. Fortunately, there exist characterizations that allow us to determine WDs for one-weight ICCs and for semiprimitive two-weight ICCs. We now recall them:

Theorem 2.1 ([8], Theorem 2). Let $a$ be any integer. Also let $\Delta$, $n$ and $u$ be integers, such that $\Delta = (q^k - 1)/(q - 1)$, $n = (q^k - 1)/\gcd(q^k - 1, a)$ and $u =$
such that $f$ is the parity check polynomial of an $[n,k]$ one-weight ICC over $\mathbb{F}_q$, whose nonzero weight is $\frac{n}{2}q^{k-1}$, if and only if $u = 1$.

**Theorem 2.2** ([8], Theorem 7). Consider the same notation and assumption as in Theorem 2.1. Define $f = \text{ord}_u(p)$, and $s = \frac{k}{f}$. Then, $h_a(x)$ is the parity check polynomial of a semiprimitive two-weight ICC $\mathcal{C}$ if and only if $u = 2$ or $u > 2$, $f$ is even, and $p^{f/2} \equiv -1 \pmod{u}$. In addition, if $\mathcal{C}$ is a semiprimitive two-weight ICC, then $\mathcal{C}$ is an $[n,k]$ cyclic code over $\mathbb{F}_q$ whose weight enumerator polynomial is

$$1 + \frac{(q^k - 1)(u - 1)}{u} \frac{q^{k/2} - 1}{\Delta} + \frac{q^k - 1}{u} \frac{q^{k/2} - 1}{\Delta}.$$

The following is a known identity among the weight enumerator polynomials of some cyclic codes (see [3, Theorem 1.1] or [9, Theorem 3]).

**Theorem 2.3.** For some integers $n$ and $l$, let $\mathcal{C}$ be an $[n,l]$ cyclic code over $\mathbb{F}_q$ with parity check polynomial $h(x)$, and whose weight enumerator polynomial is $A(z)$. Let also $e$ be any positive integer such that $\gcd(q,e) = 1$. Then, $h(x^e)$ is the parity check polynomial of an $[en,el]$ cyclic code whose weight enumerator polynomial is $A(z)^e$.

3. Preliminary results

The following preliminary result, which is essential for this work, shows that the parity check polynomial $m_{a,e}(x)$, of the cyclic code $\mathcal{M}(a,e)$, is nothing else than the polynomial $h_{a,e}(x^e)$, where $h_{a,e}(x)$ is the minimal polynomial of $\gamma^{-ae}$ and also the parity check polynomial of the ICC $\mathcal{C}_{ae}$.

**Lemma 3.1.** Let $a$ and $e$ be integers, such that $e > 1$ and $e \mid (q^k - 1)$. Then, $m_{a,e}(x) = h_{a,e}(x^e)$.

**Proof.** For some integer $0 \leq i < e$, let $h_{a+\frac{q^{k-1}}{e_1}}(x)$ be an irreducible factor of $m_{a,e}(x)$. Since $\gamma^{-a-\frac{q^{k-1}}{e_1}}$ is a root of both $h_{a+\frac{q^{k-1}}{e_1}}(x)$ and $h_{a,e}(x^e)$, $h_{a+\frac{q^{k-1}}{e_1}}(x)$ is an irreducible factor of $h_{a,e}(x^e)$, and $m_{a,e}(x) \mid h_{a,e}(x^e)$. Now, let $f(x)$ be an irreducible factor of $h_{a,e}(x^e)$. Since $\text{ord}(h_{a,e}(x)) \mid \frac{q^k - 1}{e}$, $h_{a,e}(x^e) \mid x^{q^k - 1} - 1$ and $h_{a,e}(x^e)$ has not repeated factors. Thereby, there exists an integer $0 \leq b < q^k - 1$, such that $f(x) = h_b(x)$. Thus, $\gamma^{-b}$ is a root of $h_{a,e}(x^e)$, and $\gamma^{-eb}$ is a root of $h_{a,e}(x)$. So, $bq^v \equiv ae \pmod{q^k - 1}$ for some integer $v$, and, since $e \mid q^k - 1$, $bq^v = a + \frac{q^{k-1}}{e}i$ for some integer $i$. That is, $f(x) = h_b(x) = h_{bq^v}(x)$ is an irreducible factor of $m_{a,e}(x)$. Consequently, $h_{a,e}(x^e) \mid m_{a,e}(x)$, and $m_{a,e}(x) = h_{a,e}(x^e)$. \square

Thus, since the parity check polynomial of the code $\mathcal{M}(a,e)$ is equal to $h_{a,e}(x^e)$, we are now able to apply Theorem 2.3 to obtain the weight enumerator polynomial of the cyclic code $\mathcal{M}(a,e)$ using the weight enumerator polynomial of the ICC $\mathcal{C}_{ae}$ of length $n = (q^k - 1)/\gcd(q^k - 1, ae)$ and dimension $l = \deg(h_{a,e}(x))$. We present this by means of the following:

**Theorem 3.2.** Consider the same hypotheses as in the previous lemma. Also, let $l$ and $n$ be integers, such that $n = (q^k - 1)/\gcd(q^k - 1, ae)$ and $l = \deg(h_{a,e}(x))$. Assume that $A(z)$ is the weight enumerator polynomial of the ICC $\mathcal{C}_{ae}$. Then $\mathcal{M}(a,e)$ is an $[en,el]$ cyclic code with weight enumerator polynomial $A(z)^e$. 

---

**Advances in Mathematics of Communications**

**Volume X, No. X (200X), X–XX**
Proof. According to Lemma 3.1, we have that $m_{(a,e)}(x) = h_{ae}(x^e)$, thus, by Theorem 2.3, and since $\gcd(q, e) = 1$, $\mathfrak{M}(a, e)$ is an $[en, e]$ cyclic code with weight enumerator polynomial $A(z)^e$. 

As mentioned earlier, by imposing the condition that the irreducible factors of $m_{(a,e)}(x)$ must be of the same degree $k$, several authors studied the WD of the family of cyclic codes of the form $\mathfrak{M}(a, e)$. In consequence, a criterion was needed to decide when such condition was satisfied. The following result, established in [11], gives the sufficient numerical condition in order that the parity check polynomial $m_{(a,e)}(x)$, of the code $\mathfrak{M}(a, e)$, is the product of exactly $e$ irreducible polynomials of degree $k$.

Lemma 3.3 ([11], Lemma 6). Let $a$ and $e$ be integers, such that $e > 1$ and $e \mid (q^k - 1)$. Also let $a_0, a_1, \ldots, a_{e-1}$ be integers, such that $a_i = a + \frac{q^k - 1}{e} i$, $0 \leq i < e$. If $\gcd\left(\frac{q^k - 1}{e}, ae\right) \leq q^{k/2}$, then $\deg(h_{a_i}(x)) = k$, and $h_{a_i}(x) \neq h_{a_j}(x)$ for any $0 \leq i \neq j < e$.

Just by looking at the degree of the polynomial $h_{ae}(x)$, it is possible to provide a more accurate result than the previous one. More specifically, our next preliminary result gives simple necessary and sufficient numerical conditions in order to see that $m_{(a,e)}(x)$ is the product of $e$ irreducible polynomials of degree $k$ over $\mathbb{F}_q$.

Lemma 3.4. Let $a$ and $e$ be integers, such that $e > 1$ and $e \mid (q^k - 1)$. Then, $\deg(h_{ae}(x)) = k$ if and only if $m_{(a,e)}(x)$ is the product of $e$ irreducible polynomials of degree $k$ over $\mathbb{F}_q$.

Proof. If $m_{(a,e)}(x)$ is the product of $e$ irreducible polynomials of degree $k$, then $\deg(m_{(a,e)}(x)) = ek$, and $\deg(h_{ae}(x^e)) = ek$ by Lemma 3.1. So, $\deg(h_{ae}(x)) = k$.

Conversely, suppose that $\deg(h_{ae}(x)) = k$. For some integer $0 \leq i < e$, let $h_{a+\frac{q^k - 1}{e} i}(x)$ be an irreducible factor of $m_{(a,e)}(x)$. The degree of $h_{a+\frac{q^k - 1}{e} i}(x)$ is the smallest positive integer $l$, such that $l|k$, and $(a+\frac{q^k - 1}{e} i)l^{ae} \equiv a + \frac{q^k - 1}{e} i \pmod{q^k - 1}$. Consequently, $aeq^{l-1} \equiv ae \pmod{q^k - 1}$, and since $\deg(h_{ae}(x)) = k$, we have that $k|l$. Thus, $l = \deg(h_{ae}(x)) = k$. Therefore, $\deg(h_{a+\frac{q^k - 1}{e} i}(x)) = k$. But $\deg(m_{(a,e)}(x) = h_{ae}(x^e)) = ek$, and since $m_{(a,e)}(x)$ has not repeated factors, $m_{(a,e)}(x)$ is the product of $e$ irreducible polynomials of degree $k$.

Since $\deg(h_{ae}(x)) = l$ iff $l$ is the smallest positive integer, such that $aeq^{l-1} \equiv ae \pmod{q^k - 1}$, it is important to note that it is not necessary to explicitly construct the polynomial $m_{(a,e)}(x)$ in order to know the degree of $h_{ae}(x)$.

4. The Weight Distribution of an Infinite Family of Cyclic Codes of the Form $\mathfrak{M}(a, e)$

Since the WDs of several ICCs are completely determined through Theorems 2.1 and 2.2, we can now use these distributions and Theorem 3.2 in order to obtain the WD of an infinite family of cyclic codes of the form $\mathfrak{M}(a, e)$. We state this by means of the following:

Theorem 4.1. Let $a$, $e$, $l$ and $n$ be integers, such that $e > 1$, $e \mid (q^k - 1)$ and $n = (q^k - 1)/\gcd(q^k - 1, ae)$. Assume that $\deg(h_{ae}(x)) = l$, and consider $N' = \gcd\left(\frac{q^k - 1}{e}, ae\right)/(\frac{q^k - 1}{e})$, $f = \text{ord}_N(p)$, and $s = lt/f$. Thus:
(a) If $N' = 1$, then $\mathfrak{M}(a, e)$ is an $[en, el]$ cyclic code with weight enumerator polynomial

\[
\left(1 + (q^l - 1)z^{\frac{n(n-1)}{q^l-1}}\right)^e.
\]

(b) If $N' = 2$ or $N' > 2$, $f$ is even and $p^{f/2} \equiv -1 \pmod{N'}$, then $\mathfrak{M}(a, e)$ is an $[en, el]$ cyclic code with weight enumerator polynomial

\[
\left(1 + (q^l - 1)\left(\frac{N'-1}{N'}\right)z^{\frac{n(q^l-1)s^{f/2}(q-1)}{q(q^l-1)}} + \frac{q^l - 1}{N'}z^{\frac{n(q^l-1)s^{f/2}(q-1)}{q(q^l-1)}}\right)^e.
\]

Proof. First, we are going to determine the WD of the code $\mathcal{C}_{(ae)}$. Clearly, $\mathcal{C}_{(ae)}$ is an $[n, l]$ ICC. Since $l$ divides $k$, $\gamma^{-ae} \in \mathbb{F}_{q^l}^*$, therefore $ae = \frac{q^l - 1}{q^l - 1}$ for some integer $b$. Let $u = \gcd\left(\frac{q^l - 1}{q^l - 1}, b\right)$, and note that $N' = u$. Thus, thanks to Theorems 2.1 and 2.2, the weight enumerator polynomial of $\mathcal{C}_{(ae)}$ is

\[
1 + (q^l - 1)z^{\frac{n(q^l-1)}{q^l-1}}
\]

if $N' = 1$, and

\[
1 + (q^l - 1)\left(\frac{N'-1}{N'}\right)z^{\frac{n(q^l-1)s^{f/2}(q-1)}{q(q^l-1)}} + \frac{q^l - 1}{N'}z^{\frac{n(q^l-1)s^{f/2}(q-1)}{q(q^l-1)}}
\]

if $N' = 2$ or $N' > 2$, $f$ is even, and $p^{f/2} \equiv -1 \pmod{N'}$. Lastly, the remaining part of the proof follows now directly from Theorem 3.2.

\[\square\]

5. Some Applications of Theorem 4.1

A common way of dealing with the WD problem of the family of codes of the form $\mathfrak{M}(a, e)$ has been through a subdivision of such family, which is done by means of the possible values of the integer $N = \gcd\left(\frac{q^l - 1}{q^l - 1}, ae\right)$ (see, for example, Concluding Remarks and Conclusion in [2] and [11], respectively, and recall that $\gcd\left(\frac{q^l - 1}{q^l - 1}, ae\right) = \gcd(k, ae)$ if $ae \mid (q-1)$). However, in view of Theorem 4.1 and its proof, it has become apparent why such subdivision is made in terms of the integer $N$. That is, note that the integer $N' = N/(\frac{q^l - 1}{q^l - 1})$, in Theorem 4.1, determines whether the code $\mathcal{C}_{(ae)}$, of dimension $l$, is a one-weight or a semiprimitive two-weight ICC, or none of them. In order to appreciate this, consider the following family of codes of the form $\mathfrak{M}(a, e)$, that has been recently studied.

Theorem 5.1 ([2], Theorem 7). Suppose that $p$ is odd, and $t$ is even. Let $h$ be a positive even divisor of $q - 1$, $e = 2$. Define $N_1 = \gcd(k, (q - 1)e/h)$. Assume there exists a positive integer $j$ such that $p^j \equiv -1 \pmod{N_1}$, and the $j$ is the least such. Let $q^k = p^{2j\alpha}$, where $\alpha = kt/2j$. Let $\mathcal{C}$ be a cyclic code with parity check polynomial $h_{-2k-1}(x)h_{-q^k-1}(x)$. Assume that $2(q - 1)/hN_1$ is odd and $N_1 > 2$.

(a) If $\alpha$, $p$, and $(p^j + 1)/N_1$ are all odd, $\mathcal{C}$ is an $[h(q^k - 1), 2k]$ cyclic code over $\mathbb{F}_q$ with the WD in Table 1, provided that $N_1 < q^{k/2} + 1$.

(b) In all other cases, $\mathcal{C}$ is an $[h(q^k - 1), 2k]$ cyclic code over $\mathbb{F}_q$ with the WD in Table 2, provided that $N_1 < q^{k/2} + 1$.

Remark 1. There is a misprint in Table II, mentioned in Theorem 7 of [2]; the frequencies in the fourth and fifth rows are interchanged.

By using Theorem 4.1, we present a simple proof of the previous theorem.

Advances in Mathematics of Communications Volume X, No. X (200X), X–XX
\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
Weight & Frequency \\
\hline
$\frac{h}{2} (q^k + q^{k/2})$ & $(N_1 - 1)^2 \frac{q^k - 1}{N_1}^2$ \\
$\frac{h}{2} (2q^k - (N_1 - 2)q^{k/2})$ & $2(N_1 - 1) \frac{q^k - 1}{N_1}^2$ \\
$\frac{h}{2} (q^k - (N_1 - 1)q^{k/2})$ & $2^2 \frac{q^k - 1}{N_1}$ \\
$\frac{h}{2} (q^k)$ & $(q^k - 1)^2$ \\
\hline
\end{tabular}
\caption{Table 1.}
\end{table}

\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
Weight & Frequency \\
\hline
$\frac{h}{2} (q^k - (-1)\alpha q^{k/2})$ & $(N_1 - 1)^2 \frac{q^k - 1}{N_1}^2$ \\
$\frac{h}{2} (2q^k - (-1)^{\alpha+1}(N_1 - 2)q^{k/2})$ & $2(N_1 - 1) \frac{q^k - 1}{N_1}^2$ \\
$\frac{h}{2} (q^k - (-1)^{\alpha+1}(N_1 - 1)q^{k/2})$ & $2^2 \frac{q}{N_1}$ \\
$\frac{h}{2} (q^k - (-1)\alpha q^{k/2})$ & $2(N_1 - 1) \frac{q^k - 1}{N_1}$ \\
$\frac{h}{2} (q^k - (-1)^{\alpha+1}(N_1 - 1)q^{k/2})$ & $(q^k - 1)^2$ \\
\hline
\end{tabular}
\caption{Table 2.}
\end{table}

Proof. Let $a = -(q - 1)/h$, and note that $h_{\alpha - \frac{k}{2} - 1}(x) = h_{\alpha + \frac{k}{2} - 1}(x)$. Since $N_1 < q^{k/2} + 1$, it is easy to see that $k$ is the smallest positive integer such that $aeq^k \equiv ae \pmod{q^k - 1}$. Thus, deg$(h_{ae}(x)) = k$, and by Lemma 3.4, $h_\alpha(x)$ and $h_{\alpha + \frac{k}{2} - 1}(x)$ are two different polynomials of degree $k$. Now, since $ae|(q - 1)$, $\gcd(q^k - 1, ae) = -ae$, and $n = (q^k - 1)/\gcd(q^k - 1, ae) = \frac{h(q^k - 1)}{2(q - 1)}$. Thus, $C = \mathcal{M}(a, e)$, and it is an $[h(q^k - 1)/2, q - 1]$ cyclic code. By Theorem 4.1, and since $ae|(q - 1)$, $N' = \gcd(q^k - 1, ae)/(q^k - 1) = \gcd(k, ae) = N_1$, $f/2 = j$, $s = \alpha$, and $n = \frac{h(q^k - 1)}{2(q - 1)}$. Thus, due to Part (b) of Theorem 4.1, the weight enumerator polynomial $C$ is:

\begin{equation}
1 + \frac{(q^k - 1)(N_1 - 1)}{N_1} z^{h(q^k - 1) + \frac{k}{2}} + \frac{q^k - 1}{N_1} z^{h(q^k - (\alpha + 1)q^{k/2})}
\end{equation}

which is in complete accordance with Table 2. Furthermore, note that Table 2 becomes Table 1 if $\alpha$ is odd. Therefore, note that the condition “If $\alpha$, $p$ and $(p^2 + 1)/N_1$ are all odd”, in Part (a) of Theorem 5.1, is excessive and unnecessary, and it can be changed simply by “If $\alpha$ odd”.

It is quite important to note that, by using our proof, it was not necessary to assume that $2(q - 1)/hN_1$ is odd, and this is because the case when $2(q - 1)/hN_1$ is even is addressed by Theorem 8 in [2], and both Theorems 7 and 8 describe RCCs whose WD is given by (1) (in fact, taking $\gamma = \alpha$, note that Tables III and IV in [2] are exactly the same as Tables 1 and 2, respectively).

The following family of codes has been also studied recently.
Theorem 5.2 ([11], Theorem 7). Let $a$, $e$ and $\delta$ be integers such that $e \geq 2$, $\delta | (q^k - 1)$, and $\delta = \gcd(q^k - 1, a, a + q^k - 1, \ldots, a + q^k - 1(e - 1))$. If $\gcd(q^k - 1, ae) = 1$ and the $e$ polynomials $h_a(x), h_{a + q^k - 1}(x), \ldots, h_{a + q^k - 1(e - 1)}(x)$ have degree $k$ and are pairwise relatively prime polynomials, then the cyclic code $C$, whose parity check polynomial is $\prod_{i=0}^{e-1} h_{a + q^k - 1(i)}(x)$, is a $\left(\frac{q^k - 1}{\delta}, ek, \frac{(q^k - 1)^{k - 1}}{e\delta}\right)$ $e$-weight cyclic code. The WD of $C$ is listed in Table 3.

Again, we use Theorem 4.1 in order to present a simpler proof.

Proof. Clearly $C = \mathfrak{M}(a, e)$, and $\deg(h_{ae}(x)) = k$ by Lemma 3.4. Since $\gcd(q^k - 1, ae) = e\delta$, the ICC $\mathcal{E}_{(ae)}$ has length $n = \frac{(q^k - 1)}{\gcd(q^k - 1, ae)} = (q^k - 1)/(e\delta)$. Now, in accordance with Theorem 4.1, $N' = \gcd(q^k - 1, ae)/(q^k - 1) = 1$. Thus, due to Part (a) of Theorem 4.1, $C$ is a $\left(\frac{q^k - 1}{\delta}, ek\right)$ cyclic code whose weight enumerator polynomial is:

$$
\left(1 + (q^k - 1)z^{\frac{(q^k - 1)^{k - 1}}{e\delta}}\right)^e
$$

which is in complete accordance with Table 3.

In a very similar way, it is possible to use Theorem 4.1 in order to almost directly obtain the WDs for the codes of the form $\mathfrak{M}(a, e)$, studied in Cases 1), 2) and 4) of the Concluding Remarks in [2, p. 8005], all the cases studied in [5, 7], Case 1) of the Conclusion in [11, p. 5992] (except when $N = 3$), and the family of codes studied in [12].

Now, it is important to note that an imposed restriction about the aforementioned cases is that the parity check polynomial $m_{(a, e)}(x)$, of $\mathfrak{M}(a, e)$, must be the product of irreducible polynomials of the same degree $k$ (see, for example, Main Assumptions in [11, p. 5985]). However, Theorems 3.2 and 4.1 reveal that we can get rid of this restriction in the sense that, in spite of $m_{(a, e)}(x)$, it is always possible to obtain the WD of $\mathfrak{M}(a, e)$ in terms of the WD of the ICC $\mathcal{E}_{(ae)}$. Particularly, if $\mathcal{E}_{(ae)}$ is either a one-weight ICC or a semiprimitive two-weight ICC, then the WD of $\mathfrak{M}(a, e)$ is determined via Theorem 4.1. In order to show this, consider the following:

Example 1. Let $p = q = 3$, $k = 6$, $a = 26$, and $e = 7$. Note that $l = 2$ is the smallest positive integer such that $aeq^{l-1} \equiv ae (\mod q^l - 1)$, therefore, $\deg(h_{ae}(x)) = 2$, $n = (q^k - 1)/\gcd(q^k - 1, ae) = 4$, and $N' = \gcd(q^k - 1, ae)/(q^k - 1) = 2$. Thus, due to Part (b) of Theorem 4.1, $\mathfrak{M}(a, e)$ is a [28, 14] cyclic code, whose weight enumerator polynomial is $(1 + 4z^2 + 4z^4)^7$. However, due to Lemma 3.4, the polynomial $m_{(a, e)}(x)$ is not the product of 7 irreducible polynomials of degree 6. In fact, if $F_{p^5} = F_3(\gamma), \gamma^6 + \gamma + 2 = 0$, then $m_{(a, e)}(x) = h_{26}(x)h_{130}(x)h_{542}(x) = (x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + 1)(x^2 + 2x^5 + 2x^3 + 2x + 1)(x^2 + 1) = \gamma^7 + 1 = h_{ae}(x^e)$, with $h_{234}(x) = h_{650}(x) = h_{26}(x)$, and $h_{332}(x) = h_{442}(x) = h_{130}(x)$. 

---

### Table 3.

| Weight | Frequency $(0 \leq u \leq e)$ |
|--------|-----------------------------|
| $\frac{(q^k - 1)^{u}}{\delta}$ | $\left(\frac{q^k - 1}{\delta}\right)(q^k - 1)^u$ |

---
6. Conclusions

In this work, we have seen that the problem of determining the WD of the codes of the form $\mathfrak{M}(a, e)$ can always be reduced to the problem of determining the WD of the ICC $\mathfrak{C}_{(ae)}$ (Theorem 3.2). We have also shown that it is possible to obtain, almost directly, the WD of all cyclic codes of the form $\mathfrak{M}(a, e)$, when $\mathfrak{C}_{(ae)}$ is either a one-weight ICC, or a semiprimitive two-weight ICC (see Theorem 4.1). We also proved that, in spite of the degree of the irreducible factors of $m_{(a,e)}(x)$, it is always possible to obtain the WD of $\mathfrak{M}(a, e)$ in terms of the WD of the ICC $\mathfrak{C}_{(ae)}$.

Finally, we want to emphasize that most of the recent works that study the family of codes of the form $\mathfrak{M}(a, e)$ resort to sophisticated techniques and tools (such as exponential sums, Gaussian periods, cyclotomic numbers, etc.), in order to obtain the possible WDs. In clear contrast, this work shows that, for such purpose, only two characterizations for some ICCs (Theorems 2.1 and 2.2) and an already known identity among the WD of some cyclic codes (Theorem 2.3) are needed.

Acknowledgments

The authors would like to express their gratitude to the anonymous referees for their valuable suggestions.

References

[1] C. S. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inform. Theory, 55 (2009), 955–960.
[2] C. S. Ding, Y. Liu, C. L. Ma and L. W. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inform. Theory, 57 (2011), 8000–8006.
[3] T. Kløve, The weight distribution for a class of ICCs, Discrete Mathematics, 20 (1977), 87–90.
[4] R. Lidl and H. Niederreiter, Finite Fields, Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.
[5] C. L. Ma, L. W. Zeng, Y. Liu, D. G. Feng and C. S. Ding, The weight enumerator of a class of cyclic codes, IEEE Trans. Inform. Theory, 57 (2011), 397–402.
[6] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. II, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
[7] G. Vega and L. B. Morales, A general description for the weight distribution of some reducible cyclic codes, IEEE Trans. Inform. Theory, 59 (2013), 5994–6001.
[8] G. Vega, A critical review and some remarks about one- and two-weight irreducible cyclic codes, Finite Fields and Their Appl., 33 (2015), 1–13.
[9] G. Vega, An improved method for determining the weight distribution of a family of $q$-ary cyclic codes, Applicable Algebra in Engineering, Communication and Computing, 28 (2017), 527–533.
[10] J. Wolfmann, Are 2-weight projective cyclic codes irreducible?, IEEE Trans. Inform. Theory, 51 (2005), 733–737.
[11] J. Yang, M. S. Xiong, C. S. Ding and J. Q. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory, 59 (2013), 5985–5993.
[12] L. Yu and H. W. Liu, The weight distribution of a family of $p$-ary cyclic codes, Des. Codes Cryptogr., 78 (2016), 731–745.

Received November 2018; 1st revision December 2018; final revision October 2019.

E-mail address: gerardov@unam.mx
E-mail address: elisandro@ciencias.unam.mx