6-2020

On Codes Over Rings: The MacWilliams Extension Theorem and the MacWilliams Identities

Noha Abdelghany
Western Michigan University, noha.abdelghany@wmich.edu

ON CODES OVER RINGS: THE MACWILLIAMS EXTENSION THEOREM AND THE MACWILLIAMS IDENTITIES

by

Noha Abdelghany

A dissertation submitted to the Graduate College
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
Mathematics
Western Michigan University
June 2020

Doctoral Committee:
Jay Wood, Ph.D., Chair
Annegret Paul, Ph.D.
David Richter, Ph.D.
Jens Zumbrägel, Ph.D.

ON CODES OVER RINGS: THE MACWILLIAMS EXTENSION THEOREM AND THE MACWILLIAMS IDENTITIES

Noha Abdelghany, Ph.D.

Western Michigan University, 2020

The MacWilliams extension theorem for code equivalence and the MacWilliams identities for weight enumerators of a code and its dual code are two of the most important results in classical coding theory. In this thesis, we study how much these two results could be extended to codes over more general alphabets, beyond finite fields. In particular, we study the MacWilliams extension theorem and the MacWilliams identities for codes over rings and modules equipped with general weight functions.

Acknowledgments

I am very grateful for the endless and priceless support that I received from my family. Specifically, my mother, Mona Shabrawy, and my six sisters: Sarah, Shaimaa, Alaa, Nada, Aya, and Salma. They pushed me during the toughest and the easiest moments of this journey by their prayers and their belief in me. I owe much of what I accomplished to them.

I wish to express my sincere appreciation to my supervisor, Dr. Jay Wood, for the countless conversations that we have had in his office over the years. I learned a great deal from him, much beyond what is in this thesis. I am very grateful and lucky to have had him as my advisor.

I am very thankful to the amazing faculty of the mathematics department at WMU. They created such a welcoming and encouraging environment for all students. They provided constant support throughout my journey at WMU and were always happy to offer help whenever it is needed.

Finally, I would like to show my gratitude to my fellow graduate students in the math department at WMU for their support and for sharing this journey with me. We shared many hardships, laughs, productive conversations, and the occasional math jokes.

Noha Abdelghany

Contents

Chapter 1

INTRODUCTION

Codes over rings started being of interest to many researchers since the appearance of [9], where it was shown that the binary nonlinear codes known as Kerdock and Preparata codes are actually dual codes when viewed as codes over $\mathbb{Z}_4$. The study of codes over rings, and later codes over modules, led to an interest in studying the validity of the two classical MacWilliams results for codes over rings and modules. Namely, the MacWilliams extension theorem for code equivalence and the MacWilliams identities for weight enumerators of a code and its dual code. In this thesis, we present the results of our research into the validity of these two classical results for codes over rings and modules. We give an introduction and a brief outline of this thesis in the following.

In 1962, MacWilliams proved that any Hamming weight isometry between two codes over a finite field extends to a monomial transformation of the ambient space [13]. The theorem is known now as the MacWilliams extension theorem. Around the early nineties, coding theorists became interested in codes over finite rings and, later, finite modules. This gave rise to the natural question of whether the MacWilliams extension theorem is valid over rings for Hamming weight and, later, for general weight functions. For an alphabet A and a weight function w, A is said to have the extension property with respect to w if every linear w-isometry between two codes extends to a monomial transformation of the ambient space.

Over the past 20 years, many sufficient conditions and a few necessary conditions were found for the extension property to hold for various alphabets and weight functions.

In 1999, Wood showed that finite Frobenius rings have the extension property with respect to the Hamming weight [17]. In fact, the class of Frobenius rings characterizes finite rings that have the extension property [18]. In 2004, Greferath et al. proved that finite Frobenius bimodules have the extension property with respect to both Hamming weight and the homogeneous weight [8]. With respect to Lee weights, see Definition 4.1.4, it was shown that $\mathbb{Z}_m$ has the extension property when m is a prime power [12] and then it was proved for any positive integer m in [4].

In Chapter 3 we develop a tool that can be used to examine the extension property, following the development in [21]. A general weight function w of the alphabet module A is just any complex-valued function on A. Due to the lack of the algebraic structure of w, it is hard to decide if the extension property holds for w. In our development of monoid-ring tools, we view the weight w as linear map from $\mathcal{R}$ to $\mathcal{F}(A)$ as defined in section 3.2.1. We then study the matrix representation W of w, and as it turns out, the nonsingularity of an induced matrix $\overline{W}$ is a sufficient condition for the extension property.

The second part of this thesis studies the MacWilliams identities. The MacWilliams identities give a relation between the Hamming weight enumerator of a linear code and the Hamming weight enumerator of its dual. For a linear code $\mathcal{C}$ over a finite field $\mathbb{F}_q$, the MacWilliams identities are given by $\mathrm{hwe}_{\mathcal{C}^\perp}(X,Y) = \frac{1}{|\mathcal{C}|}\,\mathrm{hwe}_{\mathcal{C}}(X+(q-1)Y, X-Y)$, where hwe refers to the Hamming weight enumerator [13]. The question we are interested in is whether there is some version of the MacWilliams identities for other alphabets and other weight functions. In 1999, Wood showed that the MacWilliams identities are valid for both additive codes and linear codes over finite Frobenius rings with respect to the Hamming weight [17].

Turning our attention to Lee weights over $\mathbb{Z}_m$, the Lee weight and the Hamming weight are equal when $m = 2$ and $m = 3$, thus the MacWilliams identities are valid in those cases. For codes over $\mathbb{Z}_4$, it is known from [9] that the Lee weight enumerator of a linear code $\mathcal{C}$

over $\mathbb{Z}_4$ and its dual are related by $\mathrm{lwe}_{\mathcal{C}^\perp}(X,Y) = \frac{1}{|\mathcal{C}|}\mathrm{lwe}_{\mathcal{C}}(X+Y, X-Y)$. For $m \geqslant 5$, it was shown by Tang et al that the change of variables $X \mapsto X + (q-1)Y$ and $Y \mapsto X - Y$ does not give a version of the MacWilliams identities for any prime power $q|m$ [16]. This leaves open the possibility of other changes of variables that might give a relation between the Lee weight enumerators of a code and its dual.

In Chapter 4, we show the nonexistence of a MacWilliams operator for Lee weights over $\mathbb{Z}_m$, $m \geqslant 5$, by showing the existence of two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ that have equal Lee weight enumerators but the dual codes $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$ have different Lee weight enumerators.

Chapter 2

Preliminaries

This chapter is dedicated to introduce the necessary notions and terminology from classical coding theory and ring theory that will be needed for the rest of this thesis. Throughout this chapter, R is a finite ring with 1 and A is a left R-module thought of as the alphabet.

2.1 Linear Codes

We start with the classical definition of codes over finite fields, and we will work our way up to codes over rings and modules. For the following, we assume that $A = R = \mathbb{F}$, a finite field.

Definition 2.1.1. A code $\mathcal{C}$ of length n over $\mathbb{F}$ is a subset of $\mathbb{F}^n$. If $\mathcal{C}$ is a k-dimensional vector subspace of $\mathbb{F}^n$, then $\mathcal{C}$ is called an $[n, k]$-linear code.

An element of a code $\mathcal{C}$ is called a codeword. The field $\mathbb{F}$ is referred to as the alphabet for the code $\mathcal{C}$. A linear code is most-commonly realized in two ways, namely a generator matrix and a parity check matrix.

Definition 2.1.2. Let $\mathcal{C}$ be an $[n, k]$-linear code over $\mathbb{F}$.

- A generator matrix G of $\mathcal{C}$ is a $k \times n$ matrix whose rows span $\mathcal{C}$. In other words,

$$\mathcal{C} = \{mG : m \in \mathbb{F}^k\}.$$

- A parity check matrix H is a $(k-n) \times n$ matrix whose rows annihilate $\mathcal{C}$. In other words, $\mathcal{C}$ is the right null space of the parity check matrix H.

$$\mathcal{C} = \{c \in \mathbb{F}^n : Hc^T = 0\}.$$

Oftentimes the generator matrix is used for encoding. The space $\mathbb{F}^k$ is thought of as the space of all messages, where a message $m \in \mathbb{F}^k$ is encoded by $m \mapsto mG$ to the codeword mG in the code $\mathcal{C}$.

If the alphabet of a code is the binary field $\mathbb{F}_2$, then the code is called a binary code.

Example 2.1.3. Let $\mathcal{H}$ be the [7,4]-binary code defined by the following generator matrix

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

This code is known as the Hamming code. A parity check matrix for $\mathcal{H}$ is given by

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

If we think of the $[7, 3]$-linear code $\mathcal{S}$ generated by the matrix H, then $\mathcal{S}$ will have G as its parity check matrix. The code $\mathcal{S}$ is known as the simplex code. The codes $\mathcal{H}$ and $\mathcal{S}$ are dual codes as defined in the following.

Definition 2.1.4. The dual code $\mathcal{C}^\perp$ of a code $\mathcal{C}$ of length n is given by

$$\mathcal{C}^\perp = \{(x_1, \ldots, x_n) \in \mathbb{F}^n : \sum x_i c_i = 0, \text{ for all } c \in \mathcal{C}\}.$$

The following lemma summarizes the main properties of dual codes.

Lemma 2.1.5. *Let $\mathcal{C}$ be a code of length n over $\mathbb{F}$. Then*

- *$\mathcal{C}^\perp$ is a linear code over $\mathbb{F}$.*
- *$(\mathcal{C}^\perp)^\perp = \mathcal{C}$.*
- *If $\mathcal{C}$ is an $[n,k]$-linear code, then $|\mathcal{C}^\perp| \cdot |\mathcal{C}| = |\mathbb{F}|^n$. Equivalently, $\dim \mathcal{C}^\perp = n - k$.*

The most common notion of weight in classical coding theory is the Hamming weight.

Definition 2.1.6. For a vector $x = (x_1, \ldots, x_n)$ in $\mathbb{F}^n$, the Hamming weight of x is defined to be the number of nonzero entires in x. That is $\mathrm{H}(x) = |\{i : x_i \neq 0\}|$.

Oftentimes the weight functions are used to define a distance function of the ambient space. For instance, the Hamming distance between x and y in $\mathbb{F}^n$ is defined by $d_{\mathrm{H}}(x,y) = \mathrm{H}(x-y)$. One of the most essential parameters of a code is its minimum weight, it determines the error-detecting and the error-correcting capacities of the code.

Definition 2.1.7. Let $\mathcal{C}$ be an $[n,k]$-linear code. Then the minimum Hamming weight $d = \min\{\mathrm{H}(c) : c \in \mathcal{C}, c \neq 0\}$. In this case, $\mathcal{C}$ is said to be an $[n,k,d]$-linear code.

Example 2.1.8. Let $\mathcal{H}$ be the $[7,4]$-binary Hamming code defined in Example 2.1.3. The list of codewords of $\mathcal{H}$ is given by

$$\begin{aligned}\mathcal{H} = \{&0000000, 1000011, 0100101, 0010110, 0001111, 1100110,\\ &1010101, 1001100, 0110011, 0101010, 0011001, 1110000,\\ &1101001, 1011010, 0111100, 1111111\}.\end{aligned}$$

It is easy to see that the minimum nonzero weight of $\mathcal{H}$ is 3, therefore $\mathcal{H}$ is a $[7, 4, 3]$-linear code.

Example 2.1.9. Let $\mathcal{G}_{12}$ be the $[12, 6]$-linear code over $\mathbb{F}_3$, the finite field of order 3, with a generator matrix

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

With some calculations, one can show that the minimum weight of $\mathcal{G}_{12}$ is 6. The code $\mathcal{G}_{12}$ is called the $[12, 6, 6]$ Golay code. This example is found in [11].

Recall A is a left R-module. Here is how we view codes over modules.

Definition 2.1.10. A code $\mathcal{C}$ of length n over A is a subset of A^n. If $\mathcal{C}$ is a left submodule of A^n, then $\mathcal{C}$ is called a left linear code.

2.2 Code Equivalence

In this section we present the different ways to view two codes as being equivalent. There are multiple ways of viewing code equivalence, some of them are more general than others. To understand the relation between the different notions of equivalence, we will define some of them here and refer to Chapter 3 for our full study of the MacWilliams extension theorem.

Unlike vector spaces with no extra structure, the notion of equivalence of linear codes requires more than two codes to have the same dimension. One of the most important parameters of a linear code comes from the weight considered. So in order to talk about equivalence of linear codes we need to fix both the alphabet and the weight function.

Remark 2.2.1. For any left R-linear homomorphism $f : A \to B$ between two left R-modules, we write inputs on the left. That is, for $x \in A$ we denote the image of x under f as xf instead of $f(x)$. One of the reasons for this notation is that the R-linearity then is expressible is the associative property: $(rx)f = r(xf)$ for all $r \in R$ and $x \in A$.

Recall A is a left R-module. We think of A as the alphabet. Notice that A admits a right module structure under the ring $\mathrm{End}_R(A)$ of all endomorphisms on A. Indeed, for $a \in A$ and $\phi \in \mathrm{End}_R(A)$, $a\phi$ =the image of a under ϕ, defines a right scalar multiplication of $\mathrm{End}_R(A)$ on A. Therefore we have that A is an $R, \mathrm{End}_R(A)$-bimodule. Let $\mathcal{U}(R)$ be the group of units of R and $\mathrm{GL}_R(A)$ the group of units of $\mathrm{End}_R(A)$, that is $\mathrm{GL}_R(A)$ is the group of left R-automorphisms on A. This implies that the group $\mathcal{U}(R)$ acts on A on the left and $\mathrm{GL}_R(A)$ acts on A on the right.

Here is what we mean by a weight function.

Definition 2.2.2. A weight w on the alphabet A is a complex-valued function $w : A \to \mathbb{C}$ on A.

Every weight function on A extends to a weight function on A^n by $w(x_1, \ldots, x_n) = \sum_i w(x_i)$ for all $x \in A^n$.

For a weight w we define what we call left and right symmetry groups of w as follows.

Definition 2.2.3. The left and right symmetry groups of a weight $w : A \to \mathbb{C}$ are given by

$$G_{lt}(w) = \{u \in \mathcal{U}(R) : w(ua) = w(a), \text{ all } a \in A\},$$

$$G_{rt}(w) = \{\tau \in \mathrm{GL}_R(A) : w(a\tau) = w(a), \text{ all } a \in A\}.$$

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two left linear codes of length n over A and let w be a weight on A. In the following we define several different notions of code-equivalence.

A linear map $f : \mathcal{C}_1 \to \mathcal{C}_2$ is said to be a w-isometry if f is an isomorphism preserving the weight w. That is $w(cf) = w(c)$ for all $c \in \mathcal{C}_1$.

Definition 2.2.4. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be w-isometric if there is a w-isometry $f : \mathcal{C}_1 \to \mathcal{C}_2$.

An automorphism $T : A^n \to A^n$ is called a monomial transformation if there are a permutation σ on n elements, and $\tau_1, \ldots, \tau_n \in \mathrm{GL}_R(A)$ such that

$$(a_1, \ldots, a_n)T = (a_{\sigma(1)}\tau_1, \ldots, a_{\sigma(n)}\tau_n).$$

If $\tau_1, \ldots, \tau_n$ are elements of some subgroup G of $\mathrm{GL}_R(A)$, then T is said to be a G-monomial transformation.

Definition 2.2.5. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be G-monomially equivalent if there is a G-monomial transformation T with $\mathcal{C}_1 T = \mathcal{C}_2$.

Definition 2.2.6. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be permutationally equivalent if there is a $\{1\}$-monomial transformation T with $\mathcal{C}_1 T = \mathcal{C}_2$. That is, all the τ's appearing in the definiton of T are in fact the identity element.

Note that $T|_{\mathcal{C}_1}$ is a w-isometry, provided T is a G_{rt}-monomial transformation. That is, two codes are w-isometric if they are G_{rt}-monomially equivalent. The converse is not always true. The converse is true for codes over finite fields equipped with the Hamming weight. This result is known as the MacWilliams extension theorem, refer to Section 3.1.

2.3 The Character Module

In this section, we define the character module, and we introduce Pontryagin's duality functor for modules. For more details, see Section 3 in [17]. Recall that A is a finite left R-module, in particular, A is a finite abelian group.

Definition 2.3.1. For any abelian group A, a character π on A is defined to be a group homomorphism $\pi : A \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the multiplicative group of non-zero complex numbers.

We let $\widehat{A}$ denote the collection of all characters on A.

Lemma 2.3.2. *The collection $\widehat{A}$ of all characters on A is an abelian group under pointwise multiplication. If A is a left R-module, then $\widehat{A}$ is a right R-module.*

Proof. Notice that $\widehat{A}$ is the collection of all group homomorphisms from A to $\mathbb{C}^\times$. In other words, $\widehat{A} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$. Since $\mathbb{C}^\times$ is an abelian group under multiplication, then so is $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$ under pointwise multiplication.

Let $\pi \in \widehat{A}$ and $r \in R$. The right scalar multiplication of π and r is denoted by π^r and is defined by

$$\pi^r(a) = \pi(ra), \text{ all } a \in A.$$

It is easy to see that this indeed defines a right R-module structure on $\widehat{A}$. □

Remark 2.3.3. Since the operation on the abelian group $\widehat{A}$ is "multiplication", and since it is known that exponentiation is distributive over multiplication, it is convenient to write the right scalar multiplication on $\widehat{A}$ in exponential form. That is, the right scalar multiplication of $\pi \in \widehat{A}$ and $r \in R$ is expressed as π^r instead πr. In this case, the distribution of the scalar multiplication on the group operation of $\widehat{A}$ is written as $(\tau\pi)^r = \tau^r\pi^r$ instead of $(\tau\pi)r = \tau r\pi r$.

Lemma 2.3.4. *For a finite abelian group A, the following hold.*

- $\sum_{\pi\in\widehat{A}} \pi(a) = \begin{cases} |A|, & \text{if } a = 0 \\ 0, & \text{if } a \neq 0 \end{cases}$.
- $\sum_{a\in A} \pi(a) = \begin{cases} |A|, & \text{if } \pi = 1 \\ 0, & \text{if } \pi \neq 1 \end{cases}$.

Proof. It is clear that $\sum_{\pi\in\widehat{A}} \pi(0) = \sum_{\pi\in\widehat{A}} 1 = |A|$. Now let $a \neq 0$ be an element of A, then there is $\tau \in \widehat{A}$ such that $\tau(a) \neq 1$, see [14, page 61]. Using the group structure on $\widehat{A}$ we get:

$$\sum_{\pi\in\widehat{A}} \pi(a) = \sum_{\pi\in\widehat{A}} (\tau\pi)(a) = \tau(a) \sum_{\pi\in\widehat{A}} \pi(a).$$

Since $\tau(a) \neq 1$ then we must have $\sum_{\pi \in \widehat{A}} \pi(a) = 0$. The second part is proved similarly. $\square$

Corollary 2.3.5. *Let S be a right submodule of the character module $\widehat{A}$. For $s \in A$,*

$$\sum_{\pi \in S} \pi(s) = \begin{cases} |S|, & s \in (A:S) \\ 0, & otherwise \end{cases},$$

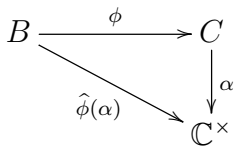
where $(A:S) = \{a \in A : \pi(a) = 1, \ all\ \pi \in S\}$.

Let R-mod denote the category of all finite left R-modules and mod-R denote the category of all finite right R-modules. The construction $\widehat{A}$ is in fact functorial, and it is known as the Pontryagin duality functor. The following lemma summarizes the main properties of this functor on the objects. A detailed study of this functor is found in [17].

Lemma 2.3.6. *The duality functor $\widehat{\ } : R\text{-}mod \rightleftharpoons mod\text{-}R$ is a contravariant functor satisfying the following, for any left (right) R-module B:*

1. *B and $\widehat{B}$ are isomorphic as groups. In particular, $|\widehat{B}| = |B|$.*
2. *$\widehat{\widehat{B}} \cong B$ as left (right) R-modules.*
3. *$\widehat{B}$ is an $(End_R(B), R)$-bimodule. $((R, End_R(B))$-bimodule).*
4. *If B is an R-bimodule, then so is $\widehat{B}$.*

The duality functor acts on the morphisms in the following way. For any ϕ in $\mathrm{Hom}_R(B, C)$, where B and C are left R-modules, there is an induced homomorphism $\widehat{\phi}$ in $\mathrm{Hom}_R(\widehat{C}, \widehat{B})$ of right R-modules given by the following diagram. For $\alpha \in \widehat{C}$, $\widehat{\phi}(\alpha)$ is given by



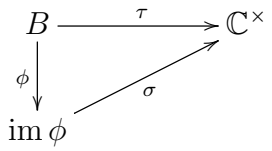
That is, $\widehat{\phi}(\alpha) = \alpha \circ \phi$.

Lemma 2.3.7. *Let B and C be left R-modules with $\phi \in Hom_R(B, C)$. Then*

$$\operatorname{im} \widehat{\phi} = (\widehat{B} : \ker \phi),$$

where $(\widehat{B} : \ker \phi) = \{\pi \in \widehat{B} : \pi(b) = 1, \text{ for all } b \in \ker \phi\}$.

Proof. Let $\tau \in (\widehat{B} : \ker \phi)$. Then $\tau(b) = 1$ for all $b \in \ker \phi$. This means that $\ker \phi \subseteq \ker \tau$, and so τ factors through $B/\ker \phi \cong \operatorname{im} \phi$. That is, there is $\sigma : \operatorname{im} \phi \to \mathbb{C}^\times$ making the following diagram commute.



Notice that σ is a character on $\operatorname{im} \phi$. We would like to extend σ to a character on the whole module C. This can be done by making use of the following exact sequence.

$$0 \to \operatorname{im} \phi \to C \to C/\operatorname{im} \phi \to 0.$$

The duality functor is an exact contravariant functor, see [17, Remark 3.3]. Therefore, we get the induced exact sequence

$$0 \leftarrow \widehat{\operatorname{im} \phi} \leftarrow \widehat{C} \leftarrow \widehat{C/\operatorname{im} \phi} \leftarrow 0.$$

The map $\widehat{\operatorname{im} \phi} \leftarrow \widehat{C}$ is surjective and σ belongs to $\widehat{\operatorname{im} \phi}$, therefore σ extends to a homomorphism $\bar{\sigma}$ on C. Since $\sigma = \bar{\sigma}$ on $\operatorname{im} \phi$, then $\tau = \sigma \circ \phi = \bar{\sigma} \circ \phi$ which, by the definition of $\widehat{\phi}$, says that $\tau = \widehat{\phi}(\bar{\sigma})$. This shows that $\tau \in \operatorname{im} \widehat{\phi}$ and so $(\widehat{B} : \ker \phi) \subseteq \operatorname{im} \widehat{\phi}$.

Conversely, if $\tau \in \operatorname{im} \widehat{\phi}$, then $\tau = \widehat{\phi}(\sigma)$ for some σ in $\widehat{C}$. For $b \in \ker \phi$,

$$\tau(b) = \widehat{\phi}(\sigma)(b) = \sigma(\phi(b)) = \sigma(0) = 1.$$

This shows $\tau \in (\widehat{B} : \ker \phi)$. □

In the following we shift our attention to R-bimodules. We define the following.

Definition 2.3.8. Let B be an R-bimodule and $r \in R$. Define λ_r to be the left scalar multiplication by r on B. That is, $\lambda_r : B \to B$ with $\lambda_r(b) = rb$, for all $b \in B$. In the case when $B = \widehat{R}$, we will use the notation $\lambda_r(\pi) = {}^r\pi$, all π in B. Similarly, ρ_r is the right scalar multiplication on B. Remark 2.3.3 explains our choice of notation.

We will not distinguish λ_r and ρ_r for different R-bimodules, it should be clear from context which module is being considered. The following lemma shows how scalar multiplication is affected by the duality functor.

Lemma 2.3.9. *For $r \in R$, we have*

$$\widehat{\lambda}_r = \rho_r \text{ and } \widehat{\rho}_r = \lambda_r.$$

Proof. Let B be an R-bimodule and $r \in R$. Then for $\pi \in \widehat{B}$ and $b \in B$,

$$\left(\widehat{\rho}_r(\pi)\right)(b) = \pi \circ \rho_r(b) = \pi(br) = {}^r\pi(b) = (\lambda_r(\pi))(b).$$

This shows that $\widehat{\rho}_r = \lambda_r$. The other equality is proven in a similar fashion. □

Lemma 2.3.10. *Let A denote the character bimodule $\widehat{R}$. Then $End_R(A_R) \cong R$ as rings.*

Proof. Define

$$\Lambda : R \to \mathrm{End}_R(A_R)$$

by $\Lambda(r) = \lambda_r$. It is clear that Λ is a ring homomorphism. Let $r \in \ker \Lambda$. Then we have ${}^r\pi$ is the trivial character for all π in A, this implies that $1 = {}^r\pi(1) = \pi(r)$, all $\pi \in A$. It follows that $\sum_{\pi \in A} \pi(r) = |A|$, and hence r must be zero by Lemma 2.3.4. This shows that Λ is injective.

Suppose that $\phi \in \mathrm{End}_R(A_R)$. We consider the character module ${}_R\widehat{A}$ of A_R. The endomorphism ϕ on A_R induces an endomorphism $\widehat{\phi}$ on ${}_R\widehat{A}$. Up to the natural isomorphism $R \cong \widehat{A}$, $\widehat{\phi}$ is a left R-endomorphism on R. And so $\widehat{\phi}$ is a right multiplication ρ_s by s, for

some $s \in R$. Noting that $\widehat{\widehat{\phi}} = \phi$, it follows that $\phi = \widehat{\rho_s}$. Lemma 2.3.9 then implies that $\phi = \lambda_s$. This implies that Λ is surjective, and hence a ring isomorphism. □

Recall that $\mathcal{U}(R)$ denotes the group of units in R. The following follows immediately form Lemma 2.3.10.

Corollary 2.3.11. *Let $A = \widehat{R}$. Then $\mathcal{U}(R) \cong GL_R(A_R)$ as groups.*

2.4 Frobenius Rings and Frobenius Bimodules

In this section we present the necessary notions of Frobenius rings and Frobenius bimodules. For a detailed presentation of this class of rings, refer to [17].

Although there is a general definition of Frobenius rings that is applicable to infinite rings, there is a simpler definition in the finite case. The following definition is usually expressed as a theorem when the full general definition is considered, see [17, Theorem 3.10].

Definition 2.4.1. A finite Frobenius bimodule A is an (R, R)-bimodule such that ${}_RA \cong {}_R\widehat{R}$ and $A_R \cong \widehat{R}_R$. A finite Frobenius ring is a finite ring that is a Frobenius bimodule over itself.

Lemma 2.4.2. *For a Frobenius R-bimodule A we have*

$$ {}_R\widehat{A} \cong {}_RR \quad \text{and} \quad \widehat{A}_R \cong R_R. $$

Proof. By dualizing the definition of a Frobenius bimodule and using Lemma 2.3.6. □

Definition 2.4.3. A left R-module B is a cyclic R-module generated by $b \in B$, if

$$ B = \{rb : r \in R\}. $$

Similarly, if B is a right R-module with $B = \{br : r \in R\}$, then B is a cyclic right R-module.

We know that R_R and ${}_RR$ are cyclic R-modules, indeed, both R_R and ${}_RR$ are generated by 1. Therefore by the above lemma, both ${}_R\widehat{A}$ and $\widehat{A}_R$ are cyclic modules. A generator for ${}_R\widehat{A}$ is called a *left generating character* and a generator for $\widehat{A}_R$ is called a *right generating character* for A.

Lemma 2.4.4. *Let A be the character bimodule $\widehat{R}$. Then the character χ in $\widehat{A}$ defined by*

$$\chi(\pi) = \pi(-1), \text{ all } \pi \in A$$

is both a left and right generating character for A.

Proof. We show that χ is a left generating character for A. The other side is proven similarly. Note that, by Lemma 2.3.6, we have that $\widehat{A} \cong R$ as bimodules. Therefore, it suffices to show that R is isomorphic to $R\chi$, the left submodule generated by χ in $\widehat{A}$. Define

$$\Psi : R \to R\chi$$
$$r \mapsto {}^r\chi$$

It is clear that Ψ is a group homomorphism and is surjective. Let r be an element of $\ker \Psi$. Then we have that ${}^r\chi(\pi) = 1$, for all π in A. That is, $\chi(\pi^r) = \pi^r(-1) = \pi(-r) = 1$ for all π in A. It follows that $\sum_{\pi \in A} \pi(-r) = |A|$, and hence r must be zero by Lemma 2.3.4. Therefore Ψ is an isomorphism. □

2.5 Multiplicity Functions

In this section we define and study multiplicity functions which are another way to describe linear codes. Fix an alphabet A, which is a left R-module, and a weight w. And let G_{lt} and G_{rt} be the left and right symmetry groups for the weight w.

Let M be a left R-module thought of as the message space of the code. First we need to define what is known as parametrized codes.

Definition 2.5.1. A parametrized code of length n is defined by the pair (M, Λ), where M is a finite left R-module and $\Lambda : M \to A^n$ is a homomorphism of left R modules.

Notice that if (M, Λ) is a parametrized code then the image $\mathcal{C} = M\Lambda$ of Λ is a classical linear code of length n over A.

Remark 2.5.2. Recall that $\mathrm{Hom}_R(M, A^n) \equiv \mathrm{Hom}_R(M, A)^n$. That means that $\Lambda \in \mathrm{Hom}_R(M, A^n)$ can be viewed as $\Lambda = (\lambda_1, \ldots, \lambda_n)$ in $\mathrm{Hom}_R(M, A)^n$.

Example 2.5.3. Let $A = R = \mathbb{F}$ be a finite field. Suppose that $\mathcal{C}$ is an $[n, k]$-linear code over $\mathbb{F}$ with a generator matrix G. Let $M = \mathbb{F}^k$ be the k-dimensional vector space over $\mathbb{F}$. Define $\Lambda : M \to \mathbb{F}^n$ by $m\Lambda = mG$. This defines a parametrized code (M, Λ) over $\mathbb{F}$. We have

$$\mathcal{C} = \{mG : m \in \mathbb{F}^k\} = M\Lambda.$$

The columns of the matrix G are really the same as the functionals $\lambda_1, \ldots, \lambda_n$. Indeed, if G_i denotes the i^{th} column of the matrix G, then $mG_i = m\lambda_i$, for $1 \leqslant i \leqslant n$.

The right symmetry group G_{rt} acts on the right on $\mathrm{Hom}_R(M, A)$ the collection of all functionals by the following. For $\phi \in G_{rt}$ and $\lambda \in \mathrm{Hom}_R(M, A)$, $\lambda\phi$ is defined by $m(\lambda\phi) = (m\lambda)\phi$ for all $m \in M$. Let $\mathcal{O}^\sharp$ denote the orbit space $\mathrm{Hom}_R(M, A)/G_{rt}$ of the above action.

Definition 2.5.4. A multiplicity function η is a function $\eta : \mathcal{O}^\sharp \to \mathbb{N}$ with $\eta(\mathrm{orb}(0)) = 0$. Let $F_0(\mathcal{O}^\sharp, \mathbb{N})$ denote the collection of all multiplicity functions.

For a fixed message space M, there is a one-to-one a correspondence between the collection all multiplicity functions $F_0(\mathcal{O}^\sharp, \mathbb{N})$ and the collections of all classes of monomially equivalent parametrized codes. Starting with a parametrized code (M, Λ), with $\Lambda = (\lambda_1, \ldots, \lambda_n)$, define a multiplicity function η to count the number of functionals λ_i's in each orbit. That is $\eta(\mathrm{orb}(\rho)) = |\{i : \lambda_i \in \mathrm{orb}(\rho)\}|$. Conversely, for a multiplicity function $\eta \in F_0(\mathcal{O}^\sharp, \mathbb{N})$, we choose $\Lambda = (\lambda_1, \ldots, \lambda_n)$ such that $\eta(\mathrm{orb}(\rho)) = |\{i : \lambda_i \in \mathrm{orb}(\rho)\}|$, this Λ is well defined up to a monomial transformation.

From now until the end of the section, we will only consider classes of monomially equivalent codes, so we use multiplicity functions to refer to them.

Let η be a multiplicity function with a corresponding parametrized code (M, Λ). The codeword corresponding to a message word $m \in M$ is $x = m\Lambda$. The weight of x is given by:

$$w(x) = \sum w(x_i) = \sum w(m\lambda_i) = \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(m\lambda)\eta(\lambda).$$

Notice that the above expression does not depend on the choice of λ, it only depends on the multiplicity function η. The list of weights of the codewords of the code $\mathcal{C} = M\Lambda$ is then given by the map $m \mapsto \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(m\lambda)\eta(\lambda)$. This is what we refer to as the W mapping. We consider the space $F_0(\mathcal{O}^\sharp, \mathbb{Q})$ instead to make use of the fact that it is a vector space over $\mathbb{Q}$.

Definition 2.5.5. The W mapping is given by

$$\begin{aligned} W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) &\to F_0(M, \mathbb{Q}) \\ \eta &\mapsto \left[m \mapsto \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(m\lambda)\eta(\lambda) \right]. \end{aligned}$$

Where $F_0(M, \mathbb{Q}) = \{f : M \to \mathbb{Q} : f(0) = 0\}$.

Lemma 2.5.6. *The W map is a linear $\mathbb{Q}$-homomorphism.*

Proof. For $q \in \mathbb{Q}$ and $\eta_1, \eta_2 \in F_0(M, \mathbb{Q})$, we have

$$\begin{aligned} W(\eta_1 + q\eta_2)(m) &= \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(m\lambda)(\eta_1 + q\eta_2)(\lambda) \\ &= \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(m\lambda)\eta_1(\lambda) + q \sum_{\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp} w(m\lambda)\eta_2(\lambda) = W(\eta_1)(m) + qW(\eta_2)(m), \end{aligned}$$

for all $m \in M$. □

Notice that the left symmetry group G_{lt} acts on M on the left, as M is a left R-module.

Let $\mathcal{O}$ denote the orbit space $G_{lt}\backslash M$. It is easy to see that $W(\eta)$ is invariant under the above action. Let $F(\mathcal{O}, \mathbb{Q})$ denote the space of invariant functions $f : M \to \mathbb{Q}$ under the action $G_{lt}\backslash M$. And let $F_0(\mathcal{O}, \mathbb{Q})$ be defined by $F_0(\mathcal{O}, \mathbb{Q}) = \{f \in F(\mathcal{O}, \mathbb{Q}) : f(\mathrm{orb}(0)) = 0\}$. Then the W mapping can be thought of as $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$.

The mapping W is used as a way to find a sufficient condition for the extension property to be satisfied as shown in the following theorem.

Theorem 2.5.7 (Theorem 7.2, [19])**.** *For an alphabet A, if the mapping $W : F_0(\mathcal{O}^\sharp, \mathbb{Q}) \to F_0(\mathcal{O}, \mathbb{Q})$ is injective for every finite R-module M, then the alphabet A has the extension property with respect to the weight w.*

The notions defined in this section will be used to describe codes in Chapter 4.

Chapter 3

The Extension Theorem for Weight Functions over Frobenius Bimodules

The main two notions of code equivalence are w-isometries and monomial equivalence. The first notion of equivalence, w-isometries, is intrinsic. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be w-isometric if there is a weight-preserving linear isomorphism f sending $\mathcal{C}_1$ to $\mathcal{C}_2$. The second notion of equivalence, monomial equivalence, is extrinsic. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be monomially equivalent if there is a monomial transformation T on the ambient space sending $\mathcal{C}_1$ to $\mathcal{C}_2$. The MacWilliams extension theorem shows that these two notions of equivalence are the same for linear codes over finite fields with respect to Hamming weights. We say that finite fields equipped with the Hamming weight have the extension property [19]. In general, an alphabet A is said to have the extension property with respect to a weight w if every w-isometry extends to a monomial transformation, see Definition 3.1.1.

The main result in this chapter is to give a characterization for a general weight function to have the extension property over the Frobenius bimodule $\widehat{R}$. We presented the essential properties of the Frobenius bimodule in section 2.3. Throughout this chapter R is a finite ring with 1 and A is a finite left R-module.

3.1 The Extension Theorem and the Extension Property

There are several notions of code equivalence as we saw in Section 2.2. In this section we cover the main results regarding the extension theorem. Recall that for a weight w, the restriction $T|_{\mathcal{C}_1}$ of a G_{rt}-monomial transformation produces a w-isometry. That implies that every pair of G_{rt}-monomially equivalent codes are w-isometric. The converse is known as the extension property.

Definition 3.1.1. Let A be a left R-module and w a weight function on A. A is said to have the extension property with respect to w if every w-isometry between two linear codes extends to a G_{rt}-monomial transformation of the ambient space A^n.

It was shown in [13] that finite fields have the extension property with respect to the Hamming weight. The result is known as the MacWilliams extension theorem.

Theorem 3.1.2 (The MacWilliams Extension Theorem)**.** *Every Hamming weight isometry f of linear codes over a finite field $\mathbb{F}$ extends to a monomial transformation T on the ambient space $\mathbb{F}^n$.*

In 1999, Wood showed that finite Frobenius rings have the extension property with respect to the Hamming weight [17]. In fact, the class of Frobenius rings characterizes finite rings that have the extension property [18]. In 2004, Greferath et al. proved that finite Frobenius bimodules have the extension property with respect to both Hamming weight and the homogeneous weight [8]. With respect to Lee weights, see Definition 4.1.4, it was shown that $\mathbb{Z}_m$ has the extension property when m is a prime power [12] and then it was proved for any positive integer m in [4].

Over the past several years, many sufficient conditions and a few necessary conditions were found for the extension property to hold for various alphabets and weight functions. In this chapter we give sufficient conditions for the Frobenius bimodule to have the extension

property with respect to a general weight function. Sufficient conditions for the extension property over Frobenius bimodules with respect to weights of maximal symmetry were given in [6].

Theorem 3.1.3. [6, Theorem 4.4] *Suppose A is a Frobenius bimodule over R with a generating character χ and w is a bi-invariant weight on A. If w satisfies*

$$\sum_{a \in S} w(a)\chi(a) \neq 0, \text{ for all nonzero submodules } S \subseteq A,$$

then w has the extension property.

This result is recovered using monoid-ring tools in Corollary 3.3.5.

3.2 Monoid-Ring Approach

In this section we follow the general setup and notations from [21]. Recall that R is a finite ring with 1. Let $\mathcal{R} = F(R, \mathbb{C})$ be the complex vector space of all complex-valued functions on R. We make $\mathcal{R}$ into a ring by defining addition to be pointwise, and multiplication is given by

$$\alpha\beta(r) = \sum_{st=r} \alpha(s)\beta(t), \text{ for } \alpha, \beta \in \mathcal{R} \text{ and } r \in R.$$

In fact, $\mathcal{R}$ is naturally isomorphic the complex monoid ring of the monoid $(R, \cdot)$ with elements thought of as complex-valued functions instead of complex formal sums. It is clear that $\mathcal{R}$ is also a complex algebra with dimension $|R|$. We think of the natural basis of $\mathcal{R}$ as $\{e_r\}_{r \in R}$, where $e_r(s)$ is 1 when $s = r$ and is zero otherwise.

A similar construction is done for the alphabet A. Let $\mathcal{F}(A) = F(A, \mathbb{C})$ be the complex vector space of all complex-valued functions on A. As a complex vector space, $\mathcal{F}(A)$ has natural basis $\{\delta_a\}_{a \in A}$, where $\delta_a(b)$ is 1 when $b = a$ and is zero otherwise. The left R-module structure on A induces a right $\mathcal{R}$-module structure on $\mathcal{F}(A)$, as follows. The following two results generalize Lemmas 13, 14 and 19 in [7].

Lemma 3.2.1. *$\mathcal{F}(A)$ is a right $\mathcal{R}$-module under the following scalar multiplication*

$$(w\alpha)(a) = \sum_{r\in R} w(ra)\alpha(r), \text{ for } w \in \mathcal{F}(A), \alpha \in \mathcal{R}, \text{ and } a \in A.$$

Proof. We verify one of the right scalar multiplication axioms. Let $\alpha, \beta \in \mathcal{R}$ and $w \in \mathcal{F}(A)$. Then

$$\begin{aligned}
(w(\alpha\beta))(a) &= \sum_{r\in R} w(ra)(\alpha\beta)(r) \\
&= \sum_{r\in R} w(ra) \sum_{st=r} \alpha(s)\beta(t) \\
&= \sum_{s,t\in R} w(sta)\alpha(s)\beta(t) \\
&= \sum_{t\in R} \left(\sum_{s\in R} w(sta)\alpha(s) \right) \beta(t) \\
&= \sum_{t\in R} (w\alpha)(ta)\beta(t) = ((w\alpha)\beta)(a).
\end{aligned}$$

This shows that $w(\alpha\beta) = (w\alpha)\beta$. The rest of the axioms can be proved in a similar fashion. □

If w in $\mathcal{F}(A)$ is thought of as a weight function, then $w\alpha$ can also be thought of as a weight function, for all $\alpha \in \mathcal{R}$.

Proposition 3.2.2. *Suppose $f : \mathcal{C}_1 \to \mathcal{C}_2$ is a w-isometry. Then f is a $w\alpha$-isometry for any $\alpha \in \mathcal{R}$.*

Proof. For $x \in \mathcal{C}_1$,

$$w\alpha(xf) = \sum_{r\in R} w(r(xf))\alpha(r) = \sum_{r\in R} w((rx)f)\alpha(r) = \sum_{r\in R} w((rx))\alpha(r) = w\alpha(x). \quad \square$$

3.2.1 The W Matrix

Let $w \in \mathcal{F}(A)$ be an arbitrary but fixed element. We think of w as a weight function on the alphabet A. The right $\mathcal{R}$-module structure on $\mathcal{F}(A)$ defines a map $\mathcal{F}(A) \times \mathcal{R} \to \mathcal{F}(A)$. By fixing $w \in \mathcal{F}(A)$, we obtain a homomorphism of right $\mathcal{R}$-modules (also denoted by w) $w : \mathcal{R} \to \mathcal{F}(A)$ given by $w(\alpha) = w\alpha$, all $\alpha \in \mathcal{R}$. We will refer to this homomorphism w as left multiplication by w.

It is clear that the left multiplication by w is a $\mathbb{C}$-linear homomorphism. Using the natural bases mentioned above for $\mathcal{R}$ and $\mathcal{F}(A)$, we can find the matrix representation of w. In fact, we have

$$w(e_r)(\pi) = we_r(\pi) = \sum_{s \in R} w({}^s\pi)e_r(s) = w({}^r\pi).$$

That is, $we_r = \sum_{\pi \in A} w({}^r\pi)\delta_\pi$, all r in R. Therefore, the matrix representation of w under the natural bases is given by $(w({}^r\pi))_{\pi \in A, r \in R}$. As simple as this matrix representation seems to be, it does not reflect much of the structures of A and R and their interrelation. In the following we will use a different basis for $\mathcal{F}(A)$ that will give a nice block structure for the matrix representation of w.

Definition 3.2.3. (Fourier Transform) Let B be a finite abelian group, and f a complex-valued function on B. The Fourier Transform $\widehat{f}$ of f is a complex-valued function on $\widehat{B}$ defined by

$$\widehat{f}(\pi) = \sum_{b \in B} f(b)\pi(b), \text{ all } \pi \in \widehat{B}.$$

From now until the end of this chapter, we take $A = \widehat{R}$ to be the character bimodule $\widehat{R}$. In this case, we get the following nice isomorphism between $\mathcal{R}$ and $\mathcal{F}(A)$ as shown in [21, Theorem 4.3.].

Theorem 3.2.4. *Let $A = \widehat{R}$. The Fourier transform $\widehat{\ }: \mathcal{R} \to \mathcal{F}(A)$ mapping α to $\widehat{\alpha}$ is an isomorphism of complex vector spaces.*

Proof. It is clear that the Fourier transform defines a linear homomorphism of complex vector

space. The inverse Fourier transform $\check{}$ is given, for $w \in \mathcal{F}(A)$ and $r \in R$, by

$$\check{w}(r) = \frac{1}{|R|} \sum_{\pi \in A} w(\pi)\pi(-r).$$

This shows that the Fourier transform is in fact an isomorphism. □

Corollary 3.2.5. *$\{\widehat{e}_s\}_{s\in R}$ forms a basis for $\mathcal{F}(A)$, where $\widehat{e}_s = \sum_{\pi\in A} \pi(s)\delta_\pi$.*

Recall that we fixed $w \in \mathcal{F}(A)$ and that $A = \widehat{R}$. We calculate the matrix representation W of the map w with respect to the bases $\{e_r\}_{r\in R}$ for $\mathcal{R}$ and $\{\widehat{e}_s\}_{s\in R}$ for $\mathcal{F}(A)$. Recall that λ_r is the left scalar multiplication by r in A, as defined in Lemma 2.3.10. Since λ_r is a right R-module homomorphism of A, we have that both $\ker \lambda_r$ and $\operatorname{im} \lambda_r$ are right submodules of A.

Fix $r \in R$. Using the inverse Fourier transform formula, it is easy to find that $\delta_\pi = \frac{1}{|R|} \sum_{s\in R} \pi(-s)\widehat{e}_s$. The column indexed by e_r in the matrix representation W of w is then given by:

$$\begin{aligned}
we_r &= \sum_{\pi\in A} w({}^r\pi)\delta_\pi \\
&= \sum_{\pi\in A} w({}^r\pi) \left(\frac{1}{|R|} \sum_{s\in R} \pi(-s)\widehat{e}_s \right) \\
&= \frac{1}{|R|} \sum_{s\in R} \left(\sum_{\pi\in A} w({}^r\pi)\pi(-s) \right) \widehat{e}_s \\
&= \frac{1}{|R|} \sum_{s\in R} \left(\sum_{\pi\in \operatorname{im}\lambda_r} w(\pi) \sum_{\tau\in\lambda_r^{-1}(\pi)} \tau(-s) \right) \widehat{e}_s.
\end{aligned}$$

For $\pi \in \operatorname{im} \lambda_r$ and $r \in R$, let $\tau_{r,\pi}$ denote an element in $\lambda_r^{-1}(\pi)$, that is $\lambda_r(\tau_{r,\pi}) = \pi$. Since

$\lambda_r^{-1}(\pi)$ is a coset of $\ker \lambda_r$, we have $\lambda_r^{-1}(\pi) = \tau_{r,\pi} \ker \lambda_r$. Thus, by Corollary 2.3.5, we get

$$\begin{aligned} we_r &= \frac{1}{|R|} \sum_{s \in R} \left(\sum_{\pi \in \operatorname{im} \lambda_r} w(\pi) \sum_{\tau \in \lambda_r^{-1}(\pi)} \tau(-s) \right) \widehat{e}_s \\ &= \frac{1}{|R|} \sum_{s \in R} \left(\sum_{\pi \in \operatorname{im} \lambda_r} w(\pi) \sum_{\tau \in \ker \lambda_r} \tau_{r,\pi}(-s)\tau(-s) \right) \widehat{e}_s \\ &= \frac{1}{|R|} \sum_{s \in R} \left(\sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(-s) \sum_{\tau \in \ker \lambda_r} \tau(-s) \right) \widehat{e}_s \\ &= \frac{|\ker \lambda_r|}{|R|} \sum_{s \in (R : \ker \lambda_r)} \left(\sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(-s) \right) \widehat{e}_s. \end{aligned}$$

It follows that the $(\widehat{e}_s, e_r)$-entry in the matrix representation of W is given by:

$$W_{\widehat{e}_s, e_r} = \begin{cases} \frac{|\ker \lambda_r|}{|R|} \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(-s), & s \in (R : \ker \lambda_r) \\ 0, & \text{otherwise} \end{cases}. \tag{3.1}$$

It seems that the entries $W_{\widehat{e}_s, e_r}$ might depend on the choice of $\tau_{r,\pi}$. We shall show that the expression of $W_{\widehat{e}_s, e_r}$ is in fact independent of the choice of $\tau_{r,\pi}$ in $\lambda_r^{-1}(\pi)$.

Lemma 3.2.6. *For $r \in R$, the left ideal $(R : \ker \lambda_r)$ is the left principal ideal generated by r.*

Proof. Recall that $\widehat{A} = R$, hence, by Lemma 2.3.7, $\operatorname{im} \widehat{\lambda}_r = (R : \ker \lambda_r)$.

By Lemma 2.3.9, we know that $\widehat{\lambda}_r$ is the right multiplication ρ_r by r on R. This implies that $\operatorname{im} \widehat{\lambda}_r = \operatorname{im} \rho_r = Rr$, hence the result follows. □

Corollary 3.2.7. *Let $r, s \in R$. Then, $Rr = Rs$ if and only if $\ker \lambda_r = \ker \lambda_s$.*

Lemma 3.2.8. *Let $r \in R$ and $s \in (R : \ker \lambda_r)$. The expression $\sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(-s)$ is independent of the choice of $\tau_{r,\pi}$ in $\lambda_r^{-1}(\pi)$.*

Proof. Since $\lambda_r^{-1}(\pi)$ is the coset $\tau_{r,\pi} \ker \lambda_r$ of $\ker \lambda_r$, any other choice of $\tau_{r,\pi}$ in $\lambda_r^{-1}(\pi)$ has the form $\tau_{r,\pi}\sigma$, with $\sigma \in \ker \lambda_r$. Plugging this into equation 3.1, we get an additional factor of $\sigma(-s)$, where $s \in (R : \ker \lambda_r)$. But $\sigma(-s) = 1$, so expressions agree. □

The following is a restatement of [17, Proposition 5.1].

Proposition 3.2.9. *Let $r, s \in R$. Then $\mathcal{U}(R)r = \mathcal{U}(R)s$ if and only if $Rr = Rs$.*

Corollary 3.2.10. *Let $r, s \in R$. Then, $\ker \lambda_r = \ker \lambda_s$ if and only if $r = us$, for some $u \in \mathcal{U}(R)$.*

Proof. Suppose that $\ker \lambda_r = \ker \lambda_s$. By Lemma 3.2.6,

$$Rr = (R : \ker \lambda_r) = (R : \ker \lambda_s) = Rs.$$

By Proposition 3.2.9, this implies that $r = us$ for some $u \in \mathcal{U}(R)$.

Conversely, suppose that $r = us$ for some $u \in \mathcal{U}(R)$. If $\pi \in \ker \lambda_s$, then

$${}^{r}\pi = {}^{us}\pi = {}^{u}({}^{s}\pi) = {}^{u}\mathbb{1} = \mathbb{1}.$$

This shows that $\pi \in \ker \lambda_r$. Similarly we get the other inclusion, and hence $\ker \lambda_r = \ker \lambda_s$. □

3.2.2 Total Ordering on R

In this section, we define an ordering on the ring R to get a block upper triangular form for the matrix W. Note that the collection $P = \{Rr\}_{r \in R}$ of principal left ideals of R is partially ordered with respect to set inclusion. We extend the above partial order to a total ordering on the collection P. Now we use this to define a total ordering on R as follows: we replace each principal left ideal Rr by an interval consisting of the elements in the coset $\mathcal{U}(R)r$ in some order. Not that this interval does not depend on the choice of the generator r of Rr, see Proposition 3.2.9. Our choice of total ordering then satisfies the following conditions.

Definition 3.2.11. We choose a total ordering $(R, <)$ on R satisfying the following two properties:

1. If Rr is a proper subideal of Rs, then $r < s$.

2. If $r < s$ and $Rr = Rs$, then for all t in the interval $[r, s]$ we must have $Rr = Rt = Rs$.

We then have that $0 < r$ all $r \neq 0$, and that the greatest element is a unit.

Notice that the group of units $\mathcal{U}(R)$ acts on R by left multiplication. Let $\mathcal{U}(R)\backslash R = \{\mathcal{O}_m\}_{m=0}^{t-1}$ denote the orbit space of this action. We choose a fixed representative t_m for the orbit $\mathcal{O}_m$ by $t_m = \min \mathcal{O}_m$. By our choice of the order on R, every orbit corresponds to an interval all of whose elements generate the same left ideal, that is $Rt_m = Rr$ for all $r \in \mathcal{O}_m$. Also, by Corollary 3.2.7, $\ker \lambda_{t_m} = \ker \lambda_r$, for all $r \in \mathcal{O}_m$. Finally, we choose to order the orbits to be compatible with the ordering on R, that is, for $m_1 < m_2$, we have $r < s$ for all $r \in \mathcal{O}_{m_1}$ and $s \in \mathcal{O}_{m_2}$.

Lemma 3.2.12. *For $0 \leqslant m < t$, the set of generators $\mathcal{O}_m$ of Rt_m is given by*

$$\mathcal{O}_m = Rt_m - \bigcup_{j=0}^{m-1} Rt_j.$$

Proof. Suppose that $s \in Rt_m$ and $s \notin Rt_j$, all $0 \leqslant j < m$, then we have $Rs \leqslant Rt_m$. If $Rs = Rt_m$, then by Proposition 3.2.9, s is a unit multiple of t_m, hence $s \in \mathcal{O}_m$. If $Rs < Rt_m$, then by definition $s < t_m$. Let k be such that $Rs = Rt_k$. By our choice of total ordering we have that $k < m$, and so $s \notin Rt_k$, a contradiction.

Conversely, suppose that $s \in \mathcal{O}_m$. If $s \in Rt_j$, for some $0 \leqslant j < m$, then we get that $Rt_m < Rt_j$, since s is a generator of Rt_m. By definition, we get that $t_m < t_j$ which contradicts the fact that $j < m$. Therefore, $s \notin Rt_j$, for $0 \leqslant j < m$ and the result follows. □

We use the total ordering on R to order the bases $\{e_r\}_{r\in R}$ of $\mathcal{R}$ and $\{\widehat{e}_s\}_{s\in R}$ of $\mathcal{F}(A)$ in the obvious way. That is, $r < s$ if and only if $e_r < e_s$ if and only if $\widehat{e}_r < \widehat{e}_s$.

Theorem 3.2.13. *Using the ordered bases $\{e_r\}_{r\in R}$ of $\mathcal{R}$ and $\{\widehat{e}_s\}_{s\in R}$ of $\mathcal{F}(A)$, the matrix representation of W is a block upper triangular matrix with t diagonal blocks given by:*

$$D_m = \left(W_{\widehat{e}_s, e_r}\right)_{s\in\mathcal{O}_m, r\in\mathcal{O}_m}, \text{ for } 0 \leqslant m < t.$$

Proof. Let $m > j$. We need to show that $W_{\widehat{e}_s,e_r} = 0$, for $s \in \mathcal{O}_m$ and $r \in \mathcal{O}_j$. Since $j < m$ and $s \in \mathcal{O}_m$, then by Lemma 3.2.12 $s \notin Rt_j$. That is, $s \notin (R : \ker \lambda_r)$ and so the coefficient of $\widehat{e}_s$ in the expansion of We_r equals to zero. Therefore $W_{\widehat{e}_s,e_r} = 0$ as desired. □

3.2.3 Factorization of $\mathcal{R}$ and $\mathcal{F}(A)$

.

We follow the results in [21, Section 5] in this subsection. We define the following invariant subspaces of $\mathcal{R}$ and $\mathcal{F}(A)$. Recall that $A = \widehat{R}$.

Definition 3.2.14. Let H be a subgroup of $\mathcal{U}(R)$ and K a subgroup of $\mathrm{GL}_R(A)$. Define

$$^H\mathcal{R} = \{\alpha \in \mathcal{R} : \alpha(hr) = \alpha(r), \text{ for all } h \in H, r \in R\},$$

$$\mathcal{F}(A)^H = \{w \in \mathcal{F}(A) : w(ha) = w(a), \text{ for all } h \in H, a \in A\},$$

$$^K\mathcal{F}(A) = \{w \in \mathcal{F}(A) : w(a\phi) = w(a), \text{ for all } \phi \in K, a \in A\}.$$

Lemma 3.2.15. *Let H be a subgroup of $\mathcal{U}(R)$. The set $^H\mathcal{R}$ is a right ideal of $\mathcal{R}$. In fact, $^H\mathcal{R}$ is a direct summand of $\mathcal{R}$ with a complement ^HY defined by*

$$^HY = \{\alpha \in \mathcal{R} : \sum_{h\in H} \alpha(hr) = 0, \text{ for all } r \in R\}.$$

Proof. It is clear that $^H\mathcal{R}$ is closed under addition. Let $\alpha \in {}^H\mathcal{R}$ and $\beta \in \mathcal{R}$. Then

$$\alpha\beta(hr) = \sum_{st=hr} \alpha(s)\beta(t) = \sum_{hs't=hr} \alpha(hs')\beta(t) = \sum_{s't=r} \alpha(s')\beta(t) = \alpha\beta(r).$$

This shows that $\alpha\beta \in {}^H\mathcal{R}$. Now we show that ^HY is also a right ideal of $\mathcal{R}$. Let $\gamma \in {}^HY$ and $\beta \in \mathcal{R}$. Then

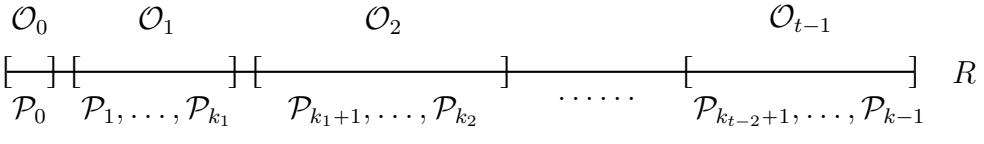
$$\sum_{h\in H} \gamma\beta(hr) = \sum_{h\in H} \sum_{st=hr} \gamma(s)\beta(t) = \sum_{s't=r} \left(\sum_{h\in H} \gamma(hs') \right) \beta(t) = 0.$$

This shows that $\gamma\beta \in {}^{H}Y$. Now we show that $\mathcal{R} = {}^{H}\mathcal{R} \oplus {}^{H}Y$. Suppose that $\alpha \in \mathcal{R}$. Define $\bar{\alpha}$ to be the average of α on the orbits of H in R. That is, $\bar{\alpha}(r) = \frac{1}{|H|}\sum_{h\in H}\alpha(hr)$, all $r \in R$. It is clear then that $\bar{\alpha}$ is an element of ${}^{H}\mathcal{R}$. Also, $\alpha - \bar{\alpha}$ belongs to ${}^{H}Y$. Indeed,

$$\begin{aligned}\sum_{h\in H}(\alpha(hr) - \bar{\alpha}(hr)) &= \sum_{h\in H}\left(\alpha(hr) - \frac{1}{|H|}\sum_{g\in H}\alpha(ghr)\right)\\ &= \sum_{h\in H}\left(\alpha(hr) - \frac{1}{|H|}\sum_{g\in H}\alpha(gr)\right)\\ &= \sum_{h\in H}\alpha(hr) - \sum_{g\in H}\alpha(gr) = 0.\end{aligned}$$

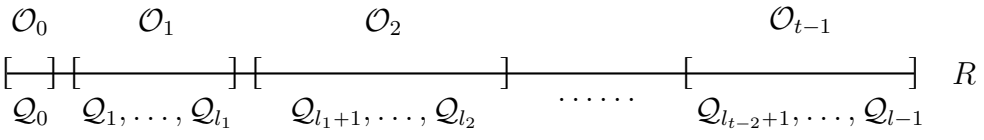
This shows that $\mathcal{R} = {}^{H}\mathcal{R} + {}^{H}Y$. And it is clear that the sum is in fact a direct sum. □

Fix a weight $w \in \mathcal{F}(A)$, and note that $w \in {}^{G_{rt}}\mathcal{F}(A) \cap \mathcal{F}(A)^{G_{lt}}$. Consider the factorizations $\mathcal{R} = {}^{G_{lt}}\mathcal{R} \oplus {}^{G_{lt}}Y$ and $\mathcal{R} = {}^{G_{rt}}\mathcal{R} \oplus {}^{G_{rt}}Y$, where G_{lt} and G_{rt} are the left and right symmetry groups of w. We will find bases for $\mathcal{R}$ that are compatible with the above factorizations. Let $G_{lt}\backslash R = \{\mathcal{P}_i\}_{i=0}^{k-1}$ be the orbit space when G_{lt} acts on R on the left, and $G_{rt}\backslash R = \{\mathcal{Q}_j\}_{j=0}^{l-1}$ be the orbit space when G_{rt} acts on R on the left. Since both G_{lt} and G_{rt} are subgroups of $\mathcal{U}(R)$, then both $\{\mathcal{P}_i\}_{i=0}^{k-1}$ and $\{\mathcal{Q}_j\}_{j=0}^{l-1}$ are refinements of $\{\mathcal{O}_m\}_{m=0}^{t-1}$, and so we choose to order them accordingly, as shown in the following chart.



(3.2)

Similarly,



(3.3)

Notice that $\mathcal{O}_0 = \mathcal{P}_0 = \mathcal{Q}_0 = \{0\}$. Using the ordering on R from Definition 3.2.11, let $r_i = \min \mathcal{P}_i$ be a fixed representative for $\mathcal{P}_i$, and $s_j = \min \mathcal{Q}_j$ be a fixed representative for $\mathcal{Q}_j$. Define

$$f_i = \frac{1}{|\mathcal{P}_i|} \sum_{r \in \mathcal{P}_i} e_r, \text{ for all } 0 \leqslant i < k,$$

$$g_j = \sum_{s \in \mathcal{Q}_j} e_s, \text{ for all } 0 \leqslant j < l.$$

Lemma 3.2.16. *The sets $\{f_i\}_{i=0}^{k-1}$ and $\{g_j\}_{i=0}^{l-1}$ form bases for the spaces ${}^{G_{lt}}\mathcal{R}$ and ${}^{G_{rt}}\mathcal{R}$, respectively.*

Proof. It is easy to see that $\{f_i\}_{i=0}^{k-1}$ is indeed a linearly independent subset of ${}^{G_{lt}}\mathcal{R}$. For any $\alpha \in {}^{G_{lt}}\mathcal{R}$, α is constant on each orbit in the orbit space $\{\mathcal{P}_i\}_{i=0}^{k-1}$. Therefore, α is written as $\alpha = \sum_{i=0}^{k-1} \alpha(r_i) f_i$. This shows that $\{f_i\}_{i=0}^{k-1}$ is a basis for ${}^{G_{lt}}\mathcal{R}$. The other part is shown similarly. □

Proposition 3.2.17. *The Fourier transform $\hat{} : {}^{G_{rt}}\mathcal{R} \to {}^{G_{rt}}\mathcal{F}(A)$ is an isomorphism of complex vector spaces.*

Proof. Consider a basis element f_i in ${}^{G_{rt}}\mathcal{R}$, we show that $\hat{f}_i$ is an element of ${}^{G_{rt}}\mathcal{F}(A)$. Let $h \in G_{rt}$,

$$\begin{aligned}\hat{f}_i(\pi^h) &= \sum_{r \in R} f_i(r)\pi^h(r) = \sum_{r \in R} f_i(r)\pi(hr) \\ &= \sum_{s \in R} f_i(h^{-1}s)\pi(s) = \sum_{s \in R} f_i(s)\pi(s) = \hat{f}_i(\pi).\end{aligned}$$

This shows that $\hat{f}_i$ is an element of ${}^{G_{rt}}\mathcal{F}(A)$. Conversely, we show that the inverse Fourier

transform maps ${}^{G_{rt}}\mathcal{F}(A)$ to ${}^{G_{rt}}\mathcal{R}$. Let $f \in {}^{G_{rt}}\mathcal{F}(A)$ and $h \in G_{rt}$, we have

$$\begin{aligned}\check{f}(hr) &= \frac{1}{|R|}\sum_{\pi\in A} f(\pi)\pi(-hr) = \frac{1}{|R|}\sum_{\pi\in A} f(\pi)\pi^h(-r) \\ &= \frac{1}{|R|}\sum_{\sigma\in A} f(\sigma^{h^{-1}})\sigma(-r) = \frac{1}{|R|}\sum_{\sigma\in A} f(\sigma)\sigma(-r) = \check{f}(r).\end{aligned}$$

This shows that $\check{f}$ is an element of ${}^{G_{rt}}\mathcal{R}$. □

Corollary 3.2.18. *The set* $\{\widehat{g}_j = \sum_{s\in\mathcal{Q}_j} \widehat{e}_s\}_{j=0}^{l-1}$ *forms a basis for* ${}^{G_{rt}}\mathcal{F}(A)$.

Proof. Follows directly from Lemma 3.2.16 and Proposition 3.2.17. □

Now we extend $\{f_i\}_{i=0}^{k-1}$ to a basis for the space $\mathcal{R}$ using the factorization $\mathcal{R} = {}^{G_{lt}}\mathcal{R}\oplus^{G_{lt}}Y$. Let $\{f_k, \ldots, f_{|R|-1}\}$ be a basis for ${}^{G_{lt}}Y$. Then $\{f_i\}_{i=0}^{|R|-1}$ is a basis for $\mathcal{R}$ that is compatible with the above factorization. Similarly, we extend the basis $\{\widehat{g}_j\}_{j=0}^{l-1}$ to $\{\widehat{g}_j\}_{j=0}^{|R|-1}$ a basis for the whole space $\mathcal{F}(A)$.

Lemma 3.2.19. *Under the map* $w : \mathcal{R} \to \mathcal{F}(A)$, *we have* $w^{G_{lt}}Y = 0$ *and* $w\mathcal{R} \subset {}^{G_{rt}}\mathcal{F}(A)$.

Proof. Let $\alpha \in {}^{G_{lt}}Y$. Since $w \in \mathcal{F}(A)^{G_{lt}}$, then for $\pi \in A$ we have

$$\begin{aligned}w\alpha(\pi) &= \sum_{r\in R} w({}^r\pi)\alpha(r) \\ &= \frac{1}{|G_{lt}|}\sum_{r\in R}\sum_{h\in G_{lt}} w({}^{hr}\pi)\alpha(r) \\ &= \frac{1}{|G_{lt}|}\sum_{h\in G_{lt}}\sum_{s\in R} w({}^s\pi)\alpha(h^{-1}s) \\ &= \sum_{s\in R} w({}^s\pi)\left(\frac{1}{|G_{lt}|}\sum_{h\in G_{lt}}\alpha(h^{-1}s)\right) = 0\end{aligned}$$

since $h \in G_{lt}$ and $\alpha \in {}^{G_{lt}}Y$. This shows that $w^{G_{lt}}Y = 0$.

Let $\alpha \in \mathcal{R}$, $h \in G_{rt}$ and $\pi \in A$. Then

$$w\alpha(\pi^h) = \sum_{r\in R} w({}^r\pi^h)\alpha(r) = \sum_{r\in R} w({}^r\pi)\alpha(r) = w\alpha(\pi).$$

Therefore we indeed have $w\mathcal{R} \subset {}^{G_{rt}}\mathcal{F}(A)$. □

In the following we show that the entry $W_{\hat{e}_s,e_r}$ depends only on the orbits of r and s under the appropriate actions.

Theorem 3.2.20. *Let r and s be elements of R such that $r \in \mathcal{P}_i$ and $s \in \mathcal{Q}_j$. Then*

$$W_{\hat{e}_s,e_r} = W_{\hat{e}_{s_j},e_{r_i}}.$$

Proof. Since $s \in \mathcal{Q}_j = \mathrm{orb}(s_j)$, then $s = us_j$ for some $u \in G_{rt}$. It is clear $s \in (R : \ker \lambda_r)$ if and only if $s_j \in (R : \ker \lambda_r)$. If $s, s_j \notin (R : \ker \lambda_r)$, then $W_{\hat{e}_s,e_r} = W_{\hat{e}_{s_j},e_r} = 0$, by equation 3.1. Otherwise, suppose that $s, s_j \in (R : \ker \lambda_r)$, then by Lemma 3.2.6 $s_j = tr$ for some $t \in R$, so we have $s = us_j = utr$. Therefore, by the right symmetry of w and by the fact that $\operatorname{im} \lambda_r$ is a right submodule,

$$\begin{aligned}
\frac{|R|}{|\ker \lambda_r|} W_{\hat{e}_{-s},e_r} &= \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(s) \\
&= \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(utr) = \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)^r \tau_{r,\pi}(ut) \\
&= \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\pi(ut) = \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\pi^u(t) \\
&= \sum_{\rho \in \operatorname{im} \lambda_r} w(\rho^{u^{-1}})\rho(t) = \sum_{\rho \in \operatorname{im} \lambda_r} w(\rho)\rho(t) \\
&= \sum_{\rho \in \operatorname{im} \lambda_r} w(\rho)\tau_{r,\rho}(tr) = \sum_{\rho \in \operatorname{im} \lambda_r} w(\rho)\tau_{r,\rho}(s_j) = \frac{|R|}{|\ker \lambda_r|} W_{\hat{e}_{-s_j},e_r}.
\end{aligned}$$

Similarly, since $r \in \mathcal{P}_i = \mathrm{orb}(r_i)$, then $r = ur_i$ for some $u \in G_{lt}$. Suppose that $s \in (R : \ker \lambda_r) = (R : \ker \lambda_{r_i})$. It is clear that $\operatorname{im} \lambda_r = u \operatorname{im} \lambda_{r_i}$ and that $|\ker \lambda_r| = |\ker \lambda_{r_i}|$, therefore

$$\frac{|R|}{|\ker \lambda_r|} W_{\hat{e}_{-s},e_r} = \sum_{\pi \in \operatorname{im} \lambda_r} w(\pi)\tau_{r,\pi}(s) = \sum_{\pi \in u \operatorname{im} \lambda_{r_i}} w(\pi)\tau_{r,\pi}(s) = \sum_{\rho \in \operatorname{im} \lambda_{r_i}} w({}^u\rho)\tau_{r,\pi}(s).$$

Notice that, if $\pi = {}^{u}\rho$, then any $\tau \in \lambda_r^{-1}(\pi)$ is an element of $\lambda_{r_i}^{-1}(\rho)$ as well. In fact

$$ {}^{r_i}\tau = {}^{u^{-1}r}\tau = {}^{u^{-1}}({}^{r}\tau) = {}^{u^{-1}}\pi = \rho. $$

Therefore $\tau_{r,\pi} \in \lambda_{r_i}^{-1}(\rho)$. Thus, by Lemma 3.2.8 and left symmetry of w, we have

$$ \frac{|R|}{|\ker \lambda_r|} W_{\hat{e}_{-s},e_r} = \sum_{\rho \in \operatorname{im} \lambda_{r_i}} w({}^{u}\rho)\tau_{r,\pi}(s) = \sum_{\rho \in \operatorname{im} \lambda_{r_i}} w(\rho)\tau_{r_i,\rho}(s) = \frac{|R|}{|\ker \lambda_{r_i}|} W_{\hat{e}_{-s},e_{r_i}} $$

This shows that $W_{\hat{e}_s,e_r} = W_{\hat{e}_{s_j},e_{r_i}}$. □

Theorem 3.2.21. *Under the bases $\{f_i\}_{i=0}^{|R|-1}$ and $\{\hat{g}_j\}_{j=0}^{|R|-1}$, the matrix representation W^2 of w is given by*

$$ W^2 = \left[\begin{array}{c|c} \left(W_{\hat{e}_{s_j},e_{r_i}}\right)_{\substack{0 \leqslant i < k \\ 0 \leqslant j < l}} & 0 \\ \hline 0 & 0 \end{array}\right] $$

Proof. By Lemma 3.2.19, $wf_i = 0$, for $i \geqslant k$. Also, $wf_i \in {}^{G_{rt}}\mathcal{F}(A)$, therefore wf_i is written as a linear combination of $\{\widehat{g}_j\}_{j=0}^{l-1}$ as follows.

$$ \begin{aligned} wf_i &= \frac{1}{|\mathcal{P}_i|} \sum_{r \in \mathcal{P}_i} we_r = \frac{1}{|\mathcal{P}_i|} \sum_{r \in \mathcal{P}_i} \sum_{s \in R} W_{\hat{e}_s,e_r} \widehat{e}_s \\ &= \frac{1}{|\mathcal{P}_i|} \sum_{s \in R} \sum_{r \in \mathcal{P}_i} W_{\hat{e}_s,e_r} \widehat{e}_s = \frac{1}{|\mathcal{P}_i|} \sum_{s \in R} |\mathcal{P}_i| W_{\hat{e}_s,e_{r_i}} \widehat{e}_s \\ &= \sum_{j=0}^{l} \sum_{s \in \mathcal{Q}_j} W_{\hat{e}_s,e_{r_i}} \widehat{e}_s = \sum_{j=0}^{l} W_{\hat{e}_{s_j},e_{r_i}} \sum_{s \in \mathcal{Q}_j} \widehat{e}_s = \sum_{j=0}^{l} W_{\hat{e}_{s_j},e_{r_i}} \widehat{g}_j, \end{aligned} \tag{3.4} $$

as desired. □

Corollary 3.2.22. *The left multiplication by w reduces to a map $\bar{w} : {}^{G_{lt}}\mathcal{R} \to {}^{G_{rt}}\mathcal{F}(A)$.*

Recall that $\{\mathcal{O}_m\}_{m=0}^{t-1}$ is the orbit space of the left action of $\mathcal{U}(R)$ on R. Let t_m be a fixed representative of the orbit $\mathcal{O}_m$ chosen by $t_m = \min \mathcal{O}_m$, for $0 \leqslant m < t$.

Theorem 3.2.23. *Under the bases $\{f_i\}_{i=0}^{k-1}$ and $\{\widehat{g}_j\}_{j=0}^{l-1}$, the matrix representation $\overline{W}$ of the*

induced $\overline{w} : {}^{G_{lt}}\mathcal{R} \to {}^{G_{rt}}\mathcal{F}(A)$ *is an* $l \times k$ *matrix given by*

$$\overline{W}_{\hat{g}_j, f_i} = W_{\hat{e}_{s_j}, e_{r_i}}, \text{ for } 0 \leqslant i < k \text{ and } 0 \leqslant j < l.$$

Moreover, $\overline{W}$ *is a block upper triangular matrix with* t *diagonal blocks given by*

$$\overline{W}_{\hat{g}_j, f_i} = \frac{|\ker \lambda_{t_m}|}{|R|} \sum_{\pi \in t_m A} w({}^{v}\pi)\chi(\pi^{u}), \text{ where}$$

$u \in G_{lt}\backslash\mathcal{U}(R)/Stab(t_m)$, $v \in G_{rt}\backslash\mathcal{U}(R)/Stab(t_m)$, *for* $0 \leqslant m \leqslant t-1$, *and* χ *is the generating character from Lemma 2.4.4.*

Proof. Let $0 \leqslant m \leqslant t-1$. Refer to charts 3.2 and 3.3, we have that $\mathcal{O}_m = \mathcal{P}_{k_{m-1}+1} \cup \cdots \cup \mathcal{P}_{k_m} = \mathcal{Q}_{l_{m-1}+1} \cup \cdots \cup \mathcal{Q}_{l_m}$. Let $k_m + 1 \leqslant i \leqslant k_{m+1}$ and $l_m + 1 \leqslant j \leqslant l_{m+1}$. The entry $\overline{W}_{\hat{g}_j, f_i} = W_{\hat{e}_{s_j}, e_{r_i}}$, by equation 3.4. Therefore, the matrix $\overline{W}$ is a block upper triangular matrix by Theorem 3.2.13.

Let $r_i, s_j \in \mathcal{O}_m$, then $r_i = ut_m$ and $s_j = vt_m$ for some $u, v \in \mathcal{U}(R)$. We would like to understand the restrictions that we can put on u and v to guarantee a unique way of describing each entry in the matrix. Notice that u and v need to only be considered up to $\mathrm{Stab}(t_m)$, the stabilizer of t_m under the action $\mathcal{U}(R)\backslash R$. That is, if $r_i = ut_m = u_1 t_m$, then $u\mathrm{Stab}(t_m) = u_1\mathrm{Stab}(t_m)$, hence $u = u_1$ in the quotient $\mathcal{U}(R)/\mathrm{Stab}(t_m)$. Similarly for v. Also, if $u' \in G_{lt}$, then $u'ut_m = u'r_i$ is an element of $\mathcal{P}_i$ which represents the same basis element f_i. Hence u is only considered up to the quotient $G_{lt}\backslash\mathcal{U}(R)$. That is, u can be thought of as an element in the double quotient $G_{lt}\backslash\mathcal{U}(R)/\mathrm{Stab}(t_m)$. Similarly $v \in G_{rt}\backslash\mathcal{U}(R)/\mathrm{Stab}(t_m)$. Notice that $s_j = vu^{-1}r_i$, and that $|\ker \lambda_{r_i}| = |\ker \lambda_{t_m}|$ by Corollary 3.2.10. Also $\sigma \in \operatorname{im} \lambda_{t_m}$

if and only if ${}^u\sigma \in \operatorname{im}\lambda_{r_i}$. By (3.1), we have

$$\begin{aligned}\frac{|R|}{|\ker\lambda_{t_m}|}\overline{W}_{\hat{g}_j,f_i} &= \frac{|R|}{|\ker\lambda_{r_i}|}W_{\hat{e}_{s_j},e_{r_i}} = \sum_{\pi\in\operatorname{im}\lambda_{r_i}}\overline{w}(\pi)\tau_{r_i\pi}(-s_j) = \sum_{\sigma\in\operatorname{im}\lambda_{t_m}} w({}^u\sigma)\tau_{r_i,{}^u\sigma}(-vu^{-1}r_i)\\ &= \sum_{\sigma\in\operatorname{im}\lambda_{t_m}} w({}^u\sigma)^{r_i}\tau_{r_i,{}^u\sigma}(-vu^{-1}) = \sum_{\sigma\in\operatorname{im}\lambda_{t_m}} w({}^u\sigma)^{u}\sigma(-vu^{-1})\\ &= \sum_{\sigma\in\operatorname{im}\lambda_{t_m}} w({}^u\sigma)\sigma(-v) = \sum_{\sigma\in\operatorname{im}\lambda_{t_m}} w({}^u\sigma)\sigma^v(-1) = \sum_{\sigma\in\operatorname{im}\lambda_{t_m}} w({}^u\sigma)\chi(\sigma^v). \qquad \square\end{aligned}$$

Now, suppose that w has maximal symmetry, that is $G_{rt} = G_{lt} = \mathcal{U}(R)$. In this case every block of the matrix $\overline{W}$ described above is in fact a 1×1 block, as both $G_{rt}\backslash\mathcal{U}(R)/\mathrm{Stab}(t_m)$ and $G_{lt}\backslash\mathcal{U}(R)/\mathrm{Stab}(t_m)$ reduce to one element. Also, $\min\mathcal{P}_m = \min\mathcal{Q}_m = \min\mathcal{O}_m = t_m$, for $1 \leqslant m < t$.

Theorem 3.2.24. *Let w have maximal symmetry. Then $\overline{W}$ is a $t\times t$ upper triangular matrix with diagonal entries*

$$\overline{W}_{\hat{g}_m,f_m} = \frac{|\ker\lambda_{t_m}|}{|R|}\sum_{\pi\in\operatorname{im}\lambda_{t_m}} w(\pi)\chi(\pi), \text{ for } 0 \leqslant m < t, \text{ where } t_m = \min\mathcal{O}_m,$$

where χ is the generating character for the Frobenius bimodule A.

Proof. Since $\min\mathcal{P}_m = \min\mathcal{Q}_m = \min\mathcal{O}_m = t_m$, then $u = v = 1$ from the proof of Theorem 3.2.23. Using Theorem 3.2.23 with $u = v = 1$ we get

$$\overline{W}_{\hat{g}_m,f_m} = \frac{|\ker\lambda_{t_m}|}{|R|}\sum_{\pi\in\operatorname{im}\lambda_{t_m}} w(\pi)\chi(\pi). \qquad \square$$

Corollary 3.2.25. *Let w have maximal symmetry. Then determinant $\overline{W}$ is given by*

$$\det\overline{W} = \prod_{m=0}^{t-1}\left(\frac{|\ker\lambda_{t_m}|}{|R|}\sum_{\pi\in\operatorname{im}\lambda_{t_m}} w(\pi)\chi(\pi)\right), \text{ where } t_m = \min\mathcal{O}_m.$$

3.3 The Extension Property

In this section we use symmetrized weight compositions to prove our main result about the extension property. Let's first recall the definition of symmetrized weight compositions on an alphabet module A.

Definition 3.3.1. Let $G_{rt} \subseteq \mathrm{GL}_R(A)$ be a subgroup of the group $\mathrm{GL}_R(A)$ of all R-automorphisms on A. The symmetrized weight composition is a function $\mathrm{swc} : A^n \times A/G_{rt} \to \mathbb{N}$ defined by

$$\mathrm{swc}_a(x) = |\{i : x_i \in \mathrm{orb}(a)\}|, \text{ all } x \in A^n, \mathrm{orb}(a) \in A/G_{rt}$$

The following result is Theorem 13 in [5].

Theorem 3.3.2. *Let A be a Frobenius bimodule over a finite ring R. Then A has the extension property with respect to the symmetrized weight composition.*

We use that fact that the symmetrized weight composition has the extension property over Frobenius bimodules, in particular over $A = \widehat{R}$, to show the following.

Theorem 3.3.3. *If $\overline{W}$ has a zero left null space, then w has the extension property.*

Proof. Let $f : \mathcal{C}_1 \to \mathcal{C}_2$ be a w-isometry of left linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq A^n$. Our goal is to show that f extends to a monomial transformation on the ambient space A^n.

Fix $x \in \mathcal{C}_1$. Then $\mathrm{swc}(x)$ can be thought of as a function from A to $\mathbb{C}$ that is constant on the right G_{rt}-orbits on A, that is $\mathrm{swc}(x)$ is a weight function on A with right symmetry group G_{rt}, hence $\mathrm{swc}(x) \in {}^{G_{rt}}\mathcal{F}(A)$.

Since $\overline{W}$ is the matrix representation of the map $\bar{w} : {}^{G_{lt}}\mathcal{R} \to {}^{G_{rt}}\mathcal{F}(A)$ and since $\overline{W}$ has zero left null space, then the map $\bar{w}$ is surjective. Indeed, the dimension of $\mathrm{im}\,\bar{w}$ plus the left nullity of $\overline{W}$ is equal to the dimension of ${}^{G_{rt}}\mathcal{F}(A)$, but since $\overline{W}$ has a zero left null space, then $\dim(\mathrm{im}\,\bar{w}) = \dim({}^{G_{rt}}\mathcal{F}(A))$ and hence $\bar{w}$ is surjective. Therefore, there is α in ${}^{G_{lt}}\mathcal{R}$ such that $\bar{w}(\alpha) = w\alpha = \mathrm{swc}(x)$. By Proposition 3.2.2, f is a $\mathrm{swc}(x)$-isometry. By Theorem 3.3.2, f extends to a G_{rt}-monomial transformation of A^n. □

The following is a our main theorem for this chapter. It follows directly from Theorem 3.3.3.

Theorem 3.3.4. *Let $A = \widehat{R}$. If each of the diagonal blocks*

$$\overline{W}_{\widehat{g}_j, f_i} = \frac{|\ker \lambda_{t_m}|}{|R|} \sum_{\pi \in t_m A} w({}^v\pi)\chi(\pi^u), \text{ where}$$

$u \in G_{lt} \backslash \mathcal{U}(R)/Stab(t_m)$ and $v \in G_{rt} \backslash \mathcal{U}(R)/Stab(t_m)$, for $0 \leqslant m \leqslant t-1$, has zero left null space, then w has the extension property.

Corollary 3.3.5. *Let w have maximal right symmetry. Suppose that*

$$\sum_{\pi \in rA} w(\pi)\chi(\pi) \neq 0, \text{ for all } r \in R.$$

Then w has the extension property.

Proof. By Theorem 3.2.24, $\det \overline{W} \neq 0$ and thus $\overline{W}$ has a zero left null space. Hence w has the extension property, by Theorem 3.3.3. □

Chapter 4

Failure of the MacWilliams Identities

The MacWilliams identities give a relation between the Hamming weight enumerator of a linear code and the Hamming weight enumerator of its dual. The MacWilliams identities are valid for linear codes over a finite Frobenius ring of size q with respect to the Hamming weight [17]. We are interested in the question of whether there is some version of the MacWilliams identities for other alphabets and other weight functions. In this chapter we focus on the Lee weight over $\mathbb{Z}_m$, the integers modulo m.

4.1 Preliminaries

We need the following definitions and terminology.

Definition 4.1.1. Let R be a finite ring with 1. The Hamming weight $\mathrm{H} : R \to \mathbb{N}$ on R is defined by $\mathrm{H}(r) = 1$ for all nonzero $r \in R$ and $\mathrm{H}(0) = 0$. The Hamming weight extends to vectors $x = (x_1, \ldots, x_n) \in R^n$ by $\mathrm{H}(x) = \sum_{i=1}^{n} \mathrm{H}(x_i)$.

The Hamming weight enumerator is defined by the following.

Definition 4.1.2. The Hamming weight enumerator for a code $\mathcal{C} \subset R^n$ over R is an element

in the polynomial ring $\mathbb{C}[X, Y]$ given by

$$\mathrm{hwe}_{\mathcal{C}}(X, Y) = \sum_{c \in \mathcal{C}} X^{n-\mathrm{H}(c)} Y^{\mathrm{H}(c)}.$$

Recall the definition of a dual code, Definition 2.1.4. MacWilliams showed in [13] that there is a relation between the Hamming weight enumerator of a linear code and the Hamming weight enumerator of its dual. These relations are known as the MacWilliams identities.

Theorem 4.1.3 (MacWilliams Identities)**.** *For a linear code $\mathcal{C}$ over a finite field $\mathbb{F}_q$, the Hamming weight enumerator of $\mathcal{C}^{\perp}$ is given by*

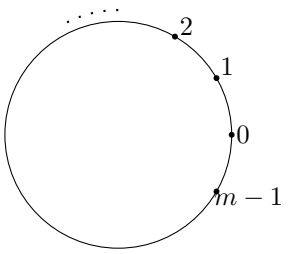
$$\mathrm{hwe}_{\mathcal{C}^{\perp}}(X, Y) = \frac{1}{|\mathcal{C}|} \mathrm{hwe}_{\mathcal{C}}(X + (q-1)Y, X - Y),$$

The same statement of the MacWilliams identities is valid for linear codes over a finite Frobenius ring of size q with respect to the Hamming weight [17]. We are interested in the question of whether there is some version of the MacWilliams identities for Lee weight over $\mathbb{Z}_m$.

Recall that a linear code $\mathcal{C}$ of length n over $\mathbb{Z}_m$ is a submodule of $\mathbb{Z}_m^n$. Vectors $v \in \mathbb{Z}_m^n$ have the form $v = (v_1, \ldots, v_n)$. The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ in $\mathbb{Z}_m^n$ is defined by $\mathcal{C}^{\perp} = \{v \in \mathbb{Z}_m^n : \sum_{i=1}^{n} v_i c_i = 0, \text{ for all } c \in \mathcal{C}\}$.

Definition 4.1.4. The Lee weight is defined on $\mathbb{Z}_m$ by $\mathrm{L}_m(i) = |i|$, the ordinary absolute value on $\mathbb{Z}$, where $\mathbb{Z}_m$ is thought of as $\mathbb{Z}_m = \{i \in \mathbb{Z} : -m/2 < i \leqslant m/2\}$.

The Lee weight essentially measures the distance from zero when the elements of $\mathbb{Z}_m$ are represented on a circle as shown below.



Example 4.1.5. The Lee weight over $\mathbb{Z}_6$ is given by:

$$\begin{aligned} \mathrm{L}_6 : \mathbb{Z}_6 &\to \mathbb{N} \\ -2 &\mapsto 2 \\ -1 &\mapsto 1 \\ 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ 2 &\mapsto 2 \\ 3 &\mapsto 3 \end{aligned}$$

We will write just $\mathrm{L}(i)$ when m is obvious from context. For vectors $v \in \mathbb{Z}_m^n$, define $\mathrm{L}(v) = \sum_{i=1}^{n} \mathrm{L}(v_i)$. For a linear code $\mathcal{C}$ of length n over $\mathbb{Z}_m$, the maximum Lee weight in $\mathcal{C}$ is $n\lfloor m/2 \rfloor$.

Definition 4.1.6. The Lee weight enumerator of a code $\mathcal{C} \subset \mathbb{Z}_m^n$ is an element in the polynomial ring $\mathbb{C}[X, Y]$ given by

$$\mathrm{lwe}_{\mathcal{C}}(X, Y) = \sum_{c \in \mathcal{C}} X^{n\lfloor \frac{m}{2} \rfloor - \mathrm{L}(c)} Y^{\mathrm{L}(c)}.$$

Let $A_i(\mathcal{C})$ denote the number of codewords of Lee weight i in $\mathcal{C}$, that is, $A_i(\mathcal{C}) = |\{c \in \mathcal{C} : \mathrm{L}(c) = i\}|$, for $0 \leqslant i \leqslant n\lfloor m/2 \rfloor$. The Lee weight enumerator of $\mathcal{C}$ can then be rewritten as

$$\mathrm{lwe}_{\mathcal{C}}(X, Y) = \sum_{i=0}^{n\lfloor m/2 \rfloor} A_i(\mathcal{C}) X^{n\lfloor \frac{m}{2} \rfloor - i} Y^i.$$

Our main goal in this chapter is to study the existence of the MacWilliams identities over $\mathbb{Z}_m$ with respect to the Lee weight. The Lee weight and the Hamming weight are equal when $m = 2$ or $m = 3$; thus the MacWilliams identities for Lee weight are valid in those cases. For codes over $\mathbb{Z}_4$, we have the following theorem.

Theorem 4.1.7 ([9]). *The Lee weight enumerator of a linear code $\mathcal{C}$ over $\mathbb{Z}_4$ and the Lee weight enumerator of its dual are related:*

$$\mathrm{lwe}_{\mathcal{C}^\perp}(X, Y) = \frac{1}{|\mathcal{C}|}\,\mathrm{lwe}_{\mathcal{C}}(X + Y, X - Y).$$

4.2 Main Theorem and a Proof Outline

For $m \geqslant 5$, it was shown in [16] that the change of variables $X \mapsto X + (q-1)Y$ and $Y \mapsto X - Y$ does not give a version of the MacWilliams identities for any prime power q with $q|m$. The main result of this chapter is that there is no well-defined relation between the Lee weight enumerators of a code and its dual for $m \geqslant 5$. Specifically, we prove the following

Theorem 4.2.1 (Theorem 1.1,[1]). *Suppose $m \geqslant 5$. There exist linear codes $\mathcal{C}_1, \mathcal{C}_2$ over $\mathbb{Z}_m$ satisfying $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ and $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$.*

Let $\mathcal{LC}(\mathbb{Z}_m)$ denote the collection of all linear codes over $\mathbb{Z}_m$, and let $\perp$: $\mathcal{LC}(\mathbb{Z}_m) \to \mathcal{LC}(\mathbb{Z}_m)$ denote the map sending a linear code $\mathcal{C}$ to its dual code $\mathcal{C}^\perp$. Then Theorem 4.2.1 says that it is impossible to find a well-defined map making the following diagram commute.

$$\begin{array}{ccc} \mathcal{LC}(\mathbb{Z}_m) & \xrightarrow{\ \perp\ } & \mathcal{LC}(\mathbb{Z}_m) \\ {\scriptstyle \mathrm{lwe}}\downarrow & & \downarrow{\scriptstyle \mathrm{lwe}} \\ \mathbb{C}[X, Y] & \overset{?}{\dashrightarrow} & \mathbb{C}[X, Y] \end{array}$$

Corollary 4.2.2. *There is not any type of MacWilliams identities relating the Lee weight enumerators of linear codes and their dual codes over $\mathbb{Z}_m$, for $m \geqslant 5$.*

Here is an outline of the proof of Theorem 4.2.1, which will also serve as a guide to the rest of this chapter. Explicit examples of linear codes $\mathcal{C}_1, \mathcal{C}_2$ over $\mathbb{Z}_m$ satisfying $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ and $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ are constructed: in an ad hoc fashion for $m = 5, 6, 8, 9$ (in Section 4.3), and in a systematic fashion for all primes $p \geqslant 7$ (in Section 4.4).

To handle other values of $m \geqslant 5$, which necessarily are integer multiples of the preceding cases, in Section 4.5 we analyze the relationship between a linear code $\mathcal{C} \subseteq \mathbb{Z}_m^n$ and the linear code $a\mathcal{C} \subseteq \mathbb{Z}_{am}^n$ defined by scalar multiplying each codeword of $\mathcal{C}$ by a. In particular, Lemma 4.5.1 shows that $\mathrm{lwe}_{\mathcal{C}}$ determines $\mathrm{lwe}_{a\mathcal{C}}$, so that $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ will imply $\mathrm{lwe}_{a\mathcal{C}_1} = \mathrm{lwe}_{a\mathcal{C}_2}$, which is Corollary 4.5.2. On the other hand, Lemma 4.5.3 allows us to compare the number of codewords of sufficiently small weight in $\mathcal{C}^\perp$ and $(a\mathcal{C})^\perp$. Consequently, if $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ because the number of codewords of a sufficiently small weight differ, then the same will be true for $(a\mathcal{C}_1)^\perp$ and $(a\mathcal{C}_2)^\perp$, so that $\mathrm{lwe}_{(a\mathcal{C}_1)^\perp} \neq \mathrm{lwe}_{(a\mathcal{C}_2)^\perp}$, which is Corollary 4.5.4.

4.3 Examples for Small Values of m

In the following we will present examples of pairs of codes $\mathcal{C}_1, \mathcal{C}_2$ with $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ and $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ over $\mathbb{Z}_m$, for $m = 5, 6, 8, 9$.

Example 4.3.1. Let $m = 5$. We will describe the codes using multiplicity functions from Section 2.5. Our codes are of dimension 2, the multiplicity functions $\eta_1, \eta_2 : \mathbb{Z}_5^2/\{\pm 1\} \to \mathbb{N}$ are given by the following table.

$\mathbb{Z}_5^2/\{\pm 1\}$	0	0	1	1	1	1	1	2	2	2	2	2
	1	2	−2	−1	0	1	2	−2	−1	0	1	2
Multiplicity η_1	5	5	5	5	10	5	5	5	5	10	5	5
Multiplicity η_2	9	6	8	5	9	8	5	5	2	6	5	2

Let G_1 and G_2 be generator matrices corresponding to the multiplicity functions η_1 and η_2. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the codes generated by G_1 and G_2.

The Lee weight enumerators of $\mathcal{C}_1$ and $\mathcal{C}_2$ are given by

$$\mathrm{lwe}_{\mathcal{C}_1}(X,Y) = \mathrm{lwe}_{\mathcal{C}_2}(X,Y) = X^{140} + 4X^{65}Y^{75} + 20X^{50}Y^{90}.$$

But $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$. In fact, $A_2(\mathcal{C}_1^\perp) = 380$ and $A_2(\mathcal{C}_2^\perp) = 400$. The counts for A_2 are obtained as follows. A dual codeword of Lee weight 2 has either one nonzero entry of the form ± 2 or two nonzero entries of the form $\pm 1, \pm 1$. There are no dual codewords of the first type (i.e., a single ± 2) because there are no zero columns in G_1 or G_2. Dual codewords of the second type (i.e., two ± 1s) must occur with opposite signs, because no column type is annihilated by 2 and no two column types sum to zero. The only dual codewords of the second type arise by subtracting, in either order, columns of the same type. Thus

$$A_2(\mathcal{C}_i^\perp) = 2\sum_{\eta} \binom{\eta}{2} = \begin{cases} 380, & i = 1, \\ 400, & i = 2, \end{cases}$$

where the sum is over the multiplicities η given in the table.

Example 4.3.2. Let $m = 6$. Consider the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ generated by

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}, \qquad G_2 = \begin{bmatrix} 1 & 1 & 3 & 3 \end{bmatrix}.$$

Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are given by

$$\mathcal{C}_1 = \{(0,0,0,0), (1,1,1,1), (2,2,2,2), (3,3,3,3), (4,4,4,4), (5,5,5,5)\},$$

$$\mathcal{C}_2 = \{(0,0,0,0), (1,1,3,3), (2,2,0,0), (3,3,3,3), (4,4,0,0), (5,5,3,3)\}.$$

Then $\mathrm{lwe}_{\mathcal{C}_1}(X,Y) = \mathrm{lwe}_{\mathcal{C}_2}(X,Y) = X^{12} + 2X^8Y^4 + 2X^4Y^8 + Y^{12}$.

We show that $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ by showing that $A_2(\mathcal{C}_1^\perp) \neq A_2(\mathcal{C}_2^\perp)$. As we saw in Example 4.3.1, a dual codeword of weight 2 either contains a single nonzero entry of ± 2 or two nonzero entries of ± 1. For $\mathcal{C}_1$, since none of the columns of G_1 is annihilated by ± 2, then all the codewords of weight 2 in $\mathcal{C}_1^\perp$ contain two nonzero entries of ± 1. It is easy to see that

if the two nonzero entries of such a codeword are equal, both equal to 1 or both equal to -1, then that codeword does not annihilate G_1. But if one entry is 1 and the other is -1 then that codeword does indeed annihilate G_1. There are $4 \cdot 3 = 12$ such vectors of length 4. Thus $A_2(\mathcal{C}_1^\perp) = 12$.

For $\mathcal{C}_2^\perp$, the third and the fourth columns of G_2 are annihilated by ± 2, therefore the four codewords $(0, 0, \pm 2, 0)$, $(0, 0, 0, \pm 2)$ are elements of $\mathcal{C}_2^\perp$. Also, adding or subtracting the last two columns of G_2 gives the zero column, therefore the four codewords $(0, 0, \pm 1, \pm 1)$ are all elements of $\mathcal{C}_2^\perp$. Finally, since the first two columns of G_2 are identical, then we get that $(1, -1, 0, 0), (-1, 1, 0, 0)$ are codewords in $\mathcal{C}_2^\perp$. Thus $A_2(\mathcal{C}_2^\perp) = 10$, and $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$.

The following example is due the referee of [20, Example 5.5] and also appeared in [15].

Example 4.3.3. Let $m = 8$. Consider the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ generated by

$$G_1 = \begin{bmatrix} 1 & 1 & 2 \end{bmatrix}, \qquad G_2 = \begin{bmatrix} 1 & 3 & 4 \end{bmatrix}.$$

We get $\mathrm{lwe}_{\mathcal{C}_1}(X, Y) = \mathrm{lwe}_{\mathcal{C}_2}(X, Y) = X^{12} + 2X^8Y^4 + 5X^4Y^8$.

We show that $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ by showing that $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$ have different numbers of codewords of weight 3. Suppose that $c = (c_1, c_2, c_3)$ has weight 3. Then c is an element of $\mathcal{C}_1^\perp$ if and only if $G_1 c^T = 0$, i.e., $c_1 + c_2 + 2c_3 = 0$. Since $\mathrm{L}(c) = 3$, the entries c_1, c_2, and c_3 can have values from $\{0, \pm 1, \pm 2, \pm 3\}$ only. It is straight forward to find that the solutions of $c_1 + c_2 + 2c_3 = 0$ with those restrictions are

$$\{(-1, -1, 1), (1, 1, -1), (2, 0, -1), (2, -1, 0), (-2, 0, 1), (-2, 1, 0)\}.$$

Thus $A_3(\mathcal{C}_1^\perp) = 6$. Similarly, we find that the codewords of weight 3 in $\mathcal{C}_2^\perp$ are

$$\{(1, 1, 1), (-1, -1, -1), (-1, -1, 1), (1, 1, -1)\}.$$

Thus $A_3(\mathcal{C}_2^\perp) = 4$. This shows that $A_3(\mathcal{C}_1^\perp) \neq A_3(\mathcal{C}_2^\perp)$ and hence $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$.

Example 4.3.4. Let $m = 9$. Define the multiplicity functions $\eta_1, \eta_2 : \mathbb{Z}_9/\{\pm 1\} \to \mathbb{N}$ by

$$\begin{array}{rcl|rcl} \eta_1 : \mathbb{Z}_9/\{\pm 1\} & \to \mathbb{N}, & \eta_2 : \mathbb{Z}_9/\{\pm 1\} & \to \mathbb{N} \\ 0 & \mapsto 0 & 0 & \mapsto 7 \\ 1 & \mapsto 33 & 1 & \mapsto 9 \\ 2 & \mapsto 24 & 2 & \mapsto 81 \\ 3 & \mapsto 70 & 3 & \mapsto 0 \\ 4 & \mapsto 6 & 4 & \mapsto 36 \end{array}$$

Let G_1 and G_2 be generator matrices corresponding to the multiplicity functions η_1 and η_2. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the codes generated by G_1 and G_2. Then $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$, but $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$. In fact,

$$\mathrm{lwe}_{\mathcal{C}_1}(X, Y) = \mathrm{lwe}_{\mathcal{C}_2}(X, Y) = X^{532} + 2X^{343}Y^{189} + 2X^{217}Y^{315} + 4X^{154}Y^{378}.$$

Because of the 0 entries in G_2, $\mathcal{C}_2^\perp$ contains codewords of weight 1, while $\mathcal{C}_1^\perp$ does not. That is, $A_1(\mathcal{C}_1^\perp) \neq A_1(\mathcal{C}_2^\perp)$.

4.4 Prime Modulus p, $p \geqslant 7$

In this section we construct examples $\mathcal{C}_1$ and $\mathcal{C}_2$ with $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ and $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ over the integers modulo a prime p, $p \geqslant 7$.

Fix a prime p, with $p \geqslant 7$. Let $t = (p-1)/2$. Let $\mathbb{Z}_p^\times$ denote the set of nonzero elements of $\mathbb{Z}_p$; $\mathbb{Z}_p^\times$ is a group under multiplication, and $\{\pm 1\}$ forms a subgroup. Let H denote the quotient group $\mathbb{Z}_p^\times/\{\pm 1\}$, and let q be the canonical quotient map $q : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times/\{\pm 1\}$. We choose the positive representative for each element in H, so we identify the elements of H with the set $\{1, 2, \ldots, t\}$.

Remark 4.4.1. Under the above identification, the quotient map q equals the Lee weight map $\mathrm{L} : \mathbb{Z}_p^\times \to \{1, 2, \ldots, t\}$.

The codes considered in this section are 1-dimensional. We fix $\eta_1, \eta_2 : \mathbb{Z}_p^\times/\{\pm 1\} \to \mathbb{N}$ defined by $\eta_1(1) = 0$ and $\eta_1(i) = t$ for all $2 \leqslant i \leqslant t$, $\eta_2(1) = 2(t-1)$ and $\eta_2(i) = t-2$ for all $2 \leqslant i \leqslant t$. Let G_1 and G_2 be generator matrices corresponding to η_1 and η_2. In particular, the matrix G_1 has size $1 \times (t(t-1))$, consisting of t entries of each i in $\{2, \ldots, t\}$. That is

$$G_1 = [2 \ldots 2 \quad 3 \ldots 3 \quad \ldots \quad t \ldots t],$$

where every number is repeated t times. And G_2 is the matrix of size $1 \times (t(t-1))$, consisting of $2(t-1)$ entries of 1 and $t-2$ entries of each i in $\{2, \ldots, t\}$. That is,

$$G_2 = [\ \overbrace{1 \ldots 1}^{2(t-1)-times} \quad \overbrace{2 \ldots 2}^{(t-2)-times} \quad \overbrace{3 \ldots 3}^{(t-2)-times} \quad \ldots \quad \overbrace{t \ldots t}^{(t-2)-times}\ ]$$

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the codes generated by G_1 and G_2.

Lemma 4.4.2. *For the linear codes given above,* $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$, *with a common weight distribution given by*

$$A_0 = 1 \text{ and } A_{t\left(\frac{t(t+1)}{2} - i\right)} = 2, \text{ for } 1 \leqslant i \leqslant t.$$

Proof. Let i be in $\{1, \ldots, t\}$. As an element of the group H, we have that $iH = H = \{1, 2, \ldots, t\}$. Let $*$ denote multiplication in H. In the following we reindex summations by using the fact that multiplying by a group element is a permutation of H. For G_1,

$$\begin{aligned} \mathrm{L}(iG_1) = \sum_{j=2}^{t} \mathrm{L}(ij)t &= t\left(\sum_{j \in H} i * j - i * 1\right) \\ &= t\left(\sum_{k=1}^{t} k - i\right) = t\left(\frac{t(t+1)}{2} - i\right). \end{aligned}$$

Since $\mathrm{L}(iG) = \mathrm{L}(-iG)$ over $\mathbb{Z}_m$, then we get that $A_{t\left(\frac{t(t+1)}{2} - i\right)}(\mathcal{C}_1) = 2$ for i in $\{1, \ldots, t\}$. For G_2,

$$\begin{aligned}
\mathrm{L}(iG_2) &= 2(t-1)\,\mathrm{L}(i) + \sum_{j=2}^{t}(t-2)\,\mathrm{L}(ij) \\
&= 2(t-1)i + (t-2)\left(\sum_{k=1}^{t} k - i\right) \\
&= 2(t-1)i + (t-2)\left(\frac{t(t+1)}{2} - i\right) \\
&= t\left(\frac{(t-2)(t+1)}{2} + i\right),
\end{aligned}$$

for all $1 \leqslant i \leqslant t$. Therefore, $A_0 = 1$ and $A_{t\left(\frac{(t-2)(t+1)}{2}+i\right)} = 2$, for $1 \leqslant i \leqslant t$. Consider the substitution $i = t + 1 - j$, then we have $1 \leqslant j \leqslant t$, and

$$\begin{aligned}
t\left(\frac{(t-2)(t+1)}{2} + i\right) &= t\left(\frac{(t-2)(t+1)}{2} + t + 1 - j\right) \\
&= t\left(\frac{t(t+1)}{2} - j\right)
\end{aligned}$$

This shows that we indeed have $A_0(\mathcal{C}_2) = 1$ and $A_{t\left(\frac{t(t+1)}{2}-i\right)}(\mathcal{C}_2) = 2$, for $1 \leqslant i \leqslant t$, as desired. □

Now we show that $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ by showing that the number of codewords of weight three in $\mathcal{C}_1^\perp$ does not equal the number of codewords of weight three in $\mathcal{C}_2^\perp$. We will study the cases when $p \equiv 1 \bmod 4$ and when $p \equiv 3 \bmod 4$ separately.

4.4.1 Primes Congruent to 1 Modulo 4

In this subsection $p \equiv 1 \bmod 4$. That is, $t = (p-1)/2$ is an even number, and so $t/2$ is an integer. Suppose that $\mathcal{C}$ is a code generated by G of size $1 \times n$ with no zero columns. The types of columns are $\{1, 2, \ldots, t\}$. Let a_i denote the number of columns in G whose entry is i, for $i \in \{1, 2, \ldots, t\}$. There are, up to a sign, five possible types of codewords in $\mathcal{C}^\perp$ of weight 3. Since $\mathcal{C}$ does not contain zero columns, a codeword with a single 3 or -3 will not appear in $\mathcal{C}^\perp$. So only four types are considered here, each in a separate sub-subsection. We

will count the number of codewords in $\mathcal{C}^\perp$ of each of the four types and then apply the count to $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$.

A 1 and a -2

Let c be a codeword in $\mathcal{C}^\perp$ with a 1 and a -2. Let $[x]$ denote a column in G whose entry is x. Suppose that 1 corresponds to column $[x]$ and -2 corresponds to column $[y]$ in the generator matrix, so that $Gc^T = x - 2y$. Since $\mathcal{C}$ has no zero columns, then $1 \leqslant x, y \leqslant t$ and so $-(2t-1) \leqslant x - 2y \leqslant t - 2$. This implies that the only way to have $x - 2y \equiv 0 \bmod p$ is to have $x - 2y = 0$. This forces x to be even. So if $x = 2i$, then $y = i$ and the number of ways that this happens is $a_{2i}a_i$. Therefore, the number of such codewords in $\mathcal{C}^\perp$ is

$$\sum_{i=1}^{t/2} a_{2i}a_i.$$

Therefore, the count for $\mathcal{C}_1^\perp$, given that $a_1 = 0$ and $a_i = t$ for all $2 \leqslant i \leqslant t$, is:

$$\sum_{i=1}^{t/2} a_{2i}a_i = \sum_{i=2}^{t/2} t^2 = \frac{t^2(t-2)}{2}.$$

And, the count for $\mathcal{C}_2^\perp$, given that $a_1 = 2(t-1)$ and $a_i = t - 2$ for all $2 \leqslant i \leqslant t$, is:

$$\begin{aligned}
\sum_{i=1}^{t/2} a_{2i}a_i &= 2(t-1)(t-2) + \sum_{i=2}^{t/2}(t-2)^2 \\
&= 2(t-1)(t-2) + \left(\frac{t}{2} - 1\right)(t-2)^2 \\
&= \frac{(t-2)}{2}\left(4(t-1) + (t-2)^2\right) \\
&= \frac{t^2(t-2)}{2}.
\end{aligned}$$

A 1 and a 2

Let c be a codeword in $\mathcal{C}^\perp$ with a 1 and a 2. Suppose that 1 corresponds to column $[x]$ and 2 corresponds to column $[y]$ in the generator matrix, that is $Gc^T = x + 2y$. Since $1 \leqslant x, y \leqslant t$, then $3 \leqslant x + 2y \leqslant 3t$. This implies that the only way to have $x + 2y \equiv 0 \bmod p$ is to have $x + 2y = p = 2t + 1$. This implies that x is an odd number. So if $x = 2i + 1$, then $y = t - i$ and the number of ways that this happens is $a_{2i+1}a_{t-i}$. Therefore, the number of such codewords in $\mathcal{C}^\perp$ is

$$\sum_{i=0}^{(t-2)/2} a_{2i+1}a_{t-i}.$$

Thus, the count for $\mathcal{C}_1^\perp$ is:

$$\sum_{i=0}^{(t-2)/2} a_{2i+1}a_{t-i} = \sum_{i=1}^{(t-2)/2} t^2 = \frac{t^2(t-2)}{2}.$$

And, the count for $\mathcal{C}_2^\perp$ is:

$$\sum_{i=0}^{(t-2)/2} a_{2i+1}a_{t-i} = 2(t-1)(t-2) + \sum_{i=1}^{(t-2)/2} (t-2)^2 = \frac{t^2(t-2)}{2}.$$

A 1 and two -1's

Let c be a codeword in $\mathcal{C}^\perp$ with a 1 and two -1's. Suppose that 1 corresponds to column $[x]$ and the -1's correspond to columns $[y]$ and $[z]$ in the generator matrix, so that $Gc^T = x - y - z$. Since $1 - 2t \leqslant x - y - z \leqslant t - 2$, then the only way to have $x - y - z \equiv 0 \bmod p$ is to have $x - y - z = 0$ and so $x = y + z$. So, if $x = 2i$ is even, then the possibilities for y and z are $y = j$ and $z = 2i - j$ for $1 \leqslant j \leqslant i$. Similarly, if $x = 2i + 1$, then $y = j$ and $z = 2i + 1 - j$ for $1 \leqslant j \leqslant i$. Therefore, the number of such codewords in $\mathcal{C}^\perp$ is

$$\sum_{i=1}^{t/2} a_{2i} \left(\sum_{j=1}^{i-1} a_j a_{2i-j} + \binom{a_i}{2} \right) + \sum_{i=1}^{(t-2)/2} a_{2i+1} \left(\sum_{j=1}^{i} a_j a_{2i+1-j} \right).$$

Therefore, the count for $\mathcal{C}_1^{\perp}$ is:

$$\begin{aligned}
&\sum_{i=2}^{t/2} t\left(\sum_{j=2}^{i-1} t^2 + \frac{t(t-1)}{2}\right) + \sum_{i=1}^{(t-2)/2} t\left(\sum_{j=2}^{i} t^2\right) \\
=&\sum_{i=2}^{t/2} t\left((i-2)t^2 + \frac{t(t-1)}{2}\right) + \sum_{i=1}^{(t-2)/2} t\left(t^2(i-1)\right) \\
=&\frac{t^2(t-2)(t^2-3t-1)}{4}.
\end{aligned}$$

And, the count for $\mathcal{C}_2^{\perp}$ is:

First part:

$$\begin{aligned}
&\sum_{i=1}^{t/2} a_{2i}\left(\sum_{j=1}^{i-1} a_j a_{2i-j} + \binom{a_i}{2}\right) \\
=&a_2\binom{a_1}{2} + \sum_{i=2}^{t/2} a_{2i}\left(a_1 a_{2i-1} + \sum_{j=2}^{i-1} a_j a_{2i-j} + \binom{a_i}{2}\right) \\
=&(t-2)\frac{(2t-2)(2t-3)}{2} \\
&+ \sum_{i=2}^{t/2}\left(2(t-1)(t-2)^2 + \sum_{j=2}^{i-1}(t-2)^3 + \frac{(t-2)^2(t-3)}{2}\right) \\
=&\frac{t^2(t-2)(t^2-2)}{8}.
\end{aligned}$$

Second part:

$$\begin{aligned}
&\sum_{i=1}^{(t-2)/2} a_{2i+1}\left(a_1 a_{2i+1-1} + \sum_{j=2}^{i} a_j a_{2i+1-j}\right) \\
=&\sum_{i=1}^{(t-2)/2} (t-2)\left(2(t-1)(t-2) + (t-2)^2(i-1)\right) \\
=&\frac{t(t-2)^3(t+2)}{8}.
\end{aligned}$$

Adding the two parts together, the total count for $\mathcal{C}_2^\perp$ for this type is:

$$\frac{t^2(t-2)(t^2-2)}{8} + \frac{t(t-2)^3(t+2)}{8} = \frac{t(t-2)(t^3-t^2-3t+4)}{4}.$$

Three 1's

Let c be a codeword in $\mathcal{C}^\perp$ with three 1's. Suppose that the ones correspond to columns $[x], [y]$ and $[z]$. Now since $3 \leqslant x+y+z \leqslant 3t$, the only way for Gc^T to be 0 mod p is when $x+y+z = p$. Since $3 \nmid p$, then x, y, z cannot all be equal. Therefore, we have two cases.

First we consider the case when two of x, y and z are the same. Assume that $y = z$. Then x is odd, and when $x = 2i+1$, $y = z = t-i$. Therefore, the number of such codewords in $\mathcal{C}^\perp$ is

$$\sum_{i=0}^{(t-2)/2} a_{2i+1} \binom{a_{t-i}}{2}.$$

Thus, the count for $\mathcal{C}_1^\perp$ is:

$$\sum_{i=1}^{(t-2)/2} \frac{t^2(t-1)}{2} = \frac{1}{4}t^2(t-1)(t-2).$$

And, the count for $\mathcal{C}_2^\perp$ is:

$$2(t-1)\frac{(t-2)(t-3)}{2} + \sum_{i=1}^{(t-2)/2} \frac{(t-2)^2(t-3)}{2} = \frac{1}{4}t^2(t-2)(t-3).$$

Let M be the number of ways p can be written as a sum of three distinct integers between 1 and t. Notice that 1 will never appear in such a partition. Indeed, if a partition contains 1, then the sum of the other two parts is $2t$, this means that the other two parts are each equal to t, and so the parts are not distinct. Therefore, this situation accounts for Mt^3 codewords in $\mathcal{C}_1^\perp$ and $M(t-2)^3$ codewords in $\mathcal{C}_2^\perp$. To find M, we need the following definition and proposition.

Definition 4.4.3. For two integers $n > k$, $Q(n,k)$ denotes the number of ways to write n

as a sum of k distinct positive integers.

Then by [2, p. 116] and [10, p. 45], we have the following.

Proposition 4.4.4. *For $p > 3$, $Q(p,3)$ is given by*

$$Q(p,3) = \left[(p-3)^2/12\right],$$

where $[\ ]$ is the nearest integer function.

Since our range for partitions is from 1 to t, we need to subtract the partitions when $t+1, t+2, \ldots, p-2$ appear in the partition. But $p-i$ appears $Q(i,2)$ times, for $i = 2, \ldots, t$. By [2, p. 116], $Q(i,2) = \lfloor (i-1)/2 \rfloor$.

$$\sum_{i=2}^{t} Q(i,2) = \sum_{i=2}^{t} \left\lfloor \frac{i-1}{2} \right\rfloor.$$

Notice that $\lfloor k/2 \rfloor = (k/2) - (1/2)$ for positive odd k, and $\lfloor k/2 \rfloor = k/2$ for even k. Since the interval $1 \leqslant i-1 \leqslant t-1$ contains $t/2$ positive odd integers, then

$$\sum_{i=2}^{t} \left\lfloor \frac{i-1}{2} \right\rfloor = \left(\sum_{i=2}^{t} \frac{i-1}{2} \right) - \frac{t}{4}.$$

Therefore,

$$\begin{aligned} \sum_{i=2}^{t} Q(i,2) &= \left(\sum_{i=2}^{t} \frac{i-1}{2} \right) - \frac{t}{4} = \left(\sum_{i=1}^{t-1} \frac{i}{2} \right) - \frac{t}{4} \\ &= \frac{t(t-1)}{4} - \frac{t}{4} = \frac{1}{4} t(t-2), \end{aligned}$$

and

$$\begin{aligned} M &= Q(p,3) - \sum_{i=2}^{t} Q(i,2) \\ &= \left[\frac{(p-3)^2}{12}\right] - \frac{1}{4}t(t-2) \\ &= \left[\frac{(2t-2)^2}{12}\right] - \frac{1}{4}t(t-2) \\ &= \left[\frac{(t-1)^2}{3}\right] - \frac{1}{4}t(t-2). \end{aligned}$$

Recall $[(t-1)^2/3]$ is the nearest integer function. Since $(t-1)^2$ is an integer, then the possible values for $[(t-1)^2/3]$ are $(t-1)^2/3$, $((t-1)^2+1)/3$ or $((t-1)^2-1)/3$. This implies that the possible values for M are:

$$\frac{1}{12}(t^2-2t+4),\ \frac{1}{12}(t^2-2t+8),\quad \text{or}\quad \frac{1}{12}t(t-2). \tag{4.1}$$

Recall that $A_3(\mathcal{C}_i^{\perp})$ is the number of codewords of weight 3 in $\mathcal{C}_i^{\perp}$ for $i = 1, 2$. Remember, we need to double our count in each type to account for the negatives of our types. Therefore,

$$\begin{aligned} A_3(\mathcal{C}_1^{\perp}) &= 2\left(2\cdot\frac{(t-2)t^2}{2} + \frac{t^2(t-2)(t^2-3t-1)}{4} + \frac{t^2(t-1)(t-2)}{4} + Mt^3\right) \\ &= \frac{1}{2}t^2(t-2)\left(t^2-2t+2\right) + 2Mt^3. \end{aligned}$$

For $A_3(\mathcal{C}_2^{\perp})$, the count is

$$\begin{aligned} A_3(\mathcal{C}_2^{\perp}) = 2\Bigg(&2\cdot\frac{(t-2)t^2}{2} + \frac{t(t-2)(t^3-t^2-3t+4)}{4} \\ &+ \frac{t^2(t-2)(t-3)}{4} + M(t-2)^3\Bigg) \\ = &\frac{1}{2}t(t-2)(t+2)(t^2-2t+2) + 2M(t-2)^3. \end{aligned}$$

Therefore, $A_3(\mathcal{C}_1^\perp) = A_3(\mathcal{C}_2^\perp)$ if and only if

$$\begin{aligned} 0 =& \frac{1}{2}t^2(t-2)\left(t^2-2t+2\right) - \frac{1}{2}t(t-2)(t+2)(t^2-2t+2) \\ &+ 2Mt^3 - 2M(t-2)^3 \\ =& -t(t-2)(t^2-2t+2) + M(12t^2-24t+16). \end{aligned}$$

It follows that $A_3(\mathcal{C}_1^\perp) = A_3(\mathcal{C}_2^\perp)$ if and only if

$$M = \frac{t(t-2)(t^2-2t+2)}{12t^2-24t+16}.$$

This expression clearly does not match any of the formulas for M from equation 4.1. Nonetheless, the above expression and the earlier formulas may yield the same value for M for certain values of t. The values of t on which the expression $((t^2-2t+2)(t-2)t)/(12t^2-24t+16)$ agrees with the first two formulas in equation 4.1 are not integers. But, the expression $((t^2-2t+2)(t-2)t)/(12t^2-24t+16)$ agrees with $t(t-2)/12$, the third formula from equation 4.1, when $t = 0$ and $t = 2$. Notice that $t = 2$ when $p = 5$. This means that $A_3(\mathcal{C}_1^\perp)$ and $A_3(\mathcal{C}_2^\perp)$ are in fact equal when $p = 5$, so that this construction does not provide a counterexample in the case $p = 5$. Otherwise, for $p \geqslant 13$, we indeed have $A_3(\mathcal{C}_1^\perp) \neq A_3(\mathcal{C}_2^\perp)$, and therefore $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ for all $p \equiv 1 \bmod 4$, $p \geqslant 13$.

4.4.2 Primes Congruent to 3 Modulo 4

In this subsection $p \equiv 3 \bmod 4$. Then $t = (p-1)/2$ is an odd number. We will use the same setup from the previous subsection. In most of the cases, the only differences are the upper limits of the summations.

A 1 and a -2

To have $x - 2y = 0$, x must be even. So if $x = 2i$, then $y = i$, and the number of ways that this happens is $a_{2i}a_i$. Therefore, the number of such codewords in $\mathcal{C}^\perp$ is

$$\sum_{i=1}^{(t-1)/2} a_{2i}a_i.$$

Therefore, the count for $\mathcal{C}_1^\perp$, given that $a_1 = 0$ and $a_i = t$ for all $2 \leqslant i \leqslant t$, is:

$$\sum_{i=1}^{(t-1)/2} a_{2i}a_i = \sum_{i=2}^{(t-1)/2} t^2 = t^2\left(\frac{t-1}{2} - 1\right) = \frac{t^2(t-3)}{2}.$$

And, the count for $\mathcal{C}_2^\perp$, given that $a_1 = 2(t-1)$ and $a_i = (t-2)$ for all $2 \leqslant i \leqslant t$, is:

$$\begin{aligned}\sum_{i=1}^{(t-1)/2} a_{2i}a_i &= 2(t-1)(t-2) + \sum_{i=2}^{(t-1)/2} (t-2)^2 \\ &= \frac{(t-2)(t^2-t+2)}{2}.\end{aligned}$$

A 1 and a 2

To have $x + 2y = p = 2t + 1$, x must be odd. So if $x = 2i + 1$, then $y = t - i$, and the number of ways that this happens is $a_{2i+1}a_{t-i}$. Therefore, the number of such codewords in $\mathcal{C}^\perp$ is

$$\sum_{i=0}^{(t-1)/2} a_{2i+1}a_{t-i}.$$

Thus, the count for $\mathcal{C}_1^\perp$ is:

$$\sum_{i=0}^{(t-1)/2} a_{2i+1}a_{t-i} = \sum_{i=1}^{(t-1)/2} t^2 = \frac{t^2(t-1)}{2}.$$

And, the count for $\mathcal{C}_2^{\perp}$ is:

$$\begin{aligned}\sum_{i=0}^{(t-1)/2} a_{2i+1}a_{t-i} &= 2(t-1)(t-2) + \sum_{i=1}^{(t-1)/2} (t-2)^2 \\ &= \frac{(t-1)(t-2)(t+2)}{2}.\end{aligned}$$

A 1 and two -1's

We need to solve $x = y + z$. If $x = 2i$ is even, then the possibilities for y and z are $y = j$ and $z = 2i - j$ for $1 \leqslant j \leqslant i$. Similarly, if $x = 2i + 1$, then $y = j$ and $z = 2i + 1 - j$ for $1 \leqslant j \leqslant i$. Therefore, the number of such codewords in $\mathcal{C}^{\perp}$ is

$$\sum_{i=1}^{(t-1)/2} a_{2i} \left(\sum_{j=1}^{i-1} a_j a_{2i-j} + \binom{a_i}{2} \right) + \sum_{i=1}^{(t-1)/2} a_{2i+1} \left(\sum_{j=1}^{i} a_j a_{2i+1-j} \right).$$

Therefore, the count for $\mathcal{C}_1^{\perp}$ is:

$$\begin{aligned}&\sum_{i=2}^{(t-1)/2} t \left(\sum_{j=2}^{i-1} t^2 + \frac{t(t-1)}{2} \right) + \sum_{i=1}^{(t-1)/2} t \left(\sum_{j=2}^{i} t^2 \right) \\ &= \sum_{i=2}^{(t-1)/2} t \left((i-2)t^2 + \frac{t(t-1)}{2} \right) + \sum_{i=1}^{(t-1)/2} t \left(t^2(i-1) \right) \\ &= \frac{t^2(t-3)(t^2-2t-1)}{4}.\end{aligned}$$

And, the count for $\mathcal{C}_2^{\perp}$ is:

First part:

$$\begin{aligned}
&\sum_{i=1}^{(t-1)/2} a_{2i}\left(\sum_{j=1}^{i-1} a_j a_{2i-j} + \binom{a_i}{2}\right)\\
=&a_2\binom{a_1}{2} + \sum_{i=2}^{(t-1)/2} a_{2i}\left(a_1 a_{2i-1} + \sum_{j=2}^{i-1} a_j a_{2i-j} + \binom{a_i}{2}\right)\\
=&(t-2)\frac{(2t-2)(2t-3)}{2}\\
&+\sum_{i=2}^{(t-1)/2}\left(2(t-1)(t-2)^2 + \sum_{j=2}^{i-1}(t-2)^3 + \frac{(t-2)^2(t-3)}{2}\right)\\
=&\frac{t(t-1)(t-2)(t^2-t+2)}{8}.
\end{aligned}$$

Second part:

$$\begin{aligned}
&\sum_{i=1}^{(t-1)/2} a_{2i+1}\left(a_1 a_{2i+1-1} + \sum_{j=2}^{i} a_j a_{2i+1-j}\right)\\
=&\sum_{i=1}^{(t-1)/2}(t-2)\left(2(t-1)(t-2) + (t-2)^2(i-1)\right)\\
=&\frac{(t-1)(t-2)^2(t^2+3t-2)}{8}.
\end{aligned}$$

Adding the two parts together, the total count for $\mathcal{C}_2^{\perp}$ for this type is:

$$\frac{(t-2)(t+2)(t-1)^3}{4}.$$

Three 1**'s**

We consider the same two cases as in paragraph 4.4.1. First we consider the case when two of x, y and z are the same. Assume that $y = z$. Then x must be odd, and when $x = 2i + 1$,

$y = z = t - i$. Therefore, the number of such codewords in $\mathcal{C}^{\perp}$ is

$$\sum_{i=0}^{(t-1)/2} a_{2i+1} \binom{a_{t-i}}{2}.$$

Thus, the count for $\mathcal{C}_1^{\perp}$ is:

$$\sum_{i=1}^{(t-1)/2} \frac{t^2(t-1)}{2} = \frac{1}{4}t^2(t-1)^2.$$

And, the count for $\mathcal{C}_2^{\perp}$ is:

$$\begin{aligned} &2(t-1)\frac{(t-2)(t-3)}{2} + \sum_{i=1}^{(t-1)/2} \frac{(t-2)^2(t-3)}{2} \\ =&\frac{1}{4}(t-1)(t-2)(t-3)(t+2). \end{aligned}$$

Recall M is the number of ways p can be written as a sum of three distinct integers between 1 and t. Notice that 1 will never appear in such a partition. This case accounts for Mt^3 codewords in $\mathcal{C}_1^{\perp}$ and $M(t-2)^3$ codewords in $\mathcal{C}_2^{\perp}$.

We know that $M = Q(p,3) - \sum_{i=2}^{t} Q(i,2) = Q(p,3) - \sum_{i=2}^{t} \lfloor (i-1)/2 \rfloor$. Since $1 \leqslant i-1 \leqslant t-1$ and there are $(t-1)/2$ odd numbers in the interval $[1, t-1]$, then

$$\begin{aligned} \sum_{i=2}^{t} \left\lfloor \frac{i-1}{2} \right\rfloor &= \sum_{i=2}^{t} \frac{i-1}{2} - \frac{t-1}{4} \\ &= \frac{t(t-1)}{4} - \frac{t-1}{4} = \frac{(t-1)^2}{4}. \end{aligned}$$

Hence,

$$M = \left\lfloor \frac{(t-1)^2}{3} \right\rfloor - \frac{1}{4}(t-1)^2.$$

The possible values for $\lfloor (t-1)^2/3 \rfloor$ are $(t-1)^2/3$, $((t-1)^2+1)/3$ or $((t-1)^2-1)/3$. This

implies that the possible values for M are:

$$\frac{1}{12}(t-1)^2,\ \frac{1}{12}(t^2-2t+5),\ \text{ or }\ \frac{1}{12}(t^2-2t-3). \tag{4.2}$$

Here are the total counts of codewords of weight 3 in $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$.

$$\begin{aligned} A_3(\mathcal{C}_1^\perp) &= 2\left(\frac{(t-3)t^2}{2}+\frac{(t-1)t^2}{2}+\frac{t^2(t-3)(t^2-2t-1)}{4}\right. \\ &\qquad \left.+\frac{t^2(t-1)^2}{4}+Mt^3\right) \\ &= \frac{t^2(t-1)(t^2-3t+4)}{2}+2Mt^3. \end{aligned}$$

And,

$$\begin{aligned} A_3(\mathcal{C}_2^\perp) &= 2\left(\frac{(t-2)(t^2-t+2)}{2}+\frac{(t-1)(t-2)(t+2)}{2}\right. \\ &\qquad +\frac{(t-2)(t+2)(t-1)^3}{4} \\ &\qquad \left.+\frac{(t-1)(t-2)(t-3)(t+2)}{4}+M(t-2)^3\right) \\ &= \frac{(t-2)(t^4-t^2+4)}{2}+2M(t-2)^3. \end{aligned}$$

Therefore, $A_3(\mathcal{C}_1^\perp) = A_3(\mathcal{C}_2^\perp)$ if and only if

$$\begin{aligned} 0 &= \frac{t^2(t-1)(t^2-3t+4)}{2}-\frac{(t-2)(t^4-t^2+4)}{2}+2Mt^3-2M(t-2)^3 \\ &= -t^4+4t^3-3t^2-2t+4+M(12t^2-24t+16). \end{aligned}$$

It follows that $A_3(\mathcal{C}_1^\perp) = A_3(\mathcal{C}_2^\perp)$ if and only if

$$M = \frac{t^4-4t^3+3t^2+2t-4}{12t^2-24t+16}.$$

This expression clearly does not match any of the formulas for M from equation 4.2. Moreover, the only integers at which the expression $(t^4-4t^3+3t^2+2t-4)/(12t^2-24t+16)$ agrees with any of the formulas in equation 4.2 are $t=0$ and $t=2$. These are not possible values for t when $p \equiv 3 \bmod 4$. Hence, for $p \geqslant 7$, we indeed have $A_3(\mathcal{C}_1^\perp) \neq A_3(\mathcal{C}_2^\perp)$, and therefore $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ for all $p \equiv 3 \bmod 4$, $p \geqslant 7$.

We summarize the results for primes $p \geqslant 7$.

Proposition 4.4.5. *For each prime $p \geqslant 7$, there exist linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{Z}_p$ with $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ and $A_3(\mathcal{C}_1^\perp) \neq A_3(\mathcal{C}_2^\perp)$.*

4.5 Propagation of Examples and Proof of the Main Theorem

We would like to say that if $\mathcal{C}_1$ and $\mathcal{C}_2$ give an example with $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$ and $\mathrm{lwe}_{\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{\mathcal{C}_2^\perp}$ over $\mathbb{Z}_m$, then $a\mathcal{C}_1$ and $a\mathcal{C}_2$ provide a corresponding example over $\mathbb{Z}_{am}$, for any positive integer a. Although the previous statement is not true in that generality, a weaker version is true and is sufficient to cover all integers $m \geqslant 5$. We need the following construction.

Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_m$. For any positive integer a, define $a\mathcal{C}$ to be the code over $\mathbb{Z}_{am}$ given by

$$a\mathcal{C} = \{(ac_1, \ldots, ac_n) \in \mathbb{Z}_{am}^n : (c_1, \ldots, c_n) \in \mathcal{C}\}.$$

Lemma 4.5.1. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{Z}_m$ and a be a positive integer. Then the weight distribution of the code $a\mathcal{C}$ is given in terms of the weight distribution of $\mathcal{C}$ as follows.*

$$A_q(a\mathcal{C}) = \begin{cases} 0, & a \nmid q, \\ A_{q/a}(\mathcal{C}), & a \mid q, \end{cases}$$

for all $0 \leqslant q \leqslant \lfloor am/2 \rfloor n$.

Proof. Let $c \in \mathcal{C}$. Assume all entries of c satisfy $-m/2 < c_i \leqslant m/2$, for all i. This implies

that $-am/2 < ac_i \leqslant am/2$ for all entries of $ac \in a\mathcal{C}$. Therefore

$$\mathrm{L}_{am}(ac) = \sum_{i=1}^{n} |ac_i| = a \sum_{i=1}^{n} |c_i| = a\, \mathrm{L}_m(c).$$

Notice that the map $\mathcal{C} \to a\mathcal{C}$, with $c \mapsto ac$, is a bijection. Therefore the result follows. □

Corollary 4.5.2. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be linear codes of length n over $\mathbb{Z}_m$ and a be a positive integer. If $\mathrm{lwe}_{\mathcal{C}_1} = \mathrm{lwe}_{\mathcal{C}_2}$, then $\mathrm{lwe}_{a\mathcal{C}_1} = \mathrm{lwe}_{a\mathcal{C}_2}$.*

The next result examines the count of low weight codewords in dual codes of the form $(a\mathcal{C})^{\perp}$.

Lemma 4.5.3. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{Z}_m$. Suppose that a and b are integers with $1 \leqslant a \leqslant b$. Then $A_q((a\mathcal{C})^{\perp}) = A_q((b\mathcal{C})^{\perp})$ for $q < am/2$. In particular, $A_q(\mathcal{C}^{\perp}) = A_q((b\mathcal{C})^{\perp})$ for $q < m/2$.*

Proof. Recall that we view $\mathbb{Z}_{am} = \{i : -am/2 < i \leqslant am/2\}$, and similarly for $\mathbb{Z}_{bm}$. Notice that a vector y in $\mathbb{Z}_{am}^n$ can then be thought of as a vector in $\mathbb{Z}_{bm}^n$ with the same entries and the same Lee weight. Conversely, for $z \in \mathbb{Z}_{bm}^n$, under the hypothesis that $\mathrm{L}(z) < am/2$, we can view z as a vector in $\mathbb{Z}_{am}^n$ with the same entries and the same Lee weight. In other words, for $0 \leqslant q < am/2$, the sets $\{y \in \mathbb{Z}_{am}^n : \mathrm{L}(y) = q\}$ and $\{z \in \mathbb{Z}_{bm}^n : \mathrm{L}(z) = q\}$ are equal, if we ignore the modulus and think of the elements as just integer vectors.

Now let $0 \leqslant q < am/2$ and let y be such that $-am/2 < y_i < am/2$ with $\sum_{i=1}^{n} |y_i| = q$, i.e., $\mathrm{L}_{am}(y) = \mathrm{L}_{bm}(y) = q$. We then have the following list of equivalent statements:

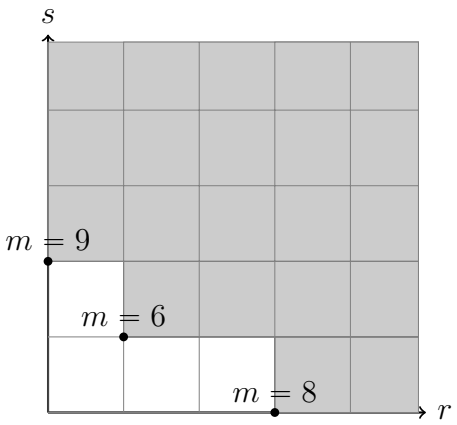
- $y \in (a\mathcal{C})^{\perp}$
- $\sum_{i=1}^{n} y_i(ac_i) \equiv 0 \bmod am$, for all $c \in \mathcal{C}$
- $am | (\sum_{i=1}^{n} y_i(ac_i))$, for all $c \in \mathcal{C}$
- $m | (\sum_{i=1}^{n} y_i c_i)$, for all $c \in \mathcal{C}$

- $bm|(\sum_{i=1}^{n} y_i(bc_i)),$ for all $c \in \mathcal{C}$
- $y \in (b\mathcal{C})^{\perp}$

This shows that $A_q(a\mathcal{C})^{\perp} = A_q(b\mathcal{C})^{\perp}$. □

Corollary 4.5.4. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be linear codes of length n over $\mathbb{Z}_m$. Let b and q positive integers with $q < m/2$. If $A_q(\mathcal{C}_1^{\perp}) \neq A_q(\mathcal{C}_2^{\perp})$, then $A_q((b\mathcal{C}_1)^{\perp}) \neq A_q((b\mathcal{C}_2)^{\perp})$.*

Proof of Theorem 4.2.1. Suppose that $m \geqslant 5$. We will consider cases based on minimal factors of m that are also greater than or equal to 5. For instance, if m is not divisible by any prime p, $p \geqslant 5$, then m is divisible only by powers of 2 and powers of 3, say $m = 2^r 3^s$. The smallest such numbers $2^r 3^s$ that are themselves greater than or equal to 5 are 6, 8 and 9, as seen in the following diagram.



Sections 4.3 and 4.4 provided examples of linear codes $\mathcal{C}_1, \mathcal{C}_2$ over $\mathbb{Z}_m$ satisfying $\text{lwe}_{\mathcal{C}_1} = \text{lwe}_{\mathcal{C}_2}$ and $A_q(\mathcal{C}_1^{\perp}) \neq A_q(\mathcal{C}_2^{\perp})$ for the cases $m = 5, 6, 8, 9$ and $m = p$ prime, $p \geqslant 7$. To extend these examples from $\mathbb{Z}_m$ to $\mathbb{Z}_{am}$ we need to verify that the numbers m and q satisfy the hypotheses of Corollary 4.5.4. We summarize the various cases in the following chart:

m	5	6	8	9	$p, p \geqslant 7$
$q : A_q(\mathcal{C}_1^{\perp}) \neq A_q(\mathcal{C}_2^{\perp})$	2	2	3	1	3

Since $q < m/2$ in all of these cases, Corollary 4.5.4 implies that the examples provided in Sections 4.3 and 4.4 yield examples with $\mathrm{lwe}_{a\mathcal{C}_1} = \mathrm{lwe}_{a\mathcal{C}_2}$ and $\mathrm{lwe}_{a\mathcal{C}_1^\perp} \neq \mathrm{lwe}_{a\mathcal{C}_2^\perp}$ over $\mathbb{Z}_{am}$ for any positive integer a. Since any $m \geqslant 5$ is necessarily a multiple of $m = 5, 6, 8, 9$ or $m = p$ prime, $p \geqslant 7$, the result follows. $\square$

Chapter 5

Conclusion and Future Work

Chapter 3 of this thesis covered much of what is known about the MacWilliams extension theorem. Studying sufficient and necessary conditions for the extension property has been an ongoing project by some researchers for several years. Although many classical and important results have been proven for the extension property, there are still many classes of alphabets and weight functions for which the validity of the extension property is still unknown. We plan to continue working on this project.

In Chapter 4 we showed that there is no valid version of the MacWilliams identities over $\mathbb{Z}_m$ with respect to the Lee weight, for $m \geqslant 5$. It is natural to consider the same problem for other weights on $\mathbb{Z}_m$, specifically the Euclidean weight and the homogeneous weight.

The Euclidean weight E is defined on $\mathbb{Z}_m$ by $\mathrm{E}(a) = \mathrm{L}(a)^2$ for $a \in \mathbb{Z}_m$. The Euclidean weight coincides with the Lee weight and the Hamming weight over $\mathbb{Z}_2$ and $\mathbb{Z}_3$, thus the MacWilliams identities hold for the Euclidean weight enumerator in these cases. The following example from [1] shows the failure of the MacWilliams identities for the Euclidean weight enumerator over $\mathbb{Z}_4$.

Example 5.0.1. Let $m = 4$. Let

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 3 & 3 & 1 & 1 \end{bmatrix},$$

$$G_2 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 0 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & 0 \end{bmatrix}.$$

Then $\mathrm{ewe}_{\mathcal{C}_1}(X,Y) = \mathrm{ewe}_{\mathcal{C}_2}(X,Y) = X^{48} + 12X^{32}Y^{16} + 3X^{16}Y^{32}$ and $\mathrm{ewe}_{\mathcal{C}_1^\perp} \neq \mathrm{ewe}_{\mathcal{C}_2^\perp}$. In fact $A_1(\mathcal{C}_1^\perp) \neq A_1(\mathcal{C}_2^\perp)$; because of the zero column in G_2, there are codewords of Euclidean weight 1 in $\mathcal{C}_2^\perp$ but not in $\mathcal{C}_1^\perp$.

The homogeneous weight over $\mathbb{Z}_m$ was defined by Constantinescu and Heise [3]. We will not give the general definition here; rather we simply state the values of the homogeneous weight for specific m as needed. For $m = p$, a prime, the homogeneous weight on $\mathbb{Z}_p$ is just a scaled version of the Hamming weight. For $m = 4$, the homogeneous weight equals the Lee weight. In those cases, the MacWilliams identities hold.

Here are two examples, also in [1], where the MacWilliams identities fail for the homogeneous weight enumerator.

Example 5.0.2. Let $m = 6$. The homogeneous weight w has the following values

a	0	1	2	3	4	5
$\mathrm{w}(a)$	0	1	3	4	3	1

Set

$$G_1 = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 3 & 3 \end{bmatrix}.$$

Then $\mathrm{howe}_{\mathcal{C}_1}(X,Y) = \mathrm{howe}_{\mathcal{C}_2}(X,Y) = X^{12} + 2X^9Y^3 + 2X^3Y^9 + Y^{12}$, but $A_2(\mathcal{C}_1^\perp) = 6$ and $A_2(\mathcal{C}_2^\perp) = 4$.

Example 5.0.3. This example is due to the referee of [20, Example 5.6]. Let $m = 8$, and

use the following values for w:

a	0	1	2	3	4	5	6	7
$\mathrm{w}(a)$	0	1	1	1	2	1	1	1

Set

$$G_1 = \begin{bmatrix} 1 & 1 & 4 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 2 & 2 & 4 \\ 0 & 4 & 0 \end{bmatrix}.$$

Then $\mathrm{howe}_{\mathcal{C}_1}(X,Y) = \mathrm{howe}_{\mathcal{C}_2}(X,Y) = X^6 + 2X^4Y^2 + 5X^2Y^4$, but $A_2(\mathcal{C}_1^\perp) = 7$ and $A_2(\mathcal{C}_2^\perp) = 23$.

To our knowledge, the validity of the MacWilliams identities for the Euclidean weight enumerator or the homogeneous weight enumerator over $\mathbb{Z}_m$ is still open in general. Except for the cases described above where the MacWilliams identities are known to hold, we expect the identities to fail.

Bibliography

[1] Noha Abdelghany and Jay A. Wood. Failure of the MacWilliams identities for the Lee weight enumerator over $\mathbb{Z}_m$, $m \geqslant 5$. *Submitted to Discrete Mathematics*, 2020.

[2] Louis Comtet. *Advanced combinatorics*. D. Reidel Publishing Co., Dordrecht, enlarged edition, 1974.

[3] I. Constantinescu and W. Heise. A metric for codes over residue class rings of integers. *Problemy Peredachi Informatsii*, 33(3):22–28, 1997.

[4] Serhii Dyshko. The extension theorem for Lee and Euclidean weight codes over integer residue rings. *Des. Codes Cryptogr.*, 87(6):1253–1269, 2019.

[5] Noha ElGarem, Nefertiti Megahed, and Jay A. Wood. The extension theorem with respect to symmetrized weight compositions. In *Coding theory and applications*, volume 3 of *CIM Ser. Math. Sci.*, pages 177–183. Springer, Cham, 2015.

[6] Oliver W. Gnilke, Marcus Greferath, Thomas Honold, Jay A. Wood, and Jens Zumbrägel. The extension theorem for bi-invariant weights over Frobenius rings and Frobenius bimodules. In *Rings, modules and codes*, volume 727 of *Contemp. Math.*, pages 117–129. Amer. Math. Soc., Providence, RI, 2019.

[7] Marcus Greferath, Cathy Mc Fadden, and Jens Zumbrägel. Characteristics of invariant weights related to code equivalence over rings. *Des. Codes Cryptogr.*, 66(1-3):145–156, 2013.

[8] Marcus Greferath, Alexandr Nechaev, and Robert Wisbauer. Finite quasi-Frobenius modules and linear codes. *J. Algebra Appl.*, 3(3):247–272, 2004.

[9] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé. The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, 40(2):301–319, 1994.

[10] Ross Honsberger. *Mathematical gems. III*, volume 9 of *The Dolciani Mathematical Expositions*. Mathematical Association of America, Washington, DC, 1985.

[11] W. Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[12] Philippe Langevin and Jay A. Wood. The extension theorem for the Lee and Euclidean weights over $\mathbb{Z}/p^k\mathbb{Z}$. *J. Pure Appl. Algebra*, 223(3):922–930, 2019.

[13] Florence Jessie MacWilliams. *Combinatorial problems of elementary abelian groups*. ProQuest LLC, Ann Arbor, MI, 1962. Thesis (Ph.D.)–Radcliffe College.

[14] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[15] Minjia Shi, Keisuke Shiromoto, and Patrick Solé. A note on a basic exact sequence for the Lee and Euclidean weights of linear codes over $\mathbb{Z}_\ell$. *Linear Algebra Appl.*, 475:151–153, 2015.

[16] Yongsheng Tang, Shixin Zhu, and Xiaoshan Kai. MacWilliams type identities on the Lee and Euclidean weights for linear codes over $\mathbb{Z}_\ell$. *Linear Algebra Appl.*, 516:82–92, 2017.

[17] Jay A. Wood. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math.*, 121(3):555–575, 1999.

[18] Jay A. Wood. Code equivalence characterizes finite Frobenius rings. *Proc. Amer. Math. Soc.*, 136(2):699–706, 2008.

[19] Jay A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. In *Codes over rings*, volume 6 of *Ser. Coding Theory Cryptol.*, pages 124–190. World Sci. Publ., Hackensack, NJ, 2009.

[20] Jay A. Wood. Some applications of the Fourier transform in algebraic coding theory. In *Algebra for secure and reliable communication modeling*, volume 642 of *Contemp. Math.*, pages 1–40. Amer. Math. Soc., Providence, RI, 2015.

[21] Jay A. Wood. Two approaches to the extension problem for arbitrary weights over finite module alphabets. 2020.