ISIT'2013 1569719987

# Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture

Julia Pinchak
Department of Mathematics
California State University Northridge
Northridge, California 91330, USA
Email: julia.pinchak.401@my.csun.edu

***Abstract*—The Belfiore-Solé conjecture states that for a unimodular lattice $\Lambda$ in $\mathbb{R}^n$, the quotient of the theta series of $\mathbb{Z}^n$ by the theta series of $\Lambda$, when restricted to the purely imaginary values $z = \imath y$, $y > 0$, attains its maximum at $y = 1$. This conjecture is vitally connected to the confusion at the eavesdropper's end in wiretap codes for Gaussian channels. In this paper we show that infinitely many lattices satisfy the Belfiore-Solé conjecture on the secrecy function of unimodular lattices. We further show that all lattices obtained by Construction A from binary, doubly even, self-dual codes of lengths up to $40$ satisfy the conjecture.**

## I. Introduction

In [1], Oggier and Belfiore consider the problem of wiretap code design for the Gaussian channel, using coset coding using lattices. Assuming that Eve's channel is more degraded than Bob's channel, they analyze the probability of both users of making a correct decision, and determine conditions under which Eve's probability of correct decoding is minimized. They express these conditions in terms of the properties of the lattices they use, encoded in a function they define called the *secrecy function.* Given a unimodular lattice $\Lambda$ in $\mathbb{R}^n$, they define the secrecy function $\Xi_\Lambda(y)$ by

$$\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^n}(\imath y)}{\Theta_\Lambda(\imath y)}, \quad y > 0. \tag{1}$$

Here, $\Theta_\Lambda(z)$ is the theta series of the lattice $\Lambda$ in terms of the complex variable $z$ (with imaginary part positive), defined by

$$\Theta_\Lambda(z) = \sum_{\mathbf{x}\in\Lambda} q^{||\mathbf{x}||^2}, \quad q = e^{\imath\pi z}, \quad Im(z) > 0. \tag{2}$$

The maximal achievable value of the secrecy function is called the secrecy gain.

In the paper [2], Belfiore and Solé further study the secrecy function of unimodular lattices. They observe, as do the authors in [1], that for a given lattice $\Lambda_e$ used for coset coding, the value of $y$ at which $\Xi_{\Lambda_e}(\imath y)$ obtains its maximum yields the value of the signal-to-noise ratio in Eve's channel that causes maximum confusion to Eve, as compared to using the standard lattice $\mathbb{Z}^n$. Thus, it is vitally important to know at what value of $y$ the secrecy function attains its maximum. The authors in [2] study some examples of lattices and make the following conjecture that is the motivation for this paper:

**Conjecture 1.** *(Belfiore-Solé [2]) The secrecy function of a unimodular lattice attains its maximum at $y = 1$.*

Recall that a unimodular lattice is an integral lattice that equals its dual.

Because the location and value of the maximum of the secrecy function is critical to wiretap code design, this conjecture is of significant interest. In [3], Ernvall-Hytónen shows that all known even, extremal, unimodular lattices satisfy the Belfiore-Solé conjecture, and in [4], the authors Lin and Oggier, using the techniques of [3], show that the conjecture is true for all unimodular lattices of dimension up to 23. Together, these lattices for which the Belfiore-Solé conjecture is so far known to be true form a finite set.

The goal of this paper is to prove the following theorems:

**Theorem 1.** *The Belfiore-Solé conjecture is true for infinitely many unimodular lattices.*

**Theorem 2.** *All unimodular lattices that arise via Construction A from doubly even self-dual codes of length up to $40$ satisfy the Belfiore-Solé conjecture.*

Thus, together, these two theorems significantly expand the cases for which the Belfiore-Solé conjecture is known to be true.

## II. Polynomial Representation of Secrecy Function

In this section we describe in brief the approach in [3] to study the maximum of the secrecy function $\Xi_\Lambda$ of a unimodular lattice $\Lambda$. In [3], Ernvall-Hytónen observed that $\Xi_\Lambda(y)$ can be written as the multiplicative inverse $p(\zeta)^{-1}$ of a polynomial $p$ with rational coefficients in the variable

$$\zeta = \frac{\vartheta_2^4(\imath y)\vartheta_4^4(\imath y)}{\vartheta_3^8(\imath y)}, \tag{3}$$

where $\vartheta_2$, $\vartheta_3$ and $\vartheta_4$ are special functions of the lattice known as Jacobi Theta Functions. These are defined by

$$\vartheta_2(z) = \sum_{n=-\infty}^{\infty} q^{(n+\frac{1}{2})^2}, \tag{4}$$

$$\vartheta_3(z) = \sum_{n=-\infty}^{\infty} q^{n^2}, \tag{5}$$

$$\vartheta_4(z) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2}, \tag{6}$$

where, as before, $q = e^{\imath\pi z}$ and $Im(z) > 0$. Note that $\vartheta_3(z)$ is not zero when $z$ is specialized to $\imath y$, $y > 0$.

Viewing $\zeta$ as a function of $z$, and specializing $z$ to $\imath y$, $y > 0$, she shows that $\zeta(y) = \zeta(\frac{1}{y})$. She uses this to show that $\zeta(y)$ has a *unique* maximum, which occurs when $y = 1$, and this maximum value for $\zeta$ is $\frac{1}{4}$. It follows from this that $\zeta(y)$ takes on values in the range $[0, \frac{1}{4}]$ for $y > 0$. Thus, to show that $\Xi_\Lambda(y)$ takes on its maximum at $y = 1$, we observe that because $\Xi_\Lambda(y) = p(\zeta)^{-1}$, and because $\zeta(y)$ takes on values in $[0, \frac{1}{4}]$, it suffices to show that $p(\zeta)$ is a decreasing function of $\zeta$ for $\zeta$ in the interval $[0, \frac{1}{4}]$. For, if this were to happen, then $p(\zeta)^{-1}$ would be an increasing function of $\zeta$ for $\zeta$ in the interval $[0, \frac{1}{4}]$, and it would hence have its maximum when $\zeta = \frac{1}{4}$. But because $\zeta$ when viewed as a function of $y$ has a *unique* maximum of $\frac{1}{4}$, and this occurs when $y = 1$, we would find that $\zeta = \frac{1}{4}$ precisely when $y = 1$. We would hence have shown that $\Xi_\Lambda(y)$ attains its maximum at $y = 1$.

## III. The class $\mathcal{C}$ of Unimodular Lattices Satisfying the Belfiore-Solé Conjecture

We define the class $\mathcal{C}$ of lattices to consist of those unimodular lattices $\Lambda$ such that if $\Xi_\Lambda(y) = p(\zeta)^{-1}$ for some polynomial $p$ with rational coefficients in the variable $\zeta = \dfrac{\vartheta_2^4(\imath y)\vartheta_4^4(\imath y)}{\vartheta_3^8(\imath y)}$, then the function $p(\zeta)$ is decreasing in the interval $[0, \frac{1}{4}]$. As described above, such lattices automatically satisfy the Belfiore-Solé conjecture. Further, the papers [3] and [4] show that the class $\mathcal{C}$ is not empty: for instance, it contains all extremal even unimodular lattices and all unimodular lattices of dimension up to 23. One of our key results is the following theorem:

**Theorem 3.** *Let $\Lambda_1$ and $\Lambda_2$ be two (not necessarily distinct) lattices in the class $\mathcal{C}$. Then the direct sum $\Lambda_1 \oplus \Lambda_2$ is also in the class $\mathcal{C}$, and therefore, the lattice $\Lambda_1 \oplus \Lambda_2$ also satisfies the Belfiore-Solé conjecture.*

*Proof:* Let $\Lambda_1$ be contained in $\mathbb{R}^{n_1}$ and $\Lambda_2$ in $\mathbb{R}^{n_2}$. Then $\Lambda := \Lambda_1 \oplus \Lambda_2$ is also unimodular, and the secrecy function of $\Lambda$ is given by

$$\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^{n_1+n_2}}(\imath y)}{\Theta_\Lambda(\imath y)}, \quad y > 0. \tag{7}$$

But it is standard that the theta series of the direct sum of two lattices is the product of the two theta series. It follows that

$$\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^{n_1}}(\imath y)}{\Theta_{\Lambda_1}(\imath y)} \frac{\Theta_{\mathbb{Z}^{n_2}}(\imath y)}{\Theta_{\Lambda_2}(\imath y)} = \Xi_{\Lambda_1}\Xi_{\Lambda_2}. \tag{8}$$

Thus, if $\Xi_{\Lambda_1} = p_1(\zeta)^{-1}$ and $\Xi_{\Lambda_2} = p_2(\zeta)^{-1}$, then by the definition of the class $\mathcal{C}$, $p_1$ and $p_2$ are decreasing for $\zeta$ in the interval $[0, \frac{1}{4}]$. In particular, the derivatives of $p_1$ and $p_2$ are both negative in this interval. Now consider the derivative of $p_1p_2$: by Leibniz rule, it equals $p_1(\zeta)p_2'(\zeta) + p_1'(\zeta)p_2(\zeta)$. Observe first that if $L$ is any lattice, then $\Theta_L(y)$ is necessarily positive, because it is an infinite sum of terms of the form $e^{-\pi y||\mathbf{x}||^2}$, where $\mathbf{x}$ ranges through the lattice $L$. Hence secrecy functions, which are quotients of $\Theta_L(y)$ for suitable $L$, are positive. In particular, this means that both $p_1$ and $p_2$ are positive for $\zeta$ in the interval $[0, \frac{1}{4}]$ because their reciprocals yield secrecy functions. By hypothesis, $p_1'(\zeta)$ and $p_2'(\zeta)$ are negative for $\zeta$ in the interval $[0, \frac{1}{4}]$. It follows that the derivative of $p_1p_2$ is negative in the interval $[0, \frac{1}{4}]$, and hence, $\Lambda_1 \oplus \Lambda_2$ also belongs to $\mathcal{C}$. ∎

Theorem 1 follows immediately from this:

*Proof:* (Theorem 1) Pick any $\Lambda$ in $\mathcal{C}$, such as one of the extremal even unimodular lattices or any of the unimodular lattices of dimension up to 23. Then, by Theorem 3, $\Lambda^n := \Lambda \oplus \cdots \oplus \Lambda$ ($n$ summands) is also in $\mathcal{C}$ for any $n$, and hence satisfies the Belfiore-Solé conjecture. Thus infinitely many lattices satisfy the Belfiore-Solé conjecture. ∎

**Remark 1.** We are grateful to one of the anonymous referees for pointing out that the multiplicativity of the secrecy function (Equation 8), along with its positivity, shows something potentially stronger: if $\Lambda_1$ and $\Lambda_2$ are *any two* unimodular lattices satisfying the Belfiore-Solé conjecture, then so does $\Lambda_1 \oplus \Lambda_2$. Of course, it is unknown at this stage if there are unimodular lattices satisfying the conjecture that do not belong to the class $\mathcal{C}$.

## IV. Doubly even Self-dual Codes of Length up to 40

In this section, we show that all unimodular lattices that arise via Construction A from doubly even self-dual codes up to length 40 satisfy the Belfiore-Solé conjecture.

Recall that doubly even codes exist only in lengths divisibly by 8. Because Lin and Oggier have already shown that unimodular lattices up to length 23 satisfy the Belfiore-Solé conjecture in [4], it therefore only remains to show that unimodular lattices arising from binary, doubly even, self-dual codes in lengths $24, 32$, and $40$ satisfy the conjecture. We will use the fact that binary, doubly even, self-dual codes of these lengths have previously been classified, in [7], [8], and [9], respectively, and we will notice that the secrecy functions of all such codes will depend solely on the number of code words of weight 4.

Recall, e.g. [5, Chap. 7], that Construction A starts with a binary code $C$ of length $n$ and dimension $k$ produces a lattice $\Lambda(C)$ of dimension $n$ as follows:

First, note that $C$ is the image of a map $\{0,1\}^k \longmapsto \{0,1\}^n$. Now consider the lattice $\mathbb{Z}^n \in \mathbb{R}^n$, and reduce it mod 2:

$$\rho : \mathbb{Z}^n \longmapsto (\mathbb{Z}/2\mathbb{Z})^n = \{0,1\}^n. \tag{9}$$

Then the lattice $\Lambda(C)$ is defined to be

$$\Lambda(C) = \frac{1}{\sqrt{2}}\rho^{-1}(C) = \bigcup_{c_i \in C} \frac{1}{\sqrt{2}}(2\mathbb{Z}^n + c_i). \tag{10}$$

The dimension of $\Lambda(C)$ is also $n$.

The theta series of a lattice can be obtained from the weight enumerator polynomial using the following lemmas, whose proofs can be found in [5, Chap. 7]:

**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*

$$\Theta_{\Lambda(C)} = W_C(\vartheta_3(2z), \vartheta_2(2z)). \tag{11}$$

**Lemma 2.** *If $C$ is a doubly even code, then*

$$W_C(x,y) \in \mathbf{C}[\psi_8, \xi_{24}], \tag{12}$$

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

We can determine the maps

$$\psi_8 \longmapsto \vartheta_3^8 - \vartheta_2^4\vartheta_4^4, \quad \text{and} \quad \xi_{24} \longmapsto \frac{1}{16}\vartheta_2^8\vartheta_3^8\vartheta_4^8, \tag{13}$$

using Lemma 1, as shown below, with the help of the following Jacobi identities, also found in [5, Chap. 4]:

$$\vartheta_3^2(z) + \vartheta_4^2(z) = 2\vartheta_3^2(2z) \tag{14}$$

$$\vartheta_3^2(z) - \vartheta_4^2(z) = 2\vartheta_2^2(2z) \tag{15}$$

$$\vartheta_2^4(z) + \vartheta_4^4(z) = \vartheta_3^4(z). \tag{16}$$

**$\psi_8$:** The polynomial $\psi_8$ transforms under Lemma 1 to

$$\vartheta_3^8(2z) + 14\vartheta_3^4(2z)\vartheta_2^4(2z) + \vartheta_2^8(2z) \tag{17}$$

Using equations 14, 15, and 16, this becomes

$$\begin{aligned}
&\left(\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_4^2(z)\right)^4 + \left(\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_4^2(z)\right)^4 \\
&\quad + 14\left(\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_4^2(z)\right)^2\left(\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_4^2(z)\right)^2 \\
&= \vartheta_3^8(z) + \vartheta_4^8(z) - \vartheta_3^4(z)\vartheta_4^4(z) \\
&= \vartheta_3^8(z) + \vartheta_4^4(z)[\vartheta_4^4(z) - \vartheta_3^4(z)] \\
&= \vartheta_3^8(z) - \vartheta_2^4(z)\vartheta_4^4(z).
\end{aligned}$$

**$\xi_{24}$:** The polynomial $\xi_{24}$ transforms under Lemma 1 to

$$\begin{aligned}
&[\vartheta_3^4(2z)\vartheta_2^4(2z)][\vartheta_3^4(2z) - \vartheta_2^4(2z)]^4 \\
&= \left(\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_4^2(z)\right)^2\left(\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_4^2(z)\right)^2 \\
&\quad \cdot \left[\left(\frac{1}{2}\vartheta_3^2(z) + \frac{1}{2}\vartheta_4^2(z)\right)^2 - \left(\frac{1}{2}\vartheta_3^2(z) - \frac{1}{2}\vartheta_4^2(z)\right)^2\right]^4 \\
&= \frac{1}{16}\vartheta_3^8(z)\vartheta_4^8(z)[\vartheta_3^4(z) - \vartheta_4^4(z)]^2 \\
&= \frac{1}{16}\vartheta_2^8(z)\vartheta_3^8(z)\vartheta_4^8(z).
\end{aligned}$$

We will now use these maps and lemmas to show that all binary self-dual codes of each length satisfy the Belfiore-Solé conjecture.

### *A. Length 24*

Binary, doubly even, self-dual codes of length 24 have weight enumerator polynomials of the form $W_{C_{24}}(x,y) = x^{24} + W_4x^{20}y^4 + W_8x^{16}y^8 + W_{12}x^{12}y^{12} + \ldots + y^{24}$, where $W_i$ denotes the number of code words of weight $i$, and $W_i = W_{24-i}$. Additionally, by Lemma 2,

$$\begin{aligned}
W_{C_{24}}(x,y) &= a_0\psi_8^3 + a_1\xi_{24} \\
&= a_0(x^8 + 14x^4y^4 + y^8)^3 \\
&\quad + a_1x^4y^4(x^4 - y^4)^4 \\
&= a_0(x^{24} + 42x^{20}y^4 + 591x^{16}y^8 \ldots + y^{24}) \\
&\quad + a_1(x^{20}y^4 - 4x^{16}y^8 + \ldots + x^4y^{20}) \\
&= a_0x^{24} + (42a_0 + a_1)x^{20}y^4 + \ldots
\end{aligned}$$

By comparing the two forms of $W_{C_{24}}(x,y)$, it is easy to see that $a_0$ is 1. This in fact will always be the case for $W_{C_n}(x,y)$, of any length n. Therefore, we have

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

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

$$W_{C_{24}}(x,y) = \psi_8^3 + (W_4 - 42)\xi_{24}, \tag{18}$$

which can be translated to theta series

$$\begin{aligned}
\Theta_{\Lambda(C_{24})} &= (\vartheta_3^8 - \vartheta_2^4\vartheta_4^4)^3 + (W_4 - 42)\frac{1}{16}\vartheta_2^8\vartheta_3^8\vartheta_4^8 \\
&= \vartheta_3^{24} - 3\vartheta_3^{16}\vartheta_2^4\vartheta_4^4 + \frac{W_4 + 6}{16}\vartheta_2^8\vartheta_3^8\vartheta_4^8 - \vartheta_2^{12}\vartheta_4^{12}.
\end{aligned}$$

Because the theta series for $\mathbb{Z}^{24}$ is $\vartheta_3^{24}(z)$, the corresponding secrecy function for a lattice obtained from a binary, doubly even, self-dual code of length 24 is

$$\begin{aligned}
\Xi_{C_{24}} &= \left[1 - 3\zeta + \frac{6 + W_4}{16}\zeta^2 - \zeta^3\right]^{-1} \\
&= \left[\left(1 - 3\zeta + \frac{3}{8}\zeta^2 - \zeta^3\right) + W_4\left(\frac{1}{16}\zeta^2\right)\right]^{-1} \\
&= [p_{24}(\zeta)]^{-1},
\end{aligned}$$

where, as before, $\zeta = \frac{\vartheta_2^4\vartheta_4^4}{\vartheta_3^8}$. The goal, once again, is to show that the polynomial $p_{24}(\zeta)$ is a decreasing function for $\zeta$ in $[0, \frac{1}{4}]$, in which case $\Lambda(C_{24})$ will belong to the class $\mathcal{C}$ and therefore satisfy the Belfiore-Solé conjecture. We therefore differentiate $p_{24}(\zeta)$ and obtain

$$p'_{24}(\zeta) = -3 + \frac{3}{4}\zeta - 3\zeta^2 + W_4\left(\frac{1}{8}\zeta\right). \tag{19}$$

The denominator $p_{24}(\zeta)$ is a linear function in $W_4$, as is its derivative. By [6] and [7], $W_4$ ranges from 0 to 66 in binary, doubly even, self-dual codes of length 24. Therefore, it suffices to show that $p'_{24}(\zeta)$ is negative for $\zeta$ in $[0, \frac{1}{4}]$ when $W_4 = 0$ and when $W_4 = 66$, because it will be negative for all values of $W_4$ in between by linearity. Doing so, we find that for all $W_4 \in [0, 66]$, $p'_{24}(\zeta) < 0$ for $\zeta$ in the interval $\zeta \in [0, \frac{1}{4}]$. Thus

the secrecy function is increasing on this interval and attains its maximum at $y = 1$. Therefore, all lattices arising from binary, doubly even, self-dual codes of length 24 satisfy the Belfiore-Solé conjecture.

### *B. Length 32*

Binary, doubly even, self-dual codes of length 32 have weight enumerators of the form $W_{C_{32}}(x,y) = x^{32} + W_4 x^{28}y^4 + \ldots + y^{32}$. Additionally, by Lemma 2,

$$\begin{aligned} W_{C_{32}}(x,y) &= \psi_8^4 + a_1\psi_8\xi_{24} \\ &= (x^8 + 14x^4y^4 + y^8)^4 + \\ &\quad a_1(x^8 + 14x^4y^4 + y^8)(x^4y^4(x^4 - y^4)^4) \\ &= x^{32} + (56 + a_1)x^{28}y^4 + \ldots \end{aligned}$$

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

$$W_{C_{32}}(x,y) = \psi_8^4 + (W_4 - 56)\psi_8\xi_{24}, \tag{20}$$

which can be translated to a lattice with theta series

$$\begin{aligned} \Theta_{\Lambda(C_{32})} &= \vartheta_3^{32} - 4\vartheta_3^{24}\vartheta_2^4\vartheta_4^4 + \frac{5}{2}\vartheta_3^{16}\vartheta_2^8\vartheta_4^8 - \frac{1}{2}\vartheta_3^8\vartheta_2^{12}\vartheta_4^{12} \\ &\quad + \vartheta_2^{16}\vartheta_4^{16} + W_4\left(\frac{1}{16}\vartheta_3^{16}\vartheta_2^8\vartheta_4^8 - \frac{1}{16}\vartheta_3^8\vartheta_2^{12}\vartheta_4^{12}\right). \end{aligned}$$

The corresponding secrecy function for this lattice is

$$\begin{aligned} &\Xi_{C_{32}} = \\ &\left[1 - 4\zeta + \frac{5}{2}\zeta^2 - \frac{1}{2}\zeta^3 + \zeta^4 + W_4\left(\frac{1}{16}\zeta^2 - \frac{1}{16}\zeta^3\right)\right]^{-1} \\ &= [p_{32}(\zeta)]^{-1}. \end{aligned}$$

The derivative of $p_{32}(\zeta)$ is

$$p'_{32}(\zeta) = \left(-4 + 5\zeta - \frac{3}{2}\zeta^2 + 4\zeta^3\right) + W_4\left(\frac{1}{8}\zeta - \frac{3}{16}\zeta^2\right). \tag{21}$$

Again, $p_{32}(\zeta)$ and $p'_{32}(\zeta)$ are linear in $W_4$. By [8], $W_4$ ranges from 0 to 120 in binary, doubly even, self-dual codes of length 32. For all $W_4 \in [0, 120]$, $p'_{32}(\zeta) < 0$ in the interval $\zeta \in [0, \frac{1}{4}]$. Thus the secrecy function is increasing on this interval and attains its maximum at $y = 1$. Therefore, all lattices arising from binary, doubly even, self-dual codes of length 32 also satisfy the Belfiore-Solé conjecture.

### *C. Length 40*

Binary, doubly even, self-dual codes of length 40 have weight enumerators of the form $W_{C_{40}}(x,y) = x^{40} + W_4 x^{36}y^4 + \ldots + y^{40}$. Additionally, by Lemma 2,

$$\begin{aligned} W_{C_{40}}(x,y) &= \psi_8^5 + a_1\psi_8^2\xi_{24} \\ &= x^{40} + (70 + a_1)x^{36}y^4 + \ldots \end{aligned}$$

Comparing the two equations for the weight enumerator polynomial, we determine that $70 + a_1 = W_4$, so $a_1 = W_4 - 70$. Thus, all binary, doubly even self-dual codes of length 40 can be written as

$$W_{C_{40}}(x,y) = \psi_8^5 + (W_4 - 70)\psi_8^2\xi_{24}, \tag{22}$$

which can be translated to a lattice with theta series

$$\begin{aligned} &\Theta_{\Lambda(C_{40})} = \\ &\quad \vartheta_3^{40} - 5\vartheta_3^{32}\vartheta_2^4\vartheta_4^4 + \frac{45}{8}\vartheta_3^{24}\vartheta_2^8\vartheta_4^8 - \frac{5}{4}\vartheta_3^{16}\vartheta_2^{12}\vartheta_4^{12} \\ &\quad + \frac{5}{8}\vartheta_3^8\vartheta_2^{16}\vartheta_4^{16} - \vartheta_2^{20}\vartheta_4^{20} \\ &\quad + W_4\left(\frac{1}{16}\vartheta_3^{24}\vartheta_2^8\vartheta_4^8 - \frac{1}{8}\vartheta_3^{16}\vartheta_2^{12}\vartheta_4^{12} + \frac{1}{16}\vartheta_3^8\vartheta_2^{16}\vartheta_4^{16}\right). \end{aligned}$$

The corresponding secrecy function for this lattice is

$$\begin{aligned} \Xi_{C_{40}} &= \left[\left(1 - 5\zeta + \frac{45}{8}\zeta^2 - \frac{5}{4}\zeta^3 + \frac{5}{8}\zeta^4 - \zeta^5\right)\right. \\ &\quad \left. + W_4\left(\frac{1}{8}\zeta - \frac{3}{8}\zeta^2 + \frac{1}{4}\zeta^3\right)\right]^{-1} = [p_{40}(\zeta)]^{-1}. \end{aligned}$$

Once again, $p_{40}(\zeta)$ is linear in $W_4$, as is $p'_{40}(\zeta)$. By [9], $W_4$ ranges from 0 to 190 in binary, doubly even, self-dual codes of length 40. For all $W_4 \in [0, 190]$, $p'_{40}(\zeta) < 0$ in the interval $\zeta \in [0, \frac{1}{4}]$. Thus the secrecy function is increasing on this interval and attains its maximum at $y = 1$. Thus, all lattices arising from binary, doubly even, self-dual codes of length 40 satisfy the Belfiore-Solé conjecture as well.

## ACKNOWLEDGMENT

This work constitutes a portion of the author's MS thesis at California State University Northridge (CSUN). She is grateful for her advisor Prof. B.A. Sethuraman's support. She is also grateful to the National Science Foundation for support under Prof. B.A. Sethuraman's grant DMS-0700904, as well as to the Interdisciplinary Research Institute for the Sciences (IRIS) at CSUN as well as the Department of Mathematics for support.

## REFERENCES

[1] Frédérique Oggier and Jean-Claude Belfiore, "Secrecy Gain: a Wiretap Lattice Code Design," in *ISITA*, 2010, pp. 174–178.

[2] Jean-Claude Belfiore and Patrick Solé, "Unimodular Lattices for the Gaussian Wiretap Channel," available online at http://arxiv.org/abs/1007.0449v1.

[3] A.-M. Ernvall-Hytönen, "On a conjecture by Belfiore and Solé on some lattices," available online at http://arxiv.org/abs/1104.3739

[4] Fuchun Lin and Frédérique Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions," available online at http://arxiv.org/pdf/1201.3688.pdf.

[5] J.H. Conway and N.J.A. Sloane, "Sphere Packings, Lattices, and Groups," Springer, 1998.

[6] J. H. Conway and Vera Pless, "On the Enumeration of Self-Dual Codes," *J. Combin. Theo. Ser. A*, vol. 28, pp. 26-53, 1980.

[7] Vera Pless and N.J.A. Sloane, "Binary Self-Dual Codes of Length 24," *Bull. Amer. Math. Soc.*, vol. 80, pp. 1173-1178, 1974.

[8] J.H. Conway, V. Pless, and N.J.A. Sloane, "The Binary Self-dual Codes of Length Up To 32: A Revised Enumeration," *J. Combin. Theo. Ser. A*, vol. 60, 1pp. 83-195, 1992.

[9] Koichi Betsumiya, Masaaki Harada, and Akihiro Munemasa, "A Complete Classification of Doubly Even Self-dual Codes of Length 40," *Electronic J. Combin.*, vol. 19, 2012.

[10] Frédérique Oggier, Patrick Solé, and Jean-Claude Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis," available online at http://arxiv.org/abs/1103.4086v1.