Results on the Secrecy Function Conjecture on the Theta Function of Lattices

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

by

Beverly Hernandez

May 2016
The thesis of Beverly Hernandez is approved:

Dr. Daniel J Katz  Date

Dr. Katherine Stevenson  Date

Dr. Bharath A Sethuraman, Chair  Date
Acknowledgments

I would first like to express my sincere gratitude to my thesis advisor, Professor B.A. Sethuraman, whose patience and guidance helped my growth and completion of this thesis. I am grateful to the National Science Foundation for their support under Professor Sethuraman’s grant CIF 1318260.

I would also like to thank Professors Daniel Katz and Katherine Stevenson for their time and involvement in my thesis. Their encouragement and support as both mentors and faculty have impacted my education to a truly gratifying experience.

Finally, I would like to thank my fiancé for his endless company and support.
Dedications

I dedicate this thesis to my family, friends, and my fiancé who have always supported and encouraged my pursuit for a higher education.
# Table of Contents

Signature Page ............................... ii  
Acknowledgements ........................... iii  
Dedications ................................ iv  
Abstract ................................... vii  

1 Introduction ................................ 1  
1.1 Background ................................ 1  
1.2 Wire Tap Codes ............................ 1  
1.3 Approach ................................ 2  
1.4 Summary ................................ 4  

2 Lattices .................................... 6  
2.1 Lattices ................................ 6  
2.2 Theta Functions ......................... 12  

3 Codes ...................................... 15  
3.1 Codes ................................ 15  
3.2 Weight Enumerator ....................... 18  
3.3 Construction A ........................... 19  

4 Coset Coding ............................... 24  
4.1 Coset Coding ............................ 24  
4.2 The Belfiore-Sóle Conjecture .......... 27  

5 Classification of Binary Self-Dual Codes of Highest Minimal Distance 28  

6 The Belfiore-Sóle Conjecture for Lattices from Maximal Self Dual Codes of Length Up To 72  
6.1 More Preliminaries ....................... 30  
6.2 Singly even code of length 24 satisfies the Belfiore-Sóle Conjecture .......... 33  
6.3 Wolfram Mathematica ................... 35  

7 A Conjecture for $\ell$ -modular Lattices 43  
7.1 $\ell$ -modular lattices ................... 43  
7.2 Leading to a modified Conjecture .......... 44  
7.3 New functions k,l, and M .................. 45  

8 $C^{(8)}$ satisfies the $\ell$ -modular secrecy function conjecture 46
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Introducing a conjecture for a certain ratio of theta functions</td>
<td>53</td>
</tr>
<tr>
<td>9.1</td>
<td>Further examples satisfying the ℓ-modular conjecture</td>
<td>56</td>
</tr>
</tbody>
</table>

References | 59 |

Appendix | 61 |
| A.1 | Results For Doubly Even Codes | 61 |
| A.1.1 | Doubly Even Code of length n=48 and minimal distance d=12 | 61 |
| A.1.2 | Doubly Even Code of length n=56 and minimal distance d=12 | 62 |
| A.1.3 | Doubly Even Code of length n=64 and minimal distance d=12 | 63 |
| A.2 | Results For Singly Even Codes | 65 |
| A.2.1 | Singly Even Code of length n=24 and minimal distance d=6 | 65 |
| A.2.2 | Singly Even Code of length n=32 and minimal distance d=8 | 66 |
| A.2.3 | Singly Even Code of length n=40 and minimal distance d=8 | 67 |
| A.2.4 | Singly Even Code of length n=48 and minimal distance d=10 | 70 |
| A.2.5 | Singly Even Code of length n=56 and minimal distance d=12 | 73 |
| A.2.6 | Singly Even Code of length n=64 and minimal distance d=12 | 77 |
| A.2.7 | Singly Even Code of length n=72 and minimal distance d=14 | 78 |
| A.3 | Wolfram Mathematica Code | 85 |
| A.3.1 | Type II | 85 |
| A.3.2 | Type I | 87 |
Abstract

Results on the Secrecy Function Conjecture on the Theta Function of Lattices

By
Beverly Hernandez
Master of Science in Mathematics

This thesis concerns lattice-based communication in a wiretap channel. The Belfiore and Solé secrecy function conjecture, which states that the inverse normalized theta series of a unimodular lattice, when evaluated on the positive $y$-axis, attains its maximum at $y = 1$, is an open problem in this area. We investigate this conjecture for unimodular lattices that arise from self-dual codes over $\mathbb{F}_2$ meeting a certain bound on their minimal distance, verifying it numerically for all such unimodular lattices of dimension up to 72. We also investigate the $\ell$-modular secrecy function conjecture of Ernvall-Hytönen and Sethuraman, and prove that the 8-modular lattice $C^{(8)}$ verifies the conjecture. We then make a key conjecture regarding a certain ratio of theta series that if true, will show that all lattices $C^{(\ell)}$ where $\ell$ is a positive integer satisfy the secrecy function conjecture. Finally we verify numerically that the $\ell$-modular lattice $C^{(\ell)}$ satisfies the conjecture for many values of $\ell$. 
Chapter 1

Introduction

1.1 Background

Introduced by A.D. Wyner in [1], wiretap codes are transmission schemes for noisy communication channels. In the beginning of Wyner's work, coding theory was at its first stages and reliability of transmission was of more importance than security of the information. In the last 10 years, there has been an increased interest in wiretap communication and their secrecy capacity for different communication channels. This is due to the development of wireless communications, which is very vulnerable to third party listeners. Under the assumption that the wiretapper’s channel is noisier than the receiver, Wyner’s method does not only provide a reliable communication source, but a secure way of transmitting confidential data to the receiver.

1.2 Wire Tap Codes

The wire tap channel is modeled by the transmitter Alice, the receiver Bob, and the wiretapper Eve. Through a discrete memoryless channel, Alice sends a message to Bob. This system is relatively noiseless, and so when Bob decodes the message, there is a high likelihood for correct decryption. At the same time we have Eve listening through a much noisier channel. Our goal is to maximize confusion for Eve in order to protect the message intended only for Bob.

Alice begins with a binary data vector,

\[ s = (s_1, ..., s_k) \]

where \( Pr\{s_i = 0\} = Pr\{s_i = 1\} = \frac{1}{2} \)

and each \( s_i \) is independent from one another. Alice then takes the vector \( s \) of length \( k \) and encodes \( s \) into a binary vector,

\[ x = (x_1, ..., x_n) \]

of length \( n \) where \( k < n \)

When there is noise in the channel, the decoder may not receive the exact vector sent from Alice, that is, error is present and Bob instead receives the following vector,

\[ \hat{x} = x + v_b, \]

where \( v_b \) is the error vector of \( \hat{x} \)

The decoder then takes \( \hat{x} \) and transforms it into the binary data vector,

\[ \hat{s} = s + u_b, \]

where \( u_b \) is the error vector of \( \hat{s} \)

The probability of error for Bob is defined to be the sum of the probability that each element of \( \hat{s} \) and \( s \) is not equal divided by \( k \),

1
\[
P_{e,B} = \frac{1}{k} \sum_{i=1}^{k} Pr\{s_i \neq \hat{s}_i\}.
\]

As Bob decodes the message some redundancy is required in order to facilitate error correction decryption. The transmission rate is defined as \(k/n\), the number of bits transmitted per channel use. The higher the transmission rate the more efficient the use of redundancy. However, this has its downfall since too high a transmission rate can lead to poor error control.

Meanwhile, we have the wiretapper Eve observing the encoded vector \(x\) through the relatively noisy channel. Since there is noise in the channel of the wiretapper, the sequence received by Eve is,

\[
\tilde{x} = x + v_e \text{ where } v_e \text{ is the error vector for Eve.}
\]

Eve then decodes her received vector \(\tilde{x}\) into the binary data vector

\[
\tilde{s} = s + u_e,
\]

where \(u_e\) is the error vector of \(\tilde{s}\). The probability of error for Eve is now defined analogously:

\[
P_{e,E} = \frac{1}{k} \sum_{i=1}^{k} Pr\{s_i \neq \tilde{s}_i\}.
\]

In order to maximize confusion for Eve while providing maximum clarity for Bob, the designer should have:

1. \(P_{e,B}\) as close to zero as possible, so that Bob hears the message clearly.
2. \(k/n\) as large as possible, for efficiency of transmission, and
3. \(P_{e,E}\) as close to one as possible, maximizing confusion for Eve

Throughout this paper our focus will be on maximizing confusion on the wiretappers end with the method known as wiretap coding.

1.3 Approach

Coset encoding as demonstrated in [6] and [9] was an effective tool in achieving confusion for the wiretapper Eve. We consider a Gaussian wiretap channel (the error vectors \(v_b\) and \(v_e\) are assumed to be normally distributed), where the sender Alice sends a message to the receiver Bob, all the while having an eavesdropper Eve listening in though a much noisier channel. The mean for \(v_b\) and \(v_e\) is taken to be zero with variance \(\sigma_b^2\) and \(\sigma_e^2\), respectively. Since Eve’s channel is noisier than Bob’s we can assume that \(\sigma_b^2 \ll \sigma_e^2\). Furthermore, we are under the assumption that Alice knows
\( \sigma_b^2 \) and \( \sigma_e^2 \) ([6] also considers the case when Alice does not know \( \sigma_e^2 \)). This can be illustrated by the figure below (also found in [6])—here, \( \Lambda_b \) and \( \Lambda_e \) are lattices used to send the message; we will explore lattices in Chapter 2 ahead:

![Diagram of the wiretap channel with data bits encoded into \( \Lambda_b \) and \( \Lambda_e \), with Eve intercepting \( \sigma_f^2 \).]

At the time that Wyner introduced the wiretap channel in [1], he provided a generic coding strategy known as coset coding. From this, other specific strategic coding methods were derived, one of which was examined by Belfiore and Oggier. In [8], Belfiore and Oggier pose a design criterion for constructing explicit lattice based codes. Further work by Belfiore, Oggier, and Solé in [6] connected their findings to the secrecy function. In [8], Belfiore and Oggier define the secrecy function of a given lattice \( \Lambda \) for a point \( y > 0 \) as the ratio of the theta function of \( \mathbb{Z}^n \) to the theta function of \( \Lambda \) at the point \( iy \). (Theta functions are explored in detail in Chapter 2.) The secrecy function of a lattice \( \Lambda \) is a measure of how much confusion the lattice presents to the eavesdropper as compared to the standard lattice \( \mathbb{Z}^n \). The work of Belfiore and Oggier resulted in the conjecture known as the Belfiore and Solé Conjecture, which states that:

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

This was further generalized, again by Belfiore, Oggier, and Solé to \( \ell \)-modular lattices, and they conjectured the following, which we will call the Generalized Belfiore and Solé Conjecture:

**The secrecy function of an \( \ell \)-modular lattice obtains its maximum at** \( y = 1/\sqrt{\ell} \).

In [3], Ernvall-Hytonen and Sethuraman showed that the generalized conjecture above is false when \( \ell \neq 1 \). They then modified the definition of the secrecy function for \( \ell \neq 1 \), and proposed a new definition of the secrecy function, which they called the \( \ell \)-modular secrecy function. Their \( \ell \)-modular secrecy function reduces to the original secrecy function of Belfiore, Oggier, and Solé when \( \ell = 1 \), but differs for \( \ell \neq 1 \). They
then proposed the following $\ell$-modular secrecy function conjecture:

The $\ell$-modular secrecy function of an $\ell$-modular lattice obtains its maximum at $y = 1/\sqrt{\ell}$.

(Since the $\ell$-modular secrecy function reduces to the original secrecy function when $\ell = 1$, the $\ell$-modular secrecy function conjecture reduces to the original (unimodular) Belfiore and Solé conjecture when $\ell = 1$.)

In this thesis, we investigate this conjecture for unimodular lattices that arise from self-dual codes over $\mathbb{F}_2$ meeting a certain bound on their minimal distance, verifying it numerically for all such unimodular lattices of dimension up to 72. We also investigate the $\ell$-modular secrecy function conjecture of Ernvall-Hytönen and Sethuraman, and prove that the 8-modular lattice $C^{(8)}$ verifies the conjecture. We then make a key conjecture regarding a certain ratio of theta series that if true, will show that all lattices $C^{(\ell)}$ where $\ell$ is a positive integer satisfy the secrecy function conjecture. Finally we verify numerically that the $\ell$-modular lattice $C^{(\ell)}$ satisfies the conjecture for many values of $\ell$.

1.4 Summary

We will begin our discussion with a brief introduction to lattices. Each lattice has a theta function known as the theta function of the lattice. This is a function of the complex variable $z$, and we give the definition in Chapter 2.

In Chapter 3, we give a brief introduction to codes. Since coset coding entails taking codes and sending them to lattice points, we will give some background of codes as well. For our purposes, we will be looking at self-dual codes. In this chapter we introduce the weight enumerator polynomial of a binary self-dual code, which bears the same relationship to codes as the series representation of theta functions do to lattices.

In chapter 3, we also make the connection between the corresponding weight enumerator polynomial of a self-dual code and the theta series of a unimodular lattice obtained by lifting the code to a sub-lattice of the standard lattice $\mathbb{Z}^n$. This connection allows us to obtain a large family of lattices satisfying the $\ell = 1$ case of the secrecy function conjecture.

In Chapter 5 we introduce Type I and Type II codes for which there are corresponding weight enumerator polynomials. We will consider these codes and list their weight enumerator polynomials which will be useful in Chapter 6. In that chapter we describe the technique we use for verifying the Belfiore and Solé conjecture for unimodular lattices. We describe the features of a symbolic computation program we developed to automate our computation of the secrecy function for lattices con-
structured from self-dual codes. Using this program, we attain more lattices satisfying the conjecture for the unimodular case.

In Chapter 7 we will switch directions and show that the $\ell$-modular secrecy function conjecture is satisfied by the 8-modular lattice $C^{(8)}$. We follow this with a conjecture on a certain ratio of $\theta$ functions, and show that if this conjecture holds true, then the $\ell$-modular secrecy function conjecture will hold for all lattices $C^{(\ell)}$, where $\ell$ is a positive integer.
2.1 Lattices

In this section we define what lattices are and explore special family of lattices. We will only consider full or complete lattices and thus define them as our standard lattice for this paper. Some basic understanding of linear algebra is assumed to be known by the reader. Consider a set of $n$ linearly independent vectors in $\mathbb{R}^n$,

\[
\mathbf{v}_1 = (v_{11}, v_{12}, \ldots v_{1n})
\]

\[
\mathbf{v}_2 = (v_{21}, v_{22}, \ldots v_{2n})
\]

\[\vdots\]

\[
\mathbf{v}_n = (v_{n1}, v_{n2}, \ldots v_{nn})
\]

**Definition 1.** A **full lattice** (or complete lattice) $\Lambda \subseteq \mathbb{R}^n$ is defined to be the subgroup of $\mathbb{R}^n$ generated by a set of $n$ linearly independent vectors such as the $\mathbf{v}_i$ above.

This means that the linear combination

\[
a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \ldots + a_n \mathbf{v}_n \quad \text{where } a_i \in \mathbb{Z}
\]

generates all the points of the lattice $\Lambda$.

**Example 1.** *(Standard Lattice in $\mathbb{R}^2$)* The standard lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$ is illustrated below,
where a basis of the lattice is $v_1 = (1, 0)$ and $v_2 = (0, 1)$

**Example 2. (Cubic Lattice)** The cubic lattice $\mathbb{Z}^3 \subset \mathbb{R}^3$ is illustrated below,

![Cubic Lattice Diagram]

where a basis of the lattice is $v_1 = (1, 0, 0)$, $v_2 = (0, 1, 0)$, $v_3 = (0, 0, 1)$

**Example 3. (Standard Lattice in $\mathbb{R}^n$)** More generally, we may consider the lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$ generated by the standard basis vectors $v_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, $i = 1, \ldots, n$, where for each $i$, the 1 is in the $i$-th slot.

**Example 4. (The Hex Lattice in $\mathbb{R}^2$)** The hex lattice is illustrated below,

![Hex Lattice Diagram]

which is generated by the basis elements $(1, 0)$ and $(-1/2, \sqrt{3}/2)$.

When we consider the matrix of all vectors $v_i$ for $i = 1, \ldots, n$ we have the following,
\[
M = \begin{bmatrix}
v_{11} & v_{12} & \ldots & v_{1n} \\
v_{21} & v_{22} & \ldots & v_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
v_{d1} & v_{d2} & \ldots & v_{dn}
\end{bmatrix}
\]

By [11], we define \( M \) to be the generator matrix of \( \Lambda \) where,
\[
\Lambda = \{ \mathbf{x} | \mathbf{x} = \mathbf{z} M \text{ for } \mathbf{z} \in \mathbb{Z}^n \}.
\]
That is, the set of vectors \( \mathbf{v}_1, \ldots, \mathbf{v}_n \) form a basis for the lattice \( \Lambda \).

**Example 5. (Lattice \( \mathbb{Z}^2 \) and \( \mathbb{Z}^3 \))**

For the standard lattice \( \mathbb{Z}^2 \) we have the generator matrix,

\[
M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

For the cubic lattice \( \mathbb{Z}^3 \) we have the generator matrix,

\[
M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}
\]

It is important to observe that the generator matrix may vary for \( \Lambda \) since there are many ways for obtaining a basis of the lattice \( \Lambda \). Although this is the case, one can uniquely determine the volume of the lattice for any given basis generating that lattice. Before defining the volume of a lattice one more definition is needed.

**Definition 2.** The **Gram matrix** of the lattice \( \Lambda \) determined by the basis \( \mathbf{v}_1, \ldots, \mathbf{v}_n \) is defined to be,

\[
A = MM^T
\]

where \( M^T \) is the transpose of the matrix \( M \).

The \((i,j)^{th}\) entry of \( A \) is the inner product \( \langle \mathbf{v}_i, \mathbf{v}_j \rangle \) defined as,

\[
v_{1i}v_{1j} + v_{2i}v_{2j} + \ldots + v_{ni}v_{nj}
\]

The determinant of \( \Lambda \) is defined to be equal to the determinant of the matrix \( A \),

\[
det \Lambda = det A
\]

**Example 6.**

\[
\det \mathbb{Z}^2 = \det A = \det \left( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) = 1
\]

Since \( M \) is a square matrix we have,
\[ det \ A = (det \ M)^2 \]

**Definition 3.** The volume of the full lattice \( \Lambda \) is defined to be,

\[ Vol(\Lambda) = \sqrt{det \ A} = \sqrt{(det \ M)^2} = |det \ M| \]

The following classes of lattices will be important for the results in this thesis.

1. Integral lattices
2. Even lattices
3. Unimodular lattices
4. \( \ell \)-modular lattices for integers \( \ell > 1 \).

**Definition 4.** A lattice \( \Lambda \subseteq \mathbb{R}^n \) is integral if the following holds,

\[ \langle x, y \rangle \in \mathbb{Z} \]

for all \( x, y \in \Lambda \), where \( \langle x, y \rangle \) is the standard inner product of the two vectors.

**Example 7.** For \( \Lambda \subseteq \mathbb{R}^n \) with basis \( \{v_i\} \), \( i = 1, \ldots, n \), consider lattice elements \( x = \sum_{i=1}^n a_i v_i \) and \( y = \sum_{j=1}^n b_j v_j \), with the \( a_i, b_j \in \mathbb{Z} \). Then the inner product

\[ \langle x, y \rangle = \sum_{i=1}^n \sum_{j=1}^n a_i b_j \langle v_i, v_j \rangle. \]

The expansion of \( \langle x, y \rangle \) above shows that if \( \langle v_i, v_j \rangle \in \mathbb{Z} \) for all \( i, j \), then \( \langle x, y \rangle \in \mathbb{Z} \). Conversely, if \( \langle x, y \rangle \in \mathbb{Z} \) for all \( x, y \in \Lambda \), then taking \( x = v_i \) and \( y = v_j \), \( 1 \leq i, j \leq n \) we find that \( \langle v_i, v_j \rangle \in \mathbb{Z} \). Hence, since the \( (i, j) \)th entry of \( A \) is the inner product \( \langle v_i, v_j \rangle \), we have that, \( \Lambda \) being integral is equivalent to having integer coefficients for the gram matrix \( A \) of \( \Lambda \).

**Definition 5.** A lattice is said to be an even lattice if,

\[ \langle x, x \rangle \in 2\mathbb{Z} \text{ for all } x \in \Lambda, \]

otherwise a lattice is said to be an odd lattice.

**Example 8.**
\( \Lambda = \{ x \in \mathbb{Z}^2 \mid x = (x_1, x_2) \text{ and } x_1, x_2 \text{ are both even or both odd} \} \) is an even lattice. This is easily seen to be a lattice, with basis \((1, 1)\) and \((2, 0)\).

**Proof.** (of Example 8)
Take \( x = (x_1, x_2) \) we have \( \langle x, x \rangle = (x_1)^2 + (x_2)^2 \). We have two cases:
1. $x_1, x_2$ are both even
   $(x_1)^2, (x_2)^2$ would both still be even, and so $(x_1)^2 + (x_2)^2$ would then be even

2. $x_1, x_2$ are both odd
   $(x_1)^2, (x_2)^2$ would both still be odd, however $(x_1)^2 + (x_2)^2$ would be even

In either case, $(x_1)^2 + (x_2)^2$ would be even,

\[\therefore \langle x, x \rangle \in 2\mathbb{Z}\]

and thus $\Lambda$ is an even lattice.

\[\Box\]

**Definition 6.** The dual of lattice $\Lambda \subseteq \mathbb{R}^n$, which is denoted by $\Lambda^\perp$, is,

\[\Lambda^\perp = \{x \in \mathbb{R}^n | \langle x, y \rangle \in \mathbb{Z} \text{ for all } y \in \Lambda\}\]

$\Lambda^\perp$ is indeed a lattice in $\mathbb{R}^n$. If $v_i, i = 1, \ldots, n$ is a basis for $\Lambda$ and $M$ is the generator matrix defined with respect to this basis, take $u_i$ to be $(M^{-1})^T e_i$, where $e_i$ is the standard basis vector for $\mathbb{R}^n$ with 0 in all slots except the $i$-th slot, where there is a 1. Then $\langle v_i, u_j \rangle = \delta_{i,j}$, and it is easy to see that $\Lambda^\perp$ is generated by the $u_j$. Moreover, the generator matrix of $\Lambda^\perp$ with respect to this basis $u_j$ is simply $(M^{-1})^T$. It follows from this last relation that $\det(\Lambda)\det(\Lambda^\perp) = 1$.

Notice that if a lattice $\Lambda$ is integral then $\Lambda \subseteq \Lambda^\perp$ since any 2 elements in $\Lambda$ have inner products in $\mathbb{Z}$.

**Definition 7.** A lattice $\Lambda$ is said to be unimodular if,

\[\Lambda = \Lambda^\perp\]

It is easy to see that a unimodular lattice $\Lambda$ is integral since equality implies inclusion in any direction. Furthermore if $\Lambda$ is unimodular, from the relation $\det (\Lambda)\det (\Lambda^\perp) = 1$ and the fact that $\Lambda = \Lambda^\perp$ we have $|\det (\Lambda)| = 1$. Now, if $\Lambda \subseteq \Lambda' \subseteq \mathbb{R}^n$ are lattices, then it is easy to see that $\det(\Lambda) = \det(\Lambda')|\Lambda'/\Lambda|^2$. Looking at the converse, if $\Lambda$ is integral and $|\det (\Lambda)| = 1$ then, $|\det (\Lambda^\perp)| = 1$ as well, and then, from

\[\det \Lambda = \det (\Lambda^\perp)|\Lambda^\perp/\Lambda|^2\]

we find $\Lambda = \Lambda^\perp$.

Therefore we have that,

A lattice $\Lambda$ is unimodular $\iff$ $\Lambda$ is integral and $|\det (\Lambda)| = 1$

**Theorem 1.**

$\mathbb{Z}^n$ is a unimodular lattice for any natural number $n$
Proof.
Let $\Lambda = \mathbb{Z}^n$. In order to show that a given lattice is unimodular we must show that the lattice is equal to its dual.

$(\Lambda^\perp \subseteq \Lambda)$: Take an arbitrary element $(x_1, \ldots, x_n) \in \Lambda^\perp$. By definition of a dual of a lattice the element $(x_1, \ldots, x_n)$ is in $\mathbb{R}^n$ and thus every $x_i \in \mathbb{R}$. Also by definition of a dual we have the following,

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) \in \mathbb{Z}$$
for all $y_i \in \Lambda$. We can then consider the element $(0, \ldots, 1, \ldots, 0) \in \Lambda$ where $y_i = 1$ and $y_j = 0$ for all $j \neq i$ and get,

$$(x_1, \ldots, x_n) \cdot (0, \ldots, 1, \ldots, 0) = x_i \in \mathbb{Z}$$
since $x_i$ was arbitrary then all $x_i \in \mathbb{Z}$ which implies that, $(x_1, \ldots, x_n) \in \mathbb{Z}^n = \Lambda$. Therefore $\Lambda^\perp \subseteq \Lambda$.

$(\Lambda \subseteq \Lambda^\perp)$: Take $(y_1, \ldots, y_n) \in \Lambda = \mathbb{Z}^n$ and consider the following,

$$(y_1, \ldots, y_n) \cdot (z_1, \ldots, z_n) = y_1z_1 + \ldots y_nz_n$$
for $(z_1, \ldots, z_n) \in \Lambda$.

By closure in $\mathbb{Z}$ it follows that $y_1z_1 + \ldots y_nz_n \in \mathbb{Z}$, and so by definition $(y_1, \ldots, y_n) \in \Lambda^\perp$. Therefore $\Lambda \subseteq \Lambda^\perp$. $\blacksquare$

Example 9. An example of a non-unimodular lattice.

Let $\Lambda = \mathbb{Z} \oplus 2\mathbb{Z}$

- To show that $\Lambda$ is a lattice:
  Consider the linearly independent vectors $v_1 = (1, 0)$ and $v_2 = (0, 2)$ in $\mathbb{R}^2$. An arbitrary element in $\Lambda$ looks like $(n, 2m)$ where $n, m \in \mathbb{Z}$. This can be written as the linear combination,

$$n(1, 0) + m(0, 2) = (n, 2m).$$

On the other hand by taking any linear combination of these two vectors with any two elements $a, b \in \mathbb{Z}$ gives us,

$$a(1, 0) + b(0, 2) = (a, 2b) \in \Lambda.$$

Therefore, $\Lambda$ is the set $\{a_1v_1 + a_2v_2 | a_1, a_2 \in \mathbb{Z}\}$ and is hence a lattice.

- To show that $\Lambda$ is integral:
  Take two arbitrary elements $(a, 2b)$ and $(c, 2d)$ in $\Lambda$. By considering their dot product we get,

$$(a, 2b) \cdot (c, 2d) = ac + 4bd,$$
which is in \( \mathbb{Z} \) by closure of \( \mathbb{Z} \) and so, \( \Lambda \) is integral.

- To show that \( \Lambda \) is a not unimodular:

  If we consider \((x, y) \in \mathbb{Z} \oplus \mathbb{Z} \subseteq \mathbb{R}^2\), we have that for any \((a, 2b) \in \Lambda\),

  \[
  (x, y) \cdot (a, 2b) = ax + 2by \in \mathbb{Z}
  \]

  which implies that \( \mathbb{Z} \oplus \mathbb{Z} \in \Lambda^\perp \). But if we take the element \((1, 1) \in \mathbb{Z} \oplus \mathbb{Z}\) we notice that this element cannot be generated by the linear combination of \((1, 0)\) and \((0, 2)\) and thus cannot be in \( \Lambda \).

  \[\therefore \Lambda^\perp \not\subseteq \Lambda\]

  which implies that \( \Lambda \) is not unimodular.

Later in Chapter 7 we will consider \( \ell \)-modular lattices for integers \( \ell \geq 1 \). We will see that unimodular lattices are precisely those for which \( \ell = 1 \), and that this example above is actually a 4 modular lattice.

We state without proof the following deep and classical theorem, see [11]:

**Fact 1** Every even unimodular lattice with dimension \( n \) satisfies the following,

\[ n \equiv 0 \mod 8 \]

### 2.2 Theta Functions

The secrecy function of a lattice \( \Lambda \) is defined in terms of its theta function, which we will discuss in this section. The theta function of a lattice is a function of the complex variable \( z \) defined via the following series representation (see [11]):

\[
\Theta_\Lambda(z) = \sum_{x \in \Lambda} q^{||x||}
\]

where \( q = e^{\pi iz} \), \( \text{Im}(z) > 0 \), and \( ||x|| \) is the squared norm of the vector \( x \). The series representation above is known as the theta series of the lattice. \( \Theta_\Lambda(z) \) converges absolutely for \( \text{Im}(z) > 0 \) and uniformly on the set \( \text{Im}(z) \geq y_0 \) for any fixed \( y_0 > 0 \). Furthermore, when \( z = iy \) is restricted to the positive \( y \)-axis we have,

\[
\Theta_\Lambda(z) = \sum_{x \in \Lambda} q^{x \cdot x} = \sum_{x \in \Lambda} (e^{\pi i (iy)}||x||) = \sum_{x \in \Lambda} 1 e^{\pi y ||x||}.
\]

This is positive since the norm is real and \( y \) is real.

For our purposes we will find it helpful to work with simpler functions known as the Jacobi theta functions. In particular we will be focusing on the following three Jacobi theta functions,
\[ \vartheta_2(z) = \sum_{n=-\infty}^{\infty} q^{(n+\frac{1}{2})^2} \]

\[ \vartheta_3(z) = \sum_{n=-\infty}^{\infty} q^{n^2} \]  \hspace{1cm} (2.2)

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

where \(q = e^{\pi i z}\) and \(\text{Im}(z) > 0\).

We can also expand these functions as infinite products as shown below,

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

\[ \vartheta_3(z) = \prod_{i=1}^{\infty} (1 - q^{2i})(1 + q^{2i+1})^2 \]  \hspace{1cm} (2.3)

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

Furthermore, it will be useful to notice that when \(\Lambda\) is the standard lattice \(\mathbb{Z}^n\) in the theta series then,

\[ \Theta_{\mathbb{Z}^n}(z) = \vartheta_3^n \]  \hspace{1cm} (2.4)

**Proof.**

For \(n=1\)

\[ \Theta_{\mathbb{Z}}(z) = \sum_{k \in \mathbb{Z}} q^{k^2} = \sum_{n=-\infty}^{\infty} q^{n^2} = \vartheta_3(z) \]

Since the the base case is trivial we take a look at when \(n=2\)

\[ \Theta_{\mathbb{Z}^2}(z) = \sum_{||(a_1, a_2)||} q^{||(a_1, a_2)||} \]

\[ = \sum_{(a_1, a_2) \in \mathbb{Z}^2} q^{a_1^2} \cdot q^{a_2^2} \]

By absolute convergence, the expression above can be arranged to be the Cauchy product
\[
\sum_{a_1 \in \mathbb{Z}} q^{a_1^2} \sum_{a_2 \in \mathbb{Z}} q^{a_2^2} \\
= \sum_{y \in \mathbb{Z}} q^{y^2} \sum_{y \in \mathbb{Z}} q^{y^2} \\
= \left( \sum_{y \in \mathbb{Z}} q^{y^2} \right)^2 \\
= \varphi_3(z)^2
\]

The proof for general \( n \) is similar, using induction. \( \blacksquare \)
Chapter 3

Codes

3.1 Codes

Coding theory plays an important part in achieving confusion for Eve. We will take time here to discuss some necessary terminology and results. A binary linear code $C$ of length $n$ is the set of vectors of a $k$-dimensional subspace of the $\mathbb{F}_2$-vector space $\mathbb{F}_2^n$ ($k < n$). The individual elements of the code $C$ are called codewords. Note that because $C$ is a linear subspace, given two elements $c_1$ and $c_2 \in C$ we have that,

$$c_1 + c_2 \in C$$

A code of length $n$ and dimension $k$ can be considered as the image of a $\mathbb{F}_2$-linear injective map $g$,

$$g : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n$$

where $n > k$.

**Definition 8.** A $k$ by $n$ generator matrix $G$ for a code $C$ of length $n$ and dimension $k$ is a matrix $G$:

$$G = \begin{bmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{k1} & a_{k2} & \cdots & a_{kn}
\end{bmatrix}$$

where $v_1 = (a_{11}, \ldots, a_{1n}), \ldots, v_k = (a_{k1}, \ldots, a_{kn})$ is a basis for the subspace $C$.

The matrix $G$ generates $C$. This means that one can take any vector $x = (x_1, x_2, \ldots x_k) \in \mathbb{F}_2^k$ and multiply it by $G$ to obtain an element in $C$,

$$(x_1, x_2, \ldots x_k) \cdot \begin{bmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{k1} & a_{k2} & \cdots & a_{kn}
\end{bmatrix} = (c_1, c_2, \ldots, c_n) \in C$$

If we consider the cardinality of $\mathbb{F}_2^k$ we see that there are $2^k$ elements in $\mathbb{F}_2^k$. This means that $G$ produces $2^k$ elements and so implies that a code with dimension $k$ has cardinality equal to $2^k$.

**Example 10.** Consider the generator matrix,

$$G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$
by multiplying the elements in $\mathbb{F}_2^2$ we get,

\[
(0,0) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = (0,0,0) \tag{3.1}
\]

\[
(0,1) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = (0,1,1) \tag{3.2}
\]

\[
(1,0) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = (1,1,0) \tag{3.3}
\]

\[
(1,1) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = (1,0,1) \tag{3.4}
\]

and so the following 4 vectors comprise the code $C$,

\[
C = \{(000), (011), (110), (101)\}
\]

and thus $|C| = 2^2 = 4$

Definition 9. The **weight** of a codeword is the number of 1s in the codeword

Example 11. The codeword (0010101) has weight 3

The codeword (0101000) has weight 2

Definition 10. The **minimum distance**, $d$, of a code is equal to the smallest weight of any nonzero codeword in the code $C$.

Definition 11. A code is denoted as $[n,k,d]$ where the $n$ is the length of the code, $k$ is the dimension of the code, and $d$ is the minimum distance of the code.

Example 12. Considering the code $C$ in Example 10, the length is 3, dimension 2, and the minimum distance of $C$ is 2, and the code is denoted as $[3,2,2]$.

Definition 12. The dual of a code $C$ is denoted as $C^\perp$ and defined as,

\[
C^\perp = \{x \in \mathbb{F}_2^n | x \cdot y = 0 \text{ for all } y \in C\}
\]

where $C$ is a $[n,k,d]$ code. Furthermore $C^\perp$ has dimension $n-k$.

We can think of $C^\perp$ as the null space of the generator matrix of $C$. So if $C$ has dimension $k$ in a $n$-dimensional space then the null set $C^\perp$ has dimension $n-k$. This follows from the rank nullity theorem found in [13].

Definition 13. We say that a code is a **self-dual code** if,

\[
C = C^\perp
\]
In the case where $C$ is a self-dual code we have that the dimension of $C$ and $C^\perp$ are equal, that is $k = n - k$ which means that $n = 2k$ for some $k$. Therefore a self-dual code $C$ is a $[2k,k,d]$ code, which implies that the length of a self-dual code is even. Lastly we note that in a self-dual code $C$, for any $c_1, c_2 \in C$ we have, $c_1 \cdot c_2 = 0$

**Example 13.** Let $C$ be a self-dual code, then for all $c_1, c_2 \in C$, $c_1 \cdot c_2 = 0$

If $c_1, c_2 \in C$ then $c_1, c_2 \in C^\perp$ and so by definition of $C^\perp$

$$c_1 \cdot c = 0 \text{ and } c_2 \cdot c = 0$$

for all $c \in C$ in particular for $c_1, c_2 \in C$. Therefore

$$c_1 \cdot c_2 = 0$$

**Fact 2** Every code contains the zero vector $(0,0,...0)$

This follows from the fact $C$ is a subspace of $\mathbb{F}_2^n$, and of course, the zero vector is an element of every subspace.

**Fact 3** The weight of any code word in a self-dual code is even.

If $c$ is a nonzero codeword, then $c \cdot c$ yields the weight of the code, modulo 2. Since $c \cdot c = 0$, the result follows.

**Fact 4** Every self-dual code contains the all-one vector $(11...1)$

If this is not the case then because $C = C^\perp$, $(11...1) \notin C^\perp$. Hence, there exist a $c \in C$ such that

$$(11...1) \cdot c = 1.$$

This means that that $c$ has odd weight, since $(11...1) \cdot c$ yields the weight of $c$. But this contradicts Fact 3 above.

$\therefore (11...1) \in C$

**Definition 14.** We define an **even code** to be a code $C$ in which all codewords in $C$ have even weight. An even code $C$ is a **doubly even** if every code word in $C$ has weight divisible by 4, otherwise we say $C$ is **singly even**.

**Fact 5** Since all self-dual codes have length and weight divisible by 2 then every self-dual code can be classified as singly even or doubly even.

**Fact 6** Doubly even codes exist only in length divisible by 8.

This proof is similar to why unimodular lattices have dimension congruent to 0 mod 8 and is explored further in [11].
3.2 Weight Enumerator

Just as unimodular lattices have an associated theta series that measures the number of lattice points of a given squared norm, self-dual codes have a weight enumerator polynomial associated to them that measures the number of code words of a given weight. The weight enumerator representation is defined as,

$$ W_C(x, y) = \sum_{m=0}^{n} W_m x^{n-m} y^m $$

(3.5)

where $W_i$ equals the number of codewords of weight $i$.

Given a self-dual code $C$ we have the following weight enumerator,

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

where $W_0 = 1$ since there is only one codeword of weight 0. Similarly $W_n = 1$ since the is only one code word of weight $n$, that is, the codes with all entries equal to 1. We now further look at some additional facts of the weight enumerator polynomial.

**Fact 7** For the weight enumerator of a self-dual code we have that, $W_j = W_{n-j}$

By Fact 3 we have that $(11\ldots1) \in C$ and so by linearity any code word $c \in C$ can be added to $(11\ldots1)$ to obtain the vector with 0’s in the 1’s position of vector $c$ and 1’s in its 0 entries. Therefore for any code word of length $j$ there is a corresponding codeword of length $n-j$.

**Example 14.** Suppose $C$ is a self-dual code of length 10 and of dimension 5. If $c = (0010111000) \in C$ where $c$ has weight 4, then since $(1111111111) \in C$ we have that,

$$(0010111000) + (1111111111) = (1101000111) \in C$$

where $(1101000111)$ has weight 6. That is, for a code of length 10 we have that every codeword of weight 4 has a one to one correspondence to a codeword of weight 6. So the number of codewords of weight 4 is equal to the number of codewords of weight 6.

$\therefore W_4 = W_6$

**Fact 8** In a self-dual code $W_j = 0$ when $j$ is odd. Since all self-dual codes have weight divisible by two it follows that no code of odd weight exist.

**Fact 9** For doubly even self-dual codes we have that $W_j = 0$ for all $j \neq 0 \mod 4$. Since all codewords in a doubly even self-dual codes have weights divisible by 4 it follows that for every $j$ not divisible by 4 we have no codewords of that weight in $C$. 

18
Therefore, for all doubly even self-dual codes we have the following weight enumerator representation,

\[ W_C(x, y) = x^n + W_4 x^{n-4} y^4 + W_8 x^{n-8} y^8 + \cdots + W_{n-4} x^4 y^{n-4} + y^n \]

### 3.3 Construction A

There is a close relationship between the weight enumerator polynomial and the theta series of a lattice. In this section we introduce construction A found in [11], which describes a parallel between codes of length \( n \) and lattices in \( \mathbb{R}^n \).

Take the standard lattice \( \mathbb{Z}^n \in \mathbb{R}^n \) and consider a \([n, k, d]\) binary code \( C \). The first step is to reduce the standard lattice to modulo 2 by using the following map,

\[ \rho : \mathbb{Z}^n \mapsto (\mathbb{Z}/2\mathbb{Z})^n = \{0, 1\}^n \]

We define the n-dimensional lattice \( \Lambda_C \) as,

\[ \Lambda_C = \langle \frac{1}{\sqrt{2}} (2\mathbb{Z}^n + c_i) \rangle, \quad c_i \in C \]

where each \( c_i \in \mathbb{Z}^n \) is a coset representatives for \( c_i \in C \subseteq (\mathbb{Z}/2\mathbb{Z})^n \). Notice that \( \Lambda_C = \frac{1}{\sqrt{2}} \rho^{-1}(C) \), that is, \( \Lambda \) can be viewed as the product of \( \frac{1}{\sqrt{2}} \) and the preimage of \( C \) in \( \mathbb{Z}^n \).

**Example 15.**

Take the \([2,1,1]\) code \( C \) with elements \( \{(0,0), (0,1)\} \). Then, \( \Lambda_C \) is the lattice generated by \( 2\mathbb{Z}^2 \) and the vector \((0,1) \in \mathbb{R}^2 \) scaled by \( \frac{1}{\sqrt{2}} \), in other words, the lattice in \( \mathbb{R}^2 \) generated by \((2,0)\) and \((0,1)\) and scaled by \( \frac{1}{\sqrt{2}} \).

Found in [11], there are also useful properties relating a code \( C \) and its corresponding lattice \( \Lambda \).

**Theorem 2.**

\( C \) is a self-dual code if and only if \( \Lambda_C \) is a unimodular lattice

**Proof.**

We will begin the proof by assuming that \( C \) is a self-dual code and show that \( \Lambda_C \) must be unimodular. This is done by showing that \( \Lambda_C = \Lambda_C^{\perp} \)

\((\Lambda_C^{\perp} \subseteq \Lambda_C)\): Let \( C \) be a self-dual code, then \( C = C^{\perp} \) and let \( \Lambda_C \) be the corresponding lattice under the mapping \( \rho \). This means that elements in \( \mathbb{Z}^n \) look like \( \frac{1}{\sqrt{2}} (2\mathbb{Z}^n + c_i) \) for \( c_i \in C \).

Consider an element \( \mathbf{v} \in \Lambda_C^{\perp} \). Since \( \frac{1}{\sqrt{2}} 2\mathbb{Z}^n \subseteq \Lambda_C \) then we have,
$$\mathbf{v} \cdot \frac{1}{\sqrt{2}}(2\mathbb{Z}^n) \subseteq \mathbb{Z}.$$ 

This means that,

$$(v_1, \ldots, v_n) \cdot \frac{1}{\sqrt{2}}(2, 0, \ldots, 0) \in \mathbb{Z}$$

$$(v_1, \ldots, v_n) \cdot \frac{1}{\sqrt{2}}(0, 2, \ldots, 0) \in \mathbb{Z}$$

$$\vdots$$

$$(v_1, \ldots, v_n) \cdot \frac{1}{\sqrt{2}}(0, 0, \ldots, 2) \in \mathbb{Z}$$

which implies that,

$$\frac{2v_1}{\sqrt{2}} \in \mathbb{Z}, \frac{2v_2}{\sqrt{2}} \in \mathbb{Z}, \ldots, \frac{2v_n}{\sqrt{2}} \in \mathbb{Z}$$

so,

$$v_1 \in \frac{\sqrt{2}}{2}\mathbb{Z}, v_2 \in \frac{\sqrt{2}}{2}\mathbb{Z}, \ldots, v_n \in \frac{\sqrt{2}}{2}\mathbb{Z}$$

$$\therefore \Lambda_C^\perp \subseteq \frac{\sqrt{2}}{2}\mathbb{Z}^n = \frac{1}{\sqrt{2}}\mathbb{Z}^n$$

Now suppose that we have $$\frac{1}{\sqrt{2}}(b_1, b_2, \ldots, b_n) \in \Lambda_C^\perp$$ for $$b_i \in \mathbb{Z}$$ then,

$$\frac{1}{\sqrt{2}}(b_1, b_2, \ldots, b_n) \cdot \frac{1}{\sqrt{2}}(c_1, c_2, \ldots, c_n) \in \mathbb{Z}$$

where $$(c_1, c_2, \ldots, c_n)$$ is an element in the preimage of C, that is,

$$(\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_n) \in C$$

where $$\bar{c}_i$$ stands for the image under modding by 2.

Now,

$$\frac{1}{\sqrt{2}}(b_1, b_2, \ldots, b_n) \cdot \frac{1}{\sqrt{2}}(c_1, c_2, \ldots, c_n) = \frac{1}{2}(b_1c_1 + \ldots + b_nc_n) \in \mathbb{Z}$$

$$\implies b_1c_1 + \ldots + b_nc_n \in 2\mathbb{Z}$$

This means that,

$$\rho(b_1c_1 + \ldots + b_nc_n) = 0$$
so,

\[(\overline{b_1}, \overline{b_2}, ..., \overline{b_n}) \cdot (\overline{c_1}, \overline{c_2}, ..., \overline{c_n}) = 0\]

since \(\frac{1}{\sqrt{2}}(b_1, ..., b_n) \in \Lambda_C^\perp\) then,

\[(\overline{b_1}, \overline{b_2}, ..., \overline{b_n}) \cdot (\overline{c_1}, \overline{c_2}, ..., \overline{c_n}) = 0\]

holds for all \((\overline{c_1}, ..., \overline{c_n}) \in C\) which implies that \((\overline{b_1}, \overline{b_2}, ..., \overline{b_n}) \in C^\perp = C\), so,

\[\frac{1}{\sqrt{2}}(b_1, ..., b_n) \in \Lambda_C\]

and thus,

\[\Lambda_C^\perp \subseteq \Lambda_C.\]

\((\Lambda_C \subseteq \Lambda_C^\perp)\): Take an arbitrary fixed element \(\frac{1}{\sqrt{2}}((2a_1, ..., 2a_n) + (c_1, ..., c_n)) \in \Lambda_C\). Now consider another arbitrary element (not fixed) \(\frac{1}{\sqrt{2}}((2b_1, ..., 2b_n) + (d_1, ..., d_n)) \in \Lambda_C\). We see that,

\[
\left(\frac{1}{\sqrt{2}}((2a_1, ..., 2a_n) + (c_1, ..., c_n)) \cdot \left(\frac{1}{\sqrt{2}}((2b_1, ..., 2b_n) + (d_1, ..., d_n))\right)\right)
\]

\[= \frac{1}{2}(2a_1 + 2b_1 + d_1 + ... + 2a_n + 2b_n + d_n)\]

\[= \frac{1}{2}((4a_1b_1 + 2a_1d_1 + 2b_1c_1 + d_1c_1) + ... + (4a_nb_n + 2a_td_n + 2b_nc_n + c_td_n))\]

\[= \frac{1}{2}((4a_1b_1 + ... + 4a_nb_n) + (2a_1d_1 + ... + 2a_n) + (2b_1c_1 + ... + 2b_n) + (c_1d_1 + ... + c_nd_n))\]

Since, \(c \cdot d = c_1d_1 + ... + c_nd_n = 2l\) for some \(l \in \mathbb{Z}\) because \(C\) is a self-dual code then,

\[
\left(\frac{1}{\sqrt{2}}((2a_1, ..., 2a_n) + (c_1, ..., c_n)) \cdot \left(\frac{1}{\sqrt{2}}((2b_1, ..., 2b_n) + (d_1, ..., d_n))\right)\right)
\]

\[= \frac{1}{2}((4a_1b_1 + ... + 4a_nb_n) + (2a_1d_1 + ... + 2a_n) + (2b_1c_1 + ... + 2b_n) + 2l)\]

\[= (a_1b_1 + ... + a_nb_n) + (a_1d_1 + ... + a_n) + (b_1c_1 + ... + b_n) + l \in \mathbb{Z}\]

and so \(\frac{1}{\sqrt{2}}((2a_1, ..., 2a_n) + (c_1, ..., c_n)) \in \Lambda_C^\perp\). Since \(\frac{1}{\sqrt{2}}((2a_1, ..., 2a_n) + (c_1, ..., c_n)) \in \Lambda_C\) was arbitrary it follows that,

\[\Lambda_C \subseteq \Lambda_C^\perp\]

Therefore \(\Lambda_C = \Lambda_C^\perp\) when \(C\) is a self-dual code.
Next we want to assume that $\Lambda$ is a unimodular lattice and show that $C$ is a self-dual code. It is sufficient to show that $C \subseteq C^\perp$ and that $C^\perp \subseteq C$.

\((C \subseteq C^\perp)\) : Take the elements $c, d \in C$. Then $\rho^{-1}(c) \in \Lambda_C$, so $\rho^{-1}(c)$ is of the form $\frac{1}{\sqrt{2}} (2z + c)$, similarly, $\rho^{-1}(d) = \frac{1}{\sqrt{2}} (2z + d)$. By taking the dot product of the elements in $\Lambda$ we get,

\[
\frac{1}{\sqrt{2}} (2y + c) \cdot \frac{1}{\sqrt{2}} (2z + d) = \frac{1}{2} (2y + c) \cdot (2z + d)
\]

By similar computation as before we have that,

\[
\frac{1}{\sqrt{2}} (2y + c) \cdot \frac{1}{\sqrt{2}} (2z + d) = \frac{1}{2} ((4y_1z_2 + \cdots + 4y_nz_n) + (2y_1d_1 + \cdots 2y_n d_n) + (2z_1 c_1 + \cdots + 2z_n c_n) + (c_1 d_1 + \cdots + c_n d_n))
\]

this implies that, $c_1 d_1 + \cdots + c_n d_n$ must be divisible by 2. Therefore $y \cdot z = 0$ in $C$, so, $C \subseteq C^\perp$.

\((C^\perp \subseteq C)\) : Now take an element $(\overline{c_1}, \ldots, \overline{c_n}) \in \mathbb{Z}/2\mathbb{Z}^n$ such that $(\overline{c_1}, \ldots, \overline{c_n}) \in C^\perp$. This means that for all $(\overline{d_1}, \ldots, \overline{d_n}) \in C$ we have that $(\overline{c_1}, \ldots, \overline{c_n}) \cdot (\overline{d_1}, \ldots, \overline{d_n}) = 0$. Consider the pre image of each of these codewords,

\[
\rho^{-1}(\overline{c_1}, \ldots, \overline{c_n}) = (c_1, \ldots, c_n)
\]

\[
\rho^{-1}(\overline{d_1}, \ldots, \overline{d_n}) = (d_1, \ldots, d_n)
\]

we have that,

\[
(c_1, \ldots, c_n) \cdot (d_1, \ldots, d_n) \in 2\mathbb{Z}
\]

In particular, we have that,

\[
\frac{1}{\sqrt{2}} (c_1, \ldots, c_n) \cdot \frac{1}{\sqrt{2}} (d_1, \ldots, d_n) \in \mathbb{Z}
\]

for all $(\overline{d_1}, \ldots, \overline{d_n}) \in C$.

Since an arbitrary element of $\Lambda_C$ is of the form $\frac{1}{\sqrt{2}} (d_1, \ldots, d_n)$ then it follows that,

\[
\frac{1}{\sqrt{2}} (c_1, \ldots, c_n) \in \Lambda_C^\perp
\]

Since $\Lambda_C = \Lambda_C^\perp$ then $\frac{1}{\sqrt{2}} (c_1, \ldots, c_n) \in \Lambda_C$ implying that $(\overline{c_1}, \ldots, \overline{c_n}) \in C$. Therefore $C = C^\perp$ when $\Lambda_C$ is unimodular.

**Theorem 3.**

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

**Proof.**

Assuming that $C$ is a doubly even code, choose and arbitrary element $\frac{1}{\sqrt{2}} (2y + c) \in \Lambda_C$ we get,
\[
\frac{1}{\sqrt{2}}(2y + c) \cdot \frac{1}{\sqrt{2}}(2y + c)
\]
\[
= \frac{1}{2}((4y^2_1 + ... + 4y^2_n) + 2(2y_1c_1 + ... 2y_nc_n) + (c_1^2 + ... + c_n^2))
\]
Since \(C\) is doubly even it follows that,
\[
c_1^2 + ... + c_n^2 = 4k
\]
this implies,
\[
\frac{1}{2}((4y^2_1 + ... + 4y^2_n) + 2(2y_1c_1 + ... 2y_nc_n) + (c_1^2 + ... + c_n^2))
\]
\[
= 2(y^2_1 + ... + y^2_n) + 2(y_1c_1 + ... y_nc_n) + 2k \in 2\mathbb{Z}
\]
\[
\therefore \Lambda_C\ is \ an \ even \ unimodular \ lattice
\]
Now let \(\Lambda_C\) be an even unimodular lattice.

Every code word \(c \in C\) as a pre image of the form \(\frac{1}{\sqrt{2}}(2y + c) \in \Lambda_C\). By taking the dot product with itself we get,
\[
\frac{1}{\sqrt{2}}(2y + c) \cdot \frac{1}{\sqrt{2}}(2y + c)
\]
\[
= \frac{1}{2}((4y^2_1 + ... + 4y^2_n) + 2(2y_1c_1 + ... 2y_nc_n) + (c_1^2 + ... + c_n^2))
\]
\[
= (2r + 2s + \frac{1}{2}(c_1^2 + ... + c_n^2))
\]
notice that \(\frac{1}{2}(c_1^2 + ... + c_n^2)\) must be in \(2\mathbb{Z}\) since \(\Lambda_C\) is an even lattice. Since the \(c_i\)'s are all 0's or 1's then there must be 4\(k\) 1's in order for \(\frac{1}{2}(c_1^2 + ... + c_n^2)\) to be even. Therefore \(c \in C\) is of weight divisible by 4. Since \(c\) was arbitrary it follows that all codewords in \(C\) are of weight divisible by 4 and thus \(C\) is a doubly even code. \(\blacksquare\)

As seen, there is a close relationship with self-dual codes and unimodular lattices. Similarly in \([11]\) we obtain the following relationship between the theta series of a lattice \(\Lambda\) and the weight enumerator of a code \(C\).

**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
\[
\Theta_{\Lambda_C} = W_C(\vartheta_3(2z), \vartheta_2(2z))
\]
where \(\vartheta_2\) and \(\vartheta_3\) are the Jacobi Theta functions defined in Chapter 2.

We will see the usefulness of these results as we move into our problem at hand in the following chapters.
Chapter 4
Coset Coding

4.1 Coset Coding

Coset encoding was demonstrated in [6] and [9] to be an effective tool in achieving confusion for the wiretapper Eve. As discussed in the introduction, the focus of this thesis is based on the wiretap scenario with Alice, Bob, and Eve. We consider a Gaussian wiretap channel where the sender Alice sends a message to the receiver Bob, all while having an eavesdropper Eve listening in through a much noisier channel. Recall that the message received by Bob and Eve is defined as,

\[ \hat{x} = x + v_b \]  where \( v_b \) is the error vector for Bob

\[ \tilde{x} = x + v_e \]  where \( v_e \) is the error vector for Eve

where \( x \) is the original message vector. The mean error for Bob and Eve is defined to be zero with variance \( \sigma_b^2 \) and \( \sigma_e^2 \) for each respectively. Since the Eve’s channel is noisier than Bob’s we can assume that \( \sigma_b^2 \ll \sigma_e^2 \). Furthermore, we are under the assumption that Alice knows \( \sigma_b^2 \) and \( \sigma_e^2 \) (further reading of [6] includes the case when Alice does not know \( \sigma_e^2 \)). This can be illustrated by the figure below also found in [6],

Alice transmits \( k \) information symbols \( s_1, s_2, ..., s_k \) for \( s_i \in \mathbb{F}_2 \) into the vector \( x = (x_1, x_2, ..., x_n) \in \mathbb{R}^n \) which then goes through the channel and is received by Bob with some error. Now the codeword \( x \) is actually a point of the lattice used in lattice coding by Alice. This means that she choses a lattice \( \Lambda_b \) where \( b \) stands for the intented receiver Bob and encodes the information into a point of the lattice \( x \in \Lambda_b \).

In order to create more confusion for Eve, the lattice \( \Lambda_b \) is a partition into a union of disjoint cosets \( \Lambda_e + c \) where \( c \) is an \( n \)-dimensional vector and \( \Lambda_e \) is a sub-lattice of \( \Lambda_b \) where \( e \) stands for Eve. Furthermore, \( |\Lambda_b/\Lambda_e| = 2^k \) in order to obtain a one-to-one correspondence with code \( C \), since \( |C| = 2^k \).

Alice now picks a codeword \( c \in C \) and maps it to a vector \( c \in \Lambda_b \) via the chosen
correspondence \( \Lambda_b/\Lambda_e \leftrightarrow C \). She then chooses a random vector \( r \in \Lambda_e \), then transmits the vector \( x = r + c \). The fact that Eve’s channel is much noisier than Bob’s \( (\sigma_b^2 \ll \sigma_e^2) \) already makes it harder for Eve to decode than for Bob. Additionally, however, an analysis of probabilities (below) shows that the fact that \( r \in \Lambda_e \) is random makes it even more difficult for Eve to decode, given her very high noise variance, while it does not make much difference to Bob.

To find the correct coset sent from Alice, Eve and Bob find the closest lattice point in \( \Lambda_b \) to their own received vector. To further understand how this works we must introduce the following,

**Definition 15.** A **Voronoi cell** for a point \( p_i \in \Lambda \) is defined as follows,

\[
\nu(p_i) = \{ x \in \mathbb{R} | d(x, p_i) < d(x, p_j) \text{ for all } j \}
\]

where \( p_j \in \Lambda, j \neq i \), and \( d(x, y) \) is the standard Euclidean metric.

For any lattice we have that the Voronoi cell is the same shape for any point in that given lattice. For simplicity we can therefore refer to the Voronoi cell of a point in \( \Lambda \) as simply the Voronoi cell of the lattice \( \Lambda \).

When Alice transmits her codeword \( x = r + c \) with Voronoi cell \( \nu(x) \) over an additive white Gaussian noise channel, the decoder Bob will make the correct decryption if and only if \( \hat{x} \) is in \( \nu(x + s) \) for any \( s \in \Lambda_e \). The assumption that Bob’s channel is of high quality (low \( \sigma_b \)) allows us to ignore the case of \( \hat{x} \) being in \( \nu(x + s) \) for any nonzero \( s \in \Lambda_e \), since the probability of this occurring is very low. Thus, we wish to consider the probability of \( \hat{x} \) being in \( \nu(x) \). The probability of this occurring is given by the following,

\[
P_{c,b} = \frac{1}{(\sigma_b \sqrt{2\pi})^n} \int_{\nu_{\Lambda_b}(x)} e^{-||\hat{x} - x||/2\sigma_b^2} d\hat{x} = \frac{1}{(\sigma_b \sqrt{2\pi})^n} \int_{\nu_{\Lambda_b}(0)} e^{-||u||/2\sigma_b^2} du
\]

where, recall that by \( ||v|| \) we mean the squared norm of the vector \( v \).

As for Eve, she will correctly decode if her received signal \( \tilde{x} \) is in \( \nu(x + s) \) for any \( s \in \Lambda_e \). This time around, we cannot ignore the cases where \( s \neq 0 \), since her noise variance is high. The probability that Eve will correctly decode is therefore given by

\[
P_{c,e} = \frac{1}{(\sigma_e \sqrt{2\pi})^n} \sum_{s \in \Lambda_e} \int_{\nu_{\Lambda_b}(x+s)} e^{-||\tilde{x} - x||/2\sigma_e^2} d\tilde{x} = \frac{1}{(\sigma_b \sqrt{2\pi})^n} \sum_{s \in \Lambda_e} \int_{\nu_{\Lambda_b}(s)} e^{-||u||/2\sigma_e^2} du
\]

There is a large amount of probability theory needed to designing the functions (4.2) and (4.3). For our purposes we note the existence of them and solely use them in this paper to better connect our results to the question in hand. These are further explored in [9] and [7]. Further analysis of (4.2) and (4.3) in [6] lead to the following,
\[
\frac{P_{c,e}}{P_{c,b}} \approx \left( \frac{\sigma_b}{\sigma_e} \right)^n \text{Vol}(\nu(\Lambda_b(0))) \sum_{s \in \Lambda_b} \frac{e^{-||s||/2\sigma^2_e}}{\int_{\nu(\Lambda_b)} e^{-||u||/2\sigma^2_b} du}
\]

(4.4)

By setting \(\Lambda_b\) fixed and finding a lattice \(\Lambda_e \subset \Lambda_b\) for which,

\[
\sum_{s \in \Lambda_e} e^{-||s||/2\sigma^2_e}
\]

can be minimized under the constraint \(|\Lambda_b/\Lambda_e| = 2^k\), high rate of failure of decryption by Eve can be attained.

Let’s consider the following,

\[
\sum_{s \in \Lambda_e} e^{-||s||/2\sigma^2_e} = \sum_{s \in \Lambda_e} (e^{1/2\sigma^2_e})^{-||s||} = \sum_{s \in \Lambda_e} ((e^{i\pi})^{-1/2i\pi\sigma^2_e})||s||
\]

and so when \(z = -\frac{1}{2i\pi\sigma^2_e}\) and \(q = e^{i\pi z} = e^{-1/2\sigma^2_e}\), we get,

\[
\sum_{s \in \Lambda_e} e^{-||s||/2\sigma^2_e} = \sum_{s \in \Lambda_e} q||s|| = \Theta_e(z)
\]

It follows that minimizing the theta series of a lattice at the point \(z = -\frac{1}{2i\pi\sigma^2_e}\) is equivalent to minimizing correct decryption on Eve’s end. Therefore, we are interested in minimizing the theta series of the lattice \(\Lambda_e\) over all possible \(\Lambda_e\) in particular when \(z = -\frac{1}{2i\pi\sigma^2_e}\).

Minimizing the theta series happens to be a problem that arises in the study of theta series and so for this reason we consider the following. Notice that \(\Lambda_e\) was arbitrary, and thus we can assume that \(\Lambda_e\) is a scaled version of \(\mathbb{Z}^n\). In [8], Belfiore and Oggier define the secrecy function of a given lattice \(\Lambda\) for a point \(y > 0\) as the ratio of the theta function of \(\mathbb{Z}^n\) to the theta function of \(\Lambda\) at the point \(iy\).

**Definition 16.** Let \(\Lambda\) be an \(n\)-dimensional lattice. The **secrecy function** of \(\Lambda\) is given by,

\[
\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^n}(iy)}{\Theta_\Lambda(iy)} \text{ for } y > 0
\]

(4.5)

Finding the maximum value of the secrecy function is of particular interest in attempting to minimize the correct decryption for Eve. This leads to the following definition,

**Definition 17.** The **secrecy gain** \(\chi_\Lambda\) is an \(n\)-dimensional lattice \(\Lambda\) defined by,

\[
\chi_\Lambda = \sup_{y > 0} \Xi_\Lambda(y)
\]

Some things to note regarding these two definitions are found in [6] and are given below,
1. When attempting to minimize $\Theta_{\Lambda_e}(y)$ under the constraint $|\Lambda_b/\Lambda_e| = 2^k$ we must consider lattices with same volume.

2. We are interested in the secrecy function at a particular point, that is $z = \frac{i}{2\sigma_e^2}$. Since we consider $\sigma_e^2$ as a variable it makes sense to maximize the secrecy function over $y > 0$. The value of $y$ that yields the lowest value of $\Theta_{\Lambda_e}(y)$ gives the optimum signal-to-noise ratio (i.e., the quantity $\sigma_e^2$) at which Eve has most confusion using $\Lambda_e$ compared to using just a scaled version of $\mathbb{Z}^n$.

This is the heart of most of the work done leading to our main conjecture.

4.2 The Belfiore-Sóle Conjecture

In [8] Belfiore and Oggier explored practical schemes for coding and error probability. This lead to finding a connection between minimizing correct decryption by Eve and maximizing the secrecy function as mentioned above. Further work in [6] by Belfiore, Solé, and Oggier focused on the significance of the secrecy gain and developed the following conjecture,

**Conjecture 4** (Belfiore-Solé Conjecture). *The secrecy function of a unimodular lattice obtains its maximum at $y=1$*

Belfiore and Solé’s conjecture is quite an undertaking and has been only proven for the following sets of lattices,

1. All known extremal unimodular lattices
2. All lattices of dimensions up to length 23
3. Given an orthogonal finite direct sum where each lattice satisfies the conjecture we have that the direct sum also satisfies the conjecture. Furthermore this results in infinitely many lattices satisfying the conjecture.
4. All unimodular lattices from doubly even self-dual codes up to length 40 satisfy the conjecture.

Using Wolfram Mathematica to facilitate the computation process we will further show that,

1. All unimodular lattices from doubly even self-dual codes up to length 64 that meet the Conway-Sloane bound on minimal distance [12] satisfy the conjecture.
2. All unimodular lattices from singly even self-dual codes up to length 72 that meet the Conway-Sloane bound on minimal distance [12] satisfy the conjecture.
Chapter 5

Classification of Binary Self-Dual Codes of Highest Minimal Distance

In [12], Conway and Sloane proved a number of results that gave new bounds to the minimal distance of a self-dual code. They determined the highest possible minimum distances of all binary self-dual codes of length up to 72, both for type I (i.e., singly even) codes, and for type II (i.e., double even) codes. Further, for all binary self-dual codes of both Type I and Type II of length up to 72, they determined the weight enumerators of all codes that achieve the highest possible minimum distance. It is to be noted that in some cases, more than one code achieves the highest possible minimum distance.

We will use Conway and Sloane’s classification, and particularly their listing of weight enumerators, to show that all lattices that arise from these codes via Construction A satisfy the Belfiore-Solé conjecture. In this chapter, we list all the weight enumerators of these codes, from [12]. Since the coefficients of these weight enumerators are palindromic, we only give the coefficient up to the midpoint.

**Type I (i.e., singly even) Codes:**

- Length n=24 with Minimal Distance d=6
  \[ W_{C_{24}} = x^{24} + 64x^{18}y^6 + 375x^{16}y^8 + 960x^{14}y^{10} + 1296x^{12}y^{12} + \ldots \]

- Length n=32 with Minimal Distance d=8
  \[ W_{C_{32}} = x^{32} + 364x^{24}y^8 + 2048x^{22}y^{10} + 6720x^{20}y^{12} + 14336x^{18}y^{14} + 18598x^{16}y^{16} + \ldots \]

- Length n=40 with Minimal Distance d=8
  \[ W_{C_{40}} = x^{40} + 285x^{32}y^8 + 1024x^{30}y^{10} + 11040x^{28}y^{12} + 46080x^{18}y^{14} + \ldots \]
  or
  \[ W_{C_{40}} = x^{40} + 125x^{32}y^8 + 1664x^{30}y^{10} + 10720x^{28}y^{12} + 44160x^{18}y^{14} + \ldots \]

- Length n=48 with Minimal Distance d=10
  \[ W_{C_{48}} = x^{48} + 704x^{38}y^{10} + 8976x^{36}y^{12} + 56896x^{34}y^{14} + 267575x^{32}y^{16} + \ldots \]
  or
  \[ W_{C_{48}} = x^{48} + 768x^{38}y^{10} + 8592x^{36}y^{12} + 57600x^{34}y^{14} + 267831x^{32}y^{16} + \ldots \]

- Length n=56 with Minimal Distance d=12
  \[ W_{C_{56}} = x^{56} + 4606x^{44}y^{12} + 45056x^{42}y^{14} + 306922x^{40}y^{16} + 1576960x^{38}y^{18} + \ldots \]
  or
  \[ W_{C_{56}} = x^{56} + 4862x^{44}y^{12} + 43008x^{42}y^{14} + 313066x^{40}y^{16} + 1570618x^{38}y^{18} + \ldots \]
• Length n=64 with Minimal Distance d=12
\[ W_{C_{64}} = x^{64} + 1824x^{52}y^{12} + 20992x^{50}y^{14} + 227884x^{48}y^{16} + \ldots \]

• Length n=72 with Minimal Distance d=14
\[ W_{C_{72}} = x^{72} + 7616x^{58}y^{14} + 134521x^{56}y^{16} + 1151040x^{54}y^{18} + \ldots \]

or
\[ W_{C_{72}} = x^{72} + 8576x^{58}y^{14} + 124665x^{56}y^{16} + 1206912x^{54}y^{18} + \ldots \]

or
\[ W_{C_{72}} = x^{72} + 8640x^{58}y^{14} + 124281x^{56}y^{16} + 1207360x^{54}y^{18} + \ldots \]

Type II (i.e., doubly even) Codes:

• Length n=48 with Minimal Distance d=12
\[ W_{C_{48}} = x^{48} + 17296x^{36}y^{12} + 535095x^{32}y^{16} + 3995376x^{28}y^{20} + 7681680x^{24}y^{24} + \ldots \]

• Length n=56 with Minimal Distance d=12
\[ W_{C_{56}} = x^{56} + 8190x^{44}y^{12} + 622314x^{40}y^{16} + 11699688x^{36}y^{20} + 64909845x^{32}y^{24} + \ldots \]

• Length n=64 with Minimal Distance d=12
\[ W_{C_{64}} = x^{64} + 2976x^{52}y^{12} + 454956x^{48}y^{16} + 18275616x^{44}y^{20} + 233419584x^{40}y^{24} + \ldots \]

The next chapter lays a foundation for the methods used to show that the type I and type II codes listed above satisfy the Belfiore and Solé conjecture.
Chapter 6

The Belfiore-Solé Conjecture for Lattices from Maximal Self Dual Codes of Length Up To 72

As seen in Chapter 5, we are given the weight enumerator polynomial for various types of self-dual codes with a given minimal distance $d$ of length up to 72, and these codes have the maximum possible minimum distance for their given length. We lift these codes to lattices using Construction A, and using this set of lattices, we wish to show that they too satisfy the Belfiore and Solé conjecture. This chapter begins by summarizing results by Ernvall-Hytönen in [2]. These results, along with two additional mappings given below, are needed to verify the conjecture for certain self-dual codes. In the next section, a manual approach showing that singly even codes of length 24 and minimal distance 6 satisfy the conjecture is given. Section 6.3 will introduce a program created to facilitate the computation seen in section 6.2. Section 6.3 also defines several functions used in Wolfram Mathematica and provides a walk through of what each component of the code does. Computations done by Wolfram Mathematica can be found in the index.

6.1 More Preliminaries

In [2], Ernvall-Hytönen observed that all unimodular lattices of length $n$ had a secrecy function representation as,

$$
\Xi_\Lambda = \frac{\Theta_{z^n}}{\Theta_\Lambda} = \left(\sum_{r=0}^{k} a_r \varphi_2^4 \varphi_4^r \right)^{-1}
$$

for $n = 8k + i$ and $i = 1, \ldots, 7$. Ernvall-Hytönen then considered the secrecy function as a function of the variable $\zeta(y) = \varphi_2^4 \varphi_4^r / \varphi_3^s$. Using Jacobian identities found in [11], she showed that the function $\zeta(y)$ has symmetry which led them to conclude the following lemma (see also [10]).

**Lemma 2.** For all $y \in \mathbb{R}^+$, the function

$$
\zeta(y) = \frac{\varphi_2^4 \varphi_4^r}{\varphi_3^s}
$$

has a unique maximum of $\frac{1}{4}$ at $y = 1$

To prove that the secrecy function obtains its maximum at $y = 1$, we consider the secrecy function representation below,

$$
\Xi_\Lambda(y) = \frac{1}{f(\zeta)}
$$
where $\zeta(y)$ takes its values on $[0, \frac{1}{4}]$. This means that the domain we want to consider for $f(\zeta)$ is also the interval $[0, \frac{1}{4}]$. If we have that the function $f$ is decreasing on this interval, then $f$ attains its minimum at $\frac{1}{4}$. This then tell us that $\frac{1}{f(\zeta)}$ is increasing on $[0, \frac{1}{4}]$ and attains its maximum $\frac{1}{4}$. By, [2] we have that $\frac{1}{f(\zeta)}$ is the secrecy function, and thus we can conclude that the secrecy function attains its maximum at $y = 1$. It is important to notice that much of the detail of these results has been left out and can be further explored in [2], as also [10]. For our purposes we only briefly summarize them here in order to use in the upcoming sections without confusion of our goal at hand.

Now recall that given a code $C$ with weight enumerator polynomial $W_C(x, y)$, the theta series of its corresponding lattice is,

$$\Theta_{\Lambda_C} = W_C(\vartheta_3(2z), \vartheta_2(2z))$$  \hspace{1cm} (6.1)

This and the following four lemmas found in [11] will allow us to take the weight enumerator polynomial and turn it into the theta series of its corresponding lattice.

**Lemma 3.** Let $C$ be a doubly even code with weight enumerator $W_C(x, y)$. Then the theta series of its corresponding lattice $\Lambda_C$ is given by,

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

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

**Lemma 4.** Under the map $x \mapsto \vartheta_3(2z), y \mapsto \vartheta_2(2z)$, we have

$$\psi_8 \mapsto \vartheta_3^8 - \vartheta_2^4 \vartheta_4^4$$

$$\xi_{24} \mapsto \frac{1}{16}\vartheta_2^8 \vartheta_3^8 \vartheta_4^8$$

**Proof.** Consider the following Jacobi identities found in [11],

$$\vartheta_3^2(z) + \vartheta_4^2(z) = 2\vartheta_3^2(2z)$$

$$\vartheta_3^2(z) - \vartheta_4^2(z) = 2\vartheta_3^2(2z)$$

$$\vartheta_3^4(z) + \vartheta_4^4(z) = 2\vartheta_3^4(z)$$

By Lemma 3 we have $\psi_8 = x^8 + 14x^4y^4 + y^8$ and $\xi_{24} = x^4y^4(x^4 - y^4)^4$.

Under the map shown, we have the following:

$$\psi_8 \mapsto (\vartheta_3(2z))^8 + 14(\vartheta_3(2z))^4(\vartheta_2(2z))^4 + (\vartheta_2(2z))^8$$ \hspace{1cm} (6.2)

$$\xi_{24} \mapsto (\vartheta_3(2z))^4(\vartheta_2(2z))^4((\vartheta_3(2z))^4 - (\vartheta_2(2z))^4)^4$$ \hspace{1cm} (6.3)
The image of \( \psi_8 \) becomes,

\[
(\vartheta_3(2z))^8 + 14(\vartheta_3(2z))^4(\vartheta_2(2z))^4 + (\vartheta_2(2z))^8
\]

\[
= (\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_2^2(z))^4 + 14(\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_2^2(z))^2(\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_2^2(z))^2 + (\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_2^2(z))^4
\]

\[
= \vartheta_3^8(z) + \vartheta_2^8(z) - \vartheta_3^4(z)\vartheta_4^4(z)
\]

\[
= \vartheta_3^8(z) + \vartheta_4^4(z)[\vartheta_4^4(z) - \vartheta_3^4(z)]
\]

\[
= \vartheta_3^8(z) - \vartheta_3^4(z)\vartheta_4^4(z)
\]

Therefore \( \psi_8 \mapsto \vartheta_3^8 - \vartheta_3^4\vartheta_4^4 \).

The image of \( \xi_{24} \) becomes,

\[
(\vartheta_3(2z))^4(\vartheta_2(2z))^4((\vartheta_3(2z))^4 - (\vartheta_2(2z))^4)
\]

\[
= (\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_2^2(z))^2(\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_2^2(z))^2([\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_2^2(z)]^2 - (\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_2^2(z))^2)^4
\]

\[
= \frac{1}{16}\vartheta_3^8(z)\vartheta_2^8(z)[\vartheta_4^4(z) - \vartheta_3^4(z)]^2
\]

\[
= \frac{1}{16}\vartheta_2^8(z)\vartheta_3^8(z)\vartheta_4^8(z)
\]

Therefore \( \xi_{24} \mapsto \frac{1}{16}\vartheta_2^8\vartheta_3^8\vartheta_4^8 \).

**Lemma 5.** Let \( C \) be a singly even code with weight enumerator \( W_C(x, y) \). Then the theta series of its corresponding lattice \( \Lambda_C \) is given by,

\[
W_C(x, y) \in \mathbb{C}[\psi_2, \xi_8]
\]

where \( \psi_2 = x^2 + y^2 \) and \( \xi_8 = x^2y^2(x^2 - y^2)^2 \)

**Lemma 6.** Under the map \( x \mapsto \vartheta_3(2z), y \mapsto \vartheta_2(2z) \), we have

\[
\psi_2 \mapsto \vartheta_3^2
\]

\[
\xi_8 \mapsto \frac{1}{4}\vartheta_3^4\vartheta_4^4 - \frac{1}{4}\vartheta_4^8
\]

**Proof.** Consider the following Jacobi identities found in [11],

\[
\vartheta_3^2(z) + \vartheta_2^2(z) = 2\vartheta_3^2(2z)
\]

\[
\vartheta_3^2(z) - \vartheta_2^2(z) = 2\vartheta_2^2(2z)
\]

\[
\vartheta_2^4(z) + \vartheta_4^4(z) = 2\vartheta_3^4(z)
\]

By Lemma 4 we have \( \psi_2 = x^2 + y^2 \) and \( \xi_8 = x^2y^2(x^2 - y^2)^2 \).

Under the map shown, we have the following:

\[
\psi_2 \mapsto (\vartheta_3(2z))^2 + (\vartheta_2(2z))^2
\]

(6.4)

32
\[
\xi_8 \mapsto \vartheta_3(2z)^2 \vartheta_2(2z)^4 ((\vartheta_3(2z))^4 - (\vartheta_2(2z))^4) \tag{6.5}
\]

The image of \(\psi_2\) becomes,
\[
(\vartheta_3(2z))^2 + (\vartheta_2(2z))^2 = \left(\frac{1}{2} \vartheta_3^2(z) + \frac{1}{2} \vartheta_4^2(z)\right) + \left(\frac{1}{2} \vartheta_3^2(z) - \frac{1}{2} \vartheta_4^2(z)\right)
\]

Therefore \(\psi_2 \mapsto \vartheta_3^2\).

The image of \(\xi_8\) becomes,
\[
(\vartheta_3(2z))^2(\vartheta_2(2z))^2 ((\vartheta_3(2z))^2 - (\vartheta_2(2z))^2)^2
\]
\[
= \left(\frac{1}{2} \vartheta_3^2(z) + \frac{1}{2} \vartheta_4^2(z)\right)\left(\frac{1}{2} \vartheta_3^2(z) - \frac{1}{2} \vartheta_4^2(z)\right)\left(\frac{1}{2} \vartheta_3^2(z) + \frac{1}{2} \vartheta_4^2(z)\right) - \left(\frac{1}{2} \vartheta_3^2(z) - \frac{1}{2} \vartheta_4^2(z)\right)^2
\]
\[
= \left(\frac{1}{4} \vartheta_3^4(z) - \frac{1}{4} \vartheta_4^4(z)\right)\left(\vartheta_3^4(z)\right)
\]
\[
= \frac{1}{4} \vartheta_3^4 \vartheta_4^4 - \frac{1}{4} \vartheta_8^8
\]

Therefore \(\xi_8 \mapsto \frac{1}{4} \vartheta_3^4 \vartheta_4^4 - \frac{1}{4} \vartheta_8^8\).

\[\blacksquare\]

6.2 Singly even code of length 24 satisfies the Belfiore-Solé Conjecture

In Chapter 5 weight enumerator for the singly even code of length 24 and minimum distance 6 is given as,
\[
W_{C_{24}}(1, y) = 1 + 64y^6 + 375y^8 + 960y^{10} + 1296y^{12} + \ldots \tag{6.6}
\]

where \(x=1\). Now, binary self-dual codes \(C\) of length 24 have an associated weight enumerator that reads as, \(x^{24} + W_2x^{22}y^2 + W_4x^{20}y^4 + \ldots + y^{24}\).

Hence, putting back the variable \(x\) into Equation 6.6, we find the weight enumerator of the length 24 code is given by,
\[
W_{C_{24}}(x, y) = x^{24} + 64x^{18}y^6 + 375x^{16}y^8 + 960x^{14}y^{10} + 1296x^{12}y^{12} + \ldots
\]

Note that only codewords of weight divisible by 2 exist since it is a singly even code (i.e. Type I). By Lemma 4 in section 6.1, \(W_{C_{24}}\) is a polynomial that can be written in terms of \(\psi_2\) and \(\xi_8\) and since \(W_{C_{24}}\) is homogenous, it is easy to see that only powers \(\psi_2^{a} \xi_8^{b}\) will appear, where \(2a + 8b = 24\).
$$W_{C_{24}} = a_0 \psi_2^{12} + a_1 \xi_8 \psi_2^8 + a_2 \xi_8^2 \psi_2^4 + a_3 \xi_8^3$$
$$= a_0 (x^2 + y^2)^{12} + a_1 x^2 y^2 (x^2 - y^2)^2 (x^2 + y^2)^8$$
$$+ a_3 x^4 y^4 (x^2 - y^2)^4 (x^2 + y^2)^4 + a_3 x^6 y^6 (x^2 - y^2)^6$$

Expanding and collecting the weight enumerator becomes,

$$W_{C_{24}} = a_0 x^{24} + (12a_0 + a_1) x^{22} y^2 + (66a_0 + 6a_1 + a_2) x^{20} y^4 + (220a_0 + 13a_1 + a_3) x^{18} y^6$$
$$+ (495a_0 + 8a_1 - 4a_2 - 6a_3) x^{16} y^8 + (792a_0 - 14a_1 + 15a_3) x^{14} y^{10}$$
$$+ (924a_0 - 28a_1 + 6a_2 - 20a_3) x^{12} y^{12} + (792a_0 - 14a_1 + 15a_3) x^{10} y^{14}$$
$$+ (495a_0 + 8a_1 - 4a_2 - 6a_3) x^8 y^{16} + (220a_0 + 13a_1 + a_3) x^6 y^{18}$$
$$+ (66a_0 + 6a_1 + a_2) x^4 y^{20} + (12a_0 + a_1) x^2 y^{22} + a_0 y^{24}$$

Now we use the weight enumerator polynomial given by Conway and Sloane to set up a system of equations that will help us solve for $a_i$

$$a_0 = 1$$
$$12a_0 + a_1 = 0$$
$$66a_0 + 6a_1 + a_2 = 0$$
$$220a_0 + 13a_1 + a_3 = 64$$

Solving for this system of linear equations we get,

$$a_0 = 1$$
$$a_1 = -12$$
$$a_2 = 6$$
$$a_3 = 0$$

Therefore our weight enumerator polynomial becomes,

$$W_{C_{24}} = 6 \xi_8^2 \psi_2^4 - 12 \xi_8 \psi_2^8 + \psi_2^{12}$$

Mapping $W_{C_{24}}$ into lattices we get,

$$\Theta_{C_{24}} = \vartheta_3^{24} - 3 \vartheta_3^{20} \vartheta_4^4 + \frac{27}{8} \vartheta_3^{16} \vartheta_4^8 - \frac{3}{4} \vartheta_3^{12} \vartheta_4^{12} + \frac{3}{8} \vartheta_3^8 \vartheta_4^{16}$$

Since the theta series for $\mathbb{Z}^{24}$ is $\vartheta_3^{24}$, then the corresponding secrecy function for a lattice obtained from a singly even code of length 24 is,

$$\Xi_{C_{24}} = \frac{\vartheta_3^{24}}{\vartheta_3^{24}} = \left( \frac{3 \vartheta_3^{16}}{8 \vartheta_3^4} - \frac{3 \vartheta_3^{12}}{4 \vartheta_3^4} + \frac{27 \vartheta_3^8}{8 \vartheta_3^4} - \frac{3 \vartheta_3^4}{\vartheta_3^4} + 1 \right)^{-1}$$

Since we have that $\zeta = \frac{\vartheta_3^4}{\vartheta_3^4}$, then we can rewrite the secrecy function as,
\[ \Xi_{c_{24}} = \left( -\frac{3}{4} \zeta^{3/2} + \frac{3}{8} \zeta^2 + \frac{27}{8} \zeta - 3\sqrt{\zeta} + 1 \right)^{-1} \]

As summarized in section 6.1 if the function \( f \) is decreasing on the interval \([0, \frac{1}{4}]\), then the secrecy function attains its maximum at \( y = 1 \), and thus satisfies the conjecture.

As shown in the graph above \( f \) does indeed decrease on this interval and thus implies that singly even codes of length 24 with minimal distance 6 satisfy the Belfiore and Solé conjecture.

6.3 Wolfram Mathematica

The computation for each lattice of length \( n \) can be a bit excessive and so, in order to provide more rapid results we used Wolfram Mathematica to construct a program that mimicked the approach shown in section 6.2.

Within the program we define the function WEpolyinIIpsi\( x_i \) for doubly even codes, and WEpolyinIpsi\( x_i \) for singly even codes. This will be our main function and will obtain a nesting of functions that rely only on four inputs. These inputs are,

- The length of the code
- The degree of \( \psi \)
- The degree of \( \xi \)
- The values of \( W_i \)

Since the code for singly even and doubly even codes parallel each other, we will look only at the doubly even code and refer to the singly even code when it differs. The program will print 8 different sections and thus we will break the code into these sections and give a brief explanation to their role. If one would like to obtain further analysis of each function used in this program, it can be found in [14]. Without loss
of generality we will be examining the doubly even [48,k,12] code $C$.

**Part 1: Code**

```mathematica
WEpolyinIpsixi[n_, b_, c_, values_] := Module[{},
Quiet[x = .];
Quiet[y = .];
Quiet[Do[Subscript[a, i - 1] = ., {i, Length[values]}]]; 
Quiet[ψ8 = .];
Quiet[ξ24 = .];
Quiet[Subscript[ϑ, 2] = .];
Quiet[Subscript[ϑ, 3] = .];
Quiet[Subscript[ϑ, 4] = .];
Quiet[s = .];
```

The first line defines the function we will be using and the inputs it will require. Notice that each variable input has an underscore immediately after, this defines this slot as a variable. We define our $\text{WEpolyinIpsixi}$ as a `Module` function. This allows us to be more creative with our computations without restrictions, that is, we can do multiple computations in a form of a loop without error. Variables that we will need later in the computation are defined with “$=$” which allows us to carry the variable until we desire to input a value. This is done with variables that are constant from length to length. Since computation is needed before input of the value, we refrain from simply defining it as the constant. For simplicity, we minimized the number of inputs required from the user and thus the variables defined as “$=$.” will not be asked by the program. The variables $\psi$ and $\xi$ vary from doubly even codes and singly even codes, for example, $\psi$ is of degree 8 and $\xi$ is degree 24, but in singly even codes we will be using $\psi$ and $\xi$ of degree 2 and 8 respectively. Finally the `Quiet` command removed any excess information the program prints out during the output of the program.

**Part 2: Code**

```mathematica
Print[Style[Weight enumerator polynomial in terms of $\xi$ and $\psi$, Bold]];
Print[Row[Riffle[Table[(Subscript[a, z]), \{z, Range[0, n/c, 1]\}] * ((Subscript[ψ, b])^((Range[n/b, 0, -c/b])) * ((Subscript[ξ, c])^((Range[0, n/c, 1]))), "+" )]];
```

**Part 2: Print**

Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_8^5 + a_1\xi_{24}\psi_8^2 + a_2\xi_{24}^2$$
The **Print** function prints anything in its brackets. This can be anything from a string of words to computation, here we see both occurring. The **Style** function allows us to stylize the font; in this case we use bold font. The **Range** and **Subscript** functions are self explanatory and can be further explored in [14]. The **Row**, **Riffle**, and **Table** functions created a string of elements which allowed us to view the weight enumerator polynomial in a form that had increasing $a_i$ values. The program does not read this polynomial as a polynomial but as a simply a string of characters and cannot do any computation with it. This print is simply for the fluidity of the output.

Let us take a closer look at the **Table**, **Row**, and **Riffle** functions. Given the **Table** function we get,

$$\{a_0\psi^5, a_1\xi_{24}\psi^8, a_2\xi^2_{24}\}$$

Adding **Riffle** to the command puts the + symbol in every other slot as follows,

$$\{a_0\psi^5, +, a_1\xi_{24}\psi^8, +, a_2\xi^2_{24}\}$$

Finally the **Row** command removes all commas and brackets,

$$a_0\psi^5 + a_1\xi_{24}\psi^8 + a_2\xi^2_{24}$$

Therefore printing the polynomial that will introduce the output.

**Part 3: Code**

```plaintext
Print[Style["Using Lemma 10, we substitute \( \xi \) and \( \psi \) ", Bold]];
Print[Total[Table[((Subscript[a, z]), \{z, Range[0, n/c, 1]\})] \* ((x^8 + 14x^4y^4 + y^8)^4 (Range[n/b, 0, -c/b]) \* (x^4*y^4)*(x^4-y^4)) \^ 4) \^ (Range[0, n/c, 1])]];
```

**Part 3: Print**

Using Lemma 10 we substitute $\xi$ and $\psi$

$$(x^8 + 14x^4y^4 + y^8)^6 a_0 + x^4y^4 (x^4 - y^4)^4 (x^8 + 14x^4y^4 + y^8)^3 a_1 + x^8y^8 (x^4 - y^4)^8 a_2$$

We use the **Table** function on the same sequence of variables as above with the exception that now $\psi$ and $\xi$ are replaced by their polynomial representations. Note that the **Table** function reads the variables as variables and not as strings. In the preceding code the **Row** and **Riffle** functions transferred the variables into strings and not the **Table** function. This again was purely to allow fluidity in the output of the code. The total function allows us to add the coefficients remaining in a math environment. One might ask why not use the **Total** function in the previous step. The reason for this is that the order of the polynomial is determined by the **Total** function and did not allow us to rearrange the terms as we pleased. Since the order of the polynomial can be important to understand how it is constructed, the **Row**, **Riffle**, and **Table** commands were useful to arrange the terms in the appropriate order.
Expanding and collecting the weight enumerator becomes, $a_0 x^{48} + (84 a_0 + a_1) x^{44} y^4 + (2946 a_0 + 38 a_1 + a_2) x^{40} y^8 + (55300 a_0 + 429 a_1 - 8 a_2) x^{36} y^{12} + (588015 a_0 + 712 a_1 + 28 a_2) x^{32} y^{16} + (3392424 a_0 - 7342 a_1 - 56 a_2) x^{28} y^{20} + (8699676 a_0 + 12324 a_1 + 70 a_2) x^{24} y^{24} + (3392424 a_0 - 7342 a_1 - 56 a_2) x^{20} y^{28} + (588015 a_0 + 712 a_1 + 28 a_2) x^{16} y^{32} + (55300 a_0 + 429 a_1 - 8 a_2) x^{12} y^{36} + (2946 a_0 + 38 a_1 + a_2) x^8 y^{40} + (84 a_0 + a_1) x^4 y^{44} + a_0 y^{48}$

A new variable is defined in this section. “CollectedExprs” is the output of a series of functions and so working inside out we begin with the Expand function (the other two have already been defined). As the name implies, this function expands out the polynomial from the previous output. The Collect command collects all like terms and finally the TraditionalForm command arranges the new polynomial with the first term having the highest degree in the variable $x$ and then decreasing with the final coefficient having the lowest degree for $x$ and highest degree for $y$. We provide the following examples for further clarification.

**Example 16. Total Function**

**input:**  $\text{Total} \left[ x, x^2, 3 x y, 5 x, (y + x)^2 \right]$

**output:** $x + x^2 + 3 x y + 5 x + (y + x)^2$

**Example 17. Expand Function**

**input:**  $\text{Expand} \left[ x + x^2 + 3 x y + 5 x + (y + x)^2 \right]$

**output:** $x + x^2 + 3 x y + 5 x + y^2 + 2 x y + x^2$

**Example 18. Collect Function**

**input:**  $\text{Collect} \left[ x + x^2 + 3 x y + 5 x + y^2 + 2 x y + x^2 \right]$

**output:** $6 x + 2 x^2 + 5 x y + y^2$
Example 19. *TraditionalForm Function*

```
input: TraditionalForm[6x + 2x^2 + 5xy + y^2]
output: 2x^2 + 6x + 5xy + y^2
```

**Part 5: Code**

```math
Print["Trimming down the list to the first terms to set up system of equations "];
TrimmedExprs=CollectedExprs /. x^q_ /; q < (n - 4*(Floor[n/c])) \rightarrow 0;
TrimmedExprs=TrimmedExprs /. y^p_/; p > (4*(Floor[n/c])) \rightarrow 0;
Trimmedlistextra = Level[TrimmedExprs, 2];
Trimmedlistfinal = Delete[Trimmedlistextra, -1];
Print[Trimmedlistfinal];
x=1;
y=1;
Answerlist=Solve[Trimmedlistfinal==values ,
Drop[a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_10,a_11, -(12-Length[values]) ]];
Do[Subscript[a,i]=Answerlist[[All,i,2]], {i,Length[values]}];
Print[Drop[a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_10,a_11, -(12-Length[values]) ] ];
```

**Part 5: Print**

```
Trimming down the list to the first terms to set up system of equations
\{x^{48}a_0, x^{44}y^4 (84a_0 + a_1), x^{40}y^8 (2946a_0 + 38a_1 + a_2)\}
\{|1|,\{-84\},\{246\}\}
```

In this section we introduce our third function and perhaps the most complex. We define the new variable “TrimmedExprs” as “CollectedExprs” minus all terms with degree of \(x\) less than \((n-4*(Floor[n/c]))\). This is done by setting those terms equal to 0. Similarly we repeat this for \(y\) terms of degree higher than \((4*(Floor[n/c]))\). We then define “Trimmedlistextra” as the `Level[TrimmedExprs, 2]` function on “TrimmedExprs” which puts each one of our remaining elements in a list and includes the entire polynomial as the last element. We fix this issue by using the `Delete` command and defining this as our “Trimmedlistfinal”

Example 20. \(x^2 + x + 4\)

```
input: Level[x^2 + x + 4, 2]
```
At this point we want to solve for all the coefficients $a_i$. Therefore we need to remove each $x$ and $y$ variable from every monomial in the weight enumerator polynomial in order to set it up as a set of linear system of equations. To do this, we set $x$ and $y$ equal to 1, which isolates our coefficient. For example our $(84a_0 + a_1)x^{44}y^4$ becomes $(84a_0 + a_1)$. The program then sets our coefficients equal to the given $W_i$ at the beginning of our program and sets them equal to each other. Notice that we have $a_0, ..., a_{11}$. We remove $a_i$’s according to the length of the binary code $C$; for our purposes we only went up to $a_{11}$ since our code’s longest weight enumerator polynomial only required up to $a_{11}$. This means that in order to continue with longer weight enumerator polynomials one will have to input a longer sequence of $a_i$’s. Finally using the Solve function, the program solves for the $a_i$’s by setting up a system of equations and solving for each $a_i$.

Part 6: Code

```mathematica
Print[" "];
Print[Style["After substituting a_i values",Bold]];
Aisubbedlist=Total[Table[(Subscript[a,z]),\{z,Range[0,n/c,1]\}]*((Subscript[ψ,b])^(Range[n/b,0,-c/b]))*((Subscript[ξ,c])^(Range[0,n/c,1]))];
AisubbedExprs=Aisubbedlist[[1]];
Print[AisubbedExprs];
```

Part 6: Print

After substituting a_i values,

$$246\xi_{24}^2 - 84\xi_{24}\psi_8^3 + \psi_8^6$$

Once Part 5 solves for each $a_i$ we run the weight enumerator polynomial once more. This will replace the $a_i$’s with the new values. Note that in the beginning of the program we did not define each $a_i$ as a variable and so once it is given a value it becomes that value for the remaining code.

Part 7: Code

```mathematica
Print["Mapping into lattices"];
ψ8=(Subscript[ψ,3]^8−Subscript[ψ,2]^4)*Subscript[ψ,4]^4; 
ξ_{24}=(Subscript[ψ,2]^8−Subscript[ψ,3]^8)*Subscript[ψ,4]^8)/16;
```

```
Part 7: Print

After substituting $a_i$ values $246\zeta_{24}^2 - 84\zeta_{24}\psi_{8}^3 + \psi_{8}^6$

Mapping into lattices

\[
\begin{align*}
\vartheta_3^{48} - 6\vartheta_2\vartheta_3^{40}\vartheta_4^4 + \frac{39}{4}\vartheta_2^5\vartheta_3^3\vartheta_4^8 - \frac{17}{4}\vartheta_2^6\vartheta_4^{12} + \frac{27}{128}\vartheta_2^{16}\vartheta_3^{16}\vartheta_4^{16} - \frac{3}{4}\vartheta_2^{20}\vartheta_3^8\vartheta_4^{20} + \vartheta_2^{24}\vartheta_4^{24} \\
\frac{\vartheta_2^{24}\vartheta_4^{24}}{\vartheta_3^{48}} - \frac{3\vartheta_2^{20}\vartheta_4^{20}}{4\vartheta_3^{40}} + \frac{27\vartheta_2^{16}\vartheta_4^{16}}{128\vartheta_3^{32}} - \frac{17\vartheta_2^{12}\vartheta_4^{12}}{4\vartheta_3^{24}} + \frac{39\vartheta_2^8\vartheta_4^8}{4\vartheta_3^{16}} - \frac{6\vartheta_2^4\vartheta_4^4}{\vartheta_3^8} + 1 \\
\zeta^6 - \frac{3\zeta^5}{4} + \frac{27\zeta^4}{128} - \frac{17\zeta^3}{4} + \frac{39\zeta^2}{4} - 6\zeta + 1
\end{align*}
\]

Notice that until this point $\psi$ and $\xi$ were variables. In this section of the code we define $\psi$ and $\xi$ with their theta series representation given in section 6.1. Since it is easier to look at the inverse of the secrecy function, we use it in part 7 and obtain our second line of this print. Lastly it simplifies the inverse of the secrecy function and defines,

\[\zeta = \frac{\vartheta_2^4\vartheta_4^4}{\vartheta_3^8}\]

Recall that for singly even codes, our $\psi$ and $\xi$ have different theta series representations and different degree.

Part 8: Code

\[\text{Print}["If the function is decreasing on the entire interval, than the secrecy function attains its maximum at } y=1, \text{ and thus satisfies the conjecture "]\];
Part 8: Print

If the function is decreasing on the entire interval, than the secrecy function attains its maximum at $y=1$, and thus satisfies the conjecture.

As described in section 6.2, we wish to know whether the secrecy function attains its maximum at $y = 1$ in the interval $[0, \frac{1}{4}]$. For this we look at the reciprocal function. We conclude this program by graphing the reciprocal of the secrecy function obtained in part 7 for the given $[48, k, 12]$ doubly even self-dual code $C$. We see that the minimum of the reciprocal is in fact at $\frac{1}{4}$, giving us a maximum at $\frac{1}{4}$ for the secrecy function and confirming our results.
A Conjecture for $\ell$-modular Lattices

We now change directions to focus on the generalized Belfiore-Solé conjecture for $\ell$-modular lattices. This chapter begins with a quick introduction of what an $\ell$-modular lattice is and then progresses to the generalized Belfiore and Solé Conjecture. This brings us to the $\ell$-modular secrecy function conjecture which is then explored in the chapter to follow.

7.1 $\ell$-modular lattices

A similarity of norm $\ell$ on the Euclidean vector space $\mathbb{R}^n$ is an $\mathbb{R}$-linear transformation $\sigma: V \rightarrow V$ such that $\sigma(v) \cdot \sigma(w) = \ell \cdot v \cdot w$ for $v, w \in V$, and where $v \cdot w$ denotes the inner product. Viewing such a similarity as $\sqrt{\ell} \circ \frac{1}{\sqrt{\ell}} \sigma$, we see that a similarity of norm $\ell$ is an orthogonal transformation followed by scaling by $\sqrt{\ell}$.

Definition 18. An $\ell$-modular lattice $\Lambda \subseteq \mathbb{R}^n$ is an integral lattice such that $\Lambda = \sigma(\Lambda^\perp)$, where $\sigma$ is a similarity of $\mathbb{R}^n$ of norm $\ell$, and where $\Lambda^\perp$ denotes the dual of $\Lambda$.

One can check that $\ell$ must be an integer as follows: For any $\tilde{u}, \tilde{v} \in \Lambda^\perp$, $\sigma(\tilde{u}) \cdot \sigma(\tilde{v})$ is an integer, since $\sigma(\tilde{u}) \in \Lambda$, as is $\sigma(\tilde{v})$, and as $\Lambda$ is integral. But by the definition of $\sigma$, $\sigma(\tilde{u}) \cdot \sigma(\tilde{v}) = \ell \cdot \tilde{u} \cdot \tilde{v} = \ell u \cdot \tilde{v}$. This shows that $\ell \Lambda^\perp \subseteq \Lambda^\perp \subseteq \Lambda^\perp \subseteq \Lambda$—this last fact that $\Lambda^\perp \subseteq \Lambda$ is standard, and follows from the fact that if $\Lambda$ has a set of basis vectors $e_i$, $i = 1, \ldots, n$, then $\Lambda^\perp$ is generated by the dual basis $f_j$, $j = 1, \ldots, n$ that satisfies $f_j \cdot e_i = \delta_{i,j}$. Now, since $\ell \Lambda^\perp \subseteq \Lambda$, we find that the vector $\ell f_1$, which is now an element of $\Lambda$, must satisfy $\ell f_1 \cdot e_1 \in \mathbb{Z}$, as $\Lambda$ is integral. Hence, $\ell \in \mathbb{Z}$.

Furthermore, the determinant of $\Lambda$ is easily seen to be $\ell^{n/2}$ as follows: From the fact that $\sigma$ represents an orthogonal transform followed by scaling by $\sqrt{\ell}$, we find that the volume of $\Lambda$ satisfies Volume($\Lambda$) = $\ell^{n/2}$Volume($\Lambda^\perp$). Using the fact that Volume($\Lambda$)Volume($\Lambda^\perp$) = 1, and that the determinant of a lattice is the square of its volume, the result follows.

Two examples of $\ell$-modular lattices that will be critical to us are $D(\ell) = \mathbb{Z} \oplus \sqrt{\ell}\mathbb{Z}$, and $C(\ell) = \bigoplus_{k|\ell} \sqrt{k}\mathbb{Z}$. We will prove that $C(\ell)$ is indeed an $\ell$-modular lattice in the next chapter; the proof that $D(\ell)$ is also $\ell$-modular is very similar.

In the following chapter we show that $C(8)$ is indeed an 8-modular lattice which satisfies the modified conjecture described in the next section. As in the unimodular case, $\ell$-modular lattices for $\ell > 1$ are also closely related to theta functions and will be used in our results to come. We restrict ourselves to the positive imaginary plane ($z = iy$ for $y > 0$) and define the generalized conjecture for $\ell$-modular lattices under this restriction.
7.2 Leading to a modified Conjecture

Further work of Belfiore and Solé lead to the following conjecture for $\ell$-modular lattices,

**Conjecture 5** (The Generalized Belfiore-Solé conjecture). The secrecy function,

$$\Xi(y) = \frac{\Theta_{\lambda \mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)}$$

of an $\ell$-modular lattice $\Lambda$ attains its maximum at $y = \frac{1}{\sqrt{\ell}}$.

The lattice $\lambda \mathbb{Z}^n$ denotes the lattice $\mathbb{Z}^n$ with each dimension scaled by a factor of $\lambda = \ell^{1/4}$ (so it now has volume $\lambda = \ell^{n/4}$). Exploration of this conjecture by Ernvall-Hytönen and Sethuraman in [3], showed that the generalized conjecture above is false when $\ell \neq 1$. This conjecture was proven to be false when the 4-modular case gave opposing results. It was proven that the secrecy function of $C^{(4)}$ has a minimum at $y = \frac{1}{\sqrt{4}}$ instead of a maximum at this point.

With this new information, Ernvall-Hytönen and Sethuraman modified the conjecture into was is known as the $\ell$-modular secrecy function conjecture. The lattice $\lambda \mathbb{Z}^n$ in the generalized secrecy function was replaced with the simplest $\ell$-modular lattice $D^{(\ell)} = \mathbb{Z} \oplus \sqrt{\ell} \mathbb{Z}$. It was believed by the authors to be the more reasonable ratio to consider, since it compared two $\ell$-modular lattices instead of a unimodular lattice and an $\ell$-modular lattice.

**Conjecture 6** ($\ell$-modular secrecy function conjecture). Let $\Lambda$ be an $\ell$-modular lattice of dimension $n$. Write $n = k \text{dim} \left( D^{(\ell)} \right)$. Then

$$\Xi_{\ell,\Lambda}(y) = \frac{(\Theta_{D^{(\ell)}}(y))^k}{\Theta_{\Lambda}(y)}$$

defined for $y > 0$, attains its (global) maximum at $\frac{1}{\sqrt{\ell}}$.

Using similar techniques as those used in the counterexample for the generalized conjecture given by Belfiore and Solé, Ernvall-Hytönen and Sethuraman were succesful in proving the $\ell$-modular secrecy function conjecture true for the 4-modular $C^{(4)}$. (They also showed it to be true for certain choices of 2-modular lattices.) In the chapter to follow we explore the $C^{(8)}$ case and prove that the new modified conjecture given by Ernvall-Hytönen and Sethuraman holds true for $C^{(8)}$. In Chapter 9 ahead, we will formulate a conjecture that, if true, will show that the $\ell$-modular secrecy function conjecture is true for all lattices $C^{(\ell)}$, and will verify numerically that our conjecture, and hence the $\ell$-modular secrecy function conjecture as well, are true for $C^{(6)}$, $C^{(10)}$, $C^{(12)}$ and $C^{(14)}$. 

44
7.3 New functions k, l, and M

In [4] we find a connection between theta series and the functions denoted by $k(q)$, $k'(q)$, $k_2(q)$, $l(q)$, $l'(q)$, and $M_2(q)$ where $q = e^{i\pi \tau}$. These functions are defined as follows,

\[
\begin{align*}
    k(q) & = \frac{\vartheta_2^2(q)}{\vartheta_3^2(q)} \\
    k'(q) & = \sqrt{1 - k^2(q)} = \frac{\vartheta_2^2(q)}{\vartheta_3^2(q)} \\
    l(q) & = k(\sqrt{q}) = \frac{\vartheta_2^2(\sqrt{q})}{\vartheta_3^2(\sqrt{q})} \\
    k'(q) & = l'(\sqrt{q}) = \frac{\vartheta_2^2(\sqrt{q})}{\vartheta_3^2(\sqrt{q})} \\
    k_2 & = k(e^{-\pi \sqrt{2}}) \\
    M_2(q) & = \frac{\vartheta_2^2(q)}{\vartheta_3^2(\sqrt{q})}
\end{align*}
\]

(7.1)

The following Jacobi Theta Function identities,

\[
\begin{align*}
    \vartheta_4^4(\tau) & = \vartheta_2^4(\tau) + \vartheta_4^4(\tau) \\
    2\vartheta_3^2(2\tau) & = \vartheta_2^2(\tau) + \vartheta_4^2(\tau) \\
    2\vartheta_2^2(\tau) & = \vartheta_3^2(\tau) - \vartheta_4^2(\tau)
\end{align*}
\]

(7.2)

which can be found in [11], allow us to rewrite $M_2(q)$, $l(q)$, and $k(q)$ as follows,

\[
\begin{align*}
    M_2(q) & = \frac{1}{1 + k(q)} = \frac{1 + l'(q)}{2}, \quad (7.3) \\
    l(q) & = \frac{2\sqrt{k(q)}}{1 + k(q)} \\
    k(q) & = \frac{1 - l'(q)}{1 + l'(q)}.
\end{align*}
\]

(7.4)

With these new functions we are ready to show our results for the $C^{(8)}$ case.
Chapter 8

$C^{(8)}$ satisfies the $\ell$-modular secrecy function conjecture

The proof will be broken down into the following scheme,

1. Show that $\Lambda = C^{(8)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus 2\mathbb{Z} \oplus 2\sqrt{2}\mathbb{Z}$ is an integral lattice.

2. Show that the dual of the lattice $\Lambda = C^{(8)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus 2\mathbb{Z} \oplus 2\sqrt{2}\mathbb{Z}$ is $\Lambda^\perp = \mathbb{Z} \oplus \frac{1}{\sqrt{2}}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2\sqrt{2}}\mathbb{Z}$.

3. Show that $\Lambda = \sqrt{8}S(\Lambda^\perp)$, where $S: \mathbb{R}^4 \rightarrow \mathbb{R}^4$ is an orthogonal transform and thus conclude $C^{(8)}$ is an 8-modular lattice.

4. Set up the 8-modular secrecy function and prove that it attains a max at $y = \frac{1}{\sqrt{8}}$ through various techniques.

**Proof.**

$C^{(8)}$ is a 8-modular integral lattice:

Let $(a_1, \sqrt{2}b_1, 2c_1, 2\sqrt{2}d_1), (a_2, \sqrt{2}b_2, 2c_2, 2\sqrt{2}d_2)$ be arbitrary elements in $C^{(8)}$. Taking the dot product we have,

$$(a_1, \sqrt{2}b_1, 2c_1, 2\sqrt{2}d_1) \cdot (a_2, \sqrt{2}b_2, 2c_2, 2\sqrt{2}d_2) = a_1a_2 + 2b_1b_2 + 4c_1c_2 + 8d_1d_2 \in \mathbb{Z}$$

since $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{Z}$

$$\therefore C^{(8)} \text{ is integral}$$

The dual of the lattice $\Lambda = C^{(8)}$ is $\Lambda^\perp = \mathbb{Z} \oplus \frac{1}{\sqrt{2}}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2\sqrt{2}}\mathbb{Z}$:

Write $T$ for $\mathbb{Z} \oplus \frac{1}{\sqrt{2}}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2\sqrt{2}}\mathbb{Z}$.

$(T \subseteq \Lambda^\perp)$: Consider $(x, \frac{1}{\sqrt{2}}y, \frac{1}{2}w, \frac{1}{2\sqrt{2}}z) \in T$ and $(a, \sqrt{2}b, 2c, 2\sqrt{2}d) \in \Lambda$. Taking the dot product we get,

$$(x, \frac{1}{\sqrt{2}}y, \frac{1}{2}w, \frac{1}{2\sqrt{2}}z) \cdot (a, \sqrt{2}b, 2c, 2\sqrt{2}d) = ax + by + cw + dz \in \mathbb{Z}$$

since $a, b, c, d, x, y, z \in \mathbb{Z}$

$$\therefore T \subseteq \Lambda^\perp.$$

$(\Lambda^\perp \subseteq T)$: Consider $(r, s, t, v) \in \Lambda^\perp$, then for all elements in $\Lambda$ we have that the dot product is in $\mathbb{Z}$. Since we have that $(1, 0, 0, 0), (0, \sqrt{2}, 0, 0), (0, 0, 2, 0)$, and $(0, 0, 0, 2\sqrt{2})$ are in $\Lambda$ then we have that

$$(r, s, t, v) \cdot (1, 0, 0, 0) = r \in \mathbb{Z} \implies r = m \text{ for } m \in \mathbb{Z}$$

46
\[(r, s, t, v) \cdot (0, \sqrt{2}, 0, 0) = \sqrt{2}s \in \mathbb{Z} \implies s = \frac{1}{\sqrt{2}}n \text{ for } n \in \mathbb{Z}\]

\[(r, s, t, v) \cdot (0, 0, 2, 0) = 2t \in \mathbb{Z} \implies t = \frac{1}{2}k \text{ for } k \in \mathbb{Z}\]

\[(r, s, t, v) \cdot (0, 0, 0, 2\sqrt{2}) = 2\sqrt{2}v \in \mathbb{Z} \implies v = \frac{1}{2\sqrt{2}}h \text{ for } h \in \mathbb{Z}\]

so, \((r, s, t, v) = (m, \frac{1}{\sqrt{2}}n, \frac{1}{2}k, \frac{1}{2\sqrt{2}}h) \in T\)

\[\therefore \Lambda^\perp \subseteq T,\]

\[\therefore \Lambda^\perp = \mathbb{Z} \oplus \frac{1}{\sqrt{2}}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2\sqrt{2}}\mathbb{Z}.\]

\[\Lambda = \sqrt{8} \cdot S(\Lambda^\perp):\]

\((\Lambda \subset \sqrt{8} \cdot S(\Lambda^\perp)):\) We define \(S: \mathbb{R}^4 \rightarrow \mathbb{R}^4\) by \(S(a, b, c, d) = (d, c, b, a)\). Since this just permutes the basis vectors, it is clearly an orthogonal transformation.

For \((a, \sqrt{2}b, 2c, 2\sqrt{2}d) \in \Lambda\), consider \((d, \frac{1}{\sqrt{2}}c, \frac{1}{2}b, \frac{1}{2\sqrt{2}}a) \in \Lambda^\perp\), then,

\[\sqrt{8} \cdot S\left((d, \frac{1}{\sqrt{2}}c, \frac{1}{2}b, \frac{1}{2\sqrt{2}}a)\right) = \sqrt{8}\left(\frac{1}{2\sqrt{2}}a, \frac{1}{2}b, \frac{1}{\sqrt{2}}c, d\right) = (a, \sqrt{2}b, 2c, 2\sqrt{2}d)\]

\[\therefore \Lambda \subseteq \sqrt{8} \cdot S(\Lambda^\perp).\]

\((\sqrt{8} \cdot S(\Lambda^\perp) \subseteq \Lambda):\) Take \(\sqrt{8} \cdot S\left((x, \frac{1}{\sqrt{2}}y, \frac{1}{2}w, \frac{1}{2\sqrt{2}}z)\right) \in \sqrt{8} \cdot S(\Lambda^\perp).\)

Since, \(\sqrt{8} \cdot S\left((x, \frac{1}{\sqrt{2}}y, \frac{1}{2}w, \frac{1}{2\sqrt{2}}z)\right) = (z, \sqrt{2}w, 2y, 2\sqrt{2}x) \in \Lambda\)

\[\therefore \sqrt{8} \cdot S(\Lambda^\perp) \subseteq \Lambda,\]

\[\therefore \Lambda = \sqrt{8} \cdot S(\Lambda^\perp).\]

By definition, we have that \(C^{(8)}\) is an 8-modular lattice.

Setting up the \(l\)-modular secrecy function:

For the 8-modular lattice we have that the modified secrecy function is,

\[\Xi_{4, C^{(8)}} = \frac{(\vartheta_3(iy) \vartheta_3(8iy))^4}{\vartheta_3(iy) \vartheta_3(2iy) \vartheta_3(4iy) \vartheta_3(8iy)} = \frac{\vartheta_3(iy) \vartheta_3(iy)}{\vartheta_3(iy) \vartheta_3(iy)}\]

Our goal is to show that \(\Xi_{4, C^{(8)}}\) attains its (global) maximum at \(y = 1/\sqrt{8}\). It will be convenient to work with the square of \(\Xi_{4, C^{(8)}}\). We have
for convenience let \( y' = 2y \). Thus to show \( \Xi \) has maximum at \( y = 1/2\sqrt{2} \) we want to show

\[
f(y') = \frac{\vartheta_3(y'/2i)^2 \vartheta_3(4y'i)^2}{\vartheta_3(y'i)^2 \vartheta_3(2y'i)^2}
\]

has maximum at \( 1/\sqrt{2} \).

A manipulation using the functions (7.1) gives us that, upon writing \( \vartheta_3(iy') \) as \( \vartheta_3(q) \) where \( q = e^{i\pi y'} \) we get,

\[
f(y') = \frac{M_2(q^4)}{M_2(q)}
\]

\[
= \frac{M_2(q^4)}{M_2(q^2)} \cdot \frac{M_2(q^2)}{M_2(q)}
\]

\[
= \frac{2}{2} \cdot \frac{(1 + k'(q^2))(1 + k(q^2))}{(1 + l(q^2))(1 + l'(q^2))}
\]

\[
= \frac{(1 + k'(q^2))(1 + k(q^2)) \left(1 + \frac{2\sqrt{k(q^2)}}{1+k(q^2)}\right)}{(1 + k'(q^2))(1 + k(q^2)) \left(1 + \frac{2\sqrt{k(q^2)}}{1+k(q^2)}\right)}
\]

\[
= \frac{2}{2} \cdot \frac{(1 + k'(q^2))(1 + k(q^2) + 2\sqrt{k(q^2)})}{2(1 + k(q^2))}
\]

\[
= \frac{(1 + \sqrt{1-k^2(q^2)})(1 + k(q^2) + 2\sqrt{k(q^2)})}{2 + 2k(q^2)}.
\]

By setting \( t = \sqrt{k(q^2)} \) and, abusing notation, setting \( f(t) = f(y') \), we have that,

\[
f(t) = \frac{(1 + \sqrt{1-t^4})(1 + t^2 + 2t)}{2 + 2t^2}.
\]

Since \( 0 < k(q^2) < 1 \) then \( 0 < t < 1 \). Our goal is to find the maximum of the function \( f(t) \). Using calculus techniques we consider the derivative of \( f \) and look at the roots of \( f'(t) \). This is done as follows,

\[
f(t) = \frac{(1 + \sqrt{1-t^4})(1 + t^2 + 2t)}{2 + 2t^2} = \frac{h(t)}{g(t)}
\]

By the quotient rule we need to evaluate \( h'(t) \) and \( g'(t) \),

\[
\Xi_{4,C(\nu)}(y)^2 = \frac{\partial_3(yi)^2 \partial_3(8yi)^2}{\partial_3(2yi)^2 \partial_3(4yi)^2}
\]
Evaluating the difference we have,

\[ h'(t) = \frac{1}{2}(1 - t^4)^{-1/2}(-4t^3)(1 + t^2 + 2t) + (1 + \sqrt{1 - t^4})(2t + 2) \]
\[ = -2t^3(1 - t^4)^{-1/2}(1 + t^2 + 2t) + 2t + 2 + 2t(1 - t^4)^{1/2} + 2(1 - t^4)^{1/2} \]
\[ = -2t^3(1 - t^4)^{-1/2} - 2t^5(1 - t^4)^{-1/2} - 4t^4(1 - t^4)^{-1/2} + 2t + 2 \]
\[ + 2t(1 - t^4)^{1/2} + 2(1 - t^4)^{1/2} \]

\[ g'(t) = 4t. \]

Derivative of the top multiplied by the original function of the bottom gives us,

\[ h'(x)g(x) = \frac{-4t^3}{\sqrt{1 - t^4}} - \frac{4t^5}{\sqrt{1 - t^4}} - \frac{8t^4}{\sqrt{1 - t^4}} + \frac{4t\sqrt{1 - t^4}}{\sqrt{1 - t^4}} + \frac{4\sqrt{1 - t^4}}{\sqrt{1 - t^4}} + \frac{4t(1 - t^4)}{\sqrt{1 - t^4}} \]
\[ + \frac{4(1 - t^4)}{\sqrt{1 - t^4}} - \frac{4t^5}{\sqrt{1 - t^4}} - \frac{4t^7}{\sqrt{1 - t^4}} - \frac{8t^6}{\sqrt{1 - t^4}} + \frac{4t^3\sqrt{1 - t^4}}{\sqrt{1 - t^4}} + \frac{4t^2\sqrt{1 - t^4}}{\sqrt{1 - t^4}} \]
\[ + \frac{4t^3(1 - t^4)}{\sqrt{1 - t^4}} + \frac{4t^2(1 - t^4)}{\sqrt{1 - t^4}} \]
\[ = \frac{-8t^7 - 12t^6 - 12t^5 - 12t^4 + 4t^2 + 4t + 4}{\sqrt{1 - t^4}} \]
\[ + \frac{4\sqrt{1 - t^4} + 4t\sqrt{1 - t^4} + 4t^2\sqrt{1 - t^4} + 4t^3\sqrt{1 - t^4}}{\sqrt{1 - t^4}}. \]

Derivative of the bottom multiplied by the original function of the top gives us,

\[ h(x)g'(x) = (1 + \sqrt{1 - t^4})(1 + 2t + t^2)(4t) \]
\[ = 4t + 8t^2 + 4t^3 + 4t\sqrt{1 - t^4} + 8t^2\sqrt{1 - t^4} + 4t^3\sqrt{1 - t^4} \]
\[ = \frac{4t\sqrt{1 - t^4} + 8t^2\sqrt{1 - t^4} + 4t^3\sqrt{1 - t^4} + 4t - 4t^5 + 8t^2 - 8t^6 + 4t^3 - 4t^7}{\sqrt{1 - t^4}}. \]

Evaluating the difference we have,

\[ h'(x)g(x) - h(x)g'(x) = \frac{-8t^7 - 12t^6 - 12t^5 - 12t^4 + 4t^2 + 4t + 4 - 4t}{\sqrt{1 - t^4}} \]
\[ + \frac{4t^5 - 8t^2 + 8t^6 - 4t^3 + 4t^7}{\sqrt{1 - t^4}} \]
\[ + \frac{\sqrt{1 - t^4}(4 + 4t + 4t^2 + 4t^3 - 4t - 8t^2 - 4t^4)}{\sqrt{1 - t^4}} \]
\[ = \frac{-4t^7 - 4t^6 - 8t^5 - 12t^4 - 4t^3 - 4t^2 + 4 + \sqrt{1 - t^4}(-4t^2 + 4)}{\sqrt{1 - t^4}}. \]
Lastly by the quotient rule we evaluate the derivative,

\[
\frac{h'(x)g(x) - h(x)g'(x)}{(g(x))^2} = \frac{-4t^7 - 4t^6 - 8t^5 - 12t^4 - 4t^3 - 4t^2 + 4 + \sqrt{1 - t^4}(-4t^2 + 4)}{\sqrt{1 - t^4}(1 + t^2)^2},
\]

\[\therefore f'(t) = \frac{-4t^7 - 4t^6 - 8t^5 - 12t^4 - 4t^3 - 4t^2 + 4 + \sqrt{1 - t^4}(-4t^2 + 4)}{\sqrt{1 - t^4}(1 + t^2)^2}.\]

To find the roots of \(f'(t)\) it is sufficient to find the roots of the numerator. We will break this down as follows,

Factor by \(-4\)

\[-4 \left( t^7 + t^6 - 2t^5 + 3t^4 + t^3 + t^2 - 1 + \sqrt{1 - t^4}(t^2 - 1) \right)\]

Factor out \((t + 1)\),

\[-4 (1 + t) \left( t^6 + 2t^4 + t^3 + t - 1 + t\sqrt{1 - t^4} - \sqrt{1 - t^4} \right),\]

\[\therefore t = -1 \text{ is a zero.}\]

Recall that if \(x\) is a solution to a given equation \(h(x) = g(x)\), then it must be a solution to \(h(x)^2 = g(x)^2\). Therefore we continue our next approach using the this result as follows,

\[t^6 + 2t^4 + t^3 + t - 1 + t\sqrt{1 - t^4} - \sqrt{1 - t^4} = 0\]

\[t^6 + 2t^4 + t^3 + t - 1 = -t\sqrt{1 - t^4} + \sqrt{1 - t^4}\]

\[t^6 + 2t^4 + t^3 + t - 1 = (1 - t)\sqrt{1 - t^4}.
\]

Here our \(h(x) = t^6 + 2t^4 + t^3 + t - 1\) and our \(g(x) = (1 - t)\sqrt{1 - t^4}\) and so we square both sides and simplify as follows,

\[t^{12} + 4t^{10} + 2t^9 + 4t^8 + 6t^7 - t^6 + 4t^5 - 2t^4 - 2t^3 + t^2 - 2t + 1 = -t^6 + 2t^5 - t^4 - t^2 + 1\]

\[t^{12} + 4t^{10} + 2t^9 + 4t^8 + 6t^7 + 2t^5 - t^4 - 2t^3 = 0.\]

Evaluating this polynomial at \(t = \sqrt{-1 + \sqrt{2}}\) we get,
\[
(\sqrt{-1 + \sqrt{2}})^{12} + 4(\sqrt{-1 + \sqrt{2}})^{10} + 2(\sqrt{-1 + \sqrt{2}})^{9} + 4(\sqrt{-1 + \sqrt{2}})^{8} \\
+ 6(\sqrt{-1 + \sqrt{2}})^{7} + 2(\sqrt{-1 + \sqrt{2}})^{5} - (\sqrt{-1 + \sqrt{2}})^{4} - 2(\sqrt{-1 + \sqrt{2}})^{3} \\
= ((-1 + \sqrt{2})^2)((-1 + \sqrt{2})^4 + 4(-1 + \sqrt{2})^3 + 4(-1 + \sqrt{2})^2 - 1) \\
+ (\sqrt{-1 + \sqrt{2}})(2(-1 + \sqrt{2})^4 + 6(-1 + \sqrt{2})^3 + 2(-1 + \sqrt{2})^2 - 2(-1 + \sqrt{2})) \\
= ((-1 + \sqrt{2})^2)(0) + (\sqrt{-1 + \sqrt{2}})(0) \\
= 0.
\]

Therefore we have that \( t = \sqrt{-1 + \sqrt{2}} \) is a zero of \( t^{12} + 4t^{10} + 2t^{9} + 6t^{7} + 2t^{5} - t^{4} - 2t^{3} \). This polynomial has only one sign change and so by Descartes rule of signs it follows that there can only be at most one positive real root. Since \( \sqrt{-1 + \sqrt{2}} \) is positive this implies that \( t = \sqrt{-1 + \sqrt{2}} \) is the only positive real root. This forces \( t^{6} + 2t^{4} + t^{3} + t - 1 + t\sqrt{1 - t^{4}} - \sqrt{1 - t^{4}} \) to have at most one positive root and if so, it must be at \( t = \sqrt{-1 + \sqrt{2}} \).

Evaluating \( t^{6} + 2t^{4} + t^{3} + t - 1 + t\sqrt{1 - t^{4}} - \sqrt{1 - t^{4}} \) at \( t = \sqrt{-1 + \sqrt{2}} \) we get,

\[
(\sqrt{-1 + \sqrt{2}})^{6} + 2(\sqrt{-1 + \sqrt{2}})^{4} + (\sqrt{-1 + \sqrt{2}})^{3} + ((\sqrt{-1 + \sqrt{2}}) - 1 \\
+ ((\sqrt{-1 + \sqrt{2}})^{2}) \sqrt{1 - (\sqrt{-1 + \sqrt{2}})^{4} - \sqrt{1 - (\sqrt{-1 + \sqrt{2}})^{4}} \\
= -1 + \sqrt{2} + \sqrt{-1 + \sqrt{2}} + (\sqrt{-1 + \sqrt{2})^{3/2} - 1} - \sqrt{-1 + \sqrt{2}} \\
= \sqrt{-1 + \sqrt{2}} + (-1 + \sqrt{2})^{3/2} - \sqrt{-1 + \sqrt{2}} - \sqrt{-1 + \sqrt{2}} \\
= 0.
\]

We conclude that the only real positive root of \( f'(t) \) is \( \sqrt{-1 + \sqrt{2}} \). Lastly by using test points to the left and the right of \( \sqrt{-1 + \sqrt{2}} \) between 0 and 1 we get that,

Test point \( 1/2 \in (0, \sqrt{-1 + \sqrt{2}}) \) gives us \( f'(1/2) = \frac{1}{25}(48 + 6\sqrt{15}) > 0. \)

Test point \( 3/4 \in (\sqrt{-1 + \sqrt{2}}, 1) \) gives us \( f'(3/4) = \frac{-7}{625}(115\sqrt{7} - 64) < 0. \)

Therefore concluding that \( \sqrt{-1 + \sqrt{2}} \) is a maximum for \( f \) and is a unique maximum of \( f \) between 0 and 1.

Since \( t = \sqrt{k(q^{2})} \implies t^{2} = k(q^{2}) \) and so \( k(q^{2}) = -1 + \sqrt{2} \)

In [4] we have that \( k_{2} = k(e^{-\pi\sqrt{2}}) \) is equal to \(-1 + \sqrt{2}\).

Since \( k(q) \) is known to be an injective function, we find what our maximum \( y \) value is by setting \( q^{2} = e^{-\pi\sqrt{2}} \) and so we get that,
\[ q = e^{-\pi \sqrt{2}} \]
\[ q = e^{-\frac{\pi}{\sqrt{2}}} \]

This means that, \( y' = \frac{1}{\sqrt{2}} \). This implies that \( y = \frac{1}{2\sqrt{2}} = \frac{1}{\sqrt{8}} \) and so we have that \( f(t) \) attains its maximum at \( \frac{1}{\sqrt{8}} \) or equivalently \( \Xi_{4,C,(8)} \) attains its maximum at \( \frac{1}{\sqrt{8}} \) thus completing the proof. \[ \blacksquare \]
Chapter 9

Introducing a conjecture for a certain ratio of theta functions

The modified conjecture in Chapter 7 opened further questions regarding \( \ell \)-modular lattices that satisfy the \( \ell \)-modular secrecy function conjecture. Our objective was to find a pattern within the \( \ell \)-modular forms in terms of our function \( k, k', l, l' \) and \( M \) and mimic the approach done for the 4 and 8 modular case and prove that the conjecture was satisfied for all \( \ell \)-modular lattices \( C^{(\ell)} \). Although this was not very successful we encountered a pattern within our theta series representation which lead to the following function defined below.

\[
S_{a,b}(y) = \frac{\vartheta_3(yi) \vartheta_3(abyi)}{\vartheta_3(ayi) \vartheta_3(byi)}, \quad y > 0.
\]

**Theorem 7.**
The square of the \( \ell \)-modular secrecy function of the \( \ell \)-modular lattice \( C^{(\ell)} \) has a representation in terms of products of the functions \( S_{a,b}(y) \) for \( a, b > 0, \ ab = \ell \).

**Proof.**
Recall that \( C^{(\ell)} \) is the direct sum \( \oplus_{d|\ell} \sqrt{d} \mathbb{Z} \), so \( C^{(\ell)} \) is a lattice in \( \mathbb{R}^n \), with \( n \) being the number of divisors of \( \ell \).

**Case 1:** \( \ell \) has an even number of factors
Let \( \ell \) be an integer with an even number of factors. Then the \( \ell \)-modular secrecy function of \( C^{(\ell)} \) can be expressed as follows

\[
\Xi_{\ell, C^{(\ell)}} = \left( \frac{\Theta_{D^{(\ell)}}(yi)}{\Theta_{C^{(\ell)}}(yi)} \right)^{\frac{n}{2}},
\]

since \( n \) is the number of factors of \( \ell \) we have that \( n = 2k \) for \( k \in \mathbb{Z} \). By the way we define \( D^{(\ell)} \), we have \( \dim(D^{(\ell)}) = 2 \) and so,

\[
= \frac{(\vartheta_3(yi) \vartheta_3(\ell yi))^{\frac{2k}{2}}}{\vartheta_3(d_2yi) \vartheta_3(d_3yi) \cdots \vartheta_3(d_{2k-2}yi) \vartheta_3(d_{2k-1}yi) \vartheta_3(\ell yi)},
\]

where \( d_1 = 1, d_{2k} = \ell \) and \( d_i \) are the remaining factors of \( \ell \) in increasing order.

Simplifying we get,

\[
\Xi_{\ell, C^{(\ell)}} = \frac{(\vartheta_3(yi) \vartheta_3(\ell yi))^{k-1}}{\underbrace{\vartheta_3(d_2yi) \vartheta_3(d_3yi) \cdots \vartheta_3(d_{2k-2}yi) \vartheta_3(d_{2k-1}yi)}_{2k-2 \text{ terms}}},
\]

53
and we group them as follows

\[
\frac{\varphi_3(yi)\varphi_3(\ell y)\varphi_3(d_2yi)\varphi_3(d_{2k-1}yi)}{\varphi_3(d_2yi)\varphi_3(d_{2k-1}yi)} \cdot \frac{\varphi_3(yi)\varphi_3(\ell y)\varphi_3(d_3yi)\varphi_3(d_{2k-2}yi)}{\varphi_3(d_3yi)\varphi_3(d_{2k-2}yi)} \cdots \frac{\varphi_3(yi)\varphi_3(\ell y)\varphi_3(d_{k}yi)}{\varphi_3(d_{k}yi)\varphi_3(d_{k+1}yi)}.
\]

Since we have an even number of factors, this implies that every factor corresponds to another factor of \( \ell \) where their product is equal to \( \ell \). Furthermore since the factors of \( \ell \) are ordered in increasing order we have that,

\[
d_2 \cdot d_{2k-1} = \ell \\
d_3 \cdot d_{2k-2} = \ell \\
\vdots \\
d_r \cdot d_{2k-(r-1)} = \ell,
\]

and so,

\[
\Xi_{\ell,C^{(\ell)}} = S_{d_2,d_{2k-1}}(y) \cdot S_{d_3,d_{2k-2}}(y) \cdot \ldots \cdot S_{d_{k-1},d_{k+1}}(y) \cdot S_{d_k,d_{k+1}}(y).
\]

All the more so, \((\Xi_{\ell,C^{(\ell)}})^2\) is a product of functions of the form \(S_{ab}(y)\), with \(ab = \ell\).

Case 2: \( \ell \) has an odd number of factors

Let \( \ell \) be an integer with an even number of factors. Then the \( \ell \)-modular secrecy function of \( C^{(\ell)} \) can be expressed as follows

\[
\Xi_{\ell,C^{(\ell)}} = \frac{(\Theta_{D^{(\ell)}}(yi))^{\dim(D^{(\ell)})}}{\Theta_{C^{(\ell)}}(yi)}
\]

since \( n \) is the number of factors of \( \ell \) we have that \( n = 2k + 1 \) for \( k \in \mathbb{Z} \). By the way we define \( D^{(\ell)} \), we have \( \dim(D^{(\ell)}) = 2 \) and so,

\[
\Xi_{\ell,C^{(\ell)}} = \frac{(\varphi_3(yi)\varphi_3(\ell y))^{2k+1}}{\varphi_3^3(yi)\varphi_3^3(d_2yi)\varphi_3^3(d_3yi)\ldots \varphi_3^3(d_{2k-1}yi)\varphi_3^3(d_{2k}yi)\varphi_3^3(\ell y)}
\]

where \( d_1 = 1, d_{2k+1} = \ell \) and \( d_i \) are the remaining factors of \( \ell \) in increasing order. We square the secrecy function and obtain,

\[
\Xi_{\ell,C^{(\ell)}}^2 = \frac{(\varphi_3^2(yi)\varphi_3^2(\ell y))^{2k+1}}{\varphi_3^6(yi)\varphi_3^6(d_2yi)\varphi_3^6(d_3yi)\ldots \varphi_3^6(d_{2k-1}yi)\varphi_3^6(d_{2k}yi)\varphi_3^6(\ell y)}
\]

\[
= \frac{(\varphi_3^2(yi)\varphi_3^2(\ell y))^{2k-1}}{\varphi_3^6(d_2yi)\varphi_3^6(d_3yi)\ldots \varphi_3^6(d_{2k-1}yi)\varphi_3^6(d_{2k}yi)}
\]

(9.1)
and we group them as follows,

\[
\frac{\varphi_2(y_i) \varphi_2(\ell y_i)}{\varphi_3(d_2 y_i) \varphi_3(d_{2k} y_i)} \cdot \frac{\varphi_2(d_3 y_i) \varphi_3(d_{2k-1} y_i)}{\varphi_3(d_{3} y_i) \varphi_3(d_{2k-2} y_i)} \cdot \ldots \cdot \frac{\varphi_2(d_k y_i) \varphi_3(d_{k+2} y_i)}{\varphi_3(d_k y_i) \varphi_3(d_{k+1} y_i)}
\]

\(k-1\) groups

Since we have an odd number of factors, this implies that \(\ell\) is a perfect square. Furthermore every factor corresponds to another factor of \(\ell\) (except the \(k + 1\) factor) where their product is equal to \(\ell\). Furthermore since the factors of \(\ell\) are ordered in increasing order we have that,

\[
d_2 \cdot d_{2k} = \ell \\
d_3 \cdot d_{2k-1} = \ell \\
\vdots \\
d_k \cdot d_{2k-(r-2)} = \ell 
\]

and so,

\[
d_{k+1} \cdot d_{2k-(k+1-2)} = d_{k+1}^2 = \ell 
\]

Similar to the even case we get that,

\[
\Xi_{\ell,C(\ell)}^2 = S_{d_2,d_{2k}}^2(y) \cdot S_{d_3,d_{2k-1}}^2(y) \cdot \ldots \cdot S_{d_k,d_{k+2}}^2(y) \cdot S_{d_{k+1},d_{k+1}}(y). \quad \blacksquare
\]

With this theorem we considered the following;

Given a finite product of functions \(S_{a_1,b_1}(y) \cdot S_{a_2,b_2}(y) \cdot \ldots\), with \(a_i b_i = \ell\) we have that if each function in this product attains a unique maximum at the same point then the product also attains a unique maximum at that point. Our next interest therefore was to find where exactly each \(S_{a,b}(y)\) attained its maximum.

**Conjecture 8.** \(S_{a,b}(y)\) attains a unique maximum at \(\frac{1}{\sqrt{ab}}\)

This conjecture still remains an open question. If however we can show this to be true, it will follow that the \(\ell\) -modular secrecy function conjecture holds for all the \(\ell\) -modular lattices \(C(\ell)\). We have used Mathematica to provide an illustration to this conjecture. With several test points \(a\) and \(b\) we got the following graphs and calculated their maximum, which can be found below each graph,
Although this does not give us a formal proof to our conjecture, it does strengthen our belief that this conjecture holds true.

9.1 Further examples satisfying the $\ell$-modular conjecture

In our last section we verify that the $\ell$-modular conjecture holds for $C^{(6)}$, $C^{(10)}$, $C^{(12)}$, $C^{(14)}$, and $C^{(16)}$ using Wolfram Mathematica. This will further reinforce our belief that the $\ell$-modular conjecture holds for all $C^{(\ell)}$. 

56
By Theorem 6, \( \Xi_{6,C(6)}(y) = S_{2,3}(y) \).
Graphing this gives us,

![Graph](image1)

This implies that \( \frac{1}{\sqrt{6}} \) is our maximum and therefore \( C^{(6)} \) satisfies the \( \ell \)-modular conjecture.

By Theorem 6, \( \Xi_{10,C(10)}(y) = S_{2,5}(y) \).
Graphing this gives us,

![Graph](image2)

This implies that \( \frac{1}{\sqrt{10}} \) is our maximum and therefore \( C^{(10)} \) satisfies the \( \ell \)-modular conjecture.

By Theorem 6, \( \Xi_{12,C(12)}(y) = S_{2,6}(y)S_{3,4}(y) \).
Graphing this gives us,
This implies that $\frac{1}{\sqrt{12}}$ is our maximum and therefore $C^{(12)}$ satisfies the $\ell$-modular conjecture.

By Theorem 6, $\Xi_{14, C^{(14)}}(y) = S_{2,7}(y)$. Graphing this gives us,

This implies that $\frac{1}{\sqrt{14}}$ is our maximum and therefore $C^{(14)}$ satisfies the $\ell$-modular conjecture.

By Theorem 6, $\Xi_{16, C^{(16)}}^2(y) = S_{2,8}^2(y)S_{4,4}(y)$. Graphing this gives us
This implies that $\frac{1}{\sqrt{16}}$ is our maximum and therefore $C^{(16)}$ satisfies the $\ell$-modular conjecture.
References


Appendix

A.1 Results For Doubly Even Codes

A.1.1 Doubly Even Code of length n=48 and minimal distance d=12

WEpolyinI[48, 8, 24, \{1, 0, 0\}]

Weight enumerator polynomial in terms of \(\xi\) and \(\psi\)

\[ a_0\psi^5 + a_1\xi \psi^2 + a_2\psi^2 \]

Using Lemma 10 we substitute \(\xi\) and \(\psi\)

\[
(x^8 + 14x^4y + y^8)^6a_0 + x^4y(x^4 - y^4)^4(x^8 + 14x^4y + y^8)^3a_1 + x^8y(x^4 - y^4)^8a_2
\]

Expanding and collecting the weight enumerator becomes,

\[
a_0x^{48} + (84a_0 + a_1)x^{44}y^4 + (2946a_0 + 38a_1 + a_2)x^{40}y^8 + (55300a_0 + 429a_1 - 8a_2)x^{36}y^{12} + (588015a_0 + 712a_1 + 28a_2)x^{32}y^{16} + (3392424a_0 - 7342a_1 - 56a_2)x^{28}y^{20} + (8699676a_0 + 12324a_1 + 70a_2)x^{24}y^{24} + (3392424a_0 - 7342a_1 - 56a_2)x^{20}y^{28} + (588015a_0 + 712a_1 + 28a_2)x^{16}y^{32} + (55300a_0 + 429a_1 - 8a_2)x^{12}y^{36} + (2946a_0 + 38a_1 + a_2)x^8y^{40} + (84a_0 + a_1)x^4y^{44} + a_0y^{48}
\]

Trimming down the list to the first terms to set up system of equations

\[
\{x^{48}a_0, x^{44}y^4(84a_0 + a_1), x^{40}y^8(2946a_0 + 38a_1 + a_2)\}
\]

\[
\{\{1\}, \{-84\}, \{246\}\}
\]

After substituting \(a_i\) values

\[ 246\psi^3 - 84\psi^2 + \psi^6 \]

Mapping into lattices

\[
\vartheta_3^{48} - 6\vartheta_2^{46}\vartheta_3^4 + \frac{39}{4}\vartheta_2^8\vartheta_3^6 - \frac{17}{4}\vartheta_2^{12}\vartheta_3^{16} + \vartheta_2^{24}\vartheta_3^{24} - \frac{17\vartheta_2^{12}\vartheta_3^{12}}{4\vartheta_3^{16}} + \frac{27\vartheta_2^{16}\vartheta_3^{8}}{4\vartheta_3^{24}} - \frac{6\vartheta_2^{24}\vartheta_3^{8}}{4\vartheta_3^{24}} + 1
\]

\[
\vartheta_3^6 = \frac{3\vartheta_3^5}{4} + \frac{27\vartheta_3^4}{128} - \frac{17\vartheta_3^3}{4} + \frac{39\vartheta_3^2}{4} - 6\vartheta_3 + 1
\]

61
If the function is decreasing on the entire interval, than the secrecy function attains its maximum at \( y=1 \), and thus satisfies the conjecture.

**A.1.2 Doubly Even Code of length \( n=56 \) and minimal distance \( d=12 \)**

\[ \text{WEpolyinIpsixi}[56,8,24,\{1,0,0\}] \]

Weight enumerator polynomial in terms of \( \xi \) and \( \psi \)

\[ a_0 \psi_8^7 + a_1 \xi_24 \psi_8^4 + a_2 \xi_24^2 \psi_8 \]

Using Lemma in 10 we substitute \( \xi \) and \( \psi \)

\[
(x^8 + 14x^4y^4 + y^8)^7a_0 + x^4y^4(x^4 - y^4)^4(x^8 + 14x^4y^4 + y^8)^4a_1 + x^8y^8(x^4 - y^4)^8(x^8 + 14x^4y^4 + y^8)a_2
\]

Expanding and collecting the weight enumerator becomes,

\[
a_0x^{56} + (98a_0 + a_1)x^{52}y^4 + (4123a_0 + 52a_1 + a_2)x^{48}y^8 + (96628a_0 + 962a_1 + 6a_2)x^{44}y^{12} + (1365161a_0 + 6756a_1 - 83a_2)x^{40}y^{16} + (11679934a_0 + 3055a_1 + 328a_2)x^{36}y^{20} + (56781627a_0 - 89752a_1 - 686a_2)x^{32}y^{24} + (128580312a_0 + 157852a_1 + 868a_2)x^{28}y^{28} + (56781627a_0 - 89752a_1 - 686a_2)x^{24}y^{32} + (11679934a_0 + 3055a_1 + 328a_2)x^{20}y^{36} + (1365161a_0 + 6756a_1 - 83a_2)x^{16}y^{40} + (96628a_0 + 962a_1 + 6a_2)x^{12}y^{44} + (4123a_0 + 52a_1 + a_2)x^8y^{48} + (98a_0 + a_1)x^4y^{52} + a_0y^{56}
\]

Trimming down the list to the first terms to set up sytem of equations

\[
\begin{align*}
\{x^{56}a_0, x^{52}y^4(98a_0 + a_1), x^{48}y^8(4123a_0 + 52a_1 + a_2)\}
\end{align*}
\]

\[
\{\{1\}, \{-98\}, \{973\}\}
\]
After substituting $a_i$ values

$$973\xi_{24}^2\psi_8 - 98\xi_{24}\psi_8^4 + \psi_8^7$$

Mapping into lattices

$$\vartheta_{36}^5 - 7\vartheta_{24}^4\vartheta_{12}^4 + \frac{119}{8}\vartheta_{2}^8\vartheta_{3}^4 - \frac{21}{4}\vartheta_{2}^{12}\vartheta_{3}^{12} - \frac{525}{256}\vartheta_{4}^{16}\vartheta_{4}^8 - \frac{7}{256}\vartheta_{2}^{20}\vartheta_{4}^{16}\vartheta_{4}^{20} -$$

$$\frac{7}{8}\vartheta_{2}^{24}\vartheta_{3}^{24}\vartheta_{4}^{24} - \vartheta_{2}^{28}\vartheta_{4}^{28} - \frac{\vartheta_{2}^{28}\vartheta_{4}^{28}}{\vartheta_{3}^{36}} + \frac{7\vartheta_{2}^{24}\vartheta_{4}^{24}}{8\vartheta_{3}^{36}} - \frac{7\vartheta_{2}^{20}\vartheta_{4}^{20}}{256\vartheta_{3}^{36}} + \frac{525\vartheta_{2}^{16}\vartheta_{4}^{16}}{256\vartheta_{3}^{36}} - \frac{21\vartheta_{2}^{12}\vartheta_{4}^{12}}{256\vartheta_{3}^{36}} + \frac{119\vartheta_{2}^{8}\vartheta_{4}^{4}}{8\vartheta_{3}^{16}} - \frac{7\vartheta_{2}^{4}\vartheta_{4}^{4}}{\vartheta_{3}^{8}} + 1$$

$$-\zeta^7 + \frac{7\zeta^6}{8} - \frac{77\zeta^5}{256} + \frac{525\zeta^4}{256} - \frac{21\zeta^3}{2} + \frac{119\zeta^2}{8} - 7\zeta + 1$$

If the function is decreasing on the entire interval, then the secrecy function attains its maximum at $y=1$, and thus satisfies the conjecture

![Graph showing a decreasing function](image)

**A.1.3 Doubly Even Code of length $n=64$ and minimal distance $d=12$**

WEpolyinIIpsixi[64,8,24,\{1,0,0\}] 

Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_8^8 + a_1\xi_{24}\psi_8^5 + a_2\xi_{24}^2\psi_8^2$$

Using Lemma 10 we substitute $\xi$ and $\psi$

$$(x^8 + 14x^4y^4 + y^8)^8a_0 + x^4y^4(x^4 - y^4)^4(x^8 + 14x^4y^4 + y^8)^5a_1 + x^8y^8(x^4 - y^4)^8(x^8 + 14x^4y^4 + y^8)^2a_2$$

Expanding and collecting the weight enumerator becomes,
(a_0 x^{64} + (112a_0 + a_1)x^{60} y^4 + (5496a_0 + 66a_1 + a_2)x^{56} y^8 + (154448a_0 + 1691a_1 + 20a_2)x^{52} y^{12} + (2722076a_0 + 20276a_1 + 2a_2)x^{48} y^{16} + (3088816a_0 + 98601a_1 - 828a_2)x^{44} y^{20} + (221665864a_0 - 40226a_1 + 3823a_2)x^{40} y^{24} + (935203024a_0 - 1095621a_1 - 8408a_2)x^{36} y^{28} + (191368762a_0 + 2030424a_1 + 10780a_2)x^{32} y^{32} + (935203024a_0 - 1095621a_1 - 8408a_2)x^{28} y^{36} + (221665864a_0 - 40226a_1 + 3823a_2)x^{24} y^{40} + (3088816a_0 + 98601a_1 - 828a_2)x^{20} y^{44} + (2722076a_0 + 20276a_1 + 2a_2)x^{16} y^{48} + (154448a_0 + 1691a_1 + 20a_2)x^{12} y^{52} + (5496a_0 + 66a_1 + a_2)x^8 y^{56} + (112a_0 + a_1)x^4 y^{60} + a_0 y^{64}

Trimming down the list to the first terms to set up system of equations

\{x^{64}a_0, x^{60}y^4(112a_0 + a_1), x^{56}y^8(5496a_0 + 66a_1 + a_2)\}

\{\{1\}, \{-112\}, \{1896\}\}

After substituting a_i values

$$1896\xi_2^2 \psi_8^2 - 112\xi_2\psi_8^5 + \psi_8^8$$

Mapping into lattices

$$\vartheta_3^{64} - 8\vartheta_3^{56}\vartheta_3^{4} + 21\vartheta_3^{48}\vartheta_3^{8} - 21\vartheta_3^{12}\vartheta_3^{40}\vartheta_3^{12} + \frac{237}{32}\vartheta_3^{16}\vartheta_3^{32}\vartheta_3^{16} - \frac{13}{16}\vartheta_3^{20}\vartheta_3^{24}\vartheta_3^{20} + \frac{13}{32}\vartheta_3^{24}\vartheta_3^{16}\vartheta_3^{24} - \vartheta_3^{28}\vartheta_3^{8}\vartheta_3^{28} + \vartheta_3^{32}\vartheta_3^{32}\vartheta_3^{32}$$

$$\frac{\vartheta_3^{32}\vartheta_3^{12}}{\vartheta_3^{44}} - \frac{\vartheta_3^{28}\vartheta_3^{8}}{\vartheta_3^{44}} + \frac{13\vartheta_3^{24}\vartheta_3^{4}}{32\vartheta_3^{4}} - \frac{13\vartheta_3^{20}\vartheta_3^{20}}{16\vartheta_3^{3}} + \frac{237\vartheta_3^{16}\vartheta_3^{16}}{32\vartheta_3^{2}} - \frac{21\vartheta_3^{12}\vartheta_3^{12}}{\vartheta_3^{4}} + \frac{21\vartheta_3^{8}\vartheta_3^{8}}{\vartheta_3^{6}} - \frac{8\vartheta_3^{4}\vartheta_3^{4}}{\vartheta_3^{8}} + 1$$

$$\zeta^8 - \zeta^7 + \frac{13\zeta^6}{32} - \frac{13\zeta^5}{16} + \frac{237\zeta^4}{32} - 21\zeta^3 + 21\zeta^2 - 8\zeta + 1$$

If the function is decreasing on the entire interval, then the secrecy function attains its maximum at y=1, and thus satisfies the conjecture
A.2 Results For Singly Even Codes

A.2.1 Singly Even Code of length n=24 and minimal distance d=6

WEpolyinIpsixi[24,2,8,\{1,0,0,64\}] 

Weight enumerator polynomial in terms of $\xi$ and $\psi$

\[ a_0\psi^8 + a_1\xi^8\psi^2 + a_2\xi^2\psi^4 + a_3\xi^3 \]

Using lemma we substitute $\xi$ and $\psi$

\[(x^2+y^2)^{12}a_0 + x^2y^2(x^2-y^2)^2a_1 + x^4y^4(x^2-y^2)^4a_2 + x^6y^6(x^2-y^2)^6a_3 \]

Expanding and collecting the weight enumerator becomes,

\[ a_0x^{24} + (12a_0 + a_1)x^{22}y^2 + (66a_0 + 6a_1 + a_2)x^{20}y^4 + (220a_0 + 13a_1 + a_3)x^{18}y^6 + \]

\[(495a_0 + 8a_1 - 4a_2 - 6a_3)x^{16}y^8 + (792a_0 - 14a_1 + 15a_3)x^{14}y^{10} + (924a_0 - 28a_1 + \]

\[ 6a_2 - 20a_3)x^{12}y^{12} + (792a_0 - 14a_1 + 15a_3)x^{10}y^{14} + (495a_0 + 8a_1 - 4a_2 - 6a_3)x^8y^{16} + \]

\20a_0 + 13a_1 + a_3)x^6y^{18} + (66a_0 + 6a_1 + a_2)x^4y^{20} + (12a_0 + a_1)x^2y^{22} + a_0y^{24} \]

Trimming down the list to the first terms to set up system of equations

\[
\{x^{24}a_0, x^{22}y^2(12a_0 + a_1), x^{20}y^4(66a_0 + 6a_1 + a_2), x^{18}y^6(220a_0 + 13a_1 + a_3)\} \\
\{\{1\}, \{-12\}, \{6\}, \{0\}\}
\]

After substituting $a_i$ values

\[ 6\xi^2\psi^2 - 12\xi\psi^8 + \psi^{12} \]

Mapping into lattices

\[ \psi^2_3 - 3\psi_3^2 \psi_4^4 + \frac{27}{8} \psi_4^{16} \psi_4^8 - \frac{3}{4} \psi_4^{12} \psi_4^4 + \frac{3}{8} \psi_4^8 \psi_4^16 \]

\[ \frac{3\psi_4^{16}}{8\psi_4^8} - \frac{3\psi_4^{12}}{4\psi_4^4} + \frac{27}{8} \psi_4^8 - \frac{3}{4} \psi_4^4 + 1 \]

\[ -\frac{3\psi_4^{1/2}}{4} + \frac{3\psi_4}{8} + \frac{27}{8} \psi_4 - 3\sqrt{2} + 1 \]

If the function is decreasing on the entire interval, than the secrecy function attains
its maximum at $y=1$, and thus satisfies the conjecture
A.2.2 Singly Even Code of length $n=32$ and minimal distance $d=8$

$\text{WEpolyinIpsixi}[32,2,8,\{1,0,0,0,364\}]$

Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^{16} + a_1\xi_8\psi_2^{12} + a_2\xi_8^2\psi_2^8 + a_3\xi_8^3\psi_2^4 + a_4\xi_8^4$$

Using lemma we substitute $\xi$ and $\psi$

$$(x^2 + y^2)^{16}a_0 + x^2y^2(x^2 - y^2)^2(x^2 + y^2)^{12}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{8}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{4}a_3 + x^8y^8(x^2 - y^2)^8a_4$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{32} + (16a_0 + a_1)x^{30}y^2 + (120a_0 + 10a_1 + a_2)x^{28}y^4 + (560a_0 + 43a_1 + 4a_2 + a_3)x^{26}y^6 + (1820a_0 + 100a_1 + 2a_2 - 2a_3 + a_4)x^{24}y^8 + (4368a_0 + 121a_1 - 12a_2 - 3a_3 - 8a_4)x^{22}y^{10} + (8008a_0 + 22a_1 - 17a_2 + 8a_3 + 28a_4)x^{20}y^{12} + (11440a_0 - 165a_1 + 8a_2 + 2a_3 - 56a_4)x^{18}y^{14} + (12870a_0 - 264a_1 + 28a_2 - 12a_3 + 70a_4)x^{16}y^{16} + (11440a_0 - 165a_1 + 8a_2 + 2a_3 - 56a_4)x^{14}y^{18} + (8008a_0 + 22a_1 - 17a_2 + 8a_3 + 28a_4)x^{12}y^{20} + (4368a_0 + 121a_1 - 12a_2 - 3a_3 - 8a_4)x^{10}y^{22} + (1820a_0 + 100a_1 + 2a_2 - 2a_3 + a_4)x^8y^{24} + (560a_0 + 43a_1 + 4a_2 + a_3)x^6y^{26} + (120a_0 + 10a_1 + a_2)x^4y^{28} + (16a_0 + a_1)x^2y^{30} + a_0y^{32}$$

Trimming down the list to the first terms to set up system of equations

$$\{x^{32}a_0, x^{30}y^2(16a_0 + a_1), x^{28}y^4(120a_0 + 10a_1 + a_2), x^{26}y^6(560a_0 + 43a_1 + 4a_2 + a_3), x^{24}y^8(1820a_0 + 100a_1 + 2a_2 - 2a_3 + a_4)\}$$

$$\{\{1\}, \{-16\}, \{40\}, \{-32\}, \{0\}\}$$

After substituting $a_i$ values
\[-32 \xi^3 \psi^4 + 40 \xi^2 \psi^8 - 16 \xi \psi^{12} + \psi^{16}\]

Mapping into lattices
\[
\vartheta_3^{32} - 4 \vartheta_3^{28} \vartheta_4^4 + \frac{13}{2} \vartheta_3^{24} \vartheta_4^8 - \frac{11}{2} \vartheta_3^{20} \vartheta_4^{12} + 4 \vartheta_3^{16} \vartheta_4^{16} - \frac{3}{2} \vartheta_3^{12} \vartheta_4^{20} + \frac{1}{2} \vartheta_3^{8} \vartheta_4^{24}
\]
\[
\frac{\vartheta_3^{24}}{2 \vartheta_4^{24}} - \frac{3 \vartheta_3^{20}}{2 \vartheta_4^{20}} + \frac{4 \vartheta_4^{16}}{2 \vartheta_4^6} - \frac{11 \vartheta_4^{12}}{2 \vartheta_4^6} + \frac{13 \vartheta_4^8}{2 \vartheta_4^6} - \frac{4 \vartheta_4^4}{\vartheta_4^2} + 1 \left(-\frac{3 \psi^{3/2}}{2} - \frac{\xi^3}{2} + 4 \xi^2 + \frac{13 \psi}{2} - 4 \sqrt{\psi} + 1\right)
\]

If the function is decreasing on the entire interval, than the secrecy function attains its maximum at \(y=1\), and thus satisfies the conjecture.

\[\text{A.2.3 Singly Even Code of length } n=40 \text{ and minimal distance } d=8\]

For this case note that we have two candidates for weight enumerator polynomial of a type I length 40 code. We provide results for both polynomials, and thus verifying that type I codes of length 40 and minimal distance 8 satisfy the conjecture.

- \(\text{WEpolyinIpsixi}[40,2,8,\{1,0,0,0,125,1664\}]\)

Weight enumerator polynomial in terms of \(\xi\) and \(\psi\)
\[
a_0 \psi_2^{20} + a_1 \xi \psi_2^{16} + a_2 \xi^2 \psi_2^{12} + a_3 \xi^3 \psi_2^{8} + a_4 \xi^4 \psi_2^{4} + a_5 \xi^5
\]

Using lemma we substitute \(\xi\) and \(\psi\)
\[
(x^2 + y^2)^{20} a_0 + x^2 y^2 (x^2 - y^2)^2 (x^2 + y^2)^{16} a_1 + x^4 y^4 (x^2 - y^2)^4 (x^2 + y^2)^{12} a_2 + x^6 y^6 (x^2 - y^2)^6 (x^2 + y^2)^8 a_3 + x^8 y^8 (x^2 - y^2)^8 (x^2 + y^2)^4 a_4 + x^{10} y^{10} (x^2 - y^2)^{10} a_5
\]

Expanding and collecting the weight enumerator becomes,
Trimming down the list to the first terms to set up system of equations

\[
\{x^{40}a_0, x^{38}y^2(20a_0 + a_1), x^{36}y^4(190a_0 + 14a_1 + a_2), x^{34}y^6(1140a_0 + 89a_1 + 8a_2 + a_3), x^{32}y^8(4845a_0 + 336a_1 + 24a_2 + 2a_3 + a_4), x^{30}y^{10}(15504a_0 + 820a_1 + 24a_2 - 5a_3 - 4a_4 + a_5)\}
\]

\[\{1\}, \{-20\}, \{90\}, \{-80\}, \{0\}, \{0\}\]

After substituting \(a_i\) values

\[-80\xi_8^3\psi_2 + 90\xi_8^2\psi_1^{12} - 20\xi_8\psi_1^{16} + \psi_2^{20}\]

Mapping into lattices

\[\begin{align*}
\partial_3^{40} - 5\partial_3^{36}\partial_4 + \frac{85}{8}\partial_3^{32}\partial_4^8 - \frac{25}{2}\partial_3^{28}\partial_4^{12} + \frac{75}{8}\partial_3^{24}\partial_4^{16} - \frac{15}{4}\partial_3^{20}\partial_4^{20} + \frac{5}{4}\partial_3^{16}\partial_4^{24} \\
\frac{5\partial_3^{24}}{4\partial_4^{24}} - \frac{15\partial_3^{20}}{4\partial_4^{20}} + \frac{75\partial_3^{16}}{8\partial_4^{16}} - \frac{25\partial_3^{12}}{2\partial_4^{12}} + \frac{85\partial_3^{8}}{8\partial_4^{8}} - \frac{5\partial_3^{4}}{\partial_4^{4}} + 1 \\
-\frac{15\zeta^{3/2}}{4} - \frac{25\zeta^{3/2}}{2} + \frac{5\zeta}{4} + \frac{75\zeta^2}{8} + \frac{85\zeta}{8} - 5\sqrt{\zeta} + 1
\end{align*}\]

If the function is decreasing on the entire interval, than the secrecy function attains its maximum at \(y=1\), and thus satisfies the conjecture.
Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^{20} + a_1\xi_8\psi_2^{16} + a_2\xi_8^2\psi_2^{12} + a_3\xi_8^3\psi_2^8 + a_4\xi_8^4\psi_2^4 + a_5\xi_8^5$$

Using lemma we substitute $\xi$ and $\psi$

$$(x^2 + y^2)^{10}a_0 + x^2y^2(x^2 - y^2)^{16}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{12}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{8}a_3 + x^8y^8(x^2 - y^2)^8(x^2 + y^2)^{4}a_4 + x^{10}y^{10}(x^2 - y^2)^{10}a_5$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{40} + (20a_0 + a_1)x^{38}y^2 + (190a_0 + 14a_1 + a_2)x^{36}y^4 + (1140a_0 + 89a_1 + 8a_2 + a_3)x^{34}y^6 + (4845a_0 + 336a_1 + 24a_2 + 2a_3 + a_4)x^{32}y^8 + (15504a_0 + 820a_1 + 24a_2 - 5a_3 - 4a_4 + a_5)x^{30}y^{10} + (38760a_0 + 128a_1 - 36a_2 - 12a_3 + 2a_4 - 10a_5)x^{28}y^{12} + (77520a_0 + 1092a_1 - 120a_2 + 9a_3 + 12a_4 + 45a_5)x^{26}y^{14} + (125970a_0 - 208a_1 - 88a_2 + 30a_3 - 17a_4 - 120a_5)x^{24}y^{16} + (167960a_0 - 2002a_1 + 88a_2 - 5a_3 - 8a_4 + 210a_5)x^{22}y^{18} + (184756a_0 - 2860a_1 + 198a_2 - 40a_3 + 28a_4 - 252a_5)x^{20}y^{20} + (167960a_0 - 2002a_1 + 88a_2 - 5a_3 - 8a_4 + 210a_5)x^{18}y^{22} + (125970a_0 - 208a_1 - 88a_2 + 30a_3 - 17a_4 - 120a_5)x^{16}y^{24} + (77520a_0 + 1092a_1 - 120a_2 + 9a_3 + 12a_4 + 45a_5)x^{14}y^{26} + (38760a_0 + 128a_1 - 36a_2 - 12a_3 + 2a_4 - 10a_5)x^{12}y^{28} + (15504a_0 + 820a_1 + 24a_2 - 5a_3 - 4a_4 + a_5)x^{10}y^{30} + (4845a_0 + 336a_1 + 24a_2 + 2a_3 + a_4)x^8y^{32} + (1140a_0 + 89a_1 + 8a_2 + a_3)x^6y^{34} + (190a_0 + 14a_1 + a_2)x^4y^{36} + (20a_0 + a_1)x^2y^{38} + a_0y^{40}$$

Trimming down the list to the first terms to set up sytem of equations

$$\{x^{40}a_0, x^{38}y^2(20a_0 + a_1), x^{36}y^4(190a_0 + 14a_1 + a_2), x^{34}y^6(1140a_0 + 89a_1 + 8a_2 + a_3), x^{32}y^8(4845a_0 + 336a_1 + 24a_2 + 2a_3 + a_4), x^{30}y^{10}(15504a_0 + 820a_1 + 24a_2 - 5a_3 - 4a_4 + a_5)\}$$

$$\{\{1\}, \{-20\}, \{90\}, \{-80\}, \{160\}, \{0\}\}$$

After substituting $a_i$ values

$$160\xi_8^4\psi_2^4 - 80\xi_8^3\psi_2^8 + 90\xi_8^2\psi_2^{12} - 20\xi_8\psi_2^{16} + \psi_2^{20}$$

Mapping into lattices

$$\frac{\vartheta^{40}_3}{5} - 5\vartheta^{36}_3\vartheta^{4}_4 + \frac{85\vartheta^{32}_3\vartheta^{4}_4}{80\vartheta^{3}_5} - \frac{\vartheta^{36}_3\vartheta^{32}_3\vartheta^{4}_4}{20\vartheta^{3}_5} - \frac{5\vartheta^{28}_3\vartheta^{12}_4}{40\vartheta^{3}_5} + \frac{10\vartheta^{24}_3\vartheta^{16}_4}{20\vartheta^{3}_5} - \frac{25\vartheta^{20}_3\vartheta^{20}_4}{80\vartheta^{3}_5} - \frac{5\vartheta^{16}_3\vartheta^{24}_4}{80\vartheta^{3}_5} - \frac{5\vartheta^{12}_3\vartheta^{28}_4}{80\vartheta^{3}_5} + 1)(-\frac{5\vartheta^{7}_3}{2} - \frac{25\vartheta^{5/2}_3}{4} - \frac{25\vartheta^{3/2}_3}{2} + \frac{5\vartheta^{3}_3}{8} + 5\vartheta^{3} + 10\vartheta^{2} + \frac{5\vartheta^{5/2}_3}{8} - 5\sqrt{\vartheta} + 1}$$
If the function is decreasing on the entire interval, than the secrecy function attains its maximum at $y=1$, and thus satisfies the conjecture.

![Graph showing a decreasing function]

### A.2.4 Singly Even Code of length $n=48$ and minimal distance $d=10$

For this case note that we have two candidates for weight enumerator polynomial of a type I length 48 code. We provide results for both polynomials, and thus verifying that type I codes of length 48 and minimal distance 10 satisfy the conjecture.

- $\text{WEPolyinPsixi}[48,2,8,\{1,0,0,0,704,8976\}]$

Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^{24} + a_1\xi_8\psi_2^{20} + a_2\xi_8^2\psi_2^{16} + a_3\xi_8^3\psi_2^{12} + a_4\xi_8^4\psi_2^8 + a_5\xi_8^5\psi_2^4 + a_6\xi_8^6$$

Using lemma we substitute $\xi$ and $\psi$

$$(x^2 + y^2)^{24}a_0 + x^2y^5(x^2 - y^2)^2(x^2 + y^2)^{20}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{16}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{12}a_3 + x^8y^8(x^2 - y^2)^8(x^2 + y^2)^8a_4 + \cdots$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{48} + (24a_0 + a_1)x^{46}y^2 + (276a_0 + 18a_1 + a_2)x^{44}y^4 + (2024a_0 + 151a_1 + 12a_2 + a_3)x^{42}y^6 + (10626a_0 + 780a_1 + 62a_2 + 6a_3 + a_4)x^{40}y^8 + (42504a_0 + 2755a_1 + 172a_2 + 9a_3 + a_5)x^{38}y^{10} + (134596a_0 + 6954a_1 + 237a_2 - 16a_3 - 8a_4 - 6a_5 + a_6)x^{36}y^{12} + (346104a_0 + 12597a_1 - 16a_2 - 60a_3 + 11a_5 - 12a_6)x^{34}y^{14} + (735471a_0 + 15504a_1 - 664a_2 - 24a_3 + 28a_4 + 4a_5 + 66a_6)x^{32}y^{16} + (1307504a_0 + 9690a_1 - 1104a_2 + 116a_3 - 39a_5 - 220a_6)x^{30}y^{18} + (1961256a_0 - 6460a_1 - 494a_2 + 144a_3 - 56a_4 + 38a_5 + 495a_6)x^{28}y^{20} + (2496144a_0 - 25194a_1 + 936a_2 - 66a_3 + 27a_5 - 792a_6)x^{26}y^{22} + (2704156a_0 - 33592a_1 + 1716a_2 - 220a_3 + 70a_4 - 72a_5 + 924a_6)x^{24}y^{24} + (2496144a_0 - 25194a_1 + 936a_2 - 66a_3 + 27a_5 - 792a_6)x^{22}y^{26} + (1961256a_0 - 6460a_1 - 494a_2 + 144a_3 - 56a_4 + 38a_5 + 495a_6)x^{20}y^{28} + \cdots$$
(1307504a_0 + 9690a_1 - 1104a_2 + 116a_3 - 39a_5 - 220a_6)x^{18}y^{30} + (735471a_0 + 15504a_1 - 664a_2 - 24a_3 + 28a_4 + 4a_5 + 66a_6)x^{16}y^{32} + (346104a_0 + 12597a_1 - 16a_2 - 60a_3 + 11a_5 - 12a_6)x^{14}y^{34} + (134596a_0 + 6954a_1 + 237a_2 - 16a_3 - 8a_4 - 6a_5 + a_6)x^{12}y^{36} + (42504a_0 + 2755a_1 + 172a_2 + 9a_3 + 5a_5)x^{10}y^{38} + (10626a_0 + 780a_1 + 62a_2 + 6a_3 + 4a_4)x^8y^{40} + (2024a_0 + 151a_1 + 12a_2 + 5a_3)x^6y^{42} + (276a_0 + 18a_1 + a_2)x^4y^{44} + (24a_0 + a_1)x^2y^{46} + a_0y^{48}

Trimming down the list to the first terms to set up system of equations

\{ x^{48}a_0, x^{46}y^2(24a_0 + a_1), x^{44}y^4(276a_0 + 18a_1 + a_2), x^{42}y^6(2024a_0 + 151a_1 + 12a_2 + a_3), x^{40}y^8(10626a_0 + 780a_1 + 62a_2 + 6a_3 + a_4), x^{38}y^{10}(42504a_0 + 2755a_1 + 172a_2 + 9a_3 + 5a_5), x^{36}y^{12}(134596a_0 + 6954a_1 + 237a_2 - 16a_3 - 8a_4 - 6a_5 + a_6) \}

\{ \{1\}, \{-24\}, \{156\}, \{-272\}, \{54\}, \{-64\}, \{0\} \}

After substituting \( a_i \) values

\[-64\xi_8^5\psi_2^4 + 54\xi_8^4\psi_2^8 - 272\xi_8^3\psi_2^{12} + 156\xi_8^2\psi_2^{16} - 24\xi_8\psi_2^{20} + \psi_2^{24} \]

Mapping into lattices

\[ \frac{\varphi_{12}^{48}}{16} - 6\varphi_{12}^{44}\varphi_4^{4} + \frac{63}{4}\varphi_{12}^{40}\varphi_4^{8} - \frac{95}{4}\varphi_{12}^{36}\varphi_4^{12} + \frac{2907}{128}\varphi_{12}^{32}\varphi_4^{16} - \frac{437}{32}\varphi_{12}^{28}\varphi_4^{20} + \frac{373}{64}\varphi_{12}^{24}\varphi_4^{24} - \frac{47}{32}\varphi_{12}^{20}\varphi_4^{28} + \frac{107}{128}\varphi_{12}^{16}\varphi_4^{32} - \frac{5}{16}\varphi_{12}^{12}\varphi_4^{36} + \frac{1}{16}\varphi_{12}^{8}\varphi_4^{40} \]

\[ \frac{\varphi_{16}^{40}}{16\varphi_3^{40}} - \frac{5\varphi_{16}^{36}}{16\varphi_3^{40}} + \frac{107\varphi_{16}^{32}}{128\varphi_3^{40}} - \frac{47\varphi_{16}^{28}}{32\varphi_3^{40}} + \frac{373\varphi_{16}^{24}}{64\varphi_3^{40}} - \frac{437\varphi_{16}^{20}}{32\varphi_3^{40}} + \frac{2907\varphi_{16}^{16}}{128\varphi_3^{40}} - \frac{95\varphi_{16}^{12}}{4\varphi_3^{40}} + \frac{63\varphi_{16}^{8}}{4\varphi_3^{40}} - \frac{6\varphi_{16}^{4}}{\varphi_3^{40}} + 1 \]

\[ - \frac{5\varphi_{9}^{9/2}}{16} - \frac{47\varphi_{7}^{7/2}}{32} - \frac{437\varphi_{5}^{5/2}}{32} - \frac{95\varphi_{3}^{3/2}}{4} + \frac{\varphi_{5}^{5}}{16} + \frac{107\varphi_{4}^{4}}{128} + \frac{373\varphi_{3}^{3}}{64} + \frac{2907\varphi_{2}^{2}}{128} + \frac{63\varphi_{4}}{4} - 6\varphi \zeta + 1 \]

If the function is decreasing on the entire interval, than the secrecy function attains its maximum at \( y=1 \), and thus satisfies the conjecture

\[
\text{WEpolyinIpsixi}[48,2,8,\{1,0,0,0,0,768,8592\}]\]
Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^{24} + a_1\xi_8\psi_2^{20} + a_2\xi_8^2\psi_2^{16} + a_3\xi_8^3\psi_2^{12} + a_4\xi_8^4\psi_2^8 + a_5\xi_8^5\psi_2^4 + a_6\xi_8^6$$

Using lemma we substitute $\xi$ and $\psi$

$$(x^2 + y^2)^{24}a_0 + x^2y^2(x^2 - y^2)^2(x^2 + y^2)^{20}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{16}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{12}a_3 + x^8y^8(x^2 - y^2)^8(x^2 + y^2)^8a_4 + x^{10}y^{10}(x^2 - y^2)^{10}(x^2 + y^2)^4a_5 + x^{12}y^{12}(x^2 - y^2)^{12}a_6$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{48} + (24a_0 + a_1)x^{46}y^2 + (276a_0 + 18a_1 + a_2)x^{44}y^4 + (2024a_0 + 151a_1 + 12a_2 + a_3)x^{42}y^6 + (10626a_0 + 780a_1 + 62a_2 + 6a_3 + a_4)x^{40}y^8 + (42504a_0 + 2755a_1 + 172a_2 + 9a_3 + a_5)x^{38}y^{10} + (134596a_0 + 6954a_1 + 237a_2 - 16a_3 - 8a_4 - 6a_5 + a_6)x^{36}y^{12} + (346104a_0 + 12597a_1 - 16a_2 - 60a_3 + 11a_5 - 12a_6)x^{34}y^{14} + (735471a_0 + 15504a_1 - 66a_2 - 24a_3 + 28a_4 + 4a_5 + 66a_6)x^{32}y^{16} + (1307504a_0 + 9690a_1 - 1104a_2 + 116a_3 - 39a_5 - 220a_6)x^{30}y^{18} + (1961256a_0 - 6460a_1 - 494a_2 + 144a_3 - 56a_4 + 38a_5 + 495a_6)x^{28}y^{20} + (2496144a_0 - 25194a_1 + 936a_2 - 66a_3 + 27a_5 - 792a_6)x^{26}y^{22} + (2704156a_0 - 33592a_1 + 1716a_2 - 220a_3 + 70a_4 - 72a_5 + 924a_6)x^{24}y^{24} + (2496144a_0 - 25194a_1 + 936a_2 - 66a_3 + 27a_5 - 792a_6)x^{22}y^{26} + (1961256a_0 - 6460a_1 - 494a_2 + 144a_3 - 56a_4 + 38a_5 + 495a_6)x^{20}y^{28} + (1307504a_0 + 9690a_1 - 1104a_2 + 116a_3 - 39a_5 - 220a_6)x^{18}y^{30} + (735471a_0 + 15504a_1 - 66a_2 - 24a_3 + 28a_4 + 4a_5 + 66a_6)x^{16}y^{32} + (346104a_0 + 12597a_1 - 16a_2 - 60a_3 + 11a_5 - 12a_6)x^{14}y^{34} + (134596a_0 + 6954a_1 + 237a_2 - 16a_3 - 8a_4 - 6a_5 + a_6)x^{12}y^{36} + (42504a_0 + 2755a_1 + 172a_2 + 9a_3 + a_5)x^{10}y^{38} + (10626a_0 + 780a_1 + 62a_2 + 6a_3 + a_4)x^{8}y^{40} + (2024a_0 + 151a_1 + 12a_2 + a_3)x^{6}y^{42} + (276a_0 + 18a_1 + a_2)x^{4}y^{44} + (24a_0 + a_1)x^{2}y^{46} + a_0y^{48}

Trimming down the list to the first terms to set up sytem of equations

$$\{x^{48}a_0, x^{46}y^2(24a_0 + a_1), x^{44}y^4(276a_0 + 18a_1 + a_2), x^{42}y^6(2024a_0 + 151a_1 + 12a_2 + a_3), x^{40}y^8(10626a_0 + 780a_1 + 62a_2 + 6a_3 + a_4), x^{38}y^{10}(42504a_0 + 2755a_1 + 172a_2 + 9a_3 + a_5), x^{36}y^{12}(134596a_0 + 6954a_1 + 237a_2 - 16a_3 - 8a_4 - 6a_5 + a_6)\}$$

$$\{\{1\}, \{-24\}, \{156\}, \{-272\}, \{54\}, \{0\}, \{0\}\}$$

After substituting $a_i$ values

$$54\xi_8^4\psi_2^8 - 272\xi_8^3\psi_2^{12} + 156\xi_8^2\psi_2^{16} - 24\xi_8\psi_2^{20} + \psi_2^{24}$$

Mapping into lattices

$$\varphi_3^{48} - 6\varphi_3^{14}\varphi_4^4 + \frac{63}{4}\varphi_3^{10}\varphi_4^8 - \frac{95}{4}\varphi_3^{36}\varphi_4^{12} + \frac{2907}{128}\varphi_3^{32}\varphi_4^{16} - \frac{435}{32}\varphi_3^{28}\varphi_4^{20} + \frac{653}{64}\varphi_3^{24}\varphi_4^{24} - \frac{27}{32}\varphi_3^{20}\varphi_4^{28} +$$

72
a type I length 56 code. We provide results for both polynomials, and thus verifying

For this case note that we have two candidates for weight enumerator polynomial of

A.2.5 Singly Even Code of length \( n = 56 \) and minimal distance \( d = 12 \)

If the function is decreasing on the entire interval, than the secrecy function attains

its maximum at \( y = 1 \), and thus satisfies the conjecture

\[
\begin{align*}
&\left( x^2 + y^2 \right)^{28} a_0 + x^2 y^2 \left( x^2 - y^2 \right)^2 \left( x^2 + y^2 \right)^{24} a_1 + x^4 y^4 \left( x^2 - y^2 \right)^4 \left( x^2 + y^2 \right)^{20} a_2 + x^6 y^6 \left( x^2 - y^2 \right)^6 \left( x^2 + y^2 \right)^{16} a_3 + x^8 y^8 \left( x^2 - y^2 \right)^8 \left( x^2 + y^2 \right)^{12} a_4 + x^{10} y^{10} \left( x^2 - y^2 \right)^{10} \left( x^2 + y^2 \right)^8 a_5 + \\
&x^{12} y^{12} \left( x^2 - y^2 \right)^{12} \left( x^2 + y^2 \right)^4 a_6 + x^{14} y^{14} \left( x^2 - y^2 \right)^{14} a_7
\end{align*}
\]

Using lemma we substitute \( \xi \) and \( \psi \)

Expanding and collecting the weight enumerator becomes,

\[
\begin{align*}
a_0 x^{56} + y^2 (28 a_0 + a_1) x^{54} + y^4 (378 a_0 + 22 a_1 + a_2) x^{52} + y^6 (3276 a_0 + 229 a_1 + 16 a_2 + \\
a_3) x^{50} + y^8 (20475 a_0 + 1496 a_1 + 116 a_2 + 10 a_3 + a_4) x^{48} + y^{10} (9828 a_0 + 6854 a_1 + 496 a_2 + \\
39 a_3 + 4 a_4 + a_5) x^{46} + y^{12} (376740 a_0 + 23276 a_1 + 1346 a_2 + 60 a_3 - 2 a_4 - 2 a_5 + a_6) x^{44} + \\
y^{14} (118404 a_0 + 60214 a_1 + 2224 a_2 - 45 a_3 - 28 a_4 - 7 a_5 - 8 a_6 + a_7) x^{42} + y^{16} (3108105 a_0 + \\
119416 a_1 + 1444 a_2 - 318 a_3 - 19 a_4 + 16 a_5 + 24 a_6 - 14 a_7) x^{40} + y^{18} (6906900 a_0 + 177859 a_1 -
\end{align*}
\]
If the function is decreasing on the entire interval, then the secrecy function attains

After substituting \(a_i\) values

Mapping into lattices

If the function is decreasing on the entire interval, then the secrecy function attains
its maximum at \(y=1\), and thus satisfies the conjecture.
Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^{28} + a_1\xi_8\psi_2^{24} + a_2\xi_8^2\psi_2^{20} + a_3\xi_8^3\psi_2^{16} + a_4\xi_8^4\psi_2^{12} + a_5\xi_8^5\psi_2^8 + a_6\xi_8^6\psi_2^4 + a_7\xi_8^7$$

Using lemma we substitute $\xi$ and $\psi$

$$(x^2 + y^2)^{28}a_0 + x^2y^2(x^2 - y^2)^2(x^2 + y^2)^{24}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{20}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{16}a_3 + x^8y^8(x^2 - y^2)^8(x^2 + y^2)^{12}a_4 + x^{10}y^{10}(x^2 - y^2)^{10}(x^2 + y^2)^{8}a_5 + x^{12}y^{12}(x^2 - y^2)^{12}(x^2 + y^2)^{4}a_6 + x^{14}y^{14}(x^2 - y^2)^{14}a_7$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{56} + y^2(28a_0 + a_1)x^{54} + y^4(378a_0 + 22a_1 + a_2)x^{52} + y^6(3276a_0 + 229a_1 + 16a_2 + a_3)x^{50} + y^8(20475a_0 + 1496a_1 + 116a_2 + 10a_3 + a_4)x^{48} + y^{10}(98280a_0 + 6854a_1 + 496a_2 + 39a_3 + 4a_4 + a_5)x^{46} + y^{12}(376740a_0 + 23276a_1 + 1346a_2 + 60a_3 + 2a_4 + 2a_5 + a_6)x^{44} + y^{14}(1184040a_0 + 60214a_1 + 222a_2 + 45a_3 + 28a_4 + 7a_5 - 8a_6 + a_7)x^{42} + y^{16}(3108105a_0 + 119416a_1 + 1444a_2 - 318a_3 - 19a_4 + 16a_5 + 24a_6 - 14a_7)x^{40} + y^{18}(6906900a_0 + 177859a_1 - 2736a_2 - 95a_3 + 80a_4 + 20a_5 + 24a_6 + 91a_7)x^{38} + y^{20}(13123110a_0 + 182666a_1 - 8721a_2 + 208a_3 + 104a_4 - 56a_5 - 36a_6 - 36a_7)x^{36} + y^{22}(21474180a_0 + 81719a_1 - 10336a_2 + 1050a_3 - 112a_4 - 28a_5 + 120a_6 + 100a_7)x^{34} + y^{24}(30421755a_0 - 118864a_1 - 258a_2 + 820a_3 - 238a_4 + 112a_5 - 88a_6 - 2002a_7)x^{32} + y^{26}(37442160a_0 - 326876a_1 + 10336a_2 + 650a_3 + 56a_4 + 14a_5 - 88a_6 + 300a_7)x^{30} + y^{28}(40116600a_0 - 416024a_1 + 16796a_2 - 1560a_3 + 308a_4 - 140a_5 + 196a_6 - 3432a_7)x^{28} + y^{30}(37442160a_0 - 326876a_1 + 10336a_2 - 650a_3 + 56a_4 + 14a_5 - 88a_6 + 300a_7)x^{26} + y^{32}(30421755a_0 - 118864a_1 - 258a_2 + 820a_3 - 238a_4 + 112a_5 - 88a_6 - 2002a_7)x^{24} + y^{34}(21474180a_0 + 81719a_1 - 10336a_2 + 1050a_3 - 112a_4 - 28a_5 + 120a_6 + 100a_7)x^{22} + y^{36}(13123110a_0 + 182666a_1 - 8721a_2 + 208a_3 + 104a_4 - 56a_5 - 36a_6 - 36a_7)x^{20} + y^{38}(6906900a_0 + 177859a_1 - 2736a_2 - 95a_3 + 80a_4 + 20a_5 + 24a_6 + 91a_7)x^{18} + y^{40}(3108105a_0 + 119416a_1 + 1444a_2 - 318a_3 - 19a_4 + 16a_5 + 24a_6 - 14a_7)x^{16} + y^{42}(1184040a_0 + 60214a_1 + 222a_2 - 45a_3 - 28a_4 + 7a_5 - 8a_6 +
\(a_7)x^{14} + y^{41}(376740a_0 + 23276a_1 + 1346a_2 + 60a_3 - 2a_4 - 2a_5 + a_6)x^{12} + y^{46}(98280a_0 + 6854a_1 + 496a_2 + 39a_3 + 4a_4 + a_5)x^{10} + y^{48}(20475a_0 + 1496a_1 + 116a_2 + 10a_3 + a_4)x^8 + y^{50}(3276a_0 + 229a_1 + 16a_2 + a_3)x^6 + y^{52}(378a_0 + 22a_1 + a_2)x^4 + y^{54}(28a_0 + a_1)x^2 + y^{56}a_0\)

Trimming down the list to the first terms to set up system of equations

\[
\{x^{56}a_0, x^{54}y^2(28a_0 + a_1), x^{52}y^4(378a_0 + 22a_1 + a_2), x^{50}y^6(3276a_0 + 229a_1 + 16a_2 + a_3), x^{48}y^8(20475a_0 + 1496a_1 + 116a_2 + 10a_3 + a_4), x^{46}y^{10}(98280a_0 + 6854a_1 + 496a_2 + 39a_3 + 4a_4 + a_5), x^{44}y^{12}(376740a_0 + 23276a_1 + 1346a_2 + 60a_3 - 2a_4 - 2a_5 + a_6), x^{42}y^{14}(1184040a_0 + 60214a_1 + 2224a_2 - 45a_3 - 28a_4 - 7a_5 - 8a_6 + a_7)\}\]

After substituting \(a_i\) values

\[256\xi_8^6\psi_2^4 - 308\xi_8^5\psi_8^8 + 525\xi_8^4\psi_1^{12} - 672\xi_8^3\psi_2^{16} + 238\xi_8^2\psi_2^{20} - 28\xi_8\psi_2^{24} + \psi_2^{28}\]

Mapping into lattices

\[
\begin{align*}
\vartheta_{48}^{32} - 7\vartheta_{33}^{52}3\vartheta_4^4 + \frac{175}{8}\vartheta_{43}^{48}\vartheta_3^8 - \frac{161}{4}\vartheta_4^{14}\vartheta_3^4 + \frac{1237}{256}\vartheta_4^{40}\vartheta_4^4 + \frac{10241}{256}\vartheta_4^{36}\vartheta_3^4 + \frac{6239}{256}\vartheta_3^{32}\vartheta_4^4 & - \\
\frac{1483}{128}\vartheta_3^{28}3\vartheta_4^6 & + \frac{1535}{256}\vartheta_3^{24}\vartheta_3^6 - \frac{705}{256}\vartheta_3^{20}\vartheta_4^6 + \frac{317}{256}\vartheta_3^{16}\vartheta_3^6 - & \frac{8}{3}\vartheta_3^{12}\vartheta_4^6 + \frac{1}{16}\vartheta_3^8\vartheta_4^8
\end{align*}
\]

\[
\begin{align*}
\vartheta_{48}^{44} & - \frac{3\vartheta_{44}^{44}}{16\vartheta_{44}^8} + \frac{317\vartheta_{44}^{40}}{256\vartheta_{44}^8} - \frac{705\vartheta_{44}^{36}}{256\vartheta_{44}^8} & + \frac{1535\vartheta_{44}^{32}}{256\vartheta_{44}^8} & - \frac{1483\vartheta_{44}^{28}}{256\vartheta_{44}^8} & + \frac{6239\vartheta_{44}^{24}}{256\vartheta_{44}^8} & - \frac{10241\vartheta_{44}^{20}}{256\vartheta_{44}^8} & + \frac{12397\vartheta_{44}^{16}}{256\vartheta_{44}^8} & - \frac{161\vartheta_{44}^{12}}{4\vartheta_{44}^8} & + \\
\frac{175\vartheta_{44}^8}{8\vartheta_{44}^4} & - \frac{7\vartheta_{44}^4}{4\vartheta_{44}^4} & + 1
\end{align*}
\]

\[
\begin{align*}
- \frac{3\zeta_{11/2}^{11/2}}{8} & - \frac{705\zeta_{9/2}^{9/2}}{256} & - \frac{1483\zeta_{7/2}^{7/2}}{128} & - \frac{1024\zeta_{5/2}^{5/2}}{256} & - \frac{161\zeta_{3/2}^{3/2}}{4} & + \zeta_{6}^6 & + \frac{317\zeta_{5}^{5}}{256} & + \frac{1535\zeta_{4}^{4}}{256} & + \frac{6239\zeta_{3}^{3}}{256} & + \frac{12397\zeta_{2}^{2}}{256} & + \\
\frac{175\zeta_{1}^{1}}{8} & - 7\sqrt{\zeta} & + 1
\end{align*}
\]

If the function is decreasing on the entire interval, then the secrecy function attains its maximum at \(y=1\), and thus satisfies the conjecture
A.2.6 Singly Even Code of length $n=64$ and minimal distance $d=12$

WEpolyinPsisi[64,2,8,\{1,0,0,0,0,0,1824,20992,20789\}]

Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^{32} + a_1\xi_8\psi_2^{28} + a_2\xi_8^2\psi_2^{24} + a_3\xi_8^3\psi_2^{20} + a_4\xi_8^4\psi_2^{16} + a_5\xi_8^5\psi_2^{12} + a_6\xi_8^6\psi_2^8 + a_7\xi_8^7\psi_2^4 + a_8\xi_8^8$$

Using lemma we substitute $x$ and $y$:

$$(x^2 + y^2)^{32}a_0 + x^2y^2(x^2 - y^2)^2(x^2 + y^2)^{28}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{21}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{20}a_3 + x^8y^8(x^2 - y^2)^8(x^2 + y^2)^{16}a_4 + x^{10}y^{10}(x^2 - y^2)^{10}(x^2 + y^2)^{12}a_5 + x^{12}y^{12}(x^2 - y^2)^{12}(x^2 + y^2)^{8}a_6 + x^{14}y^{14}(x^2 - y^2)^{14}(x^2 + y^2)^{4}a_7 + x^{16}y^{16}(x^2 - y^2)^{16}a_8$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{64} + y^2(32a_0 + a_1)x^{62} + y^4(496a_0 + 26a_1 + a_2)x^{60} + y^6(4960a_0 + 323a_1 + 20a_2 + a_3)x^{58} + y^8(3595060a_0 + 25484a_1 + 186a_2 + 14a_3 + a_4)x^{56} + y^{10}(201376a_0 + 14301a_1 + 1060a_2 + 85a_3 + 8a_4 + a_5)x^{54} + y^{12}(306192a_0 + 601606a_1 + 4091a_2 + 280a_3 + 20a_4 + 2a_5 + a_6)x^{52} + y^{14}(3365856a_0 + 200655a_1 + 11064a_2 + 470a_3 - 8a_4 - 9a_5 - 4a_6 + a_7)x^{50} + y^{16}(10518300a_0 + 528840a_1 + 20516a_2 + 28a_3 - 126a_4 - 20a_5 - 2a_6 - 10a_7 + a_8)x^{48} + y^{18}(28048800a_0 + 1116765a_1 + 22624a_2 - 1658a_3 - 168a_4 + 35a_5 + 28a_6 + 41a_7 - 16a_8)x^{46} + y^{20}(64512240a_0 + 1874730a_1 - 759a_2 - 340a_3 + 196a_4 + 9a_5 - 19a_6 - 80a_7 - 120a_8)x^{44} + y^{22}(129024480a_0 + 2417415a_1 - 53636a_2 - 1805a_3 + 680a_4 - 75a_5 - 80a_6 + 36a_7 - 560a_8)x^{42} + y^{24}(225792840a_0 + 2134860a_1 - 105754a_2 + 4370a_3 + 239a_4 - 240a_5 + 104a_6 + 168a_7 + 1820a_8)x^{40} + y^{26}(347373600a_0 + 596505a_1 - 99636a_2 + 9367a_3 - 1072a_4 + 90a_5 + 112a_6 - 36a_7 - 436a_8)x^{38} + y^{28}(471435600a_0 - 1927170a_1 - 7429a_2 + 5168a_3 - 124a_4 + 420a_5 - 238a_6 + 208a_7 + 8008a_8)x^{36} + y^{30}(56572720a_0 - 435965a_1 + 118864a_2 - 6460a_3 + 560a_4 - 42a_5 - 56a_6 + 286a_7 - 114a_8)x^{34} + y^{32}(601080390a_0 - 5348880a_1 + 178296a_2 + 12920a_3 + 1820a_4 - 50a_5 + 308a_6 - 572a_7 + 12870a_8)x^{32} + y^{34}(56572720a_0 - 4345965a_1 + 118864a_2 - 6460a_3 + 560a_4 - 42a_5 - 56a_6 + 286a_7 - 114a_8)x^{30} + y^{36}(471435600a_0 - 1927170a_1 - 7429a_2 + 5168a_3 - 124a_4 + 420a_5 - 238a_6 + 208a_7 + 8008a_8)x^{28} + y^{38}(347373600a_0 + 596505a_1 - 99636a_2 + 9367a_3 - 1072a_4 + 90a_5 + 112a_6 - 36a_7 - 436a_8)x^{26} + y^{40}(225792840a_0 + 2134860a_1 - 105754a_2 + 4370a_3 + 239a_4 - 240a_5 + 104a_6 + 168a_7 + 1820a_8)x^{24} + y^{42}(129024480a_0 + 2417415a_1 - 53636a_2 - 1805a_3 + 680a_4 - 75a_5 - 80a_6 + 36a_7 - 560a_8)x^{22} + y^{44}(64512240a_0 + 1874730a_1 - 759a_2 - 340a_3 + 196a_4 + 9a_5 - 19a_6 - 80a_7 - 120a_8)x^{20} + y^{46}(28048800a_0 + 1116765a_1 + 22624a_2 - 1658a_3 - 168a_4 + 35a_5 + 28a_6 + 41a_7 - 16a_8)x^{18} + y^{48}(10518300a_0 + 528840a_1 + 20516a_2 + 28a_3 - 126a_4 - 20a_5 - 2a_6 + 10a_7 + a_8)x^{16} + y^{50}(3365856a_0 + 200655a_1 + 11064a_2 + 470a_3 - 8a_4 - 9a_5 - 4a_6 + a_7)x^{14} + y^{52}(906192a_0 + 601606a_1 + 4091a_2 + 280a_3 + 20a_4 + 2a_5 + a_6)x^{12} + y^{54}(201376a_0 + 14301a_1 + 1060a_2 + 85a_3 + 8a_4 + a_5)x^{10} + y^{56}(3595060a_0 + 25484a_1 + 186a_2 + 14a_3 + a_4)x^{8} + y^{58}(4960a_0 + 323a_1 + 20a_2 + a_3)x^{6} + y^{60}(4960a_0 + 26a_1 + a_2)x^{4} + y^{62}(32a_0 + a_1)x^{2} + y^{64}a_0$$

Trimming down the list to the first terms to set up system of equations
\{x^{64}a_0, x^{62}y^2(32a_0 + a_1), x^{60}y^4(496a_0 + 26a_1 + a_2), x^{58}y^6(4960a_0 + 323a_1 + 20a_2 + a_3), x^{56}y^8(35960a_0 + 2548a_1 + 186a_2 + 14a_3 + a_4), x^{54}y^{10}(201376a_0 + 14301a_1 + 1060a_2 + 85a_3 + 8a_4 + a_5), x^{52}y^{12}(906192a_0 + 60606a_1 + 4091a_2 + 280a_3 + 20a_4 + 2a_5 + a_6), x^{50}y^{14}(3365856a_0 + 200655a_1 + 11064a_2 + 470a_3 - 8a_4 - 9a_5 - 4a_6 + a_7), x^{48}y^{16}(10518300a_0 + 528840a_1 + 20516a_2 + 28a_3 - 126a_4 - 20a_5 - 2a_6 - 10a_7 + a_8)\}

\{\{1\}, \{-32\}, \{336\}, \{-1344\}, \{1896\}, \{-832\}, \{512\}, \{0\}, \{0\}\}

After substituting \(a_i\) values

\[512\xi^6\psi^8 - 832\xi^5\psi^{12} + 1896\xi^4\psi^{16} - 1344\xi^3\psi^{20} + 336\xi^2\psi^{24} - 32\xi\psi^{28} + \psi^{32}\]

Mapping into lattices

\[\psi_{3}^{64} - 8\psi_{3}^{60} \psi_{4}^{2} + 29\psi_{3}^{56} \psi_{4}^{3} - 63\psi_{3}^{52} \psi_{4}^{4} + 2925\psi_{3}^{48} \psi_{4}^{6} - 1495\psi_{3}^{44} \psi_{4}^{8} + 557\psi_{3}^{40} \psi_{4}^{10} - 77\psi_{3}^{36} \psi_{4}^{12} + 557\psi_{3}^{32} \psi_{4}^{14} - 105\psi_{3}^{28} \psi_{4}^{16} + 1344\psi_{3}^{24} \psi_{4}^{18} + 336\psi_{3}^{20} \psi_{4}^{20} + 32\psi_{3}^{16} \psi_{4}^{22} - \psi_{3}^{12} \psi_{4}^{24} + \psi_{3}^{8} \psi_{4}^{26} + \psi_{3}^{4} \psi_{4}^{28} + \psi_{3}^{0} \psi_{4}^{30}\]

\[-3\xi^{11/2} - 105\xi^{9/2} - 77\xi^{7/2} - 1495\xi^{5/2} - 63\xi^{3/2} + \xi^{1} - 43\xi^{1/2} - 28\xi^{0} + 8\xi^{-1} + 1\]

If the function is decreasing on the entire interval, than the secrecy function attains its maximum at \(y=1\), and thus satisfies the conjecture.

\[\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{chart.png}
\end{figure}\]

A.2.7 Singly Even Code of length \(n=72\) and minimal distance \(d=14\)

For this case note that we have three candidates for weight enumerator polynomial of type I length 72 code. We provide results for all three polynomials, and thus verifying that type I codes of length 72 and minimal distance 14 satisfy the conjecture.

- \text{WEpolylinIpsixi}\{72,2,8,\{1,0,0,0,0,0,0,0,7616,13452,1151040\}\]

Weight enumerator polynomial in terms of \(\xi\) and \(\psi\)

78
Using lemma we substitute $\xi$ and $\psi$

\begin{align*}
  (x^2 + y^2)^3 & a_0 + x^2 y^2 (x^2 - y^2)^2 (x^2 + y^2)^2 a_1 + x^2 y^4 (x^2 - y^2)^4 (x^2 + y^2)^2 a_2 + x^6 y^6 (x^2 - y^2)^6 (x^2 + y^2)^2 a_3 + x^8 y^8 (x^2 - y^2)^8 (x^2 + y^2)^2 a_4 + x^{10} y^{10} (x^2 - y^2)^{10} (x^2 + y^2)^2 a_5 + x^{12} y^{12} (x^2 - y^2)^{12} (x^2 + y^2)^2 a_6 + x^{14} y^{14} (x^2 - y^2)^{14} (x^2 + y^2)^2 a_7 + x^{16} y^{16} (x^2 - y^2)^{16} a_8 + x^{18} y^{18} (x^2 - y^2)^{18} a_9
\end{align*}

Expanding and collecting the weight enumerator becomes,

\begin{align*}
  a_0 x^{72} + y^2 (36 a_0 + a_1) x^{60} + y^4 (630 a_0 + 30 a_1 + a_2) x^{58} + y^6 (7140 a_0 + 433 a_1 + 24 a_2 + a_3) x^{56} + y^8 (58905 a_0 + 4000 a_1 + 272 a_2 + 18 a_3 + a_4) x^{54} + y^{10} (376992 a_0 + 26536 a_1 + 1928 a_2 + 147 a_3 + 12 a_4 + a_5) x^{52} + y^{12} (1947792 a_0 + 134416 a_1 + 9528 a_2 + 708 a_3 + 58 a_4 + 6 a_5 + a_6) x^{50} + y^{14} (8347680 a_0 + 539400 a_1 + 34552 a_2 + 2157 a_3 + 124 a_4 + 5 a_5 + a_7) x^{48} + y^{16} (30260340 a_0 + 1754848 a_1 + 93744 a_2 + 3942 a_3 - 5 a_4 - 40 a_5 - 12 a_6 - 6 a_7 + a_8) x^{46} + y^{18} (94143280 a_0 + 469278 a_1 + 188136 a_2 + 2479 a_3 - 632 a_4 + 40 a_5 - 9 a_6 + 7 a_7 - 12 a_8 + a_9) x^{44} + y^{20} (2541686856 a_0 + 10378056 a_1 + 259740 a_2 - 7704 a_3 - 124 a_4 + 76 a_5 + 66 a_6 + 28 a_7 + 62 a_8 - 18 a_9) x^{42} + y^{22} (6008052960 a_0 + 18932940 a_1 + 170040 a_2 - 24771 a_3 - 56 a_4 + 406 a_5 - 77 a_7 - 172 a_8 + 153 a_9) x^{40} + y^{24} (1251677700 a_0 + 28048800 a_1 - 215280 a_2 - 29854 a_3 + 3337 a_4 + 120 a_5 - 220 a_6 - 14 a_7 + 237 a_8 - 816 a_9) x^{38} + y^{26} (2310789600 a_0 + 32256120 a_1 - 825240 a_2 + 759 a_3 + 4580 a_4 - 925 a_5 + 245 a_7 + 16 a_8 + 306 a_9) x^{36} + y^{28} (3796297200 a_0 + 24812400 a_1 - 1255800 a_2 + 58236 a_3 - 1178 a_4 - 870 a_5 + 495 a_6 - 176 a_7 - 66 a_8 - 856 a_9) x^{34} + y^{30} (5567902560 a_0 + 2481240 a_1 - 985320 a_2 + 86089 a_3 - 9196 a_4 + 11435 a_5 - 358 a_7 + 1104 a_8 + 1856 a_9) x^{32} + y^{32} (7307872110 a_0 - 29774880 a_1 + 104880 a_2 + 34086 a_3 - 74294 a_4 + 1968 a_5 - 792 a_6 + 532 a_7 - 494 a_8 - 3182 a_9) x^{30} + y^{34} (8597496600 a_0 - 58929450 a_1 + 1415880 a_2 - 66861 a_3 + 5168 a_4 - 540 a_5 + 182 a_7 - 936 a_8 + 43758 a_9) x^{30} + y^{36} (9075135000 a_0 - 70715340 a_1 + 2005830 a_2 - 118864 a_3 + 1292 a_4 - 2520 a_5 + 924 a_6 - 728 a_7 + 1716 a_8 - 4862 a_9) x^{28} + y^{38} (8597496600 a_0 - 58929450 a_1 + 1415880 a_2 - 66861 a_3 + 5168 a_4 - 540 a_5 + 182 a_7 - 936 a_8 + 43758 a_9) x^{30} + y^{40} (3707872110 a_0 - 29774880 a_1 + 104880 a_2 + 53486 a_3 - 74294 a_4 + 1968 a_5 - 792 a_6 + 532 a_7 - 494 a_8 - 3182 a_9) x^{32} + y^{42} (5567902560 a_0 + 2481240 a_1 - 985320 a_2 + 86089 a_3 - 9196 a_4 + 11435 a_5 - 358 a_7 + 1104 a_8 + 1856 a_9) x^{40} + y^{44} (3796297200 a_0 + 2481240 a_1 - 1255800 a_2 + 58236 a_3 - 1178 a_4 - 870 a_5 + 495 a_6 - 176 a_7 - 66 a_8 - 856 a_9) x^{38} + y^{46} (2310789600 a_0 + 32256120 a_1 - 825240 a_2 + 759 a_3 + 4580 a_4 - 925 a_5 + 245 a_7 + 16 a_8 + 306 a_9) x^{36} + y^{48} (7140 a_0 + 433 a_1 + 24 a_2 + a_3) x^{56} + y^{50} (6008052960 a_0 + 18932940 a_1 + 170040 a_2 - 24771 a_3 - 56 a_4 + 406 a_5 - 77 a_7 - 172 a_8 + 153 a_9) x^{52} + y^{52} (2541686856 a_0 + 10378056 a_1 + 259740 a_2 - 7704 a_3 - 124 a_4 + 76 a_5 + 66 a_6 + 28 a_7 + 62 a_8 - 18 a_9) x^{50} + y^{54} (94143280 a_0 + 469278 a_1 + 188136 a_2 + 2479 a_3 - 632 a_4 - 9 a_6 + 7 a_7 - 12 a_8 + a_9) x^{48} + y^{56} (30260340 a_0 + 1754848 a_1 + 93744 a_2 + 3942 a_3 - 5 a_4 - 40 a_5 - 12 a_6 - 6 a_7 + a_8) x^{46} + y^{58} (8347680 a_0 + 539400 a_1 + 34552 a_2 + 2157 a_3 + 124 a_4 + 5 a_5 + a_7) x^{44} + y^{60} (1947792 a_0 + 134416 a_1 + 9528 a_2 + 708 a_3 + 58 a_4 + 6 a_5 + a_6) x^{42} + y^{62} (376992 a_0 +
26536a_1 + 1928a_2 + 147a_3 + 12a_4 + a_5)x^{10} + y^{64}(58905a_0 + 4000a_1 + 272a_2 + 18a_3 + a_4)x^8 + y^{6}(7140a_0 + 433a_1 + 24a_2 + a_3)x^6 + y^{68}(630a_0 + 30a_1 + a_2)x^4 + y^{70}(36a_0 + a_1)x^2 + y^{72}a_0

Trimming down the list to the first terms to set up system of equations

\{x^{72}a_0, x^{70}y^2(36a_0 + a_1), x^{68}y^4(630a_0 + 30a_1 + a_2), x^{66}y^6(7140a_0 + 433a_1 + 24a_2 + a_3), x^{64}y^8(58905a_0 + 4000a_1 + 272a_2 + 18a_3 + a_4), x^{62}y^{10}(376992a_0 + 26536a_1 + 1928a_2 + 147a_3 + 12a_4 + a_5), x^{60}y^{12}(1947792a_0 + 134416a_1 + 9528a_2 + 708a_3 + 58a_4 + 6a_5 + a_6), x^{58}y^{14}(8347680a_0 + 539400a_1 + 34552a_2 + 2157a_3 + 12a_4 + 5a_5 + a_7), x^{56}y^{16}(30260340a_0 + 175484a_1 + 93744a_2 + 3942a_3 - 5a_4 - 40a_5 - 12a_6 - 6a_7 + a_8), x^{54}y^{18}(94143280a_0 + 4692780a_1 + 188136a_2 + 2479a_3 - 632a_4 - 90a_5 + 7a_7 - 12a_8 + a_9)}\}

\{\{1\}, \{-36\}, \{450\}, \{-2352\}, \{5031\}, \{-3924\}, \{546\}, \{-1024\}, \{-116973\}, \{-1452828\}\}

After substituting \(a_i\) values

\[-1452828c_8^3 - 116973c_8^2 + 1024c_8^7c_2^3 - 546c_8^6c_2^5 - 3924c_8^5c_2^9 - 2352c_8^3c_2^{12} + 450c_8^2c_2^{28} - 36c_8c_2^{32} + c_2^{36}\]

Mapping into lattices

\[
\frac{\varphi_3^{72}}{2} - 9\varphi_3^{68} \varphi_4^4 + \frac{297}{8} \varphi_3^{64} \varphi_4^8 - 93\varphi_3^{60} \varphi_4^{12} + \frac{40455}{256} \varphi_3^{56} \varphi_4^{16} - \frac{49329}{256} \varphi_3^{52} \varphi_4^{20} + \frac{35065}{4} \varphi_3^{48} \varphi_4^{24} - \\
\frac{1261994}{1024} \varphi_3^{44} \varphi_4^{28} + \frac{3842035}{32768} \varphi_3^{40} \varphi_4^{32} - \frac{943839}{2} \varphi_3^{36} \varphi_4^{36} + \frac{65536}{32768} - \frac{65536}{16384} - \frac{65536}{32768} + \frac{32768}{16384} + \frac{32768}{32768} + \frac{32768}{65536} - \frac{65536}{65536}\]

\[
\frac{363207}{5} \varphi_3^{72} - \frac{363207}{5} \varphi_3^{68} \varphi_4^4 + \frac{12958479}{65536} \varphi_3^{64} \varphi_4^8 - \frac{7393401}{65536} \varphi_3^{60} \varphi_4^{12} + \frac{1206199}{32768} \varphi_3^{56} \varphi_4^{16} - \frac{1962133}{32768} \varphi_3^{52} \varphi_4^{20} + \frac{1120815}{12288} \varphi_3^{48} \varphi_4^{24} - \\
\frac{49329}{16384} \varphi_3^{44} \varphi_4^{28} + \frac{16384}{65536} - \frac{16384}{32768} - \frac{16384}{2} \varphi_3^{36} \varphi_4^{36} + \frac{65536}{65536} + \frac{65536}{65536} - \frac{65536}{65536} + \frac{65536}{65536}\]

\[
\frac{49329}{256} \varphi_3^{72} - \frac{49329}{256} \varphi_3^{68} \varphi_4^4 + \frac{7393401}{65536} \varphi_3^{64} \varphi_4^8 - \frac{1962133}{32768} \varphi_3^{60} \varphi_4^{12} + \frac{16384}{65536} \varphi_3^{56} \varphi_4^{16} - \frac{49329}{256} \varphi_3^{52} \varphi_4^{20} + \frac{1206199}{256} \varphi_3^{48} \varphi_4^{24} - \\
\frac{49329}{256} \varphi_3^{44} \varphi_4^{28} + \frac{65536}{65536} - \frac{65536}{65536} - \frac{65536}{65536} + \frac{65536}{65536} + \frac{65536}{65536} + \frac{65536}{65536}\]

If the function is decreasing on the entire interval, than the secrecy function attains its maximum at \(y=1\), and thus satisfies the conjecture
Weight enumerator polynomial in terms of $\xi$ and $\psi$

$$a_0\psi_2^3 + a_1\xi_8\psi_2^{32} + a_2\xi_8^2\psi_2^{28} + a_3\xi_8^3\psi_2^{24} + a_4\xi_8^4\psi_2^{20} + a_5\xi_8^5\psi_2^{16} + a_6\xi_8^6\psi_2^{12} + a_7\xi_8^7\psi_2^8 + a_8\xi_8^8\psi_2^4 + a_9\xi_8^9$$

Using lemma we substitute $\xi$ and $\psi$

$$(x^2 + y^2)^3 a_0 + x^2 y^2(x^2 - y^2)^2(x^2 + y^2)^2 a_{11} + x^4 y^4(x^2 - y^2)^4(x^2 + y^2)^2 a_2 + x^6 y^6(x^2 - y^2)^6(x^2 + y^2)^2 a_3 + x^8 y^8(x^2 - y^2)^8(x^2 + y^2)^2 a_4 + x^{10} y^{10}(x^2 - y^2)^{10}(x^2 + y^2)^2 a_5 + x^{12} y^{12}(x^2 - y^2)^{12}(x^2 + y^2)^2 a_6 + x^{14} y^{14}(x^2 - y^2)^{14}(x^2 + y^2)^2 a_7 + x^{16} y^{16}(x^2 - y^2)^{16} a_8 + x^{18} y^{18}(x^2 - y^2)^{18} a_9$$

Expanding and collecting the weight enumerator becomes,

$$a_0 x^{72} + y^3(36a_0 + a_1)x^{70} + y^4(630a_0 + 30a_1 + a_2)x^{68} + y^6(7140a_0 + 433a_1 + 24a_2 + a_3)x^{66} + y^8(58905a_0 + 4000a_1 + 272a_2 + 18a_3 + a_4)x^{64} + y^{10}(376992a_0 + 26536a_1 + 1928a_2 + 147a_3 + 12a_4 + a_5)x^{62} + y^{12}(1947792a_0 + 134416a_1 + 9528a_2 + 708a_3 + 58a_4 + 6a_5 + a_6)x^{60} + y^{14}(8347680a_0 + 539400a_1 + 34552a_2 + 2157a_3 + 124a_4 + 5a_5 + a_7)x^{58} + y^{16}(3026340a_0 + 175484a_1 + 93744a_2 + 3942a_3 - 5a_4 - 40a_5 - 12a_6 - 6a_7 + a_8)x^{56} + y^{18}(94143280a_0 + 4692780a_1 + 188136a_2 + 2479a_3 - 632a_4 - 90a_5 + 5a_6 + 12a_7 - 7a_8)x^{54} + y^{20}(254186856a_0 + 10378056a_1 + 259740a_2 - 770a_3 + 124a_4 + 76a_5 + 66a_6 + 28a_7 + 62a_8 - 18a_9)x^{52} + y^{22}(600805296a_0 + 18932940a_1 + 170040a_2 - 24771a_3 - 56a_4 + 406a_5 - 77a_6 - 172a_7 + 153a_8)x^{50} + y^{24}(1251677700a_0 + 28048800a_1 - 215280a_2 - 29854a_3 + 3337a_4 + 120a_5 - 220a_6 - 14a_7 + 237a_8 - 81a_9)x^{48} + y^{26}(2310789600a_0 + 32256120a_1 - 825240a_2 + 759a_3 + 458a_4 - 925a_5 + 245a_7 + 16a_8 + 306a_9)x^{46} + y^{28}(3796297200a_0 + 24812400a_1 - 1255800a_2 + 582363a_3 - 1178a_4 - 870a_5 + 495a_6 - 176a_7 - 664a_8 - 8568a_9)x^{44} + y^{30}(5567902560a_0 + 2481240a_1 - 985320a_2 + 86089a_3 - 9196a_4 + 1143a_5 - 358a_7 + 110a_8 + 18564a_9)x^{42} + y^{32}(7307872110a_0 - 29774880a_1 + 104880a_2 + 34086a_3 - 7429a_4 + 1968a_5 - 792a_6 + 532a_7 - 494a_8 - 31824a_9)x^{40} + y^{34}(859749660a_0 - 58929450a_1 + 1415880a_2 - 66861a_3 + 5168a_4 - 540a_5 + 182a_7 - 936a_8 + 43758a_9)x^{38} + \cdots
After substituting $a_i$ values

\[-64s_8^7\psi_2 + 546s_8^6\psi_2^{12} - 3924s_8^5\psi_2^{16} + 5031s_8^4\psi_2^{20} - 2352s_8^3\psi_2^{24} + 450s_8^2\psi_2^{28} - 36s_8\psi_2^{32} + \psi_2^{36}\]

Mapping into lattices
If the function is decreasing on the entire interval, than the secrecy function attains its maximum at $y=1$, and thus satisfies the conjecture.

- $WEpolyinIpsi[x, \{72,2,8,\{1,0,0,0,0,0,0,8640,124281,1207360\}\}]$

Weight enumerator polynomial in terms of $\xi$ and $\psi$:

$$a_0\psi^{36} + a_1\xi_8\psi^{32} + a_2\xi_8^2\psi^{28} + a_3\xi_8^3\psi^{24} + a_4\xi_8^4\psi^{20} + a_5\xi_8^5\psi^{16} + a_6\xi_8^6\psi^{12} + a_7\xi_8^7\psi^8 + a_8\xi_8^8\psi^4 + a_9\xi_8^9$$

Using lemma we substitute $\xi$ and $\psi$:

$$(x^2 + y^2)^{36}a_0 + x^2y^2(x^2 - y^2)^2(x^2 + y^2)^{32}a_1 + x^4y^4(x^2 - y^2)^4(x^2 + y^2)^{28}a_2 + x^6y^6(x^2 - y^2)^6(x^2 + y^2)^{24}a_3 + x^8y^8(x^2 - y^2)^8(x^2 + y^2)^{20}a_4 + x^{10}y^{10}(x^2 - y^2)^{10}(x^2 + y^2)^{16}a_5 + x^{12}y^{12}(x^2 - y^2)^{12}(x^2 + y^2)^{12}a_6 + x^{14}y^{14}(x^2 - y^2)^{14}(x^2 + y^2)^8a_7 + x^{16}y^{16}(x^2 - y^2)^{16}(x^2 + y^2)^4a_8 + x^{18}y^{18}(x^2 - y^2)^{18}a_9$$

Expanding and collecting the weight enumerator becomes,

$$a_0x^{72} + y^2(36a_0 + a_1)x^{70} + y^4(630a_0 + 30a_1 + a_2)x^{68} + y^6(7140a_0 + 433a_1 + 24a_2 + a_3)x^{66} + y^8(58905a_0 + 4000a_1 + 272a_2 + 18a_3 + a_4)x^{64} + y^{10}(376992a_0 + 26536a_1 + 1928a_2 + 147a_3 + 12a_4 + a_5)x^{62} + y^{12}(1947792a_0 + 134416a_1 + 9528a_2 + 708a_3 + 58a_4 + 6a_5 + a_6)x^{60} + y^{14}(8347680a_0 + 539400a_1 + 34552a_2 + 2157a_3 + 12a_4 + 5a_5 + a_7)x^{58} + y^{16}(30260340a_0 + 1754848a_1 + 93744a_2 + 3942a_3 - 5a_4 - 40a_5 - 12a_6 - 6a_7 + a_8)x^{56} + y^{18}(94143280a_0 + 4692780a_1 + 188136a_2 + 2479a_3 - 632a_4 - 90a_5 + 7a_7 - 12a_8 + a_9)x^{54} + y^{20}(254186856a_0 + 10378056a_1 + 25974a_2 - 7704a_3 - 1244a_4 + 76a_5 + 66a_6 + 28a_7 + 62a_8 - 18a_9)x^{52} + y^{22}(600805296a_0 + 18932940a_1 + 170040a_2 - 24771a_3 - 56a_4 + 406a_5 - 77a_7 - 172a_8 + 153a_9)x^{50} + y^{24}(1251677700a_0 + 28048800a_1 - 215280a_2 - 29854a_3 + 3337a_4 + 120a_5 - 220a_6 - 14a_7 + 237a_8 + 816a_9)x^{48} + y^{26}(2310789600a_0 + 32256120a_1 - 825240a_2 + 759a_3 + 4580a_4 - 925a_5 + 245a_7 + 16a_8 + 3060a_9)x^{46} + y^{28}(3796297200a_0 + 24812400a_1 - 1255800a_2 + 58236a_3 - 1178a_4 - 870a_5 + 495a_6 + 176a_7 - 664a_8 - 856a_9)x^{44} + y^{30}(556790256a_0 + 2481240a_1 - 985320a_2 + 86089a_3 - 9196a_4 + 1143a_5 - 358a_7 + 1104a_8 + 1856a_9)x^{42} + y^{32}(7307872110a_0 - 29774880a_1 + 104880a_2 + 11188a_3 + 58236a_4 + 1143a_5 - 358a_7 + 1104a_8 + 1856a_9)x^{40}$$
\[34086a_3 - 7429a_4 + 1968a_5 - 792a_6 + 532a_7 - 494a_8 - 31824a_9) x^{40} + y^{34} (8597496600a_0 - 58929450a_1 + 1415880a_2 - 66861a_3 + 5168a_4 - 540a_5 + 182a_7 - 936a_8 + 43758a_9) x^{38} + y^{36} (9075135300a_0 - 70715340a_1 + 2005830a_2 - 118864a_3 + 12920a_4 - 2520a_5 + 924a_6 - 728a_7 - 1716a_8 - 48620a_9) x^{36} + y^{38} (8597496600a_0 - 58929450a_1 + 1415880a_2 - 66861a_3 + 5168a_4 - 540a_5 + 182a_7 - 936a_8 + 43758a_9) x^{34} + y^{40} (7307872110a_0 - 29774880a_1 + 104880a_2 - 34068a_3 - 7429a_4 - 1968a_5 - 792a_6 + 532a_7 - 494a_8 - 31824a_9) x^{32} + y^{42} (5567902560a_0 + 2481240a_1 - 985320a_2 + 8608a_3 - 9196a_4 + 1143a_5 - 358a_7 + 1104a_8 + 1856a_9) x^{30} + y^{44} (3796297200a_0 + 2481240a_1 - 125580a_2 + 58236a_3 - 1178a_4 - 870a_5 + 495a_6 - 176a_7 - 664a_8 - 856a_9) x^{28} + y^{46} (2310789600a_0 + 32256120a_1 - 825240a_2 + 759a_3 + 4580a_4 - 925a_5 + 245a_7 + 16a_8 + 3060a_9) x^{26} + y^{48} (1251677700a_0 + 28048800a_1 - 215280a_2 - 29854a_3 + 337a_4 + 120a_5 - 220a_6 - 14a_7 + 237a_8 - 816a_9) x^{24} + y^{50} (6008052960a_0 + 18932940a_1 + 170040a_2 - 24771a_3 - 56a_4 + 406a_5 - 77a_7 - 172a_8 + 153a_9) x^{22} + y^{52} (254186856a_0 + 10378056a_1 + 259740a_2 - 704a_3 - 124a_4 + 76a_5 + 66a_6 + 28a_7 + 62a_8 - 18a_9) x^{20} + y^{54} (94143280a_0 + 4692780a_1 + 188136a_2 + 2479a_3 - 632a_4 - 90a_5 + 7a_7 - 12a_8 + a_9) x^{18} + y^{56} (30260340a_0 + 1754848a_1 + 9374a_2 + 3943a_3 - 5a_4 - 4a_5 - 12a_6 - 6a_7 - 8a_9) x^{16} + y^{58} (8347680a_0 + 539400a_1 + 34552a_2 + 2157a_3 + 124a_4 + 5a_5 + a_7) x^{14} + y^{60} (1947792a_0 + 134416a_1 + 9528a_2 + 708a_3 + 58a_4 + 6a_5 + a_6) x^{12} + y^{62} (376992a_0 + 26536a_1 + 1928a_2 + 147a_3 + 12a_4 + a_5) x^{10} + y^{64} (589050a_0 + 4000a_1 + 272a_2 + 18a_3 + a_4) x^{8} + y^{66} (7140a_0 + 433a_1 + 24a_2 + 3a_3) x^{6} + y^{68} (630a_0 + 30a_1 + a_2) x^{4} + y^{70} (36a_0 + a_1)x^{2} + y^{72} a_0
onumber
\]

Trimming down the list to the first terms to set up sytem of equations

\[
\{x^{72} a_0, x^{70} y^2(36a_0 + a_1), x^{68} y^4(630a_0 + 30a_1 + a_2), x^{66} y^6(7140a_0 + 433a_1 + 24a_2 + a_3), x^{64} y^8(589050a_0 + 4000a_1 + 272a_2 + 18a_3 + a_4), x^{62} y^{10}(376992a_0 + 26536a_1 + 1928a_2 + 147a_3 + 12a_4 + a_5), x^{60} y^{12}(1947792a_0 + 134416a_1 + 9528a_2 + 708a_3 + 58a_4 + 6a_5 + a_6), x^{58} y^{14}(8347680a_0 + 539400a_1 + 34552a_2 + 2157a_3 + 124a_4 + 5a_5 + a_7), x^{56} y^{16}(30260340a_0 + 1754848a_1 + 9374a_2 + 3943a_3 - 5a_4 - 4a_5 - 12a_6 - 6a_7 - 8a_9), x^{54} y^{18}(94143280a_0 + 4692780a_1 + 188136a_2 + 2479a_3 - 632a_4 - 90a_5 + 7a_7 - 12a_8 + a_9)\}
\]

After substituting \(a_i\) values

\[
546\xi_8^6\psi_2^{12} - 3924\xi_5^4\psi_2^{16} + 5031\xi_4^8\psi_2^{20} - 2352\xi_3^8\psi_2^{24} + 450\xi_2^8,\psi_2^{28} - 36\xi_8^8\psi_2^{32} + \psi_2^{36}
\]

Mapping into lattices

\[
\begin{align*}
\vartheta_3^{12} & - 9\vartheta_3^6\vartheta_4^4 + \frac{297\vartheta_3^4\vartheta_4^8}{28048} - \frac{93\vartheta_3^6\vartheta_4^4}{1024} + \frac{40455\vartheta_3^4\vartheta_4^8}{256} - \frac{9329\vartheta_3^8\vartheta_4^4}{256} + \frac{356265\vartheta_3^4\vartheta_4^{10}}{2048} - \frac{2048}{2048}, \nonumber \\
\vartheta_3^8 & - \frac{8199\vartheta_3^4\vartheta_4^8}{2048} + \frac{11943\vartheta_4^{10}}{2048} - \frac{1175\vartheta_3^8\vartheta_4^4}{512} + \frac{122823\vartheta_3^8\vartheta_4^{10}}{2048} - \frac{120555\vartheta_3^8\vartheta_4^{12}}{1024} + \frac{356265\vartheta_3^4\vartheta_4^{10}}{256} - \frac{49299\vartheta_3^{12}}{256}, \nonumber \\
\vartheta_3^4 & - \frac{93\vartheta_3^12}{\vartheta_3^4} + \frac{297\vartheta_3^8\vartheta_4^4}{28048} - \frac{9\vartheta_3^4}{\vartheta_3^4} + 1
\end{align*}
\]
If the function is decreasing on the entire interval, than the secrecy function attains its maximum at $y=1$, and thus satisfies the conjecture

$$\frac{-819\zeta^{11/2}}{1024} - \frac{11175\zeta^{9/2}}{512} - \frac{120555\zeta^{7/2}}{356025\zeta^3} + \frac{49329\zeta^{5/2}}{256} + \frac{93\zeta^3}{2048} + \frac{273\zeta^5}{2048} + \frac{11943\zeta^7}{2048} + \frac{122823\zeta^9}{2048} + 356265\zeta^{11/2} + 40455\zeta^{13/2} + 297\zeta^{15/2} - 9\sqrt{\zeta} + 1$$

### A.3 Wolfram Mathematica Code

#### A.3.1 Type II

```mathematica
WEpolyinIIpsixi[n_(*Length of Code*), b_(* value for psi*), c_(* value for xi*), values_(*values of W_i*)]:=Module[{},
(*Variablesusedduringcomputationthattakeonmultiplevaluesi.e.multiplesubstitutions*)
Quiet[x=.;];
Quiet[y=.;];
Quiet[Do[Subscript[a, i-1]=., {i, Length[values]}]];(*psi and xi specific to doubly even codes*)
Quiet[ψ8=.;];
Quiet[ξ24=.;];
Quiet[Subscript[ϑ, 2]=.;];
Quiet[Subscript[ϑ, 3]=.;]
Quiet[Subscript[ϑ, 4]=.;]
Quiet[s=.;];(*Showing linear combinations of weight enumerator polynomial*)
Print[Style["Weight enumeratropolynomial in terms of ξ and ψ", Bold]];Print[Row[Riffle[Table[(Subscript[a, z]), {z, Range[0, n/c, 1]}] * 
((Subscript[ψ, b])^(Range[n/b, 0, -c/b])) * ((Subscript[ξ, c])^(Range[0, n/c, 1])), "+"])];(*Substituting xi and psi and displaying")
Print[""];
Print[Style["Using Lemma in Julie’s paper we substitute ξ and ψ", Bold]];Print[Total[Table[(Subscript[a, z]), {z, Range[0, n/c, 1]}] *
((x^8 + 14x^4y^4 + y^8)^(Range[n/b, 0, -c/b])) *
```

85
((x^4 \cdot y^4 \cdot (x^4 - y^4)^4 \cdot (\text{Range}[0, n/c, 1]))];
(*Expanding and collecting weight enumerator and printing result*)
Print["""];
Print[Style["Expanding and collecting the weight enumarator becomes,", Bold]];
CollectedExprs =
TraditionalForm[
Collect[
Expand[Total[Table[(Subscript[a, z], {z, Range[0, n/c, 1]})]
\cdot ((x^8 + 14x^4y^4 + y^8)^\cdot (\text{Range}[n/b, 0, -c/b]))
\cdot ((x^4 \cdot y^4 \cdot (x^4 - y^4)^4 \cdot (\text{Range}[0, n/c, 1]))), \{x, y\}]];
Print[CollectedExprs];
(*Trimming down the polynomial to the first terms. This is done to solve for the a_i's*)
Print["""];
Print[Style["Trimming down the list to the first terms to set up system of equations", Bold]];
(*the value 4 in code below specific to doubly even codes and needs to change to 2 for singly even*)
TrimmedExprs = CollectedExprs /. x^q /; q < (n - 4 * (\text{Floor}[n/c])) \rightarrow 0;
TrimmedExprs = TrimmedExprs /. y^p /; p > (4 * (\text{Floor}[n/c])) \rightarrow 0;
(*Turning our polynomial expression into a list, put the total of the expression as the last cell in the list*)
Trimmedlistextra = Level[TrimmedExprs, 2];
Trimmedlistfinal = Delete[Trimmedlistextra, -1];
Print[Trimmedlistfinal];
(*Setting x and y = 1 so that our coefficients can be solved for*)
x = 1;
y = 1;
(*Solving for the coefficients*)
Print["""];
(*Drop [...] tells what variables we're resolving for (a_0, a_1, a_2, ...)*)
Answerlist = Solve[Trimmedlistfinal == values, Drop[{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_10, a_11}, -(12 - Length[values])];
Do[Subscript[a, i - 1] = Answerlist[[All, i, 2]], {i, Length[values]}];
(*Printing out the list of a_i values*)
Print[Drop[{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_10, a_11}, -(12 - Length[values])];
(*Substituting a_i values into weight enumerator, and displaying*)
Print["""];
Print[Style["After substituting a_i values", Bold]];}
Aisubbedlist = Total[Table[(Subscript[a, z], {z, Range[0, n/c, 1]})]
\cdot ((Subscript[\psi, b])^\cdot (\text{Range}[n/b, 0, -c/b]))
\cdot ((Subscript[\xi, c])^\cdot (\text{Range}[0, n/c, 1]));
AisubbedExprs = Aisubbedlist[[1]]; (*pulls first element of Aisubbedlist and set it as AisubbedExprs*)
Print[AisubbedExprs];
(*Translating to theta series by substituting psi and xi this again for specified for
doubly even codes*)
Print[“”];
Print[Style[“Mapping into lattices”, Bold]];
ψ₈ = (Subscript[ϑ, 3] ∧ 8 − Subscript[ϑ, 2] ∧ 4 * Subscript[ϑ, 4] ∧ 4);
(*Print[Subscript[ψ, 8]]; *)
ξ₂₄ = (Subscript[ϑ, 2] ∧ 8 * Subscript[ϑ, 3] ∧ 8 * Subscript[ϑ, 4] ∧ 8)/16;
(*Print[Subscript[ξ, 2₄]]; *)
(*Printing the collected and expanded form of translation*)
Latticelist =
Collect[
Expand[Total[Table[(Subscript[a, z]), {z, Range[0, n/c, 1]}] *
((Subscript[ψ, b])^(Range[n/b, 0, -c/b])) *
((Subscript[ξ, c])^(Range[0, n/c, 1]))], {Subscript[ϑ, 2], Subscript[ϑ, 3], Subscript[ϑ, 4]}];
LatticeExprs = Latticelist[[1]];
Print[LatticeExprs];
Print[TraditionalForm[Total[MonomialList[LatticeExprs]/Subscript[ϑ, 3] ∧ n]]];
Subscript[ϑ, 2] = 1;
Subscript[ϑ, 3] = ζ^(-1/8); (*Specific to doubly even code*)
Subscript[ϑ, 4] = 1;
Secrecyfunction = Expand[Total[MonomialList[LatticeExprs]/Subscript[ϑ, 3] ∧ n]];
Print[TraditionalForm[Secrecyfunction]]; Print[“”];
Print[Style[
*If the function is decreasing on the entire interval, than the secrecy function attains
its maximum at
y=1, and thus satisfies the conjecture”, Bold]]; (*Plot secrecy function*)
Plot[ζ, {ζ, 0, .25}]]

A.3.2 Type I

WEpolyinIpsixi[n_(*Length of Code*), b_(* value for psi*), c_(* value for xi*), values_
(*values of W_i*):=Module[{}], (*Variablesuseddurecomputations that take on multiple values i.e. multiplesubstitutions*)
Quiet[x=.;]
Quiet[y=.;]
Quiet[Do[Subscript[a, i − 1] =., {i, Length[values]}]];
(*psi and xi specific to singly even codes*)
Quiet[ψ₂=.;]
Quiet[ξ₈=.;]
 Quiet[Subscript[ϑ, 2] =.];
Quiet[Subscript[\(\vartheta\), 3] = .];
Quiet[Subscript[\(\vartheta\), 4] = .];
Quiet[s = .];
(* Showing linear combinations of weight enumerator polynomial *)
Print[Style[“Weight enumerator polynomial in terms of \(\xi\) and \(\psi\)”, Bold]]; Print[Row[Riffle[Table[(Subscript[a, z]), {z, Range[0, n/c, 1]}] * ((Subscript[\(\vartheta\), b])^ (Range[n/b, 0, -c/b])) * ((Subscript[\(\vartheta\), c])^ (Range[0, n/c, 1])), “+”]]];
(* Substituting \(x\) and \(y\) and displaying *)
Print[“”];
Print[Style[“Using lemma we substitude \(\xi\) and \(\psi\)”, Bold]]; Print[Total[Table[(Subscript[a, z]), {z, Range[0, n/c, 1]}] * ((x^2 + y^2)^ (Range[n/b, 0, -c/b])) * ((x^2 * y^2 * (x^2 - y^2)^2)^ (Range[0, n/c, 1])), {x, y}]]; (* Expanding and collecting weight enumerator and printing result *)
Print[“”];
Print[Style[“Expanding and collecting the weight enumerator becomes,”, Bold]]; CollectedExprs = TraditionalForm[Collect[Expand[Total[Table[(Subscript[a, z]), {z, Range[0, n/c, 1]}] * ((x^2 + y^2)^ (Range[n/b, 0, -c/b])) * ((x^2 * y^2 * (x^2 - y^2)^2)^ (Range[0, n/c, 1])), {x, y}])];
(* Trimming down the polynomial to the first \(n/c\) + 1 terms. This is done to solve for the \(a_i\)’s *)
Print[“”];
Print[Style[“Trimming down the list to the first terms to set up system of equations”, Bold]]; (* the value 4 in code below specific to doubly even codes and needs to change to 2 for singly even *)
TrimmedExprs = CollectedExprs /. x^ q /; q < (n - 2 * (Floor[n/c])) \[RightArrow] 0;
TrimmedExprs = TrimmedExprs /. y^ p /; p > (2 * (Floor[n/c])) \[RightArrow] 0;
(* Turning our polynomial expression into list, put the total of the expression as the last cell in the list *)
Trimmedlistextra = Level[TrimmedExprs, 2];
Trimmedlistfinal = Delete[Trimmedlistextra, -1];
Print[Trimmedlistfinal]; (* Setting \(x\) and \(y\) = 1 so that our coefficients can be solved for *)
x = 1;
y = 1;
(* Solving for the coefficients *)
Print[“”];
(* Drop[...] tells what variables we resolving for \(a_0, a_1, a_2, \ldots\)*) Answerlist = Solve[Trimmedlistfinal == values, Drop[{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_10, a_11}] ;

88
- \((12 - \text{Length}[\text{values}])\];

Do[Subscript[a, i - 1] = Answerlist[[All, i, 2]], \{i, \text{Length}[\text{values}]\}];

(*Printing out the list of a_i values*)

Print[Drop[\{subscript[a,0], subscript[a,1], subscript[a,2], subscript[a,3], subscript[a,4], subscript[a,5], subscript[a,6], subscript[a,7], subscript[a,8], subscript[a,9], subscript[a,10], subscript[a,11]\}, -(12 - \text{Length}[\text{values}])];

(*Substituting a_i values into weight enumerator, and displaying*)

Print["");

Print[Style["After substituting a_i values", \text{Bold}]];

Aisubbedlist = Total[Table[Subscript[a, z], \{z, \text{Range}[0, n/c, 1]\}]*\((\text{Subscript}[\psi, b])^\text{\text{Range}[n/b, 0, -c/b])\) \ast \((\text{Subscript}[\xi, c])^\text{\text{Range}[0, n/c, 1]}\)];

AisubbedExprs = Aisubbedlist[[1]]; (*pulls first element of Aisubbedlist and set it as AisubbedExprs*)

Print[AisubbedExprs];

(*Translating to theta series by substituting psi and xi this again for specified for doubly even codes*)

Print["");

Print[Style["Mapping into lattices", \text{Bold}]];

\(\psi_2 = \text{Subscript}[\vartheta, 3]^2;\)

(*Print[Subscript[\psi, 2]];*)

\(\xi_8 = (\text{Subscript}[\vartheta, 3]^4 \ast \text{Subscript}[\vartheta, 4]^4 - \text{Subscript}[\vartheta, 4]^8)/4;\)

(*Print[Subscript[\xi, 8]];*)

(*Printing the collected and expanded form of translation*)

Latticelist = Collect[

Expand[Total[Table[Subscript[a, z], \{z, \text{Range}[0, n/c, 1]\}]*\((\text{Subscript}[\psi, b])^\text{\text{Range}[n/b, 0, -c/b])\) \ast \((\text{Subscript}[\xi, c])^\text{\text{Range}[0, n/c, 1]}\)];

LatticeExprs = Latticelist[[1]];]

Print[LatticeExprs];

Print[TraditionalForm[Total[\text{MonomialList}[\text{LatticeExprs}]/\text{Subscript}[\vartheta, 3]^n]]];

\text{Subscript}[\vartheta, 2] = 1;

\text{Subscript}[\vartheta, 3] = \zeta(-1/8); (*Specific to doubly even code*)

\text{Subscript}[\vartheta, 4] = 1;

Secrecyfunction = Expand[Total[\text{MonomialList}[\text{LatticeExprs}]/\text{Subscript}[\vartheta, 3]^n]];}

Print[TraditionalForm[Secrecyfunction]];}

Print[

"If the function is decreasing on the entire interval, than the secrecy function attains its maximum at y=1, and thus satisfies the conjecture";

(*Plot secrecy function*)

Plot[\{\zeta, 0, .25\}]]