Spring 1-1-2011

Analytic Proofs of Certain MacWilliams Identities

David Parker Keyes
University of Colorado at Boulder, dpkeyes@gmail.com

Analytic Proofs of Certain MacWilliams Identities

by

David Parker Keyes

B.A., University of California Berkeley, 2006

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

2011

This thesis entitled:
Analytic Proofs of Certain MacWilliams Identities
written by David Parker Keyes
has been approved for the Department of Mathematics

_____

David Grant

_____

Eric Stade

Date _____

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.

Keyes, David Parker (Ph.D., Mathematics)

Analytic Proofs of Certain MacWilliams Identities

Thesis directed by Professor David Grant

The relationship between vector codes and lattices has been studied extensively over the past 40 years. Since Leech and Sloane described how to attach lattices in $\mathbb{R}^n$ to linear codes $C \subseteq \mathbb{F}_2^n$ [35], lattices have been attached to codes defined over a variety of finite rings. Much research has been conducted on theta functions defined over these code lattices and their modular properties.

Codes C are modeled mathematically as a subset of matrices (codewords) with entries in a finite alphabet B. Weight functions measure the "size" of elements $v \in C$. A weight enumerator is a generating function that encodes the weight distribution of a code. If the code C is a vector space, then its dual $C^\perp$ is the orthogonal vector space under the dot product.

Duality theory for codes was pioneered by Sloane, MacWilliams, and Delsarte [43], [21], [32]. *MacWilliams Identities* are at the center of this theory. MacWilliams Identities are functional equations that relate the weight enumerator of a code to that of its dual. An analytic proof of the Hamming weight MacWilliams Identity exists for linear codes $C \subseteq \mathbb{F}_2^n$ [7], and an analytic proof of the Lee weight MacWilliams Identity exists for self-orthogonal, $C \subseteq C^\perp$, linear codes $C \subseteq \mathbb{F}_p^n$ [13].

We extend the class of codes for which there exists an analytic proof of the MacWilliams Identity. In Chapter 3, we describe how to attach theta functions to matrix codes $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$. (We believe this is the first time theta functions have been attached to matrix codes.) We provide an analytic proof of the column distance weight MacWilliams Identity for linear codes $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ and an analytic proof of the rank weight MacWilliams Identity for linear codes $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$. In Chapter 4, we improve upon the work of van der Geer, Hirzebruch, Choie, and Jeong [27], [13]. We provide an analytic proof of the Hamming weight MacWilliams Identity for linear vector codes $C \subseteq \mathbb{F}_p^n$. In Chapter 5, we provide a general framework for this problem and study the relationship between codes and theta functions in the context of association schemes.

Dedication

I would like to dedicate this dissertation to all my friends who made graduate school a fun experience.

Acknowledgements

I would like to acknowledge and thank my advisor David Grant; I am forever grateful to him for his mathematical guidance. I would also like to acknowledge my wife Reed for her compassion and patience in dealing with a cranky husband when the proofs weren't working out. Last, but certainly not least, I would like to thank my parents Sally and Richard for their unconditional love and support, and their remarkable ability to somehow raise two children with doctorate degrees.

Contents

Chapter

1 Introduction 1

1.1 Information Theory and Coding Theory 1

1.2 Duality Theory and Theta Functions 2

1.3 Dissertation Results 3

2 Preliminaries 4

2.1 Codes 4

2.1.1 Weight and Diversity Functions 5

2.1.2 Weight Enumerators 6

2.1.3 Duality 8

2.2 Theta Functions 9

2.2.1 Theta Functions of Genus One 9

2.2.2 Symplectic Theta Functions 10

2.2.3 Theta Functions Defined over Number Fields 10

2.3 Theta Functions and Codes 11

3 $\mathbb{F}_2$-Matrix Codes 13

3.1 Linear $\mathbb{F}_p$-Matrix Codes and Real Lattices 13

3.2 Theta Functions Attached to $\mathbb{F}_2$-Matrix Codes 15

3.3 Rank and Column Distance Group Actions 19

3.3.1 Rank Group Action . . . 19
3.3.2 Column Distance Group Action . . . 21
3.4 Theta Functions and Weight Enumerators . . . 22
3.5 Inversion Formulas . . . 28
3.6 MacWilliams Identities . . . 35
3.7 $\mathbb{F}_2$-Column Distance Codes and $\mathbb{F}_4$-Hamming Codes . . . 39

4 $\mathbb{F}_p$-Vector Codes 41
4.1 Linear $\mathbb{F}_p$-Codes and Real Lattices . . . 41
4.2 Number Fields, Ideals, and Theta Functions . . . 43
4.3 Theta Functions Attached to $\mathbb{F}_p$-Hamming Codes . . . 47
4.4 Lattices Attached to $\mathbb{F}_p$-Codes and Theta Functions . . . 51
4.5 Inversion Formulas . . . 58
4.6 MacWilliams Identity . . . 61

5 Association Schemes and Linear Codes 64
5.1 Association Schemes . . . 64
5.2 Weight Functions, Diversity Functions, and Abelian Schemes . . . 68
5.3 Weight Enumerators and Abelian Schemes . . . 71
5.3.1 Linear Weight Enumerators . . . 71
5.3.2 Total Weight Enumerators . . . 72
5.4 MacWilliams Identities and Abelian Schemes . . . 75
5.5 Theta Functions, Analytic Proofs, and Abelian Schemes . . . 78
5.5.1 Attaching Lattices to Linear Codes . . . 78
5.5.2 Attaching Theta Functions to Codes and Weight Enumerators . . . 81
5.5.3 Inversion Formulas and Algebraic Independence . . . 82
5.5.4 Problems and Issues . . . 83
5.6 The Game . . . 84

Bibliography 86

Chapter 1

Introduction

1.1 Information Theory and Coding Theory

In 1948, Shannon revolutionized the communication industry with his paper, *A Mathematical Theory of Communication*. He is regarded as the father of information theory and modern coding theory. Information theory is the probabilistic study of data transmission over a noisy channel. Coding theory is the study of *codes*, which are used to encode messages to be sent across these noisy networks. The reason to employ a code is to systematically add redundancy to messages to assist the decoder with error correction. For a set of messages M, let C be the set of encoded messages, called *codewords*, and let Y be the set of received words. The following diagram models data transmission over a noisy channel.

We hope to successfully decode Y into C; for that we want to have a low probability of decoding error. To this end, an understanding of the channel will often provide us with a distance function on the space of received words Y, and we will decode the received word to the *closest* codeword in C. This is often best achieved by imbuing the encoded message C with mathematical structure. Codes are therefore studied in the context of number theory, abstract algebra, and algebraic geometry.

1.2 Duality Theory and Theta Functions

Codes C are modeled mathematically as a subset of matrices (codewords) with entries in a finite alphabet B. Weight functions are a type of *distance* function which assign a *weight* to each codeword $v \in C$. A *weight enumerator* is a generating function that encodes the weight distribution of a code. If the code C is a vector space, then its *dual* $C^{\perp}$ is the orthogonal vector space under the dot product.

Duality theory for codes was pioneered by Sloane, MacWilliams, and Delsarte [43], [21], [32]. *MacWilliams Identities* are at the center of this theory. MacWilliams Identities are functional equations that relate the weight enumerator of a code to that of its dual. Common weights to consider are Hamming weight, column distance weight, rank weight, complete weight, and Lee weight [27], [21], [32].

If a MacWilliams Identity exists, then knowing the weight distribution of a code is sufficient to recover the weight distribution for its dual. The existence of MacWilliams Identities have led to a number of results including, but not limited to, Duursma's conjectures concerning the "Riemann Hypothesis analogue for linear codes" and Gleason's theorem for self-dual codes [3], [25], [26], [21].

In 1972, Berlekamp, MacWilliams, and Sloane related coding theory to the theory of modular forms in a beautiful way [3]. They defined a real lattice associated to a binary vector code, attached a theta function to that lattice, and showed that the Hamming weight enumerator could be written in terms of theta functions. Broué and Enguehard proved the Hamming weight MacWilliams Identity via the inversion formula for those theta functions [7]. In the mid-1980's, van der Geer and Hirzebruch attached theta functions defined over number rings to self-orthogonal, $C \subseteq C^{\perp}$, vector codes over $\mathbb{F}_p$, for p a prime. They showed that the Lee weight enumerator could be written in terms of these theta functions, which were Hilbert-Siegel modular forms for a specific congruence subgroup [27]. Choie and Jeong extended this result to Jacobi theta functions and provided an analytic proof of the Lee weight MacWilliams Identity for such codes [13].

1.3 Dissertation Results

In this dissertation, we extend the class of codes for which there exists an analytic proof of the MacWilliams Identity via theta function inversion formulas. In Chapter 2, we provide the reader with the necessary preliminaries. In Chapter 3, we attach theta functions to matrix codes $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$. (We believe this is the first time theta functions have been attached to matrix codes. Matrix codes arise from multiple transmit antenna systems where each antenna transmits a row vector.) We provide an analytic proof of the column distance weight MacWilliams Identity for linear codes $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ and an analytic proof of the rank weight MacWilliams Identity for linear codes $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$. In Chapter 4, we improve upon the work of van der Geer, Hirzebruch, Choie, and Jeong [27], [13]. We provide an analytic proof of the Hamming weight MacWilliams Identity for linear vector codes $C \subseteq \mathbb{F}_p^n$. In Chapter 5, we provide a general framework for this problem of providing analytic proofs of MacWilliams Identities by considering codes to be contained in abelian schemes (a type of association scheme). We discuss the pitfalls we encountered when attempting to generalize this analytic argument to other codes. We conclude this exposition by offering a set of guidelines to aide future researchers on this problem.

Chapter 2

Preliminaries

> "Coding theory represents a beautiful example of the applicability of abstract algebra." - Lidl and Pilz [36]

2.1 Codes

For us, a code C is a finite set of matrices of fixed size defined over an alphabet B. Elements $v \in C$ are called *codewords*. The *size of* v is its dimension as a matrix. Let $m, n \in \mathbb{Z}_{>0}$. A *matrix code* C is a subset of $\mathrm{Mat}_{m\times n}(B)$. If $C \subseteq \mathrm{Mat}_{m\times n}(B)$, then $n = 1$ implies C is a (column) vector code of length m and $m = 1$ implies C is a (row) vector code of length n. We now define a linear code.

Definition 2.1.1. Let $m, n, k \in \mathbb{Z}_{>0}$. Let B be a finite commutative ring with identity $1 \neq 0$ and $X = \mathrm{Mat}_{m\times n}(B)$. (Note that X is a B-module.) A code $C \subseteq X$ is called a *linear code of dimension* k *iff* C is a free B-module of rank k.

A *space-time code* $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{C})$ is an $m \times n$ matrix code which is used to send data across multiple antenna information networks by sending row vectors of length n over each of the m antennas [32]. Grant and Varanasi show that each space-time code can be arbitrarily well approximated by a code lifted from a finite field [33]. Hence, B is often taken to be $\mathbb{F}_q$, for q a power of a prime. Until Chapter 5, we let $B = \mathbb{F}_p$ for p a prime, $X = \mathrm{Mat}_{m\times n}(B)$, and $C \subseteq X$ be a k-dimensional linear code.

2.1.1 Weight and Diversity Functions

Weight functions measure the "size" of elements $v \in X$. A weight function, $wt(\cdot)$, is a function on X whose image lies in X or $\mathbb{Z}_{\geq 0}$. Let v_0 be the zero element in X. If the image of $wt(\cdot)$ lies in X, then we define $wt(v_0) = v_0$. If the image of $wt(\cdot)$ lies in $\mathbb{Z}_{\geq 0}$, then we define $wt(v_0) = 0$. That is, the weight of the zero element is always 0.

Diversity functions, $d(\cdot, \cdot)$, measure the "distance" between two elements $u, v \in X$. (We put "distance" in quotation marks because a diversity function may not be a metric.) Diversity functions are functions on $X \times X$ whose image lies in X or $\mathbb{Z}_{\geq 0}$. A weight function $wt(\cdot)$ defines a diversity function $d(\cdot, \cdot)$ by

$$d(u, v) = wt(u - v). \tag{2.1}$$

[We can recover the weight function by $wt(u) = d(u, v_0)$.]

We denote the image of $d(\cdot, \cdot)$, which equals the image of $wt(\cdot)$, by R_d. Hence, $R_d \subseteq X$ or $R_d \subseteq \mathbb{Z}_{\geq 0}$. The *weight distribution of* C is the vector

$$a(C) = (a_r)_{r \in R_d} \tag{2.2}$$

of length $|R_d|$, such that ([32])

$$a_r = |\{v \in C \mid wt(v) = r\}|. \tag{2.3}$$

We now define the weight functions studied in Chapters 3, 4, and 5. We begin with the *Hamming weight function*. For $v \in X$, define the *Hamming weight of* v to be

$$wt_{\mathrm{H}}(v) = |\{(i, j),\ 1 \leq i \leq m,\ 1 \leq j \leq n \mid v_{ij} \neq 0\}|. \tag{2.4}$$

We denote the *Hamming diversity function* by $d_{\mathrm{H}}(\cdot, \cdot)$ and its image by $R_{d_{\mathrm{H}}}$. Note that $R_{d_{\mathrm{H}}} = \{0, 1, \ldots, mn\}$. By (2.1), $d_{\mathrm{H}}(u, v)$ equals the number of entries in which u and v differ.

Let $\vec{0} \in B^m$ be the zero vector and $v_j \in B^m$ be the j^{th} column of $v \in X$ for $1 \leq j \leq n$. We define the *column distance weight of* v to be

$$wt_{\mathrm{cd}}(v) = \left|\left\{1 \leq j \leq n \mid v_j \neq \vec{0}\right\}\right|, \tag{2.5}$$

and the *rank weight of* v to be

$$wt_{\mathrm{rk}}(v) = \mathrm{Rank}(v). \tag{2.6}$$

We denote the *column distance diversity function* by $d_{\mathrm{cd}}(\cdot,\cdot)$ and the *rank diversity function* by $d_{\mathrm{rk}}(\cdot,\cdot)$. We denote their images by $R_{d_{\mathrm{cd}}}$, and $R_{d_{\mathrm{rk}}}$, respectively. Note that $R_{d_{\mathrm{cd}}} = \{0,1,\ldots,n\}$ and $R_{d_{\mathrm{rk}}} = \{0,1,\ldots,\min(m,n)\}$. By (2.5), $d_{\mathrm{cd}}(u,v)$ equals the number of columns in which u and v differ. (Note that the Hamming weight, $wt_{\mathrm{H}}(\cdot)$, on the set of row vectors with entries in B^m, $(B^m)^n$, equals the column distance weight, $wt_{\mathrm{cd}}(\cdot)$, on $\mathrm{Mat}_{m\times n}(B)$.) By (2.6), $d_{\mathrm{rk}}(u,v)$ equals the rank of the matrix $(u-v)$.

We now define two weight functions whose images are in X instead of $\mathbb{Z}_{\geq 0}$. Define the *complete weight function* to be the identity function on X. That is,

$$wt_{\mathrm{c}}(v) = v. \tag{2.7}$$

Recall that $X = \mathrm{Mat}_{m\times n}(\mathbb{F}_p)$. Hence, $|X| = p^{mn}$. Let $X = \{v_0, v_1, \ldots, v_{p^{mn}-1}\}$, where v_0 denotes the zero codeword and $v_i = -v_{p^{mn}-i}$ for all $1 \leq i \leq p^{mn}-1$. Define the *Lee weight function* to be

$$wt_{\mathrm{L}}(v_i) = \begin{cases} v_i, & 0 \leq i \leq \frac{p^{mn}-1}{2} \\ v_{p^{mn}-i}, & \frac{p^{mn}-1}{2}+1 \leq i \leq p^{mn}-1 \end{cases}. \tag{2.8}$$

We denote the *complete diversity function* by $d_{\mathrm{c}}(\cdot,\cdot)$ and the *Lee diversity function* by $d_{\mathrm{L}}(\cdot,\cdot)$. We denote their images by $R_{d_{\mathrm{c}}}$, and $R_{d_{\mathrm{L}}}$, respectively. Note that

$$R_{d_{\mathrm{c}}} = X \quad \text{and} \quad R_{d_{\mathrm{L}}} = \left\{ v_0, v_1, \ldots, v_{\frac{p^{mn}-1}{2}} \right\}. \tag{2.9}$$

In the next section, we define the generating functions for the weight distribution of C as defined in (2.2) and (2.3).

2.1.2 Weight Enumerators

Let $wt(\cdot)$ be a weight function and $d(\cdot,\cdot)$ its corresponding diversity function. Let $a(C) = (a_r)_{r\in R_d}$ be the weight distribution for a code C as defined in (2.2) and (2.3). For the $|R_d|$ inde-

pendent variables $\vec{x}_r = \{x_r\}_{r \in R_d}$, we define the *linear weight enumerator* W_C *of* C to be [8]

$$\mathrm{W}_C\left(\vec{x}_r\right) = \sum_{r \in R_d} a_r x_r. \tag{2.10}$$

The linear Hamming weight enumerator, linear column distance weight enumerator, linear rank weight enumerator, linear complete weight enumerator, and linear Lee weight enumerator are all defined to be $\mathrm{W}_C(\cdot)$ in (2.10) for their respective weight distributions $a(C) = (a_r)_{r \in R_d}$.

Weight enumerators can be *non-linear* functions as well. (These are sometimes referred to as *total weight enumerators*.) The Hamming weight enumerator we study in Chapter 4 is a degree mn homogeneous polynomial in 2 variables and the column distance weight enumerator we study in Chapter 3 is a degree n homogeneous polynomial in 2 variables. We now define these two weight enumerators.

Let $wt_{\mathrm{H}}(\cdot)$ be as in (2.4). Let $a(C) = (a_r)_{r \in R_{d_{\mathrm{H}}}}$ be the Hamming weight distribution for a code C. For the independent variables x_0 and x_1, we define the *Hamming weight enumerator of* C to be

$$\mathrm{HW}_C(x_0, x_1) = \sum_{r=0}^{mn} a_r x_0^{mn-r} x_1^r. \tag{2.11}$$

Let $wt_{\mathrm{cd}}(\cdot)$ be as in (2.5). Let $a(C) = (a_r)_{r \in R_{d_{\mathrm{cd}}}}$ be the column distance weight distribution for a code C. For the independent variables x_0 and x_1, we define the *column distance weight enumerator of* C to be

$$\mathrm{CDW}_C(x_0, x_1) = \sum_{r=0}^{n} a_r x_0^{n-r} x_1^r. \tag{2.12}$$

Gadouleau and Yan study a rank weight enumerator with a similar form to the column distance weight enumerator in (2.12) [31]. In [32], Grant and Varanasi prove the rank weight MacWilliams Identity for matrix codes $C \subseteq \mathrm{Mat}_{m \times n}(\mathbb{F}_q)$ with a rank weight enumerator of the form

$$\sum_{r=0}^{\min(m,n)} a_r f_r,$$

where for a variable x,

$$f_r = \prod_{i=0}^{r-1} \frac{x - q^j}{q^{\max(m,n)} - q^j}.$$

Non-linear complete weight enumerators and non-linear Lee weight enumerators are studied in [17], [13], [27], [10], [11], [9].

Recall from Section 1.2 that a MacWilliams Identity is a functional equation that relates the weight enumerator of a code C to that of its dual. We now make precise the notion of a dual code.

2.1.3 Duality

For a square matrix A, let $\mathrm{Tr}(A)$ denote the sum of the diagonal entries of A and ${}^tA$ denote the transpose of A. For $u, v \in X$, we denote the standard dot product by

$$u \cdot v = \mathrm{Tr}\left({}^tuv\right). \tag{2.13}$$

If x, y are row or column vectors of length n, then $\mathrm{Tr}\left({}^txy\right) = \sum_{j=1}^{n} x_j y_j$, and $(\cdot)$ in (2.13) is the standard vector dot product. The dual code is the orthogonal space to C with respect to the standard dot product in (2.13). That is,

$$C^{\perp} = \{u \in X \mid u \cdot v = 0 \ \ \forall v \in C\}. \tag{2.14}$$

In order for a duality theory to exist, $a\left(C^{\perp}\right)$ must be a function of $a(C)$ for every linear code $C \subseteq X$ [32]. Let $\mathrm{W}_C(\cdot)$ be as in (2.10). If $d(\cdot,\cdot)$ partitions X into an abelian association scheme (see Chapter 5), then there exists a MacWilliams Identity that relates $\mathrm{W}_C(\cdot)$ and $\mathrm{W}_{C^{\perp}}(\cdot)$ ([8], Property 5.42). A functional equation relating $\mathrm{W}_C(\cdot)$ and $\mathrm{W}_{C^{\perp}}(\cdot)$ also relates $a\left(C^{\perp}\right)$ and $a(C)$. Hence, a MacWilliams Identity implies a duality theory. For the weight enumerators defined in Section 2.1.2 a MacWilliams Identity exists [32], [20], [8], [12], [22].

MacWilliams Identities are often proved by algebraic and combinatoric methods. All known analytic proofs of MacWilliams Identities use the inversion formulas of theta functions to derive the functional equation. For linear codes $C \subseteq \mathbb{F}_2^n$, there exists an analytic proof of the Hamming weight MacWilliams Identity [7], [27]. For self-orthogonal, $C \subseteq C^{\perp}$, linear codes $C \subseteq \mathbb{F}_p^n$, for p a prime, there exists an analytic proof of the Lee weight MacWilliams Identity [13].

The goal of our work is to extend the class of codes for which there exist analytic proofs of the MacWilliams Identity. To this end, we now introduce theta functions.

2.2 Theta Functions

2.2.1 Theta Functions of Genus One

We begin with a classical definition of theta functions (for more details see [28], [40]). Let

$$\mathbb{H} = \{x + iy \in \mathbb{C} \mid y \in \mathbb{R}_{>0}\} \tag{2.15}$$

denote the complex upper half plane. Theta functions are analytic functions on $\mathbb{H}$.

Let $\tau \in \mathbb{H}$, $u, v \in \mathbb{C}^n$ be column vectors, $(\cdot)$ be the standard vector dot product as in (2.13), and $\exp(\cdot)$ be the exponential function. The *theta function with characteristic* $\begin{bmatrix} v \\ u \end{bmatrix}$ is defined to be

$$\Theta\left(\tau, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \sum_{\lambda \in \mathbb{Z}^n} \exp\left[\pi i \left(\tau\left(\lambda + v\right) \cdot \left(\lambda + v\right) + 2(\lambda \cdot u) + u \cdot v\right)\right]. \tag{2.16}$$

Let $Q \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a positive definite symmetric matrix; i.e. $Q > 0$ and ${}^tQ = Q$. For a column vector $x \in \mathbb{C}^n$, let $Q[x] = {}^txQx$. We define the *theta function with quadratic form Q and characteristic* $\begin{bmatrix} v \\ u \end{bmatrix}$ to be

$$\Theta\left(\tau, Q, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \sum_{\lambda \in \mathbb{Z}^n} \exp\left[\pi i \left(\tau Q\left[\lambda + v\right] + 2(\lambda \cdot u) + v \cdot u\right)\right]. \tag{2.17}$$

Let I_n be the $n \times n$ identity matrix. Note that $x \cdot x = I[x]$ for $(\cdot)$ in (2.13). By (2.16) and (2.17), we have

$$\Theta\left(\tau, I_n, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \Theta\left(\tau, \begin{bmatrix} v \\ u \end{bmatrix}\right).$$

The relationship between theta functions and positive definite quadratic forms plays a central role in the results of this thesis. Finding a symmetric positive definite matrix Q with *nice properties*

allows us to attach theta functions to our code that, in an appropriate sense, respect the weight functions described in Section 2.1.1. For more on this topic we refer the reader to Chapter 5. We now introduce the more general symplectic theta functions.

2.2.2 Symplectic Theta Functions

The *Siegel upper half plane* generalizes the notion of the complex upper half plane to any genus $g \in \mathbb{Z}_{>0}$, and is denoted by

$$\mathfrak{H}_g = \left\{ Z \in \mathrm{Mat}_{g\times g}(\mathbb{C}) \mid {}^tZ = Z \text{ and } \mathrm{Im}(Z) > 0 \right\}. \tag{2.18}$$

If $g = 1$, then $\mathfrak{H}_1 = \{x + iy \in \mathbb{C} \mid y > 0\}$ is the complex upper half plane ($\mathfrak{H}_1 = \mathbb{H}$). Symplectic theta functions are analytic functions on $\mathfrak{H}_g$.

Let $Z \in \mathfrak{H}_g$, $u, v \in \mathbb{C}^g$ be column vectors, $(\cdot)$ be the standard vector dot product as in (2.13), and $\exp(\cdot)$ be the exponential function. The *symplectic theta function with characteristic* $\begin{bmatrix} v \\ u \end{bmatrix}$ is defined to be

$$\Theta\left(Z, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \sum_{\lambda\in\mathbb{Z}^g} \exp\left[\pi i \left(Z[\lambda + v] + 2(\lambda \cdot u) + v \cdot u\right)\right]. \tag{2.19}$$

Note that the theta functions defined in (2.16), (2.17), and (2.19) all have integral summands. It will be convenient for us to consider theta functions with summands in a more general lattice in $\mathbb{R}^g$ when studying $\mathbb{F}_p$-codes (see Chapter 4).

2.2.3 Theta Functions Defined over Number Fields

The notion of attaching theta functions to a number field F goes back to Hecke. In [51] Stark provides a nice description of this process so we follow his setup here with some slight modifications. Let the number field F be an abelian extension of $\mathbb{Q}$ of degree $d = [F : \mathbb{Q}]$. Let $\sigma_1, \ldots, \sigma_{r_1(F)}$ be its $r_1(F)$ real embeddings and for $r_1(F) + 1 \le j \le r_1(F) + r_2(F)$, $\left(\sigma_j, \sigma_{j+r_2(F)}\right)$ be its $r_2(F)$ pairs of complex conjugate embeddings. For $\gamma \in F$, we write $\sigma_j(\gamma) = \gamma^{(j)}$; i.e. if $\overline{(\cdot)}$ denotes complex

conjugation then for $\gamma \in F$ and $r_1(F) + 1 \leq j \leq r_1(F) + r_2(F)$,

$$\gamma^{(j+r_2(F))} = \overline{\gamma^{(j)}}. \tag{2.20}$$

We denote the trace of γ by

$$\mathrm{Tr}_{\mathbb{Q}}^{F}(\gamma) = \sum_{j=1}^{d} \gamma^{(j)}. \tag{2.21}$$

Note that since F is an abelian extension of $\mathbb{Q}$, there is a unique notion of complex conjugation for $\gamma \in F$ which we also denote by $\overline{(\cdot)}$. With this notation, consider the following definition.

Definition 2.2.1. Let $\tau \in \mathbb{H}$, the complex upper half plane. Let a number field F be an abelian extension of $\mathbb{Q}$ and $u, v \in F^n$ be column vectors for some $n \in \mathbb{Z}_{>0}$. Let $\mathfrak{a}$ be a non-zero fractional ideal of F. Define the *theta function attached to F and $\mathfrak{a}$ with characteristic* $\begin{bmatrix} v \\ u \end{bmatrix}$ to be

$$\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v \\ u \end{bmatrix}\right)$$
$$= \sum_{\lambda \in \mathfrak{a}^n} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^{F}\left((\lambda + v) \cdot \overline{(\lambda + v)}\right) - 2\pi i \mathrm{Tr}_{\mathbb{Q}}^{F}\left(u \cdot \lambda + \frac{u \cdot v}{2}\right)\right],$$

where $\exp(\cdot)$ is the exponential function, $(\cdot)$ is the standard dot product on F^n, and $\mathrm{Tr}_{\mathbb{Q}}^{F}(\cdot)$ is as in (2.21).

The theta function in Definition 2.2.1 is a specialization of a symplectic theta function of sufficiently large dimension [49], [6], [44], [45], [46]. There exist more general definitions of theta functions attached to number fields than the one we cited here [46], but we will not need to employ them. We now say a few words about attaching theta functions to codes.

2.3 Theta Functions and Codes

Leech and Sloane attached real lattices to linear codes $C \subseteq \mathbb{F}_2^n$ [35]. Berlekamp, MacWilliams, and Sloane took this idea a step further by attaching a theta function to this code lattice and showing that it was equal to the Hamming weight enumerator in (2.11) with x_0 and x_1 replaced by

genus one theta functions [3]. Sloane generalizes this theory by attaching complex lattices to linear codes $C \subseteq \mathbb{F}_4^n$ [50]. Choie and Betsumiya attached Hilbert-Siegel modular forms to such codes [4]. Maher attached theta functions and real lattices to linear codes $C \subseteq \mathbb{F}_p^n$ and related them to the Lee weight enumerator [37], [38]. Duke is one of the first to generalize this theory to include Siegel modular forms. He defines a *joint weight enumerator* and relates theta functions defined on $\mathfrak{H}_2$ to a product of binary codes [23]. This idea is further explored by Choie and Oura in [16]. Other generalizations of this theory include attaching Jacobi theta functions to codes defined over finite fields and finite rings [5], [13], [17], [12], [11], [10].

Although theta functions have been attached to codes and related to their weight enumerators in many cases, analytic proofs of the MacWilliams Identities are not often provided. In Chapter 3, we provide an analytic proof of the column distance weight MacWilliams Identity for linear codes $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ and an analytic proof of the rank weight MacWilliams Identity for linear codes $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$. In Chapter 4, we provide an analytic proof of the Hamming weight MacWilliams Identity for linear codes $C \subseteq \mathbb{F}_p^n$. Hence, we extend the class of codes for which there exists an analytic proof of the MacWilliams Identity.

Chapter 3

$\mathbb{F}_2$-Matrix Codes

Berlekamp, MacWilliams, and Sloane attached theta functions to linear vector codes $C \subseteq \mathbb{F}_2^n$, and related them to the Hamming weight enumerator [3]. Broué and Enguehard provided an analytic proof of the Hamming weight MacWilliams Identity for such codes [7]. We attach theta functions to linear *matrix* codes $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$. We study two weight functions for such codes: The column distance weight of a matrix codeword is the number of non-zero columns and the rank weight of a matrix codeword is the rank of the matrix. We provide analytic proofs of the column distance weight MacWilliams Identity for linear matrix codes $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ and the rank weight MacWilliams Identity for linear matrix codes $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$.

Recent work on space-time codes for multiple-antenna systems has led to a renewal of the study of matrix codes over finite fields endowed with various metrics. Among these are column distance codes and rank codes. Grant and Varanasi provide a nice weight enumerator for such codes, and give a combinatorial proof of the MacWilliams Identities for these weight enumerators [32]. For a history of such codes, we refer the reader to [31], [30], [32].

3.1 Linear $\mathbb{F}_p$-Matrix Codes and Real Lattices

Let p be a prime. Let $k, m, n \in \mathbb{Z}_{>0}$. A k-dimensional linear matrix code $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_p)$ is an $\mathbb{F}_p$-subspace of dimension k. Let $v \in C$. Let $v_j \in \mathbb{F}_p^m$ denote the j^{th} column of v. Elements $v = \left[v_1|\cdots|v_n\right] \in C$ are called *codewords*. Let $\vec{0}$ denote the zero (column) vector of length m. We

define the *column distance weight of* v to be

$$wt_{\mathrm{cd}}(v) = \left|\left\{1 \leq j \leq n \mid v_j \neq \vec{0}\right\}\right|.$$

We define the *rank weight of* v to be

$$wt_{\mathrm{rk}}(v) = \mathrm{Rank}(v).$$

Let $u, v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_p)$. Note that $d_{\mathrm{cd}}(u,v) = wt_{\mathrm{cd}}(u-v)$ and $d_{\mathrm{rk}}(u,v) = wt_{\mathrm{rk}}(u-v)$ are both metrics on $\mathrm{Mat}_{m\times n}(\mathbb{F}_p)$. Throughout, we assume that $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_p)$ is a k-dimensional linear code.

Definition 3.1.1. For the independent variables x_0 and x_1, define the *column distance weight enumerator of* C to be

$$\mathrm{CDW}_C(x_0, x_1) = \sum_{r=0}^{n} a_r x_0^{n-r} x_1^r, \tag{3.1}$$

where for $0 \leq r \leq n$,

$$a_r = \left|\{v \in C \mid wt_{\mathrm{cd}}(v) = r\}\right|.$$

For the independent variables $x_0, \ldots, x_{\min(m,n)}$, define the *linear rank weight enumerator of* C to be

$$\mathrm{RW}_C\left(x_0, \ldots, x_{\min(m,n)}\right) = \sum_{r=0}^{\min(m,n)} a_r x_r, \tag{3.2}$$

where for $0 \leq r \leq \min(m,n)$,

$$a_r = \left|\{v \in C \mid wt_{\mathrm{rk}}(v) = r\}\right|.$$

Note that $\mathrm{CDW}_C(x_0, x_1)$ in (3.1) is a homogeneous polynomial in 2 variables of degree n. Note that $\mathrm{RW}_C\left(x_0, \ldots, x_{\min(m,n)}\right)$ in (3.2) is a homogeneous polynomial in $\min(m,n)$ variables of degree 1. This explains the use of the term linear. Note that the linear rank weight enumerator in Definition 3.1.1 has a different form than the rank weight enumerator of Delsarte's in ([20], (3.10)) and of Grant and Varanasi's in ([32], Theorem 3). We choose this form for the rank weight enumerator because we found it to be the most natural one to relate to theta functions.

Weight enumerators are generating functions that encode the weight distribution $a(C) = (a_r)_{r=0}^n$ of a code C. For a square matrix A, let $\mathrm{Tr}(A)$ denote the sum of the diagonal elements of A and ${}^tA$ denote the transpose of A. For $u, v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_p)$, we denote the dot product of u and v by

$$u \cdot v = \mathrm{Tr}\left({}^tuv\right). \tag{3.3}$$

Let x, y be vectors of length n. Note that $\mathrm{Tr}\left({}^txy\right) = \sum_{j=1}^n x_j y_j$. Hence, the dot product in (3.3) is the standard vector dot product. For $(\cdot)$ as in (3.3), define the *dual code* to be

$$C^\perp = \{u \in \mathrm{Mat}_{m\times n}(\mathbb{F}_p) \mid u \cdot v = 0 \ \ \forall v \in C\}. \tag{3.4}$$

If $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_p)$ is a k-dimensional linear code, then $C^\perp$ is an $(mn-k)$-dimensional linear code [27].

A *real lattice* (of dimension n) is a full rank discrete additive subgroup of $\mathbb{R}^n$. That is, Λ is a real lattice *iff*

$$\Lambda = \mathbb{Z}x_1 \oplus ... \oplus \mathbb{Z}x_n, \tag{3.5}$$

where $\{x_1, ..., x_n\}$ is a basis of column vectors for $\mathbb{R}^n$. Let $\det(\cdot)$ denote the determinant function. The *volume of* Λ is defined to be

$$\mathrm{vol}(\mathbb{R}^n/\Lambda) = \left|\det\left[x_1|\cdots|x_n\right]\right|. \tag{3.6}$$

If Λ is a real lattice of dimension n as in (3.5), we define the *dual lattice* to be

$$\Lambda^* = \{x \in \mathbb{R}^n \mid x \cdot y \in \mathbb{Z}, \ \forall y \in \Lambda\}, \tag{3.7}$$

where $(\cdot)$ denotes the standard vector dot product on $\mathbb{R}^n$.

3.2 Theta Functions Attached to $\mathbb{F}_2$-Matrix Codes

We introduce symplectic theta functions. The *Siegel upper half plane* generalizes the notion of the complex upper half plane to any genus $g \in \mathbb{Z}_{>0}$, and is denoted by

$$\mathfrak{H}_g = \left\{Z \in \mathrm{Mat}_{g\times g}(\mathbb{C}) \mid {}^tZ = Z \text{ and } \mathrm{Im}(Z) > 0\right\}.$$

If $g = 1$, then $\mathfrak{H}_1 = \{x + iy \in \mathbb{C} \mid y > 0\}$ is the complex upper half plane. Throughout, we let

$$\mathbb{H} = \mathfrak{H}_1. \tag{3.8}$$

Let $u, v, x \in \mathbb{C}^g$ be column vectors, $Z \in \mathfrak{H}_g$, and $Z[x] = {}^t xZx$. The *symplectic theta function with characteristic* $\begin{bmatrix} v \\ u \end{bmatrix}$ is defined to be

$$\Theta\left(Z, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \sum_{\lambda \in \mathbb{Z}^g} \exp\left(\pi i \left(Z\left[\lambda + v\right] + 2\left(\lambda \cdot u\right) + v \cdot u\right)\right), \tag{3.9}$$

where $\exp(\cdot)$ is the exponential function and $(\cdot)$ is the standard vector dot product on $\mathbb{C}^g$.

Let I_g be the $g \times g$ identity matrix. The *symplectic group of genus* g is

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \left\{ \gamma \in \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}) \mid {}^t\gamma \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix} \gamma = \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix} \right\}. \tag{3.10}$$

Let $A, B, C, D \in \mathrm{Mat}_{g\times g}(\mathbb{Z})$ be such that $\gamma = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$. The symplectic group of genus g acts on $Z \in \mathfrak{H}_g$ by

$$\gamma \circ Z = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \circ Z = (AZ + B)(CZ + D)^{-1}.$$

Throughout, we set $p = 2$. We now describe how to attach a symplectic theta function to each codeword $v = \begin{bmatrix} v_1 | \cdots | v_n \end{bmatrix} \in \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$. First, we identify a matrix codeword $v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$ with a vector in $\mathbb{F}_2^{mn}$ by the "stacking" map

$$\begin{aligned} \Phi : &\mathrm{Mat}_{m\times n}(\mathbb{F}_2) \longrightarrow \mathbb{F}_2^{mn} \\ &\begin{bmatrix} v_1 | \cdots | v_n \end{bmatrix} \longmapsto \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}. \end{aligned} \tag{3.11}$$

Let $e_1, \ldots, e_n \in \{0,1\}^n \subseteq \mathbb{Z}^n$ be the standard basis (column) vectors of length n. Note that

$$\Phi(v) = (I_n \otimes v) \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}, \tag{3.12}$$

where $\otimes$ denotes the Kronecker product of matrices. (Note that an $\mathbb{F}_2$-linear map $\Phi^{-1} : \mathbb{F}_2^{mn} \longrightarrow \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$ also exists.)

Let $u, v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$. Note that $u \cdot v = \Phi(u) \cdot \Phi(v)$ for $(\cdot)$ as in (3.3). Next, we follow [35] and define the $\mathbb{Z}$-module homomorphism

$$\begin{aligned} \rho : &\mathbb{Z}^{mn} \to (\mathbb{Z}/2\mathbb{Z})^{mn} = \mathbb{F}_2^{mn} \\ &\begin{bmatrix} x_1 \\ \vdots \\ x_{mn} \end{bmatrix} \longmapsto \begin{bmatrix} x_1 \bmod 2 \\ \vdots \\ x_{mn} \bmod 2 \end{bmatrix}. \end{aligned} \tag{3.13}$$

For ease of notation, define

$$\Phi(v) = \widehat{v}. \tag{3.14}$$

For $\widehat{v}$ as in (3.14), define

$$\widetilde{v} \in \{0,1\}^{mn} \subseteq \mathbb{Z}^{mn}, \tag{3.15}$$

such that $\rho(\widetilde{v}) = \widehat{v}$. Hence,

$$\rho^{-1}(\widehat{v}) = 2\mathbb{Z}^{mn} + \widetilde{v}. \tag{3.16}$$

For $Z \in \mathfrak{H}_{mn}$, we define the *theta function attached to* v to be

$$\Theta_v(Z) = \sum_{\lambda \in \rho^{-1}(\widehat{v})} \exp\left(\pi i \frac{Z}{4}[\lambda]\right). \tag{3.17}$$

By (3.16) and (3.17), we have

$$\Theta_v(Z) = \sum_{\lambda \in 2\mathbb{Z}^{mn} + \widetilde{v}} \exp\left(\pi i \frac{Z}{4}[\lambda]\right). \tag{3.18}$$

Let $\lambda = 2\mu + \widetilde{v}$. Note that λ runs through $(2\mathbb{Z}^{mn} + \widetilde{v})$ as μ runs through $\mathbb{Z}^{mn}$. By (3.18),

$$\Theta_v(Z) = \sum_{\mu \in \mathbb{Z}^{mn}} \exp\left(\pi i \frac{Z}{4} [2\mu + \widetilde{v}]\right). \tag{3.19}$$

We factor the $\frac{1}{4}$ into the square brackets. By (3.19),

$$\Theta_v(Z) = \sum_{\mu \in \mathbb{Z}^{mn}} \exp\left(\pi i Z \left[\mu + \frac{1}{2}\widetilde{v}\right]\right). \tag{3.20}$$

By (3.9) and (3.20), we conclude that

$$\Theta_v(Z) = \Theta\left(Z, \begin{bmatrix} \frac{1}{2}\widetilde{v} \\ 0 \end{bmatrix}\right). \tag{3.21}$$

Define

$$\widehat{C} = \{\widehat{v} \mid v \in C\}, \tag{3.22}$$

for $\widehat{v}$ in (3.14). Define the *lattice attached to* C to be

$$\Lambda_C = \frac{1}{\sqrt{2}} \rho^{-1}\left(\widehat{C}\right). \tag{3.23}$$

Note that $\Lambda_C \subseteq \mathbb{R}^{mn}$ is a real lattice of dimension mn as in (3.5) (since C is a linear code). This is why we only consider linear codes. The following lemma demonstrates the importance of the scalar $\frac{1}{\sqrt{2}}$.

Lemma 3.2.1. *Let $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$ be a linear code of dimension k, Λ_C be as in* (3.23)*, and * denote the dual lattice as in* (3.7)*. Then*

$$\Lambda_C^* = \Lambda_{C^\perp}.$$

Proof. Recall the definitions of Λ_C in (3.23), $\widehat{C}$ in (3.22), $C^\perp$ in (3.4), and $(\cdot)$ in (3.3). By ([27], Lemma 1.10), $\Lambda_C^* = \Lambda_{C^\perp}$. □

We define the *theta function attached to* C to be

$$\Theta_C(Z) = \sum_{\lambda \in \Lambda_C} \exp\left(\pi i Z[\lambda]\right). \tag{3.24}$$

Since $\rho^{-1}\left(\widehat{C}\right) = \bigcup_{v\in C} \rho^{-1}\left(\widehat{v}\right)$, by (3.17), (3.23), and (3.24), we have

$$\Theta_C(Z) = \sum_{v\in C} \sum_{\lambda \in \frac{1}{\sqrt{2}}\rho^{-1}(\widehat{v})} \exp(\pi i Z[\lambda]) = \sum_{v\in C} \Theta_v(2Z). \tag{3.25}$$

3.3 Rank and Column Distance Group Actions

3.3.1 Rank Group Action

Let $\mathrm{GL}_n(\mathbb{F}_2)$ be the general linear group of $n \times n$ matrices over $\mathbb{F}_2$. Let $u, v \in \mathrm{Mat}_{n\times n}(\mathbb{F}_2)$ and $M, N \in \mathrm{GL}_n(\mathbb{F}_2)$. (Throughout, we assume $m = n$ when considering rank codes.) The group $H = \mathrm{GL}_n(\mathbb{F}_2) \times \mathrm{GL}_n(\mathbb{F}_2)$ acts on $\mathrm{Mat}_{n\times n}(\mathbb{F}_2)$ by

$$(M, N) \circ v = Mv \left({}^tN\right). \tag{3.26}$$

This action consists of row operations and column operations on elements $v \in \mathrm{Mat}_{n\times n}(\mathbb{F}_2)$.

Let $wt_{\mathrm{rk}}(v) = j$. We say a block-diagonal matrix v is in *reduced rank form* if

$$v = \begin{bmatrix} I_j & \\ & \mathbf{0}_{(n-j)} \end{bmatrix},$$

where $\mathbf{0}_{(n-j)}$ is the $(n-j) \times (n-j)$ zero matrix. Note that $wt_{\mathrm{rk}}(u) = wt_{\mathrm{rk}}(v)$ *iff* u and v have the same reduced rank form. Hence, u and v have the same reduced rank form *iff* there exists a set of elementary row operation matrices $\{R_i\}_{i=1}^{l_1} \subseteq \mathrm{GL}_n(\mathbb{F}_2)$ and a set of elementary column operation matrices $\{C_i\}_{i=1}^{l_2} \subseteq \mathrm{GL}_n(\mathbb{F}_2)$, such that

$$u = (R_{l_1} \cdots R_1)\, v \left({}^tC_1 \cdots {}^tC_{l_2}\right) = (R_{l_1} \cdots R_1)\, v \left({}^t(C_{l_2} \cdots C_1)\right). \tag{3.27}$$

Let $\Phi(\cdot)$ be as in (3.11). We define a subgroup

$$G_{\mathrm{rk}} \subseteq \mathrm{GL}_{n^2}(\mathbb{F}_2)$$

whose action on $\Phi(\mathrm{Mat}_{n\times n}(\mathbb{F}_2)) = (\mathbb{F}_2)^{n^2}$ by left multiplication represents the action of H on $\mathrm{Mat}_{n\times n}(\mathbb{F}_2)$ in (3.26). To this end, we define the map

$$\begin{aligned} \alpha :& \mathrm{GL}_n(\mathbb{F}_2) \longrightarrow \mathrm{GL}_{n^2}(\mathbb{F}_2) \\ & M \quad \longmapsto \; M \otimes I_n. \end{aligned} \tag{3.28}$$

Note that $\alpha(\cdot)$ sends each non-zero entry of $M \in \mathrm{GL}_n(\mathbb{F}_2)$ to I_n and each zero entry of $M \in \mathrm{GL}_n(\mathbb{F}_2)$ to $\mathbf{0}_n$, the $n \times n$ zero matrix. Also, note that

$$\alpha(MN) = \alpha(M)\alpha(N). \tag{3.29}$$

We define the matrix $M_{TR} \in \mathrm{GL}_{n^2}(\mathbb{F}_2)$, whose action on $\Phi\left(\mathrm{Mat}_{n\times n}(\mathbb{F}_2)\right)$ by left multiplication represents the matrix operation of transpose. That is,

$$M_{TR}\Phi(v) = \Phi\left({}^{t}v\right). \tag{3.30}$$

Note that $M_{TR} \in \mathrm{GL}_{n^2}(\mathbb{F}_2)$ is a permutation matrix. This matrix allows us to act on the rows of v, in addition to the columns of v, via left multiplication by elements in $\mathrm{GL}_{n^2}(\mathbb{F}_2)$.

By the definitions of $\Phi(\cdot)$ in (3.11) and (3.12), $\alpha(\cdot)$ in (3.28), and properties of the Kronecker product,

$$\Phi\left((I_n, M)\circ v\right) = \Phi\left(v\left({}^{t}M\right)\right) = \alpha(M)\Phi(v) \tag{3.31}$$

and

$$\Phi\left((M, I_n)\circ v\right) = \Phi(Mv) = M_{TR}\alpha(M)M_{TR}\Phi(v). \tag{3.32}$$

By (3.31) and (3.32), we have

$$\Phi\left((M, N)\circ v\right) = \Phi\left(Mv\left({}^{t}N\right)\right) = M_{TR}\alpha(M)M_{TR}\alpha(N)\Phi(v). \tag{3.33}$$

By (3.27), (3.29), and (3.33), u and v have the same reduced rank form (i.e. $wt_{\mathrm{rk}}(u) = wt_{\mathrm{rk}}(v)$) *iff* there exists a set of elementary row operation matrices $\{R_i\}_{i=1}^{l_1} \subseteq \mathrm{GL}_n(\mathbb{F}_2)$ and a set of elementary column operation matrices $\{C_i\}_{i=1}^{l_2} \subseteq \mathrm{GL}_n(\mathbb{F}_2)$, such that

$$\Phi(u) = M_{TR}\left(\alpha\left(R_{l_1}\right)\cdots\alpha\left(R_1\right)\right)M_{TR}\left(\alpha\left(C_{l_2}\right)\cdots\alpha\left(C_1\right)\right)\Phi(v). \tag{3.34}$$

Since $\mathrm{GL}_n(\mathbb{F}_2)$ is generated by the set of elementary matrices, $\mathcal{E}$, we define $G_{\mathrm{rk}} \subseteq \mathrm{GL}_{n^2}(\mathbb{F}_2)$ to be the group generated by the set of matrices $\alpha\left(\mathcal{E}\right) \cup \{M_{TR}\}$. The left (multiplicative) group action of G_{rk} partitions $\Phi\left(\mathrm{Mat}_{n\times n}\left(\mathbb{F}_2\right)\right) = \left(\mathbb{F}_2\right)^{n^2}$ into the set of orbits $\{\mathfrak{O}_j\}_{j=0}^{n}$, such that

$$\mathfrak{O}_j = \left\{\Phi(v) \mid wt_{\mathrm{rk}}(v) = j\right\}. \tag{3.35}$$

3.3.2 Column Distance Group Action

Let $v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$ be such that $wt_{\mathrm{cd}}(v) = j$. Let $w = {}^t(1, 0, \ldots, 0) \in \mathbb{F}_2^m$. Recall that $\vec{0}$ denotes the zero (column) vector of length m. We say v is in *reduced column distance form* if the first j-columns of v equal w, and the last $(n-j)$-columns of v equal $\vec{0}$.

As in Section 3.3.1, we define a subgroup $G_{\mathrm{cd}} \subseteq \mathrm{GL}_{mn}(\mathbb{F}_2)$ whose action on $\Phi\left(\mathrm{Mat}_{m\times n}(\mathbb{F}_2)\right) = \mathbb{F}_2^{mn}$ by left multiplication yields the partition $\{\mathfrak{O}_j\}_{j=0}^n$, such that

$$\mathfrak{O}_j = \{\Phi(v) \mid wt_{\mathrm{cd}}(v) = j\}. \tag{3.36}$$

To this end, consider the following lemma.

Lemma 3.3.1. *Let $v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$. Define the subgroup $G_{\mathrm{cd}} \subseteq \mathrm{GL}_{mn}(\mathbb{F}_2)$ to be generated by the:*

(1) Matrices representing the generators of the permutation group on n elements acting on the columns of v.

(2) Matrices representing the generators of the permutation group on m elements acting on the entries of the first column of v.

(3) Matrix representing the addition of the $(1,1)$-entry to the $(2,1)$-entry of v.

The action of G_{cd} on $\mathbb{F}_2^{mn}$ by left multiplication partitions $\mathbb{F}_2^{mn}$ into the set of orbits $\{\mathfrak{O}_j\}_{j=0}^n$, for $\mathfrak{O}_j$ as in (3.36).

As in (3.34), u and v have the same reduced column distance form (i.e. $wt_{\mathrm{cd}}(u) = wt_{\mathrm{cd}}(v)$) *iff* there exists matrices $\{E_i\}_{i=1}^l \subseteq G_{\mathrm{cd}}$, such that

$$\Phi(u) = \left(\prod_{i=1}^{l} E_i\right)\Phi(v).$$

Throughout, we set $m = 2$. For $m > 2$, we were unable to provide an analytic proof for the column distance weight or rank weight MacWilliams Identities because we could not write the column distance weight enumerator in (3.1) or the rank weight enumerator in (3.2) in terms of theta functions. In the following section, we relate $\Theta_C(Z)$ in (3.25) to the weight enumerators in Definition 3.1.1.

3.4 Theta Functions and Weight Enumerators

We begin by defining two theta functions that play a central role in the analytic proof of the column distance weight MacWilliams Identity.

Definition 3.4.1. Let $n = 1$. Let

$$q = \frac{1}{\sqrt{3}} \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}. \tag{3.37}$$

Note that $q > 0$ and $\det(q) = 1$. Let $\tau \in \mathbb{H}$ and $Z = \tau q \in \mathfrak{H}_2$. Recall that $\vec{0} \in \mathrm{Mat}_{2\times 1}(\mathbb{F}_2)$ denotes the zero vector and $w = {}^t(1,0) \in \mathrm{Mat}_{2\times 1}(\mathbb{F}_2)$. Note that $\vec{0}$ and w are in reduced column distance form. For $\Theta_v(Z)$ in (3.21), we define

$$\Theta_0(\tau) = \Theta_{\vec{0}}(Z) \quad \text{and} \quad \Theta_1(\tau) = \Theta_w(Z). \tag{3.38}$$

If $Z = \tau q$ as in Definition 3.4.1, we write $\Theta_v(\tau)$ for $\Theta_v(Z)$ in (3.21). The reason we are working with theta functions defined over the subset $\tau q \subseteq \mathfrak{H}_2$ is due to the following lemmas.

Lemma 3.4.2. *Define the matrices $M_{ES}, M_{EA} \in \mathrm{GL}_2(\mathbb{F}_2)$ to be*

$$M_{ES} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } M_{EA} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{3.39}$$

The subscripts ES, and EA, stand for Entry Switch, and Entry Add, respectively. Let G_{cd} be as in Lemma 3.3.1. Note that G_{cd} is generated by M_{ES} and M_{EA}, and $G_{\mathrm{cd}} = \mathrm{GL}_2(\mathbb{F}_2)$. Define the matrices $\widetilde{M}_{ES}, \widetilde{M}_{EA} \in \mathrm{GL}_2(\mathbb{Z})$ to be

$$\widetilde{M}_{ES} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \widetilde{M}_{EA} = \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}. \tag{3.40}$$

Let $\widetilde{G}_{\mathrm{cd}}$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z})$ generated by $\widetilde{M}_{ES}$ and $\widetilde{M}_{EA}$. Then $\widetilde{G}_{\mathrm{cd}}$ surjects onto G_{cd}, and for all $M \in \widetilde{G}_{\mathrm{cd}}$,

$${}^tMqM = q. \tag{3.41}$$

Proof. Let $\rho(\cdot)$ be the (mod 2) map as in (3.13). Extending ρ to act componentwise on matrices (instead of just on vectors), by (3.39) and (3.40) we have $\rho\left(\widetilde{M}_{ES}\right) = M_{ES}$ and $\rho\left(\widetilde{M}_{EA}\right) = M_{EA}$. Note that $\mathrm{GL}_2(\mathbb{F}_2)$ is the non-abelian group of order 6, so

$$M_{ES} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } M_{EA} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

generate the group. Hence, $\widetilde{G}_{\mathrm{cd}}$ surjects onto $G_{\mathrm{cd}} = \mathrm{GL}_2(\mathbb{F}_2)$.

To prove (3.41), it is a quick calculation to check that

$$^t\widetilde{M}_{ES} q \widetilde{M}_{ES} = q \quad \text{and} \quad ^t\widetilde{M}_{EA} q \widetilde{M}_{EA} = q. \tag{3.42}$$

□

The property of q illustrated in (3.42) is crucial to our results. The existence of a quadratic form which is *invariant* under transpose conjugation by column distance preserving matrices plays a central role in the analytic proof of the column distance MacWilliams Identity. The following result builds upon Lemma 3.4.2.

Lemma 3.4.3. *Let $Z = \tau q$ as in Definition 3.4.1, $\Theta_v(\tau)$ be as in* (3.21)*, $\Theta_0(\tau)$ and $\Theta_1(\tau)$ be as in* (3.38)*, and $x, y \in \mathrm{Mat}_{2\times 1}(\mathbb{F}_2)$. Then,*

$$\Theta_x(\tau) = \begin{cases} \Theta_0(\tau), & x = \vec{0} \\ \Theta_1(\tau), & x \neq \vec{0} \end{cases}. \tag{3.43}$$

So, $wt_{\mathrm{cd}}(x) = wt_{\mathrm{cd}}(y)$ implies $\Theta_x(\tau) = \Theta_y(\tau)$.

Proof. Let $M \in \mathrm{GL}_2(\mathbb{F}_2)$. Recall from Lemma 3.4.2 that M_{ES} and M_{EA} in (3.39) generate $\mathrm{GL}_2(\mathbb{F}_2)$. The action of M_{ES}, and M_{EA} on $\mathrm{Mat}_{2\times 1}(\mathbb{F}_2)$ (by left multiplication), represents switching the first and second entries, and adding the first entry to the second, respectively. Hence, $\mathrm{GL}_2(\mathbb{F}_2)$ partitions $\mathrm{Mat}_{2\times 1}(\mathbb{F}_2)$ into the two orbits $\mathfrak{O}_0 = \left\{\vec{0}\right\}$ and $\mathfrak{O}_1 = \{^t(1,0), ^t(0,1), ^t(1,1)\}$, and it suffices to show that $\Theta_{Mx}(\tau) = \Theta_x(\tau)$.

By (3.20), we have

$$\Theta_x(\tau) = \sum_{\lambda \in \mathbb{Z}^2} \exp\left(\pi i \tau q\left[\lambda + \frac{1}{2}\widetilde{x}\right]\right). \tag{3.44}$$

By (3.44),

$$\begin{aligned}\Theta_{Mx}(\tau) &= \sum_{\lambda\in\mathbb{Z}^2} \exp\left(\pi i\tau q\left[\lambda + \frac{1}{2}\widetilde{M}\widetilde{x}\right]\right) \\ &= \sum_{\lambda\in\mathbb{Z}^2} \exp\left(\pi i\tau\left({}^t\widetilde{M}q\widetilde{M}\right)\left[\widetilde{M}^{-1}\lambda + \frac{1}{2}\widetilde{x}\right]\right). \end{aligned} \tag{3.45}$$

Let $\mu = \widetilde{M}^{-1}\lambda$. Since $\widetilde{M}^{-1} \in \mathrm{GL}_2(\mathbb{Z})$, μ runs through $\mathbb{Z}^2$ as λ does. By Lemma 3.4.2, ${}^t\widetilde{M}q\widetilde{M} = q$. Hence,

$$\Theta_{Mx}(\tau) = \sum_{\mu\in\mathbb{Z}^2} \exp\left(\pi i\tau q\left[\mu + \frac{1}{2}\widetilde{x}\right]\right) = \Theta_x(\tau). \tag{3.46}$$

□

We now define three theta functions that play a central role in the analytic proof of the *rank weight* MacWilliams Identity.

Definition 3.4.4. Let $n = 2$. Let

$$R = \frac{1}{3}\begin{bmatrix} 4 & -2 & -2 & 1 \\ -2 & 4 & 1 & -2 \\ -2 & 1 & 4 & -2 \\ 1 & -2 & -2 & 4 \end{bmatrix}. \tag{3.47}$$

Note that $R > 0$ and $\det(R) = 1$. Let $\tau \in \mathbb{H}$ and $Z = \tau R \in \mathfrak{H}_4$. Let $u_0, u_1, u_2 \in \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$ be codewords such that

$$u_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad u_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{and} \quad u_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3.48}$$

Note that u_0, u_1, and u_2 are in reduced rank form. For $\Theta_v(Z)$ in (3.21), we define

$$\theta_0(\tau) = \Theta_{u_0}(Z), \quad \theta_1(\tau) = \Theta_{u_1}(Z), \quad \text{and} \quad \theta_2(\tau) = \Theta_{u_2}(Z). \tag{3.49}$$

If $Z = \tau R$ as in Definition 3.4.4, we write $\Theta_v(\tau)$ for $\Theta_v(Z)$ as in (3.21). The reason we are working with theta functions defined over the subset $\tau R \subseteq \mathfrak{H}_4$ is due to the following lemmas.

Lemma 3.4.5. *Define the matrices* $M_{CS}, M_{CA}, M_{TR} \in \mathrm{GL}_4(\mathbb{F}_2)$ *to be*

$$M_{CS} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \; M_{CA} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \; M_{TR} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.50}$$

The subscripts CS, CA, *and* TR *stand for Column Switch, Column Add, and Transpose, respectively. Let* G_{rk} *be as in Section 3.3.1. Note that* G_{rk} *is the subgroup of* $\mathrm{GL}_4(\mathbb{F}_2)$ *generated by* M_{CS}, M_{CA}, *and* M_{TR}. *Define the matrices* $\widetilde{M}_{CS}, \widetilde{M}_{CA}, \widetilde{M}_{TR} \in \mathrm{GL}_4(\mathbb{Z})$ *to be*

$$\widetilde{M}_{CS} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \; \widetilde{M}_{CA} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}, \; \widetilde{M}_{TR} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.51}$$

Let $\widetilde{G}_{\mathrm{rk}}$ *be the subgroup of* $\mathrm{GL}_4(\mathbb{Z})$ *generated by* $\widetilde{M}_{CS}$, $\widetilde{M}_{CA}$, *and* $\widetilde{M}_{TR}$. *Then* $\widetilde{G}_{\mathrm{rk}}$ *surjects onto* G_{rk} *and for all* $M \in \widetilde{G}_{\mathrm{rk}}$,

$$^tMRM = R. \tag{3.52}$$

Proof. The proof is similar to that for Lemma 3.4.2. □

As in (3.42), the property of R illustrated in (3.52) is crucial to the analytic proof of the rank weight MacWilliams Identity. The following result builds upon Lemma 3.4.5.

Lemma 3.4.6. *Let* $Z = \tau R$ *as in Definition 3.4.4,* $\Theta_v(\tau)$ *be as in* (3.21), $\theta_0(\tau)$, $\theta_1(\tau)$, *and* $\theta_2(\tau)$ *be as in* (3.49), *and* $x, y \in \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$. *Then,*

$$\Theta_x(\tau) = \begin{cases} \theta_0(\tau), & wt_{\mathrm{rk}}(x) = 0 \\ \theta_1(\tau), & wt_{\mathrm{rk}}(x) = 1 \\ \theta_2(\tau), & wt_{\mathrm{rk}}(x) = 2 \end{cases}. \tag{3.53}$$

So, $wt_{\mathrm{rk}}(x) = wt_{\mathrm{rk}}(y)$ *implies* $\Theta_x(\tau) = \Theta_y(\tau)$.

Proof. Let $M \in G_{\mathrm{rk}}$ and $\widehat{v}$ be as in (3.14). The left multiplication action of M_{CS}, M_{CA}, and M_{TR} on $\mathbb{F}_2^4$, represents switching the first and second columns, adding the first and second columns, and taking the transpose, respectively. The action of G_{rk} on $\mathbb{F}_2^4$ yields the partition described in (3.35). Hence, it suffices to show that $\Theta_{Mx}(\tau) = \Theta_x(\tau)$.

The remaining argument is similar to the proof of Lemma 3.4.3. □

The results in the previous lemmas culminate in the following theorem.

Theorem 3.4.7. *Let $\tau \in \mathbb{H}$, q be as in (3.37), R be as in (3.47), and $\Theta_v(\tau)$ be as in (3.21). Define the $2n \times 2n$ symmetric positive definite block diagonal matrix*

$$Q = \begin{bmatrix} q & & \\ & \ddots & \\ & & q \end{bmatrix}. \tag{3.54}$$

Note that $Q > 0$ and $det(Q) = 1$. For $n \in \mathbb{Z}_{>0}$, let

$$\mathcal{D}_{\mathrm{cd}} = \{Z \in \mathfrak{H}_{2n} \mid Z = \tau Q\}. \tag{3.55}$$

For $n = 2$, let

$$\mathcal{D}_{\mathrm{rk}} = \{Z \in \mathfrak{H}_4 \mid Z = \tau R\}. \tag{3.56}$$

If $Z \in \mathcal{D}_{\mathrm{cd}}$ and $wt_{\mathrm{cd}}(v) = wt_{\mathrm{cd}}(u)$, then $\Theta_v(\tau) = \Theta_u(\tau)$. Likewise, if $Z \in \mathcal{D}_{\mathrm{rk}}$ and $wt_{\mathrm{rk}}(v) = wt_{\mathrm{rk}}(u)$, then $\Theta_v(\tau) = \Theta_u(\tau)$.

Proof. We proved the second statement in Lemma 3.4.6. To prove the first, let $n \in \mathbb{Z}_{>0}$. Let $Z \in \mathcal{D}_{\mathrm{cd}}$ and $wt_{\mathrm{cd}}(v) = wt_{\mathrm{cd}}(u)$. Then $Z = \tau Q$ for Q as in (3.54). Let $v \in \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ be a codeword and recall that $v_j \in \mathrm{Mat}_{2\times 1}(\mathbb{F}_2)$ is the j^{th} column of v. As in (3.15), define the column vector $\widetilde{v}_j \in \{0,1\}^2 \subseteq \mathbb{Z}^2$, such that $\rho(\widetilde{v}_j) = v_j$. Hence, $\rho^{-1}(v_j) = 2\mathbb{Z}^2 + \widetilde{v}_j$. As in (3.44), we have

$$\Theta_{v_j}(\tau) = \sum_{\lambda \in \mathbb{Z}^2} \exp\left(\pi i \tau q \left[\lambda + \frac{1}{2}\widetilde{v}_j\right]\right). \tag{3.57}$$

By (3.20), we have

$$\Theta_v(\tau) = \sum_{\lambda \in \mathbb{Z}^{2n}} \exp\left(\pi i \tau Q \left[\lambda + \frac{1}{2}\widetilde{v}\right]\right). \tag{3.58}$$

By (3.54), $\Theta_v(\tau)$ in (3.58) factors. By (3.57), (3.58), and Lemma 3.4.3, we have

$$\Theta_v(\tau) = \prod_{j=1}^{n} \Theta_{v_j}(\tau) = \Theta_0(\tau)^{n-wt_{\mathrm{cd}}(v)}\Theta_1(\tau)^{wt_{\mathrm{cd}}(v)}. \tag{3.59}$$

By (3.59), $\Theta_v(\tau) = \Theta_u(\tau)$. □

Remark 3.4.8. When $m = 2$, we found matrices Q, and R, which were invariant under the transpose conjugation action by matrices representing elementary column distance operations, and matrices representing elementary row and column operations, respectively. When $m > 2$, we failed to find such matrices. Hence, we were unable to generalize these results to higher dimensions.

Recall the definition of $\Theta_C(Z)$ in (3.24). If $Z \in \mathcal{D}_{\mathrm{cd}}$, we write

$$\Theta_C(\tau) = \sum_{\lambda \in \Lambda_C} \exp\left(\pi i \tau Q\left[\lambda\right]\right). \tag{3.60}$$

If $Z \in \mathcal{D}_{\mathrm{rk}}$, we write

$$\theta_C(\tau) = \sum_{\lambda \in \Lambda_C} \exp\left(\pi i \tau R\left[\lambda\right]\right). \tag{3.61}$$

Note that $\Theta_C(\tau)$ in (3.60) and $\theta_C(\tau)$ in (3.61) are theta functions which depend on a real lattice and a positive definite quadratic form. We now provide a formal definition of such theta functions.

Definition 3.4.9. Let $\Lambda \subseteq \mathbb{R}^n$ be an n-dimensional real lattice as in (3.5). Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a symmetric matrix such that $A > 0$. For $\tau \in \mathbb{H}$, define the *theta function attached to* Λ *and* A to be

$$\Theta_{\Lambda,A}(\tau) = \sum_{\lambda \in \Lambda} \exp\left(\pi i \tau A\left[\lambda\right]\right).$$

By (3.60), (3.61), and Definition 3.4.9,

$$\Theta_C(\tau) = \Theta_{\Lambda_C,Q}(\tau) \quad \text{and} \quad \theta_C(\tau) = \Theta_{\Lambda_C,R}(\tau). \tag{3.62}$$

We relate $\Theta_C(\tau)$ in (3.60) to $\mathrm{CDW}_C(\cdot,\cdot)$ in (3.1) and $\theta_C(\tau)$ in (3.61) to $\mathrm{RW}_C(\cdot,\cdot,\cdot)$ in (3.2). The results in this section culminate in the following theorem.

Theorem 3.4.10. *Let $Z \in \mathcal{D}_{\mathrm{cd}}$ be as in* (3.55), $\mathrm{CDW}_C(x_0, x_1)$ *be as in* (3.1), Λ_C *be as in* (3.23), $\Theta_C(\tau)$ *be as in* (3.60), *and* $\Theta_0(\tau)$ *and* $\Theta_1(\tau)$ *be as in Definition 3.4.1. Then,*

$$\Theta_C(\tau) = \mathrm{CDW}_C(\Theta_0(2\tau), \Theta_1(2\tau)). \tag{3.63}$$

Likewise, let $Z \in \mathcal{D}_{\mathrm{rk}}$ be as in (3.56), $\mathrm{RW}_C(x_0, x_1, x_2)$ *be as in* (3.2) *for $m = n = 2$, and $\theta_0(\tau)$, $\theta_1(\tau)$, and $\theta_2(\tau)$ be as in* (3.49). *Then ,*

$$\theta_C(\tau) = \mathrm{RW}_C\left(\theta_0(2\tau), \theta_1(2\tau), \theta_2(2\tau)\right). \tag{3.64}$$

Proof. We show (3.63) first. Let $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ and $Z \in \mathcal{D}_{\mathrm{cd}}$. By (3.25) and (3.59),

$$\begin{aligned}
\Theta_C(\tau) &= \sum_{v\in C} \Theta_v(2\tau) \\
&= \sum_{v\in C} \Theta_0(2\tau)^{n-wt_{\mathrm{cd}}(v)} \Theta_1(2\tau)^{wt_{\mathrm{cd}}(v)} \\
&= \sum_{r=0}^{n} a_r \Theta_0(2\tau)^{n-r} \Theta_1(2\tau)^{r} \\
&= \mathrm{CDW}_C(\Theta_0(2\tau), \Theta_1(2\tau)).
\end{aligned}$$

We now prove (3.64). Let $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$ and $Z \in \mathcal{D}_{\mathrm{rk}}$. By (3.25) and Theorem 3.4.7, we have

$$\begin{aligned}
\theta_C(\tau) &= \sum_{v\in C} \Theta_v(2\tau) \\
&= \sum_{r=0}^{2} a_r \theta_r(2\tau) \\
&= \mathrm{RW}_C(\theta_0(2\tau), \theta_1(2\tau), \theta_1(2\tau)).
\end{aligned}$$

□

3.5 Inversion Formulas

The theta function inversion formula plays a central role in the analytic proofs of MacWilliams Identities. We provide the pertinent inversion formulas for our results here. A proof of the following theorem can be found in ([28], pg. 355).

Theorem 3.5.1. *Let $\tau \in \mathbb{H}$, $(\cdot)$ be the standard dot product on $\mathbb{C}^n$, and $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a symmetric matrix such that $A > 0$. Then*

$$\sum_{\mu\in\mathbb{Z}^n} \exp\left(\pi i \tau A\left[\mu\right]\right) = \left(\sqrt{\frac{\tau}{i}}\right)^{-n} \frac{1}{\sqrt{\det(A)}} \sum_{\mu\in\mathbb{Z}^n} \exp\left(\pi i \left(-\frac{1}{\tau}\right) A^{-1}[\mu]\right),$$

where $\sqrt{\cdot}$ is the principal branch of the square root.

Using Theorem 3.5.1, we prove the following theorem.

Theorem 3.5.2. *Let $\tau \in \mathbb{H}$, $\Theta_{\Lambda,A}(\tau)$ be as in Definition 3.4.9,* $\mathrm{vol}(\cdot)$ *be as in* (3.6)*, and Λ^* be as in* (3.7)*. Then,*

$$\Theta_{\Lambda,A}\left(-\frac{1}{\tau}\right) = \left(\sqrt{\frac{\tau}{i}}\right)^{n} \frac{1}{\mathrm{vol}\left(\mathbb{R}^n/\Lambda\right)} \frac{1}{\sqrt{\det\left(A\right)}} \Theta_{\Lambda^*,A^{-1}}(\tau). \tag{3.65}$$

Proof. Since Λ is a real lattice of dimension n, it has a nonsingular generating matrix $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ such that $\Lambda = M\mathbb{Z}^n$. Note that [27],

$$\det\left(M\right) = \mathrm{vol}\left(\mathbb{R}^n/\Lambda\right). \tag{3.66}$$

We have,

$$\Theta_{\Lambda,A}\left(\tau\right) = \sum_{\lambda\in\Lambda} \exp\left(\pi i \tau A[\lambda]\right) = \sum_{\lambda\in M\mathbb{Z}^n} \exp\left(\pi i \tau A[\lambda]\right). \tag{3.67}$$

Let $\lambda = M\mu$ and note that λ runs through Λ as μ runs through $\mathbb{Z}^n$. By (3.67),

$$\Theta_{\Lambda,A}\left(\tau\right) = \sum_{\mu\in\mathbb{Z}^n} \exp\left(\pi i \tau \left({}^tMAM\right)[\mu]\right). \tag{3.68}$$

Let $S = \left({}^tMAM\right)$. Note that S is a symmetric matrix and $S > 0$. By (3.68) and Theorem 3.5.1 (letting $A = S$), we have

$$\Theta_{\Lambda,A}(\tau) = \left(\sqrt{\frac{\tau}{i}}\right)^{-n} \frac{1}{\sqrt{\det(S)}} \sum_{\mu\in\mathbb{Z}^n} \exp\left(\pi i \left(-\frac{1}{\tau}\right) S^{-1}[\mu]\right). \tag{3.69}$$

Note that $S^{-1} = \left(M^{-1}\right)\left(A^{-1}\right)\left({}^tM^{-1}\right)$. Hence,

$$S^{-1}[\mu] = A^{-1}\left[{}^tM^{-1}\mu\right]. \tag{3.70}$$

Note that $\left({}^tM^{-1}\right)$ is the generating matrix for Λ^*. Hence, $\eta = {}^tM^{-1}\mu$ runs through Λ^* as μ runs through $\mathbb{Z}^n$. We have,

$$\Theta_{\Lambda,A}(\tau) = \left(\sqrt{\frac{\tau}{i}}\right)^{-n} \frac{1}{\sqrt{\det(S)}} \sum_{\eta\in\Lambda^*} \exp\left(\pi i \left(-\frac{1}{\tau}\right) A^{-1}[\eta]\right). \tag{3.71}$$

By the multiplicative property of the determinant function and (3.66),

$$\frac{1}{\sqrt{\det(S)}} = \frac{1}{\sqrt{(\det(M))^2}} \frac{1}{\sqrt{\det(A)}} = \frac{1}{\mathrm{vol}\left(\mathbb{R}^n/\Lambda\right)} \frac{1}{\sqrt{\det\left(A\right)}}. \tag{3.72}$$

By (3.71), (3.72), and Definition 3.4.9,

$$\begin{aligned}\Theta_{\Lambda,A}\left(\tau\right) &= \left(\sqrt{\frac{\tau}{i}}\right)^{-n} \frac{1}{\mathrm{vol}\left(\mathbb{R}^n/\Lambda\right)} \frac{1}{\sqrt{\det\left(A\right)}} \sum_{\lambda\in\Lambda^*} \exp\left(\pi i \left(-\frac{1}{\tau}\right) A^{-1}[\lambda]\right) \\ &= \left(\sqrt{\frac{\tau}{i}}\right)^{-n} \frac{1}{\mathrm{vol}\left(\mathbb{R}^n/\Lambda\right)} \frac{1}{\sqrt{\det\left(A\right)}} \Theta_{\Lambda^*,A^{-1}}\left(-\frac{1}{\tau}\right). \end{aligned} \tag{3.73}$$

Sending $\tau \mapsto -\frac{1}{\tau}$ in (3.73) proves (3.65). □

We now show the theta functions in (3.62) are invariant under $Q \mapsto Q^{-1}$ and $R \mapsto R^{-1}$. To this end, we prove the following proposition about the quadratic forms Q and R.

Proposition 3.5.1. *Let R be as in* (3.47) *and Q be as in* (3.54) *and* (3.37)*. There exists a matrix $h \in \mathrm{GL}_4(\mathbb{Z})$ such that $h \equiv I_4 \bmod 2$ and $R^{-1} = {}^thRh$. Likewise, there exists a matrix $g \in \mathrm{GL}_{2n}(\mathbb{Z})$ such that $g \equiv I_{2n} \bmod 2$ and $Q^{-1} = {}^tgQg$.*

Proof. Define

$$h = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad g = \begin{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} & & \\ & \ddots & \\ & & \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix}. \tag{3.74}$$

Note that $h \in \mathrm{GL}_4(\mathbb{Z})$ and $h \equiv I_4 \bmod 2$. Note that $g \in \mathrm{GL}_{2n}(\mathbb{Z})$ and $g \equiv I_{2n} \bmod 2$. A quick

calculation shows that

$$R^{-1} = \frac{1}{3}\begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 4 & 1 & 2 \\ 2 & 1 & 4 & 2 \\ 1 & 2 & 2 & 4 \end{bmatrix} = {}^t hRh,$$

and

$$Q^{-1} = \begin{bmatrix} q^{-1} & & \\ & \ddots & \\ & & q^{-1} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{3}}\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} & & \\ & \ddots & \\ & & \frac{1}{\sqrt{3}}\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \end{bmatrix} = {}^t gQg. \qquad \square$$

The following lemma is crucial in the analytic proof of the column distance weight and rank weight MacWilliams Identities.

Lemma 3.5.3. *Let Λ_C be as in* (3.23)*, Q be as in* (3.54) *and* (3.37)*, R be as in* (3.47)*, and $\Theta_{\Lambda,A}(\tau)$ be as in Definition 3.4.9. Then, for all $n \in \mathbb{Z}_{>0}$,*

$$\Theta_{\Lambda_C, Q^{-1}}(\tau) = \Theta_{\Lambda_C, Q}(\tau),$$

and for $n = 2$,

$$\Theta_{\Lambda_C, R^{-1}}(\tau) = \Theta_{\Lambda_C, R}(\tau).$$

Proof. Let h be as in (3.74). By Definition 3.4.9 and Proposition 3.5.1,

$$\Theta_{\Lambda_C, R^{-1}}(\tau) = \sum_{\lambda \in \Lambda_C} \exp\left(\pi i \tau R^{-1}[\lambda]\right) = \sum_{\lambda \in \Lambda_C} \exp\left(\pi i \tau R[h\lambda]\right).$$

Let $\mu = h\lambda$. Since $h \in \mathrm{GL}_4(\mathbb{Z})$ and $h \equiv I_4 \bmod 2$, μ runs through Λ_C as λ does. (This is the crucial fact in this argument.) Hence,

$$\Theta_{\Lambda_C, R^{-1}}(\tau) = \sum_{\mu \in \Lambda_C} \exp\left(\pi i \tau R[\mu]\right) = \Theta_{\Lambda_C, R}(\tau).$$

Likewise, let g be as in (3.74). By Definition 3.4.9 and Proposition 3.5.1,

$$\Theta_{\Lambda_C,Q^{-1}}(\tau) = \sum_{\lambda\in\Lambda_C} \exp\left(\pi i\tau Q^{-1}\left[\lambda\right]\right) = \sum_{\lambda\in\Lambda_C} \exp\left(\pi i\tau Q\left[g\lambda\right]\right).$$

Let $\mu = g\lambda$. Since $g \in \mathrm{GL}_{2n}(\mathbb{Z})$ and $g \equiv I_{2n} \bmod 2$, μ runs through Λ_C as λ does. Hence,

$$\Theta_{\Lambda_C,Q^{-1}}(\tau) = \sum_{\mu\in\Lambda_C} \exp\left(\pi i\tau Q\left[\mu\right]\right) = \Theta_{\Lambda_C,Q}(\tau). \qquad \square$$

The following theorem gives the inversion formulas for $\Theta_C(\tau)$ in (3.60) and $\theta_C(\tau)$ in (3.61).

Theorem 3.5.4. *Let Λ_C be as in* (3.23)*, $C^\perp$ be as in* (3.4)*, $\Theta_C(\tau)$ be as in* (3.60)*, and $\theta_C(\tau)$ be as in* (3.61)*. Then,*

$$\Theta_C\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^n 2^{k-n}\Theta_{\Lambda_{C^\perp}}(\tau), \tag{3.75}$$

and

$$\theta_C\left(-\frac{1}{\tau}\right) = -\tau^2 2^{k-2}\theta_{\Lambda_{C^\perp}}(\tau). \tag{3.76}$$

Proof. Since the proofs for both statements are similar, we show (3.75). By (3.62), $\Theta_C(\tau) = \Theta_{\Lambda_C,Q}(\tau)$. Recall that $\det(Q) = 1$. By Theorem 3.5.2 (with $n = 2n$),

$$\Theta_C\left(-\frac{1}{\tau}\right) = \left(\sqrt{\frac{\tau}{i}}\right)^{2n} \frac{1}{\mathrm{vol}\left(\mathbb{R}^{2n}/\Lambda_C\right)}\Theta_{\Lambda_C^*,Q^{-1}}(\tau).$$

By Lemmas 3.2.1 and 3.5.3,

$$\Theta_C\left(-\frac{1}{\tau}\right) = \left(\frac{\tau}{i}\right)^n \frac{1}{\mathrm{vol}\left(\mathbb{R}^{2n}/\Lambda_C\right)}\Theta_{\Lambda_{C^\perp},Q}(\tau).$$

It suffices to show $\mathrm{vol}\left(\mathbb{R}^{2n}/\Lambda_C\right) = 2^{n-k}$. Let $\left|\mathbb{Z}^{2n} : \rho^{-1}\left(\widehat{C}\right)\right|$ denote the index of $\rho^{-1}\left(\widehat{C}\right)$ in $\mathbb{Z}^{2n}$. By (3.23) and ([27], pg. 2),

$$\mathrm{vol}\left(\mathbb{R}^{2n}/\Lambda_C\right) = \left(\frac{1}{\sqrt{2}}\right)^{2n} \mathrm{vol}\left(\mathbb{R}^{2n}/\rho^{-1}\left(\widehat{C}\right)\right) \tag{3.77}$$

and

$$\mathrm{vol}\left(\mathbb{R}^{2n}/\rho^{-1}\left(\widehat{C}\right)\right) = \mathrm{vol}\left(\mathbb{R}^{2n}/\mathbb{Z}^{2n}\right)\left|\mathbb{Z}^{2n} : \rho^{-1}\left(\widehat{C}\right)\right|. \tag{3.78}$$

Note that $\mathrm{vol}\left(\mathbb{R}^{2n}/\mathbb{Z}^{2n}\right) = 1$. Since ρ is a surjective map, we have

$$\left|\mathbb{Z}^{2n}/\rho^{-1}\left(\widehat{C}\right)\right| = \left|\mathbb{F}_2^{2n}/\widehat{C}\right| = 2^{2n-k}. \tag{3.79}$$

By (3.77), (3.78), and (3.79), we have

$$\text{vol}\left(\mathbb{R}^{2n}/\Lambda_C\right) = \left(\frac{1}{\sqrt{2}}\right)^{2n} 2^{2n-k} = 2^{n-k}. \qquad \square$$

Using Theorems 3.5.4 and 3.4.10, we show the inversion formulas for $\Theta_0(\tau)$, $\Theta_1(\tau)$, $\theta_0(\tau)$, $\theta_1(\tau)$, and $\theta_2(\tau)$.

Theorem 3.5.5. *Let $\Theta_0(\tau)$ and $\Theta_1(\tau)$ be as in Definition 3.4.1. Let $\theta_0(\tau)$, $\theta_1(\tau)$, and $\theta_2(\tau)$ be as in* (3.49)*. Then,*

$$\begin{bmatrix} \Theta_0(-\frac{2}{\tau}) \\ \Theta_1(-\frac{2}{\tau}) \end{bmatrix} = \frac{\tau}{2i} \begin{bmatrix} 1 & 3 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \Theta_0(2\tau) \\ \Theta_1(2\tau) \end{bmatrix}, \tag{3.80}$$

and

$$\begin{bmatrix} \theta_0(-\frac{2}{\tau}) \\ \theta_1(-\frac{2}{\tau}) \\ \theta_2(-\frac{2}{\tau}) \end{bmatrix} = -\frac{\tau^2}{4} \begin{bmatrix} 1 & 9 & 6 \\ 1 & 1 & -2 \\ 1 & -3 & 2 \end{bmatrix} \begin{bmatrix} \theta_0(2\tau) \\ \theta_1(2\tau) \\ \theta_2(2\tau) \end{bmatrix}. \tag{3.81}$$

Proof. We break the argument up into 2 parts.

Part 1: We prove (3.80). Let $C = \left\{\vec{0}\right\} \subseteq \text{Mat}_{2\times 1}(\mathbb{F}_2)$ be the trivial code. Then $C^\perp = \text{Mat}_{2\times 1}(\mathbb{F}_2)$. Note that there exists 1 codeword of column distance 0 and 3 codewords of column distance 1 in $\text{Mat}_{2\times 1}(\mathbb{F}_2)$. By Theorem 3.4.10,

$$\Theta_C(\tau) = \Theta_0(2\tau) \quad \text{and} \quad \Theta_{C^\perp}(\tau) = \Theta_0(2\tau) + 3\Theta_1(2\tau). \tag{3.82}$$

By (3.82) and Theorem 3.5.4 (with $n = 1$ and $k = 0$),

$$\Theta_0\left(-\frac{2}{\tau}\right) = \frac{\tau}{2i}\left(\Theta_0(2\tau) + 3\Theta_1(2\tau)\right). \tag{3.83}$$

Replace τ with $-\frac{1}{\tau}$ in (3.83) to see

$$\Theta_0(2\tau) = -\frac{1}{2i\tau}\left(\Theta_0\left(-\frac{2}{\tau}\right) + 3\Theta_1\left(-\frac{2}{\tau}\right)\right). \tag{3.84}$$

We solve for $\Theta_1\left(-\frac{2}{\tau}\right)$. Substituting (3.83) for $\Theta_0\left(-\frac{2}{\tau}\right)$ on the right hand side of (3.84) gives,

$$\Theta_0(2\tau) = \frac{i}{2\tau}\left(\frac{\tau}{2i}\left(\Theta_0(2\tau) + 3\Theta_1(2\tau)\right) + 3\Theta_1\left(-\frac{2}{\tau}\right)\right). \tag{3.85}$$

Rearranging terms in (3.85) yields

$$\Theta_1\left(-\frac{2}{\tau}\right) = \frac{\tau}{2i}\left(\Theta_0(2\tau) - \Theta_1(2\tau)\right). \tag{3.86}$$

The statement in (3.80) follows from (3.83) and (3.86).

Part 2: We prove (3.81). Let $C = \{\mathbf{0}_2\} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$ be the trivial code. Then $C^\perp = \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$. Note that there exists 1 codeword of rank 0, 9 codewords of rank 1, and 6 codewords of rank 2 in $\mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$. By Theorem 3.4.10,

$$\theta_C(\tau) = \theta_0(2\tau) \quad \text{and} \quad \theta_{C^\perp}(\tau) = \theta_0(2\tau) + 9\theta_1(2\tau) + 6\theta_2(2\tau).$$

By Theorem 3.5.4 (with $k = 0$),

$$\theta_0\left(-\frac{2}{\tau}\right) = -\frac{\tau^2}{4}\left(\theta_0(2\tau) + 9\theta_1(2\tau) + 6\theta_2(2\tau)\right). \tag{3.87}$$

Replace τ with $-\frac{1}{\tau}$ in (3.87) to see

$$\theta_0(2\tau) = -\frac{1}{4\tau^2}\left(\theta_0\left(-\frac{2}{\tau}\right) + 9\theta_1\left(-\frac{2}{\tau}\right) + 6\theta_2\left(-\frac{2}{\tau}\right)\right). \tag{3.88}$$

Substituting (3.87) for $\theta_0\left(-\frac{2}{\tau}\right)$ on the right hand side of (3.88) gives,

$$\begin{aligned}\theta_0(2\tau) = -\frac{1}{4\tau^2}\Bigg(&\left(-\frac{\tau^2}{4}\left(\theta_0(2\tau) + 9\theta_1(2\tau) + 6\theta_2(2\tau)\right)\right) \\ &+ 9\theta_1\left(-\frac{2}{\tau}\right) + 6\theta_2\left(-\frac{2}{\tau}\right)\Bigg).\end{aligned} \tag{3.89}$$

Rearranging terms in (3.89) yields

$$9\theta_1\left(-\frac{2}{\tau}\right) + 6\theta_2\left(-\frac{2}{\tau}\right) = -\frac{\tau^2}{4}\left(15\theta_0(2\tau) - 9\theta_1(2\tau) - 6\theta_2(2\tau)\right). \tag{3.90}$$

Now, let $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$ be the 2 dimensional code:

$$C = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Then $C^{\perp}$ is the 2 dimensional code:

$$C^{\perp} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

By Theorem 3.4.10,

$$\theta_C(\tau) = \theta_{C^{\perp}}(\tau) = \theta_0(2\tau) + 2\theta_1(2\tau) + \theta_2(2\tau).$$

By Theorem 3.5.4 (with $k = 2$),

$$\theta_0\left(-\frac{2}{\tau}\right) + 2\theta_1\left(-\frac{2}{\tau}\right) + \theta_2\left(-\frac{2}{\tau}\right) = -\tau^2\left(\theta_0(2\tau) + 2\theta_1(2\tau) + \theta_2(2\tau)\right). \tag{3.91}$$

Replace τ with $-\frac{1}{\tau}$ in (3.91) to see

$$\theta_0(2\tau) + 2\theta_1(2\tau) + \theta_2(2\tau) = -\frac{1}{\tau^2}\left(\theta_0\left(-\frac{2}{\tau}\right) + 2\theta_1\left(-\frac{2}{\tau}\right) + \theta_2\left(-\frac{2}{\tau}\right)\right). \tag{3.92}$$

As in (3.89), substituting (3.87) for $\theta_0\left(-\frac{2}{\tau}\right)$ on the right hand side of (3.92) and rearranging terms gives

$$2\theta_1\left(-\frac{2}{\tau}\right) + \theta_2\left(-\frac{2}{\tau}\right) = -\frac{\tau^2}{4}\left(3\theta_0(2\tau) - \theta_1(2\tau) - 2\theta_2(2\tau)\right). \tag{3.93}$$

Solving the system of equations (3.90) and (3.93), yields

$$\theta_1\left(-\frac{2}{\tau}\right) = -\frac{\tau^2}{4}\left(\theta_0(2\tau) + \theta_1(2\tau) - 2\theta_2(2\tau)\right) \tag{3.94}$$

$$\theta_2\left(-\frac{2}{\tau}\right) = -\frac{\tau^2}{4}\left(\theta_0(2\tau) - 3\theta_1(2\tau) + 2\theta_2(2\tau)\right). \tag{3.95}$$

The statement in (3.81) follows from (3.87), (3.94), and (3.95). □

3.6 MacWilliams Identities

We are now ready to provide analytic proofs of the column distance weight and rank weight MacWilliams Identities.

Theorem 3.6.1. Column Distance Weight MacWilliams Identity

Let $\mathrm{CDW}_C(x_0, x_1)$ *be as in Definition 3.1.1. Then*

$$\mathrm{CDW}_{C^{\perp}}(x_0, x_1) = \frac{1}{|C|}\mathrm{CDW}_C(x_0 + 3x_1, x_0 - x_1).$$

Proof. We follow the proof in the case of linear Hamming weight codes $C \subseteq \mathbb{F}_2^n$ described in ([27], Theorem 2.6) by evaluating

$$\mathrm{CDW}_C\left(\Theta_0\left(-\frac{2}{\tau}\right), \Theta_1\left(-\frac{2}{\tau}\right)\right),$$

in two different ways. First, by Theorem 3.4.10 and Theorem 3.5.4,

$$\begin{aligned}
&\mathrm{CDW}_C\left(\Theta_0\left(-\frac{2}{\tau}\right), \Theta_1\left(-\frac{2}{\tau}\right)\right) \\
&= \Theta_C\left(-\frac{1}{\tau}\right) \\
&= \left(\frac{\tau}{i}\right)^n 2^{k-n} \Theta_{\Lambda_{C^\perp}}(\tau) \\
&= \left(\frac{\tau}{i}\right)^n 2^{k-n} \mathrm{CDW}_{C^\perp}(\Theta_0(2\tau), \Theta_1(2\tau)). \qquad (3.96)
\end{aligned}$$

Second, recall that $\mathrm{CDW}_C(x_0, x_1)$ is a homogeneous polynomial of degree n. By Theorem 3.5.5,

$$\begin{aligned}
&\mathrm{CDW}_C\left(\Theta_0\left(-\frac{2}{\tau}\right), \Theta_1\left(-\frac{2}{\tau}\right)\right) \\
&= \mathrm{CDW}_C\left(\frac{\tau}{2i}\left(\Theta_0(2\tau) + 3\Theta_1(2\tau)\right), \frac{\tau}{2i}\left(\Theta_0(\tau) - \Theta_1(2\tau)\right)\right) \\
&= \left(\frac{\tau}{2i}\right)^n \mathrm{CDW}_C\left(\Theta_0(2\tau) + 3\Theta_1(2\tau), \Theta_0(2\tau) - \Theta_1(2\tau)\right) \qquad (3.97)
\end{aligned}$$

Sending $\tau \mapsto \frac{\tau}{2}$ in (3.96) and (3.97), setting (3.96) and (3.97) equal, canceling like terms, and dividing by $|C| = 2^k$ yields

$$\mathrm{CDW}_{C^\perp}(\Theta_0(\tau), \Theta_1(\tau)) = \frac{1}{|C|}\mathrm{CDW}_C(\Theta_0(\tau) + 3\Theta_1(\tau), \Theta_0(\tau) - \Theta_1(\tau)).$$

Define the homogeneous polynomial in 2 variables of degree n,

$$P(w, z) = \mathrm{CDW}_{C^\perp}(w, z) - \frac{1}{|C|}\mathrm{CDW}_C(w + 3z, w - z).$$

To conclude the proof, it suffices to show that $P(\Theta_0(\tau), \Theta_1(\tau)) = 0$ implies $P(w, z)$ is the zero polynomial. Since $P(w, z)$ is a homogeneous polynomial in 2 variables of degree n, it factors over $\mathbb{C}$ into a product of linear forms $L_j(w, z)$ for $1 \leq j \leq n$. Since the ring of analytic functions on the connected domain $\mathbb{H}$ is an integral domain, there exists an j such that $L_j\left(\Theta_0(\tau), \Theta_1(\tau)\right)$ vanishes. Hence, there exist $a, b \in \mathbb{C}$ such that

$$a\Theta_0(\tau) + b\Theta_1(\tau) = 0.$$

We will show that $\Theta_0(\tau)$ and $\Theta_1(\tau)$ are linearly independent, i.e. $a, b = 0$. Recall that q is a positive definite matrix. Therefore, the constant term in the Fourier expansion of $\Theta_0(\tau)$ is 1 and the constant term in the Fourier expansion of $\Theta_1(\tau)$ is zero since ${}^t\left(-\frac{1}{2}, 0\right) \notin \mathbb{Z}^2$. Hence, $\Theta_0(\tau)$ and $\Theta_1(\tau)$ are linearly independent if $\Theta_1(\tau)$ is not the zero function. We have just shown that $\Theta_0(\tau)$ is not the zero function, and by (3.80) we have

$$\Theta_0\left(-\frac{2}{\tau}\right) - \Theta_1\left(-\frac{2}{\tau}\right) = \frac{2\tau}{i}\Theta_1(2\tau). \tag{3.98}$$

So, $\Theta_1(\tau) \neq 0$, too.

This implies $\Theta_0(\tau)$ and $\Theta_1(\tau)$ are linearly independent, so P is identically zero. We conclude that,

$$\mathrm{CDW}_{C^\perp}(x_0, x_1) = \frac{1}{|C|}\mathrm{CDW}_C(x_0 + 3x_1, x_0 - x_1). \qquad \square$$

Theorem 3.6.2. Rank Weight MacWilliams Identity

Let $\mathrm{RW}_C(x_0, x_1, x_2)$ *be as in Definition 3.1.1. Then*

$$\begin{aligned}&\mathrm{RW}_{C^\perp}(x_0, x_1, x_2)\\ &= \frac{1}{|C|}\mathrm{RW}_C(x_0 + 9x_1 + 6x_2, x_0 + x_1 - 2x_2, x_0 - 3x_1 + 2x_2).\end{aligned}$$

Proof. We likewise evaluate

$$\mathrm{RW}_C\left(\Theta_0\left(-\frac{2}{\tau}\right), \Theta_1\left(-\frac{2}{\tau}\right), \Theta_2\left(-\frac{2}{\tau}\right)\right),$$

in two different ways. First, by Theorem 3.4.10 and Theorem 3.5.4,

$$\begin{aligned}&\mathrm{RW}_C\left(\theta_0\left(-\frac{2}{\tau}\right), \theta_1\left(-\frac{2}{\tau}\right), \theta_2\left(-\frac{2}{\tau}\right)\right)\\ &= \theta_C\left(-\frac{1}{\tau}\right)\\ &= -\tau^2 2^{k-2}\theta_{\Lambda_{C^\perp}}(\tau)\\ &= -\tau^2 2^{k-2}\mathrm{RW}_{C^\perp}(\theta_0(2\tau), \theta_1(2\tau), \theta_2(2\tau)).\end{aligned} \tag{3.99}$$

Second, recall that $\mathrm{RW}_C(x_0, x_1, x_2)$ is a linear homogeneous polynomial. By Theorem 3.5.5,

$$\begin{aligned}
&\mathrm{RW}_C\left(\theta_0\left(-\frac{2}{\tau}\right), \theta_1\left(-\frac{2}{\tau}\right), \theta_2\left(-\frac{2}{\tau}\right)\right) \\
&= -\frac{\tau^2}{4}\mathrm{RW}_C(\theta_0(2\tau) + 9\theta_1(2\tau) + 6\theta_2(2\tau), \\
&\qquad \theta_0(2\tau) + \theta_1(2\tau) - 2\theta_2(2\tau), \\
&\qquad \theta_0(2\tau) - 3\theta_1(2\tau) + 2\theta_2(2\tau)).
\end{aligned} \tag{3.100}$$

Sending $\tau \mapsto \frac{\tau}{2}$ in (3.99) and (3.100), setting equations (3.99) and (3.100) equal, canceling like terms, and dividing by $|C| = 2^k$ yields

$$\begin{aligned}
&\mathrm{RW}_{C^\perp}(\theta_0(2\tau), \theta_1(2\tau), \theta_2(2\tau)) \\
&= \frac{1}{|C|}\mathrm{RW}_C(\theta_0(2\tau) + 9\theta_1(2\tau) + 6\theta_2(2\tau), \\
&\qquad \theta_0(2\tau) + \theta_1(2\tau) - 2\theta_2(2\tau), \\
&\qquad \theta_0(2\tau) - 3\theta_1(2\tau) + 2\theta_2(2\tau)).
\end{aligned}$$

Define the linear homogeneous polynomial in 3 variables,

$$\begin{aligned}
P(w, y, z) &= \mathrm{RW}_{C^\perp}(w, y, z) \\
&\quad - \frac{1}{|C|}\mathrm{RW}_C(w + 9y + 6z, w + y - 2z, w - 3y + 2z).
\end{aligned}$$

To conclude the proof, it suffices to show that $P(\theta_0(\tau), \theta_1(\tau), \theta_2(\tau)) = 0$ implies $P(w, y, z)$ is the zero polynomial. Since $P(w, y, z)$ is a linear polynomial, there exist $a, b, c \in \mathbb{C}$ such that

$$a\theta_0(\tau) + b\theta_1(\tau) + c\theta_2(\tau) = 0.$$

Let $q = \exp(2\pi i\tau)$. The initial terms in the Fourier expansions of $\theta_0(\tau)$, $\theta_1(\tau)$, and $\theta_2(\tau)$ can be computed to be:

$$\begin{aligned}
\theta_0(\tau) &= 1 + 18q^{\frac{2}{3}} + 12q + 36q^{\frac{5}{3}} + \dots \\
\theta_1(\tau) &= 2q^{\frac{1}{6}} + 4q^{\frac{1}{2}} + 8q^{\frac{2}{3}} + 8q + \dots \\
\theta_2(\tau) &= 2q^{\frac{1}{4}} + 6q^{\frac{5}{12}} + 2q^{\frac{3}{4}} + 12q^{\frac{11}{12}} + \dots
\end{aligned}$$

It follows that $\theta_0(2\tau)$, $\theta_1(2\tau)$, and $\theta_2(2\tau)$ are linearly independent. Hence, P is identically zero. We conclude that,

$$\begin{aligned}&\mathrm{RW}_{C^\perp}(x_0, x_1, x_2)\\ &= \frac{1}{2^k}\mathrm{RW}_C(x_0 + 9x_1 + 6x_2, x_0 + x_1 - 2x_2, x_0 - 3x_1 + 2x_2).\end{aligned}$$ □

Remark 3.6.3. It should be noted that the rank weight MacWilliams Identity in Theorem 3.6.2 involves a different weight enumerator than the rank weight MacWilliams Identities proved in [32] and [31]. Let q be a power of a prime. In [32], Grant and Varanasi prove the rank weight MacWilliams Identity for matrix codes $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$, using a rank weight enumerator of the form

$$\sum_{r=0}^{\min(m,n)} a_r f_r,$$

where for a variable x,

$$f_r = \prod_{i=0}^{r-1} \frac{x - q^j}{q^{\max(m,n)} - q^j}.$$

In [31], Gadouleau and Yan prove the rank weight MacWilliams Identity for matrix codes $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$, using a rank weight enumerator of the form,

$$\mathrm{RW}_C(x_0, x_1) = \sum_{r=0}^{\min(m,n)} a_r x_0^{\min(m,n)-r} x_1^r.$$

[The result in [31] can be deduced from the result in [32].] We considered the linear rank weight enumerator in (3.2) because it seemed to be the most natural one to write in terms of theta functions.

3.7 $\mathbb{F}_2$-Column Distance Codes and $\mathbb{F}_4$-Hamming Codes

We now describe Gabidulin's method for considering a column distance matrix code $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ as a Hamming vector code $C \subseteq (\mathbb{F}_{q^m})^n$ [32]. Let $v \in (\mathbb{F}_{q^m})^n$ be a vector codeword. We define the *Hamming weight of* v to be

$$wt_{\mathrm{H}}(v) = |\{1 \le k \le n \mid v_k \neq 0\}|.$$

Let $v \in \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ and $v_1, \ldots, v_m \in \mathbb{F}_q^n$ denote the m rows of v. Fix a basis $\mathcal{B} = \{b_1, \ldots, b_m\}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and consider the map

$$\sigma_{\mathcal{B}} : \mathrm{Mat}_{m\times n}(\mathbb{F}_q) \to (\mathbb{F}_{q^m})^n$$
$$v \longmapsto \sum_{i=1}^{m} b_i v_i.$$

Note that $\sigma_{\mathcal{B}}(\cdot)$ is a bijection, $\sigma_{\mathcal{B}}(v)$ is a row vector of length n, and $wt_{\mathrm{cd}}(v) = wt_{\mathrm{H}}(\sigma_{\mathcal{B}}(v))$ [32]. If $C \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ is a $\mathbb{F}_q$-linear code then $\sigma_{\mathcal{B}}(C)$ is a $\mathbb{F}_q$-linear code but *may not be* a $\mathbb{F}_{q^m}$-linear code.

Let $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ be a linear column distance code. By the remarks above, $\sigma_{\mathcal{B}}(C) \subseteq \mathbb{F}_4^n$ is a $\mathbb{F}_2$-linear Hamming vector code. Sloane attaches complex lattices and theta functions to $\mathbb{F}_4$-linear Hamming vector codes [50]. He discusses the modular properties of these theta functions and states their inversion formulas, but does not provide an analytic proof of the Hamming weight MacWilliams Identity. Note in this paper, we have analytically proved the MacWilliams Identity for the larger class of $\mathbb{F}_2$-linear Hamming vector codes $C \subseteq \mathbb{F}_4^n$.

Chapter 4

$\mathbb{F}_p$-Vector Codes

Hirzebruch and van der Geer attached theta functions to self-orthogonal, $C \subseteq C^{\perp}$, linear codes $C \subseteq \mathbb{F}_p^n$, for p an odd prime, and related them to the Lee weight enumerator for the code ([27], Ch. 5). Choie and Jeong extended this result to Jacobi theta functions and provided an analytic proof of the Lee weight MacWilliams Identity for such C [13]. We provide an analytic proof of the Hamming weight MacWilliams Identity for linear codes $C \subseteq \mathbb{F}_p^n$, generalizing the seminal result for binary codes $C \subseteq \mathbb{F}_2^n$ [7].

There are two important differences between this result and the work of Hirzebruch, van der Geer, Choie, and Jeong for the Lee weight enumerator [27], [13]. The first is that we do not restrict our focus to self-orthogonal codes. (The previous authors considered self-orthogonal codes to ensure that the code lattices would be even and integral so that the theta functions attached to the code would be modular forms.) We are only interested in proving the MacWilliams Identity, and do not require this extra assumption. The second difference is that we take our theta functions to be defined over $\mathbb{Q}(\zeta_p, \zeta_{p-1})$ instead of $\mathbb{Q}(\zeta_p)$, so that they depend only on the Hamming weight of a codeword instead of on the Lee weight.

4.1 Linear $\mathbb{F}_p$-Codes and Real Lattices

Let p be a prime. A k-dimensional linear (column) vector code $C \subseteq \mathbb{F}_p^n$ is an $\mathbb{F}_p$-subspace of dimension k. Elements $v = {}^t(v_1, \ldots, v_n) \in C$ are called *codewords*. We define the *Hamming weight*

of v to be

$$wt_{\mathrm{H}}(v) = |\{1 \leq k \leq n \mid v_k \neq 0\}|\,.$$

Throughout we assume that $C \subseteq \mathbb{F}_p^n$ is a k-dimensional linear Hamming weight code and that $p \geq 5$ (for $p = 2$ or $p = 3$, the main results of this paper are known [7], [13].)

Definition 4.1.1. For variables x_0 and x_1, define the *Hamming weight enumerator of* C to be

$$\mathrm{HW}_C(x_0, x_1) = \sum_{r=0}^{n} a_r x_0^{n-r} x_1^r, \tag{4.1}$$

where for $0 \leq r \leq n$,

$$a_r = |\{v \in C \mid wt_{\mathrm{H}}(v) = r\}|\,.$$

Weight enumerators are generating functions that encode the *weight distribution* $a(C) = (a_r)_{r=0}^n$ of a code C. For $u, v \in \mathbb{F}_p^n$, we denote the standard dot product by

$$u \cdot v = \sum_{k=1}^{n} u_k v_k. \tag{4.2}$$

For $(\cdot)$ in (4.2), define the *dual code* of C to be

$$C^{\perp} = \left\{u \in \mathbb{F}_p^n \mid u \cdot v = 0,\ \ \forall v \in C\right\}.$$

Note that if C is a k-dimensional linear code, then $C^{\perp}$ is an $(n-k)$-dimensional linear code.

A *real lattice* (of dimension n) is a full rank discrete additive subgroup of $\mathbb{R}^n$. That is, Λ is a real lattice *iff*

$$\Lambda = \mathbb{Z}x_1 \oplus ... \oplus \mathbb{Z}x_n, \tag{4.3}$$

where $\{x_1, ..., x_n\}$ is a basis of column vectors for $\mathbb{R}^n$. Let $\det(\cdot)$ denote the determinant function. The *volume of* Λ is defined to be

$$\mathrm{vol}\,(\mathbb{R}^n/\Lambda) = \left|\det\left[x_1|\cdots|x_n\right]\right|.$$

If Λ is a real lattice of dimension n as in (4.3), we define the *dual lattice* to be

$$\Lambda^* = \{x \in \mathbb{R}^n \mid x \cdot y \in \mathbb{Z},\ \forall y \in \Lambda\}\,, \tag{4.4}$$

where $(\cdot)$ denotes the standard dot product on $\mathbb{R}^n$.

4.2 Number Fields, Ideals, and Theta Functions

Let a number field F be an abelian extension of degree d over $\mathbb{Q}$. Let $\mathfrak{O}_F$ be its ring of integers, $r_1(F)$ the number of its real embeddings, $r_2(F)$ the number of its pairs of complex conjugate embeddings, δ_F its different, and D_F its discriminant. Let $\sigma_1, \ldots, \sigma_{r_1(F)}$ be its $r_1(F)$ real embeddings and for $r_1(F)+1 \leq j \leq r_1(F)+r_2(F)$, $\left(\sigma_j, \sigma_{j+r_2(F)}\right)$ be its $r_2(F)$ pairs of complex conjugate embeddings. For $\gamma \in F$, we write $\sigma_j(\gamma) = \gamma^{(j)}$; i.e. if $\overline{(\cdot)}$ denotes complex conjugation then for $\gamma \in F$ and $r_1(F)+1 \leq j \leq r_1(F)+r_2(F)$,

$$\gamma^{(j+r_2(F))} = \overline{\gamma^{(j)}}. \tag{4.5}$$

The notion of attaching theta functions to a number field F goes back to Hecke. In [51], Stark provides a nice description of this process so we follow his setup here with some slight modifications. For $\gamma \in F$ we denote the trace of γ by

$$\mathrm{Tr}_{\mathbb{Q}}^{F}(\gamma) = \sum_{j=1}^{d} \gamma^{(j)}. \tag{4.6}$$

Note that since F is an abelian extension of $\mathbb{Q}$, there is a unique notion of complex conjugation for $\gamma \in F$ which we also denote by $\overline{(\cdot)}$. With this notation, consider the following definition.

Definition 4.2.1. Let $\tau \in \mathbb{H}$, the complex upper half plane. Let a number field F be an abelian extension of degree d over $\mathbb{Q}$ and $u, v \in F^n$ be column vectors for $n \in \mathbb{Z}_{>0}$. Let $\mathfrak{a}$ be a non-zero fractional ideal of F. Define the *theta function attached to F and $\mathfrak{a}$ with characteristic* $\begin{bmatrix} v \\ u \end{bmatrix}$ to be

$$\begin{aligned}
&\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v \\ u \end{bmatrix}\right) \\
&= \sum_{\lambda \in \mathfrak{a}^n} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^{F}\left((\lambda + v) \cdot \overline{(\lambda + v)}\right) - 2\pi i \mathrm{Tr}_{\mathbb{Q}}^{F}\left(u \cdot \lambda + \frac{u \cdot v}{2}\right)\right],
\end{aligned}$$

where $\exp(\cdot)$ is the exponential function, $(\cdot)$ is the standard dot product on F^n, and $\mathrm{Tr}_{\mathbb{Q}}^{F}(\cdot)$ is as in (4.6).

If $\tau = iy$ for $y \in \mathbb{R}_{>0}$, then this is the theta function considered in [51] (with $y_j = y$ for all $1 \leq j \leq d$). When the characteristic vector $v \in F^n$ is translated by a vector $z \in \mathfrak{a}^n$, the theta function is just multiplied by a root of unity. Further, if $u \in F^n$ is the zero vector, $\vec{0}$, then the theta function depends only on v mod $\mathfrak{a}$. To see this, consider

$$\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v+z \\ u \end{bmatrix}\right) = \sum_{\lambda \in \mathfrak{a}^n} \exp\Big[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^F\left([(\lambda+z)+v] \cdot \overline{[(\lambda+z)+v]}\right) - 2\pi i \mathrm{Tr}_{\mathbb{Q}}^F\left(u \cdot \lambda + \frac{u \cdot (v+z)}{2}\right)\Big].$$

Let $\mu = \lambda + z$ and note that μ runs through $\mathfrak{a}^n$ as λ does. Thus,

$$\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v+z \\ u \end{bmatrix}\right) = \sum_{\mu \in \mathfrak{a}^n} \exp\Big[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^F\left((\mu+v)\overline{(\mu+v)}\right) - 2\pi i \mathrm{Tr}_{\mathbb{Q}}^F\left(u \cdot (\mu - z) + \frac{u \cdot v}{2} + \frac{u \cdot z}{2}\right)\Big].$$

Rearranging terms in the second part of the exponent yields,

$$\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v+z \\ u \end{bmatrix}\right) = \zeta \Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v \\ u \end{bmatrix}\right), \tag{4.7}$$

where $\zeta = \exp\left[\pi i \mathrm{Tr}_{\mathbb{Q}}^F(u \cdot z)\right]$. It is clear that when $u = \vec{0}$, $\zeta = 1$.

Theorem 4.2.2. *The theta function in Definition 4.2.1 satisfies the following inversion formula:*

$$\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \mathrm{N}_{\mathbb{Q}}^F(\mathfrak{a})^{-n} \left|D_F\right|^{-\frac{n}{2}} \tau^{-\frac{nd}{2}} \Theta\left(F, -\frac{1}{\tau}, \mathfrak{a}^{-1}\delta_F^{-1}, \begin{bmatrix} u \\ -v \end{bmatrix}\right),$$

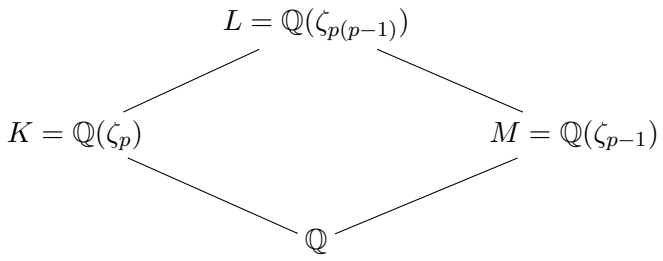
where D_F is the discriminant of F, δ_F^{-1} is the inverse different of F, $d = r_1(F) + 2r_2(F)$, and $\mathrm{N}_{\mathbb{Q}}^F(\mathfrak{a})$ is the absolute norm of the fractional ideal $\mathfrak{a}$.

Proof. By analytic continuation, it suffices to show the inversion formula in the case where $\tau = iy$ for $y \in \mathbb{R}_{>0}$. The case where $n = 1$ appears in [51]. For general n, note that since the trace and the dot product are linear, we have

$$\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v \\ u \end{bmatrix}\right) = \prod_{k=1}^{n} \Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v_k \\ u_k \end{bmatrix}\right). \tag{4.8}$$

Applying the result in [51] to each $\Theta\left(F, \tau, \mathfrak{a}, \begin{bmatrix} v_k \\ u_k \end{bmatrix}\right)$ in (4.8) completes the proof. □

Recall that p is a prime such that $p \geq 5$. For any $n > 1$, let ζ_n denote a primitive n^{th} root of unity. Consider the following field diagram.



For ease of notation let $m = p(p-1)$ so $L = \mathbb{Q}(\zeta_m)$. We are interested in studying the properties of the number field L. Consider the following lemma.

Lemma 4.2.3. *Let $\beta = (1 - \zeta_p)$. Let $\Phi_{p-1}(x)$ be the $(p-1)^{\text{st}}$ cyclotomic polynomial, $\Phi'_{p-1}(x)$ denote its derivative with respect to x, and $\alpha = \Phi'_{p-1}(\zeta_{p-1})$ [24]. Then,*

(1) $p\mathfrak{O}_L = (\beta\mathfrak{O}_L)^{p-1} = \left(\prod_{l=1}^{\phi(p-1)} Q_l\right)^{p-1}$, *for prime ideals Q_l in $\mathfrak{O}_L$ such that $\mathfrak{O}_L/Q_l \cong \mathbb{F}_p$, for all $1 \leq l \leq \phi(p-1)$.*

(2) $\delta_L^{-1} = \frac{1}{p\alpha}(\beta\mathfrak{O}_L)$.

(3) $D_L = (-1)^{\frac{\phi(m)}{2}} \left(p^{p-2}\right)^{\phi(p-1)} D_M^{p-1}$.

(4) $r_1(L) = 0$ *and* $r_2(L) = \frac{\phi(m)}{2}$.

Proof. Since $p \geq 5$, $L \neq \mathbb{Q}$ and (4) is trivial.

We show (1). Note that p splits completely in $\mathfrak{O}_N$ because $p \equiv 1 \bmod (p-1)$, and ramifies completely in $\mathfrak{O}_K$ because $D_K = (-1)^{\frac{p-1}{2}} p^{p-2}$ [39]. It follows that the ideal $p\mathfrak{O}_L$ has the prime factorization

$$p\mathfrak{O}_L = (\beta\mathfrak{O}_L)^{p-1} = \left(\prod_{l=1}^{\phi(p-1)} Q_l\right)^{p-1},$$

and that $\mathfrak{O}_L/Q_l \cong \mathbb{F}_p$ for all $1 \leq l \leq \phi(p-1)$, (see [39], [53]).

We now prove (2) and (3). Since the extension $K/\mathbb{Q}$ is totally and tamely ramified at the prime p and unramified at all other primes, $\delta_K = \beta^{p-2}\mathfrak{O}_K$ [39], [27]. Since $\mathfrak{O}_N = \mathbb{Z}[\zeta_{p-1}]$, we have that $\delta_M = \alpha\mathfrak{O}_N$, where $\alpha = \Phi'_{p-1}(\zeta_{p-1})$ ([34], Proposition 2). Since p is unramified in M, D_M and D_K are relatively prime. Further, K and M are linearly disjoint. Thus,

$$D_L = D_K^{\phi(p-1)} D_M^{p-1} = (-1)^{\frac{\phi(m)}{2}} \left(p^{p-2}\right)^{\phi(p-1)} D_M^{p-1},$$

and (3) is proved ([34], Proposition 17). Also,

$$\delta_L = \delta_K \delta_M \mathfrak{O}_L = \beta^{p-2}(\alpha\mathfrak{O}_L).$$

Therefore,

$$\begin{aligned}
\delta_L^{-1} &= \beta\beta^{-1}\delta_L^{-1} \\
&= \beta\beta^{-1}\left(\beta^{p-2}\right)^{-1}\left(\frac{1}{\alpha}\mathfrak{O}_L\right) \\
&= \beta\left(\beta^{p-1}\right)^{-1}\left(\frac{1}{\alpha}\mathfrak{O}_L\right) \\
&= \frac{1}{p\alpha}(\beta\mathfrak{O}_L), \qquad (4.9)
\end{aligned}$$

and (2) is shown. □

By the Chinese Remainder Theorem, there exists an isomorphism

$$\psi : \mathfrak{O}_L/\beta \longrightarrow \bigoplus_{l=1}^{\phi(p-1)} \mathfrak{O}_L/Q_l. \qquad (4.10)$$

By Lemma 4.2.3, $\mathfrak{O}_L/Q_l \cong \mathbb{F}_p$ for all $1 \leq l \leq \phi(p-1)$. We can extend the isomorphism $\psi(\cdot)$ to an isomorphism from $(\mathfrak{O}_L/\beta)^n$ onto $\bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n$ componentwise. Therefore,

$$(\mathfrak{O}_L/\beta)^n \cong \bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n. \qquad (4.11)$$

For $x = {}^t(x_1, \ldots, x_n) \in \mathfrak{O}_L^n$ consider the surjective $\mathfrak{O}_L$-module homomorphism

$$\begin{aligned}
\eta : \mathfrak{O}_L^n &\longrightarrow (\mathfrak{O}_L/\beta)^n \\
\eta(x) &= \begin{bmatrix} x_1 \bmod \beta \\ \vdots \\ x_n \bmod \beta \end{bmatrix}. \qquad (4.12)
\end{aligned}$$

With η from (4.12) and the extension of ψ from (4.11), define the map $\rho = \psi \circ \eta$ to be

$$\rho : \mathfrak{O}_L^n \longrightarrow \bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n$$

$$\rho(x) = \left(\vec{y}_1, \ldots, \vec{y}_{\phi(p-1)}\right), \tag{4.13}$$

where for $1 \leq l \leq \phi(p-1)$,

$$\vec{y}_l = \begin{bmatrix} x_1 \bmod Q_l \\ \vdots \\ x_n \bmod Q_l \end{bmatrix}.$$

We use the ρ map from (4.13) to attach theta functions to $\mathbb{F}_p$-codes.

4.3 Theta Functions Attached to $\mathbb{F}_p$-Hamming Codes

We start by embedding C into $\bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n$ and $\mathcal{P}\left(\bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n\right)$, where $\mathcal{P}(S)$ denotes the power set of S.

Definition 4.3.1. Define the two maps A and B to be

$$A : C \longrightarrow \bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n$$

$$v \longmapsto (v, \vec{0}, \ldots, \vec{0}),$$

and

$$B : C \longrightarrow \mathcal{P}\left(\bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n\right)$$

$$v \longmapsto \left\{ x = \left(\vec{x}_1, \ldots, \vec{x}_{\phi(p-1)}\right) \in \bigoplus_{l=1}^{\phi(p-1)} \mathbb{F}_p^n \mid \vec{x}_1 = v \right\}.$$

Note that the maps $A(\cdot)$ and $B(\cdot)$ are injective. For notational convenience, we write

$$C_A = A(C) \quad \text{and} \quad C_B = \bigcup_{v \in C} B(v). \tag{4.14}$$

Similarly, for $v \in C$, we write $v_A = A(v)$ and $v_B = B(v)$. We attach a theta function to both v_A and v_B for each $v \in C$. Note that if $x \in \rho^{-1}(v_A)$, then $y \in \rho^{-1}(v_A)$ *iff* $x \equiv y \bmod \beta\mathfrak{O}_L$. Also, if $x \in \rho^{-1}(v_B)$, then $y \in \rho^{-1}(v_B)$ *iff* $x \equiv y \bmod Q_1$. Hence, choosing $\widetilde{v}_A \in \rho^{-1}(v_A)$ and $\widetilde{v}_B \in \rho^{-1}(v_B)$ to be our coset representatives, we have $\rho^{-1}(v_A) = (\beta\mathfrak{O}_L)^n + \widetilde{v}_A$ and $\rho^{-1}(v_B) = Q_1^n + \widetilde{v}_B$. We define the *theta function attached to* v_A to be

$$\Theta_{v_A}(\tau) = \sum_{\lambda \in \rho^{-1}(v_A)} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda \cdot \overline{\lambda}}{p}\right)\right]. \tag{4.15}$$

Writing $\lambda = \mu + \widetilde{v}_A$ yields

$$\Theta_{v_A}(\tau) = \sum_{\mu \in (\beta\mathfrak{O}_L)^n} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{(\mu + \widetilde{v}_A) \cdot \overline{(\mu + \widetilde{v}_A)}}{p}\right)\right].$$

The theta function attached to v_B has a slightly less natural definition than $\Theta_{v_A}(\tau)$. This is due to the added complexity of working over the number field L instead of K as in [27]. Recall the definition of α from Lemma 4.2.3. We define the theta function attached to v_B to be

$$\widehat{\Theta}_{v_B}(\tau) = \sum_{\lambda \in \overline{\rho^{-1}(v_B)}} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\frac{1}{\alpha}\lambda \cdot \overline{\frac{1}{\alpha}\lambda}}{p}\right)\right]. \tag{4.16}$$

Writing $\lambda = \overline{\mu + \widetilde{v}_B}$ yields

$$\begin{aligned}\widehat{\Theta}_{v_B}(\tau) &= \sum_{\mu \in Q_1^n} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\frac{1}{\alpha}\overline{(\mu + \widetilde{v}_B)} \cdot \overline{\frac{1}{\alpha}}(\mu + \widetilde{v}_B)}{p}\right)\right] \\ &= \sum_{\mu \in Q_1^n} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\frac{1}{\alpha}(\mu + \widetilde{v}_B) \cdot \overline{\frac{1}{\alpha}(\mu + \widetilde{v}_B)}}{p}\right)\right].\end{aligned}$$

By Definition 4.2.1, it can be checked that

$$\Theta_{v_A}(\tau) = \Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix}\widetilde{v}_A \\ \\ 0\end{bmatrix}\right) \text{ and } \widehat{\Theta}_{v_B}(\tau) = \Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix}\frac{1}{\alpha}\widetilde{v}_B \\ \\ 0\end{bmatrix}\right). \tag{4.17}$$

By (4.7), both $\Theta_{v_A}(\tau)$ and $\widehat{\Theta}_{v_B}(\tau)$ are well defined because they are independent of the choice of characteristic vector $\widetilde{v}_A$ and $\frac{1}{\alpha}\widetilde{v}_B$. In order to understand them better, we define the following four theta functions (for n=1).

Definition 4.3.2. Let $\tau \in \mathbb{H}$. Fix a $w \in \mathfrak{O}_L$ such that $w \in Q_l$ for all $2 \leq l \leq \phi(p-1)$ but $w \notin Q_1$. Fix a $z \in \mathfrak{O}_L$ such that $z \notin Q_1$. Define

$$\Theta_0(\tau) = \Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix} 0 \\ 0 \end{bmatrix}\right), \quad \Theta_1(\tau) = \Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix} w \\ 0 \end{bmatrix}\right) \tag{4.18}$$

and

$$\widehat{\Theta}_0(\tau) = \Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix} 0 \\ 0 \end{bmatrix}\right), \quad \widehat{\Theta}_1(\tau) = \Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix} \frac{1}{\alpha}z \\ 0 \end{bmatrix}\right). \tag{4.19}$$

The reason we are working with theta functions defined over L instead of K is due to the following lemma.

Lemma 4.3.3. *The definitions of $\Theta_0(\tau), \Theta_1(\tau), \widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)$ in 4.3.2 are independent of the choice of w and z. In particular, if $x \in \prod_{l=2}^{\phi(p-1)} Q_l$ and $y \in \mathfrak{O}_L$, then*

$$\Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix} x \\ 0 \end{bmatrix}\right) = \begin{cases} \Theta_0(\tau), & x \in Q_1 \\ \Theta_1(\tau), & x \notin Q_1 \end{cases} \tag{4.20}$$

and

$$\Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix} \frac{1}{\alpha}y \\ 0 \end{bmatrix}\right) = \begin{cases} \widehat{\Theta}_0(\tau), & y \in Q_1 \\ \widehat{\Theta}_1(\tau), & y \notin Q_1 \end{cases}. \tag{4.21}$$

Proof. We begin by showing that

$$\Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix} x \\ 0 \end{bmatrix}\right) \quad \text{and} \quad \Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix} \frac{1}{\alpha}y \\ 0 \end{bmatrix}\right)$$

are invariant under the maps $x \mapsto \zeta_{p-1}x$ and $y \mapsto \zeta_{p-1}y$. Consider,

$$\begin{aligned} &\Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix} \zeta_{p-1}x \\ 0 \end{bmatrix}\right) \\ &= \sum_{\lambda \in \beta\mathfrak{O}_L} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{(\lambda + \zeta_{p-1}x)\overline{(\lambda + \zeta_{p-1}x)}}{p}\right)\right] \\ &= \sum_{\lambda \in \beta\mathfrak{O}_L} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\zeta_{p-1}(\zeta_{p-1}^{-1}\lambda + x)\overline{\zeta_{p-1}(\zeta_{p-1}^{-1}\lambda + x)}}{p}\right)\right]. \end{aligned}$$

Since ζ_{p-1} is a root of unity, $\zeta_{p-1}\overline{\zeta_{p-1}} = 1$ and $\mu = \zeta_{p-1}^{-1}\lambda$ runs through $\beta\mathfrak{O}_L$ as λ does. Therefore,

$$\Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix}\zeta_{p-1}x\\ 0\end{bmatrix}\right) = \Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix}x\\ 0\end{bmatrix}\right).$$

If $x \in Q_1$, it follows from Lemma 4.2.3 that $x \in \beta\mathfrak{O}_L$. Hence, by (4.7), if $x \in Q_1$, then $\Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix}x\\ 0\end{bmatrix}\right) = \Theta_0(\tau)$.

The mod Q_1 reduction map, $\mathfrak{O}_L \to \mathfrak{O}_L/Q_1$, maps $\langle\zeta_{p-1}\rangle$ isomorphically onto $(\mathfrak{O}_L/Q_1)^\times$. Therefore, if $x \notin Q_1$, there exists a $s \in \mathbb{Z}_{>0}$ such that $w = \zeta_{p-1}^s x$ and $\Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix}x\\ 0\end{bmatrix}\right) = \Theta_1(\tau)$.

The proof for $\Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix}\frac{1}{\alpha}y\\ 0\end{bmatrix}\right)$ is similar. Without loss of generality we can take $z = 1$ and will do so for the rest of the paper. □

With Lemma 4.3.3, we prove the following theorem.

Theorem 4.3.4. *Let $u, v \in \mathbb{F}_p^n$ and $\Theta_0(\tau), \Theta_1(\tau), \widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)$ be as in Definition 4.3.2. If $wt_{\mathrm{H}}(v) = r$, then*

$$\Theta_{v_A}(\tau) = \Theta_0(\tau)^{n-r}\Theta_1(\tau)^r \quad \text{and} \quad \widehat{\Theta}_{v_B}(\tau) = \widehat{\Theta}_0(\tau)^{n-r}\widehat{\Theta}_1(\tau)^r.$$

In particular, if $wt_{\mathrm{H}}(v) = wt_{\mathrm{H}}(u)$, then

$$\Theta_{v_A}(\tau) = \Theta_{u_A}(\tau) \quad \text{and} \quad \widehat{\Theta}_{v_B}(\tau) = \widehat{\Theta}_{u_B}(\tau).$$

Proof. Let $\widetilde{v}_A = {}^t(x_1, \ldots, x_n)$ and $\widetilde{v}_B = {}^t(y_1, \ldots, y_n)$. By (4.8),

$$\Theta_{v_A}(\tau) = \prod_{k=1}^{n} \Theta\left(L, \frac{\tau}{p}, \beta\mathfrak{O}_L, \begin{bmatrix}x_k\\ 0\end{bmatrix}\right) \text{ and } \widehat{\Theta}_{v_B}(\tau) = \prod_{k=1}^{n} \Theta\left(L, \frac{\tau}{p}, \frac{1}{\alpha}Q_1, \begin{bmatrix}\frac{1}{\alpha}y_k\\ 0\end{bmatrix}\right).$$

The theorem now follows from Lemma 4.3.3. □

4.4 Lattices Attached to $\mathbb{F}_p$-Codes and Theta Functions

Let $\Gamma \subseteq L^n$.We call Γ an *L-lattice iff* Γ is a free $\mathbb{Z}$-module of dimension $n\phi(m) = n[L : \mathbb{Q}]$. (Note that $\mathfrak{O}_L^n$ is an L-lattice.) We define two subsets of $\mathfrak{O}_L^n$ which depend on the two embeddings of C from Definition 4.3.1.

Definition 4.4.1. $\mathcal{A}_C = \rho^{-1}(C_A)$ and $\mathcal{B}_C = \overline{\rho^{-1}(C_B)}$.

Since $\mathcal{A}_C$ is an abelian group such that $\beta^n \subseteq \mathcal{A}_C \subseteq \mathfrak{O}_L^n$, $\mathcal{A}_C$ is a free $\mathbb{Z}$-module of dimension $n\phi(m)$. The same goes for $\mathcal{B}_C$. Hence, $\mathcal{A}_C$ and $\mathcal{B}_C$ are L-lattices. We now define theta functions attached to $\mathcal{A}_C$ and $\mathcal{B}_C$.

Definition 4.4.2. For $\tau \in \mathbb{H}$, define

$$\Theta_{\mathcal{A}_C}(\tau) = \sum_{\lambda \in \mathcal{A}_C} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda \cdot \overline{\lambda}}{p}\right)\right]$$

and

$$\widehat{\Theta}_{\mathcal{B}_C}(\tau) = \sum_{\lambda \in \mathcal{B}_C} \exp\left[\pi i \tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\frac{1}{\alpha}\lambda \cdot \overline{\frac{1}{\alpha}\lambda}}{p}\right)\right].$$

It follows immediately from Definition 4.4.1, Definition 4.4.2, (4.15), and (4.16), that

$$\Theta_{\mathcal{A}_C}(\tau) = \sum_{v \in C} \Theta_{v_A}(\tau) \quad \text{and} \quad \widehat{\Theta}_{\mathcal{B}_C}(\tau) = \sum_{v \in C} \widehat{\Theta}_{v_B}(\tau). \tag{4.22}$$

We now relate these theta functions to the Hamming weight enumerator.

Proposition 4.4.1. *With* $\mathrm{HW}_C(x_0, x_1)$ *as in Definition 4.1.1,*

$$\Theta_{\mathcal{A}_C}(\tau) = \mathrm{HW}_C\left(\Theta_0(\tau), \Theta_1(\tau)\right),$$
$$\widehat{\Theta}_{\mathcal{B}_C}(\tau) = \mathrm{HW}_C\left(\widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)\right).$$

Proof. Since the proof is similar for both statements, we show the second equality. By (4.22),

Theorem 4.3.4, and Definition 4.1.1,

$$\begin{aligned}\widehat{\Theta}_{\mathcal{B}_C}(\tau) &= \sum_{v\in C} \widehat{\Theta}_{v_B}(\tau) \\ &= \sum_{v\in C} \widehat{\Theta}_0(\tau)^{n-wt_{\mathrm{H}}(v)}\widehat{\Theta}_1(\tau)^{wt_{\mathrm{H}}(v)} \\ &= \sum_{r=0}^{n} a_r \widehat{\Theta}_0(\tau)^{n-r}\widehat{\Theta}_1(\tau)^{r} \\ &= \mathrm{HW}_C\left(\widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)\right). \end{aligned}$$ □

Let $I(\cdot)$ be the embedding from L to $\mathbb{R}^{\phi(m)}$ such that for $x \in L$,

$$I(x) = \sqrt{\frac{2}{p}}\left[t\left(\mathrm{Re}\left(x^{(1)}\right), \mathrm{Im}\left(x^{(1)}\right), \ldots, \mathrm{Re}\left(x^{(r_2(L))}\right), \mathrm{Im}\left(x^{(r_2(L))}\right)\right)\right]. \tag{4.23}$$

We can extend the map $I(\cdot)$ to a map from L^n into $\mathbb{R}^{n\phi(m)}$ componentwise. Let $\Gamma \subseteq L^n$ be an L-lattice. If $\left\{\gamma_1, \ldots, \gamma_{n\phi(m)}\right\}$ is an integral basis for Γ, note that $\left\{I(\gamma_1), \ldots, I(\gamma_{n\phi(m)})\right\}$ is an integral basis for $I(\Gamma) \subseteq \mathbb{R}^{n\phi(m)}$. Hence, $I(\Gamma)$ is an $\mathbb{R}$-lattice as in (4.3). Up to the scalar $\sqrt{\frac{2}{p}}$, $I(\cdot)$ is a standard way to map free $\mathbb{Z}$-submodules of L to real lattices [39], [18]. The reason for the scalar is the following:

Proposition 4.4.2. *Let $\Gamma \subseteq \mathfrak{O}_L^n$ be an L-lattice and define the set*

$$\Gamma' = \left\{y \in L^n \mid \mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{y\cdot\overline{x}}{p}\right) \in \mathbb{Z}, \ \ \forall x \in \Gamma\right\}. \tag{4.24}$$

Then $I\left(\Gamma'\right) = I(\Gamma)^*$, where * denotes the dual of a real lattice as in (4.4).

Proof. We break the proof into 2 parts.

Part 1: $I\left(\Gamma'\right) \subseteq I(\Gamma)^*$.

We first show that for $x, y \in L^n$, $I(x)\cdot I(y) = \mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{x\cdot\overline{y}}{p}\right)$. A quick calculation shows

$$I(x)\cdot I(y) = \frac{2}{p}\sum_{k=1}^{n}\sum_{j=1}^{r_2(L)} \mathrm{Re}\left(x_k^{(j)}\right)\mathrm{Re}\left(y_k^{(j)}\right) + \mathrm{Im}\left(x_k^{(j)}\right)\mathrm{Im}\left(y_k^{(j)}\right). \tag{4.25}$$

By Lemma 4.2.3, $r_1(L) = 0$. For $\gamma \in L$, $\gamma^{(j+r_2(L))} = \overline{\gamma^{(j)}}$ for all $1 \le j \le r_2(L)$ as in (4.5). Therefore, for all $1 \le k \le n$,

$$\mathrm{Re}\left(x_k^{(j)}\right) = \mathrm{Re}\left(x_k^{(j+r_2(L))}\right) \quad \text{and} \quad \mathrm{Im}\left(x_k^{(j)}\right) = -\mathrm{Im}\left(x_k^{(j+r_2(L))}\right).$$

The same is true for all y_k. Hence,

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{x\cdot\overline{y}}{p}\right) &= \frac{1}{p}\sum_{k=1}^{n}\sum_{j=1}^{\phi(m)}\mathrm{Re}\left(x_k^{(j)}\right)\mathrm{Re}\left(y_k^{(j)}\right)+\mathrm{Im}\left(x_k^{(j)}\right)\mathrm{Im}\left(y_k^{(j)}\right)\\ &= \frac{2}{p}\sum_{k=1}^{n}\sum_{j=1}^{r_2(L)}\mathrm{Re}\left(x_k^{(j)}\right)\mathrm{Re}\left(y_k^{(j)}\right)+\mathrm{Im}\left(x_k^{(j)}\right)\mathrm{Im}\left(y_k^{(j)}\right). \qquad (4.26)\end{aligned}$$

By (4.25) and (4.26), we have

$$I(x)\cdot I(y) = \mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{x\cdot\overline{y}}{p}\right). \qquad (4.27)$$

To establish Part 1, take any $z\in\Gamma'$. For all $x\in\Gamma$, $\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{z\cdot\overline{x}}{p}\right)\in\mathbb{Z}$. By (4.27), $I(z)\cdot I(x)\in\mathbb{Z}$ for all $I(x)\in I(\Gamma)$. Hence, $I\left(\Gamma'\right)\subseteq I(\Gamma)^*$ by (4.4).

Part 2: $I(\Gamma)^*\subseteq I\left(\Gamma'\right)$

By (4.27), since $I(\cdot)$ is injective, it suffices to show that $I(\Gamma)^*\subseteq I(L^n)$. Let $c=|\mathfrak{O}_L^n/\Gamma|$ be the index of Γ in $\mathfrak{O}_L^n$. Since $\Gamma\subseteq\mathfrak{O}_L^n$ is an L-lattice, c is finite. Hence,

$$c\mathfrak{O}_L^n\subseteq\Gamma\subseteq\mathfrak{O}_L^n.$$

Since $I(\cdot)$ in (4.23) is a group homomorphism,

$$cI\left(\mathfrak{O}_L^n\right)\subseteq I(\Gamma)\subseteq I(\mathfrak{O}_L^n). \qquad (4.28)$$

Taking duals, we have

$$\frac{1}{c}I(\mathfrak{O}_L^n)^*\supseteq I(\Gamma)^*\supseteq I(\mathfrak{O}_L^n)^*. \qquad (4.29)$$

If $I(\mathfrak{O}_L^n)^*\subseteq I(L^n)$, then $I(\Gamma)^*\subseteq\frac{1}{c}I(\mathfrak{O}_L^n)^*\subseteq I(L^n)$ by (4.29), and we are done. To prove $I(\mathfrak{O}_L^n)^*\subseteq I(L^n)$, we show $I(\mathfrak{O}_L^n)^* = pI\left(\left(\delta_L^{-1}\right)^n\right)$. The definition of the inverse different of L is

$$\begin{aligned}\delta_L^{-1} &= \left\{y\in L\mid \mathrm{Tr}_{\mathbb{Q}}^{L}(yx)\in\mathbb{Z},\ \ \forall x\in\mathfrak{O}_L\right\}\\ &= \left\{y\in L\mid \mathrm{Tr}_{\mathbb{Q}}^{L}(y\overline{x})\in\mathbb{Z},\ \ \forall x\in\mathfrak{O}_L\right\}. \qquad (4.30)\end{aligned}$$

By (4.24),

$$\left(\mathfrak{O}_L^n\right)' = \left\{y\in L^n\mid \mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{y\cdot\overline{x}}{p}\right)\in\mathbb{Z},\ \ \forall x\in\mathfrak{O}_L^n\right\}.$$

Hence,

$$\frac{1}{p}(\mathfrak{O}_L^n)' = \left\{ y \in L^n \mid \mathrm{Tr}_{\mathbb{Q}}^L (y \cdot \overline{x}) \in \mathbb{Z}, \ \ \forall x \in \mathfrak{O}_L^n \right\}. \tag{4.31}$$

By (4.30) and (4.31),

$$\left(\delta_L^{-1}\right)^n \subseteq \frac{1}{p}(\mathfrak{O}_L^n)'. \tag{4.32}$$

As in (4.28), by (4.32) and Part 1, we have

$$I\left(\left(\delta_L^{-1}\right)^n\right) \subseteq \frac{1}{p} I\left((\mathfrak{O}_L^n)'\right) \subseteq \frac{1}{p} I\left(\mathfrak{O}_L^n\right)^*.$$

To prove $I(\mathfrak{O}_L^n)^* = pI\left(\left(\delta_L^{-1}\right)^n\right)$, it suffices to show

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\left(\delta_L^{-1}\right)^n\right)\right) = \mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/\frac{1}{p} I\left(\mathfrak{O}_L^n\right)^*\right). \tag{4.33}$$

We first calculate $\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/\frac{1}{p} I\left(\mathfrak{O}_L^n\right)^*\right)$. Note that

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/\frac{1}{p} I\left(\mathfrak{O}_L^n\right)^*\right) = p^{-n\phi(m)} \mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathfrak{O}_L^n\right)^*\right). \tag{4.34}$$

By ([27], pg. 3),

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathfrak{O}_L^n\right)^*\right) = \frac{1}{\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathfrak{O}_L^n\right)\right)}. \tag{4.35}$$

Adjusting for our rescaling of the standard embedding by a factor of $\sqrt{\frac{2}{p}}$ in (4.23), by ([39], Thm 36)

$$\mathrm{vol}\left(\mathbb{R}^{\phi(m)}/I(\mathfrak{O}_L)\right) = p^{-\frac{\phi(m)}{2}} \sqrt{|D_L|}.$$

Hence,

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathfrak{O}_L^n)\right) = p^{-\frac{n\phi(m)}{2}} |D_L|^{\frac{n}{2}}. \tag{4.36}$$

By (4.34), (4.35), and (4.36),

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/\frac{1}{p} I\left(\mathfrak{O}_L^n\right)^*\right) = p^{-\frac{n\phi(m)}{2}} |D_L|^{-\frac{n}{2}}. \tag{4.37}$$

Next, we calculate

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\left(\delta_L^{-1}\right)^n\right)\right).$$

For the absolute norm, $\mathrm{N}_{\mathbb{Q}}^{L}(\cdot)$, note that $\mathrm{N}_{\mathbb{Q}}^{L}\left(\delta_L^{-1}\right) = |D_L|^{-1}$ [34]. By a corollary to ([39], Thm. 36), we have

$$\mathrm{vol}\left(\mathbb{R}^{\phi(m)}/I\left(\delta_L^{-1}\right)\right) = \frac{1}{|D_L|}p^{-\frac{\phi(m)}{2}}\sqrt{|D_L|} = p^{-\frac{\phi(m)}{2}}|D_L|^{-\frac{1}{2}}.$$

Hence,

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\left(\delta_L^{-1}\right)^n\right)\right) = p^{-\frac{n\phi(m)}{2}}|D_L|^{-\frac{n}{2}}. \tag{4.38}$$

(4.37) and (4.38) imply (4.33). Combining Parts 1 and 2 gives the result $I\left(\Gamma^{'}\right) = I(\Gamma)^{*}$. □

The following theorem relates $\mathcal{A}_C^{'}$ and $\mathcal{B}_{C^{\perp}}$, similar to ([27], Lemma 5.5).

Theorem 4.4.3. *For α as in Lemma 4.2.3, and $\mathcal{A}_C$, $\mathcal{B}_C$ as in Definition 4.4.1,*

$$\frac{1}{\alpha}\mathcal{B}_{C^{\perp}} = \mathcal{A}_C^{'}.$$

Proof. We break the proof into 2 parts.

Part 1: $\frac{1}{\alpha}\mathcal{B}_{C^{\perp}} \subseteq \mathcal{A}_C^{'}$.

By (4.9), $\delta_L^{-1} = \frac{1}{p\alpha}(\beta\mathfrak{O}_L)$. It follows from Definition 4.3.1 and (4.14) that $z_1 \in C_A$, $z_2 \in \left(C^{\perp}\right)_B$ implies $z_1 \cdot z_2 \equiv 0 \bmod \beta$. Let $x \in \mathcal{A}_C$ and $y \in \mathcal{B}_{C^{\perp}}$. By Definition 4.4.1, $x \in \rho^{-1}(C_A)$, $\overline{y} \in \rho^{-1}\left(\left(C^{\perp}\right)_B\right)$ and

$$\begin{aligned} &\rho(\overline{y}) \cdot \rho(x) \equiv 0 \bmod \beta \\ \implies &\rho(\overline{y} \cdot x) \equiv 0 \bmod \beta \\ \implies &\overline{y} \cdot x \in \beta\mathfrak{O}_L. \end{aligned} \tag{4.39}$$

(4.39) follows because ρ is an $\mathfrak{O}_L$-module homomorphism. Note that $x \in \beta\mathfrak{O}_L$ *iff* $\overline{x} \in \beta\mathfrak{O}_L$ since $\beta\mathfrak{O}_L$ is closed under all elements in $\mathrm{Gal}(L/\mathbb{Q})$. Thus, $y \cdot \overline{x} \in \beta\mathfrak{O}_L$, and by Lemma 4.2.3 we have

$$\frac{(y \cdot \overline{x})}{p\alpha} \in \delta_L^{-1} \implies \mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{\left(\frac{1}{\alpha}y\right) \cdot \overline{x}}{p}\right) \in \mathbb{Z}.$$

Therefore, $\frac{1}{\alpha}y \in \mathcal{A}_C^{'}$ and $\frac{1}{\alpha}\mathcal{B}_{C^{\perp}} \subseteq \mathcal{A}_C^{'}$.

Part 2: $\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathcal{A}_C^{'}\right)\right) = \mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\frac{1}{\alpha}\mathcal{B}_{C^{\perp}}\right)\right)$.

We first compute $\mathrm{vol}\Big(\mathbb{R}^{n\phi(m)}/I(\mathcal{A}_C)\Big)$. By ([39], pg. 135),

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathcal{A}_C)\right) = |\mathfrak{O}_L^n/\mathcal{A}_C|\,\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathfrak{O}_L^n)\right). \tag{4.40}$$

We compute $|\mathfrak{O}_L^n/\mathcal{A}_C|$. By Definition 4.3.1, Definition 4.4.1, and (4.13), we have

$$\begin{aligned}|\mathfrak{O}_L^n/\mathcal{A}_C| &= |\mathfrak{O}_L^n/\rho^{-1}(C_A)| \\ &= \left|\left(\bigoplus_{l=1}^{\phi(p-1)} (\mathfrak{O}_L/Q_l)^n\right) / \Big(C \oplus \vec{0} \oplus \ldots \oplus \vec{0}\Big)\right|.\end{aligned}$$

Recall that C is a k-dimensional linear code and $\mathfrak{O}_L/Q_l \cong \mathbb{F}_p$ for all $1 \le l \le \phi(p-1)$ by Lemma 4.2.3. We have,

$$\begin{aligned}|\mathfrak{O}_L^n/\mathcal{A}_C| &= |(\mathfrak{O}_L/Q_1)^n/C| \prod_{l=2}^{\phi(p-1)} |(\mathfrak{O}_L/Q_l)^n| \\ &= p^{n-k}\,(p^n)^{\phi(p-1)-1} \\ &= p^{n\phi(p-1)-k}.\end{aligned} \tag{4.41}$$

By (4.36),

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathfrak{O}_L^n\right)\right) = p^{-\frac{n\phi(m)}{2}}|D_L|^{\frac{n}{2}}.$$

By Lemma 4.2.3,

$$|D_L| = \left(p^{p-2}\right)^{\phi(p-1)}|D_M|^{p-1}.$$

Since $\phi(m) = (p-1)\phi(p-1)$, note that

$$\begin{aligned}\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathfrak{O}_L^n)\right) &= p^{-\frac{n\phi(m)}{2}}\left(p^{\phi(m)-\phi(p-1)}|D_M|^{p-1}\right)^{\frac{n}{2}} \\ &= p^{-\frac{n\phi(p-1)}{2}}|D_M|^{\frac{n(p-1)}{2}}.\end{aligned} \tag{4.42}$$

By (4.40), (4.41), and (4.42), we have

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathcal{A}_C)\right) = p^{\frac{n\phi(p-1)}{2}-k}|D_M|^{\frac{n(p-1)}{2}}. \tag{4.43}$$

As in (4.35),

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathcal{A}_C)^*\right) = \frac{1}{\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathcal{A}_C)\right)}. \tag{4.44}$$

By Proposition 4.4.2, (4.43), and (4.44),

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathcal{A}'_C\right)\right) = \mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathcal{A}_C)^*\right) = p^{k-\frac{n\phi(p-1)}{2}}|D_M|^{-\frac{n(p-1)}{2}}. \tag{4.45}$$

We now find the volume of $I\left(\frac{1}{\alpha}\mathcal{B}_{C^\perp}\right)$. We first find the volume of $I\left(\mathcal{B}_{C^\perp}\right)$. Recall that $C^\perp$ is an $(n-k)$-dimensional linear code (Section 4.1). As in (4.40), we have

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathcal{B}_{C^\perp}\right)\right) = |\mathfrak{O}_L^n/\mathcal{B}_{C^\perp}|\,\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I(\mathfrak{O}_L^n)\right). \tag{4.46}$$

We compute $|\mathfrak{O}_L^n/\mathcal{B}_{C^\perp}|$. Again, by Definition 4.3.1, Definition 4.4.1, and (4.13), note that

$$\begin{aligned}
|\mathfrak{O}_L^n/\mathcal{B}_{C^\perp}| &= \left|\mathfrak{O}_L^n/\overline{\rho^{-1}(C_B^\perp)}\right| \\
&= \left|\mathfrak{O}_L^n/\rho^{-1}(C_B^\perp)\right| \\
&= \left|(\mathfrak{O}_L/Q_1)^n/C^\perp\right| \prod_{l=2}^{\phi(p-1)} \left|(\mathfrak{O}_L/Q_l)^n/\mathbb{F}_p^n\right|.
\end{aligned}$$

By Lemma 4.2.3,

$$|\mathfrak{O}_L^n/\mathcal{B}_{C^\perp}| = p^{n-(n-k)} = p^k. \tag{4.47}$$

By (4.42), (4.46), and (4.47), we have

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathcal{B}_{C^\perp}\right)\right) = p^{k-\frac{n\phi(p-1)}{2}}|D_M|^{\frac{n(p-1)}{2}}. \tag{4.48}$$

Recall from Lemma 4.2.3 that $\delta_M\mathfrak{O}_L = \alpha\mathfrak{O}_L$. Thus,

$$\mathrm{N}_{\mathbb{Q}}^L\left(\frac{1}{\alpha}\mathfrak{O}_L\right) = \mathrm{N}_{\mathbb{Q}}^M\left(\mathrm{N}_M^L\left(\frac{1}{\alpha}\mathfrak{O}_L\right)\right) = \mathrm{N}_{\mathbb{Q}}^M\left(\frac{1}{\alpha^{p-1}}\mathfrak{O}_N\right) = |D_M|^{-(p-1)}. \tag{4.49}$$

Note that scaling an L-lattice $\Gamma \subseteq \Gamma^n$ by a constant $c \in L$, scales the volume of the lattice $I(\Gamma)$ by $\left(\mathrm{N}_{\mathbb{Q}}^L(c)\right)^n$ [39]. Therefore,

$$\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\frac{1}{\alpha}\mathcal{B}_{C^\perp}\right)\right) = \left(\mathrm{N}_{\mathbb{Q}}^L\left(\frac{1}{\alpha}\right)\right)^n \mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathcal{B}_{C^\perp}\right)\right). \tag{4.50}$$

By (4.48), (4.49), (4.50), and (4.45), we have

$$\begin{aligned}
\mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\frac{1}{\alpha}\mathcal{B}_{C^\perp}\right)\right) &= |D_M|^{-n(p-1)}p^{k-\frac{n\phi(p-1)}{2}}|D_M|^{\frac{n(p-1)}{2}} \\
&= p^{k-\frac{n\phi(p-1)}{2}}|D_M|^{-\frac{n(p-1)}{2}} \\
&= \mathrm{vol}\left(\mathbb{R}^{n\phi(m)}/I\left(\mathcal{A}'_C\right)\right). \qquad \square
\end{aligned}$$

Combining Parts 1 and 2 gives the result $\frac{1}{\alpha}\mathcal{B}_{C^\perp} = \mathcal{A}'_C$.

4.5 Inversion Formulas

The following theorem provides the inversion formula for $\Theta_{\mathcal{A}_C}(\tau)$ in Definition 4.4.2.

Theorem 4.5.1. *For $\tau \in \mathbb{H}$,*

$$\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) = \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}|C|\widehat{\Theta}_{\mathcal{B}_{C^\perp}}(\tau).$$

Proof. By (4.17), and after identifying τ with $-\frac{1}{p\tau}$ in Theorem 4.2.2, we have

$$\begin{aligned}\Theta_{v_A}\left(-\frac{1}{\tau}\right) &= \Theta\left(L, -\frac{1}{p\tau}, \beta\mathfrak{O}_L, \begin{bmatrix}\widetilde{v}_A\\ 0\end{bmatrix}\right)\\ &= \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}\left(-\frac{1}{p\tau}\right)^{-\frac{n\phi(m)}{2}}\Theta\left(L, p\tau, \beta^{-1}\delta_L^{-1}, \begin{bmatrix}0\\ -\widetilde{v}_A\end{bmatrix}\right).\end{aligned}$$

By Lemma 4.2.3, $\beta^{-1}\delta_L^{-1} = \frac{1}{p\alpha}\mathfrak{O}_L$. By (4.22) and Definition 4.2.1, note that

$$\begin{aligned}\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) &= \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}\\ &\quad\cdot\sum_{v\in C}\sum_{\lambda\in\frac{1}{p\alpha}\mathfrak{O}_L^n}\exp\left[\pi i(p\tau)\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\lambda\cdot\overline{\lambda}\right)\right]\exp\left[2\pi i\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\lambda\cdot\widetilde{v}_A\right)\right].\end{aligned}$$

Writing $\frac{\lambda}{p}$ for λ, we have

$$\begin{aligned}\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) &= \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}\\ &\quad\cdot\sum_{v\in C}\sum_{\lambda\in\frac{1}{\alpha}\mathfrak{O}_L^n}\exp\left[\pi i\tau\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{\lambda\cdot\overline{\lambda}}{p}\right)\right]\exp\left[2\pi i\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{\lambda\cdot\widetilde{v}_A}{p}\right)\right].\end{aligned}$$

Exchanging the order of summation in this absolutely convergent series yields

$$\begin{aligned}\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) &= \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}\\ &\quad\cdot\sum_{\lambda\in\frac{1}{\alpha}\mathfrak{O}_L^n}\exp\left[\pi i\tau\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{\lambda\cdot\overline{\lambda}}{p}\right)\right]\sum_{v\in C}\exp\left[2\pi i\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{\lambda\cdot\widetilde{v}_A}{p}\right)\right].\end{aligned}$$

For $\lambda\in\frac{1}{\alpha}\mathfrak{O}_L^n$, define the finite sum

$$S_\lambda = \sum_{v\in C}\exp\left[2\pi i\mathrm{Tr}_{\mathbb{Q}}^{L}\left(\frac{\lambda\cdot\widetilde{v}_A}{p}\right)\right].$$

Since $\delta_L^{-1} = \frac{1}{p\alpha}(\beta\mathfrak{O}_L)$, $\exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{v}_A}{p}\right)\right]$ is independent of the choice for $\widetilde{v}_A$. We now calculate S_λ.

Case 1: If $\overline{\lambda} \notin \mathcal{A}_C'$ then $S_\lambda = 0$.

If $\overline{\lambda} \notin \mathcal{A}_C'$, there exists $x \in \mathcal{A}_C$ such that $\mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\overline{\lambda}\cdot\overline{x}}{p}\right) = \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot x}{p}\right) \notin \mathbb{Z}$. Writing $x = \widetilde{u}_A$ for $u \in C$, we know there exists a $u \in C$ such that

$$\exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{u}_A}{p}\right)\right] \neq 1.$$

Since C is a linear code,

$$\begin{aligned}
&\exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{u}_A}{p}\right)\right] S_\lambda \\
&= \sum_{v\in C} \exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot(\widetilde{v}_A+\widetilde{u}_A)}{p}\right)\right] \\
&= \sum_{v\in C} \exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{(u+v)}_A}{p}\right)\right] \\
&= \sum_{v\in C} \exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{v}_A}{p}\right)\right] \\
&= S_\lambda.
\end{aligned}$$

But $\exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{u}_A}{p}\right)\right] \neq 1$, so $S_\lambda = 0$.

Case 2: If $\overline{\lambda} \in \mathcal{A}_C'$ then $S_\lambda = |C|$.

If $\overline{\lambda} \in \mathcal{A}_C'$, $\mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot x}{p}\right) \in \mathbb{Z}$ for all $x \in \mathcal{A}_C$. Therefore, for all $u \in C$,

$$\exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{u}_A}{p}\right)\right] = 1$$

and

$$S_\lambda = \sum_{v\in C} \exp\left[2\pi i \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\widetilde{v}_A}{p}\right)\right] = \sum_{v\in C} 1 = |C|. \tag{4.51}$$

Recall that S_λ is defined *only* for $\lambda \in \frac{1}{\alpha}\mathfrak{O}_L^n$. By Theorem 4.4.3, Definition 4.3.1, and Definition 4.4.1, if C is the trivial code, C_0, then $\mathcal{A}_{C_0}' = \frac{1}{\alpha}\mathfrak{O}_L^n$. Thus, $\mathcal{A}_C' \subseteq \frac{1}{\alpha}\mathfrak{O}_L^n$ for any linear code $C \subseteq \mathbb{F}_p^n$. By (4.51), $S_\lambda \neq 0$ if $\overline{\lambda} \in \mathcal{A}_C$, implying

$$\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) = \mathrm{N}_{\mathbb{Q}}^L(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}|C| \sum_{\overline{\lambda}\in\mathcal{A}_C'} \exp\left[\pi i\tau \mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{\lambda\cdot\overline{\lambda}}{p}\right)\right]. \tag{4.52}$$

Since $x \cdot \overline{x} = \overline{x} \cdot x$, note that

$$\sum_{\lambda \in \mathcal{A}'_C} \exp\left[\pi i \tau \mathrm{Tr}^L_{\mathbb{Q}}\left(\frac{\lambda \cdot \overline{\lambda}}{p}\right)\right] = \sum_{\overline{\lambda} \in \mathcal{A}'_C} \exp\left[\pi i \tau \mathrm{Tr}^L_{\mathbb{Q}}\left(\frac{\lambda \cdot \overline{\lambda}}{p}\right)\right]. \tag{4.53}$$

By Theorem 4.4.3, $\mathcal{A}'_C = \frac{1}{\alpha}\mathcal{B}_{C^\perp}$. By (4.52) and (4.53), we have

$$\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) = \mathrm{N}^L_{\mathbb{Q}}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}|C|\widehat{\Theta}_{\mathcal{B}_{C^\perp}}(\tau). \qquad \square$$

The following theorem provides the inversion formulas for $\Theta_0(\tau)$ and $\Theta_1(\tau)$ in Definition 4.3.2.

Theorem 4.5.2. *For $\tau \in \mathbb{H}$,*

$$\Theta_0\left(-\frac{1}{\tau}\right) = \mathrm{N}^L_{\mathbb{Q}}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau) + (p-1)\widehat{\Theta}_1(\tau)\right)$$

and

$$\Theta_1\left(-\frac{1}{\tau}\right) = \mathrm{N}^L_{\mathbb{Q}}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau) - \widehat{\Theta}_1(\tau)\right).$$

Proof. Let $C = \{v_0\} \subseteq \mathbb{F}_p$ be the trivial code of length 1, i.e. $v_0 = 0$. Then $\mathcal{A}_C = \rho^{-1}(0, \ldots, 0) = \beta\mathfrak{O}_L$ and $\Theta_{\mathcal{A}_C}(\tau) = \Theta_{v_0}(\tau) = \Theta_0(\tau)$. Clearly, $C^\perp = \mathbb{F}_p$. By Definitions 4.3.1 and 4.4.1, $\mathcal{B}_{C^\perp} = \overline{\rho^{-1}(\mathbb{F}_p^{\phi(p-1)})} = \mathfrak{O}_L$. By Definition 4.3.2 and Theorem 4.5.1,

$$\begin{aligned}\Theta_0\left(-\frac{1}{\tau}\right) &= \mathrm{N}^L_{\mathbb{Q}}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\widehat{\Theta}_{\mathcal{B}_{C^\perp}}(\tau) \\ &= \mathrm{N}^L_{\mathbb{Q}}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau) + (p-1)\widehat{\Theta}_1(\tau)\right). \end{aligned} \tag{4.54}$$

Now let $C = \mathbb{F}_p$. Then $\mathcal{A}_C = \rho^{-1}(\mathbb{F}_p, 0, \ldots, 0) = \prod_{j=2}^{\phi(p-1)} Q_j$, and

$$\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) = \Theta_0\left(-\frac{1}{\tau}\right) + (p-1)\Theta_1\left(-\frac{1}{\tau}\right). \tag{4.55}$$

Note that $C^\perp = \{0\}$ and $\mathcal{B}_{C^\perp} = \overline{\rho^{-1}(0, \mathbb{F}_p, \ldots, \mathbb{F}_p)} = \overline{Q_1}$. It is easily checked that $\widehat{\Theta}_0(\tau)$ is invariant under complex conjugation of the summand Q_1. Since $|C| = p$, applying Theorem 4.5.1 yields

$$\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right) = \mathrm{N}^L_{\mathbb{Q}}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}(p)\widehat{\Theta}_0(\tau). \tag{4.56}$$

Substituting (4.54) for $\Theta_0\left(-\frac{1}{\tau}\right)$ on the right hand side of (4.55), substituting (4.56) for $\Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right)$ on the left hand side of (4.55), and rearranging terms yields

$$\Theta_1\left(-\frac{1}{\tau}\right) = \frac{1}{p-1}\Big(\mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}(p)\widehat{\Theta}_0(\tau) - \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau)+(p-1)\widehat{\Theta}_1(\tau)\right)\Big). \tag{4.57}$$

Simplifying (4.57) gives

$$\Theta_1\left(-\frac{1}{\tau}\right) = \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau)-\widehat{\Theta}_1(\tau)\right). \tag{4.58}$$

□

4.6 MacWilliams Identity

We are now ready to provide an analytic proof of the Hamming weight MacWilliams Identity for linear codes $C \subseteq \mathbb{F}_p^n$.

Theorem 4.6.1. Hamming weight MacWilliams Identity

With $\mathrm{HW}_C(x_0, x_1)$ *as in Definition 4.1.1,*

$$\mathrm{HW}_{C^\perp}(x_0,x_1) = \frac{1}{|C|}\mathrm{HW}_C\left(x_0+(p-1)x_1, x_0-x_1\right).$$

Proof. We follow the proof in the case of linear Hamming weight codes $C \subseteq \mathbb{F}_2^n$ described in ([27], Theorem 2.6) by evaluating

$$\mathrm{HW}_C\left(\Theta_0\left(-\frac{1}{\tau}\right), \Theta_1\left(-\frac{1}{\tau}\right)\right),$$

in two different ways. First, by Proposition 4.4.1 and Theorem 4.5.1,

$$\begin{aligned}
&\mathrm{HW}_C\left(\Theta_0\left(-\frac{1}{\tau}\right), \Theta_1\left(-\frac{1}{\tau}\right)\right)\\
&= \Theta_{\mathcal{A}_C}\left(-\frac{1}{\tau}\right)\\
&= \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}|C|\widehat{\Theta}_{\mathcal{B}_{C^\perp}}(\tau)\\
&= \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}}|C|\mathrm{HW}_{C^\perp}\left(\widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)\right).
\end{aligned} \tag{4.59}$$

Second, recall that $\mathrm{HW}_C(x_0, x_1)$ is a homogeneous polynomial of degree n from Definition 4.1.1. By Theorem 4.5.2,

$$\begin{aligned}
&\mathrm{HW}_C\left(\Theta_0\left(-\frac{1}{\tau}\right), \Theta_1\left(-\frac{1}{\tau}\right)\right) \\
&= \mathrm{HW}_C\Big(\mathrm{N}_{\mathbb{Q}}^L(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau) + (p-1)\widehat{\Theta}_1(\tau)\right), \\
&\qquad\qquad \mathrm{N}_{\mathbb{Q}}^L(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}\left(\widehat{\Theta}_0(\tau) - \widehat{\Theta}_1(\tau)\right)\Big) \\
&= \mathrm{N}_{\mathbb{Q}}^L(\beta)^{-n}|D_L|^{-\frac{n}{2}}(-p\tau)^{\frac{n\phi(m)}{2}} \qquad (4.60) \\
&\quad \cdot \mathrm{HW}_C\left(\widehat{\Theta}_0(\tau) + (p-1)\widehat{\Theta}_1(\tau), \widehat{\Theta}_0(\tau) - \widehat{\Theta}_1(\tau)\right).
\end{aligned}$$

Setting (4.59) and (4.60) equal, canceling like terms, and dividing by $|C|$ yields

$$\begin{aligned}
&\mathrm{HW}_{C^\perp}\left(\widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)\right) \qquad (4.61) \\
&= \frac{1}{|C|}\mathrm{HW}_C\left(\widehat{\Theta}_0(\tau) + (p-1)\widehat{\Theta}_1(\tau), \widehat{\Theta}_0(\tau) - \widehat{\Theta}_1(\tau)\right).
\end{aligned}$$

Define the homogeneous polynomial in 2 variables of degree n,

$$P(w, z) = \mathrm{HW}_{C^\perp}(w, z) - \frac{1}{|C|}\mathrm{HW}_C(w + (p-1)z, w - z).$$

To conclude the proof, it suffices to show that $P\left(\widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)\right) = 0$ implies $P(w, z)$ is the zero polynomial. Since $P(w, z)$ is a homogeneous polynomial of degree n in 2 variables, it factors over $\mathbb{C}$ into a product of linear forms $L_k(w, z)$ for $1 \leq k \leq n$. Since the ring of analytic functions on the connected domain $\mathbb{H}$ is an integral domain, there exists a k such that $L_k\left(\widehat{\Theta}_0(\tau), \widehat{\Theta}_1(\tau)\right)$ vanishes. Hence, there exist $a, b \in \mathbb{C}$ such that

$$a\widehat{\Theta}_0(\tau) + b\widehat{\Theta}_1(\tau) = 0.$$

We will show that $\widehat{\Theta}_0(\tau)$ and $\widehat{\Theta}_1(\tau)$ are linearly independent, i.e. $a, b = 0$. Note that $\mathrm{Tr}_{\mathbb{Q}}^L(\cdot)$ is a positive definite form on L since for $x \neq 0$,

$$\mathrm{Tr}_{\mathbb{Q}}^L\left(\frac{x\overline{x}}{p}\right) = \frac{1}{p}\sum_{j=1}^{\phi(m)} x^{(j)}\overline{x^{(j)}} > 0.$$

Therefore, the constant term in the Fourier expansion of $\widehat{\Theta}_0(\tau)$ is 1 and the constant term in the Fourier expansion of $\widehat{\Theta}_1(\tau)$ is zero since $\frac{1}{\alpha} \notin \frac{1}{\alpha}Q_1$. Hence, $\widehat{\Theta}_0(\tau)$ and $\widehat{\Theta}_1(\tau)$ are linearly independent if $\widehat{\Theta}_1(\tau)$ is not the zero function. Subtracting (4.58) from (4.54), we have

$$\Theta_0\left(-\frac{1}{\tau}\right) - \Theta_1\left(-\frac{1}{\tau}\right) = \mathrm{N}_{\mathbb{Q}}^{L}(\beta)^{-1}|D_L|^{-\frac{1}{2}}(-p\tau)^{\frac{\phi(m)}{2}}p\widehat{\Theta}_1(\tau). \tag{4.62}$$

By (4.7) and Definition 4.3.2, it is clear that $\Theta_0(\tau) \neq \Theta_1(\tau)$. By (4.62), $\widehat{\Theta}_1(\tau) \neq 0$. Hence, $\widehat{\Theta}_0(\tau)$ and $\widehat{\Theta}_1(\tau)$ are linearly independent, so P is identically zero. We conclude that,

$$\mathrm{HW}_{C^\perp}(x_0, x_1) = \frac{1}{|C|}\mathrm{HW}_C(x_0 + (p-1)x_1, x_0 - x_1). \qquad \square$$

Chapter 5

Association Schemes and Linear Codes

After demonstrating new results in Chapters 3 and 4, we now frame our work in the context of association schemes. We begin by introducing the theory of association schemes. We then describe how *abelian schemes* (a type of association scheme) can be created by weight and diversity function partitions. We consider linear codes in Definition 2.1.1 to be contained in these abelian schemes. We define weight enumerators over such abelian schemes and state their MacWilliams Identities. We discuss how to attach lattices and theta functions to linear codes in a general setting, and when we can write the weight enumerators in terms of these theta functions. We conclude by summarizing the pitfalls of our argument. We also provide a list of steps to follow to analytically prove MacWilliams Identities in order to aide future researchers. All comments on association schemes are based on the seminal work of Delsarte in the 1970's [21], [8].

5.1 Association Schemes

Let $N \in \mathbb{Z}_{>0}$. A *commutative association scheme* consists of a finite set X and a set of relations $S = \{S_0, \ldots, S_N\} \subseteq X \times X$ on X that satisfies the following conditions $(A_1) - (A_5)$.

(A_1) The diagonal relation $\{(x, x) \mid x \in X\}$ is the relation S_0 of S.

(A_2) The set S forms a partition of $X \times X$. That is, $S_i \neq \emptyset$ for all $0 \leq i \leq N$, $S_i \cap S_j = \emptyset$ if $i \neq j$, and

$$X \times X = S_0 \cup \ldots \cup S_N.$$

(A_3) The reciprocal relation of S_i,

$$ {}^tS_i = \{(x,y) \mid (y,x) \in S_i\}, \tag{5.1}$$

also belongs to S for all $0 \leq i \leq N$. That is, there exists a σ in the permutation group on N elements such that ${}^tS_i = S_{\sigma(i)}$ for all $1 \leq i \leq N$.

(A_4) For any triple of integers $i, j, k \in \{0, 1, \ldots, N\}$, the number of $z \in X$ such that $(x,z) \in S_i$ and $(z,y) \in S_j$ does not depend on the choice of (x,y) in S_k. This constant number is denoted by p_{ij}^k.

(A_5) For p_{ij}^k as in (A_4), we have $p_{ij}^k = p_{ji}^k$ for all $0 \leq i, j, k \leq N$.

We denote a commutative association scheme by the pair (X, S). For a treatment of non-commutative association schemes, which satisfy properties $(A_1) - (A_4)$ but not (A_5), we refer the reader to [2]. Throughout, we call a commutative association scheme an *association scheme*.

Let ${}^tS_i$ be as in (5.1). (X, S) is *symmetric iff* ${}^tS_i = S_i$ for all $0 \leq i \leq N$. That is,

$$ (x,y) \in S_i \Longleftrightarrow (y,x) \in S_i, \tag{5.2}$$

for all $0 \leq i \leq N$. If (X, S) is not symmetric, it can be "symmetrized" in the following way ([8], Exercise 1.8).

Definition 5.1.1. Let (X, S) be an association scheme and let σ be the permutation on N elements as described in (A_3). Define the partition on $X \times X$

$$ \overline{S} = \left\{ \overline{S}_0, \ldots, \overline{S}_{\overline{N}} \mid \overline{S}_i = S_i \cup {}^tS_i \right\},$$

where $\overline{N}$ is the number of orbits of the action of σ on $\{1, \ldots, N\}$. $\left(X, \overline{S}\right)$ is the *symmetrization of* (X, S) and is a symmetric association scheme.

A relation S_i on $X \times X$ can be described by its $|X| \times |X|$ *adjacency matrix* in $\mathrm{Mat}_{|X|\times|X|}(\mathbb{C})$,

$$ D_i = \begin{cases} 1, & (x,y) \in S_i \\ 0, & (x,y) \notin S_i \end{cases}. \tag{5.3}$$

We now give an alternative definition of an association scheme based on adjacency matrices. Let X be a finite set, $S = \{S_0, \ldots, S_N\} \subseteq X \times X$ be a set of relations on X, and $\mathcal{D} = \{D_0, \ldots, D_N\}$ be the set of corresponding adjacency matrices for S. Then X and the set of relations S on X form an association scheme *iff* $\mathcal{D}$ satisfies the following conditions $(C_1) - (C_5)$.

(C_1) $D_0 = I_{|X|}$, the identity matrix of dimension $|X| \times |X|$.

(C_2) $\sum_{i=0}^{N} D_i = J$, where J is the all 1's matrix. (This shows the D_i are linearly independent over $\mathbb{Q}$.)

(C_3) ${}^tD_i \in \mathcal{D}$.

(C_4) For p_{ij}^k in (A_4), we have $D_iD_j = \sum_{k=0}^{N} p_{ij}^k D_k$.

(C_5) $D_iD_j = D_jD_i$ for all $0 \leq i, j \leq N$.

Since the D_i are linearly independent, (C_4) and (C_5) imply (A_4) and (A_5). Let A be a matrix with complex entries. Let ${}^tA$ denote the transpose of A and $\overline{A}$ denote the complex conjugate of A. Let D_i be as in (5.3). (X, S) is *symmetric iff* ${}^tD_i = D_i$ for all $0 \leq i \leq N$. (This explains the notation in (5.1).) The adjacency matrices generate an algebra over $\mathbb{C}$ called the *BMD (Bose-Mesner-Delsarte) algebra*, which we denote by $\mathcal{A}_{\mathcal{D}}$. A matrix algebra is *normal iff* every element commutes with its conjugate transpose. Let $M \in \mathcal{A}_{\mathcal{D}}$. By (C_3) and (C_5), M is normal since ${}^t\overline{M} \in \mathcal{A}_{\mathcal{D}}$, which is generated by real matrices [8]. Hence, $\mathcal{A}_{\mathcal{D}}$ is a normal algebra of dimension $N + 1$ ([8], Remark 1.7).

Let p_{ij}^k be as in (A_4). For $0 \leq i \leq N$, define the $(N + 1) \times (N + 1)$ matrices

$$[L_i]_{jk} = p_{ij}^k. \tag{5.4}$$

L_i is the i^{th} *intersection matrix of* (X, S). Let $\mathcal{L} = \{L_0, \ldots, L_N\}$ be the set of intersection matrices for (X, S). The intersection matrices generate an algebra over $\mathbb{C}$ called the *intersection algebra*, which we denote by $\mathcal{A}_{\mathcal{L}}$. $\mathcal{A}_{\mathcal{L}}$ is the left regular representation of $\mathcal{A}_{\mathcal{L}}$ acting on $\mathcal{D}$ ([8], Section 1.4

(3)). $\mathcal{A}_{\mathcal{L}}$ is isomporhic to $\mathcal{A}_{\mathcal{D}}$ and both are normal algebras of dimension $(N+1)$ ([8], Section 1.4 (3)). Association schemes are often studied in the context of $\mathcal{A}_{\mathcal{D}}$ and $\mathcal{A}_{\mathcal{L}}$.

Note that the adjacency matrices have size $|X| \times |X|$ while the intersection matrices have size $(N+1) \times (N+1)$. It is usually the case that $(N+1) \ll |X|$. Hence, it is more computationally efficient to work over $\mathcal{A}_{\mathcal{L}}$ instead of $\mathcal{A}_{\mathcal{D}}$. Nevertheless, $\mathcal{A}_{\mathcal{D}}$ plays a central role in the duality theory of association schemes. We discuss this further in Section 5.4.

To relate linear codes to association schemes, we now define an *abelian scheme* ([8], Definition 4.1).

Definition 5.1.2. Let X be an abelian group. Let (X, S) be an association scheme that is *invariant under translation*, i.e.

$$(x, y) \in S_i \iff (x + w, y + w) \in S_i,$$

for all $w \in X$ and $0 \leq i \leq N$. In particular,

$$(x, y) \in S_i \iff (x - y, 0) \in S_i.$$

We call (X, S) an *abelian scheme*.

Let (X, S) be an abelian scheme. There is a natural way to define a partition T of X associated to the partition S of $X \times X$.

Definition 5.1.3. Let (X, S) be an abelian scheme as in Definition 5.1.2. Define the *partition of X associated to* (X, S) to be $T = \{T_0, \ldots, T_N\}$ such that for all $0 \leq i \leq N$,

$$z \in T_i \iff (z, 0) \in S_i.$$

The partition T of X *defines the abelian scheme* (X, S) by specifying

$$(x, y) \in S_i \iff x - y \in T_i.$$

In the next section, we relate abelian schemes (X, S) to linear codes $C \subseteq X$. We now recall the definition of a linear code from Definition 2.1.1.

Definition 5.1.4. Let $m, n, k \in \mathbb{Z}_{>0}$. Let B be a finite commutative ring with identity $1 \neq 0$ and $X = \mathrm{Mat}_{m\times n}(B)$. (Note that X is a B-module.) A code $C \subseteq X$ is called a *linear code of dimension k iff* C is a free B-module of rank k.

Throughout, let B be a finite commutative ring with identity $1 \neq 0$ and $X = \mathrm{Mat}_{m\times n}(B)$. We relate linear codes $C \subseteq X$ to abelian schemes (X, S) using weight functions and diversity functions. (For examples of weight functions and diversity functions we refer the reader to Section 2.1.1.) We will see that diversity functions partition $X \times X$ into a set of relations S. If (X, S) is an abelian scheme, then the corresponding weight function partitions X into the set T as in Definition 5.1.3. Restricting this weight partition to $C \subseteq X$ allows us to consider linear codes to be contained in abelian schemes. We investigate these ideas further in the following section.

5.2 Weight Functions, Diversity Functions, and Abelian Schemes

Let $d(\cdot, \cdot)$ be a diversity function on $X \times X$ and $wt(\cdot)$ be its corresponding weight function (see Section 2.1.1). Let $u, v \in X$. By (2.1), recall that

$$d(u, v) = wt(u - v). \tag{5.5}$$

Recall that the image of $d(\cdot, \cdot)$, which equals the image of $wt(\cdot)$, is denoted by R_d. Recall that $R_d \subseteq X$ or $R_d \subseteq \mathbb{Z}_{\geq 0}$. Let $R_d = \{r_0, \ldots, r_N\}$. Note that $|R_d| = N + 1$. If $R_d \subseteq X$, we set $r_0 = v_0$, where v_0 is the zero codeword. If $R_d \subseteq \mathbb{Z}_{\geq 0}$, we set $r_0 = 0$. We define the *diversity partition of* $X \times X$ to be

$$S_d = \{S_0, \ldots, S_N\}, \tag{5.6}$$

such that for all $0 \leq i \leq N$,

$$(u, v) \in S_i \iff d(u, v) = r_i. \tag{5.7}$$

This is exactly the partition from the fibers of $d(\cdot, \cdot)$. By (5.5), (5.6), and (5.7), S_d is translation invariant. That is, for all $w \in X$ and $0 \leq i \leq N$,

$$(u, v) \in S_i \iff (u + w, v + w) \in S_i. \tag{5.8}$$

By Definition 5.1.3, (5.5), (5.6), and (5.7), we define the partition of X relative to (X, S_d) to be

$$T_d = \{T_0, \ldots, T_N\}, \tag{5.9}$$

such that for all $0 \leq i \leq N$,

$$v \in T_i \iff wt(v) = r_i. \tag{5.10}$$

The following proposition will help determine when (X, S_d) is an abelian scheme ([8], Property 4.45).

Proposition 5.2.1. *Let* $\mathrm{Aut}(X)$ *be the group of group automorphisms of* X*. Let* $H \subseteq \mathrm{Aut}(X)$ *be a subgroup. Let* v_0 *be the zero codeword of* X*. Let* $T_0 = \{v_0\}, T_1, \ldots, T_N$*, be the orbits of* X *under* H*. Then the partition*

$$T = \{T_0, T_1, \ldots, T_N\},$$

of X *defines an Abelian scheme as in Definition 5.1.3.*

We now show that the partitions associated to the weight functions considered in Section 2.1.1 yield abelian schemes.

Theorem 5.2.1. *Let* $d_{\mathrm{H}}(\cdot,\cdot)$*,* $d_{\mathrm{cd}}(\cdot,\cdot)$*,* $d_{\mathrm{rk}}(\cdot,\cdot)$*,* $d_{\mathrm{c}}(\cdot,\cdot)$*, and* $d_{\mathrm{L}}(\cdot,\cdot)$*, denote the Hamming diversity function, column distance diversity function, rank diversity function, complete diversity function, and Lee diversity function as defined in Section 2.1.1, respectively. Let* S_d *be as in* (5.6) *and* (5.7)*. Let* T_d *be as in* (5.9) *and* (5.10)*. If* $d \in \{d_{\mathrm{H}}, d_{\mathrm{c}}, d_{\mathrm{L}}\}$*, then* (X, S_d) *is an abelian scheme. If* $B = \mathbb{F}_q$ *where* q *is a power of a prime and* $d \in \{d_{\mathrm{rk}}, d_{\mathrm{cd}}\}$*, then* (X, S_d) *is an abelian scheme.*

Proof. It is well known that $(X, S_{d_{\mathrm{H}}})$ is a symmetric abelian scheme by ([21], Section II, Example 1); or, we can see this directly from Proposition 5.2.1 by letting H be the subgroup generated by the automorphisms of X that permute the elements of a matrix or act on a given entry by an element of the symmetric group of B which fixes the zero element.

For the diversity functions $d_{\mathrm{c}}(\cdot,\cdot)$ and $d_{\mathrm{L}}(\cdot,\cdot)$, by Proposition 5.2.1 it suffices to show there exists a subgroups $H_{d_{\mathrm{c}}}, H_{d_{\mathrm{L}}} \subseteq \mathrm{Aut}(X)$ whose orbits are of the form $T_{d_{\mathrm{c}}}$, and $T_{d_{\mathrm{L}}}$, respectively.

Let $H_{d_c} \subseteq \mathrm{Aut}(X)$ be the trivial subgroup. Let $X = \left\{v_0, v_1, \ldots, v_{|X|-1}\right\}$, where v_0 denotes the zero codeword. Recall from (2.9) that $R_{d_c} = X$. Note that $T_{d_c} = \left\{T_0, T_1, \ldots, T_{|X|-1}\right\}$, such that for $0 \leq i \leq |X| - 1$,

$$v \in T_i \iff v = v_i.$$

By (2.7) and (5.10), (X, S_{d_c}) is an abelian scheme.

Let $H_{d_L} \subseteq \mathrm{Aut}(X)$ be the subgroup generated by $\{\pm 1\}$. Order the elements of X so that

$$X = \left\{v_0, v_1, \ldots, v_{|X|-1}\right\},$$

where v_0 denotes the zero codeword and $v_i = -v_{|X|-i}$ for all $1 \leq i \leq |X| - 1$. We define $R_{d_L} = \left\{v_0, v_1, \ldots, v_{\left\lceil \frac{|X|-1}{2} \right\rceil}\right\}$. Hence, $T_{d_L} = \left\{T_0, T_1, \ldots, T_{\left\lceil \frac{|X|-1}{2} \right\rceil}\right\}$, such that for $0 \leq i \leq \left\lceil \frac{|X|-1}{2} \right\rceil$,

$$v \in T_i \iff v = v_i \quad \text{or} \quad v = v_{|X|-i}.$$

By (2.8) and (5.10), (X, S_{d_L}) is an abelian scheme

Now, set $B = \mathbb{F}_q$ for q a power of a prime. Then, by letting $\mathrm{GL}_m(B)$ and $\mathrm{GL}_n(B)$ act on the left and on the right of a matrix in $\mathrm{Mat}_{m\times n}(B)$, by Proposition 5.2.1 we see that $(X, S_{d_{\mathrm{rk}}})$ is an abelian scheme ([8], Example 4.66). In Section 3.2, we consider $X = \mathrm{Mat}_{m\times n}(\mathbb{F}_2)$ as a set of vectors under the "stacking" map $\Phi(\cdot)$. (Note that this is just the special case when $q = 2$.) Recall that we write $\Phi(X) = \widehat{X}$ to denote the set of stacked matrices. In Lemma 3.3.1, we define the group $G_{\mathrm{cd}} \subseteq \mathrm{GL}_{mn}(\mathbb{F}_2)$ whose action by left multiplication on $\widehat{X}$ yields the partition (for $0 \leq i \leq n$)

$$\mathfrak{O}_i = \{\Phi(v) \mid wt_{\mathrm{cd}}(v) = i\}.$$

Hence, if $B = \mathbb{F}_2$, we explicitly defined a subgroup $G_{\mathrm{cd}} \subseteq \mathrm{Aut}\left(\widehat{X}\right)$ partitioning $\widehat{X}$ into its distinct column distance classes. Defining $T_i = \Phi^{-1}(\mathfrak{O}_i)$ for all $0 \leq i \leq n$, we see that the corresponding partition T of X defines an abelian scheme (Proposition 5.2.1). This argument can be extended to the case when $B = \mathbb{F}_q$ to show that $(X, S_{d_{\mathrm{cd}}})$ is an abelian scheme. (One can even view $\mathrm{Mat}_{m\times n}(B)$ as $\mathcal{B}^n$ where $\mathcal{B} = B^m$ and recognize column distance weight on $\mathrm{Mat}_{m\times n}(B)$ as Hamming weight on $\mathcal{B}^n$.) $\square$

We call $(X, S_{d_{\mathrm{H}}})$, $(X, S_{d_{\mathrm{c}}})$, and $(X, S_{d_{\mathrm{L}}})$, the *Hamming scheme*, *complete scheme*, and *Lee scheme*, respectively. If $B = \mathbb{F}_q$, we call $(X, S_{d_{\mathrm{rk}}})$, and $(X, S_{d_{\mathrm{cd}}})$, the *rank scheme*, and *column distance scheme*, respectively. Note that there can be multiple association schemes (X, S) for a fixed X. Note that $(X, S_{d_{\mathrm{L}}})$ is the *symmetrization* of $(X, S_{d_{\mathrm{c}}})$ as in Definition 5.1.1. The following definition provides a means of comparing two association schemes with the same underlying set.

Definition 5.2.2. Let (X, S) and (X, W) be association schemes such that $S = \{S_0, \ldots, S_{N_1}\}$, $W = \{W_0, \ldots, W_{N_2}\}$, and $N_2 \leq N_1$. We say that (X, S) is *covered by* (X, W) *iff* $W_i = \cup_{l \in I_i} S_l$ where $\{I_0, \ldots, I_{N_2}\}$ is a partition of $\{0, 1, \ldots, N_1\}$. If (X, S) is covered by (X, W) we write $(X, S) \preceq (X, W)$. The partition S is *finer* than W and the partition W is *coarser* than S.

By Definition 5.2.2, note that

$$(X, S_{d_{\mathrm{c}}}) \preceq (X, S_{d_{\mathrm{L}}}) \preceq (X, S_{d_{\mathrm{H}}}) \,. \tag{5.11}$$

5.3 Weight Enumerators and Abelian Schemes

We now associate weight enumerators to an abelian scheme. Recall that $X = \mathrm{Mat}_{m \times n}(B)$ where B is a finite commutative ring with identity $1 \neq 0$. Let (X, S) be an abelian scheme as in Definition 5.1.2, T be the partition of X associated to the abelian scheme (X, S) as in Definition 5.1.3, and $C \subseteq X$ be a linear code as in Definition 5.1.4.

5.3.1 Linear Weight Enumerators

Let $x_0, \ldots, x_N$ be $(N+1)$-independent variables. We define the *linear weight enumerator of* C to be

$$\mathrm{W}_C(x_0, \ldots, x_N) = \sum_{r=0}^{N} a_r x_r, \tag{5.12}$$

where for $0 \leq r \leq N$,

$$a_r = |C \cap T_r| \,. \tag{5.13}$$

Note that the weight enumerators in (2.10) and (5.12) are equal if $(X, S) = (X, S_d)$ for a diversity function $d(\cdot, \cdot)$. (The definitions of a_r in (2.3) and (5.13) are equivalent in this case.)

We have that $\mathrm{W}_C(\cdot)$ in (5.12) is a linear combination of independent variables, each of which represents a class in the partition T associated to an abelian scheme. In the following section, we deal with weight enumerators which are general polynomials in which every *monomial* represents a class in the partition T associated to an abelian scheme. For examples of such weight enumerators consider the Hamming weight enumerator in (2.11) and the column distance weight enumerator in (2.12).

5.3.2 Total Weight Enumerators

We begin by stating a theorem which defines an association scheme on the Cartesian product of two association schemes ([8], Theorem 4.82).

Theorem 5.3.1. *Let (X_1, S) be an association scheme such that $S = \{S_0, \ldots, S_{N_1}\} \subseteq X_1 \times X_1$. Let (X_2, W) be an association scheme such that $W = \{W_0, \ldots, W_{N_2}\} \subseteq X_2 \times X_2$. Let $X_1 \times X_2$ be the Cartesian product of X_1 and X_2. Let $S \otimes W = \{S_i \otimes W_j\}_{0 \leq i \leq N_1, 0 \leq j \leq N_2}$ denote the partition of $(X_1 \times X_2)^2$, where the elements of $S_i \otimes W_j$ are precisely the pairs $((x, y), (u, v))$ for $(x, u) \in S_i$ and $(y, v) \in W_j$. Then $(X_1 \times X_2, S \otimes W)$ is an association scheme.*

Let $Y = \mathrm{Mat}_{m \times 1}(B)$, $U = \{U_0, \ldots, U_M\} \subseteq Y \times Y$ be a set of relations on Y, and (Y, U) be an abelian scheme as in Definition 5.1.2. Let

$$V = \{V_0, \ldots, V_M\},$$

be the partition of Y associated to the abelian scheme (Y, U) as in Definition 5.1.3. We now apply Theorem 5.3.1 to the set $Y \times Y$ (setting $X_1 = X_2 = Y$ and $S = W = U$). We denote the pair of the finite set $Y^2 \times Y^2$ and the partition $L = U \otimes U$ by $(Y, U)^{\otimes 2} = \left(Y^2, L\right)$.

Since (Y, U) is an abelian scheme, we have that $(Y, U)^{\otimes 2}$ is also an abelian scheme and we call it the *extension scheme of length* 2 ([8], Theorem 4.86). By Theorem 5.3.1, we can inductively define an abelian scheme on Y^n, $(Y, U)^{\otimes n}$, which we call the *extension scheme of length* n ([8], Theorem 4.86). In this case, each component of the partition

$$L = \bigotimes^{n} U = \{U_{i_1} \otimes \cdots \otimes U_{i_n}\}_{0 \leq i_j \leq M},$$

for all $1 \leq j \leq n$, consists of all couples $((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \in Y^n \times Y^n$ such that $(x_1, y_1) \in U_{i_1}, \ldots, (x_n, y_n) \in U_{i_n}$.

We now discuss *Delsarte extension schemes*, which specialize the notion of extension schemes (summarizing the work in ([8], Section 4.11)). Let $(Y, U)^{\otimes n}$ be the extension scheme of length n described above. Recall that $X = \mathrm{Mat}_{m \times n}(B)$, so $X = Y^n$ and $(X, L) = (Y, U)^{\otimes n}$. Let S_n denote the symmetric group on n elements. A permutation $\sigma \in S_n$ acting on $\{1, \ldots, n\}$ induces a permutation κ acting on $X \times X$; the image under κ of a couple $((x_1, \ldots, x_n), (y_1, \ldots, y_n))$ is $\left(\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right), \left(y_{\sigma(1)}, \ldots, y_{\sigma(n)}\right)\right)$. Hence, κ maps $U_{i_1} \otimes \cdots \otimes U_{i_n}$ onto $U_{i_{\sigma(1)}} \otimes \cdots \otimes U_{i_{\sigma(n)}}$ and permutes the components of the partition L of the association scheme (X, L).

Note that the diagonal relation $U_0 \otimes \cdots \otimes U_0$ is a fixed point under this action. The orbits of the action of S_n acting on L form a partition S on $X \times X$ which is coarser than L. The pair (X, S) is called the *Delsarte extension scheme* and is an abelian scheme ([8], Theorem 4.97).

The Hamming scheme (for $m = 1$), $(X, S_{d_{\mathrm{H}}})$, and the column distance scheme, $(X, S_{d_{\mathrm{cd}}})$, are Delsarte extension schemes because both the Hamming weight, and the column distance weight, are invariant under entry switching, and column switching, respectively ([8], Example 5.54). We now associate total weight enumerators to Delsarte extension schemes.

We begin by defining the *exact weight enumerator*. Let $\{x_\alpha\}_{\alpha \in Y}$ be a set of $|Y|$-independent variables. (We're picking a variable x_α for each column vector $\alpha \in Y$. Note that if $m = 1$, then $Y = B$, so the variable x_α represents one element $\alpha \in B$, and $X = Y^n$ is the ring of row vectors in B.) Let $v_j \in Y$ denote the j^{th} column of $v \in X$. We define the *exact weight enumerator of* C to be

$$\mathrm{EW}_C(\vec{x}_\alpha) = \sum_{v \in C} \prod_{\alpha \in Y} x_\alpha^{n_v(\alpha)}, \tag{5.14}$$

where

$$n_v(\alpha) = |\{1 \leq j \leq n \mid v_j = \alpha\}|. \tag{5.15}$$

[This is a specialization of the weight enumerator in ([8], Definition 5.39). The difference is that the exact weight enumerator in (5.14) does not respect the order of the columns in v. For more on the exact weight enumerator in (5.14), we refer the reader to [17], [10], [11], [9].]

Note that the column distance weight enumerator in (2.12) comes from the exact weight enumerator in (5.14) after specializing the variables x_α to x_0 if $\alpha = \vec{0}$, and x_α to x_1 if $\alpha \neq \vec{0}$. If $m = 1$, the Hamming weight enumerator in (2.11) comes from the exact weight enumerator in (5.14) after specializing the variables x_α to x_0 if $\alpha = 0$, and x_α to x_1 if $\alpha \neq 0$. (If $m \neq 1$, we can always think of our matrix code as a row vector code by taking the transpose of our matrix code's image under the "stacking" map $\Phi(\cdot)$ in (3.11).)

We can obtain a *total weight enumerator* from the exact weight enumerator in (5.14). Indeed, let $0 \leq s \leq M$ and recall that $V = \{V_0, \ldots, V_M\}$. We get the total weight enumerator by specializing x_α to x_s for every $\alpha \in V_s$ in the exact weight enumerator. We make this idea precise with the following definition.

Definition 5.3.2. Let $Y = \mathrm{Mat}_{m\times 1}(B)$ and (Y, U) be an abelian scheme. Let (X, S) be the Delsarte extension scheme described above. Let $[0, n] = \{0, 1, \ldots, n\}$. Let $\mathbf{I}$ denote the set of $\mathbf{i} = (i_0, \ldots, i_M) \in [0, n]^{M+1}$ such that $\sum_{s=0}^{M} i_s = n$. We define the *total weight enumerator of* C to be

$$\mathrm{TW}_C(x_0, \ldots, x_M) = \sum_{\mathbf{i}\in\mathbf{I}} a_{\mathbf{i}} \prod_{s=0}^{M} x_s^{n_v(s)}, \tag{5.16}$$

where

$$n_v(s) = |\{1 \leq j \leq n \mid v_j \in V_s\}|, \tag{5.17}$$

and if $\mathbf{i} = (i_0, \ldots, i_M)$, $a_{\mathbf{i}}$ is the number of $v \in C$ such that $i_s = n_v(s)$ for all $0 \leq s \leq M$.

[This is a specialization of the weight enumerator in ([8], Definition 5.45). The difference is that the total weight enumerator in (5.16) does not respect the order of the columns in v.]

In Chapter 3, we analytically proved the column distance weight MacWilliams Identity for $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ with the total weight enumerator in (5.16) for the Delsarte extension scheme $(X, S_{d_{\mathrm{cd}}})$. In Chapter 4, we analytically proved the Hamming weight MacWilliams Identity for $C \subseteq \mathbb{F}_p^n$ with the total weight enumerator in (5.16) for the Delsarte extension scheme $(X, S_{d_{\mathrm{H}}})$. In each of these cases, the representative theta functions for $T_r \in T_d$, $0 \leq r \leq N$, factored in a natural way corresponding to the definitions of the total weight enumerators. In the case of linear

rank codes $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$, the representative theta functions for $T_r \in T_d$, $0 \leq r \leq 2$, did not apparently factor in a natural way corresponding to a total weight enumerator. (For an example of a total rank weight enumerator see [32] and [31].) So, in this case we analytically proved the MacWilliams Identity for the linear rank weight enumerator.

To extend the class of codes for which there exists an analytic proof of the MacWilliams Identity, we believe it would be beneficial to understand which diversity functions, $d(\cdot,\cdot)$, yield Delsarte extension schemes, (X, S_d). (For more details on Delsarte extension schemes see ([8], Section 4.11).)

In the next section, we state the MacWilliams Identity for the linear weight enumerator in (5.12) for linear codes contained in an abelian scheme. We also cite the existence of the MacWilliams Identity for the total weight enumerator in (5.16) for linear codes contained in a Delsarte extension scheme.

5.4 MacWilliams Identities and Abelian Schemes

Let (X, S) be an abelian scheme as in Definition 5.1.2. Recall that $\mathcal{A}_{\mathcal{D}}$ denotes the BMD algebra which is generated by the set of adjacency matrices $\mathcal{D}$ defined in (5.3). We now define an *idempotent* element of an algebra ([8], Definition 2.1).

Definition 5.4.1. Let $\mathcal{A}$ be an algebra. An element $u \in \mathcal{A}$ is an *idempotent* if $u \neq 0$ and $u^2 = u$. It is a *primitive idempotent* if it is not the sum of two idempotents.

Since $\mathcal{A}_{\mathcal{D}}$ is a commutative normal algebra, there exists a basis of primitive idempotents for $\mathcal{A}_{\mathcal{D}}$ ([8], Lemma 2.11). We denote this basis by $\mathcal{J} = \{J_0, J_1, \ldots, J_N\}$. Let P be the transpose change of basis matrix from $\mathcal{J}$ to $\mathcal{D}$. That is, for all $0 \leq k \leq N$,

$$D_k = \sum_{i=0}^{N} [P]_{ik} J_i, \tag{5.18}$$

where $[P]_{ik}$ is the $(i,k)^{\text{th}}$-entry of P. Then P is called the *first eigenmatrix of the association scheme*.

Since P is a change of basis matrix, P is invertible. Hence, for all $0 \leq k \leq N$, we can write

$$J_k = |X|^{-1} \sum_{i=0}^{N} [Q]_{ik} D_i. \tag{5.19}$$

The matrix Q is called the *second eigenmatrix of the association scheme*. The two eigenmatrices, P and Q, play a central role in the duality theory of abelian schemes. Note that $PQ = QP = |X|I$, where I is the $|X| \times |X|$ identity matrix.

Before stating the MacWilliams Identities for the linear weight enumerator in (5.12) and the total weight enumerator in (5.16), we give a more general definition for the dual code than that in (2.14). This requires a short introduction to character theory.

Recall that $X = \mathrm{Mat}_{m\times n}(B)$ for B a finite commutative ring with identity $1 \neq 0$, so X is a finite additive abelian group. A *character* χ of a finite abelian group is a homomorphism of that group into the multiplicative group $\mathbb{C}^*$ of the complex numbers ([8], Section 4.2.1). We denote the set of characters χ of X, by $X^{'}$. It is well known that $X^{'}$ is an abelian group. We now give a general definition of a dual code $C^{\perp}$.

Definition 5.4.2. Let $X = \mathrm{Mat}_{m\times n}(B)$ for B a finite commutative ring with identity $1 \neq 0$, $X^{'}$ be its character group, and $C \subseteq X$ be a k-dimensional linear code as in Definition 5.1.4. Then,

$$C^{\perp} = \left\{ \chi \in X^{'} \mid \chi(v) = 1, \ \forall v \in C \right\}. \tag{5.20}$$

That is, the dual code of C is the set of all characters which are trivial on every element in C.

This definition is compatible with the definition of $C^{\perp}$ in (2.14). To see this, consider the following theorem ([8], Theorem 4.8).

Theorem 5.4.3. *The character group $X^{'}$ of a finite abelian group X is (noncanonically) isomorphic to X; X is (canonically) the character group of $X^{'}$.*

It is common to fix an isomorphism and consider the character group $X^{'}$ as X. Following Example 4.21 in [8], we leave it to the reader to see that the definitions of $C^{\perp}$ in (2.14) and (5.20) are compatible.

The following theorem shows there exists a MacWilliams Identity for $\mathrm{W}_C(\cdot)$ in (5.12) defined for linear codes contained in abelian schemes ([8], Property 5.42).

Theorem 5.4.4. *Let* $\mathrm{W}_C(\cdot)$ *be as in* (5.12). *Let* $\vec{x} = (x_0, \ldots, x_N)$. *Let* $a(C) = (a_0, a_1, \ldots, a_N)$ *be the weight distribution of a linear code* C *in an abelian scheme* (X, S). *Let* $C^\perp$ *be the dual code as in* (5.20). *Let* Q *be the second eigenmatrix of the abelian scheme* (X, S) *as in* (5.19). *Then,*

$$\mathrm{W}_{C^\perp}(\vec{x}) = \frac{1}{|C|}\mathrm{W}_C(Q\vec{x}).$$

Likewise, there exists a MacWilliams Identity for $\mathrm{TW}_C(\cdot)$ in (5.16) defined for linear codes contained in Delsarte extension schemes ([8], Theorem 5.46). Hence, a MacWilliams Identity exists for both $\mathrm{W}_C(\cdot)$ in (5.12) and $\mathrm{TW}_C(\cdot)$ in (5.16).

In this dissertation, we attempted to answer the following question: When does an *analytic proof* of these MacWilliams Identities exist? Unfortunately, we were unable to fully answer this question. However, we do know an analytic proof exists for the following types of linear codes:

(1) Hamming weight vector codes $C \subseteq \mathbb{F}_2^n$ ([7], [27]).

(2) Self-orthogonal Lee weight vector codes $C \subseteq C^\perp \subseteq \mathbb{F}_p^n$ ([13], [27]).

(3) Column distance matrix codes $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$ (Chapter 3).

(4) Rank weight matrix codes $C \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$ (Chapter 3).

(5) Hamming weight vector codes $C \subseteq \mathbb{F}_p^n$ (Chapter 4), generalizing (1).

(6) Hamming weight vector codes $C \subseteq \mathbb{F}_4^n$ ([50], Section 3.7).

In the next section, we describe how to attach theta functions to linear codes contained in abelian schemes and relate them to weight enumerators. We also discuss problems that arise when analytically proving MacWilliams Identities.

5.5 Theta Functions, Analytic Proofs, and Abelian Schemes

In this section, we make some simplifying assumptions. Let (X, S) be an abelian scheme such that the associated partition T of X is the result of a group action $H \subseteq \mathrm{Aut}(X)$ on X and (X, S) is self dual (which ensures that the weight enumerator for the code and its dual are defined on the same abelian scheme ([8], Section 4.15)).

Let a number field K be an abelian extension over $\mathbb{Q}$ and let $\mathfrak{O}_K$ be its ring of integers. Let $\mathcal{I} = \{I_1, \ldots, I_f\}$ be a set of pairwise relatively prime integral ideals in $\mathfrak{O}_K$ that is Galois invariant; i.e. $\sigma(\mathcal{I}) = \mathcal{I}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We further require that all $\mathfrak{O}_K/I_l$, $1 \leq l \leq f$, be isomorphic, and we fix an isomorphism to $B = \mathfrak{O}_K/I_l$. Let

$$I = \prod_{l=1}^{f} I_f \subseteq \mathfrak{O}_K. \tag{5.21}$$

Let $C \subseteq X$ be a linear code as in Definition 5.1.4. We now describe how to attach a lattice to such a C. This setup includes all cases we handled in Chapters 3 and 4.

5.5.1 Attaching Lattices to Linear Codes

Let $v \in X = \mathrm{Mat}_{m\times n}(B)$ and $v_j \in B^m$ be the j^{th}-column of v for $1 \leq j \leq n$. First, we identify a matrix codeword $v \in \mathrm{Mat}_{m\times n}(B)$ with a (column) vector in B^{mn} by the "stacking" map

$$\begin{aligned} \Phi :&\mathrm{Mat}_{m\times n}(B) \longrightarrow B^{mn} \\ &\left[v_1|\cdots|v_n\right] \longmapsto \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}. \end{aligned} \tag{5.22}$$

Let $e_1, \ldots, e_n \in \{0,1\}^n \subseteq B^n$ be the standard basis (column) vectors of length n. Note that

$$\Phi(v) = (I_n \otimes v) \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}, \tag{5.23}$$

where $\otimes$ denotes the Kronecker product of matrices. (Note that a B-linear map $\Phi^{-1} : B^{mn} \longrightarrow \mathrm{Mat}_{m\times n}(B)$ also exists.)

For ease of notation, define

$$\Phi(v) = \widehat{v}. \tag{5.24}$$

For $\widehat{v}$ in (5.24), let

$$\widehat{X} = \{\widehat{v} \mid v \in X\} \quad \text{and} \quad \widehat{C} = \{\widehat{v} \mid v \in C\}. \tag{5.25}$$

Note that $\widehat{X} = B^{mn}$. Let ${}^t(y_1, \ldots, y_{mn}) \in \mathfrak{O}_K^{mn}$. We define the *reduction map homomorphism*

$$\rho : \mathfrak{O}_K^{mn} \longrightarrow \mathcal{X} = \bigoplus_{l=1}^{f} \widehat{X} \tag{5.26}$$

$$\rho \begin{bmatrix} y_1 \\ \vdots \\ y_{mn} \end{bmatrix} = \left(\begin{bmatrix} y_1 \bmod I_1 \\ \vdots \\ y_{mn} \bmod I_1 \end{bmatrix}, \cdots, \begin{bmatrix} y_1 \bmod I_f \\ \vdots \\ y_{mn} \bmod I_f \end{bmatrix} \right). \tag{5.27}$$

In Chapter 3, $\mathfrak{O}_K = \mathbb{Z}$, $\mathfrak{I} = \{2\mathbb{Z}\}$ (so $f = 1$ and $B = \mathbb{F}_2$), and $\widehat{X} = \mathbb{F}_2^{mn}$. In Chapter 4, $\mathfrak{O}_K = \mathbb{Z}[\zeta_{p(p-1)}]$, $\mathfrak{I} = \left\{Q_1, \ldots, Q_{\phi(p-1)}\right\}$ for Q_l defined in Lemma 4.2.3 (so $f = \phi(p-1)$ and $B = \mathbb{F}_p$), and $n = 1$, so $\widehat{X} = \mathbb{F}_p^m$.

Let $A : \widehat{X} \longrightarrow \mathcal{X}$ be a B-linear injection. We denote the image of $\widehat{v}$ under A as $\widehat{v}_A$ and the image of $\widehat{C}$ under A as $\widehat{C}_A$. We pick

$$\widetilde{v}_A \in \mathfrak{O}_K^{mn}, \tag{5.28}$$

to be some element such that $\rho(\widetilde{v}_A) = \widehat{v}_A$. Let I^{mn} denote the set of column vectors of length mn with entries in I, for I in (5.21). Hence,

$$\rho^{-1}(\widehat{v}_A) = I^{mn} + \widetilde{v}_A. \tag{5.29}$$

Since $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module, $\mathfrak{O}_K$ can be embedded into a real lattice. (For a standard embedding into $\mathbb{R}^{[K:\mathbb{Q}]}$, we refer the reader to ([39], Chapter 5).) We extend this to a componentwise embedding of $\mathfrak{O}_K^{mn}$ into $\mathbb{R}^{mn[K:\mathbb{Q}]}$. We call this embedding $E(\cdot)$. Note that $\rho^{-1}\left(\widehat{C}_A\right) \subseteq \mathfrak{O}_K^{mn}$ is also a finitely generated $\mathbb{Z}$-module since $C \subseteq X$ is a linear code. Hence, the

image of $\rho^{-1}\left(\widehat{C}_A\right)$ in $\mathbb{R}^{mn[K:\mathbb{Q}]}$ under $E(\cdot)$ is a real lattice as well. We've seen it's convenient to rescale $E\left(\rho^{-1}\left(\widehat{C}_A\right)\right)$.

Definition 5.5.1. For a constant $\gamma_A \in \mathbb{R}_{>0}$, define the lattice attached to a linear code $C \subseteq X$ with respect to the B-linear injection A to be

$$\mathcal{A}_C = \gamma_A E\left(\rho^{-1}\left(\widehat{C}_A\right)\right) \subseteq \mathbb{R}^{mn[K:\mathbb{Q}]}. \tag{5.30}$$

We now recall the definition of a dual real lattice from (3.7).

Definition 5.5.2. If Λ is a real lattice of dimension r as in (3.5), we define the *dual lattice* to be

$$\Lambda^* = \{x \in \mathbb{R}^r \mid x \cdot y \in \mathbb{Z},\ \forall y \in \Lambda\},$$

where $(\cdot)$ denotes the standard vector dot product on $\mathbb{R}^r$.

Recall the definition of $C^\perp$ in (5.20). Theorem 5.4.3 says we can identify $C^\perp \subseteq X$. Hence, we can identify $\widehat{C^\perp} \subseteq \widehat{X}$. We now define another space of $\mathcal{X}$ corresponding to C. Let

$$\widehat{C}_D = \left(\left(\widehat{C^\perp}\right)_A\right)^\perp. \tag{5.31}$$

[Note where the inner $^\perp$ and outer $^\perp$ take place.]

Recall that K is an abelian extension of $\mathbb{Q}$, so let $\overline{(\cdot)}$ denote complex conjugation. *In all the cases we had success with analytic proofs of MacWilliams Identities, we have needed the following statement to hold:*

$$\mathcal{A}_C = \left[\gamma_D E\left(\overline{\rho^{-1}\left(\left(\widehat{C^\perp}\right)_D\right)}\right)\right]^*, \tag{5.32}$$

for some $\gamma_D \in \mathbb{R}_{>0}$.

Note that (5.32) holds in Lemma 3.2.1 (Chapter 3) and in Theorem 4.4.3 (Chapter 4). In Lemma 3.2.1, $\gamma_A = \gamma_D = \frac{1}{\sqrt{2}}$, and in Theorem 4.4.3, $\gamma_A = 1$ and $\gamma_D = \mathrm{N}_{\mathbb{Q}}^L\left(\frac{1}{\Phi'_{p-1}(\zeta_{p-1})}\right)$. Hence, in Chapter 3 and Chapter 4 this relation held. For more examples of attaching lattices to codes, see [35], [18], [27], [13], [50], [37], [38], [11], [10].

5.5.2 Attaching Theta Functions to Codes and Weight Enumerators

We will denote the theta function attached to the code by $\Theta_C(\cdot)$, and the theta function attached to the codeword $v \in X$ by $\Theta_v(\cdot)$. For examples of such theta functions we refer the reader to Chapter 3 and Chapter 4. Note that the domain of $\Theta_C(\cdot)$ and $\Theta_v(\cdot)$ will always be embedded into a Siegel upper half space of sufficiently large dimension [44], [45], [46], [49]. Hence, we assume $\Theta_C(\cdot)$ and $\Theta_v(\cdot)$ to be defined over a domain $\Delta \subseteq \mathfrak{H}_g$ for $g \in \mathbb{Z}_{>0}$ and $\mathfrak{H}_g$ as defined in (2.18). Let $Z \in \Delta$. We have

$$\Theta_C(Z) = \sum_{v \in C} \Theta_v(Z).$$

[In Chapter 3, note that we write $\Theta_C(Z) = \sum_{v \in C} \Theta_v(2Z)$. This is simply a result of playing around with a constant to make the proof look nicer. The important fact is we can write $\Theta_C(\cdot)$ as a sum over $v \in C$ of $\Theta_v(\cdot)$.]

Recall that $H \subseteq \mathrm{Aut}(X)$ partitions X into T, which is associated to the abelian scheme (X, S). Let $\widehat{H} \subseteq \mathrm{Aut}\left(\widehat{X}\right)$ be a representation of H which acts correspondingly on the set of "stacked" matrices, $\widehat{X}$. Assume that the group $\widehat{H}$ can be represented as a subgroup $\widetilde{H} \subseteq \mathrm{GL}_g(\mathbb{Z})$. An element $\widetilde{h} \in \widetilde{H}$ acts on $\mathfrak{H}_g$ via the symplectic matrix

$$\begin{bmatrix} {}^t\widetilde{h} & 0 \\ 0 & \widetilde{h}^{-1} \end{bmatrix}.$$

In this sense, $\widetilde{H}$ is "lifted" from $\widehat{H}$. Further, assume that $\widetilde{H}$ surjects onto $\widehat{H}$ under the reduction map $\rho(\cdot)$. Finally, assume that there exists a nontrivial subdomain $\mathcal{S} \subseteq \Delta$ such that ${}^t\widetilde{h}\tau\widetilde{h} = \tau$ for all $\widetilde{h} \in \widetilde{H}$ and for all $\tau \in \mathcal{S}$. *If all of these assumptions are met*, then for $\tau \in \mathcal{S}$, for all $u, v \in X$, and for all $0 \leq r \leq N$, we have

$$u, v \in T_r \Longrightarrow \Theta_u(\tau) = \Theta_v(\tau). \tag{5.33}$$

For our matrix code results in Chapter 3, the subdomain $\mathcal{S}$ had the form τA for $\tau \in \mathbb{H}$ an upper half plane variable and A a symmetric positive definite matrix. If (5.33) holds for some subdomain $\mathcal{S} \subseteq \Delta$, fix an $0 \leq r \leq N$ and let $v \in T_r$. We call $\Theta_v(\tau)$ the *theta function representing*

the set $T_r \in T$, and we denote it by $\Theta_r(\tau)$. Then we have

$$\Theta_C(\tau) = \mathrm{W}_C\left(\Theta_0(\tau), \Theta_1(\tau), \ldots, \Theta_N(\tau)\right).$$

We now recall our setup from Section 5.3.2. Let $Y = \mathrm{Mat}_{m\times 1}(B)$, (Y, U) be an abelian scheme, and V be the partition of Y associated to the abelian scheme (Y, U). Note that $X = Y^n$ and assume that (X, S) is the Delsarte extension scheme of (Y, U). (Recall that $(X, S_{d_{\mathrm{H}}})$ and $(X, S_{d_{\mathrm{cd}}})$ are both Delsarte extension schemes.) Then $\mathrm{W}_C(\cdot)$ can be specified to $\mathrm{TW}_C(\cdot)$ and we could hope to do the same for $\Theta_C(\tau)$. Let V_s be the s^{th} component in the partition V of Y for $0 \leq s \leq M$ and let $\tau \in \mathcal{S}$. We denote the theta function attached to V_s by $\Theta_s(\tau)$. But, we need each $\Theta_r(\tau)$ to factor into a product of $\Theta_s(\tau)$'s, $0 \leq s \leq M$, in order to write the *total weight enumerator* in terms of the theta functions $\Theta_s(\tau)$'s. If so, we have

$$\Theta_C(\tau) = \mathrm{TW}_C\left(\Theta_0(\tau), \ldots, \Theta_M(\tau)\right).$$

For an example of theta functions that factor, we refer the reader to Chapter 3 in the case of linear column distance weight codes $C \subseteq \mathrm{Mat}_{2\times n}(\mathbb{F}_2)$, and Chapter 4 in the case of linear Hamming weight codes $C \subseteq \mathbb{F}_p^n$.

5.5.3 Inversion Formulas and Algebraic Independence

Assume that we can write either the linear or total weight enumerator in terms of theta functions. To analytically prove a MacWilliams Identity for such a weight enumerator, we apply the inversion formulas for the theta functions involved. The analytic proof of the MacWilliams Identity follows by evaluating $\Theta_C\left(-\frac{1}{\tau}\right)$ in two different ways (see the proofs of Theorems 3.6.1, 3.6.2, and 4.6.1).

The final step is to prove the algebraic independence of the theta functions. This algebraic independence argument can be highly nontrivial (see (1) in Section 5.5.4). We believe more analytic proofs would exist if not for this issue. There are many papers which show that the exact weight enumerator and the total Lee weight enumerator can be written in terms of theta functions [14], [15],

[9], [12], [11], [10], [17], [23]. However, *none* of these provide an analytic proof of the MacWilliams Identities for these weight enumerators. We believe this is due to the difficulty of the algebraic independence argument.

5.5.4 Problems and Issues

We list three debilitating problems we encountered with such an analytic argument.

(1) It is *extremely* difficult to find a nontrivial subdomain $\mathcal{S} \subseteq \Delta$. Recall that $H \subseteq \mathrm{Aut}(X)$ is the group whose partition T is associated to the abelian scheme (X, S). Note that $|\mathcal{X}| \geq |B|^{mn}$ Let $Z \in \Delta$. Initially, the number of distinct $\Theta_v(Z)$'s is bounded below by $|B|^{mn}$. Note that

$$\sum_{k=1}^{g} k = \frac{g(g+1)}{2}$$

is an upper bound on the dimension of the domain of $\Theta_v(Z)$. Also, $mn[K : \mathbb{Q}] \approx g$. If $|H|$ is large, then to find a suitable $\mathcal{S} \subseteq \Delta$ we must solve many equations of the type $\Theta_v(Z) = \Theta_u(Z)$. Hence, we are forced to consider large number fields for there to exist a nontrivial subdomain $\mathcal{S} \subseteq \Delta$. We found it to be unlikely that such a nontrivial subset $\mathcal{S} \subseteq \mathfrak{H}_g$ exists in all cases.

(2) It is difficult to equate the dual of a lattice attached to a code C to a lattice attached to the dual code $C^{\perp}$ (i.e. a statement similar to (5.32)). (The proof of Theorem 4.4.3 in Chapter 4 was the most difficult challenge to overcome for this thesis.)

(3) It is difficult to prove the algebraic independence of the theta series involved. Of course, unless one is lucky or careful they may not be algebraically independent! Let δ be the dimension of $\mathcal{S}$. Then, any set of more than $\delta + 1$ functions defined on $\mathcal{S}$ are *necessarily* algebraically dependent. So, if the number of representative theta functions used to define the weight enumerator is greater than $\delta + 1$, there is no hope for algebraic independence. In all of our results, $\delta = 1$.

We call the process of providing analytic proofs for MacWilliams Identities "The Game." To conclude, we summarize the rules of the game.

5.6 The Game

> "I'll do what I can to help y'all. But, the game's out there, and it's play or get played. That simple."
> - Omar Little, The Wire

To assist future researchers, we now state the rules of the game.

(1) Choose a number field K that is abelian over $\mathbb{Q}$ (with ring of integers $\mathfrak{O}_K$) and a Galois invariant set of pairwise relatively prime integral ideals $\mathfrak{I} = \{I_1, \ldots, I_f\}$ such that $\mathfrak{O}_K/I_l$ are isomorphic for all $1 \leq l \leq f$. Set $B = \mathfrak{O}_K/I_l$ and I as in (5.21).

(2) Let $X = \mathrm{Mat}_{m\times n}(B)$ and $C \subseteq X$ be a linear code. Let (X, S) be a self dual abelian scheme coming from a group action H (it must be self dual so that the weight enumerators on both sides of the MacWilliams Identity are the same). Does $(X, S) = (X, S_d)$ for some diversity function $d(\cdot, \cdot)$? If so, this abelian scheme will be of more interest!

(3) Choose an isomorphism between the group of characters X' and the group X to consider $C^{\perp} \subseteq X$. Consider $\widehat{C}, \widehat{C^{\perp}} \subseteq \widehat{X} = B^{mn}$ via the "stacking map" $\Phi(\cdot)$ in (5.22).

(4) Choose an embedding A of $\widehat{C}$ into $\mathcal{X}$ such that the space $\widehat{C}_D$ is well defined as in (5.31).

(5) Choose an embedding $E(\cdot)$ and a real number $\gamma_A \in \mathbb{R}_{>0}$ to define $\mathcal{A}_C$ as in (5.30). (For an example of such an embedding see (4.23).) Then the notion of a dual lattice (and volume of a lattice!) is well defined.

(6) Choose a $\gamma_D \in \mathbb{R}_{>0}$ such that $\mathcal{A}_C$ satisfies (5.32).

(7) Define the necessary theta functions $\Theta_C(\cdot)$'s and $\Theta_v(\cdot)$'s. (For examples of theta functions to consider, see (2.16), (2.17), (2.19), and Definition 2.2.1.)

(8) Find a subdomain $\mathcal{S}$ such that (5.33) holds. This is very difficult (and perhaps impossible)!

(9) Check if the abelian scheme (X, S) is a Delsarte extension scheme. If so, do the $\Theta_r(\tau)$ factor in a natural way corresponding to the total weight enumerator? If so, what are the $\Theta_s(\tau)$'s? Write either the linear weight enumerator or the total weight enumerator in terms of these theta functions.

(10) Prove the inversion formulas for all theta functions involved.

(11) Prove that the theta functions involved are algebraically independent.

(12) Follow the proofs of Theorems 3.6.1, 3.6.2, and 4.6.1 to analytically prove the MacWilliams Identity for linear codes $C \subseteq X$.

To conclude, this dissertation generates more questions than answers. We were successful in extending the class of codes for which there exists an analytic proof of the MacWilliams Identity. However, we were unable to confidently state when there exists (or does not exist) such an analytic proof. We believe that attaching theta functions to linear codes contained in abelian schemes is the way to continue working on this problem. We would like to thank the reader for their interest in our results.

Bibliography

[1] A.N. Andrianov. Quadratic Forms and Hecke Operators. Springer-Verlag, 1987.

[2] E. Bannai and T. Ito. Algebraic Combinatorics I, Association Schemes. The Benjamin/Cummings Publishing Company, 1984.

[3] E. Berlekamp, F.J. MacWilliams, and N. Sloane. Gleason's theorem on self-dual codes. IEEE Transactions on Information Theory, 18:409–414, 1972.

[4] K. Betsumiya and Y. Choie. Codes over $\mathbb{F}_4$, Jacobi forms and Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$. European Journal of Combinatorics, 26:629–650, 2005.

[5] K. Betsumiya and Y. Choie. Jacobi forms over totally real fields and type II codes over Galois rings $\mathrm{GR}(2^m, f)$. European Journal of Combinatorics, 25:475–486, 2005.

[6] C. Blex. Eine explizite Version der Jacquet-Langlands-Korrespondenz für den dreidimensionalen hyperbolischen Raum. PhD thesis, Westfälischen Wilhelms-Universität Münster, 2004.

[7] M. Broué and M. Enguehard. Polynômes des poids de certains codes et fonctions theta de certains réseaux. Ann. Scie Ecole Norm. Sup., 5:157–181, 1972.

[8] P. Camion. Codes and association schemes: Basic properties of association schemes relevant to coding. In Handbook of Coding Theory Volume II, 1998.

[9] Y. Choie and S. Dougherty. Codes, lattices and modular forms. IEEE Information Theory Workshop, ITW2003:259–282, 2003.

[10] Y. Choie and S. Dougherty. Codes over σ_{2m} and Jacobi forms over the quaternions. AAECC, 15:129–147, 2004.

[11] Y. Choie and S. Dougherty. Codes over rings, complex lattices and Hermitian modular forms. European Journal of Combinatorics, 26:145–165, 2005.

[12] Y. Choie, S. Dougherty, and H. Kim. Complete joint weight enumerators and self-dual codes. IEEE Transactions on Information Theory, 49(5):1275–1282, 2003.

[13] Y. Choie and E. Jeong. Jacobi forms over totally real fields and codes over $\mathbb{F}_p$. Illinois Journal of Mathematics, 46.2:627–643, 2002.

[14] Y. Choie and H. Kim. Codes over $\mathbb{Z}_{2m}$ and Jacobi forms of genus n. Journal of Combinatorial Theory, Series A 95:335–348, 2001.

[15] Y. Choie and N. Kim. The complete weight enumerator of type II codes over $\mathbb{Z}_{2m}$ and Jacobi forms. IEEE Transactions on Information Theory, 47(1):396–399, 2001.

[16] Y. Choie and M. Oura. The joint weight enumerators and Siegel modular forms. AMS, 1934(9):2711–2718, 2006.

[17] Y. Choie and P. Solé. Ternary codes and Jacobi forms. Discrete Mathematics, 282:81–87, 2004.

[18] J.H. Conway and N.J.A. Sloane. Sphere Packings, Lattices, and Groups. Springer-Verlag, 1999.

[19] T. Cover and J. Thomas. Elements of Information Theory. Wiley-Interscience, 2006.

[20] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory, Series A, 25:226–241, 1978.

[21] P. Delsarte and V. Levenshtein. Association schemes and coding theory. IEEE Transactions on Information Theory, 44(6):2477–2504, 1998.

[22] S. Dougherty. Macwilliams relations for joint weight enumerator for codes over rings.

[23] W. Duke. On codes and Siegel modular forms. International Mathematics Research Notices, 1933(5):125–136, 1993.

[24] D. Dummit and R. Foote. Abstract Algebra. John Wiley & Sons, Inc., 1999.

[25] I. Duursma. From weight enumerators to zeta functions. Discrete Applied Mathematics, 111:55–73, 2001.

[26] I. Duursma. A Riemann hypothesis analogue for self-dual codes. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 56:115–124, 2001.

[27] W. Ebeling. Lattices and Codes: A course partially based on lectures by F. Hirzebruch. Vieweg, 1994.

[28] E. Freitag and R. Busam. Complex Analysis. Springer-Verlag, 2005.

[29] S. Friedberg. On theta functions associated to indefinite quadratic forms. Journal of Number Theory, 23:255–267, 1986.

[30] E. Gabidulin. Theory of codes with maximal rank distance. Problems of Information Transmission, 21(1):1–12, 1985.

[31] M. Gadouleau and Z. Yan. Macwilliams Identity for codes with the rank metric. EURASIP Journal on Wireless Communications and Networking, 2008:13, 2008.

[32] D. Grant and M. Varanasi. Duality theory for space-time codes over finite fields. Advances in the Mathematics of Communications, 2:35–54, 2008.

[33] D. Grant and M. Varanasi. The equivalence of space-time codes and codes over finite fields and Galois rings. Advances in the Mathematics of Communications, 2:131–145, 2008.

[34] S. Lang. Algebraic Number Theory. Springer-Verlag, 1986.

[35] J. Leech and N.J.A. Sloane. Sphere packings and error-corrective codes. Canadian Journal of Mathematics, 23:718–745, 1971.

[36] R. Lidl and G. Pilz. Applied Abstract Algebra. Springer, 1998.

[37] D. Maher. Lee polynomials of codes and theta functions of lattices. Canadian Journal of Mathematics, 30(4):738–747, 1978.

[38] D. Maher. Modular forms from codes. Canadian Journal of Mathematics, 32(1):40–58, 1980.

[39] D. Marcus. Number Fields. Springer-Verlag, 1997.

[40] D. Mumford. Tata Lectures on Theta 1. Birkhäuser, 1983.

[41] D. Mumford. Tata Lectures on Theta 2. Birkhäuser, 1984.

[42] H. Opolka. The finite Fourier-transform and theta functions. Mathematical Institute, University of Göttingen, 1986.

[43] E.M. Rains and N.J.A. Sloane. Self-dual codes. In Handbook of Coding Theory, 1998.

[44] O. Richter. Theta functions of indefinite quadratic forms over real number fields. Proceedings of the American Mathematical Society, 128:701–708, 1999.

[45] O. Richter. Theta functions of quadratic forms over imaginary quadratic fields. Acta Arithmetica, XCII.1, 2000.

[46] O. Richter. Theta functions with harmonic coefficients over number fields. Journal of Number Theory, 95:101–121, 2002.

[47] J.P. Serre. Cours d'Arithmetique. Presses Univ. France, 1970.

[48] C.L. Siegel. On the theory of indefinite quadratic forms. The Annals of Mathematics, Second Series, 45(3):577–622, 1944.

[49] H. Skogman. Jacobi Forms over Number Fields. PhD thesis, University of California San Diego, 1999.

[50] N.J.A. Sloane. Codes over GF(4) and complex lattices. Journal Algebra, 52:168–181, 1978.

[51] H.M. Stark. Modular forms and related objects. CMS Conference Proceedings, 7:421–455, 1987.

[52] B. van Asch and F. Martens. Lee weight enumerators of self-dual codes and theta functions. Advances in Mathematics of Communications, 2(4):393–402, 2008.

[53] L.C. Washington. Introduction to Cyclotomic Fields. Springer-Verlag, 1997.