The Belfiore-Solé Conjecture for Unimodular Lattices

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Mathematics

by

Julia Pinchak

August 2013
The thesis of Julia Pinchak is approved:

Dr. Jerry Rosen
Date

Dr. Daniel Katz
Date

Dr. B.A. Sethuraman, Chair
Date

California State University, Northridge
Dedications

I dedicate this thesis to my grandmother, who always told me to trust my instincts and pursue a career in Mathematics.
Acknowledgments

I would first and foremost like to acknowledge my thesis advisor, Professor B.A. Sethuraman, whose guidance and support has allowed me to successfully complete this thesis. I am grateful to the National Science Foundation for support under Professor Sethuraman’s grant DMS-0700904, and to the Interdisciplinary Research Institute for the Sciences (IRIS) at CSUN as well as the Department of Mathematics for support.

I would like to thank Professors Daniel Katz and Jerry Rosen for their time and involvement in my thesis committee.

I would also like to acknowledge my family, who always have my back and remind me of my capabilities. Additionally, I would like to acknowledge my friends who have stood by me through this entire process.

Finally, I would like to thank my dog for his endless company and comfort.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Page</td>
<td>ii</td>
</tr>
<tr>
<td>Dedications</td>
<td>iii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>Abstract</td>
<td>vi</td>
</tr>
<tr>
<td>1 Wiretap Codes, Lattices, and the Belfiore-Solé Conjecture</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Wire Tap Codes</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Lattices</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Coset Coding</td>
<td>5</td>
</tr>
<tr>
<td>1.4 The Belfiore-Solé Conjecture</td>
<td>7</td>
</tr>
<tr>
<td>2 Codes</td>
<td>9</td>
</tr>
<tr>
<td>3 Infinitely Many Lattices Satisfy the Belfiore-Solé Conjecture</td>
<td>13</td>
</tr>
<tr>
<td>3.1 Ernvall-Hytönen’s Framework for Studying Belfiore-Solé Conjecture</td>
<td>13</td>
</tr>
<tr>
<td>for Unimodular Lattices</td>
<td></td>
</tr>
<tr>
<td>3.2 Proof that Infinitely Many Lattices Satisfy the Belfiore-Solé Conjecture</td>
<td>21</td>
</tr>
<tr>
<td>4 Doubly Even Self-dual Codes up to Length 40 Satisfy the Belfiore-</td>
<td>26</td>
</tr>
<tr>
<td>Solé Conjecture</td>
<td></td>
</tr>
<tr>
<td>4.1 Length 24</td>
<td>27</td>
</tr>
<tr>
<td>4.2 Length 32</td>
<td>30</td>
</tr>
<tr>
<td>4.3 Length 40</td>
<td>31</td>
</tr>
<tr>
<td>5 Appendix</td>
<td>33</td>
</tr>
<tr>
<td>Bibliography</td>
<td>35</td>
</tr>
</tbody>
</table>
Abstract

The Belfiore-Solé Conjecture for Unimodular Lattices

by

Julia Pinchak

Master of Science in Mathematics

In this thesis we study the Belfiore-Solé conjecture on the secrecy function of unimodular lattices. This conjecture states that for a lattice $\Lambda$ in $\mathbb{R}^n$, the quotient of the theta series of $\mathbb{Z}^n$ by the theta series of $\Lambda$, when restricted to the purely imaginary values $z = iy, y > 0$, attains its maximum at $y = 1$. This conjecture is vitally connected to the confusion at the eavesdropper’s end in wiretap codes for Gaussian channels. We show that if $\Lambda_1$ and $\Lambda_2$ are lattices that satisfy the Ernvall-Hytönen criterion on derivatives [1], then so does the direct sum $\Lambda_1 \oplus \Lambda_2$. It follows immediately that infinitely many lattices satisfy the Belfiore-Solé conjecture. Further, we show that all lattices obtained by Construction A from doubly even self-dual codes of lengths up to 40 satisfy the Belfiore-Solé conjecture.
Chapter 1

Wiretap Codes, Lattices, and the Belfiore-Solé Conjecture

Our thesis involves a conjecture concerning wiretap codes, lattices, and their relation to minimizing proper decryption by eavesdroppers. This chapter will lay the framework for our thesis and introduce important concepts.

1.1 Wire Tap Codes

In [10], Wyner describes a method for transmitting confidential data to an intended recipient in the presence of an eavesdropper. This method is called the wire tap channel. The system is modeled on transmitter A, or Alice, encoding messages to intended receiver B, or Bob, through a discrete memoryless channel, which means that the messages are encoded into binary bits and each transmission is independent of previous messages. In this system, the channel between Alice and Bob is relatively noiseless, which means that there are very few hindrances to transmitting the correct message to Bob. However, this system is being wiretapped by an eavesdropper Eve, who is listening in through a second, much noisier channel.

Alice transforms a binary sequence $s_k = (s_1, \ldots, s_k)$ of length $k$ into a binary vector $x_n = (x_1, \ldots, x_n)$ of length $n$, for $n > k$. The vector $x_n$ is then sent to Bob, who receives the vector $\hat{x}_n = x_n + v_b$, where $v_b$ is an error vector for Bob’s received message. Due to the fact that the channel is relatively noiseless, the probability that $v_b = 0$, or $x_n = \hat{x}_n$ is relatively high. Bob then uses various estimation techniques regarding the received $\hat{x}_n$ to obtain $\hat{s}_k$. The error probability is the average error for each individual bit, that is

$$P_{\text{error}} = \frac{1}{K} \sum_{k=1}^{K} P(s_k \neq \hat{s}_k),$$

where $P(s_k \neq \hat{s}_k)$ is the probability that each individual received component $\hat{s}_k$ does not match the original individual component $s_k$. The transmission rate is $k/n$, and higher transmission rates are desired because they allow for faster and less redundant code transmission [11]. Some redundancy is required because it allows Bob some error-correcting capabilities (why this is can also be found in [11]), but the goal is to require as little redundancy as possible, which makes the code more efficient.

Now, wiretapper Eve is observing the transmitted vector $x_n$ through her channel with crossover probability $p_0$, $0 < p_0 \leq \frac{1}{2}$, where the crossover probability is defined as the probability of the opposite bit than is intended. Due to noise on her end, Eve
does not actually receive $x_n$ but receives $z_n = x_n + v_e$, where $v_e$ is the error vector for Eve’s received message. We define $\Delta$ as

$$\Delta = \frac{1}{k} H(s_k|z_n),$$

(1.2)

where $H(s_k|z_n)$ is an entropy function relating the probabilities of $s_k$ and $z_n$. The actual meaning of the entropy function is not as significant here as the fact that the goal is to minimize $P_{\text{error}}$ while maximizing $k/n$ and $\Delta$. To do this, certain knowledge about lattices and coset coding will prove very useful.

### 1.2 Lattices

This section will help to establish certain lattice definitions and calculations that will be used throughout the thesis.

If the vectors

\[
\begin{align*}
v_1 &= (v_{11}, v_{12}, \ldots, v_{1n}), \\
v_2 &= (v_{21}, v_{22}, \ldots, v_{2n}), \\
&\quad \vdots \\
v_n &= (v_{n1}, v_{n2}, \ldots, v_{nn}),
\end{align*}
\]

are $n$ linearly independent vectors in $\mathbb{R}^n$, then a (full) lattice $\Lambda$ is the discrete set of points in $\mathbb{R}^n$ given by all

$$a_1 v_1 + \ldots + a_n v_n, \quad a_i \in \mathbb{Z} \ \forall \ i = 1, \ldots, n.$$  

(1.3)

Collecting all vectors $v_i$ into the matrix

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{pmatrix},$$

(1.4)

we find

$$\Lambda = \{ x = uM \mid u \in \mathbb{Z}^n \}$$

(1.5)

([5], [4]). $M$ is called the generator matrix of $\Lambda$, and

$$A = MM^T$$

(1.6)

is called the Gram Matrix of $\Lambda$. Note that the $(i, j)^{th}$ entry of $A$ is $\langle v_i, v_j \rangle$, the inner
product of $v_i$ and $v_j$. The determinant of a lattice $\Lambda$ is equal to the determinant of its Gram matrix, so
\[
\det \Lambda = \det A \tag{1.7}
\]

There are many different types of lattices, and we will be focusing on lattices that are integral, unimodular, even, and extremal.

The following definitions will be useful:

1. A lattice $\Lambda$ is called integral if $\langle x, y \rangle \in \mathbb{Z}$ for all $x \in \Lambda$. This is equivalent to the Gram matrix having integer coefficients because if $x = \sum_{i=1}^{n} a_i v_i$ and $y = \sum_{i=1}^{n} b_i v_i$, then $\langle x, y \rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j \langle v_i, v_j \rangle$, where $a_i, b_i \in \mathbb{Z}$ for any lattice. Recall that $\langle v_i, v_j \rangle = A_{ij}$, the $(i, j)^{th}$ entry of $A$.

Therefore, $\langle x, x \rangle \in \mathbb{Z}$ for all $x$, or $\Lambda$ is integral, if and only if $A_{ij} \in \mathbb{Z}$ for all $i, j = 1, \ldots, n$, that is, if and only if its Gram matrix has integral coefficients.

2. An even lattice is a lattice in which $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in \Lambda$. Every even unimodular lattice has dimension $n$, where $n \equiv 0 \mod 8$. The proof of this is lengthy and can therefore be further explored in [4]. If a lattice is not even, then it is called an odd lattice.

3. The dual $\Lambda^\perp$ of a lattice $\Lambda$ is defined as
\[
\Lambda^\perp = \{ x \in \mathbb{R}^n \mid \langle x, y \rangle \in \mathbb{Z} \ \forall \ y \in \Lambda \}. \tag{1.8}
\]

For every integral lattice $\Lambda$, $\Lambda \subseteq \Lambda^\perp$, because the inner product of any 2 vectors in an integral lattice is in $\mathbb{Z}$.

4. The volume $\text{Vol}(\mathbb{R}^n/\Lambda)$ of a lattice $\Lambda$ is defined as
\[
\text{Vol}(\mathbb{R}^n/\Lambda) = \sqrt{\det(\Lambda)} = \sqrt{\det(A)}. \tag{1.9}
\]

Note that in the case of a full lattice, $M$ is just a square matrix, so $\sqrt{\det(A)} = |\det(M)|$.

5. Given a sublattice $\Lambda' \subset \Lambda$,
\[
\text{Vol}(\mathbb{R}^n/\Lambda') = \text{Vol}(\mathbb{R}^n/\Lambda)|\Lambda/\Lambda'|, \tag{1.10}
\]

or equivalently,
\[
\det(\Lambda') = \det(\Lambda)|\Lambda/\Lambda'|^2, \tag{1.11}
\]

where $|\Lambda/\Lambda'|$ is the index of $\Lambda'$ in $\Lambda$.

6. A lattice $\Lambda$ is called unimodular if $\Lambda = \Lambda^\perp$. This is equivalent to $\Lambda$ being integral with $|\det(\Lambda)| = 1$. This is because $\det(\Lambda) \det(\Lambda^\perp) = 1$, so when $\Lambda = \Lambda^\perp$,
| det(Λ)| = 1. Conversely, if Λ is integral and | det(Λ)| = 1, then Λ ⊆ Λ⊥. Also, because | det(Λ)| = 1,

\[ \det(Λ) = \det(Λ⊥)|Λ⊥/Λ|^2, \quad (1.12) \]

where det(Λ) = 1, and det(Λ⊥) and |Λ⊥/Λ|^2 are both greater than or equal to 1, so each must equal 1 and therefore Λ = Λ⊥.

7. Because every even unimodular lattice has dimension divisible by 8, its dimension can be written as

\[ n = 24m + 8k, \quad \text{for } m, k ∈ \mathbb{N}, \quad k = 0, 1, 2, \text{ where } m \text{ is the largest factor of } 24 \text{ that divides } n, \text{ so } 8k \text{ is the remainder term.} \]

An even unimodular lattice Λ is extremal if for the shortest nonzero vector \( x \in Λ, \sqrt{⟨x, x⟩} = 2m + 2 \), according to [1]. Extremal lattices are significant because of the ideal ratio to the norm of the shortest vector and the dimension.

Every lattice has an associated theta series. The theta series \( Θ_Λ(z) \) of a lattice Λ is a function of the complex variable \( z \) restricted to the upper half plane, defined as:

\[ Θ_Λ(z) = \sum_{x ∈ Λ} q^{|x|^2}, \quad q = e^{iπz}, \quad Im(z) > 0. \quad (1.13) \]

The series converges absolutely for \( Im(z) > 0 \) and uniformly for \( Im(z) ≥ y_0 > 0 \) for any fixed \( y_0 \). Also, when \( z \) is restricted to the positive \( y \)-axis, so \( z = iy, \ y > 0 \), then \( Θ_Λ(iy) \) is a summation of real powers of \( e \), so no term is negative. In [3], Oggier and Belfiore define a secrecy function \( Ξ_Λ(y) \) as

\[ Ξ_Λ(y) = \frac{Θ_Σ^n(iy)}{Θ_Λ(iy)}, \quad y > 0. \quad (1.14) \]

They define the maximum value of the secrecy function as the secrecy gain and study methods to obtain it.

The following three functions, known as the Jacobi theta functions, are particularly useful while studying lattices:

\[ \vartheta_2(z) = \sum_{n=−∞}^{∞} q^{(n+\frac{1}{2})^2}, \]

\[ \vartheta_3(z) = \sum_{n=−∞}^{∞} q^{n^2}, \]

\[ \vartheta_4(z) = \sum_{n=−∞}^{∞} (-q)^{n^2}. \]

Note that in all of the above definitions, \( q = e^{iπz}, \ Im(z) > 0 \), as before. These
functions can also be written with product representation, as follows:

\[ \vartheta_2(z) = q^{1/4} \prod_{n=1}^{\infty} (1 - q^{2n})(1 + q^{2n})(1 + q^{2n-2}), \]

\[ \vartheta_3(z) = \prod_{n=1}^{\infty} (1 - q^{2n})(1 + q^{2n-1})^2, \]

\[ \vartheta_4(z) = \prod_{n=1}^{\infty} (1 - q^{2n})(1 - q^{2n-1})^2. \]

These functions will be very useful in our later discussions. It will also be useful to know that for the standard lattice \( \mathbb{Z}^n \),

\[ \Theta_{\mathbb{Z}^n}(z) = \vartheta_3^n(z). \quad (1.15) \]

### 1.3 Coset Coding

Oggier and Belfiore, and later Oggier, Sole and Belfiore demonstrate the usefulness of the coset encoding system of lattices in [3] and [5]. Recall that Alice intends to submit confidential information to Bob through a discrete memoryless channel with negligible noise, while Eve is listening in through a rather noisy wiretap channel. Let \( \sigma_B^2 \) be Bob’s noise variance and \( \sigma_E^2 \) be Eve’s. Because Bob’s channel has much less noise, we can assume that \( \sigma_B^2 \ll \sigma_E^2 \). Consider a binary code of length \( n \) and dimension \( k \) that Alice wants to transmit to Bob. A binary code of length \( n \) can be thought of an \( n \)-dimensional vector with components in \( \mathbb{F}_2 \). The dimension \( k \) of a code \( C \), which will be explained in more depth in the next chapter, is the number of basis vectors spanning the code. Alice will use two lattices, one embedded in the other, to transmit her message. Alice chooses lattices \( \Lambda_b \), where \( b \) stands for Bob, and she chooses \( \Lambda_e \), where \( e \) stands for Eve, such that \( \Lambda_e \subset \Lambda_b \), and \( |\Lambda_b/\Lambda_e| = 2^k \). Now we will see in the next chapter that \( |C| = 2^k \), so the number of codewords is now in 1 to 1 correspondence with the number of cosets in \( \Lambda_b/\Lambda_e \). Each coset looks like \( \Lambda_e + c \), where \( c \) is a codeword in \( C \). She therefore translates her codeword into a lattice point using an injective mapping between the \( C \) and the cosets. However, her codeword now translates to an entire coset, not just one lattice point. Therefore, to create confusion, she can now choose any lattice point in that coset. Therefore, she selects at random a point \( x \) in the coset to represent her word and transmits \( x \), or equivalently \( r + c \), for suitable \( r \in \Lambda_e \), to Bob. The lattice \( \Lambda_b \) is chosen so that Bob, using classical techniques for low noise channels, decodes his received messages with relative ease. Eve has much more difficulty decoding the word.

Before moving forward, the definition of the Voronoi cell of a lattice \( \Lambda \) will be
useful. For each lattice point \( p_i \) of a lattice \( \Lambda \), the Voronoi cell, denoted \( \mathcal{V}(p_i) \), is defined as

\[
\mathcal{V}(p_i) = \{ x \in \mathbb{R}^n \mid d(x, p_i) < d(x, p_j) \forall j \},
\]

(1.16)

where \( d(x, y) \) is the standard Euclidean metric. Given any lattice, the Voronoi cell for each point will be the same shape, so it is often easier to speak of the Voronoi cell of a lattice than the cell of a point. We denote the Voronoi cell of a lattice by \( \mathcal{V}(\Lambda) \).

Now given a point \((x_n)\) that has been sent to the recipient, the probability that it is correctly decoded is the probability that \((\hat{x}_n)\) falls into the Voronoi cell of that point. In the case of coset coding, it is the probability that it falls into the union of the Voronoi cells of all points in the coset \( \Lambda_c + c \). This probability of correct decision by the recipient is given by

\[
P_{c,b} = \frac{1}{(\sigma_b \sqrt{2\pi})^n} \sum_{r \in \Lambda_e} \int_{\mathcal{V}(\Lambda) + r} e^{-||u||^2/2\sigma_b^2} du.
\]

(1.17)

Much of the mathematics behind this calculation rely on arguments from probability theory that will not be introduced in this paper.

Now Eve’s probability of correct decision is modeled by

\[
P_{c,e} = \frac{1}{(\sigma_e \sqrt{2\pi})^n} \sum_{r \in \Lambda_e} \int_{\mathcal{V}(\Lambda_e) + r} e^{-||u||^2/2\sigma_e^2} du.
\]

(1.18)

Notice that we can now integrate around \( \mathcal{V}(\Lambda_e) + r \), because all codewords are transmitted from \( \Lambda_b \), and we can equivalently talk about the Voronoi cell of a lattice point or its whole lattice. Considering similar probability of correct decoding for Bob and after further calculation, which can be seen in [3] and [5], we arrive at

\[
\frac{P_{c,e}}{P_{c,b}} = \left( \frac{\sigma_b}{\sigma_e} \right)^n \frac{\operatorname{Vol}(\mathcal{V}(\Lambda_b))}{\operatorname{Vol}(\mathcal{V}(\Lambda_e))} \frac{\sum_{r \in \Lambda_e} e^{-||r||^2/2\sigma_e^2}}{\int_{\mathcal{V}(\Lambda_b)} e^{-||u||^2/2\sigma_b^2} du}.
\]

(1.19)

where \( \operatorname{Vol}(\mathcal{V}(\Lambda_b)) \) is the volume of the Voronoi cell of \( \Lambda_b \), as defined earlier.

Now given that we can hold \( \Lambda_b \) fixed, the task at hand is to find a lattice \( \Lambda_e \subseteq \Lambda_b \) for which Eve’s probability of correct decryption is minimal, that is, for which

\[
\sum_{r \in \Lambda_e} e^{-||r||^2/2\sigma_e^2}
\]

(1.20)

is minimal under the constraint \(|\Lambda_b/\Lambda_e| = 2^k\).
We see that we can rewrite \( \sum_{r \in \Lambda_c} e^{-\|r\|^2/2\sigma_c^2} \) as
\[
\sum_{r \in \Lambda_c} e^{-\|r\|^2/2\sigma_c^2} = \sum_{r \in \Lambda_c} \left( e^{-1/2\sigma_c^2} \right) \|r\|^2 \\
= \sum_{r \in \Lambda_c} \left( e^{i\pi/2} \right) \|r\|^2 \\
= \Theta_{\Lambda_c}(z), \text{ at the point } z = \frac{-1}{2i\pi\sigma_c^2}
\]
where \( \Theta_{\Lambda}(z) \) is the theta series of a lattice \( \Lambda \), \( q = e^{i\pi z} \), and
\[
Im \left( \frac{-1}{2i\pi\sigma_c^2} \right) = Im \left( \frac{i}{2\pi\sigma_c^2} \right) > 0. \tag{1.21}
\]
Therefore, minimizing Eve’s probability of correct decoding is equivalent to minimizing \( \Theta_{\Lambda_c}(z) \) at the point \( z = i/2\pi\sigma_c^2 \). We will do this by setting \( y = iz \) and restricting \( y \) to \( y > 0 \). Our goal now is to minimize
\[
\Theta_{\Lambda_c}(iy) = \sum_{r \in \Lambda_c} q^{\|r\|^2}, \quad q = e^{-\pi y}, \quad y > 0, \tag{1.22}
\]
at the point \( y = \frac{1}{2\pi\sigma_c^2} \), among all lattices \( \Lambda_c \subseteq \Lambda_b \) with the constraint \( |\Lambda_b/\Lambda_c| = 2^k \).

It is convenient to normalize the quantity \( \Theta_{\Lambda_c}(y) \) that we seek to minimize by dividing it into the corresponding quantity for the standard cubic lattice \( \mathbb{Z}^n \). Accordingly, we obtain the following definition:

**Definition 1** Let \( \Lambda \) be an \( n \)-dimensional lattice. Then the secrecy function of \( \Lambda \) is defined by
\[
\Xi_{\Lambda}(y) = \frac{\Theta_{\mathbb{Z}^n}(iy)}{\Theta_{\Lambda}(iy)} = \frac{\vartheta^n_3(iy)}{\vartheta_3(iy)} \tag{1.23}
\]
for \( y > 0 \).

It is for this reason, so as to minimize Eve’s probability of correct decryption, that our goal is to find the maximum value of the secrecy function at \( y = \frac{1}{2\pi\sigma_c^2} \), among all lattices \( \Lambda_c \subseteq \Lambda_b \) with the constraint \( |\Lambda_b/\Lambda_c| = 2^k \). This is the motivation behind the work done in [1], [3], [5], and [6].

### 1.4 The Belfiore-Solé Conjecture

The secrecy function, originally studied only at the value \( y = \frac{1}{2\pi\sigma_c^2} \), is now an item of independent interest, worth studying for its own sake. In [3], Oggier and Belfiore consider the secrecy functions for certain lattices and determine, as previously stated,
that minimizing the probability of correct decryption at the eavesdropper’s end is related to maximizing the secrecy function, or determining the secrecy gain. In [5], Belfiore and Solé further study the significance of the secrecy function and develop the following conjecture, which is central to our thesis:

**Conjecture 1 (Belfiore-Solé Conjecture)** The secrecy function of a unimodular lattice obtains its maximum at \( y = 1 \).

Belfiore and Solé conjecture that all unimodular lattices satisfy the Belfiore-Solé conjecture. This is quite an undertaking to prove, though many strides have been made in doing so. In [1], Ernvall-Hytönen shows that all known even extremal unimodular lattices satisfy the Belfiore-Solé conjecture. In [6], Lin and Oggier, using the techniques of [1], further show that the conjecture holds for all lattices of dimension up to 23. However, both of these classes of lattices each contain only a finite number of lattices, so until now, only a finite number of lattices have been known to satisfy the conjecture. We will further expand the class of unimodular lattices satisfying the conjecture. We will prove later in this thesis that the following classes of unimodular lattices satisfy the Belfiore-Solé conjecture:

1. The orthogonal finite direct sum of certain lattices that individually satisfy the Belfiore-Solé conjecture. This opens up the class of lattices satisfying the conjecture to infinitely many lattices.

2. All unimodular lattices from doubly even self-dual codes up to length 40. This further expands the number of lattices satisfying this conjecture.
Chapter 2

Codes

A binary linear code \( C \) of length \( n \) is an \( \mathbb{F}_2 \) subspace the vector space \( \mathbb{F}_2^n \). That is, a binary code of length \( n \) consists of length \( n \) arrays of elements in \( \{0,1\} \). Every codeword in a binary code of length \( n \) is a vector in \( \mathbb{F}_2^n \). In this paper, every code \( C \) will be considered to be binary and linear. Therefore, in this paper, for all codes \( C \),

\[
c_1 + c_2 \in C, \quad \forall \ c_1, c_2 \in C, \tag{2.1}
\]

where addition of two codewords is just binary vector addition. A code of length \( n \) and dimension \( k \) can be considered as the image of an \( \mathbb{F}_2 \)-linear injective map

\[
g : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n, \quad n > k. \tag{2.2}
\]

Every code \( C \) of length \( n \) and dimension \( k \) has a \( k \times n \) generator matrix \( G \), where

\[
G = \begin{pmatrix}
a_{11} & a_{12} & \ldots & a_{1n} \\
a_{21} & a_{22} & \ldots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{k1} & a_{k2} & \ldots & a_{kn}
\end{pmatrix}, \tag{2.3}
\]

where \( a_{ij} \in \mathbb{F}_2 \) for all \( i = 1, \ldots, n, \ j = 1, \ldots, k \). Multiplication of \( G \) with any vector \( x \in \mathbb{F}_2^k \) produces a code word in \( C \). Because there are \( 2^k \) vectors in \( x \in \mathbb{F}_2^k \), there are \( 2^k \) vectors that can multiply with \( G \) to produce a code word in \( C \). It is for this reason that if \( C \) is of dimension \( k \), then \( |C| = 2^k \).

**Example 1** [11, Chap. 2] The generator matrix

\[
G = \begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 1
\end{pmatrix}, \tag{2.4}
\]

generates a 2-dimensional code of length 3. There are \( 2^2 = 4 \) elements of \( \mathbb{F}_2^2 \); these are \( \{00, 01, 10, 11\} \). Multiplication of these vectors respectively with \( G \) produces the code \( C = \{000, 011, 110, 101\} \), and \( |C| = 2^2 = 4 \).

The following definitions pertaining to codes will be useful to the reader:

1. The weight of a codeword is the number of 1s in the codeword. For instance, the codeword \((011000)\) has weight 2.
2. The minimum distance, $d$, of a code is equal to the smallest weight of any nonzero codeword in the code. A code is denoted as an $[n, k, d]$ code, where $n$ is the code’s length, $k$ is the dimension, and $d$ is the minimum distance.

3. The dual $C^\perp$ of a $[n, k, d]$ code $C$ is defined as

$$C^\perp = \{ x \in \mathbb{F}_2^n \mid x \cdot y = 0 \ \forall \ y \in C \}. \quad (2.5)$$

The dimension of $C^\perp$ is $n - k$. This is because $C^\perp$ is essentially the null space of $C$, so if $C$ is a $k$-dimensional subspace of an $n$-dimensional space, then its null space, or $C^\perp$ in this case, has dimension $n - k$.

4. A code $C$ is called self-dual if $C = C^\perp$. Notice that when this is the case, $k = \frac{n}{2}$. Therefore, the length of all self-dual codes is divisible by 2, and a self-dual code $C$ is an $[n, \frac{n}{2}, d]$ code. In a self-dual code $C$, $c_1 \cdot c_2 = 0$ for any $c_1$ and $c_2$ in $C$.

5. The all-zero vector $(00\ldots0)$ is in $C$ by linearity. Note that every code word $c$ in a self-dual code $C$ must have even weight. Otherwise, $c \cdot c = 1$, which is a contradiction to the duality of $C$.

6. The all-one vector $(11\ldots1)$ is in a self-dual code $C$ as well. To see this, assume it is not. Then there exists a $c \in C$ such that $(11\ldots1) \cdot c = 1$. Then if $(11\ldots1) \cdot c = 1$, this must mean that $c$ has odd weight, which is a contradiction because $C$ is a self-dual code. Therefore, $(11\ldots1) \in C$.

7. A code $C$ is called even if all of its codewords have weight divisible by 2. $C$ is called doubly even if the weights of all of the codewords in $C$ are divisible by 4. Otherwise, $C$ is called singly even. Because all self-dual codes have length and weight divisible by 2, all self-dual codes can be classified as either singly even or doubly even. Doubly even self-dual codes exist only in lengths divisible by 8. The proof is similar to why even unimodular lattices exist only in dimension 8 (and pertains to the relationship between lattices and codes, which will be discussed below), and this once again can be further explored in [4].

Every binary, self-dual code $C$ of length $n$ has an associated weight enumerator polynomial $W_C(x, y)$, defined as

$$W_C(x, y) = x^n + W_2 x^{n-2} y^2 + W_4 x^{n-4} y^4 + \ldots + W_{n-2} x^2 y^{n-2} + y^n, \quad (2.6)$$

where $W_j$ equals the number of codewords of weight $j$. The $x^n$ term has coefficient 1 because there is only one codeword of weight 0, namely $(00\ldots0)$. Similarly, $y^n$ has coefficient 1 because there is only one codeword of weight $n$, namely $(11\ldots1)$. 
Also, $W_j = W_{n-j}$. This is because $(11\ldots1) \in C$, so by linearity, for any code word $c \in C$, the code word with all 0s replaced by 1s and vice versa are in $C$ as well. For example, if $(11000011) \in C$, then because $(11111111) \in C$, $(11000011)+(11111111) = (00111100) \in C$. Therefore, for any $c \in C$ with weight $j$, there is a code word $c' \in C$ with weight $n - j$. Notice that $W_j = 0$ for all $j$ odd, because the weights of all codewords in a binary-self dual code are divisible by 2. Notice also that for all doubly even self-dual codes, $W_j = 0$ for all $j \neq 0 \mod 4$. Therefore, for all doubly even self-dual codes,

$$W_C(x, y) = x^n + W_4x^{n-4}y^4 + W_8x^{n-8}y^8 + \ldots + W_{n-4}x^4y^{n-4} + y^n. \quad (2.7)$$

Additionally, there is a significant relationship between codes of length $n$ and lattices in $\mathbb{R}^n$, and every binary code can be translated into a lattice using a method called Construction A [4, Chp. 7], which works as follows:

Consider an $[n, k, d]$ binary code $C$. Recall that $C$ is the image of a bijective map $h : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n$. Now consider the lattice $\mathbb{Z}^n \subseteq \mathbb{R}^n$, and reduce it mod 2:

$$\rho : \mathbb{Z}^n \mapsto (\mathbb{Z}/2\mathbb{Z})^n = \{0, 1\}^n. \quad (2.8)$$

Then the lattice $\Lambda_C$ is defined to be

$$\Lambda_C = \frac{1}{\sqrt{2}}\rho^{-1}(C) = \bigcup_{c_i \in C} \frac{1}{\sqrt{2}}(2\mathbb{Z}^n + c_i). \quad (2.9)$$

The dimension of $\Lambda_C$ is also $n$. By this construction, singly even self-dual codes give rise to unimodular odd lattices, and doubly even self-dual codes give rise to unimodular even lattices.

The following are two useful properties regarding the relationship between a code $C$ and its corresponding lattice $\Lambda_C$ [2, Chp. 1]:

1. $C$ is a self-dual code if and only if $\Lambda_C$ is a unimodular lattice.
2. $C$ is a doubly even code if and only if $\Lambda_C$ is an even lattice.

This second property follows from examining the relationship between the theta series of a lattice and the weight enumerator polynomial of its corresponding code. Given the close connection between a code and its corresponding lattice, it follows that their theta series and weight enumerator polynomials are related as well. In fact, the transformation of a weight enumerator polynomial of a code $C$ into the theta series of its corresponding lattice $\Lambda_C$ is given below [4, Chp. 7]:

$$11$$
Lemma 1 Let $C$ be a linear code, with weight enumerator $W_C(x, y)$. Then the theta series of its corresponding lattice $\Lambda_C$ is given by

$$\Theta_{\Lambda_C} = W_C(\vartheta_3(2z), \vartheta_2(2z)), \quad (2.10)$$

where $\vartheta_2$ and $\vartheta_3$ are Jacobi theta functions, as defined in section 1.2.
Chapter 3

Infinitely Many Lattices Satisfy the Belfiore-Solé Conjecture

In this chapter, we prove a central result of our thesis, which is that infinitely many lattices satisfy the Belfiore-Solé conjecture. We begin by reviewing Ernvall-Hytönen’s framework for the analysis of the secrecy function of a unimodular lattice, which she employs in [1] to show that even, extremal, unimodular lattices satisfy the Belfiore-Solé conjecture. We then use this framework to define a class of unimodular latices; the definition ensures that the members of this class satisfy the Belfiore-Solé conjecture as well. We also show that this class is closed under taking direct sums, from which our central result immediately follows.

3.1 Ernvall-Hytönen’s Framework for Studying Belfiore-Solé Conjecture for Unimodular Lattices

In [1], Ernvall-Hytönen observes that the theta series of any even unimodular lattice

\[
\Theta_{\Lambda} = E_4^{3m+k} \sum_{j=1}^{m} b_j E_4^{3(m-j)+k} \Delta^j,
\]

where \(E_4 = \frac{1}{2} (\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8)\); \(\Delta = \frac{1}{256} \vartheta_2^8 \vartheta_3^8 \vartheta_4^8\); \(\vartheta_2^8, \vartheta_3^8, \vartheta_4^8\) are the Jacobi theta functions defined earlier; and the value of each \(b_j\) is determined by each lattice. Also, as mentioned earlier,

\[
\Theta_{\mathbb{Z}^n} = \vartheta_3^n, \forall \ n. \tag{3.2}
\]

Therefore, the secrecy function of even unimodular \(\Lambda\) of dimension \(n\) can be written as

\[
\Xi_{\Lambda} = \frac{\Theta_{\mathbb{Z}^n}}{\Theta_{\Lambda}} = \frac{\vartheta_3^n}{E_4^{3m+k} \sum_{j=1}^{m} b_j E_4^{3(m-j)+k} \Delta^j}, \tag{3.3}
\]

which becomes, after substitution of \(E_4\) and \(\Delta\) and minor calculations,

\[
\left(1 - \frac{\vartheta_2^8 \vartheta_4^8}{\vartheta_3^8} \right)^{3m+k} + \sum_{j=1}^{m} \frac{b_j}{256} \left(1 - \frac{\vartheta_2^8 \vartheta_4^8}{\vartheta_3^8} \right)^{3(m-j)+k} \cdot \left(\frac{\vartheta_2^8 \vartheta_4^8}{\vartheta_3^8}\right)^{2j} \right)^{-1}. \tag{3.4}
\]

Therefore, the secrecy function of any even unimodular lattice can be written as a function of the variable \(\zeta = \frac{\vartheta_2^8 \vartheta_4^8}{\vartheta_3^8}\).

Ernvall-Hytönen then shows that the same can be done for unimodular lattices in general. Unimodular lattices in general exist in all dimensions \(n\), which can always be expressed as \(n = 8\mu + \nu\), where \(0 \leq \nu < 7\). Given any unimodular lattice \(\Lambda\) of
dimension $n$, the theta series $\Theta_{\Lambda}$ can be expressed as

$$\Theta_{\Lambda} = \sum_{r=0}^{\mu} a_r \vartheta_3^{-n+8r} \Delta_8^r,$$  \hspace{1cm} (3.5)

where $\Delta_8 = \frac{1}{16} \vartheta_2^4 \vartheta_4^4$ and the value of $a_r$ is determined by the lattice. The secrecy function can then be written as

$$\Xi_{\Lambda} = \frac{\Theta_{Z^n}}{\Theta_{\Lambda}} = \left( \sum_{r=0}^{\mu} \frac{a_r \vartheta_2^4 \vartheta_4^4}{16^r \vartheta_3^8} \right)^{-1},$$  \hspace{1cm} (3.6)

so by the same process as done above, it can be shown that the theta series, now of any unimodular lattice, can be written in terms of a function of the variable $\zeta = \frac{\vartheta_2^4 \vartheta_4^4}{\vartheta_3^8}$.

Next, Ernvall-Hytönen shows that the function $\zeta(y) = \frac{\vartheta_2^4(y) \vartheta_4^4(y)}{\vartheta_3^8(y)}$ has symmetry; that is, $\zeta(y) = \zeta \left( \frac{1}{y} \right)$. Similarly, if we consider

$$\phi(y) = \sqrt{\zeta(y)} = \frac{\vartheta_2(iy) \vartheta_4(iy)}{\vartheta_3^2(iy)},$$  \hspace{1cm} (3.7)

then Ernvall-Hytönen’s proof shows the following:

**Lemma 2 ([1, Lemma 3])** The function

$$\phi(y) = \frac{\vartheta_2(iy) \vartheta_4(iy)}{\vartheta_3^2(iy)}$$  \hspace{1cm} (3.8)

has symmetry; that is,

$$\phi(y) = \phi \left( \frac{1}{y} \right).$$  \hspace{1cm} (3.9)

**Proof.** We employ the following Jacobian identities, which are also found in [4, Chp. 4]:

$$\vartheta_2 \left( \frac{i}{y} \right) = \sqrt{y} \vartheta_4(iy)$$  \hspace{1cm} (3.10)

$$\vartheta_3 \left( \frac{i}{y} \right) = \sqrt{y} \vartheta_3(iy)$$  \hspace{1cm} (3.11)

$$\vartheta_4 \left( \frac{i}{y} \right) = \sqrt{y} \vartheta_2(iy).$$  \hspace{1cm} (3.12)
Substituting the above identities yields

$$\phi(y) = \frac{\varphi_2(iy) \varphi_4(iy)}{\varphi_3^2(iy)} = \frac{y^{-\frac{1}{2}} \varphi_4 \left(\frac{i}{y}\right) y^{-\frac{1}{2}} \varphi_2 \left(\frac{i}{y}\right)}{y^{-1} \varphi_3^2 \left(\frac{i}{y}\right)} = \frac{\varphi_2 \left(\frac{i}{y}\right) \varphi_4 \left(\frac{i}{y}\right)}{\varphi_3^2 \left(\frac{i}{y}\right)} = \phi \left(\frac{1}{y}\right).$$ (3.13)

Therefore $\phi(y)$ is a symmetric function.

Ernvall-Hytönen then proves the following lemma:

**Lemma 3** ([1, Lemma 4]) For all $y \in \mathbb{R}^+$, the function

$$\zeta(y) = \frac{\varphi_2^4(iy) \varphi_4^4(iy)}{\varphi_3^8(iy)}$$ (3.14)

attains its maximum value at $y = 1$, and this maximum value is $\frac{1}{4}$.

We will fill in additional steps to Ernvall-Hytönen’s method of proof for clarity. To highlight the place where we introduce our own argument, we will divide the proof into several steps. Before proving the result, however, we provide three product identities that will help us in the proof and are also found in [1]:

$$\prod_{n=1}^{\infty} (1 + g^{2n}) = 2 \prod_{n=1}^{\infty} (1 + g^{2n})^4,$$ (3.15)

$$\prod_{n=1}^{\infty} (1 - g^{2n-1})^{-4} = \left( \prod_{n=1}^{\infty} (1 + g^{2n}) \right)^4 \left( \prod_{n=1}^{\infty} (1 - g^{2n-1}) \right)^4,$$ (3.16)

$$\prod_{n=1}^{\infty} (1 + (-g)^n) = \prod_{n=1}^{\infty} (1 + g^{2n}) \prod_{n=1}^{\infty} (1 - g^{2n-1}).$$ (3.17)

**Proof.**

**Step 1** ([1]): We write $\phi(y)$ in product representation:

Once again, we will examine

$$\phi(y) = \sqrt{\zeta(y)} = \frac{\varphi_2(iy) \varphi_4(iy)}{\varphi_3^2(iy)},$$ (3.18)

and then relate it to $\zeta(y) = \frac{\varphi_2^4(iy) \varphi_4^4(iy)}{\varphi_3^8(iy)}$. Substituting in product representations for
the Jacobi theta functions yields
\[
\frac{\vartheta_2(iy)\vartheta_4(iy)}{\vartheta_3^2(iy)} = \frac{(g^{1/4} \prod_{n=1}^{\infty} (1 - g^{2n})(1 + g^{2n})(1 + g^{2n-2})) (\prod_{n=1}^{\infty} (1 - g^{2n})(1 + g^{2n-1})^2)}{(\prod_{n=1}^{\infty} (1 - g^{2n})(1 - g^{2n-1})^2)^2},
\]
(3.19)
where we let \( g = e^{-\pi y} \). This is because when evaluating at \( z = yi \),
\[
q = e^{\pi iz} = e^{ni(y)} = e^{\pi i^2 y} = e^{-\pi y}.
\]

Simplifying yields
\[
\frac{(g^{1/4} \prod_{n=1}^{\infty} (1 + g^{2n})(1 + g^{2n-2})) (\prod_{n=1}^{\infty} (1 + g^{2n-1})^2)}{(\prod_{n=1}^{\infty} (1 - g^{2n-1})^2)^2} = g^{1/4} \left( \prod_{n=1}^{\infty} (1 + g^{2n})(1 + g^{2n-2}) \right)^2 \left( \prod_{n=1}^{\infty} (1 + g^{2n-1})^2 \right) \left( \prod_{n=1}^{\infty} (1 - g^{2n-1})^{-4} \right).
\]

Then, substituting in identities 3.15 and 3.16 yields
\[
\frac{\vartheta_2(iy)\vartheta_4(iy)}{\vartheta_3^2(iy)} = 2g^{1/4} \left( \prod_{n=1}^{\infty} (1 + g^{2n})^2 \right) \left( \prod_{n=1}^{\infty} (1 - g^{2n-1})^2 \right) \left( \prod_{n=1}^{\infty} (1 + g^{2n}) \right)^2 \left( \prod_{n=1}^{\infty} (1 - g^{2n-1}) \right)^4
\]
\[
= 2g^{1/4} \left( \prod_{n=1}^{\infty} (1 + g^{2n}) \right)^6 \left( \prod_{n=1}^{\infty} (1 - g^{2n-1}) \right)^6
\]

Using identity 3.17 helps us to finally obtain
\[
\phi(y) = \frac{\vartheta_2(iy)\vartheta_4(iy)}{\vartheta_3^2(iy)} = 2 \left( g^{1/24} \prod_{n=1}^{\infty} (1 + (-g)^n) \right)^6.
\]
(3.21)

**Step 2 ([1]):** We show that \( \frac{d\phi}{dy} = 0 \) when \( y = 1 \):

Recall that \( \phi(y) \) has symmetry, so \( \phi(y) = \phi \left( \frac{1}{y} \right) \). Therefore, by differentiating both sides of this equation, we obtain
\[
\frac{d\phi}{dy} \bigg|_y = -\left( \frac{d\phi}{dy} \right) \bigg|_{\frac{1}{y}} \left( \frac{1}{y^2} \right).
\]
(3.22)
We now observe the behavior of \( \frac{d\phi}{dy} \) when \( y = 1, y > 1, \) and \( y < 1. \) When \( y = 1, \)
\[
\frac{d\phi}{dy} = -\frac{d\phi}{dy}, \tag{3.23}
\]
which only occurs if \( \frac{d\phi}{dy} = 0. \) Therefore, \( y = 1 \) is a critical point of \( \phi. \) We will then show that \( \frac{d\phi}{dy} \) is positive on \( y \in (0,1) \) and negative on \( y \in (1,\infty), \) which will prove that \( y = 1 \) is the only critical value, and a maximum, so \( \phi \) obtains its unique maximum at \( y = 1. \) We will then relate this to \( \zeta(y) \) to see that it obtains its maximum at \( y = 1 \) as well. Also, we notice from Equation 3.22 that for all \( y \neq 1, \) the derivatives at \( y \) and of \( \frac{1}{y} \) have opposite signs. This will be instrumental later in our proof.

**Step 3 ([1]):** We relate \( \frac{d\phi}{dy} \) to \( \frac{d\phi}{dg}. \) It is at this point that we depart slightly from Ernvall-Hytönen’s proof so we can fill in additional details:

Our goal is to show that the first derivative has no additional zeroes and is decreasing on the interval \( y \in (1,\infty), \) or increasing on \( g \in (0,e^{-\pi}) \) (note that when \( y \to \infty, g \to 0, \) and when \( y \to 1, g \to e^{-\pi}, \) so \( y \in (1,\infty) \leftrightarrow g \in (0,e^{-\pi}). \) First, considering the change of variables from \( g \) to \( y, \) we notice that the derivative of \( \phi \) can be written as
\[
\frac{d\phi}{dy} = \left( \frac{d\phi}{dg} \right) \left( \frac{dg}{dy} \right), \tag{3.24}
\]
where
\[
\frac{dg}{dy} = \frac{d(e^{-\pi y})}{dy} = -\pi e^{-\pi y}, \tag{3.25}
\]
so
\[
\frac{d\phi}{dy} = \left( \frac{d\phi}{dg} \right) (-\pi e^{-\pi y}). \tag{3.26}
\]

Now, to show that \( \frac{d\phi}{dy} \bigg| \bigg|_{y} < 0 \forall y \in (1,\infty), \) and considering equation 3.28, it is sufficient to show that \( \frac{d\phi}{dg} > 0 \) for all \( g \in (0,e^{-\pi}). \) This is because \(-\pi e^{-\pi y} \) is negative for all \( y > 0, \) so \( \frac{d\phi}{dg} \) will clearly be negative if \( \frac{d\phi}{dg} \) is positive. Additionally, when \( y = 1, g = e^{-\pi}, \) so \( \frac{d\phi}{dg} = 0 \) at \( g = e^{-\pi}. \)

**Step 4:** We return to Ernvall-Hytönen’s method of proof and show that the derivative of \( \phi \) can be written as the product of two terms, one of which is always positive:
We differentiate $\phi$ with respect to $g$. We obtain

$$
\frac{d}{dg} \left( g^{1/24} \prod_{n=1}^{\infty} (1 + (-g)^n) \right) = \left( g^{1/24} \prod_{n=1}^{\infty} (1 + (-g)^n) \right) \left( \frac{1}{24g} + \sum_{n=1}^{\infty} \frac{n(-1)^ng^{n-1}}{1 + (-g)^n} \right).
$$

(3.29)

Let us denote the first term of the derivative, $g^{1/24} \prod_{n=1}^{\infty} (1 + (-g)^n)$, as $A$. We notice that $A$ is always positive, because $g^{1/24}$ is just real powers of $e$ and is therefore always positive. Similarly, $(1 + (-g)^n)$ is always positive because $(-g)^n < 1$ for all $n$ and for all $g \in (1, \infty)$. Therefore, because $A$ is always positive, it is sufficient to analyze the second part, $\frac{1}{24g} + \sum_{n=1}^{\infty} \frac{n(-1)^ng^{n-1}}{1 + (-g)^n}$. We will call this second term $B$. When $g = e^{-\pi}$, we notice that $B$ must be zero (because $A$ is strictly nonzero, and $\frac{d\phi}{dg} = AB = 0$ at $g = e^{-\pi}$).

**Step 5 ([1]):** We show $\frac{dB}{dg} < 0$ for $g \in (0, e^{-\pi})$. This will show that $B$ is decreasing on $g \in (0, e^{-\pi})$, all the way down to $g = e^{-\pi}$, where $B = 0$. If $B$ decreases along an interval and finally terminates at $B = 0$, this implies that $B$ must be positive on the entire interval. By this argument, $B$ will be positive on $g \in (0, e^{-\pi})$, and $A$ is already positive on this interval, so $\frac{d\phi}{dg} = AB > 0$ on $g \in (0, e^{-\pi})$:

Differentiating $B$, we obtain

$$
\frac{dB}{dg} = \frac{d}{dg} \left( \frac{1}{24g} + \sum_{n=1}^{\infty} \frac{n(-1)^ng^{n-1}}{1 + (-g)^n} \right)
= -\frac{1}{24g^2} + \sum_{n=1}^{\infty} \left( \frac{n(n-1)(-1)^ng^{n-2}}{1 + (-g)^n} - \frac{n^2g^{2(n-1)}}{(1 + (-g)^n)^2} \right).
$$

(3.30)

(3.31)

To show that the derivative of $B$ is negative for $g \in (0, e^{-\pi})$, we will consider the terms of the summation pairwise and show that each pair is negative. First we show that $-\frac{1}{24g^2}$ outside of the summation, along with the terms $n = 1$ and $n = 2$ in the summation, are negative. These three terms have sum

$$
-\frac{1}{24g^2} - \frac{1}{(1-g)^2} + \frac{2 - 2g^2}{(1+g^2)^2} = \frac{-73g^6 + 98g^5 - 51g^4 - 92g^3 + 21g^2 + 2g - 1}{24g^2(1-g)^2(1+g^2)^2}.
$$

(3.32)

The denominator of this function is positive for all values of $g$ in our interval. The numerator is negative for all positive values of $g$, so it is negative on $g \in (0, e^{-\pi})$ (the numerator does have to real roots, but these occur for negative values of $g$, and we are only concerned with the behavior of $g > 0$).

We now consider two terms, an odd term and its subsequent even term (therefore, we will show the third and fourth term, fifth and sixth term, and so on, are negative).
For any odd $n > 2$, the sum of odd $n$ and even $n + 1$ is

\[
\begin{align*}
\frac{n(n-1)g^{n-2}}{1-g^n} - \frac{n^2g^{2(n-1)}}{(1-g^n)^2} + \frac{n(n+1)g^{n-1}}{1+g^{n+1}} - \frac{(n+1)^2g^{2n}}{(1+g^{n+1})^2} &= g^{n-2}n\left(-\frac{n-1}{1-g^n} - \frac{ng^n}{(1-g^n)^2} + \frac{(n+1)g}{1+g^{n+1}} - \frac{n^{-1}(n+1)^2g^{n+2}}{(1+g^{n+1})^2}\right) \\
&< g^{n-2}n\left(-\frac{n-1}{1-g^n} - \frac{ng^n}{(1-g^n)^2} + \frac{(n+1)g}{1+g^{n+1}} - \frac{(n+1)^2g^{n+2}}{(1+g^{n+1})^2}\right) ,
\end{align*}
\]

because $-\frac{(n+1)^2}{n} < -(n+1)$

\[
\begin{align*}
&= g^{n-2}n\left(-\frac{n-1+g^n}{(1-g^n)^2} + \frac{(n+1)g}{(1+g^{n+1})^2}\right) \\
&< g^{n-2}n\left(-\frac{n-1+g^n}{(1+g^{n+1})^2} + \frac{(n+1)g}{(1+g^{n+1})^2}\right) \\
&= g^{n-2}n\left(-\frac{(n-1)-g^n+(n+1)g}{(1+g^{n+1})^2}\right) < 0 \\
\leftrightarrow & \quad -(n-1) - g^n + (n+1)g < 0 \\
\leftrightarrow & \quad g(n+1) < (n-1) + g^n
\end{align*}
\]

Now

\[
(n-1) < (n-1) + g^n \quad \forall n, \quad (3.33)
\]

and

\[
g(n+1) < (n+1)e^{-\pi} < \frac{n+1}{10} < n-1 \\
\leftrightarrow & \quad n + 1 < 10n - 10 \leftrightarrow 11 < 9n \leftrightarrow 2 \leq n,
\]

for all integers $n$. Therefore the derivative of $B$ is negative for all $g \in (0, e^{-\pi})$ terminating at $B = 0$ when $g = e^{-\pi}$, so as mentioned before, $B$ is positive on $g \in (0, e^{-\pi})$, and $AB = \frac{d\phi}{dy} > 0$ on $g \in (0, e^{-\pi})$. This must mean that

\[
\frac{d\phi}{dy} < 0 \quad (3.34)
\]

for all $y \in (1, \infty)$.

**Step 6 ([1]):** We now use symmetry of the functions to show that $\frac{d\phi}{dy} > 0$ for all $y \in (0, 1)$:
To show that \( \phi \) is increasing on \( y \in (0, 1) \), recall that \( \phi \) is symmetric, and

\[
\frac{d\phi}{dy} \bigg|_y = -\left( \frac{d\phi}{dy} \right) \bigg|_{\frac{1}{y}} \left( \frac{1}{y^2} \right).
\] (3.35)

Therefore, the derivative at \( y \) is the negative sign of the derivative of \( \frac{1}{y} \). Thus, if the derivative is negative on \( y \in (1, \infty) \), then it is positive on \( y \in (0, 1) \). Therefore, \( \phi \) is increasing on \( y \in (0, 1) \), so \( \phi(y) \) obtains its unique maximum at \( y = 1 \). Because

\[
\zeta(y) = (\phi(y))^4,
\] (3.36)

this means that \( \zeta(y) \) also obtains its unique maximum at \( y = 1 \).

Now, to show that \( \zeta(1) = \frac{1}{4} \), we use the identities 3.10 and 3.12, along with the following identity:

\[
\vartheta^4_2 + \vartheta^4_4 = \vartheta^8_3.
\] (3.37)

Using these identities at \( y = 1 \) yields

\[
\frac{\vartheta^4_2(i)\vartheta^4_4(i)}{\vartheta^8_3(i)} = \frac{\vartheta^4_4(i)}{\vartheta^8_3(i)} = \frac{\vartheta^4_2(i)\vartheta^4_4(i)}{(\vartheta^4_2(i) + \vartheta^4_4(i))^2} = \frac{\vartheta^8_3(i)}{\vartheta^4_2(i) + 2\vartheta^4_4(i)\vartheta^4_2(i) + \vartheta^8_3(i)} = \frac{\vartheta^8_3(i)}{\vartheta^4_2(i) + 2\vartheta^4_4(i) + \vartheta^8_3(i)} = \frac{1}{4}.
\]

Keep in mind that because \( \zeta = \frac{\vartheta^4_2\vartheta^4_4}{\vartheta^8_3} \) is a square function, its range is nonnegative. Also, because its maximum value is \( \frac{1}{4} \), \( \zeta \) is only defined on the interval \([0, \frac{1}{4}]\).

Ernvall-Hytönen used this framework to prove the following theorem:

**Theorem 1** The secrecy function of all known even, extremal, unimodular lattices obtains its maximum at \( y = 1 \).

Even, extremal, unimodular lattices exist in dimensions \( 8k \), for \( k = 1, \ldots, 10 \), and there are only a finite number of such lattices. In [6], Lin and Oggier use similar framework to prove this following theorem as well:

**Theorem 2** All unimodular lattices up to dimension 23 obtain their maximum at \( y = 1 \).

There are also a finite number of lattices in this class. Therefore, the conjecture has previously only been proven for a finite number of unimodular lattices.
### 3.2 Proof that Infinitely Many Lattices Satisfy the Belfiore-Solé Conjecture

To prove that a secrecy function obtains its maximum at \( y = 1 \), we observe that the secrecy functions for unimodular lattices can be written as \( \Xi_\Lambda(y) = f(\zeta)^{-1} \), for some polynomial \( f \), and for \( \zeta = \frac{\Theta(y)}{\Theta(y)} \). For all lattices that can be written in this way, we observe that because \( \zeta(y) \) takes on values on \([0, \frac{1}{4}]\), it suffices to show that \( f(\zeta) \) is a decreasing function of \( \zeta \in [0, \frac{1}{4}] \). If this happens, then \( f(\zeta)^{-1} \) is increasing on \([0, \frac{1}{4}]\), so it obtains its maximum when \( \zeta = \frac{1}{4} \). Then, because \( \zeta(y) \) has a unique maximum of \( \frac{1}{4} \), which occurs when \( y = 1 \), this will imply that \( \Xi_\Lambda(y) = f(\zeta)^{-1} \) obtains its maximum at \( y = 1 \) as well. This is the motivation behind the following definition of a class of lattices:

**Definition 2** The class \( \mathcal{C} \) consists of all unimodular lattices \( \Lambda \) whose secrecy functions \( \Xi_\Lambda \) can be written as \( \frac{1}{f(\zeta)} \), for some polynomial \( f \) in the variable \( \zeta \), such that \( f'(\zeta) \) is negative on \([0, \frac{1}{4}]\).

Recall that because the secrecy function is a ratio of two theta series, each of which is always positive, a secrecy function is always positive as well. Also notice that all lattices in \( \mathcal{C} \) satisfy the Belfiore-Solé conjecture. Also, the class of lattices that both Ernvall-Hytonen in [1] and Lin and Oggier in [6] proved to satisfy the Belfiore-Solé conjecture also fall into the class \( \mathcal{C} \).

The following is a key result of this thesis:

**Theorem 3** Let \( \Lambda_1, \ldots, \Lambda_n \) be unimodular lattices in the class \( \mathcal{C} \). Then the finite orthogonal direct sum \( \Lambda_1 \oplus \ldots \oplus \Lambda_n \) is also in \( \mathcal{C} \) and thus satisfies the Belfiore-Solé conjecture.

Before proving this result, certain lemmas are required.

**Lemma 4** The finite orthogonal direct sum of integral lattices is integral.

**Proof.** Let \( \Lambda_1, \ldots, \Lambda_n \) be integral lattices. Then \( \langle x, x \rangle \in \mathbb{Z} \) for all \( x \in \Lambda_i \), \( i = 1 \ldots n \). By definition of orthogonal sum, all vectors in \( \Lambda_i \) are orthogonal to all vectors in \( \Lambda_j \), \( i \neq j \). Hence, for \( x_1 + \ldots + x_n \in \Lambda_1 \oplus \ldots \oplus \Lambda_n \),

\[
\langle x_1 + \ldots + x_n, x_1 + \ldots + x_n \rangle = \sum_{i,j=1}^{n} \langle x_i, x_j \rangle = \langle x_1, x_1 \rangle + \ldots + \langle x_n, x_n \rangle,
\]

because \( \langle x_i, x_j \rangle = 0 \) for all \( i \neq j \). Because each \( \langle x_i, x_i \rangle \in \mathbb{Z} \), then \( \langle x_1, x_1 \rangle + \ldots + \langle x_n, x_n \rangle \in \mathbb{Z} \), so \( \langle x_1 + \ldots + x_n, x_1 + \ldots + x_n \rangle \in \mathbb{Z} \), and \( x_1 + \ldots + x_n \) is integral.
Lemma 5 The finite orthogonal direct sum of unimodular lattices is unimodular.

Proof. Let $\Lambda_1, \ldots, \Lambda_n$ be unimodular lattices. By the previous theorem, $\Lambda_1 \oplus \ldots \oplus \Lambda_n \subset (\Lambda_1 \oplus \ldots \oplus \Lambda_n)^\perp$, because recall that for any integral lattice $\Lambda$, $\Lambda \subset \Lambda^\perp$. Therefore, it remains to show that $(\Lambda_1 \oplus \ldots \oplus \Lambda_n)^\perp \subset \Lambda_1 \oplus \ldots \oplus \Lambda_n$. This can be done by induction.

First, let $\Lambda_1$ and $\Lambda_2$ be unimodular lattices of dimension $d_1$ and $d_2$, respectively. Let $((x, y), (z, w)) \in \mathbb{Z} \forall (z, w) = (z_1, \ldots, z_{d_1}, w_1, \ldots, w_{d_2}) \in \Lambda_1 \oplus \Lambda_2$. Then

$$\langle (x, y), (z, w) \rangle \in \mathbb{Z} \forall (z, w) = (z_1, \ldots, z_{d_1}, w_1, \ldots, w_{d_2}) \in \Lambda_1 \oplus \Lambda_2. \quad (3.39)$$

This means that

$$x_1 z_1 + \ldots + x_{d_1} z_{d_1} + y_1 w_1 + \ldots + y_{d_2} w_{d_2} \in \mathbb{Z}, \forall (z, w) \in \Lambda_1 \oplus \Lambda_2. \quad (3.40)$$

Because this is true for all $z \in \Lambda_{d_1}$, let $z = (0, \ldots, 0)$. Then

$$y_1 w_1 + \ldots + y_{d_2} w_{d_2} \in \mathbb{Z}, \forall w_i \in \Lambda_2. \quad (3.41)$$

Then $y \in \Lambda_{d_1} \oplus \Lambda_2$. Similarly, let $w = (0, \ldots, 0)$. Then

$$x_1 z_1 + \ldots + x_{d_1} z_{d_1} \in \mathbb{Z}, \forall z_i \in \Lambda_1. \quad (3.42)$$

Then $x \in \Lambda_{d_1} \oplus \Lambda_2$. Therefore, $x \in \Lambda_1$, $y \in \Lambda_2$, so $(x, y) \in \Lambda_1 \oplus \Lambda_2$. Thus,

$$(\Lambda_1 \oplus \Lambda_2)^\perp \subset \Lambda_1^\perp \oplus \Lambda_2^\perp \subset \Lambda_1 \oplus \Lambda_2, \quad (3.43)$$

so $\Lambda_1 \oplus \Lambda_2$ is unimodular.

The remainder of the proof follows from a simple induction step to show that the finite orthogonal direct sum $\Lambda_1 \oplus \ldots \oplus \Lambda_n$ is unimodular for all unimodular lattices $\Lambda_1, \ldots, \Lambda_n$.

Note: An alternative proof is as follows: Let $b_{i_1}, \ldots, b_{n_i}$ be a $\mathbb{Z}$-basis for $\Lambda_i$. Then, because any vector in $\Lambda_i$ is orthogonal to any vector in $\Lambda_j$, for $i \neq j$, the generator matrix $M$ for $\Lambda = \Lambda_1 \oplus \ldots \oplus \Lambda_n$ is of the form
\[
M = \begin{pmatrix}
M_1 & 0 & \ldots & 0 \\
0 & M_2 & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & M_n
\end{pmatrix},
\]
(3.44)

where each \(M_i\) is the generator matrix for \(\Lambda_i\). Now \(\det(M) = \prod_{i=1}^{n} \det(M_i)\), and \(\det(M_i) = \pm 1 \forall i\), so \(\det(M) = \pm 1\) as well.

**Lemma 6** Let \(\Lambda_1, \ldots, \Lambda_n\) be unimodular lattices. Then
\[
\Theta_{\Lambda_1 \oplus \ldots \oplus \Lambda_n} = \Theta_{\Lambda_1} \cdots \Theta_{\Lambda_n}
\]
(3.45)

**Proof.** We show this for the \(n = 2\) case, and the case for any \(n\) follows by simple induction:

Let \(\Lambda_1\) and \(\Lambda_2\) be unimodular lattices with theta series
\[
\Theta_{\Lambda_1} = \sum_{x \in \Lambda_1} q^{|x|^2} \quad \text{and} \quad \Theta_{\Lambda_2} = \sum_{y \in \Lambda_2} q^{|y|^2},
\]
respectively. Then the theta series for \(\Lambda_1 \oplus \Lambda_2\) is
\[
\Theta_{\Lambda_1 \oplus \Lambda_2} = \sum_{x+y \in \Lambda_1 \oplus \Lambda_2} q^{|x+y|^2} = \sum_{x+y \in \Lambda_1 \oplus \Lambda_2} q^{\langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle},
\]
where \(\langle x, y \rangle\) and \(\langle y, x \rangle = 0\) because \(\Lambda_1\) and \(\Lambda_2\) are orthogonal, so
\[
= \sum_{x+y \in \Lambda_1 \oplus \Lambda_2} q^{\langle x, x \rangle} q^{\langle y, y \rangle} = \sum_{x \in \Lambda_1} q^{\langle x, x \rangle} \sum_{y \in \Lambda_2} q^{\langle y, y \rangle} = \sum_{x \in \Lambda_1} q^{|x|^2} \sum_{y \in \Lambda_2} q^{|y|^2} = \Theta_{\Lambda_1} \Theta_{\Lambda_2}.
\]
Therefore, \(\Theta_{\Lambda_1 \oplus \Lambda_2} = \Theta_{\Lambda_1} \Theta_{\Lambda_2}\).

**Lemma 7** Let \(\Lambda_1, \ldots, \Lambda_n\) be unimodular lattices. Then
\[
\Xi_{\Lambda_1 \oplus \ldots \oplus \Lambda_n} = \Xi_{\Lambda_1} \cdots \Xi_{\Lambda_n}.
\]
(3.47)

**Proof.** Let \(\Lambda_1, \ldots, \Lambda_n\) be unimodular lattices with respective dimensions \(d_1, \ldots, d_n\) and respective theta series \(\Theta_{\Lambda_1}, \ldots, \Theta_{\Lambda_n}\). Then \(\Lambda_1 \oplus \cdots \oplus \Lambda_n\) has dimension \(d_1 + \cdots + d_n\) and
Now we will complete the proof of Theorem 3.

**Proof.** (Theorem 3:) Let \( \Lambda_1, \ldots, \Lambda_n \) be lattices in the class \( \mathcal{C} \). Then for all \( i = 1, \ldots, n \),

\[
\Xi_{\Lambda_i} = \frac{1}{f_i(\zeta)}, \text{ some function } f_i. \tag{3.49}
\]

Furthermore,

\[
f_i'(\zeta) < 0 \text{ on } \left[0, \frac{1}{4}\right]. \tag{3.50}
\]

Now consider \( \Lambda = \Lambda_1 \oplus \ldots \oplus \Lambda_n \). By our previous lemmas, \( \Lambda \) is unimodular with secrecy function

\[
\Xi_{\Lambda} = \Xi_{\Lambda_1 \oplus \ldots \oplus \Lambda_n} = \Xi_{\Lambda_1} \cdots \Xi_{\Lambda_n} = \frac{1}{f_1(\zeta)} \cdots \frac{1}{f_n(\zeta)} = \frac{1}{f_1(\zeta) \cdots f_n(\zeta)}. \tag{3.51}
\]

Now the derivative of the denominator is

\[
(f_1(\zeta) \cdots f_n(\zeta))' = f_1'(\zeta)f_2(\zeta) \cdots f_n(\zeta) + f_1(\zeta)f_2'(\zeta) \cdots f_n(\zeta) + \ldots + f_1(\zeta)f_2(\zeta) \cdots f_n'(\zeta).
\]

Notice that because \( \Xi_{\Lambda_i} = \frac{1}{f_i(\zeta)} \) and \( \Xi_{\Lambda_i} > 0 \), \( f_i(\zeta) > 0 \) as well. Also notice that because each term

\[
f_1(\zeta) \cdots f_{i-1}(\zeta)f_i'(\zeta)f_{i+1}(\zeta) \cdots f_n(\zeta)
\]

is the product of \( n-1 \) positive functions and 1 negative function, each term is negative. Also, the sum of finite number of negative sums is negative, so \((f_1(\zeta) \cdots f_n(\zeta))'\) is negative on \([0, \frac{1}{4}]\). Therefore, \( f_1(\zeta) \cdots f_n(\zeta) \) is decreasing on \([0, \frac{1}{4}]\), so \( \Xi_{\Lambda_1 \oplus \ldots \oplus \Lambda_n} \) is increasing on this interval and obtains its maximum for \( \zeta = \frac{1}{4} \), which is when \( y = 1 \). Therefore, the finite orthogonal direct sum is also in the class \( \mathcal{C} \) and thus also satisfies the Belfiore-Solé conjecture.

We now come to one of the main theorems of our thesis:

**Theorem 4** Infinitely Many Lattices Satisfy the Belfiore-Solé Conjecture.
\textbf{Proof.} Pick any $\Lambda$ in $\mathcal{C}$, such as one of the extremal even unimodular lattices or any of the unimodular lattices of dimension up to 23. Then, by Theorem 3, $\Lambda^n := \Lambda \oplus \cdots \oplus \Lambda$ ($n$ summands) is also in $\mathcal{C}$ for any $n$, and hence satisfies the Belfiore-Solé conjecture. Thus infinitely many lattices satisfy the Belfiore-Solé conjecture.

$\blacksquare$
Chapter 4

Doubly Even Self-dual Codes up to Length 40 Satisfy the Belfiore-Solé Conjecture

The following section shows that all unimodular lattices that arise via Construction A from doubly even self-dual codes up to length 40 satisfy the Belfiore-Solé conjecture.

Recall that doubly even codes exist only in lengths divisibly by 8. Because Lin and Oggier have already shown that unimodular lattices up to length 23 satisfy the Belfiore-Solé conjecture in [6], it only remains to show that lattices arising from doubly even self-dual codes in lengths 24, 32, and 40 satisfy the conjecture.

Recall that Lemma 1 states that if $C$ is a linear code with weight enumerator polynomial $W_C(x, y)$, then the theta series of its corresponding lattice $\Lambda_C$ is given by

$$\Theta_{\Lambda_C} = W_C(\vartheta_3(2z), \vartheta_2(2z)). \quad (4.1)$$

This lemma and the following lemma, also found in [4, Chp. 7], will help turn the weight enumerator polynomial of a doubly even code into the theta series of its corresponding lattice.

**Lemma 8** If $C$ is a doubly even code, then

$$W_C(x, y) \in \mathbb{C}[\psi_8, \xi_{24}], \quad (4.2)$$

where $\psi_8 = x^8 + 14x^4y^4 + y^8$ and $\xi_{24} = x^4y^4(x^4 - y^4)^4$.

The two maps

$$\psi_8 \mapsto \vartheta_3^8 - \vartheta_2^1\vartheta_4^4 \quad (4.3)$$

and

$$\xi_{24} \mapsto \frac{1}{16} \vartheta_2^8\vartheta_3^8\vartheta_4^8 \quad (4.4)$$

can be determined using Lemma 1 and the following Jacobi identities, found in [4, Chap. 4]:

$$\vartheta_3^2(z) + \vartheta_4^1(z) = 2\vartheta_3^2(2z) \quad (4.5)$$

$$\vartheta_3^2(z) - \vartheta_4^1(z) = 2\vartheta_2^1(2z) \quad (4.6)$$

$$\vartheta_2^4(z) + \vartheta_4^1(z) = \vartheta_3^4(z). \quad (4.7)$$

$\psi_8$: Because $\psi_8 = x^8 + 14x^4y^4 + y^8$, which is actually the weight enumerator polynomial for the doubly even self-dual code $E_8$, we can apply Lemma 1 to $\psi_8$, which
transforms to
\[ \psi^8_3(2z) + 14\psi^4_3(2z)\psi^4_2(2z) + \psi^8_2(2z) \] (4.8)

Using equations 4.5 and 4.6, this becomes
\[
\left( \frac{1}{2} \psi^2_3(z) + \frac{1}{2} \psi^2_2(z) \right)^4 + 14 \left( \frac{1}{2} \psi^2_3(z) + \frac{1}{2} \psi^2_2(z) \right)^2 \left( \frac{1}{2} \psi^2_3(z) - \frac{1}{2} \psi^2_2(z) \right)^2 + \left( \frac{1}{2} \psi^2_3(z) - \frac{1}{2} \psi^2_2(z) \right)^4
\]
\[ = \psi^8_3(z) + \psi^4_3(z) - \psi^4_2(z) \psi^4_1(z) \]
\[ = \psi^8_3(z) + \psi^4_3(z) [ \psi^4_1(z) - \psi^3_3(z) ] \]
\[ = \psi^8_3(z) - \psi^4_2(z) \psi^4_1(z), \]
where the final line is obtained from equation 4.7.

\( \xi_{24} \): Because \( \xi_{24} = x^4 y^4 (x^4 - y^4)^4 \), which is equivalent to the weight enumerator polynomial of the linear binary code \( G_{24} \), called the Golay code, \( \xi_{24} \) we can apply Lemma 1 to transform \( \xi_{24} \) as follows:
\[
\xi_{24} = [ \psi^4_3(2z) \psi^4_2(2z) ] [ \psi^4_3(2z) - \psi^4_2(2z) ]^4
\]
\[ = \left( \frac{1}{2} \psi^2_3(z) + \frac{1}{2} \psi^2_2(z) \right)^2 \left( \frac{1}{2} \psi^2_3(z) - \frac{1}{2} \psi^2_2(z) \right)^2 \left( \frac{1}{2} \psi^2_3(z) + \frac{1}{2} \psi^2_2(z) \right)^2 - \left( \frac{1}{2} \psi^2_3(z) - \frac{1}{2} \psi^2_2(z) \right)^4
\]
\[ = \frac{1}{16} \psi^8_3(z) \psi^8_2(z) [ \psi^4_3(z) - \psi^4_1(z) ]^2
\]
\[ = \frac{1}{16} \psi^8_2(z) \psi^8_3(z) \psi^8_2(z). \]

These maps and lemmas will now help to show that all binary self-dual codes of each length satisfy the Belfiore-Solé conjecture. Interestingly, we will see that determining the secrecy functions, and therefore whether or not a code satisfies the Belfiore-Solé conjecture, depends only upon the number of code words of weight 4 for codes of length 24, 32, and 40.

### 4.1 Length 24

Binary doubly even self-dual codes of length 24 have weight enumerator polynomials of the form
\[
W_{C_{24}}(x, y) = x^{24} + W_4 x^{20} y^4 + W_8 x^{16} y^8 + W_{12} x^{12} y^{12} + \ldots + y^{24}, \tag{4.9}
\]
where \( W_i \) denotes the number of code words of weight \( i \), and where \( W_i = W_{24-i} \). Also, \( W_{C_{24}} \) is a homogeneous polynomial of degree 24 that can be written in terms of \( \psi_8 \) and \( \xi_{24} \), where \( \psi_8 \) is a homogeneous polynomial of degree 8 and \( \xi_{24} \) is a homogeneous polynomial of degree 24. Therefore, it will have terms of \( \psi_8^3 \) and \( \xi_{24} \). It cannot, for
instance, have a term of $\psi_8^2$ because $\psi_8^2$ is a homogeneous polynomial of degree 16. Therefore, it will only have the two terms, so by Lemma 8,

$$W_{C_{24}}(x, y) = a_0 \psi^3_8 + a_1 \xi_{24}$$

$$= a_0(x^8 + 14x^4y^4 + y^8) + a_1x^4y^4(x^4 - y^4)$$

$$= a_0(x^{24} + 42x^{20}y^4 + 591x^{16}y^8 + \ldots + y^{24}) + a_1(x^{20}y^4 - 4x^{16}y^8 + \ldots + x^4y^{20})$$

$$= a_0x^{24} + (42a_0 + a_1)x^{20}y^4 + \ldots$$

By comparing the two forms of $W_{C_{24}}(x, y)$, it is easy to see that $a_0$ is 1. (This, in fact, will always be the case for $W_{C_n}(x, y)$, of any length $n = 8k$. This is because $W_{C_{8k}}$ will always have first term $x^{8k}$ with coefficient 1, so comparing the two forms of the weight enumerator polynomial will yield $a_0 = 1$, for all $k$.)

Therefore, knowing that $a_0 = 1$, we determine that

$$W_{C_{24}}(x, y) = x^{24} + (42 + a_1)x^{20}y^4 + \ldots$$

We also know from equation 5.1 that

$$W_{C_{24}}(x, y) = x^{24} + W_4x^{20}y^4 + \ldots$$

Comparing the two equations, we see that $42 + a_1 = W_4$, so $a_1 = W_4 - 42$. Therefore, all doubly even self-dual codes of length 24 can be written as

$$W_{C_{24}}(x, y) = \psi^3_8 + (W_4 - 42)\xi_{24}, \quad (4.10)$$

which, using the maps from equations 4.3 and 4.4 above, can be translated to theta series

$$\Theta_{\Lambda_{C_{24}}} = (\varphi^8_3 - \varphi^4_2)^3 + (W_4 - 42)\frac{1}{16}\varphi^8_2\varphi^8_3\varphi^8_4$$

$$= \varphi^{24}_3 - 3\varphi^{16}_3\varphi^4_2 + \frac{W_4 + 6}{16}\varphi^8_2\varphi^8_3\varphi^8_4 - \varphi^{12}_2\varphi^{12}_4.$$ 

Because the theta series for $\mathbb{Z}^{24}$ is $\varphi^{24}_3$, the corresponding secrecy function for a lattice
obtained from a doubly even self-dual code of length 24 is

$$
\Xi_{C_{24}} = \frac{\varphi_{24}^{3}}{\Theta_{\Lambda_{C_{24}}}} = \left[ \frac{\varphi_{3}^{24} - 3\varphi_{3}^{16}\varphi_{4}^{4} + \frac{W_{4} + 6}{16}\varphi_{3}^{8}\varphi_{4}^{8} - \varphi_{2}^{12}\varphi_{4}^{12}}{\varphi_{3}^{24}} \right]^{-1}
= \left[ 1 - 3\zeta + \frac{6 + W_{4}}{16}\zeta^2 - \zeta^3 \right]^{-1}
= \left[ \left( 1 - 3\zeta + \frac{3}{8}\zeta^2 - \zeta^3 \right) + W_{4}\left( \frac{1}{16}\zeta^2 \right) \right]^{-1}
= \left[ f_{24}(\zeta) \right]^{-1},
$$

where, as before, \( \zeta = \frac{\varphi_{4}^{3}}{\varphi_{3}^{3}} \). As before, we want to show \( f_{24}'(\zeta) \) is negative for \( \zeta \in [0, \frac{1}{4}] \), which shows that \( \Xi_{C_{24}} \) is increasing on that interval and obtains its maximum at \( \zeta = \frac{1}{4} \), which, as before, is equivalent to \( y = 1 \). Differentiating \( f_{24} \) yields

$$
f_{24}'(\zeta) = -3 + \frac{3}{4}\zeta - 3\zeta^2 + W_{4}\left( \frac{1}{8}\zeta \right). \quad (4.11)
$$

If we think of this equation as a function of \( W_{4} \), then it is linear in \( W_{4} \). By [6] and [7], \( W_{4} \) ranges from 0 to 66 in doubly even self-dual codes of length 24 (see Table 5.1 in the Appendix). Therefore, if we can show that \( f_{24}'(\zeta) < 0 \) for both \( W_{4} = 0 \) and for \( W_{4} = 66 \), then by linearity, it is negative for all possible values of \( W_{4} \). When \( W_{4} = 0 \), \( f_{24}'(\zeta) = -3 + \frac{3}{4}\zeta - 3\zeta^2 \), which, by completing the square, equals

$$
-3 \left( \zeta - \frac{1}{8} \right)^2 - \frac{189}{64} < 0, \quad \text{for all } \zeta. \quad (4.12)
$$

When \( W_{4} = 66 \), the derivative is

$$
-3 + \frac{3}{4}\zeta - 3\zeta^2 + 66\left( \frac{1}{8}\zeta \right)
= -3\zeta^2 + 9\zeta - 3
= -3 \left( \zeta - \frac{3}{2} \right)^2 + \frac{15}{4},
$$

which is the function of a concave-down parabola. Its smaller zero is at \( \zeta = \frac{3}{2} - \frac{\sqrt{5}}{2} \), so \( f_{24}' \) is negative for all \( \zeta < \frac{3}{2} - \frac{\sqrt{5}}{2} \). Now, because \( \zeta < \frac{3}{2} - \frac{\sqrt{5}}{2} \) for all \( \zeta \in [0, \frac{1}{4}] \), \( f_{24}'(\zeta) \) is negative for all \( \zeta \in [0, \frac{1}{4}] \). Therefore, for all \( W_{4} \in [0, 66] \), \( f_{24}'(\zeta) \) is negative for all \( \zeta \in [0, \frac{1}{4}] \). Thus the secrecy function is increasing on this interval and attains its maximum at \( y = 1 \). Therefore, all lattices arising from doubly even self-dual codes of length 24 satisfy the Belfiore-Solé conjecture.
4.2 Length 32

Binary doubly even self-dual codes of length 32 have the form

\[ W_{C_{32}}(x, y) = x^{32} + W_4 x^{28} y^4 + W_8 x^{24} y^8 + \ldots + y^{32}. \] (4.13)

Additionally, because \( W_{C_{32}} \) is a homogeneous polynomial of degree 32, and because it can be written in terms of \( \psi_8 \) and \( \xi_{24} \), it will have terms of \( \psi_8^4 \) and \( \psi_8 \xi_{24} \). Therefore, recalling that \( \psi_8^4 \) has coefficient 1, and by Lemma 8,

\[
W_{C_{32}}(x, y) = \psi_8^4 + a_1 \psi_8 \xi_{24} \\
= (x^8 + 14x^4 y^4 + y^8)^4 + a_1 (x^8 + 14x^4 y^4 + y^8) (x^4 y^4 (x^4 - y^4)^4) \\
= (x^{32} + 56x^{28} y^4 + 1180x^{24} y^8 \ldots + y^{32}) + a_1 (x^{28} y^4 + 10x^{24} y^8 \ldots + x^4 y^{28}) \\
= x^{32} + (56 + a_1)x^{28} y^4 + \ldots
\]

Comparing the two equations of the weight enumerator polynomial shows that \( 56 + a_1 = W_4 \), so \( a_1 = W_4 - 56 \). Therefore, all doubly even self-dual codes of length 32 can be written as

\[ W_{C_{32}}(x, y) = \psi_8^4 + (W_4 - 56) \psi_8 \xi_{24}, \] (4.14)

which can be translated to a lattice with theta series

\[
\Theta_{\Lambda_{C_{32}}} = (\psi_3^8 - \varphi_2^4 \varphi_4^4)^4 + (W_4 - 56) (\psi_3^8 - \varphi_2^4 \varphi_4^4) \left( \frac{1}{16} \varphi_3^8 \varphi_2^8 \varphi_4^8 \right) \\
= \psi_3^{32} - 4\psi_3^{24} \varphi_2^4 \varphi_4^4 + \frac{5}{2} \psi_3^{16} \varphi_2^8 \varphi_4^8 - \frac{1}{2} \varphi_3^8 \varphi_2^{12} \varphi_4^{12} + \varphi_2^{16} \varphi_4^{16} \\
+ W_4 \left( \frac{1}{16} \psi_3^{16} \varphi_2^8 \varphi_4^8 - \frac{1}{16} \varphi_3^8 \varphi_2^{12} \varphi_4^{12} \right).
\]

The corresponding secrecy function for a lattice obtained from a doubly even self-dual code of length 32 is

\[
\Xi_{C_{32}} = \left[ 1 - 4\zeta + \frac{5}{2} \zeta^2 - \frac{1}{2} \zeta^3 + \zeta^4 + W_4 \left( \frac{1}{16} \zeta^2 - \frac{1}{16} \zeta^3 \right) \right]^{-1} = [f_{32}(\zeta)]^{-1}. \] (4.15)

Differentiating \([f_{32}(\zeta)]\) yields

\[
[f'_{32}(\zeta)] = \left( -4 + 5\zeta - \frac{3}{2} \zeta^2 + 4\zeta^3 \right) + W_4 \left( \frac{1}{8} \zeta - \frac{3}{16} \zeta^2 \right). \] (4.16)

Again, \( f'_{32} \) is a linear function in \( W_4 \). Also, by [8], \( W_4 \) ranges from 0 to 120 in doubly even self-dual codes of length 32 (see Table 5.2 in the Appendix). Similar calculations, as were done in the previous section, can show that \( f'_{32}(\zeta) < 0 \), both
when $W_4 = 0$, and when $W_4 = 120$. Therefore, $f'_{42}(\zeta) < 0$ for all $W_4 \in [0, 120]$. Thus the secrecy function is increasing on this interval and attains its maximum at $y = 1$. Therefore, all lattices arising from doubly even self-dual codes of length 32 also satisfy the Belfiore-Solé conjecture.

4.3 Length 40

Binary doubly even self-dual codes of length 40 have the form

$$W_{C_{40}}(x, y) = x^{40} + W_4 x^{36} y^4 + W_8 x^{32} y^8 + \ldots + y^{40}. \quad (4.17)$$

Additionally, because $W_{C_{40}}$ is a homogeneous polynomial of degree 40, and because it can be written in terms of $\psi_8$ and $\xi_{24}$, it will have terms of $\psi_8^5$ and $\psi_8^2 \xi_{24}$. Therefore, by Lemma 8,

$$W_{C_{40}}(x, y) = \psi_8^5 + W_4 \psi_8^2 \xi_{24}$$

Comparing the two equations for the weight enumerator polynomial determines that $a_1 = W_4 - 70$. Therefore, all doubly even self-dual codes of length 40 can be written as

$$W_{C_{40}}(x, y) = \psi_8^5 + (W_4 - 70) \psi_8^2 \xi_{24}, \quad (4.18)$$

which can be translated to a lattice with theta series

$$\Theta_{\Lambda_{C_{40}}} = (\psi_3^3 - \psi_2^4)\psi_4^5 + (W_4 - 70) (\psi_3^5 - \psi_2^4)\psi_4^2 \left( \frac{1}{16} \psi_2^8 \psi_3^8 \psi_4^8 \right)$$

$$= \psi_4^{40} - 5\psi_3^{32} \psi_2^4 \psi_4^4 + \frac{45}{8} \psi_3^{24} \psi_2^8 \psi_4^8 - \frac{5}{4} \psi_3^{16} \psi_2^{12} \psi_4^{12} + \frac{5}{8} \psi_3^8 \psi_2^{16} \psi_4^{16} - \psi_2^{20} \psi_4^{20}$$

$$+ W_4 \left( \frac{1}{16} \psi_3^{24} \psi_2^8 \psi_4^8 - \frac{1}{8} \psi_3^{16} \psi_2^{12} \psi_4^{12} + \frac{1}{16} \psi_3^8 \psi_2^{16} \psi_4^{16} \right).$$

The corresponding secrecy function for this lattice obtained from the doubly even self-dual code of length 40 is

$$\Xi_{C_{40}} = \left[ \left( 1 - 5\zeta + \frac{45}{8} \zeta^2 - \frac{5}{4} \zeta^3 + 5 \zeta^4 - \zeta^5 \right) + W_4 \left( \frac{1}{8} \zeta - \frac{3}{8} \zeta^2 + \frac{1}{4} \zeta^3 \right) \right]^{-1} = [f'_{40}(\zeta)]^{-1}.$$
$W_4 \in [0, 190]$. Thus the secrecy function is increasing on this interval and attains its maximum at $y = 1$. Therefore, all lattices arising from doubly even self-dual codes of length 40 satisfy the Belfiore-Solé conjecture as well.

Therefore, we have now shown that all lattices arising from doubly even codes up to length 40 fall into class $C$ and therefore satisfy the Belfiore-Solé conjecture. These lattices also help to expand that class of lattices satisfying the Belfiore-Solé conjecture, further suggesting that the Belfiore-Solé conjecture may hold for all unimodular lattices.
Chapter 5

Appendix

Tables for Binary Self-dual Codes in Lengths 24, 32, and 40

Binary Doubly Even Self-dual Codes of Length 24 and Number of Codes of Weight 4

<table>
<thead>
<tr>
<th>$W_4$</th>
<th># Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
</tr>
<tr>
<td>42</td>
<td>2</td>
</tr>
<tr>
<td>66</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 5.1: There are 9 inequivalent binary doubly even self-dual codes of length 24, as listed above [7]. The complete weight enumerator polynomials for these codes can also be found in [7].

Binary Doubly Even Self-dual Codes of Length 32 and Number of Codes of Weight 4

<table>
<thead>
<tr>
<th>$W_4$</th>
<th># Codes</th>
<th>$W_4$</th>
<th># Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>26</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>28</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>29</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>30</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>32</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>36</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>44</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>50</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>5</td>
<td>56</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>60</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>80</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>120</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.2: There are 85 inequivalent binary doubly even self-dual codes of length 32, as listed above [8]. The complete weight enumerator polynomials for these codes can also be found in [7].
Table 5.3: There are 94343 inequivalent binary doubly even self-dual codes of length 40, as listed above [9]. A formula for calculating the complete weight enumerator polynomial using $W_4$ can also be found in [9].
Bibliography


