Weighted Generating Functions and Configuration Results for Type II Lattices and Codes

An honors thesis presented
by

Scott Duke Kominers

to
The Department of Mathematics
in partial fulfillment of the requirements
for the degree of
Bachelor of Arts with Honors
in the subject of

Mathematics

Harvard University
Cambridge, Massachusetts
March 2009

Thesis Advisor: Professor Noam D. Elkies

Abstract

We present an exposition of weighted theta functions, which are weighted generating functions for the norms and distribution of lattice vectors. We derive a decomposition theorem for the space of degree-d homogeneous polynomials in terms of spaces of harmonic polynomials and then prove that the weighted theta functions of Type II lattices are examples of modular forms. Our development of these results is structural, related to the infinite-dimensional representation theory of the Lie algebra $\mathfrak{sl}_2$. We give several applications of weighted theta functions: a condition on the root systems of Type II lattices of rank 24; a proof that extremal Type II lattices yield spherical t-designs; and configuration results for extremal Type II lattices of ranks 8, 24, 32, 40, 48, 56, 72, 80, 96, and 120, one of which has not appeared previously.

Then, we give a new structural development of harmonic weight enumerators—the coding-theoretic analogs of weighted theta functions—in analogy with our approach to weighted theta functions. We use the finite-dimensional representation theory of $\mathfrak{sl}_2$ to derive a decomposition theorem for the space of degree-d discrete homogeneous polynomials in terms of the spaces of discrete harmonic polynomials and then prove a generalized MacWilliams identity for harmonic weight enumerators. Next, we present several applications of harmonic weight enumerators analogous to those given for weighted theta functions: an equivalent characterization of t-designs and the extremal Type II code case of the Assmus–Mattson Theorem; a condition on the tetrad systems of Type II codes of length 24; and configuration results for extremal Type II codes of lengths 8, 24, 32, 48, 56, 72, and 96. Nearly all of these applications are original to this thesis, and many explicitly use components of our development of the harmonic weight enumerator theory.

Acknowledgments

First and foremost, I owe uncountably many thanks to my advisor, Professor Noam D. Elkies, without whose continuous teaching, advice, collaboration, support, and friendship I would never have dreamed of undertaking the project contained herein. Additionally, I am deeply grateful to my high school mathematics teacher, Mrs. Susan Schwartz Wildstrom, for fostering and encouraging my love of mathematics and for always pushing me to think beyond what has already been proven.

I especially appreciate the helpful comments and suggestions of Professors Henry Cohn, John H. Conway, Benedict H. Gross, Abhinav Kumar, Gabriele Nebe, Ken Ono, Vera Pless, Eric M. Rains, and two anonymous referees on components of this work, and thank Professors John Rickert and Jenny Sendova and Mr. Christopher C. Mihelich for their training in the art of mathematical presentation. I also thank my other research advisors, Professors Susan Athey, Erik D. Demaine, Edward L. Glaeser, William R. Kerr, Alvin E. Roth, David Smith, Kay Kaufman Shelemay, and Andrei Shleifer, for their support and guidance over the course of my undergraduate years.

The work leading up to this thesis spanned several years, during which my research was supported by two fellowships from the Harvard College Program for Research in Science and Engineering (PRISE), funding from the Harvard Mathematics Department Tutorial Program, funding from the Center for Excellence in Education Research Science Institute (RSI), and a Harvard Mathematics Department Highbridge fellowship. Additionally, I received funding towards presentations of this work from the Mathematical Association of America. I am extremely grateful for all this generous financial support, and moreover for the energetic and encouraging research environments provided at PRISE and RSI. The organizational staffs of both PRISE and RSI have also been integral to my research endeavors, and two members of these staffs require particular acknowledgment for their unceasing inspiration and advice: Mr. Gregory Llacer and Mrs. Maite Ballestero.

Finally, many of my friends commented upon components of this thesis work: notably, Zachary Abel, Pablo Azar, Ernest E. Fontes, David Hansen, Rezwan Haque, Kelley Harris, John Hawksley, Nathan Kaplan, Stella J. M. Lee, Maria Monks, Gil Moss, Steffano U. Saldrium, Julia Schlozman, Robert W. Sinnott, Shrenik N. Shah, and Dmitry Taubinsky. Andrea J. Hawksley, Ellen and William Kominers, and particularly my brother, Paul M. Kominers, have made substantial contributions, both personal and professional, in the years since I began this work. Thank you all, $\mathbb{QED}$.

Contents

Chapter 0

Preface

This thesis is concerned with two mathematical theories: those of *lattices* and *binary linear codes*. A *lattice* is a regularly spaced array of points in n-dimensional Euclidean space $\mathbb{R}^n$ formed by taking all integer linear combinations of a collection of vectors, as in Figure 1. Lattices are by definition infinite. *Binary linear codes* (or just *codes*, throughout the remainder of this Preface) are finite analogs of lattices: a code is formed by taking all linear combinations of a set of vectors in $\mathbb{F}_2^n$, the finite space of length-n binary strings. That is, a code is a linear subspace of $\mathbb{F}_2^n$.

Many lattices are well-known throughout mathematics. For example, the set $\mathbb{Z}^2$ of integer points in the two-dimensional Euclidean plane, pictured in Figure 2, is a lattice generated by unit vectors on the axes. This lattice appears early in mathematics education—on graph paper. Additionally, three-dimensional lattices have a variety of applications. They appear in the organizations of solid compounds[1] and yield optimal packings of spherical objects such as identically-sized oranges.[2] Although less directly visible, codes also appear in common applications: most notably, they underlie electronic communication channels.[3]

The theories of lattices and codes are deeply connected. Many concepts from these theories are in direct correspondence, leading to a systematic analogy between the theories. Lattices can be constructed from codes, and such constructions often map properties of codes into the corresponding properties of lattices. Additionally, the theories of lattices and codes exhibit surprising

[1] For example, the face-centered cubic lattice is a common crystal structure and hence appears in most chemistry textbooks (see [CS99, p. 11] for further discussion).

[2] The optimality of a particular lattice packing among all possible packings in $\mathbb{R}^3$ is actually a recent result. This problem stood open as the *Kepler Conjecture* until 2005, when Hales [Hal05] provided a proof (see also [HHM$^+$09], which presents some corrections to [Hal05]).

[3] Conway and Sloane [CS99, pp. 11–12] discuss these applications in detail and provide numerous references.

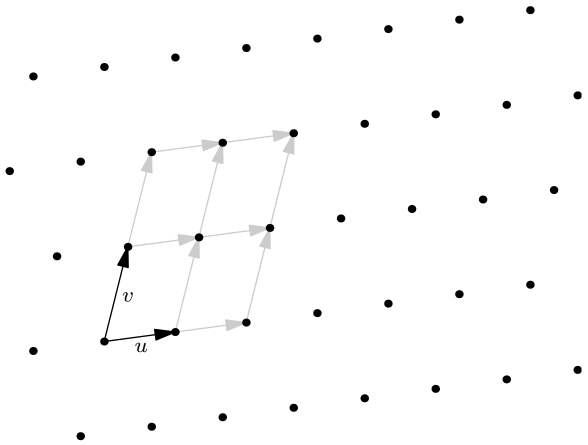

Figure 1: A two-dimensional lattice formed by integer linear combinations of the vectors v and u.

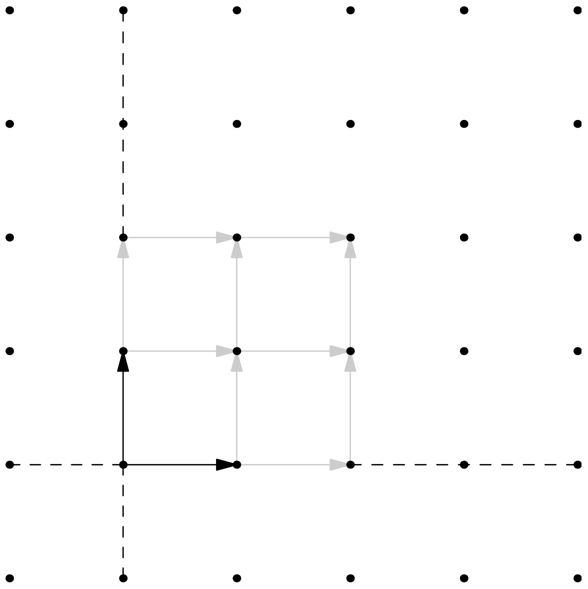

Figure 2: The two-dimensional lattice $\mathbb{Z}^2$ of integer points in the Euclidean plane $\mathbb{R}^2$.

connections to other branches of mathematics, especially number theory. To provide an example of both types of connection, we now introduce the *theta functions* of lattices.

Each lattice L has an associated generating function $\theta_L(z)$, called the *theta function* of L, defined by

$$\theta_L(z) := \sum_{x \in L} e^{\pi i z \langle x, x \rangle}. \tag{0.1}$$

Here, i denotes the principal complex square root of -1 and $\langle x, x \rangle := \sum_{j=1}^n x_j^2$ is the *norm* of the vector $x = (x_1 \ldots, x_n) \in L$, representing the squared length of x. Thus, $\theta_L(z)$ can be interpreted as encoding the lengths of the vectors of L. Indeed, rearrangement of (0.1) gives

$$\theta_L(z) = 1 + \sum_{k>0} a_k(L) e^{k\pi i z},$$

where $a_k(L)$ is the number of vectors in L having norm k. For example, the theta function of the $\mathbb{Z}^2$ lattice is given by

$$\Theta_{\mathbb{Z}^2}(z) = 1 + 4e^{1\pi i z} + 4q^{2\pi i z} + 0q^{3\pi i z} + 4q^{4\pi i z} + 8q^{5\pi i z} + 0q^{6\pi i z} + \cdots ; \tag{0.2}$$

the coefficient of $e^{k\pi i z}$ in (0.2) encodes the number of ways of writing k as a sum of two squares of integers.

By a mathematical miracle, the theta functions of certain lattices, called *Type II lattices*, turn out to be examples of a class of functions, called *modular forms*, which are of particular interest in number theory. Using results from the theory of modular forms, it is often possible to determine the theta function of a lattice having prescribed properties. This approach is so effective that theta functions may sometimes be used to classify lattices having certain properties, or to rule out existence of such lattices altogether.[4] Likewise, each code C has an associated generating function called a *weight enumerator*. These functions are similar to the theta functions of lattices, and the weight enumerator of a code C typically leads directly to the theta series of lattices constructed from C. Moreover, there is a class of codes called *Type II codes* which give rise to Type II lattices and have weight enumerators which behave, in a sense, like finite analogs of modular forms.

The lattice–code analogy is beautiful and somewhat surprising, and is also of substantial mathematical importance. Problems are typically posed or solved either for lattices or for codes; appeal to the analogy then offers insight towards parallel problems. For example, an important 1969 theorem of Assmus and Mattson [AM69] showed that the elements of certain codes are examples of

[4] Examples of such results can be found in our exposition: Theorems 3.10 and Theorems 3.11 are results of the former type and the first assertion of Theorem 3.6 is a result of the latter type.

a class of combinatorial objects, called *t-designs*, which satisfy strict distribution constraints. This result led Venkov [Ven84b] to seek and obtain an analogous theorem for lattices in 1984. In the proof of his result, Venkov established new, lattice-specific techniques using a class of generalized theta functions called *weighted theta functions*. In 1999, Bachoc [Bac99] brought these developments full circle by adapting Venkov's methods to the coding setting. She introduced coding-theoretic analogs of weighted theta functions, called *harmonic weight enumerators*, and used them to give a new proof of the Assmus–Mattson Theorem which originally inspired Venkov.

This thesis adds another layer to this story, giving a new development and interpretation of Bachoc's theory of harmonic weight enumerators, along with new applications. Our approaches and results are inspired by the theory of lattices; they consequently fill several holes in the lattice–code analogy.

Chapter 1

Introduction

1.1 Overview of the Thesis

After reviewing relevant terminology and notation in Chapter 2 and giving expository presentations in Chapters 3 and 4, we fill several holes in the analogy between lattices and codes in Chapters 5 and 6. Specifically, we make four original contributions, which we list here and explain in further detail below.

1. First, in Chapter 5, we give new structural developments of the theories of discrete harmonic polynomials and harmonic weight enumerators, in analogy with those for harmonic polynomials and weighted theta functions.

2. Then, in Section 6.1, we use these developments to give a new proof of a characterization of t-designs due to Delsarte [Del78] which is analogous to a well-known characterization of spherical t-designs.

3. Next, in Section 6.2 we use harmonic weight enumerators in analogy with an argument of Venkov [Ven80] to give a new, purely coding-theoretic proof of a condition of Koch [Koc87] on the tetrad systems of length-24 Type II codes.[1]

4. Finally, in Section 6.3, we present new configuration results for extremal Type II codes analogous to those obtained for extremal Type II lattices by Venkov [Ven84a], Ozeki [Oze86a], [Oze89], [Oze86b], and the author [Kom09].

[1] Although this result has already been presented in a paper of Elkies and the author [EK09a], we consider it a contribution of the thesis work since the inspiration for the argument and the work on the paper arose as part of the thesis research.

We use the lattice–code analogy heavily throughout the presentations of our new contributions, and so the thesis is organized in order to exploit this analogy wherever possible.

1.2 Outline of the Thesis

We review the standard terminology and notations of lattices and codes in Sections 2.1 and 2.2 of Chapter 2, respectively. Then, we discuss aspects of the lattice–code analogy in Section 2.3, providing an important construction of lattices from codes. Finally, we define t-designs and their lattice analogs, spherical t-designs, in Section 2.4.

In Chapter 3, we give an exposition of the theory of weighted theta functions of lattices, following an approach related to $\mathfrak{sl}_2$ which we later apply to the theory of harmonic weight enumerators. In Section 3.1.3, we develop the classical theory of theta functions. We then present the developments of harmonic polynomials and weighted theta functions in Sections 3.2 and 3.3, respectively. In Section 3.4, we introduce the zonal spherical harmonic polynomials, a special class of harmonic polynomials used in many of our applications of weighted theta functions.

We then give several applications of weighted theta functions in Chapter 4. We discuss the classification of rank-24 Type II lattices in Section 4.1 and prove a condition of Venkov [Ven80] on the possible root systems of such lattices. Next, in Section 4.2, we apply the theory developed in Section 3.2 to show that, for any extremal Type II lattice L and $m > 0$, the set of norm-m vectors of L is a spherical design whenever it is nonempty. Finally, we prove configuration results for extremal Type II codes of ranks $n = 8, 24, 32, 40, 48, 56, 72, 80, 96, 120$ in Section 4.3. Although most of the configuration results we present are already in the literature, half of these results are original to the author and a collaborator.[2] Our expository presentation of these results collects and unifies the previous work. Additionally, we obtain a new configuration result of Elkies and the author [EK09b] at the end of Section 4.3.

We present our new development of harmonic weight enumerators in Chapter 5, in analogy with the presentation of Chapter 3. As a warm-up, we review classical results from the theory of weight enumerators in Section 5.1.2. We review the the finite-dimensional representation theory of $\mathfrak{sl}_2$ in Section 5.1.3, and then use this to develop the theory of discrete harmonic polynomials in Section 5.2. We proceed with the development of harmonic weight enumerators in Section 5.3. Finally, in Section 3.4, we develop the zonal harmonic polynomials, a useful class of discrete harmonic

[2] Specifically, the configuration results for Type II lattices of ranks $n = 56, 72, 96$ are original to the author [Kom09] and those for ranks $n = 80, 120$ are original to the author and Abel [KA08].

polynomials analogous to the zonal spherical harmonic polynomials of Section 3.4. Although many of the key results proven in Chapter 5 have been obtained previously by either Delsarte [Del78] or Bachoc [Bac99], our proofs of these results are novel and original to this thesis. While the approaches of Delsarte [Del78] and Bachoc [Bac99] are combinatorial, our methods are structural, analogous to those used in the structural development of weighted theta functions for lattices.

Lastly, in Chapter 6, we obtain new applications of harmonic weight enumerators: coding-theoretic analogs of the results of Chapter 4. In Section 6.1, we use the machinery developed in Section 5.2 to give a new proof of a characterization of t-designs due to Delsarte [Del78]. This characterization is analogous to the characterization of spherical t-designs obtained in Section 4.2 and consequently leads to coding-theoretic analogs of the result that extremal Type II lattices yield spherical t-designs. We then use harmonic weight enumerators to give the first purely coding-theortic proof of a condition of Koch [Koc87] on the tetrad systems of length-24 Type II codes in Section 6.2. Our approach to Koch's condition uses harmonic weight enumerators in a fashion inspired by and analogous to the use of weighted theta functions in the proof of the Venkov [Ven80] condition on rank-24 Type II lattices. Finally, we prove configuration results for extremal Type II codes of lengths $n = 8, 24, 32, 48, 56, 72, 96$ in Section 6.3. These results are analogous to the configuration results of Section 4.3, are entirely original to this thesis, and are the first configuration results ever obtained for extremal Type II codes.

Chapter 2

Background and Conventions

In this chapter, we review relevant definitions and notations from the theories of lattices and codes. We discuss and give examples of lattices and codes in Sections 2.1 and 2.2, respectively. These sections are organized in analogy to each other, so as to highlight the similarities between concepts from the two theories. We survey the analogy between lattices and codes in Section 2.3. There, we also introduce *Construction A*, a fundamental construction of lattices from codes. Finally, we introduce the notions of *t-designs* and *spherical t-designs* in Section 2.4.

2.1 Lattices

2.1.1 Basic Definitions and Examples

Throughout, $\mathbb{R}$ and $\mathbb{C}$ denote the real and complex numbers. Additionally, $\{\varepsilon^{(1)}, \ldots, \varepsilon^{(n)}\}$ denotes the standard basis of n-dimensional real space, $\mathbb{R}^n$.[1] We denote the space of smooth functions from $\mathbb{R}^n \to \mathbb{C}$ by $\mathscr{C}^\infty(\mathbb{R}^n)$, or just by $\mathscr{C}^\infty$ when the dimension of the domain is clear from context.

A *rank-n lattice L* is a free $\mathbb{Z}$-module of rank n equipped with an inner product

$$\langle \cdot, \cdot \rangle : L \times L \to \mathbb{R}$$

for which the bilinear extension to $L \otimes \mathbb{R}$ is positive-definite and symmetric. A minimal spanning subset of a lattice L is called a *$\mathbb{Z}$-basis* (or just *basis*) of L. We call $\langle x, x \rangle$ the *norm* of a vector $x \in L$.

[1] We use the somewhat nonstandard notation "$\cdot^{(\cdot)}$" for bases, because we often have to discuss the coordinates of vectors, which are denoted with subscripts.

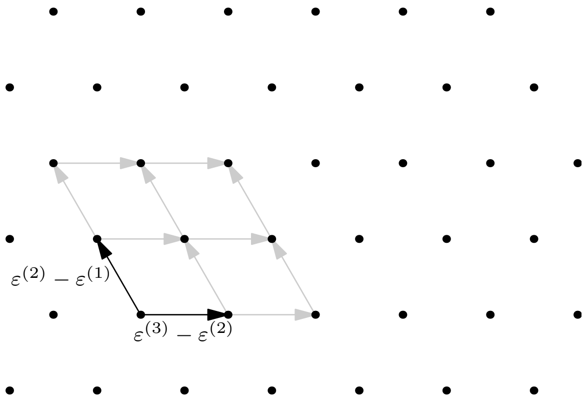
$\varepsilon^{(2)} - \varepsilon^{(1)}$
$\varepsilon^{(3)} - \varepsilon^{(2)}$

Figure 3: The planar hexagonal lattice, A_2.

For two lattices L and L' of ranks n and n', the orthogonal direct sum of L and L', denoted $L \oplus L'$, is a lattice of rank $n + n'$. Additionally, we write

$$L^k := \underbrace{L \oplus \cdots \oplus L}_{k \text{ times}}.$$

If two lattices L and L' are isomorphic, then we write $L \cong L'$. A lattice L is *reducible* if it can be expressed in the form $L \cong L' \oplus L''$ for nonzero $L', L'' \subset L$, and is *irreducible* otherwise.

The simplest example of a lattice is the rank-1 lattice $\mathbb{Z}$ with basis $\{\varepsilon^{(1)}\}$ and inner product induced by that of $\mathbb{R}$ (so that $\langle \varepsilon^{(1)}, \varepsilon^{(1)} \rangle = 1$). More generally, $\mathbb{Z}^n$ is the set of integral points in $\mathbb{R}^n$ with basis $\{\varepsilon^{(j)}\}_{j=1}^n$ and inner product given by

$$\langle \varepsilon^{(j)}, \varepsilon^{(k)} \rangle = \begin{cases} 1 & j = k, \\ 0 & j \neq k. \end{cases}$$

Another common lattice is A_2—the *planar hexagonal lattice*, pictured above in Figure 3—which is the rank-2 sublattice of $\mathbb{Z}^3$ generated by the basis $\{\varepsilon^{(2)} - \varepsilon^{(1)}, \varepsilon^{(3)} - \varepsilon^{(2)}\}$. More generally, we define the family of lattices $\{A_n\}_{n=1}^\infty$ by

$$A_n := \left\{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} : x_1 + \cdots + x_{n+1} = 0\right\};$$

A_n has rank n, with basis $\{\varepsilon^{(2)} - \varepsilon^{(1)}, \ldots, \varepsilon^{(n+1)} - \varepsilon^{(n)}\}$. Via a similar construction, we define a family of lattices $\{D_n\}_{n=3}^\infty$ by

$$D_n := \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \equiv 0 \bmod 2\}.^2$$

[2] We have explicitly excluded the choices $n = 1, 2$. To see why, we observe that taking either $n = 1$ or $n = 2$ in the definition of D_n produces a degenerate definition: $\left\{(x_1) \in \mathbb{Z}^1 : x_1 \equiv 0 \bmod 2\right\} = 2\mathbb{Z}$ and $\left\{(x_1, x_2) \in \mathbb{Z}^2 : x_1 + x_2 \equiv 0 \bmod 2\right\} = A_1 \oplus A_1$.

By construction, D_n is of rank n, with basis $\{\varepsilon^{(2)} - \varepsilon^{(1)}, \ldots, \varepsilon^{(n)} - \varepsilon^{(n-1)}, \varepsilon^{(1)} + \varepsilon^{(2)}\}$. From this, we see that $D_3 \cong A_3$ (although $D_n \neq A_n$ for $n > 3$).[3]

One last example which will be of particular interest in our discussion is the rank-8 lattice E_8 with basis $\left\{\varepsilon^{(2)} - \varepsilon^{(1)}, \ldots, \varepsilon^{(7)} - \varepsilon^{(6)}, \frac{1}{2}\left(\varepsilon^{(1)} + \cdots + \varepsilon^{(8)}\right)\right\}$. This lattice is the set of points in $\mathbb{R}^n$ with integer or half-integer coordinates and with even integer coordinate sum. That is,

$$E_8 = \left\{ (x_1, \ldots, x_8) \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2}\right)^8 : x_1 + \cdots + x_8 \equiv 0 \bmod 2 \right\},$$

where $(\mathbb{Z} + \frac{1}{2})^n := \{(x_1, \ldots, x_n) \in \mathbb{R}^n : (x_1 + \frac{1}{2}, \ldots, x_n + \frac{1}{2}) \in \mathbb{Z}^n\}$.[4]

A lattice L is said to be *integral* if $\langle x, x' \rangle \in \mathbb{Z}$ for all $x, x' \in L$; in this case, the map $L \to \mathbb{Z}/2\mathbb{Z}$ defined by $x \mapsto \langle x, x \rangle \bmod 2$ is a homomorphism. An integral lattice L is called *even* if this homomorphism just described is trivial. Equivalently, L is even if and only if all its vectors have norms which are even integers, i.e. if $\langle x, x \rangle \in 2\mathbb{Z}$ for all vectors $x \in L$. To check that either of these conditions holds for a lattice L, it suffices to show that the condition holds for a basis of L. If L is a lattice with basis $\{x^{(1)}, \ldots, x^{(n)}\}$ and $\langle x^{(j)}, x^{(k)} \rangle \in \mathbb{Z}$ for all $1 \leq j \leq k \leq n$, then the integrality of L follows easily from the bilinearity of the inner product $\langle \cdot, \cdot \rangle$ on L. For any integral lattice L and $x, x' \in L$, if $\langle x, x \rangle \in 2\mathbb{Z}$ and $\langle x', x' \rangle \in 2\mathbb{Z}$, then

$$\langle x + x', x + x' \rangle = \langle x, x \rangle + 2\langle x', x \rangle + \langle x', x' \rangle \in 2\mathbb{Z}.$$

The *dual lattice* of a lattice L, denoted by L^*, is defined by

$$L^* = \{x' \in L \otimes \mathbb{R} : \langle x', x \rangle \in \mathbb{Z} \text{ for all } x \in L\}.$$

From this definition, we see that an alternate condition necessary and sufficient for the integrality of L is that $L^* \supset L$. An integral lattice L with the property that $L^* = L$ is said to be *self-dual*.

Clearly, the lattice $\mathbb{Z}^n$ is integral but not even. Furthermore, if $\mathbb{Z}^n \otimes \mathbb{R} \ni x' \notin \mathbb{Z}^n$, then the j-th coordinate x'_j of x' is nonintegral for some $1 \leq j \leq n$. In this case, $\langle x', \varepsilon^{(j)} \rangle \notin \mathbb{Z}$; it follows that $(\mathbb{Z}^n)^* = \mathbb{Z}^n$, hence $\mathbb{Z}^n$ is self-dual. By examining the bases given above, we see that the lattices A_n and D_n are even, as is E_8. As we see next, A_n and D_n are not self-dual, but E_8 is.

For any basis $\{x^{(1)}, \ldots, x^{(n)}\}$ of a lattice L, the *fundamental parallelotope* is the region

$$\mathcal{P}(L, \{x^{(1)}, \ldots, x^{(n)}\}) := \left\{\lambda_1 x^{(1)} + \cdots + \lambda_n x^{(n)} : (\lambda_1, \ldots, \lambda_n) \in [0,1]^n\right\}.$$

[3] Note that we have chosen our basis presentations of D_3 and A_3 so that the isomorphism $D_3 \cong A_3$ is immediately apparent.

[4] Here, we have used the so-called *even coordinate system for* E_8 (see [CS99, p. 120]). Throughout our discussion, and particularly in our definitions of the lattices E_7 and E_6 below, we assume this coordinate system for E_8.

For the remainder of this section, we fix an identification of $(L \otimes \mathbb{R}, \langle \cdot, \cdot \rangle)$ with $\mathbb{R}^n$.[5] The $\mathbb{R}^n$-volume of the fundamental parallelotope of L (for any choice of basis) is equal to $\mathrm{vol}(\mathbb{R}^n/L)$ and is an invariant of L. For lattices $L \subset L'$, the index $[L' : L]$ is finite and

$$\mathrm{vol}(\mathbb{R}^n/L) = \mathrm{vol}(\mathbb{R}^n/L') \cdot [L' : L]. \tag{2.1}$$

Additionally, we have

$$\mathrm{vol}(\mathbb{R}^n/L) = \mathrm{vol}(\mathcal{P}(L, \{x^{(1)}, \ldots, x^{(n)}\})) = |\det(M)| = \sqrt{\det(A)},$$

where $M := (x^{(j)})_{1 \le j \le n}$ is the $n \times n$ matrix of L with j-th row equal to $x^{(j)}$ and the matrix $A := MM^{\mathrm{T}} = (\langle x^{(j)}, x^{(k)} \rangle)_{1 \le j,k \le n}$ is the inner product matrix (sometimes called the *Gram matrix*) of L.

Writing $\{y^{(1)}, \ldots, y^{(n)}\}$ for the basis of L^* dual to $\{x^{(1)}, \ldots, x^{(n)}\}$, we observe that $y^{(j)} = \sum_{k=1}^n b_{jk} y^{(k)}$, with $B := (b_{jk})_{1 \le j,k \le n} = A^{-1}$. We then compute that

$$\langle y^{(j)}, y^{(k)} \rangle = \left\langle \sum_{\ell=1}^n b_{j\ell} y^{(\ell)}, y^{(k)} \right\rangle = b_{jk},$$

finding that $B = (\langle y^{(j)}, y^{(k)} \rangle)_{1 \le j,k \le n}$, as well. It then follows that

$$\mathrm{vol}(\mathbb{R}^n/L) = \sqrt{\det(A)} = \frac{1}{\sqrt{\det(A^{-1})}} = \frac{1}{\sqrt{\det(B)}} = \frac{1}{\mathrm{vol}(\mathbb{R}^n/L^*)}. \tag{2.2}$$

We call $\det(A)$ the *discriminant* of L, and write $\mathrm{disc}(L) := \det(A)$. Clearly, $\mathrm{disc}(L)$ is an invariant of L. A lattice L for which $\mathrm{disc}(L) = 1$ is said to be *unimodular*. Taking $L' = L^*$ in (2.1) and applying (2.2), we see that $\mathrm{disc}(L) = [L^* : L]$ if $L^* \supset L$. In particular, an integral lattice is self-dual if and only if it is unimodular.

It follows that L is self-dual if and only if the inner product matrix of L is integral with unit determinant. This gives a second proof that $\mathbb{Z}^n$ is self-dual. Additionally, we may demonstrate by explicit determinant computation that E_8 is self-dual and that the lattices A_n and D_n are not. Indeed,

$$\mathrm{disc}(A_n) = n + 1, \quad \mathrm{disc}(D_n) = [\mathbb{Z}_n : D_n]^2 = 4.$$

2.1.2 Root Lattices

We write $L_k := \{x \in L : \langle x, x \rangle = k\}$ for the set of norm-k vectors of L and denote by $\mathcal{L}_m(L)$ the lattice generated by L_m. In this section, we consider in particular the set L_2, called the

[5] Here, $\langle \cdot, \cdot \rangle$ denotes the bilinear extension of the inner product on L.

root system of L. We call $\mathcal{L}_2(L)$ the *root sublattice* of L, and if $\mathcal{L}_2(L) = L$, then we say that L is a *root lattice*. Such a lattice is necessarily even. Clearly, the lattices $\{A_n\}_{n=1}^{\infty}$, $\{D_n\}_{n=3}^{\infty}$, and E_8 are irreducible root lattices. In fact, there are only two more irreducible root lattices beyond these (see [CS99, pp. 97–98] or [Ebe02, pp. 26–27]), the lattices E_7 and E_6 defined by

$$\begin{aligned} E_7 &:= \{(x_1, \dots, x_8) \in E_8 : x_1 + \cdots + x_8 = 0\}, \\ E_6 &:= \{(x_1, \dots, x_8) \in E_8 : x_1 + x_8 = x_2 + \cdots + x_7 = 0\}, \end{aligned}$$

and of ranks 7 and 6, respectively.[6] Furthermore, any root lattice decomposes uniquely into an orthogonal direct sum of irreducible root lattices (see [Ebe02, p. 22]). For L a root lattice of rank n, the number $h(L) := \frac{1}{n}|L_2|$ is called the *Coxeter number* of L. The irreducible root lattices have Coxeter numbers

$$h(A_n) = n + 1, \quad h(D_n) = 2(n-1), \quad h(E_6) = 12, \quad h(E_7) = 18, \quad h(E_8) = 30. \tag{2.3}$$

and it is well-known that if $\dot{x} \in \mathbb{R}^n$ and L is an irreducible root lattice, then

$$\sum_{x \in L_2} \langle x, \dot{x} \rangle^2 = 2 \cdot h(L) \cdot \langle \dot{x}, \dot{x} \rangle \tag{2.4}$$

(see [Ebe02, p. 30]).

2.1.3 Theta Series and Theta Functions

We associate to a lattice L the *theta series* Θ_L defined by

$$\Theta_L(q) := \sum_{x \in L} q^{\frac{1}{2}\langle x, x \rangle},$$

for $0 \leq q < 1$. By construction, Θ_L is a generating function encoding the norms of the vectors of L:

$$\Theta_L(q) = 1 + \sum_{k > 0} a_{2k}(L) q^k,$$

where $a_{2k}(L) := |L_{2k}|$. For example, we have

$$\begin{aligned} \Theta_{\mathbb{Z}^2}(q) &= 1 + 4q^{1/2} + 4q + 0q^{3/2} + 4q^2 + 8q^{5/2} + 0q^3 + 0q^{7/2} + O(q^4), \\ \Theta_{A_2}(q) &= 1 + 6q^{1/2} + 0q + 6q^{3/2} + 6q^2 + 0q^{5/2} + 0q^6 + 12q^{7/2} + O(q^4). \end{aligned}$$

[6] For details and constructions of these lattices, see [CS99, pp. 124–127] or [Ebe02, pp. 24–25].

The first of these functions, $\Theta_{\mathbb{Z}^2}(q)$, may be interpreted as the generating function where the coefficient of $q^{k/2}$ is the number of representations of k as a sum of two integer squares.[7] By construction, theta series are multiplicative, i.e.

$$\theta_L(z) \cdot \theta_{L'}(z) = \theta_{L \oplus L'}(z).$$

Indeed, we see that

$$\Theta_{\mathbb{Z}^2}(q) = \left(1 + 2\sum_{k=1}^{\infty} q^{k^2/2}\right)^2 = \left(\Theta_{\mathbb{Z}}(q)\right)^2$$

We denote by $\mathcal{H}$ the *upper half plane* of complex numbers, $\mathcal{H} := \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$. Often, we will take $z \in \mathcal{H}$ and $q = e^{2\pi i z}$, considering the *theta function of* L defined by

$$\theta_L(z) := \Theta_L\left(e^{2\pi i z}\right) = \sum_{x \in L} e^{\pi i z \langle x, x \rangle}.$$

We will discuss theta series and theta functions in more detail in Section 3.1.3. There, we prove that theta functions of even unimodular lattices are examples of *modular forms* and give several applications. In Sections 3.2 and 3.3, we introduce and discuss a powerful generalization of theta functions called *weighted theta functions*. We give applications of these generalized theta functions in Chapter 4.

2.1.4 Type II Lattices

If a self-dual lattice L is even, then it is said to be of *Type II*; it is said to be of *Type I* otherwise. As we will demonstrate in Theorem 3.6 of Section 3.1.3, Type II lattices may exist only in dimensions which are multiples of 8: if a rank-n lattice L is of Type II, then $n = 8n'$ for some $n' > 0$. Meanwhile, the existence of the Type II lattice E_8 shows that, for each $n' > 0$, there exists at least one Type II lattices of rank $8n'$. (To see this, it suffices to note that the lattice $E_8^{n'}$ is of Type II.)

We denote by $\min(L)$ the *minimal nonzero norm* (or just *minimal norm*) of vectors in L,

$$\min(L) := \min_{\substack{x \in L \\ x \neq 0}} \langle x, x \rangle > 0.^{8}$$

[7] We remarked upon this fact in the Preface, while using slightly different notation.

[8] Lattices with large minimal norms are especially important for one of the key applications of lattices, as they give rise to especially dense sphere packings.

For lattices of large ranks, computing $\min(L)$ is computationally difficult to the point of intractability. However, Mallows, Odlyzko, and Sloane [MOS75] (see also [CS99, p. 194]) showed the following upper bound using theta functions: when L is a Type II lattice of rank $8n'$, the minimal norm $\min(L)$ is bounded above by

$$2\lfloor n'/3\rfloor + 2. \tag{2.5}$$

A Type II lattice attaining this bound (2.5) is called *extremal*.

The Type II lattices of rank $8n'$ have been fully classified for $n' \leq 3$. For ranks 8 and 16, Witt [Wit41] (see also [CS99, p. 48]) showed that there are respectively one and two Type II lattices: E_8 for rank 8 and $E_8 \oplus E_8$ and a second lattice, called D_{16}^+ and defined by

$$D_{16}^+ := D_{16} \cup \left\{(x_1, \dots, x_{16}) \in \left(\mathbb{Z} + \frac{1}{2}\right)^{16} : \left(x_1 + \frac{1}{2}, \dots, x_{16} + \frac{1}{2}\right) \in D_{16}\right\},^{9}$$

for rank 16; all three of these lattices are extremal.[10] We will prove these classifications of Type II lattices of ranks 8 and 16 in Section 3.1.3.

Niemeier [Nie73] classified the Type II lattices of rank 24, finding exactly 24 such lattices. Only one of these lattices is extremal, the Type II lattice Λ_{24} of minimal norm 4 originally found by Leech [Lee67]. Niemeier's approach was greatly simplified by Venkov [Ven80], who constrained the possible root systems of Type II lattices via the theory of weighted theta functions. We will present this argument in Section 4.1.2, as an illustrative application of weighted theta functions and to set the stage for an analogous result we obtain in Section 6.2.

Full classifications of the Type II lattices of ranks $8n'$ for $n' > 3$ are unknown and appear to be out of reach. Indeed, the Minkowski–Siegel mass formula shows that there are at least 80000000 such lattices of rank 32 (see [CS99, p. 50]). For sufficiently large n, extremal Type II lattices cannot exist (see [CS99, p. 194]). Nonetheless, extremal Type II lattices of ranks $n = 8, 16, 24, 32, 40, 48, 56, 64, 80$ are known (see [BN98] for rank $n = 80$, and [CS99, p. 194] for the other ranks). It is unknown whether an extremal Type II lattice of rank $n = 72$ exists (see [CS99, p. 194–195]).

[9] In general, for $n \geq 8$, it is possible to define a lattice D_n^+ by

$$D_n^+ := D_n \cup \left\{(x_1, \dots, x_n) \in \left(\mathbb{Z} + \frac{1}{2}\right)^{n} : \left(x_1 + \frac{1}{2}, \dots, x_n + \frac{1}{2}\right) \in D_n\right\}.$$

With this definition, we have $D_8^+ = E_8$.

[10] Since these lattices are even and the right side of (2.5) equals 2 for $n' = 1, 2$, the extremality of these lattices holds *a priori*.

2.2 Codes

2.2.1 Basic Definitions and Examples

Throughout, $\mathbb{F}_q$ denotes a finite field with q elements.[11] By a *q-ary code C of length n* (or just *code of length n*, when q is implicit), we mean a nonempty subset C of $\mathbb{F}_q^n$. A q-ary code of length n is *linear* if it is a linear subspace of $\mathbb{F}_q^n$. Nearly all codes we consider will be linear, hence we will often omit this descriptor in the sequel.

The elements of a code are called *codewords*. For any length-n code $C \subset \mathbb{F}_q^n$ and two codewords $c, c' \in C$, we write $c \cap c' := (c_1c'_1, \ldots, c_nc'_n)$ for the *intersection* of c and c'. There is a natural scalar product on codewords $c, c' \in C$ defined by $(c, c') := \sum_{j=1}^n c_jc'_j \in \mathbb{F}_q$. The *Hamming weight* $\mathrm{wt}(c)$ of a codeword $c \in C$ is the number of nonzero coordinates of c, i.e.

$$\mathrm{wt}(c) = |\{j : c_j \neq 0\}|.$$

This norm gives rise to a natural metric, the *Hamming distance* between two codewords $c, c' \in C$, defined by $\mathrm{wt}(c - c')$. The *minimal nonzero Hamming distance* $d_{\min}(C)$ of a code C is defined by

$$d_{\min}(C) := \min_{\substack{c,c' \in C \\ c \neq c'}} \mathrm{wt}(c - c').$$

We say that a code is an $[n, k, d]$ code if its length, dimension, and minimal nonzero Hamming distance are n, k, and d, respectively.

As with lattices, we write $C \oplus C'$ for the length-$(n + n')$ orthogonal direct sum of two codes $C \subseteq \mathbb{F}_q^n$ and $C' \subseteq \mathbb{F}_q^{n'}$.[12] As with lattices, we write

$$C^k := \underbrace{C \oplus \cdots \oplus C}_{k \text{ times}}.$$

A code C is *reducible* if it can be expressed in the form $C = C' \oplus C''$ for $C', C'' \subset C$, and is *irreducible* otherwise. For a q-ary code C, the *dual code* of C, denoted by $C^\perp$, is defined by

$$C^\perp = \{c' \in \mathbb{F}_q^n : (c', c) = 0 \text{ for all } c \in C\}.$$

[11] Unfortunately, the notation q is already well-established both for the variable of a power series and for the order of a finite field. Since these two uses are endemic in the literature and rarely (if ever) come into direct contact, we abuse notation slightly and employ both here.

Additionally, it is well-known that a field with q elements exists if and only if q is a prime power (see [Art91, p. 509–513]). Thus, we implicitly assume that q is a prime power whenever q is a finite field order.

[12] Whenever we use this notation, the codes involved will be codes over the same field.

We have that

$$\dim(C) + \dim(C^{\perp}) = n. \tag{2.6}$$

A code C is *self-orthogonal* if $C^{\perp} \supseteq C$, and is moreover *self-dual* if $C^{\perp} = C$. From (2.6), we see that a self-orthogonal code necessarily has $\dim(C) \leq n/2$ and that a self-dual code has $\dim(C) = n/2$.

Both the full space $\mathbb{F}_q^n$ and the trivial space $\{(0, \dots, 0)\} \subset \mathbb{F}_q^n$ are linear codes of length n; these codes are respectively called the *full code* and *trivial code*. These codes are duals of each other and respectively have minimal nonzero Hamming distances 1 and ∞.[13]

Most of our discussion focuses on *binary codes of length* n, that is 2-ary codes $C \subset \mathbb{F}_2^n$. Thus, henceforth by a *code of length* n (or just *code*, when n is clear or undetermined) we mean a binary linear code of length n except where otherwise indicated.

We now introduce two particularly rich examples of binary codes which will appear often in our later discussion: the family of codes $\{d_{2n'}\}_{n'=2}^{\infty}$ and the *Hamming code* H. The code $d_{2n'}$ consists of all words $c \in \mathbb{F}_2^{2n'}$ of weight divisible by 4 such that $c_{2j-1} = c_{2j}$ for each $j = 1, 2, \dots, n'$; for each n', the code $d_{2n'}$ is a $[2n', n', 4]$ code. The Hamming code H is the $[7, 4, 3]$ code consisting of the 16 codewords in the columns of the matrix

$$\begin{pmatrix}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}.$$[14]

For any binary code C of length n, we may construct a new binary code $\tilde{C}$ of length $n+1$ by adding a "parity check" bit at the end of each codeword:

$$\tilde{C} = \{(c_1, \dots, c_{n+1}) : (c_1, \dots, c_n) \in C \text{ and } c_1 + \cdots + c_{n+1} \equiv 0 \bmod 2\}.$$

The code $\tilde{C}$ constructed in this fashion is called the *extended code of* C. For example, the codewords

[13] More simple examples of q-ary codes can be found in [CS99, p. 79] and [GZ08].

[14] This code has several equivalent characterizations. For example, the Hamming code may be interpreted as encoding the space of affine-linear functions on $\mathbb{F}_2^3$.

of the *extended Hamming code* $e_8 := \tilde{H}$ are given by the columns of the matrix

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

A binary code C is said to be *even* if all its codewords have even weight, i.e. if $2 \mid \mathrm{wt}(c)$ for all $c \in C$. As for even lattices, to show that C is even it suffices to show for some basis $\{c^{(1)}, \ldots, c^{(n)}\}$ of C that $2 \mid \mathrm{wt}(c^{(j)})$ for all j ($1 \leq j \leq n$), since

$$\mathrm{wt}(c + c') = \mathrm{wt}(c) + \mathrm{wt}(c') - 2\mathrm{wt}\left(c \cap c'\right).$$

If additionally all of the codewords of C have weights divisible by 4, the code C is said to be *doubly even*.

For a binary code C and $c \in C$, we have $(c, c) \equiv \mathrm{wt}(c) \bmod 2$; it follows that any self-dual code is even. It follows that the Hamming code H is not self-dual[15]; we denote $e_7 := H^\perp \neq H$. The extended Hamming code e_8, is self-dual however, and is also doubly even.

2.2.2 Tetrad Codes

For a code C, we denote $C_w := \{c \in C : \mathrm{wt}(c) = w\}$ and write $\mathcal{C}_w(C)$ for the linear code generated by C_w. In analogy with the theory of root lattices, we consider the set C_4, called the *tetrad system* of C. We call $\mathcal{C}_4(C)$ the *tetrad subcode* of C and say that C is a *tetrad code* if $\mathcal{C}_4(C) = C$. The codes $d_{2n'}$ ($n' \geq 2$), e_7, and e_8 are irreducible tetrad codes.

As was the case with root lattices, any tetrad code decomposes into an orthogonal direct sum of irreducible tetrad codes (see [Koc87]). In analogy with the Coxeter number, the *tetrad number* $\eta(C) := \frac{1}{n}|C_4|$ is an important invariant of irreducible tetrad codes. Quick computation shows that

$$\eta(d_{2k}) = (k-1)/4, \quad \eta(e_7) = 1, \quad \eta(e_8) = 7/4.$$

[15] To see this more easily, it suffices to note that the Hamming code H is of length 7, and so we cannot have

$$\dim(H) = \dim(H^\perp) = 7/2.$$

2.2.3 Weight Enumerators

Analogous to the theta functions of lattice theory, the *Hamming weight enumerator* (or just *weight enumerator*) $W_C(x, y)$ of a length-n code $C \subset \mathbb{F}_q^n$, defined by

$$W_C(x, y) := \sum_{c \in C} x^{n - \mathrm{wt}(c)} y^{\mathrm{wt}(c)},$$

is a generating function encoding the weights of the codewords of C. Unlike theta functions, which are infinite series, weight enumerators are finite generating functions. Thus, for example, we may obtain the number of codewords $|C| = q^{\dim(C)}$ of $C \subset \mathbb{F}_q^n$ by evaluating W_C:

$$W_C(1, 1) = \sum_{c \in C} 1^{n - \mathrm{wt}(c)} 1^{\mathrm{wt}(c)} = \sum_{c \in C} 1 = |C|.$$

The weight enumerators of the full binary code of length n, the Hamming code, and the extended Hamming code are respectively

$$\begin{aligned} W_{\mathbb{F}_2^n}(x, y) &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = (x + y)^n, \\ W_H(x, y) &= x^7 + 7x^4y^3 + 7x^3y^4 + y^7, \\ W_{e_8}(x, y) &= x^8 + 14x^4y^4 + y^8. \end{aligned}$$

As we did for theta series, we defer most of our discussion of weight enumerators until a later section, specifically Section 5.1.2. Most of Chapter 5 is dedicated to the development of *harmonic weight enumerators*, a generalization of weight enumerators analogous to the weighted theta functions of lattice theory.

2.2.4 Type II Codes

A self-dual binary code is said to be of *Type II* if it is doubly even, and of *Type I* otherwise. As with Type II lattices, Type II codes must have lengths which are multiples of 8, and conversely exist for all lengths which are multiples of 8.[16]

Mallows and Sloane [MS73] (see also [CS99, p. 194]) showed using weight enumerators that when $C \subset \mathbb{F}_2^n$ is a Type II code of length $8n'$, the *minimal nonzero weight* of codewords of C, denoted $\min(C) := \min_{\substack{c \in C \\ c \neq 0}} \mathrm{wt}(c)$, is bounded above by

$$\min(C) \leq 4\lfloor n'/3 \rfloor + 4. \tag{2.7}$$

[16] Indeed, the code $e_8^{n'}$ is a Type II code of length $8n'$ for any $n' > 0$.

A Type II code is said to be *extremal* if it attains the bound (2.7).

The Type II codes of length $8n'$ have been fully classified for $n' \leq 4$. All self-dual codes of lengths $n \leq 20$, both of Type I and of Type II, were classified by Pless [Ple72]; this classification was extended to include lengths $n = 22, 24$ by Pless and Sloane [PS75], who cited unpublished work of Conway for the Type II case. Conway and Pless [CP80] classified the Type II codes of length 32 (see [CP92] for minor corrections of [CP80]). These classification results indicate that there is a unique Type II code of length 8 (the extended Hamming code e_8), two Type II codes of length 16, nine of length 24, and eighty-five of length 32.

Complete classifications of the Type II codes of sufficiently large lengths are likely out of reach. Rains and Sloane [RS98] used the mass formula of MacWilliams, Sloane, and Thompson [MST72] to compute that there are at least 17493 Type II codes of length 40, then remarking that "length 32 is probably a good place to stop [seeking complete classification results]." King [Kin01] determined that at least 12579 of these Type II codes are extremal, suggesting that it may even be unreasonable to ask for a classification of extremal Type II codes of length 40.

Extremal Type II codes of lengths

$$n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136$$

are known (see [Pas81] for $n = 64$, [Har08] for $n = 112$, and [RS98, p. 273] for the other lengths).[17] As with lattices in $\mathbb{R}^{72}$, the existence of an extremal Type II code in dimension 72 is a longstanding open question (see [Slo73]).

2.3 The Relationship Between Lattices and Codes

As we have already suggested, the theories of lattices and codes are deeply related. The analogy indicated by our discussion and terminology is persistent: concepts from coding and lattice theory correspond directly, and constructions of lattices from codes often map corresponding properties onto each other. The following "dictionary" (Table 1) summarizes this correspondence and gives the page references for each concept.

[17] The full classifications of extremal Type II codes of lengths $n = 8, 16, 24, 32$ are implicit from the results of Pless [Ple72], Pless and Sloane [PS75], and Conway and Pless [CP80].

Lattice Theory	**Coding Theory**
lattice (p. 8)	code (p. 15)
minimal norm (p. 13)	minimal weight (p. 18)
self-dual (p. 10)	self-dual (p. 16)
even (p. 10)	doubly even (p. 17)
Type I (p. 13)	Type I (p. 18)
Type II (p. 13)	Type II (p. 18)
theta series (p. 12)	weight enumerator (p. 18)
weighted theta function (p. 23)	harmonic weight enumerator (p. 58)
root system (p. 12)	tetrad system (p. 17)
$h(\cdot)$ (p. 12)	$\eta(\cdot)$ (p. 17)
spherical t-design (p. 22)	t-design (p. 21)

Table 1: The correspondence “dictionary.”

2.3.1 Construction A

We now introduce a simple construction of lattices from binary codes which preserves corresponding properties. This construction, originally due to Leech and Sloane [LS71], relates length-n binary codes $C \subset \mathbb{F}_2^n$ to certain lattices $L_C \subset \mathbb{R}^n$.

Construction A ([CS99, pp. 182–183])**.** For a code $C \subset \mathbb{F}_2^n$, the lattice $L_C \subset \mathbb{R}^n$ consists of all $x \in \mathbb{R}^n$ such that $2^{1/2}x \in \mathbb{Z}^n$ and $(2^{1/2}x) \bmod 2 \in C$.

For example, we may compute directly that $L_{e_8} \cong E_8$.[18]

Construction A in some sense “preserves” two important features of the input code C. Specifically,

- the lattice $L_{C^\perp}$ is the dual L_C^* of L_C and
- if C is doubly even, then L_C is even (see [Ebe02, pp. 12–13]).

The first of these conditions guarantees that the lattice L_C associated to C is self-dual if and only if C is self-dual. Taken together, these conditions imply that the Construction A lattice L_C is of

[18] Ebeling [Ebe02, pp. 13–14] gives the details of this computation.

Type II (resp. Type I) if and only if C is of Type II (resp. Type I). Furthermore, if C is an irreducible tetrad code, then L_C is an irreducible root lattice. Namely,

$$L_{d_{2k}} \cong D_{2k}, \quad L_{e_7} \cong E_7, \quad L_{e_8} \cong E_8. \tag{2.8}$$

2.4 Designs

2.4.1 t-designs

A t-(n, w, λ)-*design* is a collection $D \neq \emptyset$ of distinct w-element subsets of $\{1, \ldots, n\}$ with the property that $|\{S' \in D : S \subseteq S'\}| = \lambda$ for every $S \subset \{1, \ldots, n\}$ with $|S| = t$. This generalizes the notion of a *Steiner system*, which corresponds to this definition in the case $\lambda = 1$. When n, w, and λ are undetermined or clear from context, we will omit the qualifier "(n, w, λ)" and simply refer to a t-(n, w, λ)-design as a t-*design*.

Each $S' \in D$ may be represented by its *indicator vector* $(c_1, \ldots, c_n)$, in which $c_j = 1$ if and only if $j \in S'$. Thus, a t-(n, w, λ)-design D corresponds to a subset of the *Hamming sphere of weight* w

$$\omega_w := \{v \in \mathbb{F}_2^n : \mathrm{wt}(v) = w\}.$$

That is, D is a nonlinear binary code of length n in which every codeword has weight w. We will henceforth treat this representation of D as completely equivalent to the setwise representation of D, using the relevant terminology interchangeably.

Often, t-designs arise as the sets of codewords of given weight within a binary code. For example, the codewords of weight 4 in the extended Hamming code e_8 form a 3-$(8, 4, 1)$-design. More generally,[19] we have the following theorem originally due to Assmus and Mattson [AM69].[20]

Theorem 2.1 (Assmus–Mattson Theorem ([AM69])). *Let C be an $[n, k, d]$ binary code and let $d^\perp$ be the minimal Hamming distance of $C^\perp$. If $t \leq d$ is such that $|\{w \leq n - t : C^\perp{}_w \neq \emptyset\}| \leq d - t$, then the set of codewords of C (resp. $C^\perp$) of fixed weight w such that $d \leq w \leq n$ (resp. w such that $d^\perp \leq w \leq n - t$) form a t-design.*

Distinct proofs of Theorem 2.1 have appeared in [AM69], [Bac99], and [Tan09]. Additionally, Theorem 2.1 has several important corollaries. For example, we have the following result.

[19] The fact that the codewords of weight 4 in the extended Hamming code e_8 form a 3-design follows from Theorem 2.1, since e_8 is an $[8, 4, 4]$ binary code.

[20] This result is the "Assmus–Mattson Theorem" mentioned both in the Preface and in Chapter 1.

Corollary 2.2 ([CS99, p. 196])**.** *If C is an extremal Type II code of length $n = 24n'$, then C_w is a 5-design for each $w \geq \min(C)$ such that $C_w \neq \emptyset$.*

In Theorem 6.4 of Chapter 6, we prove Theorem 2.1 for the case in which C is an extremal Type II code, and hence also prove Corollary 2.2.

2.4.2 Spherical t-designs

A *spherical t-design* is a finite, nonempty subset X of the $(n-1)$-dimensional unit sphere,

$$\Omega_n := \left\{ x \in \mathbb{R}^n : x_1^2 + \cdots + x_n^2 = 1 \right\},$$

having the property that the integral of any polynomial P with degree at most t over Ω_n equals the average of P over X. Formally, this means that

$$\int_{\Omega_n} P \, d\mu = \frac{1}{|X|} \sum_{x \in X} P(x), \tag{2.9}$$

where here μ is the Lebesgue measure on the sphere, normalized so that $\int_{\Omega_n} d\mu = 1$. If X is a spherical t-design and we have (2.9) additionally for P of degree $t+3$ (but not necessarily for P of degrees $t+1$ or $t+2$), then we say that X is a *spherical $(t+\frac{1}{2})$-design*.[21]

We illustrate with Proposition 6.1 in Section 6.1 that there exists an alternative characterization of t-designs directly analogous to (2.9). Thus, spherical t-designs correspond, in the code-lattice dictionary, to t-designs.

As we described earlier in the introduction, results corresponding to cases of the Assmus–Mattson Theorem have more recently been obtained for lattices. For example, we have the following result of Venkov [Ven84b] which is a lattice analog of Corollary 2.2.

Proposition 2.3 ([Ven84b])**.** *If L is an extremal Type II lattice of rank $24n'$, then L_m is a spherical 11-design for any $m > 0$ such that $L_m \neq \emptyset$.*

[21] This terminology is due to Venkov (see [Ven01]).

Chapter 3

Weighted Theta Functions

We now introduce the *weighted theta series* $\Theta_{L,P}$ and associated *weighted theta function* $\theta_{L,P}$ of a lattice $L \subset \mathbb{R}^n$, defined by

$$\Theta_{L,P}(q) := \sum_{x \in L} P(x) q^{\frac{1}{2}\langle x,x\rangle}, \quad \theta_{L,P}(z) := \Theta_{L,P}(e^{2\pi i z}). \tag{3.1}$$

Here, P is a *spherical harmonic polynomial* on $\mathbb{R}^n$; the formal definition and discussion of such polynomials is given in Section 3.2. Weighted theta series and weighted theta functions generalize theta series and theta functions respectively, encoding both the number and distribution of the norm-k vectors of L, for each $k > 0$. Weighted theta functions of Type II lattices are examples of a well-studied class of functions called *modular forms*, and throughout Chapter 4 we use classical results about modular forms to study the weighted theta functions of Type II lattices.

We review the relevant results from the theory of modular forms in Sections 3.1.1 and 3.1.2. As a warm-up for our discussion of weighted theta functions, we prove in Section 3.1.3 that the ordinary theta function θ_L of a Type II lattice L is a modular form. We then introduce spherical harmonic polynomials in Section 3.2 and formally define and discuss weighted theta series in Section 3.3. Finally, in Section 3.4, we define and characterize the *zonal spherical harmonic polynomials*, particular spherical harmonic polynomials which are useful for the applications of weighted theta functions we present in Chapter 4.

3.1 Preliminaries

3.1.1 Modular Forms for $\mathrm{PSL}_2(\mathbb{Z})$

In this section, we introduce the classical theory of modular forms for $\mathrm{PSL}_2(\mathbb{Z})$. This material is predominantly standard, and its presentation here owes much to Ebeling [Ebe02] and Serre [Ser73]. This section is essential, however, to establish conventions and for completeness. Throughout this section, we will take $q = e^{2\pi i z}$ with $z \in \mathcal{H}$.

Basic Definitions

There is a natural action of the *special linear group*

$$\mathrm{SL}_2(\mathbb{R}) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{R}; ad - bc = 1 \right\}$$

on $\mathcal{H}$, defined by fractional linear transformations:

$$z \xmapsto{\gamma} \frac{az+b}{cz+d},$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$. From this definition, we see that $\mathrm{Im}(\gamma z) = \mathrm{Im}(z)/|cz+d|^2$. We let $\mathrm{SL}_2(\mathbb{Z})$ be the discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ consisting of matrices with integer coefficients. The action of the center $\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ of SL_2 on $\mathcal{H}$ is trivial, hence we define the *modular group* $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$.

A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is said to be a *modular form of weight k for* $\mathrm{PSL}_2(\mathbb{Z})$ (or just *modular form of weight k*, hereafter[1]) if

1. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for all $z \in \mathcal{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z})$ and
2. f is holomorphic at $i\infty$, that is, $f(z)$ has a power series expansion in $q = e^{2\pi i z}$ in a neighborhood of the origin.

If f satisfies the first condition of this definition, then in particular $f(z+1) = f(z)$. It follows that a modular form f has a power series expansion in q on the punctured disk of radius 1, hence

[1] This usage is somewhat nonstandard, since modular forms may be defined, more generally, for all subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. However, in our discussion we are only concerned with modular forms for the full modular group $\mathrm{PSL}_2(\mathbb{Z})$, hence this abbreviated terminology is sufficient for our purposes and seems appropriate.

the second defining condition is a natural extension of the first condition.[2] A modular form which vanishes at $i\infty$ is called a *cusp form*.[3]

The modular group $\mathrm{PSL}_2(\mathbb{Z})$ is generated by

$$\sigma := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad \tau := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right),$$

which respectively correspond to the actions

$$z \xmapsto{\sigma} -\frac{1}{z} \quad \text{and} \quad z \xmapsto{\tau} z+1$$

(see [Ebe02, pp. 41–43] or [Ser73, pp. 78–79]). Direct computation shows that

$$\sigma^2 = (\sigma\tau)^3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right). \tag{3.2}$$

In light of these observations, we see that a holomorphic function $f(z) = \sum_{j=0}^{\infty} a_j q^j$ is a modular form of weight k if and only if

$$f\left(-\frac{1}{z}\right) = f(\sigma z) = z^k f(z). \tag{3.3}$$

The Eisenstein Series

For $k > 1$, we define the *unnormalized Eisenstein series of index* $2k$, denoted G_{2k}, to be the function $\mathrm{G}_{2k} : \mathcal{H} \to \mathbb{C}$ given by

$$\mathrm{G}_{2k}(z) := \sum_{(c,d)\in\mathbb{Z}^n\setminus(0,0)} \frac{1}{(cz+d)^{2k}}.$$

These functions G_{2k} are clearly periodic and satisfy the identity (3.3) for weight $2k$. In fact, they are also holomorphic on $\mathcal{H} \cup \{i\infty\}$, giving the following proposition.

Proposition 3.1 ([Ebe02, p. 48]; [Ser73, p. 83])**.** *For each $k > 1$, the unnormalized Eisenstein series G_{2k} of index $2k$ is a modular form of weight $2k$.*

Clever computation shows that

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{j=1}^{\infty} \sigma_{k-1}(j) q^j,$$

[2] Serre [Ser73, p. 80] avoids the complications inherent in the definition we have presented by first defining *weakly modular functions for* $\mathrm{PSL}_2(\mathbb{Z})$. We have chosen not to follow Serre's approach, however, as weakly modular functions are rarely used in practice and—more pertinently—are not directly relevant to this thesis.

[3] Equivalently, a modular form is a cusp form if and only if the constant term of its power series vanishes.

where $\zeta(s) := \sum_{j=1}^{\infty} 1/j^s$ is the *Riemann zeta function* and $\sigma_{k-1}(s) := \sum_{d|s} d^{k-1}$ (see [Ebe02, p. 51] or [Ser73, p. 92]). It is well-known that

$$\zeta(2k) = -\frac{(2\pi i)^{2k}}{2(2k!)} B_{2k},$$

where the *Bernoulli numbers* $\{B_{2k}\}_{k=1}^{\infty}$ are defined by the generating function

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_{2k} \frac{x^{2k}}{(2k)!}$$

(see, for example, [Ebe02, p. 52] or [Ser73, p. 91]).[4] Thus, we obtain the expression

$$G_{2k}(z) = -\frac{(2\pi i)^k}{k!} B_{2k} + \frac{2(2\pi i)^k}{(k-1)!} \sum_{j=1}^{\infty} \sigma_{k-1}(j) q^j.$$

Normalizing $\mathrm{G}_{2k}(z)$ to have constant term 1, we obtain the *normalized Eisenstein series of index* $2k$ (or just *Eisenstein series of index* $2k$)

$$\mathrm{E}_{2k}(z) := \frac{1}{2\zeta(2k)} \mathrm{G}_{2k}(z) = 1 - \frac{2k}{B_{2k}} \sum_{j=1}^{\infty} \sigma_{k-1}(j) q^j.$$

From this formula, we may compute Eisenstein series explicitly. For example,

$$\mathrm{E}_4(z) = 1 + 240q + 2160q^2 + 6720q^3 + O(q^4),$$
$$\mathrm{E}_6(z) = 1 - 504q - 16632q^2 - 122976q^3 + O(q^4).$$

Now, $\mathrm{E}_4^3 - \mathrm{E}_6^2$ is a modular form of weight 12; we see from these expressions that it has constant term 0. It is therefore a nontrivial cusp form of weight 12. Computation shows that the first nonzero coefficient of $\mathrm{E}_4^3 - \mathrm{E}_6^2$ is 1728; we will normalize further and write

$$\Delta := \frac{1}{1728}(\mathrm{E}_4^3 - \mathrm{E}_6^2) = q - 24q^2 + 252q^3 - 1472q^4 + \cdots .$$

The Spaces of Modular Forms

For each $k \in \mathbb{Z}$, we let $\mathcal{M}_k$ and $\mathcal{M}_k^0$ be the $\mathbb{C}$-vector spaces of weight-k modular forms and cusp forms for $\mathrm{PSL}_2(\mathbb{Z})$, respectively. Residue theorem computations give conditions which allow us to completely characterize these spaces, as in the following theorems.

[4] Note that we may extend this definition to that of a sequence $\{B_k\}_{k=0}^{\infty}$ defined by the generating function

$$\frac{x}{e^x - 1} = \sum_{k=1}^{\infty} B_k \frac{x^k}{k!};$$

this extended definition implies that $B_{2k+1} = 0$ for $k \geq 1$.

Theorem 3.2 ([Ebe02, p. 59]; [Ser73, p. 88])**.** *We have*

1. $\dim(\mathcal{M}_k) = \dim(\mathcal{M}_k^0) = 0$*, for k odd, $k < 0$, and $k = 2$;*
2. $\dim(\mathcal{M}_{2k}) = 1$ *and* $\dim(\mathcal{M}_{2k}^0) = 0$*, for* $4 \leq 2k \leq 10$ *and* $2k = 14$*.*

Additionally, multiplication by the form Δ gives an isomorphism $\mathcal{M}_{k-12} \xrightarrow{\sim} \mathcal{M}_k^0$.

Corollary 3.3 ([Ser73, pp. 88–89])**.** *For $k \geq 0$, we have*

$$\dim(\mathcal{M}_k) = \begin{cases} \lfloor k/6 \rfloor & k \equiv 0 \bmod 6, \\ \lfloor k/6 \rfloor + 1 & \textit{otherwise}. \end{cases}$$

Theorem 3.4 ([Ebe02, p. 60]; [Ser73, p. 89])**.** *The algebra $\mathcal{M} := \bigoplus_{k=0}^{\infty} \mathcal{M}_k$ is isomorphic to the polynomial algebra $\mathbb{C}[\mathrm{E}_4, \mathrm{E}_6]$ of complex polynomials in the Eisenstein series E_4 and E_6.*

These characterization results allow us to determine modular forms explicitly from information about a few power series coefficients. For example, if $f : \mathcal{H} \to \mathbb{C}$ is a modular form with constant term 1 and vanishing q^1 coefficient, then

$$f \equiv \mathrm{E}_4^3 - 720\Delta = 1 + 196560q^2 + 16773120q^3 + O(q^4). \tag{3.4}$$

We will return to this modular form in Section 3.1.3.

3.1.2 The Poisson Summation Formula

In this section, we give the necessary preliminaries for and a proof of the *Poisson summation formula*. This powerful formula relates the sums of a Schwartz function over a lattice $L \subset \mathbb{R}^n$ to the sums of the function's Fourier transform over L^*, the dual lattice of L.

We first recall that, for an absolutely integrable function $f : \mathbb{R}^n \to \mathbb{C}$, the *Fourier transform* $\hat{f}$ of f is the function $\hat{f} : \mathbb{R}^n \to \mathbb{C}$ defined by

$$\hat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{2\pi i \langle x, y \rangle} \, d\mu(x),$$

where $\mu(x)$ is the measure on $\mathbb{R}^n$. We let $\mathcal{S}$ be the space of *rapidly decreasing functions* (or *Schwartz functions*), those $\mathscr{C}^\infty$ functions $f : \mathbb{R}^n \to \mathbb{C}$ such that, for all k and as $\langle x, x \rangle \to \infty$, $f(x)$ and all its partial derivatives decay as $o(\langle x, x \rangle^k)$. The Fourier transform operator acts as an isomorphism $\mathcal{S} \to \mathcal{S}$; the equality $\hat{\hat{f}}(x) = f(-x)$ yields the inverse isomorphism.

Theorem 3.5 (Poisson Summation Formula)**.** *Let $L \subset \mathbb{R}^n$ be a lattice and let $f \in \mathcal{S}$. Then,*

$$\sum_{x\in L} f(x) = \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \sum_{y\in L^*} \hat{f}(y). \tag{3.5}$$

The proof we follow is standard. Serre [Ser73, p. 107] gives a slightly more concise approach based upon the same method, and Ebeling [Ebe02, pp. 44–45] proves Theorem 3.5 under weaker conditions.[5]

Proof of Theorem 3.5. Let $\mathcal{D}$ be any fundamental domain for L and let $F : \mathbb{R}^n \to \mathbb{C}$ be the function defined by $F(z) := \sum_{x\in L} f(x+z)$. By construction, $F(z)$ is continuous and L-periodic in z. The function f therefore descends to a $\mathscr{C}^\infty$ function on $\mathbb{R}^n/L$ with a Fourier expansion

$$F(z) = \sum_{y\in L^*} \widehat{F}(-y)e^{2\pi i\langle y,z\rangle}. \tag{3.6}$$

Here, $\widehat{F}$ denotes the Fourier coefficient of F computed over $\mathbb{R}^n/L$:

$$\begin{aligned}\widehat{F}(y) &= \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \int_{z\in\mathbb{R}^n/L} F(z)e^{2\pi i\langle z,y\rangle}\, d\mu(z)\\ &= \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \int_{z\in\mathcal{D}} F(z)e^{2\pi i\langle z,y\rangle}\, d\mu(z)\\ &= \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \int_{z\in\mathcal{D}} \sum_{x\in L} \left(f(x+z)e^{2\pi i\langle z,y\rangle}\right)\, d\mu(z)\\ &= \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \sum_{x\in L} \int_{z\in(\mathcal{D}-x)} \left(f(z)e^{2\pi i\langle z,y\rangle}\right)\, d\mu(z). \end{aligned} \tag{3.7}$$

Now, by the definition of $\mathcal{D}$, we have $\mathbb{R}^n = \coprod_{x\in L}(\mathcal{D}-x)$. Thus, we obtain from (3.7) that

$$\widehat{F}(y) = \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \int_{z\in\mathbb{R}^n} f(z)e^{2\pi i\langle z,y\rangle}\, d\mu(z) = \hat{f}(y). \tag{3.8}$$

Substituting (3.8) into (3.6), we obtain

$$F(z) = \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} \sum_{y\in L^*} \hat{f}(-y)e^{2\pi i\langle y,z\rangle}. \tag{3.9}$$

Taking $z = 0$ in (3.9) then proves the desired result, since $F(0) = \sum_{x\in L} f(x)$ and

$$\sum_{y\in L^*} \hat{f}(-y) = \sum_{y\in L^*} \hat{f}(y). \qquad \square$$

[5] Specifically, Ebeling [Ebe02, pp. 44–45] proves that (3.5) holds whenever $L \subset \mathbb{R}^n$ is a lattice and $f : \mathbb{R}^n \to \mathbb{C}$ is a function such that

- $\int_{\mathbb{R}^n} |f(x)|\, d\mu(x) < \infty$,
- $\sum_{x\in L} |f(x+u)|$ converges uniformly for all u in a compact subset of $\mathbb{R}^n$, and
- $\sum_{x\in L^*} \hat{f}(y)$ converges absolutely.

3.1.3 Theta Functions as Modular Forms

From the Poisson summation formula (3.5), we obtain that θ_L is a modular form whenever L is a Type II lattice. *En route* to this result, we prove that every Type II lattice has rank divisible by 8, a statement encountered in the introduction.

Theorem 3.6. *Let L be a Type II lattice of rank n. Then, $n \equiv 0 \bmod 8$ and θ_L is a modular form of weight $n/2$.*

The proof of Theorem 3.6 will proceed quickly from the following lemmata.

Lemma 3.7. *For any lattice $L \subset \mathbb{R}^n$ and positive $t \in \mathbb{R}$, the theta series Θ_L satisfies the identity*

$$\Theta_L\left(e^{-2\pi/t}\right) = \frac{1}{\operatorname{vol}(\mathbb{R}^n/L)} t^{n/2}\Theta_{L^*}(e^{-2\pi t}).$$

Proof. We let $f(x) = e^{-\pi\langle x,x\rangle/t} \in \mathcal{S}$; we will show that

$$\hat{f}(y) = t^{-n/2}e^{-\pi\langle x,x\rangle t}. \tag{3.10}$$

The lemma will then follow directly from Theorem 3.5 since $\Theta_L\left(e^{-2\pi/t}\right) = \sum_{x\in L} e^{-\pi\langle x,x\rangle/t}$. Writing the integral defining $\hat{f}(y)$ with respect to the the standard orthogonal basis of $\mathbb{R}^n$, we obtain

$$\hat{f}(y) = \prod_{j=1}^{n}\int_{-\infty}^{\infty} e^{-\pi x_j^2/t}e^{2\pi i x_j y_j}\,dx_j.$$

Thus, it suffices to prove (3.10) when $n = 1$; in this case, the claim is just the well-known integral

$$\int_{-\infty}^{\infty} e^{-\pi x^2/t}e^{2\pi i xy}\,dx = e^{-\pi t y^2}. \qquad \square$$

Lemma 3.8. *For any lattice $L \subset \mathbb{R}^n$, the theta function $\theta_L(z) = \sum_{x\in L} e^{\pi i z\langle x,x\rangle}$ converges absolutely to a holomorphic function for all $z \in \mathcal{H}$.*

Proof. It suffices to show that $\theta_L(z)$ converges absolutely and uniformly for all z in every half-plane $\mathcal{H}' \subseteq \mathcal{H}$. To see this, we let $M \in \mathrm{GL}_n(\mathbb{R})$ be the matrix of basis vectors of L, so that $L = M \cdot \mathbb{Z}^n$. Then, we set $\epsilon := \min_{|x|=1}\langle Mx, Mx\rangle > 0$ so that $\langle Mx, Mx\rangle \geq \epsilon\langle x,x\rangle$ for all $x \in \mathbb{R}^n$, and set $z_0 := \min\{\operatorname{Im}(z) : z \in \mathcal{H}'\}$. The estimate

$$\begin{aligned}|\theta_L(z)| = \left|\sum_{x\in L} e^{\pi i z\langle x,x\rangle}\right| \leq \sum_{x\in L}\left|e^{\pi i z\langle x,x\rangle}\right| &= \sum_{x\in\mathbb{Z}^n}\left|e^{\pi i z\langle Mx,Mx\rangle}\right| \\ &\leq \sum_{x\in\mathbb{Z}^n} e^{-\pi z_0\epsilon\langle x,x\rangle} = \left(\sum_{j=-\infty}^{\infty} e^{-\pi z_0\epsilon j^2}\right)^n < \infty\end{aligned}$$

then follows, proving the desired result. $\square$

Lemma 3.9. *For any self-dual lattice $L \subset \mathbb{R}^n$ and $\mathcal{H} \ni z \neq 0$, the theta function θ_L satisfies the identity*

$$\theta_L\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{n/2} \theta_L(z). \tag{3.11}$$

Proof. By Lemma 3.8, both sides of (3.11) are holomorphic in $z \in \mathcal{H}$. It therefore suffices to prove (3.11) when $\mathbb{R} \ni t > 0$ and $z = it$. Now, since $L = L^*$, we have $\mathrm{vol}(\mathbb{R}^n/L) = 1$. The identity (3.11) follows directly from Lemma 3.7 because $\theta_L(it) = \sum_{x \in L} e^{-\pi t \langle x,x\rangle} = \Theta_L\left(e^{-2\pi t}\right)$ and $\theta_L(-1/it) = \sum_{x\in L} e^{-\pi\langle x,x\rangle/t} = \Theta_L\left(e^{-2\pi/t}\right)$. □

The derivation of Lemma 3.9 just presented is predominantly a hybrid of the presentations of Elkies [Elk09b] and Serre [Ser73, p. 107]. Our work in Section 3.3 will directly generalize this approach. Ebeling [Ebe02, p. 47] gives a slightly different argument, which proves Lemma 3.9 without direct appeal to Lemma 3.7.[6]

We may now present the proof of Theorem 3.6.

Proof of Theorem 3.6. As in the proposition statement, let $L \subset \mathbb{R}^n$ be a Type II lattice of rank n. We first prove that $n \equiv 0 \bmod 8$. Supposing otherwise, we may assume $n \equiv 4 \bmod 8$, by replacing L with $L \oplus L$ or $L \oplus L \oplus L \oplus L$ as necessary. Then, recalling that $\mathrm{vol}(\mathbb{R}^n/L) = 1$ because L is unimodular, we obtain from Lemma 3.9 that

$$\theta_L(\sigma z) = \theta_L\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{n/2} \theta_L(z) = (-1)^{n/4}(z)^{n/2}\theta_L(z) = -z^{n/2}\theta_L(z).$$

From this formula and the fact that $\theta_L(\tau z) = \theta_L(z)$, we compute that

$$\theta_L((\tau\sigma)z) = -z^{n/2}\theta_L(z).$$

It then follows that

$$\theta_L\left((\tau\sigma)^3 z\right) = -\left(\frac{1}{1-z}\right)^{n/2}\left(\frac{z-1}{z}\right)^{n/2} z^{n/2}\theta_L(z) = -(-1)^{n/2}\theta_L(z) = -\theta_L(z).$$

But this is a contradiction, since we have from (3.2) that $(\tau\sigma)^3 = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Thus, we must have $n \equiv 0 \bmod 8$.

[6] In fact, Ebeling [Ebe02, p. 47] omits the hypothesis that L is self-dual and proves the slightly stronger identity

$$\theta_L\left(-\frac{1}{z}\right) = \frac{1}{\mathrm{vol}(\mathbb{R}^n/L)}\left(\frac{z}{i}\right)^{n/2}\theta_{L^*}(z).$$

Now, since $8 \mid n$, we may simplify the identity (3.11) to obtain

$$\theta_L\left(-\frac{1}{z}\right) = z^{n/2}\theta_L(z). \tag{3.12}$$

Combining (3.12) with Lemma 3.8 shows that θ_L is a modular form of weight $n/2$. □

Applications to Classification of Low-rank Type II Lattices

Combining Theorems 3.2 and 3.6 , we can quickly determine the theta function θ_{E_8} of the E_8 lattice. By Theorem 3.6, θ_{E_8} is a modular form of weight $8/2 = 4$. We know from Theorem 3.2 that the space $\mathcal{M}_4$ of such forms is one-dimensional, generated by the weight-4 form E_4. Since θ_{E_8} has constant term 1, we must have

$$\theta_{E_8}(z) \equiv \mathrm{E}_4(z) = 1 + 240q + 2160q^2 + O(q^3), \tag{3.13}$$

where $q = e^{2\pi i z}$. We may read directly from (3.13) that $a_2(E_8) = 240$, that is, that E_8 has exactly 240 roots. Moreover, any Type II lattice L of rank 8 must have theta function $\theta_L \equiv \theta_{E_8}$; this gives an immediate proof that E_8 is the unique Type II lattice of rank 8.

Theorem 3.10. *If L is a Type II lattice of rank 8, then $L \cong E_8$.*

Proof. If L is a Type II lattice of rank 8, then $a_2(L) = 240$ by the argument above. Since E_8 is the only root lattice of rank at most 8 with at least 240 roots, we must have $\mathcal{L}_2(L) \cong E_8$. Since E_8 has rank 8 and is self-dual, this implies that $L \cong E_8$. □

Additionally, we may now fully classify the Type II lattices of rank 16.

Theorem 3.11. *If L is a Type II lattice of rank 16, then either $L \cong E_8^2$ or $L \cong D_{16}^+$.*

Proof. First, we obtain from Theorems 3.2 and 3.6 that $\theta_L \equiv (\mathrm{E}_4)^2$, hence $a_2(L) = 480$. It then follows from the classification of root systems that either $\mathcal{L}_2(L) \cong E_8^2$ or $\mathcal{L}_2(L) \cong D_{16}$. In the former case, we have $L \cong E_8^2$. In the latter case, we must have

$$D_{16} \subset L \subset D_{16}^*,$$

hence either $L \cong \mathbb{Z}^{16}$ or $L \cong D_{16}^+$. Since $\mathbb{Z}^{16}$ is not even, the result follows. □

Now, if L is an extremal Type II lattice of rank 24, then θ_L is a modular form of weight 12 with constant term 1 and vanishing coefficient of $q^1 = e^{2\pi i z}$. In this case, we see that the theta series of L must be the modular form of equation (3.4); L therefore has 196560 vectors of minimal norm. Mallows, Odlyzko, and Sloane [MOS75] obtained their upper bound for the minimal norms of Type II lattice vectors via more general application of this approach.

3.2 The Space of Harmonic Polynomials

We now introduce *spherical harmonic polynomials* (or just *harmonic polynomials*), which serve as the "weighting" factors P in the weighted theta series $\Theta_{L,P}(q) = \sum_{x \in L} P(x) q^{\langle x,x \rangle/2}$ and weighted theta functions $\theta_{L,P}(z) = \Theta_{L,P}(e^{2\pi i z})$. We define these polynomials in Section 3.2.1 and discuss simple examples. We then prove a decomposition theorem for space of homogeneous polynomials in Section 3.2.2. Although we will not use this decomposition result directly until Section 4.2 of Chapter 4, it provides important intuition regarding the nature of harmonic polynomials. In Section 3.2.3, we provide some remarks on the relationship between our development of harmonic polynomials and the representation theory of $\mathfrak{sl}_2$.

3.2.1 Basic Definitions and Examples

We denote by $\mathscr{P}$ the $\mathbb{C}$-vector space of polynomials in n variables. We then let $\mathscr{P}_d \subset \mathscr{P}$ denote the subspace of degree-d homogenous polynomials, so that

$$\mathscr{P} = \bigoplus_{d=0}^{\infty} \mathscr{P}_d.$$

We adopt the convention that $\mathscr{P}_d = \{0\}$ for $d < 0$. The operator

$$\Delta := \sum_{j=1}^{n} \frac{\partial^2}{\partial x_j^2} : \mathscr{C}^{\infty}(\mathbb{R}^n) \to \mathscr{C}^{\infty}(\mathbb{R}^n)$$

is called the *Laplacian*; it maps $\mathscr{P}$ to $\mathscr{P}$ and more specifically maps $\mathscr{P}_d$ to $\mathscr{P}_{d-2}$. In this definition, we have fixed an orthogonal coordinate system $x_1, \ldots, x_n$ of $\mathbb{R}^n$. However, the operator Δ is still essentially canonical, as it commutes with transformations in the *orthogonal group*

$$\mathrm{O}_n(\mathbb{R}) := \left\{ M \in \mathrm{GL}_n(\mathbb{R}) : M^{\mathrm{T}} M = M M^{\mathrm{T}} = I \right\}.$$

Now, we define the *space of degree-d harmonic polynomials on* $\mathbb{R}^n$, denoted $\mathscr{P}_d^0$:

$$\mathscr{P}_d^0 := \ker \left(\Delta : \mathscr{P}_d \to \mathscr{P}_{d-2} \right).$$

The direct sum

$$\mathscr{P}^0 := \bigoplus_{d=0}^{\infty} \mathscr{P}_d^0 = \ker \left(\Delta : \mathscr{P} \to \mathscr{P} \right)$$

is called the *space of harmonic polynomials on* $\mathbb{R}^n$.

Simple Examples

If $P \in \mathscr{P}_0$ is a constant function, then we have $\Delta P \equiv 0$, hence $P \in \mathscr{P}_0^0$. Conversely, $\mathscr{P}_0^0 \subseteq \mathscr{P}_0$, so we see that $\mathscr{P}_0^0 = \mathscr{P}_0$ and $\dim(\mathscr{P}_0^0) = \dim(\mathscr{P}_0) = 1$ for any n. Similarly, we see that $\mathscr{P}_1^0 = \mathscr{P}_1$ and $\dim(\mathscr{P}_1^0) = \dim(\mathscr{P}_1) = n$. For any n and $P = \sum_{j=1}^n \sum_{k=j}^n a_{jk} x_j x_k \in \mathscr{P}_2$, we have $P \in \mathscr{P}_2^0$ if and only if $\sum_{j=1}^n a_{jj} = 0$ because $\Delta P = 2\sum_{j=1}^n a_{jj}$.

3.2.2 Decomposition of Degree-d Homogenous Polynomials

We now introduce two additional operators on $\mathscr{C}^\infty(\mathbb{R}^n)$ which restrict to operators on $\mathscr{P}$:

$$\mathsf{E} := x \cdot \nabla = \sum_{j=1}^n x_j \frac{\partial}{\partial x_j}, \quad \mathsf{F} := \langle x, x \rangle = \sum_{j=1}^n x_j^2.$$

The following fact regarding the operator E dates back to Euler.

Fact 3.12. *The space $\mathscr{P}_d$ of degree-d homogenous polynomials is the d-eigenspace of $\mathsf{E}|_{\mathscr{P}}$. That is, $\mathsf{E}P = d \cdot P$ for any $P \in \mathscr{P}_d$.*

The F operator is multiplication by the norm, which clearly restricts to an injection $\mathscr{P}_d \to \mathscr{P}_{d+2}$. From this and the definition of $\mathscr{P}_d^0$, we obtain the following fact.

Fact 3.13. *We have $\mathscr{P}_d^0 = \ker(\mathsf{F}\Delta : \mathscr{P}_d \to \mathscr{P}_d)$. That is, the space $\mathscr{P}_d$ of degree-d harmonic polynomials is the 0-eigenspace of $\mathsf{F}\Delta|_{\mathscr{P}_d}$*

The remainder of this section works towards a proof of the following result which decomposes the spaces of degree-d homogenous polynomials in terms of the spaces of harmonic polynomials. For $k = 0, 1, \ldots, \lfloor d/2 \rfloor$, we define $\mathscr{P}_d^k := \mathsf{F}^k \mathscr{P}_{d-2k}^0$; this notation is consistent with the notation $\mathscr{P}_d^0$ for the space of degree-d harmonic polynomials.

With these definitions, we have the following decomposition theorem.

Proposition 3.14. *1. The map $\Delta : \mathscr{P}_d \to \mathscr{P}_{d-2}$ is surjective.*

2. *We have the direct sum decomposition $\mathscr{P}_d = \bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathscr{P}_d^k = \mathscr{P}_d^0 \oplus \mathsf{F}\mathscr{P}_{d-1}$.*

3. *With $\lambda_d(k) := k(4(d-k-1) + 2n)$ and for each $k = 0, 1, \ldots, \lfloor d/2 \rfloor$, the space $\mathscr{P}_d^k$ is the $\lambda_d(k)$-eigenspace of $\mathsf{F}\Delta|_{\mathscr{P}_d}$. Furthermore, $\{\lambda_d(k)\}_{k=0}^{\lfloor d/2 \rfloor}$ is the full set of eigenvalues of $\mathsf{F}\Delta|_{\mathscr{P}_d}$.*

4. *$\dim(\mathscr{P}_d^0) = \dim(\mathscr{P}_d) - \dim(\mathscr{P}_{d-2}) = \binom{n+d-1}{d} - \binom{n+d-3}{d}$.*

In the sequel, we only directly apply the second part of Proposition 3.14. The remaining components are presented for intuition regarding the spaces $\mathscr{P}_d^0$.

The proof of Proposition 3.14 will require several intermediate results. Our presentation here is heavily based upon that of Elkies [Elk09b]. In particular, the lemmata we present appear in [Elk09b].

Commutation Relations for Δ, E, and F

First, we prove a lemma which gives commutation relations for the operators Δ, E, and F. Here, the *commutator* $[A, B]$ of two operators A and B (on any vector space) is given by

$$\big[A, B\big] := AB - BA.$$

From this definition, it is immediate that $[A, B] = -[B, A]$.

Lemma 3.15. *We have the commutation relations*

$$\big[\Delta, \mathsf{F}\big] = 4\mathsf{E} + 2n, \quad \big[\mathsf{E}, \Delta\big] = -2\Delta, \quad \big[\mathsf{E}, \mathsf{F}\big] = 2\mathsf{F}. \tag{3.14}$$

Proof. The relations (3.14) follow upon direct computation. Details of these computations are given in [Elk09b]. □

The $\lambda_d(k)$-eigenspaces of $\mathsf{F}\Delta$

Now, we examine the $\lambda_d(k)$-eigenspaces of $\mathsf{F}\Delta|_{\mathscr{P}_d}$, where

$$\lambda_d(k) = k(4(d - k - 1) + 2n)$$

is as defined in the third part of Proposition 3.14. The commutation relation for $[\Delta, \mathsf{F}]$ found in Lemma 3.15 shows that

$$\mathsf{F}\Delta\mathsf{F}P = \mathsf{F}\left(\mathsf{F}\Delta + \big[\Delta, \mathsf{F}\big]\right)P = \mathsf{F}(\mathsf{F}\Delta + 4\mathsf{E} + 2n)P = \mathsf{F}(\lambda + 4d + 2n)P,$$

hence if $P \in \mathscr{P}_d$ is in the λ-eigenspace of $\mathsf{F}\Delta$ for some λ, then $\mathsf{F}P \in \mathscr{P}_{d+2}$ is in the $(\lambda+4d+2n)$-eigenspace of $\mathsf{F}\Delta|_{\mathscr{P}_{d+2}}$. It then follows that F^kP is an eigenvector of $\mathsf{F}\Delta|_{\mathscr{P}_{d+2k}}$ with eigenvalue

$$\lambda + \sum_{j=0}^{k-1} (4(d + 2j) + 2n) = \lambda + k\left(4(d + k - 1) + 2n\right). \tag{3.15}$$

Taking $\lambda = 0$ and $d \mapsto (d - 2k)$ in (3.15) shows that any $P \in \mathscr{P}_{d-2k}^0$ is a $\lambda_d(k)$-eigenvector of the operator $\mathsf{F}\Delta|_{\mathscr{P}_d}$.

Lemma 3.16. *For a fixed $d \geq 0$ and any k and k' with $0 \leq k < k' \leq d/2$, we have $\lambda_d(k) < \lambda_d(k')$.*

Proof. The result is immediate by induction, since

$$\lambda_d(k) - \lambda_d(k-1) = 2n + 4(d-2k) \geq 2n \geq 0$$

for $k \leq d/2$. □

Proof of the Decomposition

With these preliminaries complete, we may now prove Proposition 3.14.

Proof of Proposition 3.14. Since $\mathscr{P}_d^k$ is contained in the $\lambda_d(k)$-eigenspace of $\mathsf{F}\Delta$ and $\lambda_d(k) \neq \lambda_d(k')$ for $k \neq k'$ by Lemma 3.16, the sum $\bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathscr{P}_d^k$ is direct. To see that this sum actually equals $\mathscr{P}_d \supseteq \bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathscr{P}_d^k$, we compare dimensions.

We have $\dim(\mathscr{P}_d^k) = \dim(\mathscr{P}_{d-2k}^0)$ because F is injective. Since

$$\mathscr{P}_{d-2k}^0 = \ker\left(\Delta : \mathscr{P}_{d-2k} \to \mathscr{P}_{d-2(k+1)}\right),$$

we obtain

$$\dim(\mathscr{P}_{d-2k}^0) \geq \dim(\mathscr{P}_{d-2k}) - \dim(\mathscr{P}_{d-2(k+1)}). \tag{3.16}$$

We then compute

$$\begin{aligned}\dim(\mathscr{P}_d) \geq \dim\left(\bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathscr{P}_d^k\right) &= \sum_{k=0}^{\lfloor d/2 \rfloor} \dim(\mathscr{P}_d^k) = \sum_{k=0}^{\lfloor d/2 \rfloor} \dim(\mathscr{P}_{d-2k}^0) \\ &\geq \sum_{k=0}^{\lfloor d/2 \rfloor} \left(\dim(\mathscr{P}_{d-2k}) - \dim(\mathscr{P}_{d-2(k+1)})\right) = \dim(\mathscr{P}_d). \end{aligned} \tag{3.17}$$

Thus, we must have equality in (3.16) for all k, hence $\Delta|_{\mathscr{P}_{d-2k}}$ is surjective for all k. This proves the first and fourth parts of the proposition, and the decomposition

$$\mathscr{P}_d = \bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathscr{P}_d^k \tag{3.18}$$

also follows from (3.17).[7] To see the remainder of the second part of the proposition, we simply note that $\mathscr{P}_d^k = \mathsf{F}\mathscr{P}_{d-2}^{k-1}$ for each $k > 0$ and compare the decompositions (3.18) of $\mathscr{P}_d$ and $\mathscr{P}_{d-2}$. Since the spaces $\mathscr{P}_d^k$ are $\lambda_d(k)$-eigenspaces of $\mathsf{F}\Delta|_{\mathscr{P}_d}$, the decomposition (3.18) diagonalizes $\mathsf{F}\Delta|_{\mathscr{P}_d}$; the third part of the proposition then follows. □

[7] Specifically, equality in (3.17) implies that $\dim(\mathscr{P}_d) = \dim(\bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathscr{P}_d^k)$.

3.2.3 The Connection with $\mathfrak{sl}_2$

The development of the harmonic weight enumerator theory we present in Sections 5.2 and 5.3 relies heavily upon connections between the spaces of the *discrete harmonic polynomials* and the finite-dimensional representation theory of $\mathfrak{sl}_2$, the complex Lie algebra generated by

$$\mathsf{X} = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \quad \mathsf{H} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \quad \mathsf{Y} = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right).$$

The discussion in this section may be interpreted in terms of the *inifinite*-dimensional representation theory of $\mathfrak{sl}_2$. Specifically, the commutation relations obtained in Lemma 3.15 imply an isomorphism of Lie algebras between $\mathfrak{sl}_2$ and the span of $\left\{\Delta, \mathsf{E} + \frac{n}{2}, \mathsf{F}\right\}$:

$$\mathsf{X} \longleftrightarrow \frac{1}{2}\Delta, \quad \mathsf{H} \longleftrightarrow -\left(\mathsf{E} + \frac{n}{2}\right), \quad \mathsf{Y} \longleftrightarrow -2\mathsf{F}. \tag{3.19}$$

An analogous isomorphism is key to our discussion in Section 5.2.

3.3 The Functional Equation for Weighted Theta Functions

In this section, we derive the following functional equation for the weighted theta series $\Theta_{L,P}(q)$ of a lattice $L \subset \mathbb{R}^n$.

Theorem 3.17. *For any lattice $L \subset \mathbb{R}^n$, real $t > 0$, and $P \in \mathscr{P}_d^0$, the weighted theta series $\Theta_{L,P}$ satisfies the functional equation*

$$\Theta_{L,P}\left(e^{-2\pi t}\right) = \frac{1}{\mathrm{vol}(\mathbb{R}^n/L)} i^{-d} t^{\frac{n}{2}+d} \Theta_{L^*,P}\left(e^{-2\pi/t}\right).^{8}$$

This result fully generalizes Lemma 3.7 to the case of weighted theta functions.[9] Our path to Theorem 3.17 will follow that of Elkies [Elk09b]. This approach will also guide our development of the harmonic weight enumerator theory in Section 5.3. Iwaniec [Iwa97, pp. 167–168] gives another approach to Theorem 3.17, via a different development of the theory of harmonic polynomials.

The key application of Theorem 3.17 in our discussion is the following corollary which we prove in Section 3.3.2.

Theorem 3.18. *For L a Type II lattice of rank n and $P \in \mathscr{P}_d^0$, the weighted theta function $\theta_{L,P}$ is a modular form of weight $\frac{n}{2} + d$. Furthermore, $\theta_{L,P}$ is a cusp form if $d > 0$.*

[8] Here and hereafter, $t^{\frac{n}{2}+d}$ denotes the $(n + 2d)$-th power of the principal square root of t.

[9] Lemma 3.7 follows from Theorem 3.17 upon taking $P \in \mathscr{P}_0^0 = \mathscr{P}_0$.

This result may be derived in a (mostly) elementary but less structural fashion by explicit computation. Ebeling [Ebe02, pp. 87–99] presents this approach, in which an analog of Theorem 3.17 arises as an intermediate step.

3.3.1 Derivation of the Functional Equation

We now develop the machinery required in the proof of Theorem 3.17.

Conjugation of $\mathsf{\Delta}$, E, and F by the Fourier transform

First, we derive conjugation relations which relate the Fourier transform $\hat{f}$ of a function $f \in \mathcal{S}$ with the Fourier transforms of $\mathsf{\Delta} f$, $\mathsf{E} f$, and $\mathsf{F} f$.

Lemma 3.19. *For any j ($1 \leq j \leq n$), the Fourier transforms of $\partial f / \partial x_j$ and $x_j f$ are respectively $-2\pi i y_j \hat{f}$ and $(2\pi i)^{-1} \partial \hat{f} / \partial y_j$. (Here, $\{x_j\}$ and $\{y_j\}$ are respectively the coordinate systems of the domain and range of the Fourier transform.)*

Proof. The first claim follows immediately upon integration by parts. The second follows upon differentiating the integral defining $\hat{f}$:

$$\frac{\partial}{\partial y_j} \hat{f}(y) = \frac{\partial}{\partial y_j} \int_{\mathbb{R}^n} f(x) e^{2\pi i \langle x, y \rangle} \, d\mu(x) = 2\pi i x_j f(x). \qquad \square$$

Lemma 3.20. *Let $f \in \mathcal{S}$. The Fourier transforms of $\mathsf{\Delta} f$, $(2\mathsf{E} + n) f$, and $\mathsf{F} f$ are respectively $-(2\pi)^2 \mathsf{F} \hat{f}$, $-(2\mathsf{E} + n) \hat{f}$, and $-(2\pi)^{-2} \mathsf{\Delta} \hat{f}$.*

Proof. The result follows from iterative applications of Lemma 3.19, used to compute the Fourier transforms of $\partial^2 f / \partial x_j^2$, $x_j \partial f / \partial x_j$, and $x_j^2 f$. For example, Lemma 3.19 gives that the Fourier transform of

$$\frac{\partial^2 f}{\partial x_j^2} = \frac{\partial \frac{\partial f}{\partial x_j}}{\partial x_j}$$

is equal to $(-2\pi i y_j)^2 \hat{f}$; we obtain the claimed relation for the Fourier transform of $\mathsf{\Delta} f$ from the sum $\sum_{j=1}^n (2\pi i)^2 y_j^2 \hat{f} = (2\pi i)^2 \mathsf{F} \hat{f}$. The claimed relation for $(2\mathsf{E} + n) f$ follows from the expression

$$(2\mathsf{E} + n) = \sum_{j=1}^n \left(x_j \frac{\partial}{\partial x_j} + \frac{\partial}{\partial x_j} \circ x_j \right). \qquad \square$$

Multiplication by Gaussians

We introduce the family of operators $\{\mathsf{G}_t\}_{t\in\mathbb{C}}$ defined by

$$\mathsf{G}_t : \mathscr{C}^\infty(\mathbb{R}^n) \to \mathscr{C}^\infty(\mathbb{R}^n), \quad g \xmapsto{\mathsf{G}_t} e^{-\pi t\langle x,x\rangle} \cdot g.$$

For each $t \in \mathbb{C}$, the operator G_t is multiplication by the Gaussian $e^{-\pi t\langle x,x\rangle}$. Clearly, we have $\mathsf{G}_t\mathsf{G}_{t'} = \mathsf{G}_{t+t'}$, hence these operators form a group parameterized by $t \in \mathbb{C}$ with $\mathsf{G}_t^{-1} = \mathsf{G}_{-t}$.

We now show two disjoint results which will both be crucial in the proof of Theorem 3.17. The first shows that if $f \in \mathsf{G}_t\mathscr{P}$, then $\hat{f} \in \mathsf{G}_{1/t}\mathscr{P}$. The second gives relations for the conjugation of Δ, E, and F by G_t.

Lemma 3.21. *Let $t \in \mathbb{C}$ with $\mathrm{Re}(t) > 0$ and suppose that $P \in \mathscr{P}_d$. Then, the Fourier transform of G_tP is equal to $\mathsf{G}_{1/t}\hat{P}$ for some $\hat{P} = \sum_{d'=0}^{d} \hat{P}_{d'}$ with $\hat{P}_{d'} \in \mathscr{P}_{d'}$ for each d' ($0 \le d' \le d$) and $\hat{P}_d = i^d t^{-\left(\frac{n}{2}+d\right)}P$.*

Proof. The proof proceeds by induction upon d, with equation (3.10) serving as the base case. We suppose that we have shown the result for $P \in \mathscr{P}_d$ and proceed to show the claim for $P \in \mathscr{P}_{d+1}$.

Since the Fourier transform is linear and $\mathscr{P}_{d+1} = (x_1\mathscr{P}_d) + \cdots + (x_n\mathscr{P}_d)$, it suffices to show the result for each x_jP ($1 \le j \le n$) with $P \in \mathscr{P}_d$. Now, by Lemma 3.19, we may compute that the Fourier transform of $\mathsf{G}_tx_jP = x_j\mathsf{G}_tP$ is

$$\frac{1}{2\pi i}\frac{\partial}{\partial y_j}\left(\mathsf{G}_{1/t}\hat{P}\right) = \mathsf{G}_{1/t}\left(\frac{1}{2\pi i}\left(\frac{\partial \hat{P}}{\partial y_j} - \frac{2\pi}{t}y_j\hat{P}\right)\right). \tag{3.20}$$

Now, $\hat{P} \in \mathscr{P}_d$ and has leading term $\hat{P}_d = i^d t^{-\left(\frac{n}{2}+d\right)}P$, by the inductive hypothesis. It follows that the term

$$\frac{1}{2\pi i}\left(\frac{\partial \hat{P}}{\partial y_j} - \frac{2\pi}{t}y_j\hat{P}\right)$$

of (3.20) is of degree $d+1$ with leading term $-\hat{P}_d/it = i\hat{P}_d/t = i^{d+1}t^{-\left(\frac{n}{2}+d+2\right)}y_jP$; this completes the induction. □

Lemma 3.22. *We have the relations*

$$\mathsf{G}_t\Delta\mathsf{G}_{-t} = \Delta + \pi t(4\mathsf{E} + 2n) + (2\pi t)^2\mathsf{F}, \quad \mathsf{G}_t\mathsf{E}\mathsf{G}_{-t} = \mathsf{E} + 2\pi t\mathsf{F}, \quad \mathsf{G}_t\mathsf{F}\mathsf{G}_{-t} = \mathsf{F}. \tag{3.21}$$

Proof. We note that $\mathsf{G}_tx_j = x_j\mathsf{G}_t$, hence the operators G_t clearly commute with F. Additionally, $\mathsf{G}_t(\partial/\partial x_j)\mathsf{G}_{-t} = 2\pi t x_j$, from which the conjugation relation for E follows quickly. The commutation relation for Δ follows similarly, by a longer computation. □

Corollary 3.23. *The operators* Δ, E, *and* F *act on* $\mathsf{G}_t\mathscr{P}$. *The subspace* $\mathsf{G}_t\mathscr{P}_d^0$ *is the intersection of* $\ker\big(\Delta + \pi t(4\mathsf{E}+2n) + (2\pi t)^2\mathsf{F}\big)$ *with the* d*-eigenspace of* $\mathsf{E}+2\pi t\mathsf{F}$ *in* $\mathsf{G}_t\mathscr{P}_d^0$.

Proof of the Functional Equation

We have developed all the ingredients required in the proof of Theorem 3.17. As a final intermediate step, we prove an expression for the Fourier transform of the product of the Gaussian $e^{-\pi\langle x,x\rangle}$ and a harmonic polynomial.

Proposition 3.24. *Fix* $t > 0$ *and* $P \in \mathscr{P}_d^0$ *and let* $f = \mathsf{G}_tP$. *Then, the Fourier transform* $\hat{f}$ *of* f *is given by*

$$i^d t^{-\left(\frac{n}{2}+d\right)}\mathsf{G}_{1/t}P. \tag{3.22}$$

Proof. By Corollary 3.23, we have that

$$\big(\Delta + \pi t(4\mathsf{E}+2n) + (2\pi t)^2\mathsf{F}\big)\, f = 0, \quad (\mathsf{E}+2\pi t\mathsf{F})\, f = d\cdot f. \tag{3.23}$$

Applying Lemma 3.20 to the Fourier transforms of the expressions in (3.23), we obtain

$$\big(-2(\pi)^2\mathsf{F} - \pi t\,(4\mathsf{E}+2n) - t^2\Delta\big)\,\hat{f} = 0, \quad -\left(\mathsf{E}+n+\frac{t}{2\pi}\Delta\right)\hat{f} = d\cdot\hat{f}. \tag{3.24}$$

By Lemma 3.21, we have $\hat{f} = \mathsf{G}_{1/t}\hat{P}$ for some $\hat{P}\in\mathscr{P}$. From (3.24), we then compute that

$$\mathsf{G}_{1/t}(d\cdot\hat{P}) = d\cdot\hat{f} = \left(\mathsf{E}+\frac{2\pi}{t}\mathsf{F}\right)\hat{f} = \left(\mathsf{E}+\frac{2\pi}{t}\mathsf{F}\right)\mathsf{G}_{1/t}\hat{P} = \mathsf{G}_{1/t}\mathsf{E}\hat{P}, \tag{3.25}$$

where the last equality is a consequence of Lemma 3.22. But (3.25) implies that $\hat{P}$ is in the d-eigenspace of E; that is, $\hat{P}\in\mathscr{P}_d$. Lemma 3.21 then gives that $\hat{P} = i^d t^{-\left(\frac{n}{2}+d\right)}P$ as desired. □

Finally, we note that Theorem 3.17 follows almost immediately from Proposition 3.24.

Proof of Theorem 3.17. The result follows directly upon application of the Poisson summation formula (Theorem 3.5) to G_tP, using the expression (3.22) for the Fourier transform of G_tP obtained in Proposition 3.24. □

3.3.2 Weighted Theta Functions as Modular Forms

Now, just as in the proof of Theorem 3.6, we will quickly obtain the fact that $\theta_{L,P}$ is a modular form whenever $L\subset\mathbb{R}^n$ is Type II and $P\in\mathscr{P}_d^0$. Indeed, this fact follows quickly from Theorem 3.17 upon proving that $\theta_{L,P}$ is holomorphic on $\mathcal{H}$.

Lemma 3.25. *For any lattice $L \subset \mathbb{R}^n$ and $P \in \mathscr{P}_d^0$, the theta function $\theta_{L,P}(z)$ converges to a holomorphic function for all $z \in \mathcal{H}$.*

Proof. As in the proof of Lemma 3.8, it suffices to show that $\theta_{L,P}(z)$ converges absolutely and uniformly for all z in some half-plane $\mathcal{H}' \subseteq \mathcal{H}$. This follows from essentially the same argument used to prove Lemma 3.8 once we note that

$$\sum_{x \in \mathbb{Z}^n} P(x) e^{-\pi z_0 \epsilon \langle x,x \rangle} < \infty. \qquad \square$$

Lemma 3.26. *For any self-dual lattice $L \subset \mathbb{R}^n$, harmonic polynomial $P \in \mathscr{P}_d^0$, and nonzero $z \in \mathcal{H}$, the weighted theta function $\theta_{L,P}$ satisfies the identity*

$$\theta_L\left(-\frac{1}{z}\right) = i^{-d} \left(\frac{z}{i}\right)^{\frac{n}{2}+d} \theta_L(z). \tag{3.26}$$

Proof. We follow an argument analogous to that for Lemma 3.9. We know that both sides of (3.26) are holomorphic in $z \in \mathcal{H}$, by Lemma 3.25. We therefore need only prove (3.26) when $t > 0$ is real and $z = it$. We have $\operatorname{vol}(\mathbb{R}^n/L) = 1$ since $L = L^*$. Then, the identity (3.26) follows from Theorem 3.17 because we have $\theta_{L,P}(it) = \sum_{x \in L} P(x) e^{-\pi t \langle x,x \rangle} = \Theta_{L,P}\left(e^{-2\pi t}\right)$ and $\theta_{L,P}(-1/it) = \sum_{x \in L} P(x) e^{-\pi \langle x,x \rangle / t} = \Theta_{L,P}\left(e^{-2\pi/t}\right)$. $\square$

Theorem 3.18 now follows immediately from Lemma 3.26.

Proof of Theorem 3.18. From Lemma 3.26, we have the identity

$$\theta_L\left(-\frac{1}{z}\right) = (-1)^{\frac{n}{4}} z^{\frac{n}{2}+d} \theta_L(z). \tag{3.27}$$

Since L is of Type II, we have $n \equiv 0 \bmod 8$ by Theorem 3.6. The fact that $\theta_{L,P}$ is a modular form of weight $\frac{n}{2} + d$ then follows immediately from (3.27) and Lemma 3.25. Now, the constant term of $\theta_{L,P}(z)$ is $\sum_{x \in L_0} P(x) e^{-\pi i z \langle x,x \rangle} = \sum_{x \in L_0} P(x) = P(0)$; this expression vanishes when $d > 0$. Thus, we see that $\theta_{L,P}$ is a cusp form when $d > 0$. $\square$

3.4 Zonal Spherical Harmonic Polynomials

In this section, we introduce a special class of harmonic polynomials, called the *zonal spherical harmonic polynomials*, which will be useful for the applications we present in Chapter 4. These polynomials are invariant under orthogonal transformations fixing a given vector $\dot{x} \in \mathbb{R}^n$.

Consequently, the zonal spherical harmonic polynomials admit an expression in terms of the *Gegenbauer polynomials of parameter* $\frac{n}{2} - 1$, a well-known class $\{G_d\}_{d=0}^{\infty}$ of degree-indexed orthogonal polynomials which satisfy the following differential equation:

$$(1 - z^2)G_d''(z) - (n-1)zG_d'(z) + d(n-2+d)G_d(z) = 0.^{10} \tag{3.28}$$

3.4.1 Preliminaries

We fix some $\dot{x} \in \mathbb{R}^n$ throughout. We denote the space of degree-d homogeneous polynomials invariant under orthogonal transformations fixing $\dot{x}$ by $\mathscr{Z}\mathscr{P}_d \subset \mathscr{P}_d$, and define the *space of degree-d zonal spherical harmonic polynomials* $\mathscr{Z}\mathscr{P}_d^0$ by

$$\mathscr{Z}\mathscr{P}_d^0 := \mathscr{Z}\mathscr{P}_d \cap \mathscr{P}_d^0.$$

Finally, we define the space $\mathscr{Z}\mathscr{P}^0$ of *zonal spherical harmonic polynomials* by

$$\mathscr{Z}\mathscr{P}^0 := \bigcup_{d=0}^{\infty} \mathscr{Z}\mathscr{P}_d^0.$$

First, we observe the following lemma.

Lemma 3.27. *If $f : \mathbb{R}^n \to \mathbb{C}$ is invariant under orthogonal transformations fixing $\dot{x} \in \mathbb{R}^n$, then $f(x)$ can be expressed as a function of $\langle x, x\rangle$ and $\langle x, \dot{x}\rangle$.*

Proof. Without loss of generality, we may assume that $\dot{x} = \varepsilon^{(n)}$, whence we translate the invariance condition into invariance under O_{n-1}. Now, for any $x, x' \in \mathbb{R}^{n-1}$ with $\langle x, x\rangle = \langle x', x'\rangle$, there is a transformation in O_{n-1} taking $x \mapsto x'$. We therefore see that we must have $f(x) = f(x')$ for any $x, x' \in \mathbb{R}^n$ with $x_n = x_n'$ and

$$\langle (x_1, \ldots, x_{n-1}), (x_1, \ldots, x_{n-1})\rangle = \langle (x_1', \ldots, x_{n-1}'), (x_1', \ldots, x_{n-1}')\rangle.$$

It then follows that we may express $f(x)$ in terms of $\langle x, x\rangle$ and $\langle x, \dot{x}\rangle$, since

$$\langle x, \dot{x}\rangle = \langle x, \varepsilon^{(n)}\rangle = x_n. \qquad \square$$

As the zonal spherical harmonic polynomials are homogeneous polynomial functions, the following corollary is immediate from Lemma 3.27.

Corollary 3.28. *If $P \in \mathscr{Z}\mathscr{P}^0$, then P is a homogeneous polynomial in $\langle x, x\rangle$ and $\langle x, \dot{x}\rangle$.*

[10] See [Vil68, pp. 457–468] for facts regarding the polynomials G_d, including the power series expression for $G_d(z)$ (see [Vil68, p. 458]) and for a development of the differential equation (3.28) (see [Vil68, p. 459]).

3.4.2 Determination of the Zonal Spherical Harmonic Polynomials

Now, we determine the zonal spherical harmonic polynomials explicitly, in terms of the Gegenbauer polynomials. For this characterization, we let $\dot{G}_d(\cdot,\cdot)$ denote the homogeneous polynomial such that $\dot{G}_d(t,1) = G_d(t)$.

Proposition 3.29. *If $P \in \mathscr{Z}\mathscr{P}_d^0$, then $d \in 2\mathbb{Z}$ and $P = b \cdot P_{d;\dot{x}}$ for some constant b, where $P_{d;\dot{x}}$ is the zonal spherical harmonic polynomial defined by*

$$P_{d;\dot{x}}(x) = \dot{G}_d\left(\langle x,\dot{x}\rangle, (\langle x,x\rangle\langle \dot{x},\dot{x}\rangle)^{1/2}\right).$$

Proof. By Corollary 3.28, we must have $d \in 2\mathbb{Z}$ and we may write an arbitrary $P \in \mathscr{Z}\mathscr{P}_d^0$ in the form

$$P = \sum_{k=0}^{d/2} b_{d-2k} \cdot \langle x,x\rangle^k \langle x,\dot{x}\rangle^{d-2k}, \tag{3.29}$$

for constants $\{b_{d-2k}\}_{k=0}^{d/2}$. Without loss of generality, we may assume that $\dot{x} = \varepsilon^{(n)}$, so that (3.29) simplifies to

$$P = \sum_{k=0}^{d/2} b_{d-2k} \cdot \langle x,x\rangle^k x_n^{d-2k}. \tag{3.30}$$

To show the proposition, it suffices to show that the ratios between consecutive coefficients of P are the same as those between consecutive coefficients of the even-degree powers of t in $G_d(t)$.[11] We now demonstrate this fact via explicit computation.

First, we use (3.30) to compute ΔP, which must vanish since $P \in \mathscr{Z}\mathscr{P}_d^0 \subset \mathscr{P}_d^0$:

$$0 = \Delta P = \sum_{k=0}^{d/2} b_{d-2k} \cdot \Big((2k(2(k-1) + n + 2(d-2k)))\, \langle x,x\rangle^{k-1} x_n^{d-2k} \\ + (d-2k)(d-2k-1)\langle x,x\rangle^k x_n^{d-2(k+1)} \Big). \tag{3.31}$$

Upon comparing the coefficients of $\langle x,x\rangle^{k-1} x_n^{d-2k}$ in (3.31), we observe that

$$\frac{b_{d-2k}}{b_{d-2(k-1)}} = -\frac{2k(2d-2k+n-2)}{(d-2k+1)(d-2k+2)}. \tag{3.32}$$

[11] This suffices because the coefficients of odd-degree powers of t in the Gegenbauer polynomials of even degree vanish (see [Vil68, p. 458]).

Now, if we express the even-degree part of G_d in the form $\sum_{k=0}^{d/2} b'_{d-2k} \cdot z^{d-2k}$, then the differential equation (3.28) implies that

$$\begin{aligned} 0 = (1-z^2) &\sum_{k=0}^{d/2} b'_{d-2k} \cdot (d-2k)(d-2k-1) z^{d-2k-2} \\ &+ (n-1)z \sum_{k=0}^{d/2} b'_{d-2k} \cdot (d-2k) z^{d-2k-1} + d(n-2+d) \sum_{k=0}^{d/2} b'_{d-2k} \cdot z^{d-2k}. \end{aligned} \tag{3.33}$$

Equating coefficients of z^{d-2k} in (3.33) shows that

$$\begin{aligned} \frac{b'_{d-2k}}{b'_{d-2(k-1)}} &= \frac{(d-2k)(d-2k-1) + (n-1)(d-2k) - d(n-2+d)}{(d-2(k-1))(d-2(k-1)-1)} \\ &= -\frac{2k(2d-2k+n-2)}{(d-2k+1)(d-2k+2)}. \end{aligned} \tag{3.34}$$

As (3.32) and (3.34) agree, we have shown the result. □

Chapter 4

Configurations of Type II Lattices

In this chapter, we apply the powerful weighted theta function machinery developed in Chapter 3. Many of the applications we present are *configuration results*, characterizing the possible configurations of short vectors of Type II lattices of certain ranks.[1] These results are derived via the theory of modular forms, hence we may discuss and obtain configuration results for extremal Type II lattices in dimensions where it is not yet known whether such lattices exist.

Weighted theta function methods suffice to give a full classification of the Type II lattices of ranks at most 24. Following classical approaches, we discuss the classifications of these lattices in Section 4.1.

As we mentioned in Section 2.1.4, a full classification of Type II lattices of ranks at least 32 appears to be out of reach. Nonetheless, we may use weighted theta functions to obtain configuration results for such lattices. In Section 4.3, we derive configuration results for extremal Type II lattices of ranks $n = 8, 24, 32, 40, 48, 56, 72, 80, 96, 120$. The results for $n = 8, 24$ are well-known[2]; those for $n = 32$ are originally due to Ozeki [Oze86a] and Venkov [Ven84a]; those for $n = 40, 48$ are due to Ozeki [Oze89] and [Oze86b], respectively; those for dimensions $n = 56, 72, 96$ are original to the author [Kom09]; and those for $n = 80, 120$ are original to the author and Abel [KA08]. We prove all of these configuration results in Section 4.3, using a unified method drawn from the approaches of [Kom09] and [KA08]. This method somewhat simplifies

[1] Our use of the term "configuration" for such results follows the previous literature: [Ven80], [Oze86a], and [Oze86b].

[2] As Theorems 3.10 and 4.2 indicate, there are unique extremal Type II lattices of ranks $n = 8, 24$. The configuration results for such lattices can therefore implicitly be obtained from the lattices themselves. As we show at the end of Section 4.3.2, these configuration results may also be derived via weighted theta function methods. This approach yields the configuration results independently of the classification results in these dimensions. This is a useful exercise, since configuration results of the sort we prove can be to show classification results.

the arguments of [Oze86a], [Ven84a], [Oze89], and [Oze86b]. Then, we prove a new configuration result of Elkies and the author [EK09b] for extremal Type II lattices of ranks $n = 40, 80$.

In Chapter 6, we present coding-theoretic results analogous to the results of this chapter for extremal Type II lattices of ranks $n = 8, 24, 32, 48, 56, 72, 96$. Our approaches to these coding-theoretic results exploit several analogies with the methods of this chapter.

4.1 Type II Lattices of Rank 24

In this section, we state and discuss the classification of rank-24 Type II lattices. Although we do not fully prove this result, we do derive a condition on the root systems of such lattices. Using this condition, we give proofs of the classifications of Type II lattices of ranks 8 and 16 alternate to those presented in Section 3.1.3.

4.1.1 Preliminaries

Much of the discussion in this section will use the following lemma.

Lemma 4.1. *Let L be a Type II lattice of rank $n = 8, 16, 24$. Then,*

1. *for all $\dot{x} \in \mathbb{R}^n$, we have $\sum_{x \in L_2} \langle x, \dot{x}\rangle^2 = \frac{1}{n} \cdot 2 \cdot a_2(L) \cdot \langle \dot{x}, \dot{x}\rangle$,*
2. *either $L_2 = \emptyset$ or L_2 spans $L \otimes \mathbb{R}$, and*
3. *all irreducible components of $\mathcal{L}_2(L)$ have Coxeter number equal to $a_2(L)/n$.*

Proof. First, we fix some $\dot{x} \in L \otimes \mathbb{R}$ and recall the explicit form of the polynomial $P_{2;\dot{x}}$:

$$P_{2;\dot{x}}(x) = \langle x, \dot{x}\rangle^2 - \frac{\langle x, x\rangle\langle \dot{x}, \dot{x}\rangle}{n}. \tag{4.1}$$

By Theorem 3.18, $\theta_{L,P_{2;\dot{x}}}$ is a cusp form of weight $(n+4)/2$. By comparing power series coefficients, it follows from Theorem 3.2 that

$$\sum_{x \in L_2} \left(\langle x, \dot{x}\rangle^2 - \frac{\langle x, x\rangle\langle \dot{x}, \dot{x}\rangle}{n} \right) = \sum_{x \in L_2} P_{2;\dot{x}}(x) = 0.$$

We then find that

$$\sum_{x \in L_2} \langle x, \dot{x}\rangle^2 = \frac{1}{n} \left(\sum_{x \in L_2} \langle x, x\rangle \right) \langle \dot{x}, \dot{x}\rangle = \frac{1}{n} \cdot 2 \cdot a_2(L) \cdot \langle \dot{x}, \dot{x}\rangle; \tag{4.2}$$

this proves the first part of the lemma.

Now, if there were some $\dot{x} \in L \otimes \mathbb{R}$ not in the span of L_2, then the left side of (4.2) would vanish. In this case, however, we would need $a_2(L) = 0$; the second part of the lemma then follows. The third part of the lemma follows from (2.4) and (4.2), upon taking $\dot{x}$ to lie in an irreducible component of $\mathcal{L}_2(L)$. □

We also recall the Coxeter numbers of the irreducible root lattices, which we first stated in (2.3):

$$h(A_n) = n + 1, \quad h(D_n) = 2(n - 1), \quad h(E_6) = 12, \quad h(E_7) = 18, \quad h(E_8) = 30.$$

4.1.2 Niemeier's Classification and Venkov's Root System Condition

Niemeier [Nie73] fully classified the Type II lattices of rank 24, showing in particular that these lattices are characterized by their root systems. Specifically, he proved the following theorem.

Theorem 4.2 ([Nie73])**.** *There are precisely* 24 *Type II lattices* L *of rank* 24*, up to isomorphism. Each of these lattices* L *is uniquely determined by its root sublattice* $\mathcal{L}_2(L)$*.*

Venkov [Ven80] rederived Theorem 4.2 via a more natural argument. Although we will not reproduce the complete proof of Theorem 4.2 here, we will prove the following intermediate result obtained by Venkov [Ven80].[3]

Proposition 4.3 ([Ven80])**.** *If* L *is a Type II lattice of rank* 24*, then* $\mathcal{L}_2(L)$ *is one of the following twenty-four lattices:*

$$\begin{gathered}
\emptyset, \quad A_1^{24}, \quad A_2^{12}, \quad A_3^{8}, \quad A_4^{6}, \quad A_6^{4}, \quad A_8^{3}, \quad A_{12}^{2}, \quad A_{24}, \\
D_4^{6}, \quad D_6^{4}, \quad D_8^{3}, \quad D_{12}^{2}, \quad D_{24}, \quad E_6^{4}, \quad E_8^{3}, \\
A_5^4 \oplus D_4, \quad A_7^2 \oplus D_5^2, \quad A_9^2 \oplus D_6, \quad A_{15} \oplus D_9, \\
A_{11} \oplus D_7 \oplus E_6, \quad A_{17} \oplus E_7, \quad D_{10} \oplus E_7^2, \quad D_{16} \oplus E_8.
\end{gathered}$$

Proof. The result follows immediately from the $n = 24$ case of Lemma 4.1. If $L_2 \neq \emptyset$ then $\mathcal{L}_2(L)$ takes the form $\mathcal{L}_2(L) = \bigoplus_{j=1}^{24} A_j^{\alpha_j} + \bigoplus_{k=4}^{24} D_k^{\beta_k} + \bigoplus_{\ell=6}^{8} E_\ell^{\gamma_\ell}$. From the second part of Lemma 4.1, we have that L_2 spans $L \otimes \mathbb{R}$, hence

$$\sum_{j=1}^{24} j\alpha_j + \sum_{k=4}^{24} k\beta_k + \sum_{\ell=6}^{8} \ell\gamma_\ell = 24.$$

[3] The proof that each of the possible candidates for $\mathcal{L}_2(L)$ listed in Proposition 4.3 corresponds to a unique Type II lattice is an exercise in coding theory rather far afield of our discussion. Details of this argument can be found in Venkov [Ven80].

Combining this equation with the condition that all irreducible components of $\mathcal{L}_2(L)$ have the same Coxeter number (the third part of Lemma 4.1), we quickly determine that the only possibilities for $\mathcal{L}_2(L)$ are those listed in the proposition statement.[4] □

Remarks

If C is a Type II code of length 24, then the lattice L_C obtained from applying Construction A to C is a Type II lattice of rank 24. It therefore follows from Proposition 4.3 that, for any such C, the tetrad subcode $\mathcal{C}_4(C)$ of C is equal to one of the following nine tetrad codes:

$$\emptyset, \quad d_4^6, \quad d_6^4, \quad d_8^3, \quad d_{12}^2, \quad d_{24}, \quad e_7^2 \oplus d_{10}, \quad e_8^3, \quad e_8 \oplus d_{16}.$$

Using the theory of harmonic weight enumerators developed in Chapter 5, we give a direct proof of this fact in Section 6.2.

Theorem 4.2 also implies more efficient proofs of Theorems 3.10 and 3.11.

Alternate Proofs of Theorems 3.10 and 3.11. Suppose that L is a Type II lattice of rank 8. Then, the lattice $L \oplus E_8 \oplus E_8$ is Type II of rank 24. By Proposition 4.3, $\mathcal{L}_2(L \oplus E_8) \cong E_8^3$. But then, we must have $L = E_8$; this proves Theorem 3.10.

Similarly, suppose that L is a Type II lattice of rank 16. Then, the lattice $L \oplus E_8$ is Type II of rank 24. By Proposition 4.3, $\mathcal{L}_2(L \oplus E_8)$ is either E_8^3 or $D_{16} \oplus E_8$, and by Theorem 4.2 we know that $L \oplus E_8$ is determined uniquely by $\mathcal{L}_2(L \oplus E_8)$. This, combined with the fact that the lattices E_8^2 and D_{16}^+ are distinct Type II lattices of rank 16, proves Theorem 3.11. □

4.2 Extremal Type II Lattices and Spherical t-Designs

We now present an important application of weighted theta functions which is relevant to our discussion in Section 4.3.

Theorem 4.4 ([Ven01])**.** *If L is an extremal Type II lattice of rank n, then L_m is a spherical $\big((2\mathrm{t}(n) + 1) + \frac{1}{2}\big)$-design for any $m > 0$ such that $L_m \neq \emptyset$, where*

$$\mathrm{t}(n) := \begin{cases} 5 & n \equiv 0 \bmod 24, \\ 3 & n \equiv 8 \bmod 24, \\ 1 & n \equiv 16 \bmod 24. \end{cases} \tag{4.3}$$

[4] This computation reduces to solving a system of linear equations in the α_j, β_k, and γ_ℓ. Explicit details are given in [Ven80].

Proposition 2.3, stated in Section 2.4.2, is a special case of this result. Our proof of Theorem 4.4 follows the argument of Venkov [Ven01]. The key to this approach is a proposition derived from the decomposition of $\mathscr{P}_d$ obtained in Proposition 3.14.

Proposition 4.5. *For a lattice L and $m > 0$ such that $L_m \neq \emptyset$, the set of vectors L_m is a spherical t-design if and only if*

$$\sum_{x \in L_m} P(x) = 0$$

for all $P \in \bigcup_{d=1}^{t} \mathscr{P}_d^0$.

Proof. The reverse direction is immediate, hence we must demonstrate only the forward direction. We must show that $\sum_{x \in L_m} P(x) = a_m(L) \int_{\Omega_n} P \, d\mu$ for any $P \in \bigcup_{d=0}^{t} \mathscr{P}_d$. But this is immediate from the hypothesis, since the second part of Proposition 3.14 shows that we may express any $P \in \bigcup_{d=1}^{t} \mathscr{P}_d$ as a sum of polynomials in the spaces $\mathscr{P}_d^k$ $(0 \leq k \leq \lfloor d/2 \rfloor)$. □

The proof of Theorem 4.4 follows naturally from Proposition 4.5.

Proof of Theorem 4.4. We fix a $d \in \{1, \ldots, 2\mathrm{t}(n)+1\} \cup \{2\mathrm{t}(n)+4\}$ and consider some $P \in \mathscr{P}_d^0$. Since L is of Type II, we know from Theorem 3.18 that

$$\theta_{L,P} \in \mathcal{M}^0_{\frac{n}{2}+d}.$$

Furthermore, since L is extremal, the coefficients of $q^1, \ldots, q^{\frac{\min(L)}{2}-1}$ in $\theta_{L,P}$ must vanish. It then follows that

$$\theta_{L,P} = \Delta^{\frac{\min(L)}{2}-1} \cdot f$$

for some $f \in \mathcal{M}_{\frac{n}{2}+d-12\lfloor\frac{n}{24}\rfloor}$. However, by Theorem 3.2, we have

$$\dim\left(\mathcal{M}_{\frac{n}{2}+d-12\lfloor\frac{n}{24}\rfloor}\right) = 0,$$

hence $f \equiv 0$. We then obtain

$$\sum_{m=0}^{\infty} \left(\sum_{x \in L_{2m}} P(x) \right) q^m = \theta_{L,P} \equiv 0.$$

By Proposition 4.5, this proves the theorem. □

Remarks

In Section 4.3, we use the parameter $\mathrm{t}(n)$ slightly more generally: to record the degrees for which we can determine information regarding the weighted theta functions $\theta_{L,P_{d;x_0}}$.[5] One result in this vein is immediate from the proof of Theorem 4.4.

Corollary 4.6. *If L is an extremal Type II lattice of rank n, then we have $\theta_{L,P_{d;x_0}} \equiv 0$ for any $d \in \{2, \ldots, 2\mathrm{t}(n)\} \cup \{2\mathrm{t}(n) + 4\}$.*

4.3 Configurations of Extremal Type II Lattices

4.3.1 Preliminaries

We recall the notation $\mathcal{L}_m(L)$ for the lattice generated by L_m. We adopt the slightly abusive notation of Ozeki [Oze89], writing $L_{m_1+\cdots+m_k} := \bigcup_{j=1}^{k} L_{m_j}$ and denoting by $\mathcal{L}_{m_1+\cdots+m_k}(L)$ the lattice generated by $L_{m_1+\cdots+m_k}$.[6]

For a lattice $L \subset \mathbb{R}^n$ and a vector $\dot{x} \in L \otimes \mathbb{R}$ and $j \in \mathbb{Z}$, we write

$$N_j(L; \dot{x}) := \left|\{x \in L_{\min(L)} : \langle x, \dot{x} \rangle = j\}\right|.$$

Via the involution $x \leftrightarrow -x$ of $L_{\min(L)}$, we see that $N_{-j}(L; \dot{x}) = N_j(L; \dot{x})$ for any $\dot{x}$ and j.

In the next sections, we examine the following question for several choices of $n = 8n'$.[7]

Question. *Let L be an extremal Type II lattice of rank n. What is the minimal value of $m_* \geq \min(L)$ such that*

$$L = \mathcal{L}_{\min(L)+\cdots+m_*}(L)? \tag{4.4}$$

We let L be an extremal Type II lattice of rank n and let

$$m_0 := \min(L) = 2\lfloor n/24 \rfloor + 2$$

be the minimal norm of vectors in L.[8] For $n = 32, 48, 56, 72, 96$, we show in Section 4.3.2 that the minimal value of m_* in (4.4) is as small as possible—in these cases, $m_* = m_0$. To prove a result of

[5] We also use this parameter in Chapter 6, since it indexes the values of t for which extremal Type II codes of length n yield t-designs.

[6] When this notation is potentially confusing, we will use parentheses to indicate norms. For example, we write $L_{m_1+m_2} = L_{m_1} \cup L_{m_2}$, while $L_{(m_1+m_2)}$ denotes the set of norm-$(m_1 + m_2)$ vectors of L.

[7] Since we are concerned with Type II lattices, it clearly only makes sense to consider n of this form.

[8] Recall the expression for the minimal norm of an extremal Type II lattice, given in equation (2.5).

this form, it suffices to show that every class $[x] \in L/(\mathcal{L}_{m_0}(L))$ is represented by a vector $\dot{x} \in [x]$ with norm $\langle \dot{x}, \dot{x} \rangle \leq m_0$.[9] Thus, we consider the equivalence classes of L modulo $\mathcal{L}_{m_0}(L)$.

Seeking a contradiction, we suppose that there is an equivalence class $[\dot{x}] \in L/(\mathcal{L}_{m_0}(L))$ with minimal-norm representative $\dot{x}$ of integral norm $\langle \dot{x}, \dot{x} \rangle = s > m_0$. In the remainder of this section, we develop a system of linear equations in the variables $N_j(L; \dot{x})$.

Lemma 4.7. *For all $x \in L_{m_0}$, we have the inequality*

$$|\langle x, \dot{x} \rangle| \leq \frac{m_0}{2}.$$

Proof. This is immediate, because if $\langle \pm x, \dot{x} \rangle > m_0/2$, then $[\dot{x}]$ contains a vector $x \mp \dot{x}$ of norm

$$\langle x \mp \dot{x}, x \mp \dot{x} \rangle = \langle x, x \rangle \mp 2\langle x, \dot{x} \rangle + \langle \dot{x}, \dot{x} \rangle < \langle \dot{x}, \dot{x} \rangle,$$

contradicting the minimality of $\dot{x}$ in $[\dot{x}]$. □

Lemma 4.8. *We have that*

$$a_{m_0}(L) = N_0(L; \dot{x}) + 2 \sum_{j=1}^{m_0/2} N_j(L; \dot{x}). \tag{4.5}$$

Proof. This is immediate, since Lemma 4.7 implies that the right side of (4.5) is equal to the number of vectors in L_{m_0}. □

Lemma 4.9. *We have the equations*

$$2 \sum_{j=1}^{m_0/2} j^{2k} \cdot N_j(L; \dot{x}) = a_{m_0}(L) \frac{1 \cdot 3 \cdots (2k-1)}{n \cdot (n+2) \cdots (n+2k-2)} m_0^k \langle \dot{x}, \dot{x} \rangle^k, \tag{4.6}$$

for $k \in \{1, \ldots, \mathrm{t}(n)\}$.

Proof. It follows from Corollary 4.6 that

$$\sum_{x \in L_{m_0}} \langle x, \dot{x} \rangle^{2k} = a_{m_0}(L) \frac{1 \cdot 3 \cdots (2k-1)}{n \cdot (n+2) \cdots (n+2k-2)} m_0^k \langle \dot{x}, \dot{x} \rangle^k, \tag{4.7}$$

for $k \in \{1, \ldots, \mathrm{t}(n)\}$.[10] Additionally, by Lemma 4.7, we have

$$\sum_{x \in L_{(m_0+2)}} \langle x, \dot{x} \rangle^{2k} = 2 \sum_{j=1}^{m_0/2} j^{2k} \cdot N_j(L; \dot{x}), \tag{4.8}$$

for all $k > 0$. Combining (4.7) with (4.8), we obtain the equations (4.6). □

[9] It suffices to show the existence of a representative $\dot{x} \in [x]$ with $\langle \dot{x}, \dot{x} \rangle = m_0$ for each $[x] \in L/(\mathcal{L}_{m_0}(L))$. Since L is extremal, $a_L(m) = 0$ for $0 < m < m_0$, hence we need only show that every class $[x] \in L/(\mathcal{L}_{m_0}(L))$ is represented by a vector $\dot{x} \in [x]$ with $\langle \dot{x}, \dot{x} \rangle \leq m_0$.

[10] The details of this computation can be found in [Ven01].

Remarks

We note that the result of Lemma 4.7 holds for all minimal representatives $\dot{x}$ of classes $[\dot{x}] \in (\mathcal{L}_{m_0}(L)^*)/(\mathcal{L}_{m_0}(L))$, hence the conclusions of Lemmata 4.8 and 4.9 hold for these $\dot{x}$ as well. We will use these observations in Section 4.3.3.

4.3.2 Extremal Type II Lattices of Ranks 32, 48, and 72

We now answer the easiest cases of the question introduced above: ranks $n = 32, 48, 72$.

Theorem 4.10. *If L is an extremal Type II lattice of rank $n = 32, 48, 72$, then*

$$L = \mathcal{L}_{m_0}(L).$$

Theorem 4.10 is an amalgam of configuration results from several sources. The rank 32 case was obtained concurrently by Ozeki [Oze86a] and Venkov [Ven84a], and the rank 48 case was first obtained by Ozeki [Oze86b]. The rank 72 case is original to the author [Kom09]. All three cases of Theorem 4.10 were originally proven using weighted theta functions, albeit via slightly different methods. Here, we give a unified argument for all three cases following the approach of [Kom09] which slightly simplifies the approaches of [Oze86a], [Ven84a], and [Oze86b].

Proof of Theorem 4.10. For the sake of contradiction, we suppose that there exists an equivalence class $[\dot{x}] \in L/(\mathcal{L}_{m_0}(L))$ with minimal-norm representative $\dot{x}$ of norm $\langle \dot{x}, \dot{x} \rangle = s$ for some $s > m_0$. Combining Lemma 4.8 with the $\mathrm{t}(n)$ equations of Lemma 4.9 gives a system of $\mathrm{t}(n) + 1$ equations in the

$$\frac{m_0}{2} + 1 < \mathrm{t}(n) + 1$$

variables $N_j(L; \dot{x})$ $(0 \leq j \leq m_0/2)$. For $n = 32, 48, 72$, the determinants of the (extended) $(\frac{m_0}{2} + 2) \times (\frac{m_0}{2} + 2)$ matrices for these inhomogeneous systems[11] are respectively

$$2^8 3^3 5^1 s \left(5s^2 - 45s + 102\right), \tag{4.9}$$

$$2^{13} 3^6 5^2 7^1 s \left(35s^3 - 630s^2 + 3822s - 7800\right), \tag{4.10}$$

$$2^{22} 3^9 5^4 7^2 s \left(42s^4 - 1400s^3 + 17745s^2 - 101270s + 219336\right). \tag{4.11}$$

Since each system is overdetermined, these determinants must vanish. However, the equations (4.9)–(4.11) have no integer solutions $s > 0$. It then follows that there is no equivalence class

[11] When there are more than $\frac{m_0}{2} + 2$ equations, we omit the equations obtained from the zonal spherical harmonic polynomials of the largest degrees.

$[\dot{x}] \in L/(\mathcal{L}_{m_0}(L))$ with minimal-norm representative $\dot{x}$ of norm $\langle \dot{x}, \dot{x} \rangle = s > m_0$, so we have the desired result. □

Remarks

The methods used to prove Theorem 4.10 also show

$$\mathcal{L}_2(E_8) = E_8, \quad \mathcal{L}_4(\Lambda_{24}) = \Lambda_{24}.$$

In these cases, the determinants

$$24s(3s-5), \quad 34560s\left(15s^2 - 105s + 182\right)$$

are obtained. As neither of these determinants has integral roots $s > 0$, we conclude the following theorem.

Theorem 4.11. *If L is an extremal Type II lattice of rank $n = 8, 24$ then $L = \mathcal{L}_{m_0}(L)$.*

However, the analogous result does not hold for extremal Type II lattices of rank 16. Indeed, the lattice D_{16}^+ is not generated by its minimal vectors; $D_{16}^+/\mathcal{L}_2(D_{16}^+)$ has equivalence classes with minimal-norm representatives of norm 4. In this case, the (extended) matrix of the system of equations obtained from Lemmata 4.8 and 4.9 has determinant

$$-1774080(s-4)(s-1)s.$$

As expected, this determinant vanishes at $s = 4$.

4.3.3 Extremal Type II Lattices of Ranks 56 and 96

With a little more effort, we can prove a result of the author [Kom09] analogous to Theorem 4.10 for extremal Type II lattices of ranks $n = 56, 96$.

Theorem 4.12. *If L is an extremal Type II lattice of rank $n = 56, 96$, then*

$$L = \mathcal{L}_{m_0}(L).$$

Before we can prove this result, we need the following lemma which extends the second conclusion of Lemma 4.1 to all extremal Type II lattices.

Lemma 4.13. *For L an extremal Type II lattice of rank n, let $m > 0$ be such that L_m is nonempty. Then, L_m spans $L \otimes \mathbb{R}$.*

Proof. We fix some $\dot{x} \in L \otimes \mathbb{R}$. By Corollary 4.6, we have

$$\sum_{x \in L_m} P_{2;\dot{x}}(x) = 0. \tag{4.12}$$

Upon substituting the explicit form (4.1) of $P_{2;\dot{x}}$ into (4.12), we find

$$\sum_{x \in L_m} \langle x, \dot{x} \rangle^2 = \frac{1}{n} \left(\sum_{x \in L_m} \langle x, x \rangle \right) \langle \dot{x}, \dot{x} \rangle = \frac{1}{n} \cdot m \cdot a_m(L) \cdot \langle \dot{x}, \dot{x} \rangle. \tag{4.13}$$

Now, if there were some $\dot{x} \in L \otimes \mathbb{R}$ not in the span of L_m, then the left side of (4.13) would vanish, implying $a_m(L) = 0$. By hypothesis, however, we have required $a_m(L) > 0$; the lemma follows. □

Proof of Theorem 4.12. We suppose that $\mathcal{L}_{m_0}(L) \neq L$ and consider $\mathcal{L}_{m_0}(L)^*$. We cannot have $\mathcal{L}_{m_0}(L)^* = \mathcal{L}_{m_0}(L)$, since in that case $\mathcal{L}_{m_0}(L)$ would be an extremal Type II lattice of rank n by Lemma 4.13. (Since L is itself of rank n, this would imply that $\mathcal{L}_{m_0}(L) = L$.)

Thus, there is some equivalence class $[\dot{x}] \in (\mathcal{L}_{m_0}(L)^*)/(\mathcal{L}_{m_0}(L))$ with minimal-norm representative $\dot{x}$ of rational norm $\langle \dot{x}, \dot{x} \rangle = s > 0$. As remarked above, the equations (4.5) and (4.7) are satisfied. Combining these $\mathrm{t}(n) + 1$ equations with the condition

$$\theta_{L, P_{2\mathrm{t}(n)+4;\dot{x}}} \equiv 0$$

of Corollary 4.6 gives a system of $\mathrm{t}(n) + 2$ equations in the

$$\frac{m_0}{2} + 1 < \mathrm{t}(n) + 2$$

variables $N_j(L; \dot{x})$ $(0 \leq j \leq m_0/2)$. For $n = 56, 96$, the determinants of the (extended) matrices for these inhomogeneous systems are respectively

$$-2^{23} 3^{10} 5^3 7^2 11^1 17^1 29^1 31^1 (s - 8) s \left(9s^3 - 168s^2 + 1008s - 1856 \right), \tag{4.14}$$

$$-2^{42} 3^{15} 5^{10} 7^5 11^1 13^1 17^1 19^1 29^1 47^1 53^1 59^1 (s - 12) s R_{96}(s), \tag{4.15}$$

where $R_{96}(s) = 25s^5 - 1275s^4 + 26112s^3 - 267444s^2 + 1362720s - 2741760$. These determinants must vanish, but all the rational solutions of equations (4.14) and (4.15) are even. We therefore see that any $x \in [\dot{x}]$ has norm

$$\langle x, x \rangle = \langle \dot{x}, \dot{x} \rangle + 2\langle \dot{x}, x_1 \rangle + \langle x_1, x_1 \rangle \in 2\mathbb{Z},$$

where $x = \dot{x} + x_1$ and $x_1 \in \mathcal{L}_{m_0}(L)$. It then follows that $\mathcal{L}_{m_0}(L)^*$ is even; in particular, $\mathcal{L}_{m_0}(L)^*$ is integral.

But then, $\operatorname{disc}(\mathcal{L}_{m_0}(L)^*) \in \mathbb{Z}$. Additionally, since $[L : \mathcal{L}_{m_0}(L)]$ is a finite positive integer and L is unimodular, we have

$$\operatorname{disc}(\mathcal{L}_{m_0}(L)) = [L : \mathcal{L}_{m_0}(L)]^2 \operatorname{disc}(L) = [L : \mathcal{L}_{m_0}(L)]^2 \in \mathbb{Z}.$$

But then we have both $[L : \mathcal{L}_{m_0}(L)]^2 \in \mathbb{Z}$ and $[L : \mathcal{L}_{m_0}(L)]^{-2} \in \mathbb{Z}$, hence $[L : \mathcal{L}_{m_0}(L)] = 1$. This proves that $L = \mathcal{L}_{m_0}(L)$, showing the theorem. □

4.3.4 Extremal Type II Lattices of Ranks 40, 80, and 120

We prove a weakened analog of Theorem 4.10 for Type II lattices of ranks $n = 40, 80, 120$. As we discuss in the remarks below, the $n = 40$ case of Theorem 4.14 is sharp, while the $n = 120$ case can be improved.

Theorem 4.14. *If L is an extremal Type II lattice of rank $n = 40, 80, 120$, then*

$$L = \mathcal{L}_{m_0+(m_0+2)}(L).$$

That is, L is generated by its vectors of norms m_0 and $m_0 + 2$.

This result is presented as it appears in work by the author and Abel [KA08]. The $n = 40$ case is originally due to Ozeki [Oze89], while the rank $n = 80, 120$ cases are original to the author and Abel [KA08].

Before proving Theorem 4.14, we introduce one additional notation. For $\dot{x} \in L \otimes \mathbb{R}$ and $j \in \mathbb{Z}$, we write

$$M_j(L; \dot{x}) := |\{x \in L_{m_0+2} : \langle \dot{x}, x \rangle = j\}| .$$

As for $N_j(L; \dot{x})$, we have $M_{-j}(L; \dot{x}) = M_j(L; \dot{x})$ for any $\dot{x}$ and j.

Proof of Theorem 4.14. We now consider the equivalence classes of $L/(\mathcal{L}_{m_0+(m_0+2)}(L))$. To show the result, it suffices to show that no class $[\dot{x}] \in L/(\mathcal{L}_{m_0+(m_0+2)}(L))$ has a minimal representative $\dot{x}$ with $\langle \dot{x}, \dot{x} \rangle = s > m_0 + 2$. Seeking a contradiction, we suppose that some class $[\dot{x}]$ with such a minimal representative $\dot{x}$ exists.

It follows from Lemma 4.7 that $N_j(L; \dot{x}) = 0$ for $j \geq \frac{m_0}{2} + 1$. An argument identical to the proof of Lemma 4.7 shows the inequality

$$|\langle x, \dot{x} \rangle| \leq \frac{m_0}{2} + 1,$$

for all $x \in L_{(m_0+2)}$; this yields $M_j(L;\dot{x}) = 0$ for $j \geq \frac{m_0}{2} + 2$. Thus, proceeding in analogy to the argument for Theorem 4.10, we seek a system of linear equations in the

$$\left(\frac{m_0}{2} + 1\right) + \left(\frac{m_0}{2} + 2\right) = m_0 + 3$$

variables $N_0(L;\dot{x}), \ldots, N_{m_0/2}(L;\dot{x}), M_0(L;\dot{x}), \ldots, M_{(m_0/2)+1}(L;\dot{x})$. Corollary 4.6 gives rise to $\mathrm{t}(n) + 1 = m_0/2$ such equations in the $N_j(L;\dot{x})$, and to another $\mathrm{t}(n) + 1 = m_0/2$ such equations in the $M_j(L;\dot{x})$. Additionally, as in Lemma 4.8, we know that

$$a_{m_0}(L) = N_0(L;\dot{x}) + 2\sum_{j=1}^{m_0/2} N_j(L;\dot{x}),$$
$$a_{m_0+2}(L) = M_0(L;\dot{x}) + 2\sum_{j=1}^{m_0/2+1} M_j(L;\dot{x}).$$

To obtain two more equations in the $N_j(L;\dot{x})$ and $M_j(L;\dot{x})$, we observe that Theorem 3.18 shows that

$$\theta_{L,P_{2\mathrm{t}(n)+2;\dot{x}}} \in \mathcal{M}^0_{\frac{n}{2}+\mathrm{t}(n)+2}, \quad \theta_{L,P_{2\mathrm{t}(n)+6;\dot{x}}} \in \mathcal{M}^0_{\frac{n}{2}+\mathrm{t}(n)+6}.$$

Comparing power series coefficients, we then obtain

$$\theta_{L,P_{\mathrm{t}(n);\dot{x}}} \equiv c_1\Delta^{2\mathrm{t}(n)+2}, \quad \theta_{L,P_{m_0;\dot{x}}} \equiv c_1\mathrm{E}_4\Delta^{2\mathrm{t}(n)+2},$$

for constants c_1 and c_2. This then yields the equations

$$\sum_{x\in L_{(m_0+2)}} P_{2\mathrm{t}(n)+2;\dot{x}}(x) = c_1 \sum_{x\in L_{m_0}} P_{2\mathrm{t}(n)+2;\dot{x}}(x)$$
$$\sum_{x\in L_{(m_0+2)}} P_{2\mathrm{t}(n)+6;\dot{x}}(x) = c_2 \sum_{x\in L_{m_0}} P_{2\mathrm{t}(n)+6;\dot{x}}(x).$$

In total, we have derived a system of $m_0 + 4$ distinct linear equations in the $m_0 + 3$ variables $N_0(L;\dot{x}), \ldots, N_{m_0/2}(L;\dot{x}), M_0(L;\dot{x}), \ldots, M_{(m_0/2)+1}(L;\dot{x})$. This system is overdetermined, hence the determinants of the (extended) $(m_0 + 4) \times (m_0 + 4)$ matrices for these systems must vanish. For $n = 40, 80, 120$, these determinants are respectively

$$2^{55}3^{7}5^{8}7^{4}11^{4}13^{1}19^{6}23^{3}(s-4)s(3s-13)\left(5s^2 - 55s + 154\right), \tag{4.16}$$

$$2^{132}3^{27}5^{16}7^{10}11^{6}13^{10}23^{4}41^{8}43^{6}47^{3}(s-8)sR_{80}(s), \tag{4.17}$$

$$2^{235}3^{48}5^{26}7^{13}11^{7}13^{7}17^{6}23^{4}31^{11}37^{1}59^{14}61^{11}67^{5}71^{3}73^{1}(s-12)sR_{120}(s), \tag{4.18}$$

where $R_{80}(s) = 1346s^5 - 60570s^4 + 1101155s^3 - 10101795s^2 + 46723754s - 87084984$, an irreducible quintic, and $R_{120}(s)$ is the irreducible septic

$$\begin{gathered}
1998988267405690993 5s^7 - 178576285221575062086 0s^6 \\
+6903215840489061660613 2s^5 - 1496426482568975234448600s^4 \\
+196383719985316669027805 44s^3 - 1559683502690964419302410 24s^2 \\
+693822341019921345575940096s - 1333059554550161112446730240.
\end{gathered}$$

For each determinant (4.16)–(4.18), there are no integer solutions $s > m_0 + 2$. It follows that there can be no equivalence class $[\dot{x}] \in L/(\mathcal{L}_{m_0+(m_0+2)}(L))$ with a minimal representative $\dot{x}$ having $\langle \dot{x}, \dot{x} \rangle = s > m_0 + 2$. □

Remarks

As remarked at the beginning of this section, the $n = 40$ case of Theorem 4.14 is sharp. That is, there exist extremal Type II lattices of rank 40 which are not generated by their vectors of minimal norm.[12] However, Elkies and the author [EK09b] have recovered the following strengthening of Theorem 4.14 for extremal Type II lattices of ranks $n = 40, 80$.

Theorem 4.15 ([EK09b]). *If L is an extremal Type II lattice of rank $n = 40, 80$ then*

$$L = \mathcal{L}_{(m_0+2)}(L).$$

Proof. By Theorem 4.14, it suffices to show that every vector in L_{m_0} is contained in $\mathcal{L}_{(m_0+2)}(L)$. We therefore suppose that there is some $\dot{x} \in L_{m_0}$ not in $\mathcal{L}_{(m_0+2)}(L)$, seeking a contradiction.

Now, for any $x \in L_{(m_0+2)}$, we must have

$$|\langle x, \dot{x} \rangle| \in \left\{0, 1, \ldots, \frac{m_0}{2} - 1, \frac{m_0}{2} + 1\right\}.$$

Indeed, if $\langle \dot{x}, \pm x \rangle > \frac{m_0}{2} + 1$, then $[\dot{x}]$ contains a vector $x \mp \dot{x}$ of norm

$$\langle x \mp \dot{x}, x \mp \dot{x} \rangle = \langle x, x \rangle \mp 2\langle x, \dot{x} \rangle + \langle \dot{x}, \dot{x} \rangle < \langle \dot{x}, \dot{x} \rangle = m_0,$$

contradicting the extremality of L. Furthermore, we cannot have $\langle x, \dot{x} \rangle = \pm m_0/2$, or else we would have $x \mp \dot{x} \in L_{(m_0+2)}$ and then $x = \pm\dot{x} + (x \mp \dot{x}) \in \mathcal{L}_{(m_0+2)}(L)$.[13]

[12] Ozeki [Oze89] constructs such lattices.

[13] The fact that $\langle x, \dot{x} \rangle = \pm m_0/2$ implies that $x \mp \dot{x} \in L_{(m_0+2)}$ is a simple computation:

$$\langle x \mp \dot{x}, x \mp \dot{x} \rangle = \langle x, x \rangle \mp 2\langle x, \dot{x} \rangle + \langle \dot{x}, \dot{x} \rangle = (m_0 + 2) - 2\left(\frac{m_0}{2}\right) + m_0 = m_0 + 2.$$

Corollary 4.6 shows that

$$\theta_{L,P_{d;\dot{x}}} \in \mathcal{M}^0_{\frac{n}{2}+d}.$$

As in the proof of Theorem 4.14, this yields $\mathrm{t}(n)+1 = m_0/2$ equations in the $\frac{m_0}{2}+1$ variables

$$M_0(L;\dot{x}), \ldots, M_{(m_0/2)-1}(L;\dot{x}), M_{(m_0/2)+1}(L;\dot{x}).$$

Additionally, we obtain the equation

$$a_{m_0+2}(L) = M_0(L;\dot{x}) + 2M_{(m_0/2)+1}(L;\dot{x}) + 2\sum_{j=1}^{m_0/2-1} M_j(L;\dot{x})$$

from the theta function of L. For $n = 40, 80$, these $\frac{m_0}{2}+1$ equations are linearly independent; we may therefore explicitly solve the system for the variables

$$M_0(L;\dot{x}), \ldots, M_{(m_0/2)-1}(L;\dot{x}), M_{(m_0/2)+1}(L;\dot{x}).$$

When $n = 40, 80$, we compute

$$M_{(m_0/2)+1}(L;\dot{x}) = -246272,$$
$$M_{(m_0/2)+1}(L;\dot{x}) = -275208192,$$

respectively. This is impossible, however, because $M_{(m_0/2)+1}(L;\dot{x}) \geq 0$ by definition. □

Surprisingly, Elkies [Elk09a] has shown that Theorem 4.14 is not sharp for rank-120 extremal Type II lattices. Specifically, the conclusion of Theorem 4.10 holds in this case.

Theorem 4.16 ([Elk09a])**.** *If L is an extremal Type II lattice of rank $n = 120$, then*

$$L = \mathcal{L}_{m_0}(L) = \mathcal{L}_{12}(L).$$

Chapter 5

A New Development of Harmonic Weight Enumerators

In analogy to the theory of weighted theta functions presented in Chapter 3, we now introduce the *harmonic weight enumerator*, a weighted generating function which generalizes the ordinary weight enumerator defined in Section 2.2.3. For a length-n binary linear code $C \subset \mathbb{F}_q^n$ and a *discrete harmonic polynomial* Q, the harmonic weight enumerator $W_{C,Q}(x, y)$ is defined by

$$W_{C,Q}(x,y) := \sum_{c \in C} Q(c) x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)}.$$

This function encodes the weights and distribution of the codewords of C, just as the weighted theta functions of a lattice L encode the norms and distribution of the vectors of L.

Discrete harmonic polynomials were first introduced by Delsarte [Del78]. The harmonic weight enumerators of binary codes were then introduced by Bachoc [Bac99], who also gave several applications.[1] Both Delsarte's development of discrete harmonic polynomials and Bachoc's development of harmonic weight enumerators are predominantly combinatorial.

The central result of this chapter is a new, structural development of these theories. Our development uses the finite-dimensional representation theory of $\mathfrak{sl}_2$, in direct analogy with the approach to weighted theta functions presented in Chapter 3.

As context, we derive the *MacWilliams identity*, a classical result regarding ordinary weight enumerators, in Sections 5.1.1 and 5.1.2. We also state *Gleason's Theorem*, an analog of

[1] Specifically, Bachoc [Bac99] used harmonic weight enumerators to give a proof of the Assmus–Mattson Theorem (Theorem 2.1), to compute *Jacobi polynomials*, and to classify the extremal even *formally self-dual* codes of length 12. Additionally, Bachoc [Bac01] developed an analogous theory for q-ary codes of length n.

the characterization of the spaces of modular forms (Theorem 3.4) which applies to weight enumerators and generalizes to the harmonic weight enumerator setting. We review relevant facts from the finite-dimensional representation theory of $\mathfrak{sl}_2$ in Section 5.1.3. Then, in Sections 5.2 and 5.3, we present our new development of the harmonic weight enumerator theory, describing the space of discrete harmonic polynomials and deriving the key identities for harmonic weight enumerators. Finally, in Section 5.4, we introduce the *zonal harmonic polynomials*, a discrete analog of the zonal spherical harmonics of Section 3.4.

5.1 Preliminaries

5.1.1 The Discrete Poisson Summation Formula

We now prove the *discrete Poisson summation formula*, a discrete analog of the Poisson summation formula (Theorem 3.5) proven in Section 3.1.2. Like its lattice analog, the discrete Poisson summation formula relates the sums of a function to the sums of the function's discrete Fourier transform. Here, however, instead of considering the sums of the function and its Fourier transform over a lattice $L \subset \mathbb{R}^n$ and its dual L^*, we consider the sums of the function and its discrete Fourier transform over a binary linear code $C \subset \mathbb{F}_2^n$ and over $C^\perp$, the dual code of C.[2]

Before proceeding, we recall that the *discrete Fourier transform* (or *Hadamard transform*) $\hat{f}$ of a function f on $\mathbb{F}_2^n$ is the function on $\mathbb{F}_2^n$ defined by

$$\hat{f}(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{(u,v)} f(v). \tag{5.1}$$

Theorem 5.1 (Discrete Poisson Summation Formula)**.** *Let $C \subset \mathbb{F}_2^n$ be a binary linear code of length n, and let f be a function from $\mathbb{F}_2^n$ into any ring. Then, we have*

$$\sum_{c \in C} f(c) = \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} \hat{f}(c'). \tag{5.2}$$

Our proof of Theorem 5.1 follows the standard argument, which is the one presented in [MS83, p. 127]. Theorem 5.1 may also be proven via an argument directly analogous to the proof of the Poisson summation formula (Theorem 3.5) given in Section 3.1.2

[2] Throughout, we use the convention that general elements of $\mathbb{F}_2^n$ are denoted $v, u \in \mathbb{F}_2^n$ while words of a code C are denoted $c \in C$. This differs from our convention for lattices, in which we denote by x both a general element of $\mathbb{R}^n$ and of a lattice L. Additionally, in Section 5.1.3, we use the notation v to denote an element of an $\mathfrak{sl}_2$-module. We have maintained these seemingly clashing conventions, as they are standard within the literatures of codes, lattices, and $\mathfrak{sl}_2$, respectively, and do not appear together in the thesis except within this footnote.

Proof of Theorem 5.1. By expanding the right side of (5.2) and rearranging the order of summation, we obtain

$$\sum_{c' \in C^\perp} \hat{f}(c') = \sum_{c' \in C^\perp} \sum_{v \in \mathbb{F}_2^n} (-1)^{(c',v)} f(v) = \sum_{v \in \mathbb{F}_2^n} f(v) \sum_{c' \in C^\perp} (-1)^{(c',v)}. \tag{5.3}$$

Now, whenever $v \in C \subset \mathbb{F}_2^n$ and $c' \in C^\perp$, we have $(c', v) = 0$ by the definition of $C^\perp$. It follows that the inner sum in (5.3) equals $|C^\perp|$ whenever $v \in C$. Furthermore, when $v \notin C$, the inner sum of (5.3) vanishes.[3] The result then follows immediately. □

5.1.2 The MacWilliams Identity and Gleason's Theorem

In this section, we present two classical results from coding theory which are closely related to the theory of lattices. The first of these results, the MacWilliams identity (Theorem 5.2, below), is analogous to Lemma 3.7; it expresses the weight enumerator of $C^\perp$ in terms of the weight enumerator of C. The second result (Theorem 5.3, below) is a famous theorem originally due to Gleason [Gle71], which shows that the weight enumerators of Type II codes can be expressed in terms of two particular weight enumerators. This is a coding-theoretic analog of the fact (Theorem 3.4) that theta functions of Type II lattices may be expressed as polynomials in E_4 and E_6.

The MacWilliams identity is proven via discrete Poisson summation, and therefore its proof serves as a warm-up for the argument we use to prove the generalized MacWilliams identity for harmonic weight enumerators (Theorem 5.16) in Section 5.3. By contrast, the methods required to prove Gleason's theorem are essentially disjoint from our discussion. Therefore, and in keeping with the expository approach of Chapter 3, we prove the MacWilliams identity here but do not prove Gleason's Theorem.[4]

Theorem 5.2 (MacWilliams Identity ([Mac63]; [CS99, p. 78]; [Ebe02, p. 74]; [MS83, p. 126]))**.** *For any binary linear code C of length n, we have*

$$W_C(x, y) = \frac{1}{|C^\perp|} W_{C^\perp}(x + y, x - y).$$

[3] In this case, (c', v) takes the values 0 and 1 equally often (see [MS83, p. 127]). (This statement is just an instance of the well-known fact that the sum of a nontrivial character on a finite group vanishes.)

[4] This expository decision is analogous to our decision to prove Lemma 3.7 but not to prove Theorem 3.4 in Chapter 3.

Proof. We let f be the function on $\mathbb{F}_2^n$ defined by $f(v) = x^{n-\mathrm{wt}(v)}y^{\mathrm{wt}(v)}$ and compute that

$$\begin{aligned}\hat{f}(u) = \sum_{v\in\mathbb{F}_2^n}(-1)^{(u,v)}x^{n-\mathrm{wt}(v)}y^{\mathrm{wt}(v)} &= \sum_{v\in\mathbb{F}_2^n}(-1)^{u_1v_1+\cdots+u_nv_n}\prod_{j=1}^{n}x^{1-v_j}y^{v_j}\\ &= \sum_{v_1=0}^{1}\cdots\sum_{v_n=0}^{1}\prod_{j=1}^{n}(-1)^{u_jv_j}x^{1-v_j}y^{v_j}\\ &= \prod_{j=1}^{n}\sum_{\ell=0}^{1}(-1)^{u_j\ell}x^{1-\ell}y^{\ell}. \end{aligned}\tag{5.4}$$

If $u_j = 0$, then we have $\sum_{\ell=0}^{1}(-1)^{u_j\ell}x^{1-\ell}y^{\ell} = x+y$; if $u_j = 1$, then $\sum_{\ell=0}^{1}(-1)^{u_j\ell}x^{1-\ell}y^{\ell} = x-y$. We therefore have from (5.4) that

$$\hat{f}(u) = (x+y)^{n-\mathrm{wt}(u)}(x-y)^{\mathrm{wt}(u)};$$

the theorem then follows directly from Discrete Poisson Summation (Theorem 5.1). □

Theorem 5.3 (Gleason's Theorem ([Gle71]; [CS99, p. 186]; [Ebe02, p. 75]))**.** *For any Type II code C, the weight enumerator $W_C(x,y)$ is a polynomial in*

$$\varphi_8 := W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8 \quad \textit{and} \quad \xi_{24} := x^4y^4(x^4-y^4)^4.$$

Remarks

Theorems 5.2 and 5.3 may be derived through an appeal to the theory of theta functions of Type II lattices, via Construction A. Ebeling [Ebe02, pp. 72–75] presents one such approach. Additionally, Ward [War00] gives an elegant elementary proof of Theorem 5.2 using differential operators.

5.1.3 The Finite-dimensional Representation Theory of $\mathfrak{sl}_2$

We now review results from the finite-dimensional representation theory of $\mathfrak{sl}_2$ which will be relevant to our discussion later in this chapter. Our presentation here follows that given by Serre [Ser01, pp. 17–20].

Basic Definitions and Commutation Relations

The simple Lie algebra $\mathfrak{sl}_2$ is the algebra of 2×2 complex matrices having trace 0. As we indicated briefly in Section 3.2.3, this algebra is generated by the matrices

$$\mathsf{X} = \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right), \quad \mathsf{H} = \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right), \quad \mathsf{Y} = \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),$$

and these generators satisfy commutation relations analogous to those obtained in Lemma 3.15.

Fact 5.4. *We have the commutation relations*

$$[\mathsf{X},\mathsf{Y}]=\mathsf{H},\quad [\mathsf{H},\mathsf{X}]=2\mathsf{X},\quad [\mathsf{H},\mathsf{Y}]=-2\mathsf{Y}.$$

The Structure of Finite-dimensional $\mathfrak{sl}_2$-modules

Now, we consider any finite-dimensional $\mathfrak{sl}_2$-module V. Throughout this section, we denote the λ-eigenspace of H in V by V^λ. As the λ- and λ'-eigenvectors of any linear operator are linearly independent for $\lambda \neq \lambda'$, we obtain the direct sum decomposition

$$\bigoplus_{\lambda\in\mathbb{C}} V^\lambda \subseteq V.$$

Lemma 5.5. *For any $v \in V^\lambda$, we have $\mathsf{X}v \in V^{\lambda+2}$ and $\mathsf{Y}v \in V^{\lambda-2}$.*

Proof. We compute directly using Fact 5.4 that

$$\mathsf{HX}v=\mathsf{XH}v+[\mathsf{H},\mathsf{X}]\,v=\lambda\mathsf{X}v+2\mathsf{X}v=(\lambda+2)\mathsf{X}v.$$

Likewise, we obtain

$$\mathsf{HY}v=\mathsf{YH}v+[\mathsf{H},\mathsf{Y}]\,v=\lambda\mathsf{Y}v-2\mathsf{Y}v=(\lambda-2)\mathsf{Y}v. \qquad \square$$

We say that a nonzero element $w \in V^\lambda$ is *primitive of weight* λ if $\mathsf{X}w = 0$. We now show that any nontrivial $\mathfrak{sl}_2$-module V contains such an element.

Lemma 5.6. *Suppose that $\dim(V) > 0$. Then, V contains a primitive element of some weight.*

Proof. Since V is finite-dimensional, H has at least one eigenvalue λ. We fix some $v \in V^\lambda$. Since X is nilpotent, the sequence $\{\mathsf{X}^j v\}_{j=0}^\infty$ has a last nonzero element $\mathsf{X}^{j_*}v$. Clearly, $\mathsf{X}(\mathsf{X}^{j_*}v) = 0$, by construction. Furthermore, since $v \in V^\lambda$, we have $\mathsf{X}^{j_*}v \in V^{\lambda+2j_*}$ by Lemma 5.5. Thus, $\mathsf{X}^{j_*}v \in V$ is primitive (of weight $\lambda + 2j_*$). $\square$

For an $\mathfrak{sl}_2$-module V with primitive element $w \in V^\lambda$ of weight λ, we set

$$w^{(j)} := \frac{1}{j!}\mathsf{Y}^j w$$

for $j \geq 0$. We adopt the convention that $w^{(-1)} = 0$. With these definitions, the $w^{(j)}$ $(j \geq -1)$ are related by the operators H, Y and X. More specifically, we have the following result.

Lemma 5.7. *1.* $\mathsf{H}w^{(j)} = (\lambda - 2j)w^{(j)}$,

2. $\mathsf{Y}w^{(j)} = (j+1)w^{(j+1)}$, *and*

3. $\mathsf{X}w^{(j)} = (\lambda - j + 1)w^{(j-1)}$.

Proof. The first identity is a consequence of the proof of Lemma 5.6, while the second identity is immediate by definition.

To prove the third identity, we proceed by induction on j. The base case ($j = 0$) is immediate; the inductive step follows from the identity

$$\begin{aligned} j\mathsf{X}w^{(j)} = \mathsf{X}\mathsf{Y}w^{(j-1)} &= \mathsf{Y}\mathsf{X}w^{(j-1)} + [\mathsf{X},\mathsf{Y}]\, w^{(j-1)} \\ &= (\lambda - j + 2)\mathsf{Y}w^{(j-2)} + \mathsf{H}w^{(j-1)} \\ &= (\lambda - 2j + 2 + (\lambda - j + 2)(j-1))w^{(j-1)} \\ &= j(\lambda - j + 1)w^{(j-1)}, \end{aligned}$$

upon dividing by j. □

The first part of Lemma 5.7 shows that the $w^{(j)}$ ($j \geq 0$) are nonzero eigenvectors of H associated to distinct eigenvalues; the nonzero $\{w^{(j)}\}_{j=0}^{\infty}$ are therefore linearly independent, and there is a $j_* > 0$ such that $w^{(j)} = 0$ for $j > j_*$. Then, Lemma 5.7 implies that $w^{(j_*)}$ is primitive of weight $\lambda - 2j_*$. It then follows that the subspace $W \subset V$ with basis $\{w^{(j)}\}_{j=0}^{j_*}$ is stable under the action of $\mathfrak{sl}_2$.

Lemma 5.8. *The subspace $W \subset V$ is an irreducible $\mathfrak{sl}_2$-module.*

Proof. It is clear that W is an $\mathfrak{sl}_2$-submodule of V. Now, if $W' \subset W$ is nontrivial and stable under the action of H, then $w^{(j)} \in W'$ for some j ($0 \leq j \leq j_*$). However, we must then have $w^{(j-1)}, \ldots, w^{(0)} \in W'$, by the third part of Lemma 5.7. The second part of Lemma 5.7 then shows that $w^{(j+1)}, \ldots, w^{(j_*)} \in W'$, as well. It follows that $W' = W$, hence W is irreducible. □

We now fix an integer $k \geq 0$ and let V_k be a $(k+1)$-dimensional vector space with basis $\{v^{(j)}\}_{j=0}^{k}$. We may give V_k the structure of a $\mathfrak{sl}_2$-module by defining the endomorphisms

$$\mathsf{H}v^{(j)} = (k - 2j)v^{(j)}, \quad \mathsf{Y}v^{(j)} = (j+1)v^{(j+1)}, \quad \mathsf{X}v^{(j)} = (k - j + 1)v^{(j-1)}.$$

As V_k is generated by $v^{(0)}$ as an $\mathfrak{sl}_2$-module, it follows from Lemma 5.8 that V_k is irreducible of dimension $\dim(V_k) = k + 1$. Our next result shows that V_k is the only irreducible $\mathfrak{sl}_2$-module of dimension $k + 1$, up to isomorphism.

Proposition 5.9. *If V' is an irreducible $\mathfrak{sl}_2$-module of dimension $k+1$, then $V' \cong V_k$.*

Proof. By Lemma 5.6, there is a primitive element $v' \in V'$. Now, the $\mathfrak{sl}_2$-module generated by v' must have dimension at most $k+1$. Since V' is irreducible, this implies that V' is generated by v'. But then we have an isomorphism $V' \cong V_k$, via the formulae of Lemma 5.7. □

Furthermore, we may decompose any finite-dimensional $\mathfrak{sl}_2$-module as a direct sum of the modules V_k.

Proposition 5.10. *If V is a finite-dimensional $\mathfrak{sl}_2$-module, then V is isomorphic to a direct sum of the modules V_k.*

Proof. This follows from Proposition 5.9 and the well-known fact that any finite-dimensional representation of a semisimple Lie algebra is completely reducible. □

5.2 The Space of Discrete Harmonic Polynomials

In this section, we present some useful results in the theory of *discrete harmonic polynomials*. These polynomials were originally introduced by Delsarte [Del78], who gave a combinatorial development. Here, we give a new approach to these polynomials using the finite-dimensional representation theory of $\mathfrak{sl}_2$ discussed in Section 5.1.3.

5.2.1 Basic Definitions and Notation

A function g on $\mathbb{F}_2$ may be interpreted as a 2×1 matrix $g = \left(\begin{smallmatrix} g_0 \\ g_1 \end{smallmatrix}\right)$, where g_v is the value assumed on input $v \in \mathbb{F}_2$. It is easily computed that the discrete Fourier transform $\hat{g}$ of g is the function

$$\hat{g} = \left(\begin{smallmatrix} g_0+g_1 \\ g_0-g_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g_0 \\ g_1 \end{smallmatrix}\right);$$

the discrete Fourier transform is therefore encoded by the matrix $\mathsf{T} := \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. There is a natural action of $\mathfrak{sl}_2$ on these functions g, defined by left-multiplication of matrices in $\mathfrak{sl}_2$. Thus, we may interpret the space of functions on $\mathbb{F}_2$ as a representation of $\mathfrak{sl}_2$ isomorphic with V_1.

More generally, a monomial function g on $\mathbb{F}_2^n$ must have total degree at most n,[5] and so may be interpreted as a pure tensor in $V_1^{\otimes n}$; such a function is denoted

$$g = \left(\begin{smallmatrix} g_{10} \\ g_{11} \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} g_{n0} \\ g_{n1} \end{smallmatrix}\right)$$

[5] This is a consequence of the fact that, for any $v \in \mathbb{F}_2^n$, we have $v_j^2 = v_j$ for all j ($1 \leq j \leq n$).

and assumes the value $g_{jv_1} \cdots g_{jv_n}$ on $v \in \mathbb{F}_2^n$. In this setting, the discrete Fourier transform corresponds to the action of the operator

$$\widetilde{\mathsf{T}} := \mathsf{T}^{\otimes n}.$$

For example, the degree-n monomial $g(v) = v_1 \cdots v_n$, which takes the value of the product of the coordinates of the input $v \in \mathbb{F}_2^n$, is the function

$$g = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right).$$

The discrete Fourier transform $\hat{g}$ of g is

$$\hat{g} = \widetilde{\mathsf{T}} g = \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right).^{6}$$

Polynomials in the Variables $(-1)^{v_j}$ $(1 \le j \le n)$

Instead of working with polynomials in the variables v_j $(1 \le j \le n)$, we work with the discrete Fourier transforms $(-1)^{v_j}$ $(1 \le j \le n)$ of these variables.[7] We denote by $\mathscr{D}$ the $\mathbb{C}$-vector space of polynomial functions Q in the variables

$$(-1)^{v_1}, \ldots, (-1)^{v_n},$$

where $v \in \mathbb{F}_2^n$. We denote by $\mathscr{D}_d$ the subspace of $\mathscr{D}$ consisting of degree-d homogeneous polynomials in the $(-1)^{v_j}$ $(1 \le j \le n)$ with each variable $(-1)^{v_j}$ in each term appearing to degree 0 or 1. We adopt the convention that $\mathscr{D}_d = \{0\}$ for $d < 0$.

The preceding discussion shows that any $Q \in \mathscr{D}$ may be interpreted as an element of $V_1^{\otimes n}$, and that the discrete Fourier transform $\hat{Q}$ of Q is equal to $\widetilde{\mathsf{T}} Q$. The action of $\mathfrak{sl}_2$ defined above gives rise to the following action on $\mathscr{D}$: if $M \in \mathfrak{sl}_2$ and $Q \in \mathscr{D}$, then the action of M on Q is given by

$$\left(\sum \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes M \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) Q.$$

Here, $\sum \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes M \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ denotes the operator equal to

$$\left(M \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) + \cdots + \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes M \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) + \cdots + \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes M\right),$$

[6] Note that this aligns with the expression

$$\hat{g}(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{(u,v)} g(v) = (-1)^{\sum_{j=1}^n u_j},$$

the more common definition (5.1) of the discrete Fourier transform given earlier.

[7] Delsarte [Del78] uses the v_j basis, rather than the $(-1)^{v_j}$ basis. We depart from Delsarte, however, because the use of the $(-1)^{v_j}$ basis greatly simplifies our development.

the sum of n tensors, the j-th of which acts as M on the j-th factor and as the identity matrix $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ on the other factors.

Conjugation of X, H, and Y by the Discrete Fourier Transform

We define the operators X', H', and Y' to be the conjugates of X, Y, and H by the Fourier transform:

$$\begin{aligned}\mathsf{X}' &:= \mathsf{T}^{-1}\mathsf{X}\mathsf{T} = \frac{1}{2}\left(\mathsf{H} - \mathsf{X} + \mathsf{Y}\right),\\ \mathsf{H}' &:= \mathsf{T}^{-1}\mathsf{H}\mathsf{T} = \mathsf{X} + \mathsf{Y},\\ \mathsf{Y}' &:= \mathsf{T}^{-1}\mathsf{Y}\mathsf{T} = \frac{1}{2}\left(\mathsf{H} + \mathsf{X} - \mathsf{Y}\right).\end{aligned}$$

Conjugation by the Fourier transform operator T induces an isomorphism of Lie algebras

$$\mathsf{X} \longleftrightarrow \mathsf{X}', \quad \mathsf{H} \longleftrightarrow \mathsf{H}', \quad \mathsf{Y} \longleftrightarrow \mathsf{Y}',$$

hence these operators $\mathsf{X}', \mathsf{H}', \mathsf{Y}'$ satisfy the commutation relations of Fact 5.4.

Fact 5.11. *We have the commutation relations*

$$\left[\mathsf{X}', \mathsf{Y}'\right] = \mathsf{H}', \quad \left[\mathsf{H}', \mathsf{X}'\right] = 2\mathsf{X}', \quad \left[\mathsf{H}', \mathsf{Y}'\right] = -2\mathsf{Y}'.$$

We write $\widetilde{\mathsf{X}'}$, $\widetilde{\mathsf{H}'}$, and $\widetilde{\mathsf{Y}'}$ for operators

$$\begin{aligned}\widetilde{\mathsf{X}'} &:= \sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{X}' \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) = \widetilde{\mathsf{T}}^{-1}\left(\sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{X} \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right)\widetilde{\mathsf{T}},\\ \widetilde{\mathsf{H}'} &:= \sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{H}' \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) = \widetilde{\mathsf{T}}^{-1}\left(\sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{H} \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right)\widetilde{\mathsf{T}},\\ \widetilde{\mathsf{Y}'} &:= \sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{Y}' \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) = \widetilde{\mathsf{T}}^{-1}\left(\sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{Y} \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right)\widetilde{\mathsf{T}},\end{aligned}$$

which represent the actions of X', H' and Y' on elements of $V_1^{\otimes n}$.

We then have the following result immediately from the definition of $\widetilde{\mathsf{H}'}$.

Lemma 5.12. *If $d \leq n/2$ and $Q \in \mathscr{D}_d$, then $\widetilde{\mathsf{H}'}Q = (n-2d)Q$.*

Proof. The result follows directly, because the 1-eigenspace of H' is the span of $\{\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)\}$ and the (-1)-eigenspace of H' is the span of $\left\{\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)\right\}$. □

Commutation Relations for $\widetilde{\mathsf{X}'}$, $\widetilde{\mathsf{H}'}$, and $\widetilde{\mathsf{Y}'}$

The commutation relations of Fact 5.11 extend to these operators, as well.

Fact 5.13. *We have the commutation relations*

$$\left[\widetilde{\mathsf{X}'}, \widetilde{\mathsf{Y}'}\right] = \widetilde{\mathsf{H}'}, \quad \left[\widetilde{\mathsf{H}'}, \widetilde{\mathsf{X}'}\right] = 2\widetilde{\mathsf{X}'}, \quad \left[\widetilde{\mathsf{H}'}, \widetilde{\mathsf{Y}'}\right] = -2\widetilde{\mathsf{Y}'}.$$

These commutation relations induce an isomorphism between $\mathfrak{sl}_2$ and the algebra generated by $\{\widetilde{\mathsf{X}'}, \widetilde{\mathsf{H}'}, \widetilde{\mathsf{Y}'}\}$.

Now, for $Q \in \mathscr{D}_d$, we observe that $\left(\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{X}' \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right) Q \in \mathscr{D}_{d-1}$, as we have

$$\mathsf{X}'\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) \quad \text{and} \quad \mathsf{X}'\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0\\0\end{smallmatrix}\right).$$

Thus, $\widetilde{\mathsf{X}'}Q = \left(\sum \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{X}' \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right) Q \in \mathscr{D}_{d-1}$. We define the *space of degree-d discrete harmonic polynomials* to be the space

$$\mathscr{D}_d^0 := \ker\left(\widetilde{\mathsf{X}'} : \mathscr{D}_d \to \mathscr{D}_{d-1}\right).$$

We then define the *space of discrete harmonic polynomials*, denoted $\mathscr{D}^0$, to be the direct sum

$$\mathscr{D}^0 := \bigoplus_{d=0}^{n} \mathscr{D}_d^0 = \ker\left(\widetilde{\mathsf{X}'} : \mathscr{D} \to \mathscr{D}\right).$$

5.2.2 Decomposition of Degree-d Discrete Homogeneous Polynomials

It is immediate from Fact 5.13 that the operator $\widetilde{\mathsf{H}'}$ maps $\mathscr{D}^0$ to itself, since if $Q \in \mathscr{D}^0$ then

$$\widetilde{\mathsf{X}'}\widetilde{\mathsf{H}'}Q = \left(\widetilde{\mathsf{H}'}\widetilde{\mathsf{X}'} - \left[\widetilde{\mathsf{H}'}, \widetilde{\mathsf{X}'}\right]\right) Q = \left(\widetilde{\mathsf{H}'}\widetilde{\mathsf{X}'} - 2\widetilde{\mathsf{X}'}\right) Q = 0.$$

As the next lemma shows, we may refine this observation substantially further.

Lemma 5.14. *If $d \leq n/2$ and $Q \in \mathscr{D}_d^0$, then Q is primitive of weight $n - 2d$ with respect to the representation of $\mathfrak{sl}_2$ induced by the action of $\widetilde{\mathsf{X}'}$, $\widetilde{\mathsf{H}'}$, and $\widetilde{\mathsf{Y}'}$.*

Proof. The result is a direct consequence of Lemma 5.12 because all $Q \in \mathscr{D}^0$ satisfy $\widetilde{\mathsf{X}'}Q = 0$. □

For $d \leq n/2$ and $k = 0, 1, \ldots, d$, we define $\mathscr{D}_d^k := (\widetilde{\mathsf{Y}'})^k \mathscr{D}_{d-k}^0$.[8] Combining Lemma 5.14 with the theory of $\mathfrak{sl}_2$ developed in Section 5.1.3, we now obtain a decomposition result for $\mathscr{D}_d$ similar to that obtained for $\mathscr{P}_d$ in Proposition 3.14.

[8] As is the case for our notation $\mathscr{P}_d^k$, the notation $\mathscr{D}_d^k$ is consistent with the notation $\mathscr{D}_d^0$ for the space of degree-d discrete harmonic polynomials.

Proposition 5.15. *For any $d \leq n/2$, we have the following results.*

1. *The map $\widetilde{\mathsf{X}}' : \mathscr{D}_d \to \mathscr{D}_{d-1}$ is surjective.*
2. *We have the direct sum decomposition $\mathscr{D}_d = \bigoplus_{k=0}^{d} \mathscr{D}_d^k = \mathscr{D}_d^0 \oplus \widetilde{\mathsf{Y}}' \mathscr{D}_{d-1}$.*
3. *For any $Q \in \mathscr{D}_d$, the space spanned by $\left\{(\widetilde{\mathsf{Y}}')^j Q\right\}_{j=0}^{n-2d}$ is an irreducible $\mathfrak{sl}_2$-module isomorphic to the module V_{n-2d}.*
4. $\dim(\mathscr{D}_d^0) = \dim(\mathscr{D}_d) - \dim(\mathscr{D}_{d-1}) = \binom{n}{d} - \binom{n}{d-1}$.

Proof. As any $Q \in \mathscr{D}_d^0$ is primitive of weight $n - 2d$, the proposition follows immediately. Indeed, the first and second parts follow from Lemma 5.7 and the third part follows directly from Lemma 5.8 and Proposition 5.10. Then, the fourth part follows from the first part. □

As with Proposition 3.14, we use only parts of this decomposition result directly; the other components of Proposition 3.14 provide contextual information regarding $\mathscr{D}^0$. Specifically, we use the second and third parts of Proposition 3.14 in Section 6.1.

5.3 The Generalized MacWilliams Identity for Harmonic Weight Enumerators

We now derive a generalized MacWilliams identity for harmonic weight enumerators.

Theorem 5.16. *For any binary linear code $C \subset \mathbb{F}_2^n$ and $Q \in \mathscr{D}_d^0$, the harmonic weight enumerator $W_{C,Q}(x,y) = \sum_{c \in C} Q(c) x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)}$ satisfies the identity*

$$W_{C,Q}(x,y) = \left(-\frac{xy}{x^2 - y^2}\right)^d \cdot \frac{2^{\frac{n}{2}+d}}{|C^\perp|} \cdot W_{C^\perp,Q}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

Theorem 5.16 was first proven by Bachoc [Bac99], via a purely combinatorial argument. Here, we give a new proof of this result in analogy with the proof of Theorem 3.17 presented in Section 3.3.

5.3.1 Derivation of the Identity

Multiplication by "Discrete Gaussians"

For $Q \in \mathscr{D}$, the function $Q(v) x^{n-\mathrm{wt}(v)} y^{\mathrm{wt}(v)}$ corresponds in the tensor representation to the function

$$\left(\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)^{\otimes n}\right) Q.$$

Therefore, in analogy with the Gaussian operators G_t defined in Section 3.3.1, we introduce the operators

$$\begin{aligned} \mathsf{W} &:= \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right), & \widetilde{\mathsf{W}} &:= \mathsf{W}^{\otimes n}, \\ \mathsf{V} &:= \begin{pmatrix} x+y & 0 \\ 0 & x-y \end{pmatrix}, & \widetilde{\mathsf{V}} &:= \mathsf{V}^{\otimes n}. \end{aligned}$$

The operator $\widetilde{\mathsf{W}}$ serves as a sort of "discrete Gaussian" for weight enumerators. Indeed, the weight enumerator $W_C(x,y)$ of a length-n binary linear code is given by

$$W_C(x,y) = \sum_{c \in C} \left(\widetilde{\mathsf{W}} \cdot \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)^{\otimes n} \right)(c),$$

and the Fourier transform of $\widetilde{\mathsf{W}} \cdot \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)^{\otimes n}$ is equal to $\widetilde{\mathsf{V}} \cdot \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)^{\otimes n}$.

Lemma 5.17. *If $Q \in \mathscr{D}_d$, then we have*

$$\left(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\right)Q = \hat{Q},$$

where $\hat{Q} = \sum_{d'=0}^{d} \hat{Q}_{d'}$ with $\hat{Q}_{d'} \in \mathscr{D}_d$ for each d' ($0 \leq d' \leq d$) and

$$\hat{Q}_d = \left(\frac{-2xy}{x^2 - y^2} \right)^d Q. \tag{5.5}$$

Proof. As in the proof of Lemma 3.21, we proceed by induction on d. The base case $d = 0$ is immediate, so we suppose that the result holds for $Q \in \mathscr{D}_d$ and show the result for $Q \in \mathscr{D}_{d+1}$.

The discrete Fourier transform operator is linear, hence it suffices to prove the result for the polynomials of the form $(-1)^{v_j} \cdot Q$ with $Q \in \mathscr{D}_d$. Now, we compute the value of $\widetilde{\mathsf{V}}\widetilde{\mathsf{T}}$ times

$$(-1)^{v_j} \cdot Q(v) \cdot x^{n-\mathrm{wt}(v)} y^{\mathrm{wt}(v)} = \widetilde{\mathsf{W}} \cdot \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right) \cdot Q$$

explicitly. We find that

$$\begin{aligned} &\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}} \left(\widetilde{\mathsf{W}} \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right) Q \right) \\ &\quad = \left(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\right) \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right) \left(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\right)^{-1} \left(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\right) Q \\ &\quad = \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right) \left(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\right) Q \\ &\quad = \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \otimes \cdots \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right) \hat{Q}, \end{aligned} \tag{5.6}$$

where the last equality in (5.6) follows on applying the inductive hypothesis to $\left(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\right)Q$.

It is clear that the right side of (5.6) has maximal degree $d+1$, since $\hat{Q}$ is of degree d and

$$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \otimes \cdots \otimes \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$$

is the identity on all but one coordinate. To finish the proof of the lemma, we compute the degree-$(d+1)$ term of (5.6). Now, since

$$\begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \frac{x^2+y^2}{x^2-y^2}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) - \frac{2xy}{x^2-y^2}\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right),$$

the degree-$(d+1)$ term of (5.6) must equal $-\frac{2xy}{x^2-y^2}\hat{Q}_d$.[9] The desired expression (5.5) then follows from the inductive hypothesis. □

Lemma 5.18. *If* $Q \in \mathscr{D}^0$ *and* $\widetilde{\mathsf{H}}'Q = \lambda \cdot Q$*, then*

1. $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\widetilde{\mathsf{X}}'\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)^{-1}Q = 0$ *and*
2. $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\widetilde{\mathsf{H}}'\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)^{-1}Q = \lambda \cdot Q$*.*

Proof. Explicit computation gives

$$\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\widetilde{\mathsf{X}}'\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)^{-1} = -\frac{x^2-y^2}{2xy}\cdot\widetilde{\mathsf{X}}', \tag{5.7}$$

$$\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\widetilde{\mathsf{H}}'\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)^{-1} = \widetilde{\mathsf{H}}' + \frac{x^2+y^2}{xy}\cdot\widetilde{\mathsf{X}}'. \tag{5.8}$$

The first and second results follow directly from (5.7) and (5.8), respectively, since

$$Q \in \mathscr{D}^0 = \ker(\widetilde{\mathsf{X}}'). \qquad □$$

Corollary 5.19. *The operators* $\widetilde{\mathsf{X}}'$ *and* $\widetilde{\mathsf{H}}'$ *act on* $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\mathscr{D}^0$*. The subspace* $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\mathscr{D}^0_d$ *is the intersection of* $\ker(\widetilde{\mathsf{X}}')$ *and the* $(n-2d)$*-eigenspace of* $\widetilde{\mathsf{H}}' + \frac{x^2+y^2}{xy}\widetilde{\mathsf{X}}'$ *in* $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)\mathscr{D}^0_d$*.*

Proof of the Generalized MacWilliams Identity

As a final intermediate step *en route* to Theorem 5.16, we prove an expression analogous to Proposition 3.24 for the discrete Fourier transform of the product of the "discrete Gaussian" $\widetilde{\mathsf{W}}$ and a discrete harmonic polynomial $Q \in \mathscr{D}^0_d$.

Proposition 5.20. *If* $Q \in \mathscr{D}^0_d$*, then*

$$\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)Q = \left(\frac{-2xy}{x^2-y^2}\right)^d Q. \tag{5.9}$$

[9] Here, $\hat{Q}_d$ is the degree-d term of $\hat{Q}$, as in the lemma statement.

Proof. From Corollary 5.19, we see that $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)Q$ is in the $(n-2d)$-eigenspace of $\widetilde{\mathsf{H}}'$. This means that $\big(\widetilde{\mathsf{V}}^{-1}\widetilde{\mathsf{T}}\widetilde{\mathsf{W}}\big)Q \in \mathscr{D}_d^0$; the result then follows immediately from Lemma 5.17. □

Finally, we obtain the generalized MacWilliams identity by combining Proposition 5.20 with the discrete Poisson summation formula (Theorem 5.1).

Proof of Theorem 5.16. We obtain the discrete Fourier transform of $\widetilde{\mathsf{W}}Q$ from Proposition 5.20:

$$\widetilde{\mathsf{T}}\big(\widetilde{\mathsf{W}}Q\big) = \left(\frac{-2xy}{x^2-y^2}\right)^d \widetilde{\mathsf{V}}Q = \left(\frac{-2xy}{x^2-y^2}\right)^d \cdot 2^{n/2} \cdot \left(\begin{pmatrix} \frac{x+y}{\sqrt{2}} & 0 \\ 0 & \frac{x-y}{\sqrt{2}} \end{pmatrix}^{\otimes n}\right) \cdot Q. \tag{5.10}$$

The result follows directly from (5.10), upon application of Theorem 5.1. □

Remarks

One interesting consequence of Theorem 5.16 is the fact that $W_{C,Q}(x,y)/(xy)^d$ is a polynomial, for $Q \in \mathscr{D}_d^0$.

Corollary 5.21. *For C a binary linear code and $Q \in \mathscr{D}_d^0$,*

$$\frac{W_{C,Q}(x,y)}{(xy)^d}$$

is a polynomial in the variables x, y.

Proof. We have from Theorem 5.16 that

$$\frac{W_{C,Q}(x,y)}{(xy)^d} = \left(-\frac{1}{x^2-y^2}\right)^d \cdot \frac{2^{\frac{n}{2}+d}}{|C^\perp|} \cdot W_{C^\perp,Q}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right). \tag{5.11}$$

As $W_{C,Q}\,(x,y)$ is a polynomial in the variables x, y, the left side of (5.11) cannot have factors of x^2-y^2 in the denominator. We therefore must have that

$$(x^2-y^2)^d \mid W_{C^\perp,Q}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

The result then follows. □

As we see at the end of Section 6.1, Corollary 5.21 also follows directly from the $\mathfrak{sl}_2$ development of discrete harmonic polynomials.

5.3.2 A Generalization of Gleason's Theorem

In addition to the generalized MacWilliams identity, Bachoc [Bac99] obtained a generalized "Gleason's theorem" for harmonic weight enumerators. As we will use this result in Section 6.1, we state it here. We omit the proof, however, as the method is disjoint from our discussion and is not affected by our development of harmonic weight enumerators via $\mathfrak{sl}_2$.

Theorem 5.22 ([Bac99])**.** *Let C be a Type II code of length n and let $Q \in \mathscr{D}_d^0$. Then, the harmonic weight enumerator $W_{C,Q}(x, y)$ is an element of the polynomial algebra $\mathbb{C}[\varphi_8, \xi_{24}, \psi_d]$, where*

$$\psi_d := \begin{cases} 0 & d \equiv 0 \bmod 4, \\ x^3y^3(x^4-y^4)^2(x^8-y^8)(x^8-34x^4y^4+y^8) & d \equiv 1 \bmod 4, \\ x^2y^2(x^4-y^4)^2 & d \equiv 2 \bmod 4, \\ xy(x^8-y^8)(x^8-34x^4y^4+y^8) & d \equiv 3 \bmod 4. \end{cases}$$

5.4 Zonal Harmonic Polynomials

We now introduce the *zonal harmonic polynomials*, a class $\mathscr{Z}\mathscr{D}^0$ of discrete harmonic polynomials analogous to the zonal spherical harmonics discussed in Section 3.4. Specifically, we fix some $\dot{v} \in \mathbb{F}_2^n$ and d with $0 \le d \le \mathrm{wt}(\dot{v})$, and determine the space $\mathscr{Z}\mathscr{D}_d^0 \subset \mathscr{D}_d^0$ of degree-d discrete harmonic polynomials invariant under coordinate permutations fixing $\dot{v}$.

5.4.1 Preliminaries

Throughout, we fix $\dot{v} \in \mathbb{F}_2^n$. We denote by $\mathscr{Z}\mathscr{D}_d \subset \mathscr{D}_d$ the space of degree-d discrete homogeneous polynomials invariant under the group of coordinate permutations fixing $\dot{v}$, and set $\mathscr{Z}\mathscr{D}_d^0 := \mathscr{Z}\mathscr{D}_d \cap \mathscr{D}_d^0$. We say that a polynomial in $\mathscr{Z}\mathscr{D}_d^0$ is a *zonal harmonic polynomial of degree d*, and we define the space $\mathscr{Z}\mathscr{D}^0$ of *zonal harmonic polynomials* by

$$\mathscr{Z}\mathscr{D}^0 := \bigcup_{d=0}^{\mathrm{wt}(\dot{v})} \mathscr{Z}\mathscr{D}_d^0.$$

Generators of $\mathscr{Z}\mathscr{D}_d$

We now fix some d with $0 \le d \le \mathrm{wt}(\dot{v})$ and let

$$\mathrm{C}_{1;\dot{v}} := \{j : \dot{v}_j = 1\}, \quad \mathrm{C}_{0;\dot{v}} := \{j : \dot{v}_j = 0\}.$$

Now, we denote by $Q_{d,k;\dot{v}}(v)$ the degree-d discrete polynomial

$$\begin{aligned} Q_{d,k;\dot{v}}(v) &:= \sum_{\substack{\{j_1,\ldots,j_k\}\subseteq \mathrm{C}_{1;\dot{v}} \\ \{j_{k+1},\ldots,j_d\}\subseteq \mathrm{C}_{0;\dot{v}}}} (-1)^{(v_{j_1}+\cdots+v_{j_k})+(v_{j_{k+1}}+\cdots+v_{j_d})} \\ &= \sum_{\substack{\{j_1,\ldots,j_k\}\subseteq \mathrm{C}_{1;\dot{v}} \\ \{j_{k+1},\ldots,j_d\}\subseteq \mathrm{C}_{0;\dot{v}}}} (-1)^{v_{j_1}}\cdots(-1)^{v_{j_k}}\cdot(-1)^{v_{j_{k+1}}}\cdots(-1)^{v_{j_d}} \in \mathscr{D}_d. \end{aligned} \tag{5.12}$$

This definition is valid for all d $(0 \leq d \leq \mathrm{wt}(\dot{v})$ since $|\mathrm{C}_{1;\dot{v}}| = \mathrm{wt}(\dot{v})$ and $|\mathrm{C}_{0;\dot{v}}| = n - \mathrm{wt}(\dot{v})$.

By construction, it is clear that $Q_{d,k;\dot{v}} \in \mathscr{X}\mathscr{D}_d$. Conversely, we have the following lemma.

Lemma 5.23. *The polynomials* $\{Q_{d,k;\dot{v}}\}_{k=0}^{\mathrm{wt}(\dot{v})}$ *generate* $\mathscr{X}\mathscr{D}_d$.

Proof. The result follows immediately from the requirement that any $Q \in \mathscr{X}\mathscr{D}_d$ must be invariant under all permutations simultaneously permuting some k $(1 \leq k \leq \mathrm{wt}(\dot{v}))$ of the nonzero coordinates of $\dot{v}$ and some $d-k$ of the vanishing coordinates in $\dot{v}$. □

Additionally, we have a combinatorial formula for $Q_{d,k;\dot{v}}(v)$.

Proposition 5.24. *We have that*

$$Q_{d,k;\dot{v}}(v) = \left(2\sum_{j=1}^{\left\lfloor\frac{k+1}{2}\right\rfloor}\binom{\mathrm{wt}(v\cap\dot{v})}{2j-1}\binom{\mathrm{wt}(\dot{v})-\mathrm{wt}(v\cap\dot{v})}{k-(2j-1)} - \binom{\mathrm{wt}(\dot{v})}{k}\right)\cdot$$
$$\left(2\sum_{j=1}^{\left\lfloor\frac{(d-k)+1}{2}\right\rfloor}\binom{\mathrm{wt}(v)-\mathrm{wt}(v\cap\dot{v})}{2j-1}\binom{(n-\mathrm{wt}(\dot{v}))-(\mathrm{wt}(v)-\mathrm{wt}(v\cap\dot{v}))}{(d-k)-(2j-1)} - \binom{n-\mathrm{wt}(\dot{v})}{d-k}\right).$$

The proof of Proposition 5.24 is immediately obtained from evaluation of the expression (5.12) for $Q_{d,k;\dot{v}}$.

The Action of $\widetilde{\mathsf{X}}'$ on $Q_{d,k;\dot{v}}$

Now, we determine the action of $\widetilde{\mathsf{X}}'$ on the polynomials $\{Q_{d,k;\dot{v}}\}_{k=0}^{\mathrm{wt}(\dot{v})}$.

Lemma 5.25. *We have*

$$\widetilde{\mathsf{X}}' Q_{d,k;\dot{v}} = \left((n-\mathrm{wt}(\dot{v}))-(d-k-1)\right)Q_{d-1,k;\dot{v}} + \left(\mathrm{wt}(\dot{v})-(k-1)\right)Q_{d-1,k-1;\dot{v}}.$$

Proof. First, we observe that

$$\widetilde{\mathsf{X}}'\cdot\left((-1)^{v_{j_1}+\cdots+v_{j_d}}\right) = \sum_{\ell=1}^{d}(-1)^{v_{j_0}+v_{j_1}+\cdots+v_{j_{\ell-1}}+v_{j_{\ell+1}}+\cdots+v_{j_d}+v_{j_{d+1}}}, \tag{5.13}$$

where we have used the convention that $v_{j_0} = 0 = v_{j_{d+1}}$.[10] It then follows from (5.13) that

$$\widetilde{\mathsf{X}}' Q_{d,k;\dot{v}} = b_k \cdot Q_{d-1,k;\dot{v}} + b_{k-1} \cdot Q_{d-1,k-1;\dot{v}}$$

for constants $b_k, b_{k-1} \in \mathbb{Z}$. To see that

$$b_{k-1} = \mathrm{wt}(\dot{v}) - (k-1),$$

we simply observe that each monomial term in $Q_{d-1,k;\dot{v}}$ can arise from $\mathrm{wt}(\dot{v}) - (k-1)$ different monomial terms in $Q_{d,k;\dot{v}}$. Likewise, we obtain that

$$b_k = (n - \mathrm{wt}(\dot{v})) - (d-k-1). \qquad \square$$

5.4.2 Determination of the Zonal Harmonic Polynomials

We now combine Lemmata 5.23 and 5.25 to characterize $\mathscr{Z}\mathscr{D}_d^0$.

Proposition 5.26. *If $Q \in \mathscr{Z}\mathscr{D}_d^0$, then $Q = b_0 \cdot Q_{d;\dot{v}}$ for some constant $b_0 \in \mathbb{C}$, where*

$$Q_{d;\dot{v}}(v) := \sum_{k=0}^{d} (-1)^k \left(\prod_{\ell=0}^{k-1} \frac{(n - \mathrm{wt}(\dot{v})) - (d-\ell-1)}{\mathrm{wt}(\dot{v}) - \ell} \right) Q_{d,k;\dot{v}}(v).$$

Proof. We consider some $Q \in \mathscr{Z}\mathscr{D}_d^0 = \mathscr{Z}\mathscr{D}_d \cap \mathscr{D}_d^0$. By Lemma 5.23, there exist constants $\{b_k\}_{k=0}^{\mathrm{wt}(\dot{v})} \subset \mathbb{C}$ such that

$$Q = \sum_{k=0}^{\mathrm{wt}(\dot{v})} b_k \cdot Q_{d,k;\dot{v}}.$$

Since $Q \in \mathscr{D}_d^0$, we have that

$$\begin{aligned}
0 = \widetilde{\mathsf{X}}' Q = \widetilde{\mathsf{X}}' \left(\sum_{k=0}^{\mathrm{wt}(\dot{v})} b_k \cdot Q_{d,k;\dot{v}} \right) &= \sum_{k=0}^{\mathrm{wt}(\dot{v})} b_k \cdot \widetilde{\mathsf{X}}' Q_{d,k;\dot{v}} \\
&= \sum_{k=0}^{\mathrm{wt}(\dot{v})} b_k \cdot \left(\left((n - \mathrm{wt}(\dot{v})) - (d-k-1) \right) Q_{d-1,k;\dot{v}} + \left(\mathrm{wt}(\dot{v}) - (k-1) \right) Q_{d-1,k-1;\dot{v}} \right) \\
&= \sum_{k=0}^{\mathrm{wt}(\dot{v})} \left(b_k \left((n - \mathrm{wt}(\dot{v})) - (d-k-1) \right) + b_{k+1} \left(\mathrm{wt}(\dot{v}) - (k) \right) \right) Q_{d-1,k;\dot{v}}.
\end{aligned}$$

[10] To avoid having to adopt this convention, we could have used the slightly more standard notation $\sum_{\ell=1}^{d} (-1)^{v_{j_1} + \cdots + \widehat{v_{j_\ell}} + \cdots + v_{j_d}}$. However, we have eschewed this notation as it conflicts with our usage of $\hat{\cdot}$ for the discrete Fourier transform.

(The penultimate inequality follows from Lemma 5.25.) By comparing coefficients, we then obtain

$$\frac{b_{k+1}}{b_k} = -\frac{(n - \mathrm{wt}(\dot{v})) - (d - k - 1)}{\mathrm{wt}(\dot{v}) - k}$$

for each k ($0 \leq k \leq \mathrm{wt}(\dot{v}) - 1$); the result follows. □

Corollary 5.27. *For each* d *(*$0 \leq d \leq \mathrm{wt}(\dot{v})$*), we have* $\dim(\mathscr{X}\mathscr{D}_d^0) = 1$.

Chapter 6

Configurations of Type II Codes

We now give several applications of the theory of harmonic weight enumerators. The results and methods we present are analogous to those given for lattices in Chapter 4. The arguments for all but one of the results discussed in this chapter are original to Elkies and the author.

First, in Section 6.1, we present an alternative characterization of t-designs analogous to characterization of spherical t-designs given in Proposition 4.5 of Section 4.2, using results derived from our development of discrete harmonic polynomials. We then prove a result analogous to Theorem 4.4 which includes the Assmus–Mattson Theorem (Theorem 2.1) for the case of an extremal Type II code.

Next, in Section 6.2, we derive a condition of Koch [Koc87] on the tetrad systems of Type II codes of length 24. Although this result is analogous to Proposition 4.3 of Section 4.1, Koch's original proof required a substantial appeal to the theory of lattices. Using harmonic weight enumerators, we give a purely coding-theoretic proof of Koch's condition in Section 6.2.2.[1]

Finally, we present configuration results for extremal Type II codes in Section 6.3. Like the configuration results for lattices, these theorems characterize the degrees to which extremal Type II codes of certain lengths are generated by their codewords of small weight. Specifically, we show that extremal Type II codes of lengths $n = 8, 24, 32, 48, 56, 72, 96$ are generated by their minimal-weight codewords. These results are original to this thesis, and are the first configuration results to be obtained for extremal Type II codes. As in the lattice case, one strength of the harmonic weight enumerator machinery is that it allows us to obtain such results for lengths ($n = 72, 96$) where it is not yet known whether extremal Type II codes exist.

[1] This argument originally appeared in [EK09a], a paper of Elkies and the author.

6.1 t-Designs and Extremal Type II Codes

6.1.1 An Equivalent Characterization of t-designs

We now introduce the following equivalent characterization of t-designs.

Proposition 6.1. *A set $D \subseteq \omega_w$ is a t-design if and only if*

$$\sum_{v \in D} Q(v) = 0$$

for all $Q \in \bigcup_{d=1}^{t} \mathscr{D}_d^0$.

Proposition 6.1 is equivalent to Theorem 7 of Delsarte [Del78]. Our development of $\mathscr{D}^0$ leads to a new proof of this result, which we present below. In Section 6.1.2, we apply Proposition 6.1 to prove a special case of the Assmus–Mattson Theorem (Theorem 2.1).

Throughout this section, we write χ_X for the characteristic function of the set X and denote by $\widetilde{\mathsf{H}}$ the action of H on $V_1^{\otimes n}$,

$$\widetilde{\mathsf{H}} := \sum \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \otimes \cdots \otimes \mathsf{H} \otimes \cdots \otimes \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right).$$

We begin with a lemma regarding projections of functions $Q \in \mathscr{D}$ to the Hamming sphere ω_w.

Lemma 6.2. *For $Q \in \mathscr{D}$, we have $Q|_{\omega_w} = \chi_{\omega_w} \cdot Q = \pi_{n-2w}(Q)$, where $\pi_{n-2w}(Q)$ is the projection of Q to the $n-2w$ eigenspace of the action of $\widetilde{\mathsf{H}}$ on $V_1^{\otimes n}$.*

Proof. This is immediate because the 1- and (-1)-eigenspaces of H are respectively spanned by $\{\left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right)\}$ and $\{\left(\begin{smallmatrix}0\\ 1\end{smallmatrix}\right)\}$. □

We now show Proposition 6.1.

Proof of Proposition 6.1. We denote by $\mathscr{O}$ the subset of $V_1^{\otimes n}$ consisting of tensor products of t copies of $\left(\begin{smallmatrix}0\\ 1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right)$ and $n-t$ copies of $\left(\begin{smallmatrix}1\\ 1\end{smallmatrix}\right)$. It is clear that $\mathscr{O}$ spans $\mathscr{P}_d$ for any d ($0 \leq d \leq t$). Now, the set D is a t-design if and only if, for all $R \in \mathscr{O}$,

$$(\chi_D, R) = (|D|, R),$$

where $|D|$ is the constant function on ω_w with value equal to the cardinality of D and $(\cdot, \cdot)$ is the inner product. It therefore suffices to show that the set of restrictions $\{R|_{\omega_w} : R \in \mathscr{O}\}$ is spanned by

$$\bigcup_{d=0}^{t} \{Q|_{\omega_w} : Q \in \mathscr{D}_d^0\}.$$

By the second part of Proposition 5.15, any $R \in \mathscr{O}$ may be written in the form

$$R = \sum_{j=0}^{t} (\widetilde{\mathsf{Y}'})^j Q_j,$$

with $Q_j \in \bigcup_{d=0}^{t-j} \mathscr{D}_d^0$. By Lemma 6.2 and the hypothesis, it then only remains to demonstrate that $\pi_{n-2w}((\widetilde{\mathsf{Y}'})^j Q_j)$ and $\pi_{n-2w}(Q_j)$ are related by a constant factor: for each $j = 0, \ldots, t$, we have

$$\pi_{n-2w}((\widetilde{\mathsf{Y}'})^j Q_j) = b \cdot \pi_{n-2w}(Q_j) \tag{6.1}$$

for some constant b depending on both j and t.

Now, given any $Q \in \mathscr{D}_d^0$, we see by the third part of Proposition 5.15 that the polynomials $(\widetilde{\mathsf{Y}'})^k Q$ $(0 \leq k \leq n-2d)$ span an irreducible representation of $\mathfrak{sl}_2$ which is isomorphic to V_{n-2d}. We may regard this representation as $(n-2d)$-th homogeneous part of the polynomial algebra $\mathbb{C}[u_0, u_1]$ with generators u_0, u_1 and with actions of $\mathsf{X}', \mathsf{H}', \mathsf{Y}'$ respectively given by

$$u_0' \frac{\partial}{\partial u_1'}, \quad \left(u_0' \frac{\partial}{\partial u_0'} - u_1' \frac{\partial}{\partial u_1'} \right), \quad u_1' \frac{\partial}{\partial u_0'},$$

where $u_0' = u_0 + u_1$ and $u_1' = u_0 - u_1$. With this identification, we may take $Q = (u_0')^{n-2d}$, as

$$Q \in \ker\bigl(\widetilde{\mathsf{X}'} : \mathscr{D}_d^0 \to \mathscr{D}_{d-1}^0\bigr).$$

We now show that $\pi_{n-2w}((\widetilde{\mathsf{Y}'})^k Q)$ and $\pi_{n-2w}(Q)$ are related by a constant factor for any k $(0 \leq k \leq n-2d)$; the desired expression (6.1) follows. We observe that $\widetilde{\mathsf{H}}$ acts as

$$u_0 \frac{\partial}{\partial u_0} - u_1 \frac{\partial}{\partial u_1}.$$

Therefore, $\pi_{n-2w}(Q) = \pi_{n-2w}((u_0 + u_1)^{n-2d})$ is equal $u_0^{n-(d+w)} u_1^{w-d}$. To see this, note that $\pi_{n-2w}((u_0+u_1)^{n-2d}) = u_0^{b_0} u_1^{b1}$ with $b_0 + b_1 = n - 2d$ and $b_0 - b_1 = n - 2w$. (The latter statement follows from the definition of $\pi_{n-2w}(\cdot)$.) Likewise,

$$\pi_{n-2w}((\widetilde{\mathsf{Y}'})^k Q) = \pi_{n-2w}((\widetilde{\mathsf{Y}'})^k (u_0 + u_1)^{n-2d})$$

is the $u_0^{n-(d+w)} u_1^{w-d}$ component of $(\widetilde{\mathsf{Y}'})^k (u_0 + u_1)^{n-2d}$. Since this component is equal to

$$u_0^{n-(d+w)} u_1^{w-d} = \pi_{n-2w}(Q)$$

up to a constant factor, we are done. □

Remarks

The constant relating $\pi_{n-2w}((\widetilde{\Upsilon}')^k Q)$ and $\pi_{n-2w}(Q)$ in the proof of Proposition 6.1 was obtained directly from the identification of $\left\{(\widetilde{\Upsilon}')^k Q\right\}_{k=0}^{n-2d}$ with V_{n-2d}. Consequently, this constant is independent of the choice of $Q \in \mathscr{D}_d^0$.

Proposition 6.1 leads to another equivalent characterization of t-designs which makes the analogy between t-designs and spherical t-designs explicit. We have the following corollary, which is equivalent to Theorem 6 of Delsarte [Del78].

Corollary 6.3. *A set $D \subseteq \omega_w$ is a t-design if and only if*

$$\frac{1}{|D|}\sum_{v\in D} Q(v) = \frac{1}{|\omega_w|}\sum_{v\in\omega_w} Q(v) \tag{6.2}$$

for all $Q \in \bigcup_{d=1}^{t} \mathscr{D}_d$.

Proof. As (6.2) is immediate when Q is constant, the result follows directly from Proposition 6.1 and the second part of Proposition 5.15. □

Finally, we note that the proof of Proposition 6.1 shows that each $Q \in \mathscr{D}_d^0$ is supported on $\bigcup_{w=d}^{n-d} \omega_w$. This fact leads to an alternate proof of Corollary 5.21.

Alternate Proof of Corollary 5.21. As $Q \in \mathscr{D}_d^0$ is supported on $\bigcup_{w=d}^{n-d} \omega_w$, we know that

$$W_{C,Q}(x,y) = \sum_{w=0}^{n}\left(\sum_{c\in C_w} Q(c)\right) x^{n-w}y^w = \sum_{w=d}^{n-d}\left(\sum_{c\in C_w} Q(c)\right) x^{n-w}y^w.$$

The result then follows immediately. □

6.1.2 The Extremal Type II Code Case of the Assmus–Mattson Theorem

To illustrate the power of Proposition 6.1, we now prove the extremal Type II code case of the Assmus–Mattson Theorem for binary codes (Theorem 2.1).[2]

Theorem 6.4. *If C is an extremal Type II code of length n and $w > 0$ is such that $C_w \neq \emptyset$, then C_w is a t-design for any $t \leq \mathrm{t}(n)$.*

By Proposition 6.1, this theorem follows quickly from the following result, which is slightly more general and is a coding-theoretic analog of Theorem 4.4.

[2] Corollary 2.2 of Section 2.4 is a special case of Theorem 6.4.

Proposition 6.5. *If C is an extremal Type II code of length n and $w > 0$, then for any choices of $d \in \{1, \ldots, \mathrm{t}(n)\} \cup \{\mathrm{t}(n) + 2\}$ and $Q \in \mathscr{D}_d^0$, we have*

$$\sum_{c \in C_w} Q(c) = 0.$$

Proposition 6.5 was originally proven by Calderbank and Delsarte [CD93]. Here, we demonstrate how Proposition 6.5 follows quickly from Theorem 5.22. This approach is due to Bachoc [Bac99] and is analogous to the proof of Theorem 4.4. Our exposition of this argument expands slightly upon that of Bachoc [Bac99], which demonstrated only four cases of the result.

Proof of Proposition 6.5. We let $d \in \{1, \ldots, \mathrm{t}(n)\} \cup \{\mathrm{t}(n) + 2\}$ and $Q \in \mathscr{D}_d^0$. Then, we consider the harmonic weight enumerator $W_{C,Q}(x, y)$. By Theorems 5.16 and 5.22, we see that $W_{C,Q}(x, y)/(xy)^d$ has a factor of the form

$$\xi_{24}^{\frac{\min(C) - d - b_d}{4}} \cdot f,$$

where b_d is equal to the valuation of y in ψ_d and $f \in \mathbb{C}[\varphi_8, \xi_{24}, \psi_d]$. This factor arises because the valuation of y in $W_{C,Q}(x, y)$ equals $\min(C)$ and we may write $W_{C,Q}(x, y)/(xy)^d$ as a product of ψ_d and an element of $\mathbb{C}[\varphi_8, \xi_{24}, \psi_d]$ if $d \not\equiv 0 \bmod 4$, or simply as an element of $\mathbb{C}[\varphi_8, \xi_{24}]$ if $d \equiv 0 \bmod 4$.

We see that if f is nonzero, then it has degree equal to

$$(n \bmod 24) + 4d - 24 \tag{6.3}$$

if $d \equiv 0 \bmod 2$. Similarly, f has degree

$$(n \bmod 24) + 4d - 36 \tag{6.4}$$

if $d \equiv 1 \bmod 2$. Since (6.3) and (6.4) are always negative for $d \in \{1, \ldots, \mathrm{t}(n)\} \cup \{\mathrm{t}(n) + 2\}$, we must have $f \equiv 0$, hence

$$\sum_{w=0}^{n} \left(\sum_{c \in C_w} Q(c) \right) x^{n-w} y^w = W_{C,Q}(x, y) \equiv 0. \qquad \square$$

We also note the following special case of Proposition 6.1 which is relevant to our proofs of configuration results in Section 6.3.

Corollary 6.6. *If C is an extremal Type II code of length n and $w > 0$, then we have*

$$\sum_{c \in C_w} Q_{t;\dot{v}}(c) = 0$$

for any $t \in \{1, \ldots, \mathrm{t}(n)\} \cup \{\mathrm{t}(n) + 2\}$.

Remarks

As Bachoc [Bac99] illustrates, it is possible to prove the full Assmus–Mattson Theorem (Theorem 2.1) with a harmonic weight enumerator argument similar to that used in the proof of Proposition 6.5. We have focused upon the case of an extremal Type II code because the full force of Corollary 6.6 is required in Section 6.3.

6.2 Type II Codes of Length 24

6.2.1 Koch's Tetrad System Condition

Through appeal to Venkov's [Ven80] condition restricting the possible root systems of Type II lattices of rank 24 (our Proposition 4.3), Koch [Koc87] obtained a condition on the tetrad systems of Type II codes of length 24. Specifically, he showed the following result.

Proposition 6.7. *If C is a Type II code of length 24, then C has one of the following nine tetrad systems:*

$$\emptyset, \quad 6d_4, \quad 4d_6, \quad 3d_8, \quad 2d_{12}, \quad d_{24}, \quad 2e_7 + d_{10}, \quad 3e_8, \quad e_8 + d_{16}.$$

The following brief argument, which is that used by Koch [Koc87], illustrates how Proposition 6.7 follows from results for lattices, specifically Proposition 4.3.

Proof of Proposition 6.7. For C Type II of length 24, the lattice L_C obtained from Construction A is Type II of rank 24. The result then follows immediately from Proposition 6.7, since we have $L_{d_{2k}} = D_{2k}$ and $L_{e_k} = E_k$, as we remarked in (2.8). □

Proposition 6.7 is also a consequence of the classification of Type II codes of length 24 given by Pless and Sloane [PS75].[3]

6.2.2 A Purely Coding-theoretic Proof of Koch's Condition

Here, we present a direct and purely coding-theoretic proof of Proposition 6.7 due to Elkies and the author [EK09a] which uses the theory of harmonic weight enumerators. This argument is closely analogous to that of Venkov [Ven80] for the proof of Proposition 4.3, and so we begin with a coding-theoretic analog of the rank-24 case of Lemma 4.1.

[3] This is unsurprising, however, as a complete classification of Type II codes of any length implicitly gives a classification of the possible tetrad systems of those codes.

Lemma 6.8. *If C is a Type II code of length 24, then*

- *either $C_4 = \emptyset$ or for each j ($1 \le j \le 24$) there exists $c \in C_4$ such that $c_j = 1$, and*
- *each irreducible component of $\mathcal{C}_4(C)$ has tetrad number equal to $|C_4|/24$.*

For each j ($1 \le j \le n$), we denote by $Q_{1,j,n}$ the discrete harmonic polynomial defined by

$$Q_{1,j,n}(v) := n \cdot (-1)^{v_j} - \sum_{k=1}^{n} (-1)^{v_k} \in \mathscr{D}_1^0.$$

Proof of Lemma 6.8. As in the proof of Proposition 6.5, we see that the harmonic weight enumerator

$$W_{C,Q_{1,j,24}}(x,y) = \sum_{w=0}^{24} \left(\sum_{c \in C_w} Q_{1,j,24}(c) \right) x^{24-w} y^w \tag{6.5}$$

vanishes for each j ($1 \le j \le 24$). We then obtain

$$\sum_{c \in C_4} (24c_j - 4) = 0 \tag{6.6}$$

for each j ($1 \le j \le 24$), since the left side of (6.6) is the $(x+y)^{20}(x-y)^4$ coefficient of the discrete Fourier transform of (6.5). Reorganizing (6.6) shows that

$$|\{c \in C_4 : c_j = 1\}| = |C_4|/6. \tag{6.7}$$

The first part of the lemma then follows. In the case that $C_4 \neq \emptyset$, we also obtain from (6.7) that each irreducible component of $\mathcal{C}_4(C)$ has tetrad number $\frac{1}{4}|C_4|/6 = |C_4|/24$. □

Proposition 6.7 now follows directly from Lemma 6.8.

Alternate Proof of Proposition 6.7. As we mentioned in Section 2.2.2, there is at most one tetrad system with tetrad number η for each $\eta \notin \{1, 7/4\}$, and for each $\eta \in \{1, 7/4\}$ there are exactly two tetrad systems with tetrad number η. Namely, d_{10} and e_7 have tetrad numbers $\eta(d_{10}) = \eta(e_7) = 1$, and d_{16} and e_8 have tetrad numbers $\eta(d_{16}) = \eta(e_8) = 7/4$.

Now, Lemma 6.8 implies that if $C_4 \neq \emptyset$, then either C_4 consists of μ copies of the tetrad system d_{2k} for some μ and $k > 1$ such that $\mu \cdot 2k = 24$, or it has one of the following two forms:

- $\delta_{10} d_{10} + \varepsilon_7 e_7$, with $\varepsilon_7 > 0$ and $10\delta_{10} + 7\varepsilon_7 = 24$, or
- $\delta_{16} d_{16} + \varepsilon_8 e_8$, with $\varepsilon_8 > 0$ and $16\delta_{16} + 8\varepsilon_8 = 24$. □

6.3 Configurations of Extremal Type II Codes

We now prove configuration results for extremal Type II codes. Specifically, we show that if C is an extremal Type II code of length $n = 8, 24, 32, 48, 56, 72, 96$, then C is generated by its minimal-weight codewords, i.e. $C = \mathcal{C}_{\min(C)}(C)$. Our approach uses the harmonic weight enumerator machinery developed in Chapter 5, following the approach used for lattices in Section 4.3.

These results are the first ever coding-theoretic analogs of the results obtained for lattices in Section 4.3.[4] Furthermore, they are all original to this thesis.

6.3.1 Preliminaries

First, we present a few brief preliminaries. For any $\dot{v} \in \mathbb{F}_2^n$, any length-$n$ binary linear code C, and any j $(0 \leq j \leq n)$, we denote by $N_j(C; \dot{v})$ the value

$$N_j(C; \dot{v}) := \left|\left\{c \in \mathcal{C}_{\min(C)}(C) : \mathrm{wt}(c \cap \dot{v}) = j\right\}\right|.^5$$

For $c \in C^{\perp}$, we must have $N_{2j'+1}(C; c) = 0$ for all j' with $0 \leq j' \leq \lfloor n/2 \rfloor$.

Throughout the remainder of this section, C denotes a length-n extremal Type II code, and $w_0 := \min(C)$ denotes the minimal weight of codewords in C. We now prove a coding-theoretic analog of Lemma 4.7.

Lemma 6.9. *For $\dot{c}$ a minimal-weight representative of the class $[\dot{c}] \in C/\mathcal{C}_{w_0}(C)$ and $c \in C_{w_0}$, we have the inequality*

$$\mathrm{wt}(c \cap \dot{c}) \leq \frac{w_0}{2}.$$

Proof. This follows quickly, because if $\mathrm{wt}(c \cap \dot{c}) > w_0/2$, then $[\dot{c}]$ contains a codeword $c + \dot{c}$ of weight

$$\mathrm{wt}(c + \dot{c}) = \mathrm{wt}(c) + \mathrm{wt}(\dot{c}) - 2\mathrm{wt}(c \cap \dot{c}) < \mathrm{wt}(\dot{c}).$$

This contradicts the minimality of $\dot{c}$ in $[\dot{c}]$. □

[4] Our results are the first configuration results for lengths n in which the full sets of extremal Type II codes are not known. Technically, however, the analogous facts have been known (if only implicitly) for extremal Type II codes of lengths 8, 24, and 32, as the extremal Type II codes of these lengths have been fully classified. As in the lattice case and as we discuss in the remarks below, our methods yield that the extremal Type II codes of these lengths are generated by their minimal codewords without appeal to the classification results or to the explicit forms of these codes.

[5] This is slightly abusive notation, since we use the notation $N_j(L; \dot{x})$ to denote the analogous but slightly different count for lattices. However, we are only concerned with codes in this chapter and it seems beneficial to use a familiar notation.

6.3.2 Extremal Type II Codes of Lengths 32, 48, and 72

As we found for lattices in Section 4.3.2, the easiest cases to examine are those when $n = 32, 48, 72$. We therefore begin with the configuration result for these n, proving a coding-theoretic analog of Theorem 4.10.

Theorem 6.10. *If C is an extremal Type II code of length $n = 32, 48, 72$, then*

$$C = \mathcal{C}_{w_0}(C).$$

Proof. We consider the equivalence classes of $C/\mathcal{C}_{w_0}(C)$ and assume for the sake of contradiction that there is some class $[\dot{c}] \in C/\mathcal{C}_{w_0}(C)$ with minimal-weight representative $\dot{c}$ with $\mathrm{wt}(\dot{c}) = s > w_0$.

As C is self-dual, we have $N_{2j'+1}(C; c) = 0$ for all $0 \leq j' \leq \lfloor n/2 \rfloor$. Additionally, by Lemma 6.9, we must have $N_{2j'}(C; \dot{c}) = 0$ for $j' > w_0/4$. We now develop a system of equations in the

$$\frac{w_0}{4} + 1$$

variables $N_0(C; \dot{c}), N_2(C; \dot{c}), \ldots, N_{w_0/2}(C; \dot{c})$.

Combining the $\mathrm{t}(n) + 1$ equations of Proposition 6.1 with the equation

$$N_0(C; \dot{c}) + N_2(C; \dot{c}) + \cdots + N_{w_0/2}(C; \dot{c}) = |C_{w_0}| \tag{6.8}$$

gives a system of

$$\mathrm{t}(n) + 2 > \frac{w_0}{4} + 1$$

equations in the variables $N_{2j'}(C; \dot{c})$ $(0 \leq j' \leq w_0/4)$.

For $n = 32, 48, 72$, the (extended) determinants of these inhomogeneous systems are

$$2^{17}3^{1}5^{2}7^{1}29^{1}31^{1}\left(\frac{7s^2 - 126s + 584}{(s-2)(s-1)^2 s^2}\right), \tag{6.9}$$

$$2^{26}3^{5}5^{2}7^{1}11^{2}23^{2}43^{1}47^{1}\left(\frac{11s^3 - 396s^2 + 4906s - 20736}{(s-3)(s-2)^2(s-1)^3 s^3}\right), \tag{6.10}$$

$$2^{42}3^{5}5^{2}7^{2}11^{2}13^{1}17^{3}23^{2}67^{2}71^{1}\left(\frac{39s^4 - 2600s^3 + 67410s^2 - 800440s + 3650496}{(s-4)(s-3)^2(s-2)^3(s-1)^4 s^4}\right), \tag{6.11}$$

respectively[6]; these determinants must vanish, as they are derived from overdetermined systems. Since equations (6.9)–(6.11) have no integer roots s, we have reached a contradiction. □

[6] These determinants were computed using the formula of Proposition 5.24. As in the proof of Theorem 4.10, we omit the equations obtained from the zonal spherical harmonic polynomials of the largest degrees when there are more than $\frac{w_0}{4} + 2$ equations obtained by this method.

Remarks

The approach used to prove Theorem 6.10 may also be applied to show that extremal Type II codes of lengths $n = 8, 24$ are generated by their minimal-weight codewords. In these cases the determinants

$$2688\left(\frac{3s-10}{(s-1)s}\right), \quad 28725903360\left(\frac{7s^2-98s+344}{(s-2)(s-1)^2s^2}\right)$$

are obtained; neither has integral roots s. We therefore observe the following result.

Theorem 6.11. *If C is an extremal Type II code of length $n = 8, 24$, then $C = \mathcal{C}_{w_0}(C)$.*

As we found for lattices, there is no configuration result analogous to Theorems 6.10 and 6.11 for extremal Type II codes of length $n = 16$. Indeed, the extremal Type II code with tetrad subcode d_{16} has codewords of weight 8 which cannot be obtained as linear combinations of codewords of weight 4. As expected, performing the method used to prove Theorem 6.10 in this case yields the determinant

$$-93184\left(\frac{s-8}{(s-1)s}\right),$$

which vanishes for $s = 8$.

6.3.3 Extremal Type II Codes of Lengths 56 and 96

Now, we prove a result for extremal Type II codes of ranks $n = 56, 96$ analogous to Theorem 6.10. The approach here is analogous to that of the proof of Theorem 4.12, hence we begin with the following lemma analogous to Lemma 4.13.

Lemma 6.12. *If C is an extremal Type II code of length n and $w > 0$ is such that $C_w \neq \emptyset$, then for each j ($1 \le j \le n$) there exists $c \in C_w$ such that $c_j = 1$.*

Proof. By Theorem 6.4, C_w is a 1-design. We then have from Corollary 6.3 that

$$\sum_{c \in C_w} c_j = \frac{|C_w|}{|\omega_w|}\sum_{v \in \omega_w} v_j > 0.$$

The result follows immediately. □

We now state and prove the configuration result for extremal Type II codes of ranks 56 and 96.

Theorem 6.13. *If C is an extremal Type II code of length $n = 56, 96$, then*

$$C = \mathcal{C}_{w_0}(C).$$

Proof. Seeking a contradiction, we suppose that $\mathcal{C}_{w_0}(C) \neq C$ and consider $\mathcal{C}_{w_0}(C)^\perp$. We must have $\mathcal{C}_{w_0}(C)^\perp \neq \mathcal{C}_{w_0}(C)$, since otherwise we would have $\mathcal{C}_{w_0}(C) = C$ by Lemma 6.12. Thus, there is some equivalence class $[\dot{c}] \in (\mathcal{C}_{w_0}(C)^\perp)/(\mathcal{C}_{w_0}(C))$ with minimal-weight representative $\dot{c}$ of weight $\mathrm{wt}(\dot{c}) = s > 0$.

Proposition 6.1 yields $\mathrm{t}(n) + 1$ equations in the variables $N_{2j'}(C; \dot{c})$ $(0 \leq j' \leq w_0/4)$.[7] Combining this with the equation (6.8), we obtain a system of $\mathrm{t}(n) + 2$ equations in the

$$\frac{w_0}{2} + 1 < \mathrm{t}(n) + 2$$

variables $N_{2j'}(C; \dot{c})$ $(0 \leq j' \leq w_0/4)$. For $n = 56, 96$, these inhomogeneous systems have (extended) matrices with determinants

$$-2^{27}3^{7}5^{3}7^{3}11^{1}13^{2}17^{1}53^{1}\left(\frac{(s-16)\left(3s^3-112s^2+1368s-5120\right)}{(s-4)(s-3)(s-2)^2(s-1)^3s^3}\right), \tag{6.12}$$

$$-2^{59}3^{9}5^{4}7^{2}11^{2}13^{2}17^{1}19^{1}23^{3}29^{1}31^{2}43^{1}47^{2}89^{2} \cdot S_{96}(s), \tag{6.13}$$

where S_{96} is the rational function

$$S_{96}(s) = \left(\frac{(s-24)\left(68s^5-6936s^4+289901s^3-6153306s^2+65640728s-277774080\right)}{(s-6)(s-5)(s-4)^2(s-3)^3(s-2)^4(s-1)^5s^5}\right).$$

These determinants must vanish, but the only integral roots of (6.12) and (6.13) are multiples of 4. Therefore, $\mathcal{C}_{w_0}(C)^\perp$ is doubly even, and it follows that $\mathcal{C}_{w_0}(C)^\perp$ is self-orthogonal. Then, $\dim(\mathcal{C}_{w_0}(C)^\perp) \leq n/2$ and so $\dim(\mathcal{C}_{w_0}(C)) \geq n/2$. We must therefore have $\mathcal{C}_{w_0}(C) = C$. □

[7] As in the proof of Theorem 6.10, the variables $N_j(C; \dot{c})$ vanish for j not of the form $2j'$ with $0 \leq j' \leq w_0/4$, as the conclusion of Lemma 6.9 holds for $[\dot{c}] \in (\mathcal{C}_{w_0}(C)^\perp)/(\mathcal{C}_{w_0}(C))$.

References

[AM69] E. F. Assmus and H. F. Mattson, *New 5-designs*, Journal of Combinatorial Theory **6** (1969), 122–151.

[Art91] M. Artin, *Algebra*, Prentice-Hall, 1991.

[Bac99] C. Bachoc, *On harmonic weight enumerators of binary codes*, Designs, Codes and Cryptography **18** (1999), 11–28.

[Bac01] ———, *Harmonic weight enumerators of non-binary codes and MacWilliams identities*, Codes and Association Schemes (A. Barg and S. Litsyn, eds.), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 56, American Mathematical Society, 2001, pp. 1–24.

[BN98] C. Bachoc and G. Nebe, *Extremal lattices of minimum 8 related to the Mathieu Group M_{22}*, Journal für die reine und angewandte Mathematik (Crelle's Journal) **494** (1998), 155–171.

[CD93] A. R. Calderbank and P. Delsarte, *On error-correcting codes and invariant linear forms*, SIAM Journal on Discrete Mathematics **6** (1993), 1–23.

[CP80] J. H. Conway and V. Pless, *On the enumeration of self-dual codes*, Journal of Combinatorial Theory, Series A **28** (1980), 26–53.

[CP92] ———, *The binary self-dual codes of length up to 32: a revised enumeration*, Journal of Combinatorial Theory, Series A **60** (1992), 183–195.

[CS99] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, 3rd ed., Springer-Verlag, 1999.

[Del78] Ph. Delsarte, *Hahn polynomials, discrete harmonics, and t-designs*, SIAM Journal on Applied Mathematics **34** (1978), 157–166.

[Ebe02] W. Ebeling, *Lattices and codes: A course partially based on lectures by F. Hirzebruch*, 2nd ed., Vieweg, 2002.

[EK09a] N. D. Elkies and S. D. Kominers, *On the classification of Type II codes of length* 24, `arXiv:0902.1942`, 2009.

[EK09b] ———, *Refined configuration results for extremal Type II lattices of ranks* 40 *and* 80, `arXiv:0905.4306`, 2009.

[Elk09a] N. D. Elkies, *On the quotient of an extremal Type II lattice of rank* 40*,* 80*, or* 120 *by the span of its minimal vectors*, in preparation, 2009.

[Elk09b] ———, *Theta-functions and weighted theta-functions of Euclidean lattices, with some applications*, Lecture notes of the Arizona Winter School on Quadratic Forms, 2009.

[Gle71] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes, Congrés International de Mathématiques (Nice, 1970), vol. 3, Gauthiers-Villars, 1971, pp. 211–215.

[GZ08] F. Greer and X. Zhu, *Error-correcting codes and sphere packings*, The Harvard College Mathematics Review **2** (2008), no. 2, 4–11.

[Hal05] T. C. Hales, *A proof of the Kepler conjecture*, Annals of Mathematics **162** (2005), 10651185.

[Har08] M. Harada, *An extremal doubly even self-dual code of length* 112, The Electronic Journal of Combinatorics **15** (2008), N33.

[HHM$^+$09] T. C. Hales, J. Harrison, S. McLaughlin, T. Nipkow, S. Obua, and R. Zumkeller, *A revision of the proof of the Kepler conjecture*, `arXiv:0902.0350`, 2009.

[Iwa97] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, vol. 17, American Mathematical Society, 1997.

[KA08] S. D. Kominers and Z. Abel, *Configurations of rank-*$40r$ *extremal even unimodular lattices (*$r = 1, 2, 3$*)*, Journal de Théorie des Nombres de Bordeaux **20** (2008), 365–371.

[Kin01] O. D. King, *The mass of extremal doubly-even self-dual codes of length* 40, IEEE Transactions on Information Theory **47** (2001), 2558–2560.

[Koc87] H. Koch, *Unimodular lattices and self-dual codes*, Proceedings of the International Congress of Mathematicians (Berkeley, Calif., 1986), American Mathematical Society, 1987, pp. 457–465.

[Kom09] S. D. Kominers, *Configurations of extremal even unimodular lattices*, International Journal of Number Theory **5** (2009), 457–464.

[Lee67] J. Leech, *Notes on sphere packings*, Canadian Journal of Mathematics **19** (1967), 251–267.

[LS71] J. Leech and N. J. A. Sloane, *Sphere packing and error-correcting codes*, Canadian Journal of Mathematics **23** (1971), 718–745.

[Mac63] F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell System Technical Journal **42** (1963), 79–84.

[MOS75] C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, *Upper bounds for modular forms, lattices and codes*, Journal of Algebra **36** (1975), 68–76.

[MS73] C. L. Mallows and N. J. A. Sloane, *An upper bound for self-dual codes*, Information and Control **22** (1973), 188–200.

[MS83] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 3rd ed., North-Holland Mathematical Library, vol. 16, North-Holland, 1983.

[MST72] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, *Good self-dual codes exist*, Discrete Mathematics **3** (1972), 153–162.

[Nie73] H.-V. Niemeier, *Definite quadratische Formen der Dimension* 24 *und Diskriminante* 1, Journal of Number Theory **5** (1973), 142–178 (German).

[Oze86a] M. Ozeki, *On even unimodular positive definite quadratic lattices of rank* 32, Mathematische Zeitschrift **191** (1986), 283–291.

[Oze86b] ———, *On the configurations of even unimodular lattices of rank* 48, Archiv der Mathematik **46** (1986), 54–61.

[Oze89] ———, *On the structure of even unimodular extremal lattices of rank* 40, Rocky Mountain Journal of Mathematics **19** (1989), 847–862.

[Pas81] G. Pasquier, *A binary extremal doubly even self-dual code* $(64, 32, 12)$ *obtained from an extended Reed-Solomon code over* F_{16}, IEEE Transactions on Information Theory **27** (1981), 807–808.

[Ple72] V. Pless, *A classification of self-orthogonal codes over* $\mathrm{GF}(2)$, Discrete Mathematics **3** (1972), 209–246.

[PS75] V. Pless and N. J. A. Sloane, *On the classification and enumeration of self-dual codes*, Journal of Combinatorial Theory, Series A **18** (1975), 313–335.

[RS98] E. M. Rains and N. J. A. Sloane, *Self-dual codes*, Handbook of Coding Theory (V. S. Pless, W. C. Huffman, and R. A. Brualdi, eds.), Elsevier, 1998.

[Ser73] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, 1973.

[Ser01] ———, *Complex Semisimple Lie Algebras*, Springer-Verlag, 2001.

[Slo73] N. J. A. Sloane, *Is there a* $(72, 36)$ $d = 16$ *self-dual code?*, IEEE Transactions on Information Theory **19** (1973), 251.

[Tan09] H. Tanaka, *New proofs of the Assmus–Mattson theorem based on the Terwilliger algebra*, European Journal of Combinatorics **30** (2009), 736–746.

[Ven80] B. B. Venkov, *On the classification of integral even unimodular* 24*-dimensional quadratic forms*, Proceedings of the Steklov Institute of Mathematics **148** (1980), 63–74.

[Ven84a] ———, *Even unimodular Euclidean lattices in dimension* 32, Journal of Mathematical Sciences **26** (1984), 1860–1867.

[Ven84b] ———, *Even unimodular extremal lattices*, Proceedings of the Steklov Institute of Mathematics **165** (1984), 47–52.

[Ven01] ———, *Réseaux et designs sphériques*, Réseaux Euclidiens, Designs Sphériques et Formes Modulaires, Monographie de L'Enseignement Mathematique, vol. 37, Enseignement Mathematique, Genève, 2001, (in French), pp. 10–86.

[Vil68] N. J. Vilenkin, *Special Functions and the Theory of Group Representations*, Translations of Mathematical Monographs, vol. 22, American Mathematical Society, 1968.

[War00] H. N. Ward, *The MacWilliams identity*, Archiv der Mathematik **74** (2000), 95–96.

[Wit41] E. Witt, *Eine Identität zwischen Modulformen zweiten Grades*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **14** (1941), 323–337.