The Belfiore-Solé Conjecture and a Certain Technique for Verifying it for a Given Lattice

Julia Pinchak
Department of Mathematics
California State University Northridge
Northridge, CA 93130, USA
Email: jpinchak@gmail.com

B.A. Sethuraman
Department of Mathematics
California State University Northridge
Northridge, CA 93130, USA
Email: al.sethuraman@csun.edu

***Abstract*—We discuss a technique provided by Ernvall-Hytónen for verifying the Belfiore-Solé conjecture for unimodular lattices, a conjecture that arises in the theory of wiretap lattice codes for the Gaussian channel. We provide an alternative proof of a key lemma of Ernvall-Hytónen that avoids dependence on a machine for verification, and as a further example of the technique, we verify the Belfiore-Solé conjecture for unimodular lattices in dimension 34 that arise from certain binary $[34, 17, 6]$ codes, which includes some with trivial automorphism group.**

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 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 Λ 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 Λ 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 Λ_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 $y = 1$.*

All attempts to prove the Belfiore-Solé conjecture so far ([3], [4], [5]) have been based on a lovely technique of Ernvall-Hytónen ([3]). Her technique furnishes a condition on a certain *polynomial* that when true, is sufficient to show that the Belfiore-Solé conjecture holds for any given unimodular lattice. What is necessary for applying this condition is knowledge of the theta series of the lattice, but once the theta series is known, the ratio of infinite theta series is replaced by a single polynomial of degree at most $\lfloor \frac{n}{8} \rfloor$.

The goal of this short note is to give an alternative proof of a key result that goes into Ernvall-Hytónen's technique—this alternative proof uses purely analytical methods and avoids the machine dependency of the original paper—and to then illustrate the technique on lattices of length 34 built via Construction A from certain self-dual $[34, 17, 6]$ codes (these include some codes having trivial automorphism group). We find that all such lattices satisfy the Belfiore-Solé conjecture, a fact that was previously unknown.

II. The technique of Ernvall-Hytónen

Ernvall-Hytónen begins with the known result that the theta series of a unimodular lattice is a polynomial $\sum a_r \vartheta_3^{n-8r} \Delta_8^r$ for r running from 0 to $\lfloor \frac{n}{8} \rfloor$ in two other (algebraically independent) modular forms ϑ_3 and $\Delta_8 = \frac{\vartheta_2^4 \vartheta_4^4}{16}$. Here, ϑ_2, ϑ_3 and ϑ_4 are special functions on the upper half plane (i.e., z such that $Im(z) > 0$), defined via the following infinite series in the variable $q = e^{\imath\pi z}$:

$$\vartheta_2(z) = \sum_{n=-\infty}^{\infty} q^{(n+\frac{1}{2})^2}, \tag{3}$$

$$\vartheta_3(z) = \sum_{n=-\infty}^{\infty} q^{n^2}, \tag{4}$$

$$\vartheta_4(z) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2}, \tag{5}$$

Using the absolute convergence for all three series for $|q| < 1$ and rewriting them by combining terms indexed by $+n$ and $-n$, it is easy to see that none of the three series sums to zero when z is specialized to $\imath y$, $y > 0$.

The theta series of $\mathbb{Z}^n$ is in fact just ϑ_3^n. Writing the theta series of Λ as $\sum a_r \vartheta_3^{n-8r} \Delta_8^r$ and writing Δ_8 in terms of ϑ_2

and ϑ_4 as above, we find that the secrecy function $\Xi_\Lambda(y)$ (where z is now constrained to be of the form $\imath y$, $y > 0$) is given by the multiplicative inverse of a polynomial expression $p(\zeta)$ of degree at most $\lfloor \frac{n}{8} \rfloor$, where $\zeta = \dfrac{\vartheta_2^4(\imath y)\vartheta_4^4(\imath y)}{\vartheta_3^8(\imath y)}$. The quantity ζ, as a function of y, satisfies the multiplicative symmetry $\zeta(1/y) = \zeta(y)$: this follows from analogous symmetry properties of the modular forms ϑ_2, ϑ_3, and ϑ_4. Ernvall-Hytónen then uses the symmetry of ζ to prove that $\zeta(y)$ has a unique maximum at $y = 1$, and this maximum is $\dfrac{1}{4}$. 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 $y = 1$, Ernvall-Hytónen observes 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 ζ for ζ in the interval $[0, \frac{1}{4}]$. For, if this were to happen, then $p(\zeta)^{-1}$ would be an increasing function of ζ for ζ in the interval $[0, \frac{1}{4}]$, and it would hence have its maximum when $\zeta = \frac{1}{4}$. But because ζ when viewed as a function of y has a *unique* maximum of $\frac{1}{4}$, and this occurs when $y = 1$, one would find that $\zeta = \frac{1}{4}$ precisely when $y = 1$. One would hence have shown that $\Xi_\Lambda(y)$ attains its maximum at $y = 1$.

To apply this technique to any one particular lattice, we only need to consider its theta series, compute the polynomial $p(\zeta)$, and show that p decreases in the interval $[0, \frac{1}{4}]$ to be able to conclude that this lattice satisfies the Belfiore-Solé conjecture.

III. Alternative proof of a key lemma of Ernvall-Hytónen

The key to this technique is the result that $\zeta(y)$ attains its unique maximum at $y = 1$. Ernvall-Hytónen's proof involves the manipulation of infinite products and careful considerations of certain infinite series. At a key point in her proof, she needs to consider the solution of a sixth degree polynomial equation, two real roots of which she determines by machine calculations. More critically, she has to resort to the machine to be able to say that there are no further real roots—a necessary ingredient of her arguments. Although this is sound, it is preferable to have a proof that can be checked without recourse to a machine, and we furnish such a proof below. Note that this proof does not invoke the multiplicative symmetry of $\zeta(y)$ either.

Lemma 1. *([3]) The function $\zeta(y)$ defined above for $y > 0$ has a unique maximum at $y = 1$, where its value is $\frac{1}{4}$.*

Proof: It is sufficient to show that $\sqrt{\frac{1}{\zeta}} = \frac{\vartheta_3^4}{\vartheta_4^2\vartheta_2^2}$ has a unique minimum at $y = 1$ (note that none of ϑ_2, ϑ_3 or ϑ_4 are zero for $z = \imath y$, $y > 0$, as already observed in the previous section). By e.g. [6, Chap. 4], $\vartheta_3^4 = \vartheta_2^4 + \vartheta_4^4$. Thus, we need to show that $(\frac{\vartheta_4}{\vartheta_2})^2 + (\frac{\vartheta_2}{\vartheta_4})^2$ has a unique minimum at $y = 1$. Putting $x = \frac{\vartheta_4}{\vartheta_2}$, we notice by calculus that $x^2 + (\frac{1}{x})^2$ has minima precisely at $x = \pm 1$. Thus, at any minimum of $(\frac{\vartheta_4}{\vartheta_2})^2 + (\frac{\vartheta_2}{\vartheta_4})^2$, we must have $\vartheta_4 = \vartheta_2$, since we may ignore $x = -1$ as both ϑ_4 and ϑ_2 are positive.

We thus wish to find y such that $\vartheta_4(\imath y) = \vartheta_2(\imath y)$. Invoking another identity, from e.g, [6, Chap. 4], we have $\vartheta_2(-\frac{1}{z}) = (\frac{z}{\imath})^{1/2}\vartheta_4(z)$ (where the square root is the principal value). Putting $z = \imath y$, we need to solve $\vartheta_2(\frac{\imath}{y}) = \sqrt{y}\vartheta_2(\imath y)$. Clearly $y = 1$ is a solution, and we need to show that it is the only solution.

We invoke the power series representation of ϑ_2 (Equation (3)). Invoking absolute convergence for $|q| < 1$, we may group the terms with indices $+n$ and $-n$ and write $\vartheta_2(\imath y) = 2q^{1/4}(1 + q^2 + q^6 + q^{12} + \cdots)$. Now let us specifically use q for $e^{-\frac{\pi}{y}}$ and p for $e^{-\pi y}$. First consider the case $y > 1$, we wish to show that $\vartheta_2(\frac{\imath}{y}) \neq \sqrt{y}\vartheta_2(\imath y)$. Since $q > p > 0$ when $y > 1$, it is enough to show that $\frac{\sqrt{y}p^{1/4}}{q^{1/4}} < 1$ when $y > 1$, since then, $\vartheta_2(\frac{\imath}{y}) - \sqrt{y}\vartheta_2(\imath y) = 2q^{1/4}\left((1 + q^2 + \cdots) - \frac{\sqrt{y}p^{1/4}}{q^{1/4}}(1 + p^2 + \cdots)\right)$, and each term in the series on the left will be greater than the corresponding term in the series on the right. Similarly, if we consider the case $y < 1$, then $p > q > 0$, and it is enough to show that $\frac{\sqrt{y}p^{1/4}}{q^{1/4}} > 1$ when $y < 1$

It is sufficient to show that the fourth power $\frac{y^2 e^{-\pi y}}{e^{-\frac{\pi}{y}}}$ is greater than 1 for $y < 1$ and less than 1 for $y > 1$. But this is an easy calculus exercise: the function is 1 at $y = 1$, and the derivative of the function is negative for all $y > 0$.

The fact that the value of ζ at 1 is $\frac{1}{4}$ is easy to see: At $y = 1$, we have already seen that $\vartheta_2(\imath) = \vartheta_4(\imath)$. Thus, $\zeta(\imath) = (\frac{\vartheta_2(\imath}{\vartheta_3(\imath)})^8$. The identity $\vartheta_2(z)^4 + \vartheta_4(z)^4 = \vartheta_3(z)^4$ now shows that $(\frac{\vartheta_2(\imath}{\vartheta_3(\imath)})^4 = \frac{1}{2}$. The result follows immediately. ∎

IV. Unimodular lattices in dimension 34 and the Belfiore-Solé conjecture

We give an example of the use of Ernvall-Hytónen's technique by showing that unimodular lattices in dimension 34 that arise from certain binary $[34, 17, 6]$ self-dual codes (which includes some with trivial automorphism group) via Construction A satisfy the Belfiore-Solé conjecture. The key to this is the classification of the weight enumerator polynomial in [7]. All such codes have weight enumerators $W(x, y)$ given by $x^{34} + (34 - 4\beta)x^{28}y^6 + (255 + 4\beta)x^{26}y^8 + (1921 + 20\beta)x^{24}y^{10} + (8466 - 20\beta)x^{22}y^{12} + \cdots$ (see [7, Section 3]), where β is an integer, or by $x^{34} + 6x^{28}y^6 + 411x^{26}y^8 + 1165x^{24}y^{10} + 10886x^{22}y^{12} + \cdots$. We show the calculations here for the first case, where codes are known to exist for $\beta = 0, 1, \ldots, 7$. Codes with trivial group have values 2, 3 and 4 for β, as reported in [7]. (The positive resolution of the Belfiore-Solé conjecture for these lattices has not been reported before in the literature, as far as we are aware.)

Recall, e.g. [6, 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:

$$\rho : \mathbb{Z}^n \longmapsto (\mathbb{Z}/2\mathbb{Z})^n = \{0,1\}^n . \tag{6}$$

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

$$\Lambda(C) = \frac{1}{\sqrt{2}}\rho^{-1}(C) = \bigcup_{c_i \in C} \frac{1}{\sqrt{2}}(2\mathbb{Z}^n + c_i). \tag{7}$$

By Gleason's theorem (see [6, Chapter 7] for instance), the weight enumerator polynomial of a binary self dual code may be written as a polynomial in $\psi_2 = x^2 + y^2$ and $\xi_8 = x^2y^2(x^2 - y^2)^2$. Invoking the homogeneity of $W(x, y)$ in x and y, we may write $W(x, y) = x^{34} + (34 - 4\beta)x^{28}y^6 + (255+4\beta)x^{26}y^8+(1921+20\beta)x^{24}y^{10}+(8466-20\beta)x^{22}y^{12}+ \cdots = a_0\psi_2^{17} + a_1\psi_2^{13}\xi_8 + a_2\psi_2^9\xi_8^2 + a_3\psi_2^5\xi_8^3 + a_4\psi_2\xi_8^4$. Equating powers of x^iy^{34-i} on both sides, we find $a_0 = 1, a_1 = -17, a_2 = 51, a_3 = (34 - 4\beta) - 34 = -4\beta$, and $a_4 = (255 + 4\beta) - 289 = -34 + 4\beta$.

The theta series of the lattice formed by Construction A is given by $\Theta_\Lambda = W(\vartheta_3(2z), \vartheta_2(2z))$ (see e.g., [6, Chapter 7]). Write A for $\vartheta_3(z)^2$, B for $\vartheta_2(z)^2$, and C for $\vartheta_4(z)^2$. Under the map $x \mapsto \vartheta_3(2z)$ and $y \mapsto \vartheta_2(2z)$, we find upon using the identities $\vartheta_3(z)^2+\vartheta_4(z)^2 = 2\vartheta_3(2z)^2$ and $\vartheta_3(z)^2-\vartheta_4(z)^2 = 2\vartheta_2(2z)^2$ ([6, Chapter 5]) that ψ_2 maps to A. Using these same identities along with one we have considered earlier: $\vartheta_2(z)^4 + \vartheta_4(z)^4 = \vartheta_3(z)^4$ we find that ξ_8 maps to $\frac{B^2C^2}{4}$.

We thus find on writing the theta series of $\mathbb{Z}^{34}$ as A^{17}, and that of Λ as $a_0A^{17} + a_1A^{13}\frac{B^2C^2}{4} + \cdots$ that $\Xi(\Lambda)$ is given by

$$\frac{1}{p(x)} = \frac{1}{1 - \frac{17x}{4} + \frac{51x^2}{4^2} - \frac{4\beta x^3}{4^3} + \frac{(-34+4\beta)x^4}{4^4}}$$

where we have written x for $\frac{B^2C^2}{A^4} = \zeta$, ζ as considered earlier. We need to show that $p(x)$ is decreasing in $[0, \frac{1}{4}]$. The derivative of $p(x)$ is

$$p'(x) = -\frac{17}{4} + \frac{51 \cdot 2x}{4^2} - \frac{4\beta \cdot 3x^2}{4^3} + \frac{(-34 + 4\beta) \cdot 4x^3}{4^4}$$

This is a cubic, and for a given value of β, can be solved analytically using Cardano's method for instance, without recourse to machine computation. But for values of β from 0 through 7, we can argue for our purposes as follows: Since the coefficient of x^3 is negative, $p'(x)$ is clearly positive for large negative values of x. Also, $p'(0) - \frac{17}{4} < 0$. Thus $p'(x)$ has one real root at least between $-\infty$ and 0. Recall that the discriminant of the cubic $ax^3 + bx^2 + cx + d$ is given by the formula $18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$. Since the discriminant of $p'(x)$ for each of the values of β in the range 0 through 7 is negative, the field generated by the roots contains an imaginary quadratic subfield, and hence cannot be real. Thus the other two roots must be complex, and this negative root must be the only real solution. Since in each of these cases, $p'(0) = -\frac{17}{4}$ and since p' does not cross the x-axis anywhere in $[0, \frac{1}{4}]$, p' must be negative everywhere on $[0, \frac{1}{4}]$. This establishes our result and shows that the Belfiore-Solé conjecture holds for these lattices.

ACKNOWLEDGMENT

The second-named author is partially supported by a grant (CCF-1318260) from the National Science Foundation.

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] Julia Pinchak, " Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture," Proceedings of ISIT 2013, pp. 2617–2620.

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

[7] J.H. Conway and N.J.A. Sloane, "A New Upper Bound on the Minimal Distance of Self-Dual Codes," *IEEE Transactions on Information Theory,* vol. 36, no. 6, November 1990. *Bull. Amer. Math. Soc.*, vol. 80, pp. 1173-1178, 1974. *J. Combin. Theo. Ser. A*, vol. 60, 1pp. 83-195, 1992.

[8] 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.