J. Algebra Comb. Discrete Appl.
10(2) • 87–96

Received: 16 March 2021
Accepted: 31 October 2022

Journal of Algebra Combinatorics Discrete Structures and Applications

Lee weight distributions of trace codes over $\mathbb{F}_q + u\mathbb{F}_q$ from irreducible cyclic codes

Research Article

Gerardo Vega

Abstract: The construction of two or few-weight codes from trace codes over the ring $\mathbb{F}_q + u\mathbb{F}_q$, where $u^2 = 0$, was recently presented in [4]. For such construction, the defining sets for the trace codes are given in terms of cyclotomic classes, and for some of these classes, it is shown that it is possible to obtain the Lee weight distributions of the corresponding trace codes. Motivated by this construction, and by the p-ary semiprimitive irreducible cyclic codes over a prime field $\mathbb{F}_p$, the Lee weight distributions of an infinite family of p-ary three-weight codes from trace codes over the ring $\mathbb{F}_p + u\mathbb{F}_p$, was recentely found in [11]. In this work, we prove that the Lee weight distribution problem for the trace codes constructed in accordance with either [4] or [11], is equivalent to the weight distribution problem for the irreducible cyclic codes. With this equivalence in mind, and by using the already known weight distributions of an infinite family of irreducible cyclic codes (semiprimitive and not semiprimitive), we follow the open problem suggested in the Conclusion of [11] to determine the Lee weight distribution of an infinite family of trace codes over the ring $\mathbb{F}_q + u\mathbb{F}_q$, that includes the infinite family found in [11].

2010 MSC: 94B15 · 11T71

Keywords: Codes over a ring, Trace codes, Semiprimitive codes and cyclotomic classes, Irreducible cyclic codes

1. Introduction

Consider the ring $R = \mathbb{F}_q + u\mathbb{F}_q$, with $u^2 = 0$, and, for any positive integer m, the ring extension $\mathfrak{R} = \mathbb{F}_{q^m} + u\mathbb{F}_{q^m}$. A *trace code*, $\mathfrak{C}_L$, with *defining set* $L = \{d_1, d_2, \cdots, d_n\} \subseteq \mathfrak{R}^*$ is defined by

$$\mathfrak{C}_L = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \cdots, \mathrm{Tr}(xd_n)) \mid x \in \mathfrak{R}\} , \tag{1}$$

where $\mathfrak{R}^*$ is the group of units of $\mathfrak{R}$, and Tr is the *trace function* from $\mathfrak{R}$ to R defined as

Gerardo Vega; Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, Mexico (gerardov@unam.mx).

$$\mathrm{Tr}(a+ub)=\sum_{j=0}^{m-1}(a^{q^j}+ub^{q^j})\ .$$

For any $a,b\in\mathbb{F}_{q^m}$. It is clear that

$$\mathrm{Tr}(a+ub)=\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a)+u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b)\ ,$$

where "$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$" denotes the standard *trace mapping* from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Note that $\mathfrak{C}_L$ is a linear code over R of length n, that is $\mathfrak{C}_L$ is a particular kind of R-submodule of R^n.

In analogy to the ring $\mathbb{Z}_4$, the Gray map ϕ from R to $\mathbb{F}_q^2$ is defined by

$$\phi(a+ub)=(b,a+b)\ ,\ \text{for all } a,b\in\mathbb{F}_q\ .$$

This map is extended naturally into a map from R^n to $\mathbb{F}_q^{2n}$.

Remark 1.1. *The* Lee weight, *w_L, over R^n is defined in terms of the standard* Hamming weight, *w_H, of the Gray image as follows*

$$w_L(a+ub)=w_H(b)+w_H(a+b)\ ,\ \textit{for all } a,b\in\mathbb{F}_q^n\ .$$

Similar to the *Hamming distance*, d_H, the *Lee distance*, d_L, over R^n is defined as $d_L(x,y)=w_L(x-y)$ for all $x,y\in R^n$. Moreover if $x=a_1+ub_1$ and $y=a_2+ub_2$, then $d_L(x,y)=w_H(b_1-b_2)+w_H(a_1-a_2+b_1-b_2)=w_H(b_1-b_2,a_1-a_2+b_1-b_2)=w_H((b_1,a_1+b_1)-(b_2,a_2+b_2))=d_H(\phi(x),\phi(y))$. Thus ϕ is a distance-preserving map or isometry from (R^n,d_L) to $(\mathbb{F}_q^{2n},d_H)$.

We recall that the *Hamming weight enumerator*, $\mathrm{Ham}_{\mathfrak{C}}(z)$, of a linear code $\mathfrak{C}$ of length n over a finite field is defined as the polynomial $\mathrm{Ham}_{\mathfrak{C}}(z)=\sum_{j=0}^{n}A_jz^j$, where A_j $(0\le j\le n)$ denote the number of codewords with Hamming weight j in the code $\mathfrak{C}$. The sequence $(A_0=1,A_1,\cdots,A_n)$ is called *the weight distribution* of the code. In a similar way for a trace code $\mathfrak{C}_L$, defined through (1), let A_j $(0\le j\le 2n)$ be the number of codewords with Lee weight j in the linear code $\mathfrak{C}_L$ of length n over R, then the *Lee weight enumerator* of $\mathfrak{C}_L$, $\mathrm{Lee}_{\mathfrak{C}_L}(z)$, is defined by $\mathrm{Lee}_{\mathfrak{C}_L}(z)=\sum_{j=0}^{2n}A_jz^j$.

Through different choices of the defining set L, and particularly when $\mathbb{F}_q$ is either the binary field $(\mathbb{F}_2)$ or a prime field $(\mathbb{F}_p)$, several optimal or nearly optimal codes from trace codes of the form $\mathfrak{C}_L$ where recently found ([4, 5, 8, 9, 11–16]). Particularly, the construction of two or few-weight codes from trace codes over the ring $\mathbb{F}_q+u\mathbb{F}_q$, was recently presented in [4]. For such construction, the defining sets for the trace codes are given in terms of cyclotomic classes, and for some of these classes, it is shown that it is possible to obtain the Lee weight distributions of the corresponding trace codes. Motivated by this construction, and by the p-ary semiprimitive irreducible cyclic codes over a prime field $\mathbb{F}_p$, the Lee weight distributions of an infinite family of p-ary three-weight codes from trace codes over the ring $\mathbb{F}_p+u\mathbb{F}_p$, was recently constructed in [11].

One of the purposes of this work is to show that there exists a direct identity between Lee weight enumerators of the trace codes constructed by [4], [8], [9] and [11], and the Hamming weight enumerators of the irreducible cyclic codes. In other words, we are going to prove that the Lee weight distribution problem for the trace codes constructed following [4], [8], [9] or [11], is equivalent to the standard Hamming weight distribution problem for the irreducible cyclic codes. With this equivalence in mind, we then follow the open problem suggested in the Conclusion of [11], and determine the Lee weight distribution of trace codes of the form $\mathfrak{C}_L$ in terms of other class of irreducible cyclic codes, with known or well-understood weight distribution. For this purpose, we use the already known weight distributions of an infinite family irreducible cyclic codes (semiprimitive and not semiprimitive, [17]), to determine the Lee weight distribution of a new infinite family of trace codes of the form $\mathfrak{C}_L$, that includes the infinite family constructed in [11].

This work is organized as follows: In Section 2, we set up some new notations and recall some definitions, particularly those related with the irreducible cyclic codes. Section 3 will show the relationship between the Lee weight distribution problem for some trace codes and the Hamming weight distribution problem for the irreducible cyclic codes. In Section 4, it is shown that all the Lee weight distributions reported in [4], [8], [9], and [11] can be obtained easily as particular instances of such relationship, which gives us a simplified view for all these Lee weight distributions. In Section 5 we use the already known weight distributions of an infinite family irreducible cyclic codes to determine the Lee weight distribution of a new infinite family of trace codes. Finally, Section 6 is devoted to conclusions.

2. Background material

Let $\mathbb{F}_q$ be a finite field of order q, where $q = p^t$ for some prime p and for some positive integer t. A subset $\mathfrak{C}$ of vectors or codewords in $\mathbb{F}_q^n$ is called an $[n, l]$ *linear code* over $\mathbb{F}_q$ if $\mathfrak{C}$ is an l-dimensional subspace of $\mathbb{F}_q^n$: n is called the *length* and l is called the *dimension* of $\mathfrak{C}$.

An M-*weight* code (either over a finite field or over a ring) is a code such that the cardinality of the set of nonzero weights is M.

A linear code $\mathfrak{C}$ over a finite field $\mathbb{F}_q$ of length n, is *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathfrak{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathfrak{C}$. 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 the 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 $\mathfrak{C}$ of length n over $\mathbb{F}_q$ corresponds to a subset of the residue class ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Moreover, it is well known that the linear code $\mathfrak{C}$ is cyclic if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ (see for example [3, Theorem 9.36]).

Now, note that every ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is principal. In consequence, if $\mathfrak{C}$ is a cyclic code of length n over $\mathbb{F}_q$, then $\mathfrak{C} = \langle g(x)\rangle$, 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 $\mathfrak{C}$ ([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 $\mathfrak{C}$.

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]).

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 $\gcd(v, w) = 1$. 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 $\mathrm{ord}_v(w)$. From now on, m will denote a positive integer, and by using γ we will denote a fixed primitive element of $\mathbb{F}_{q^m}$. For any integer a, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the *minimal polynomial* of γ^{-a} ([3, Definition 1.81]). In addition, $\mathfrak{C}_{(a)}$ will denote the irreducible cyclic code whose parity check polynomial is $h_a(x)$. Note that $\mathfrak{C}_{(a)}$ is an $[n, l]$ linear code, where $n = \frac{q^m-1}{\gcd(q^m-1,a)}$, and $l = \deg(h_a(x)) = \mathrm{ord}_n(q)$ is a divisor of m. For any positive divisor e of $q^m - 1$ and for any $0 \le i \le e - 1$, we define $\mathfrak{D}_i^{(e,q^m)} := \gamma^i \langle \gamma^e \rangle$, where $\langle \gamma^e \rangle$ denotes the subgroup of $\mathbb{F}_{q^m}^*$ generated by γ^e. The cosets $\mathfrak{D}_i^{(e,q^m)}$ are called the *cyclotomic classes* of order e in $\mathbb{F}_{q^m}$.

An alternative definition for an irreducible cyclic code is as follows:

Definition 2.1. *[7, Definition 2.2] Let n be a positive divisor of $q^m - 1$, write $e = (q^m - 1)/n$, and let ω*

be a primitive n-th root of unity in $\mathbb{F}_{q^m}$. Then, an irreducible cyclic code of length n over $\mathbb{F}_q$, is the set

$$\{(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(y\omega^i))_{i=0}^{n-1} \mid y \in \mathbb{F}_{q^m}\} .$$

Remark 2.2. *Note that, thanks to Delsarte's Theorem (see for example [1]), the parity-check polynomial of the irreducible cyclic code under the previous definition is $h_{-e}(x)$, if $\omega = \gamma^e$.*

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 3 in [17], an irreducible cyclic code $\mathfrak{C}_{(a)}$ of dimension m over $\mathbb{F}_q$ is called *semiprimitive* if $\mu \geq 2$ and p is semiprimitive modulo μ, where $\mu = \gcd(\frac{q^m-1}{q-1}, a)$ (recall $q = p^t$).

3. A relationship between the Hamming and the Lee weight enumerators

Let n be a positive divisor of $q^m - 1$, and write $e = (q^m - 1)/n$. For each $\beta \in \mathbb{F}_{q^m}$ define $c(n, e, \beta)$ as the vector of length n over $\mathbb{F}_q$, given by

$$c(n, e, \beta) = (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta\gamma^{ei}))_{i=0}^{n-1} . \tag{2}$$

Now, since the elements γ^{ei} $(0 \leq i < n)$ are the n roots of the unity in $\mathbb{F}_{q^m}$, we have, in accordance with Definition 2.1, that the irreducible cyclic code $\mathfrak{C}_{(e)}$ can be described as

$$\mathfrak{C}_{(e)} = \{c(n, e, \beta) \mid \beta \in \mathbb{F}_{q^m}\} .$$

Remark 3.1. *$\mathfrak{C}_{(e)}$ is an irreducible cyclic code of length n, whose dimension will be m iff $\mathrm{ord}_n(q) = m$.*

We will now focus our attention on the trace codes of the form $\mathfrak{C}_L$, and for this purpose we are going to fix the defining set in terms of the cyclotomic class $\mathfrak{D}_0^{(e,q^m)}$, where e is any divisor of $q^m - 1$. Therefore, from now on $\mathfrak{C}_{L_e}$ will denote the trace code defined through (1), where the defining set $L_e = \mathfrak{D}_0^{(e,q^m)} + u\mathbb{F}_{q^m}$. Since, $|\mathfrak{D}_0^{(e,q^m)}| = \frac{q^m-1}{e}$, the length of trace code $\mathfrak{C}_{L_e}$ is $\frac{q^{2m}-q^m}{e}$. For $a \in \mathfrak{R}$ (recall $\mathfrak{R} = \mathbb{F}_{q^m} + u\mathbb{F}_{q^m}$) define the evaluation map $\mathrm{Ev}(a)$ as

$$\mathrm{Ev}(a) = (\mathrm{Tr}(ax))_{x \in L_e} .$$

Thus $\mathfrak{C}_{L_e} = \{\mathrm{Ev}(a) \mid a \in \mathfrak{R}\}$. Next, we will show that there exists a direct relationship between the Lee weight of some codewords in $\mathfrak{C}_{L_e}$ and the Hamming weight of the codewords in the irreducible cyclic code $\mathfrak{C}_{(e)}$.

Theorem 3.2. *Let n be a positive divisor of $q^m - 1$, and write $e = (q^m - 1)/n$. Consider $\mathfrak{C}_{L_e}$ and $\mathfrak{C}_{(e)}$ as before. Let $a \in \mathfrak{R}$, then*

(i) If $a = 0$, then $w_L(\mathrm{Ev}(a)) = 0$.

(ii) If $\beta \in \mathbb{F}_{q^m}^*$ and $a = u\beta$, then $w_L(\mathrm{Ev}(a)) = 2q^m w_H(c(n, e, \beta))$, where $c(n, e, \beta)$ is the codeword in $\mathfrak{C}_{(e)}$ given by (2).

(iii) If $\alpha \in \mathbb{F}_{q^m}^*$, $\beta \in \mathbb{F}_{q^m}$, and $a = \alpha + u\beta$, then $w_L(\mathrm{Ev}(a)) = 2\frac{q-1}{eq}(q^{2m} - q^m)$.

Proof. Part (i) is direct. Suppose that $a = u\beta$, for some $\beta \in \mathbb{F}_{q^m}^*$. Let $x = w + uw' \in L_e$, where $w \in \mathfrak{D}_0^{(e,q^m)}$ and $w' \in \mathbb{F}_{q^m}$. Therefore $ax = u\beta w$ and $\mathrm{Tr}(ax) = u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w)$. Taking Gray map yields

$$\begin{aligned}\phi(\mathrm{Ev}(a)) &= \phi((u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w))_{w,w'}) \\ &= (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w), \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w))_{w,w'} ,\end{aligned}$$

where $(u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w))_{w,w'}$ is the vector of length $\frac{q^{2m}-q^m}{e}$ whose elements are all possible evaluations of $u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w)$ by taking $w' \in \mathbb{F}_{q^m}$ and $w \in \mathfrak{D}_0^{(e,q^m)} = \langle\gamma^e\rangle$ (in a similar way for $(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w), \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w))_{w,w'}$) . Now, by considering Remark 1.1, we have

$$\begin{aligned}w_L(\mathrm{Ev}(a)) &= 2w_H((\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w))_{w,w'}) \\ &= 2q^m w_H((\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta w))_w) \\ &= 2q^m w_H((\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta\gamma^{ei}))_{i=0}^{n-1}) \\ &= 2q^m w_H(c(n,e,\beta)) ,\end{aligned}$$

where the last equality comes from (2). Lastly, suppose $a = \alpha + u\beta \in \mathfrak{R}^*$, with $\alpha \in \mathbb{F}_{q^m}^*$ and $\beta \in \mathbb{F}_{q^m}$. Let $x = w + uw' \in L_e$, where $w \in \mathfrak{D}_0^{(e,q^m)}$ and $w' \in \mathbb{F}_{q^m}$. Therefore, $ax = \alpha w + u(\alpha w' + \beta w)$ and $\mathrm{Tr}(ax) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w) + u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w)$. Taking Gray map yields

$$\begin{aligned}\phi(\mathrm{Ev}(a)) &= \phi((\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w) + u\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w))_{w,w'}) \\ &= (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w), \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w + \alpha w))_{w,w'} .\end{aligned}$$

By considering Remark 1.1 again,

$$w_L(\mathrm{Ev}(a)) = w_H((\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w), \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w + \alpha w))_{w,w'}) .$$

Thus the Lee weight of the codeword $\mathrm{Ev}(a) \in \mathfrak{C}_{L_e}$ is equal to $2\frac{q^{2m}-q^m}{e} - Z(a)$, where

$$\begin{aligned}Z(a) = \ &\sharp\{(w,w') \in \mathfrak{D}_0^{(e,q^m)} \times \mathbb{F}_{q^m} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w) = 0\} + \\ &\sharp\{(w,w') \in \mathfrak{D}_0^{(e,q^m)} \times \mathbb{F}_{q^m} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha w' + \beta w + \alpha w) = 0\} .\end{aligned}$$

If χ' and χ are, respectively, the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ (see for example [3, Chapter 5]), then χ' and χ are related by $\chi'(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\varepsilon)) = \chi(\varepsilon)$ for all $\varepsilon \in \mathbb{F}_{q^m}$. Therefore

$$\begin{aligned} Z(a) &= \frac{1}{q} \sum_{w \in \mathfrak{D}_0^{(e,q^m)}} \sum_{w' \in \mathbb{F}_{q^m}} \sum_{s \in \mathbb{F}_q} \chi'(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s(\alpha w' + \beta w))) + \\ &\quad \frac{1}{q} \sum_{w \in \mathfrak{D}_0^{(e,q^m)}} \sum_{w' \in \mathbb{F}_{q^m}} \sum_{s \in \mathbb{F}_q} \chi'(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s(\alpha w' + \beta w + \alpha w))) \\ &= 2\frac{q^{2m} - q^m}{eq} + \frac{1}{q} \sum_{w \in \mathfrak{D}_0^{(e,q^m)}} \sum_{s \in \mathbb{F}_q^*} \chi(s\beta w) \sum_{w' \in \mathbb{F}_{q^m}} \chi(s\alpha w') + \\ &\quad \frac{1}{q} \sum_{w \in \mathfrak{D}_0^{(e,q^m)}} \sum_{s \in \mathbb{F}_q^*} \chi(s(\beta w + \alpha w)) \sum_{w' \in \mathbb{F}_{q^m}} \chi(s\alpha w') \\ &= 2\frac{q^{2m} - q^m}{eq} , \end{aligned}$$

because $\sum_{w' \in \mathbb{F}_{q^m}} \chi(s\alpha w') = 0$. Thus $w_L(\mathrm{Ev}(a)) = 2\frac{q-1}{eq}(q^{2m} - q^m)$. □

The previous theorem strongly suggests the existence of a relationship between Hamming and the Lee weight enumerators. We establish this result by means of the following:

Corollary 3.3. *With our current notation, let n be a positive divisor of $q^m - 1$ such that $\mathrm{ord}_n(q) = m$. Fix $e = (q^m - 1)/n$. Let $\mathrm{Ham}_{\mathfrak{C}_{(e)}}(z)$ and $\mathrm{Lee}_{\mathfrak{C}_{L_e}}(z)$ be, respectively, the Hamming and the Lee weight enumerators of $\mathfrak{C}_{(e)}$ and $\mathfrak{C}_{L_e}$. Then the Gray image of $\mathfrak{C}_{L_e}$ is a code over $\mathbb{F}_q$ of length $2\frac{q^{2m}-q^m}{e}$ and size q^{2m}. Furthermore, the Lee weight enumerator of $\mathfrak{C}_{L_e}$ (and therefore the Hamming weight enumerator of its Gray image) is*

$$\mathrm{Lee}_{\mathfrak{C}_{L_e}}(z) = \mathrm{Ham}_{\mathfrak{C}_{(e)}}(z^{2q^m}) + (q^{2m} - q^m) z^{2\frac{q-1}{eq}(q^{2m}-q^m)} . \tag{3}$$

Proof. This is a direct consequence of Theorem 3.2 and Remark 3.1. □

What (3) is saying is that if $\mathfrak{C}_{(e)}$ is an M-weight code, then the trace code $\mathfrak{C}_{L_e}$ (or alternatively its Gray image) is an $(M+1)$-weight code. As elaborated below, this property and particularly (3), is in complete accordance with the Lee weight enumerators recently reported in [4], [8], [9] and [11].

4. In perspective with some already reported Lee weight distributions

Let q and n be as before, and suppose that $\gcd(q, n) = 1$. Just by looking at the length n it is possible to determine the existence or nonexistence of either a one-weight or a semiprimitive two-weight irreducible cyclic code of dimension $\mathrm{ord}_n(q)$ over any finite field $\mathbb{F}_q$. We recall such characterization by means of the following:

Theorem 4.1. *[17, Theorem 4] Let n and m be positive integers, such that $\gcd(n, q) = 1$ and $m = \mathrm{ord}_n(q)$. Fix $e = (q^m - 1)/n$ and $\mu = \gcd(\frac{q^m-1}{q-1}, e)$. Then, either there exists a one-weight, or a semiprimitive two-weight irreducible cyclic code $\mathfrak{C}_{(e)}$ of length n, and dimension m iff $\mu = 1$, or p is semiprimitive modulo μ. If such code exists then its Hamming weight enumerator is*

$$1 + \frac{(q^m - 1)}{\mu}((\mu - 1) z^{\frac{(q-1)q^{m/2}}{eq}(q^{m/2} - (-1)^s)} + z^{\frac{(q-1)q^{m/2}}{eq}(q^{m/2} + (-1)^s(\mu - 1))}) ,$$

where $s = (mt)/\mathrm{ord}_\mu(p)$ *(recall that* $q = p^t$*).*

From previous theorem note that if $\mu = 1$, then $e \mid (q-1)$, and $\mathfrak{C}_{(e)}$ is a one-weight irreducible cyclic code of length n and dimension m, whose Hamming weight enumerator is $\mathrm{Ham}_{\mathfrak{C}_{(e)}}(z) = 1+(q^m-1)z^{\frac{q-1}{eq}q^m}$. But if $e \mid (q-1)$ then it is easy to see that $\gcd(m, e) = \gcd(\frac{q^m-1}{q-1}, e) = \mu = 1$, and the condition in [4, Theorem 3.3] is fulfilled. This, of course, is right because Corollary 3.3 tells us that $\mathfrak{C}_{L_e}$ is a two-weight trace code of length $\frac{q^{2m}-q^m}{e}$ over R, whose Lee weight enumerator is

$$\begin{aligned}\mathrm{Lee}_{\mathfrak{C}_{L_e}}(z) &= \mathrm{Ham}_{\mathfrak{C}_{(e)}}(z^{2q^m}) + (q^{2m}-q^m)z^{2\frac{q-1}{eq}(q^{2m}-q^m)} \\ &= 1 + (q^m-1)z^{2\frac{q-1}{eq}q^{2m}} + (q^{2m}-q^m)z^{2\frac{q-1}{eq}(q^{2m}-q^m)} \ ,\end{aligned}$$

which is the same Lee weight enumerator reported in [4, Theorem 3.3].

If $\mu = 2$ in Theorem 4.1, then q and p are an odd integers. Therefore, clearly, p is semiprimitive modulo μ. Thus, $\mathfrak{C}_{(e)}$ is a two-weight irreducible cyclic code of length n and dimension m, whose Hamming weight enumerator is

$$\mathrm{Ham}_{\mathfrak{C}_{(e)}}(z) = 1 + \frac{(q^m-1)}{2}(z^{\frac{(q-1)(q^m-q^{m/2})}{eq}} + z^{\frac{(q-1)(q^m+q^{m/2})}{eq}}) \ ,$$

and by Corollary 3.3, $\mathfrak{C}_{L_e}$ is a three-weight trace code of length $\frac{q^{2m}-q^m}{e}$ over R, whose Lee weight enumerator is

$$\begin{aligned}\mathrm{Lee}_{\mathfrak{C}_{L_e}}(z) &= 1 + \frac{(q^m-1)}{2}(z^{\frac{2(q-1)(q^{2m}-q^{3m/2})}{eq}} + z^{\frac{2(q-1)(q^{2m}+q^{3m/2})}{eq}}) + \\ &\quad (q^{2m}-q^m)z^{2\frac{q-1}{eq}(q^{2m}-q^m)} \ ,\end{aligned}$$

which is the same Lee weight enumerator reported in [4, Theorem 3.7]. In fact, in the particular case when $e = 2$, $\mu = \gcd(\frac{q^m-1}{q-1}, e) = 2$. That is, in this case, we have $(\mu = e = 2) | (p-1)$ and $\mathfrak{D}_0^{(2,q^m)} = \mathfrak{Q}$, where $\mathfrak{Q}$ is the set of all square elements of $\mathbb{F}_{q^m}^*$. Therefore, as is correctly pointed out in [4, Remark 3.8], [9, Theorem 1] is a special case of [4, Theorem 3.7].

Now, suppose that $q = p$ and that $e > 2$ is an integer such that $e \mid p^r + 1 \mid p^m - 1$, for some integer r, and let l be the smallest integer such that $e \mid p^l + 1$. But, under these conditions, it is easy to see that $2l \mid m$, and therefore $\mu = \gcd(\frac{p^m-1}{p-1}, e) = e$, and $\mathrm{ord}_\mu(p) = 2l$. Thus, Theorem 4.1 tell us that $\mathfrak{C}_{(e)}$ is a two-weight irreducible cyclic code over the prime field $\mathbb{F}_p$, of length $\frac{p^m-1}{e}$ and dimension m, whose Hamming weight enumerator, $\mathrm{Ham}_{\mathfrak{C}_{(e)}}(z)$, is

$$1 + \frac{(p^m-1)}{e}((e-1)z^{\frac{(p-1)p^{m/2}}{ep}(p^{m/2}-(-1)^{\frac{m}{2l}})} + z^{\frac{(p-1)p^{m/2}}{ep}(p^{m/2}+(-1)^{\frac{m}{2l}}(e-1))}) \ ,$$

and by Corollary 3.3, $\mathfrak{C}_{L_e}$ is a three-weight trace code of length $\frac{p^{2m}-p^m}{e}$ over the prime ring $R = \mathbb{F}_p + u\mathbb{F}_p$, whose Lee weight enumerator is

$$\begin{aligned}\mathrm{Lee}_{\mathfrak{C}_{L_e}}(z) &= 1 + \frac{(p^m-1)}{e}[(e-1)z^{\frac{2(p-1)p^{3m/2}}{ep}(p^{m/2}-(-1)^{\frac{m}{2l}})} + \\ &\quad z^{\frac{2(p-1)p^{3m/2}}{ep}(p^{m/2}+(-1)^{\frac{m}{2l}}(e-1))}] + \\ &\quad (p^{2m}-p^m)z^{2\frac{p-1}{ep}(p^{2m}-p^m)} \ ,\end{aligned}$$

which is the same Lee weight enumerator reported in [11, Table 1] (in such table $N = e$).

Note that the conditions $e \mid (q-1)$ or $\mu = e$ are quite restrictive, but fortunately Theorem 4.1 tells us that we can get rid of it, and we show this by means of the following:

Example 4.2. *Let $q = p = 5$ and $n = 3$. Then $m = \mathrm{ord}_3(5) = 2$, $e = (p^2-1)/3 = 8$, and $\mu = \gcd(\frac{p^2-1}{p-1}, e) = 2$. By Theorem 4.1, $\mathfrak{C}_{(8)}$ is a two-weight irreducible cyclic code over $\mathbb{F}_5$, of length 3 and dimension 2, whose Hamming weight enumerator is $\mathrm{Ham}_{\mathfrak{C}_{(8)}}(z) = 1 + 12z^2 + 12z^3$. Now, by Corollary 3.3, the Gray image of $\mathfrak{C}_{L_8}$ is a three-weight code over the prime field $\mathbb{F}_5$, of length $2\frac{p^{2m}-p^m}{e} = 150$, and size $p^{2m} = 625$, whose Hamming weight enumerator is $\mathrm{Lee}_{\mathfrak{C}_{L_8}}(z) = 1 + 12z^{100} + 12z^{150} + 600z^{120}$.*

In this example, in addition that $e \nmid (q-1)$ and $e \neq \mu$, also note that $(e = 8) \nmid 5^r + 1$, for any positive integer r. Therefore the three-weight trace code in Example 4.2 is new in the context of [4], [9] and [11], but not the binary case of [8].

Up to now we used Theorem 4.1 to construct two or three-weight trace codes of the form $\mathfrak{C}_{L_e}$. In fact, since Theorem 4.1 is a characterization, there are no others two or three-weight trace codes of the form $\mathfrak{C}_{L_e}$. However, as is outlined below, it possible to construct M-weight trace codes of the form $\mathfrak{C}_{L_e}$, with $M > 3$.

Let e be a divisor of $q^m - 1$. Suppose that $\mu = \gcd(m, e) = \gcd(\frac{q^m-1}{q-1}, e) = 3$, and that $p \equiv 1 \pmod 3$ (that is p is not semiprimitive modulo μ). Under these conditions, and with the help of [2, Theorem 18], $\mathfrak{C}_{(e)}$ is a three-weight irreducible cyclic code over $\mathbb{F}_q$, of length $\frac{q^m-1}{e}$ and dimension m, whose Hamming weight enumerator is

$$1 + \frac{q^m-1}{3}(z^{\frac{(q-1)(q^m - c_1 q^{\frac{m}{3}})}{eq}} + z^{\frac{(q-1)(q^m - \frac{1}{2}(c_1 - 9d_1)q^{\frac{m}{3}})}{eq}} + z^{\frac{(q-1)(q^m - \frac{1}{2}(c_1 + 9d_1)q^{\frac{m}{3}})}{eq}}) ,$$

where c_1 and d_1 are uniquely given by $4q^{m/3} = c_1^2 + 27d_1^2$, $c_1 \equiv 1 \pmod 3$ and $\gcd(c_1, p) = 1$. Through a direct application of Corollary 3.3, over the earlier Hamming weight enumerator, it is easy to see that $\mathfrak{C}_{L_e}$ is a four-weight trace code, whose Lee weight enumerator is precisely the Lee weight distribution reported in the first part of [4, Table II]. In a quite similar way, it is easy to see that the Lee weight distribution reported in the first part of [4, Table III], is just the result of direct application of Corollary 3.3 over the Hamming weight enumerator reported in [2, Theorem 20].

Lastly, note that the families of codes in the second parts of [4, Table II and Table III] are three-weight trace codes that come, as we already explained above, from two-weight semiprimitive irreducible cyclic codes.

5. The Lee weight distribution of an extended family of trace codes over $\mathbb{F}_q + u\mathbb{F}_q$

We are now going to follow the open problem suggested in the Conclusion of [11], and determine the Lee weight distribution of trace codes of the form $\mathfrak{C}_{L_e}$ in terms of other class of irreducible cyclic codes, with known or well-understood weight distribution. For this purpose, we recall the following result.

Theorem 5.1. *[17, Theorem 10] Let n, m and r be three positive integers, such that $\gcd(n, q) = 1$, $m = \mathrm{ord}_n(q)$, and $r \geq 1$. If $r \geq 2$, suppose that the prime factors of r divide n but not $(q^m-1)/n$, and that $q^m \equiv 1 \pmod 4$, if $4 \mid r$. Fix $\mu = \gcd(\frac{q^m-1}{q-1}, \frac{q^m-1}{n})$. Assume also that $\mu = 1$ or p is semiprimitive modulo μ. Then, the weight enumerator polynomial of any $[nr, mr]$ irreducible cyclic code is*

$$(1 + \frac{(q^m-1)}{\mu}((\mu-1)z^{\frac{(q-1)q^{m/2}}{eq}(q^{m/2}-(-1)^s)} + z^{\frac{(q-1)q^{m/2}}{eq}(q^{m/2}+(-1)^s(\mu-1))}))^r ,$$

where $s=(mt)/\mathrm{ord}_\mu(p)$.

Combining previous theorem with Corollary 3.3 we get:

Theorem 5.2. *Let* n*,* m *and* r *be three positive integers, such that* $\gcd(n,q)=1$*,* $m=\mathrm{ord}_n(q)$*, and* $r\geq 1$*. If* $r\geq 2$*, suppose that the prime factors of* r *divide* n *but not* $(q^m-1)/n$*, and that* $q^m\equiv 1 \pmod 4$*, if* $4\mid r$*. Fix* $\mu=\gcd(\frac{q^m-1}{q-1},\frac{q^m-1}{n})$*,* $e=\frac{q^m-1}{n}$*, and* $e'=\frac{q^{mr}-1}{nr}$*. Assume also that* $\mu=1$ *or* p *is semiprimitive modulo* μ*. Then the Gray image of* $\mathfrak{C}_{L_{e'}}$ *is a code over* $\mathbb{F}_q$ *of length* $2\frac{q^{2mr}-q^{mr}}{e'}$ *and size* q^{2mr}*. Furthermore, the Lee weight enumerator of* $\mathfrak{C}_{L_{e'}}$ *is*

$$\begin{aligned}&(1+\frac{(q^m-1)}{\mu}((\mu-1)z^{f(q)(q^{m/2}-(-1)^s)}+z^{f(q)(q^{m/2}+(-1)^s(\mu-1))}))^r+\\&(q^{2mr}-q^{mr})z^{2\frac{q-1}{e'q}(q^{2mr}-q^{mr})}\ ,\end{aligned}$$

where $s=(mt)/\mathrm{ord}_\mu(p)$*, and* $f(q)=\frac{2q^{mr}(q-1)q^{m/2}}{eq}$.

Proof. This is a direct consequence of Theorem 5.1 and Corollary 3.3. □

Example 5.3. *Let* $q=p=5$*,* $n=8$*, and* $r=2$*. Then* $m=ord_8(5)=2$*,* $\mu=\gcd(\frac{q^m-1}{q-1},\frac{q^m-1}{n})=3$*,* $e=\frac{q^m-1}{n}=3$*,* $e'=\frac{q^{mr}-1}{nr}=39$*,* $s=1$*, and clearly* p *is semiprimitive modulo* μ*, and* r *divide* n *but not* $(q^m-1)/n$*. Thus, the Gray image of* $\mathfrak{C}_{L_{39}}$ *is a five-weight code over the prime field* $\mathbb{F}_5$*, of length* $2\frac{q^{2mr}-q^{mr}}{e'}=20000$*, and size* $q^{2mr}=5^8$*, whose Hamming weight enumerator is* $\mathrm{Lee}_{\mathfrak{C}_{L_{39}}}(z)=(1+8z^{5000}+16z^{10000})^2+390000z^{16000}=1+16z^{5000}+96z^{10000}+256z^{15000}+390000z^{16000}+256z^{20000}$.

Finally, note that Theorem 5.1 includes all the semiprimitive irreducible cyclic codes, when $r=1$. Therefore, the new infinite family of trace codes of the form $\mathfrak{C}_{L_e}$, described in Theorem 5.2, includes the infinite family found in [11].

6. Conclusion

In this work, we showed that there exists an identity between Lee weight enumerators of the trace codes of the form $\mathfrak{C}_{L_e}$, and the Hamming weight enumerators of the irreducible cyclic codes of the form $\mathfrak{C}_{(e)}$. In other words, we proved that the Lee weight distribution problem for the trace codes constructed following [4], [8], [9] or [11], is equivalent to the standard Hamming weight distribution problem for the irreducible cyclic codes. In fact, this identity allowed us to present a simplified view for all the Lee weight distributions reported in these works. Finally, we used the already known weight distributions of an infinite family irreducible cyclic codes (semiprimitive and not semiprimitive), to determine the Lee weight distribution of a new infinite family of trace codes of the form $\mathfrak{C}_{L_e}$, that includes the infinite family found in [11].

As a future work, it could be interesting to explore the possible existence of an identity, like that in Corollary 3.3, for trace codes of the form $\mathfrak{C}_{L_e}$ when they are defined over a different ring (for example, a semi-local ring similar to that in [10]).

Acknowledgment: The author want to express his gratitude to the anonymous referee for his valuable suggestions.

References

[1] P. Delsarte, On subfield subcodes of Reed-Solomon codes, IEEE Trans. Inf. Theory 21(5) (1975) 575–576.

[2] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math. 313(4) (2013) 434–446.

[3] R. Lidl, H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, U.K. (1997).

[4] H. Liu, Y. Maouche, Two or few-weight trace codes over $\mathbb{F}_q + u\mathbb{F}_q$, IEEE Trans. Inf. Theory 65(5) (2019) 2696–2703.

[5] G. Luo, X. Cao, G. Xu, S. Xu, A new class of optimal linear codes with flexible parameters, Discrete Appl. Math. 237 (2018) 126–131.

[6] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, The Netherlands: North-Holland, Amsterdam (1977).

[7] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, Finite Fields and Their Appl. 8 (2002) 1–17.

[8] M. Shi, Y. Liu, P. Solé, Optimal two-weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Commun. Lett. 20(12) (2016) 2346–2349.

[9] M. Shi, R. Wu, Y. Liu, P. Solé, Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$, Cryptogr. Commun. 9(5) (2017) 637–646.

[10] M. Shi, Y. Guan, P. Solé, Two new families of two-weight codes, IEEE Trans. Inf. Theory 63(10) (2017) 6240–6246.

[11] M. Shi, T. Helleseth, P. Solé, Three-weight codes from semiprimitive irreducible cyclic codes, Preprint, 2019.

[12] M. Shi, Y. Guan, C. Wang, P. Solé, Few-weight codes from trace codes over R_k, Bulletin of the Australian Mathematical Society, 98(1) (2018) 167–174.

[13] M. Shi, Y. Liu, P. Solé, Optimal binary codes from trace codes over a non-chain ring, Discrete Applied Mathematics 219 (2017) 176–181.

[14] M. Shi, L. Qian, P. Solé, Few-weight codes from trace codes over a local ring, Applicable Algebra Eng. Commun. Computin. 29 (2018) 335–350.

[15] M. Shi, H. Zhu, P. Solé, Optimal three-weight cubic codes, Appl. Comput. Math. 17(2) (2018) 175–184.

[16] M. Shi, R. Wu, L. Qian, L. Sok, P. Solé, New Classes of p-Ary Few Weight Codes, Bulletin of the Malaysian Mathematical Sciences Society 42(4) (2019) 1393–1412.

[17] G. Vega, A characterization of all semiprimitive irreducible cyclic codes in terms of their lengths, Applicable Algebra Eng. Commun. Computin. 30(5) (2019) 441–452.