

ON THE SECRECY GAIN OF ℓ -MODULAR LATTICES

ESA V. VESALAINEN AND ANNE-MARIA ERNVALL-HYTÖNEN

ABSTRACT. We show that for every $\ell > 1$, there is a counterexample to the ℓ -modular secrecy function conjecture by Oggier, Solé and Belfiore. These counterexamples all satisfy the modified conjecture by Ernvall-Hytönen and Sethuraman. Furthermore, we provide a method to prove or disprove the modified conjecture for any given ℓ -modular lattice rationally equivalent to a suitable amount of copies of $\mathbb{Z} \oplus \sqrt{\ell} \mathbb{Z}$ with $\ell \in \{3, 5, 7, 11, 23\}$. We also provide a variant of the method for strongly ℓ -modular lattices when $\ell \in \{6, 14, 15\}$.

1. INTRODUCTION

Wyner [21] introduced the wiretap channel as a discrete memoryless and possibly noisy broadcast channel, where the sender transmits confidential messages to a legitimate receiver in the presence of an eavesdropper. Belfiore and Oggier defined in [1] the secrecy gain

$$\max_{y \in \mathbb{R}_+} \frac{\Theta_{\mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)},$$

where

$$\Theta_{\Lambda}(y) = \sum_{x \in \Lambda} e^{-\pi \|x\|^2 y}$$

for $y \in \mathbb{R}_+$, as a lattice invariant to measure how much confusion the eavesdropper will experience when a unimodular lattice Λ is used in Gaussian wiretap coding. Here we have simplified notation by writing $\Theta_{\Lambda}(y)$ instead of the traditional $\Theta_{\Lambda}(yi)$ as this is more convenient. The function $\Xi_{\Lambda}(y) = \Theta_{\mathbb{Z}^n}(y)/\Theta_{\Lambda}(y)$ is called the secrecy function. Belfiore and Solé [2] conjectured that the secrecy function attains its maximum at $y = 1$. This function was further studied by Oggier, Solé and Belfiore [14], by Lin and Oggier [11, 12], and by Ernvall-Hytönen and Hollanti [4]. A method to prove the conjecture for any given lattice was derived by Ernvall-Hytönen [3], and a new proof for this method was given by Pinchak and Sethuraman [15, 16].

An n -dimensional integral lattice Λ is ℓ -modular, where $\ell \in \mathbb{Z}_+$, if there exists a similarity σ of \mathbb{R}^n multiplying norms by ℓ and mapping Λ^* to Λ . Oggier, Solé and Belfiore [14] defined the secrecy function Ξ_{Λ} for ℓ -modular lattices by

$$\Xi_{\Lambda}(y) = \frac{\Theta_{(\ell^{1/4}\mathbb{Z})^n}(y)}{\Theta_{\Lambda}(y)},$$

This work was supported by the Academy of Finland project 303820, and E. V. V. was supported by the Magnus Ehrnrooth Foundation, by the Basque Government through the BERC 2014–2017 program and by Spanish Ministry of Economy and Competitiveness MINECO: BCAM Severo Ochoa excellence accreditation SEV-2013-0323.

again for $y \in \mathbb{R}_+$, when n is the dimension of the lattice Λ . So, the lattice Λ is compared against a cubic lattice with the same volume. This quantity for 2-modular and 3-modular lattices was studied by Lin, Oggier and Solé [13], and for 5-modular lattices by Hou, Lin and Oggier [8], and in the thesis by Lin [10]. Furthermore, it was conjectured that this function obtains its maximum at the natural symmetry point $1/\sqrt{\ell}$. It was proved by Ernvall-Hytönen and Sethuraman that this is not always the case: they provided the 4-modular lattice $2\mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \mathbb{Z}$ as a counterexample. Strey [20] provided pictures of some other counterexamples. In this paper, we show that these values of ℓ are not exceptions: there are counterexamples for every integer value $\ell > 1$.

Ernvall-Hytönen and Sethuraman [5] suggested normalizing with a suitable power of the theta function of the lattice D^ℓ , instead of the scaled cubic lattice:

$$\tilde{\Theta}_\Lambda(y) = \frac{\Theta_{D^\ell}^{n/2}(y)}{\Theta_\Lambda(y)},$$

where n is the dimension of the lattice Λ and $y \in \mathbb{R}_+$. It is worth noting that n is even unless ℓ is a square. They conjectured that the secrecy function conjecture would be true when the normalization is done using this lattice instead of the cubic lattice. This normalization has the added benefit that the lattice D^ℓ is ℓ -modular (not necessarily strongly ℓ -modular). Furthermore, they gave a method to prove or disprove this modified conjecture for any given 2-modular lattice.

We will show that whenever $\ell \in \{3, 5, 7, 11, 23\}$ and an ℓ -modular lattice is rationally equivalent to the direct sum of $n/2$ copies of D^ℓ , to check whether the function Θ_Λ satisfies the modified conjecture formulated by Ernvall-Hytönen and Sethuraman, it suffices to check whether a certain polynomial obtains its minimal value on the interval

$$\left] 0, \left(\frac{\eta\left(\frac{1}{2\sqrt{\ell}}\right) \eta\left(\frac{2}{\sqrt{\ell}}\right) \eta\left(\frac{\sqrt{\ell}}{2}\right) \eta\left(2\sqrt{\ell}\right)}{\eta^2\left(\frac{1}{\sqrt{\ell}}\right) \eta^2\left(\sqrt{\ell}\right)} \right)^{\alpha_\ell} \right]$$

at the right endpoint, where η is the classical Dedekind η -function discussed in more detail later and the exponent α_ℓ is defined precisely in Section 5. The polynomial is obtained from the representation for Θ_Λ given by Rains and Sloane [17].

This paper is structured as follows: We first in Section 2 give a useful convolution identity. We will then move in Section 3 to the conjecture by Hernandez and Sethuraman about the behavior of the function ϑ_3 , and we determine exactly when the conjecture is true. In Section 4 we give counterexamples to the original ℓ -modular conjecture and prove that they satisfy the modified conjecture. In Section 5, we give a method to prove or disprove the modified conjecture under certain conditions for any given ℓ -modular lattice for certain values of ℓ . The last two Sections 6 and 7 give some rather technical lemmas about ϑ_3 and η needed in the proofs.

2. A CONVOLUTION IDENTITY

The following simple convolution identity will be quite useful for us later. For any given real numbers h and k with $0 \leq k < h$, we define the auxiliary trapezoid function $T(\cdot; k, h): \mathbb{R} \rightarrow \mathbb{R}$, depicted in Figure 1, by setting

$$T(x; k, h) = \begin{cases} 0 & \text{when } x \leq -h, \\ x + h & \text{when } -h \leq x \leq -k, \\ h - k & \text{when } -k \leq x \leq k, \\ h - x & \text{when } k \leq x \leq h, \text{ and} \\ 0 & \text{when } x \geq h, \end{cases}$$

for all $x \in \mathbb{R}$. Of course, for $k = 0$ the trapezoid reduces to a triangle.

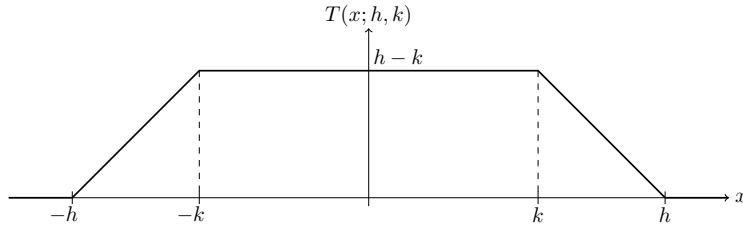


FIGURE 1. The function $T(x; k, h)$.

Lemma 1. *Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a twice continuously differentiable function, and let $h, k \in [0, \infty[$ with $k < h$. Then*

$$f(x+h) - f(x+k) - f(x-k) + f(x-h) = \int_{-\infty}^{\infty} f''(u) T(u-x; k, h) du,$$

for all $x \in \mathbb{R}$.

Proof. By straightforward calculation, we have

$$\begin{aligned} \int_{-\infty}^{\infty} f''(u) T(u-x; k, h) du &= \int_{-\infty}^{\infty} f''(x+u) T(u; k, h) du \\ &= \int_{-h}^{-k} f''(x+u) (u+h) du + \int_{-k}^k f''(x+u) (h-k) du + \int_k^h f''(x+u) (h-u) du \\ &= \left[f'(x+u) (u+h) \right]_{-h}^{u=-k} - \int_{-h}^{-k} f'(x+u) du + (h-k) f'(x+k) - (h-k) f'(x-k) \end{aligned}$$

$$\begin{aligned}
& + f'(x+u)(h-u) \Big|_k^{u=h} + \int_k^h f'(x+u) \, du \\
& = (h-k) f'(x-k) - f(x-k) + f(x-h) + (h-k) f'(x+k) \\
& \quad - (h-k) f'(x-k) - (h-k) f'(x+k) + f(x+h) - f(x+k) \\
& = f(x+h) - f(x+k) - f(x-k) + f(x-h),
\end{aligned}$$

as claimed. □

3. CONJECTURE OF HERNANDEZ AND SETHURAMAN

The classical function ϑ_3 is defined by setting

$$\vartheta_3(y) = \Theta_{\mathbb{Z}}(y) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 y} = 1 + 2 \sum_{n=1}^{\infty} e^{-\pi n^2 y}$$

for all $y \in \mathbb{R}_+$, where we have employed the usual simplification of notation by writing $\vartheta_3(y)$ instead of $\vartheta_3(yi)$. The results in Section 4 depend on understanding the behaviour of certain kinds of expressions involving ϑ_3 .

Hernandez and Sethuraman [9, 19] made the following conjecture which is Conjecture 8 in [9]:

Conjecture 2 (Hernandez and Sethuraman). *Let $a, b \in \mathbb{R}_+$. Then the expression*

$$\frac{\vartheta_3(y) \vartheta_3(aby)}{\vartheta_3(ay) \vartheta_3(by)},$$

defined for $y \in \mathbb{R}_+$, obtains its unique maximum at $1/\sqrt{ab}$.

This conjecture was supported by several illustrations. The following theorem implies that the conjecture is essentially true, except for some ranges of a and b where the behaviour of the expression is naturally opposite. In Section 4, Theorem 3 is used to both derive counterexamples to the original ℓ -modular conjecture and to prove that the counterexamples satisfy the modified conjecture.

Theorem 3. *Let $\kappa, \lambda \in \mathbb{R}_+$ with $1 \leq \kappa < \lambda$, and let us define a function $g: \mathbb{R}_+ \rightarrow \mathbb{R}_+$ by setting*

$$g(y) = \frac{\vartheta_3(\lambda y) \vartheta_3(y/\lambda)}{\vartheta_3(\kappa y) \vartheta_3(y/\kappa)}$$

for $y \in \mathbb{R}_+$. Then the function g has a strict global maximum at the point 1, is strictly increasing in $]0, 1]$, and is strictly decreasing in $[1, \infty[$.

The proof of the theorem requires some very technical lemmas which are stated and proved in Section 6.

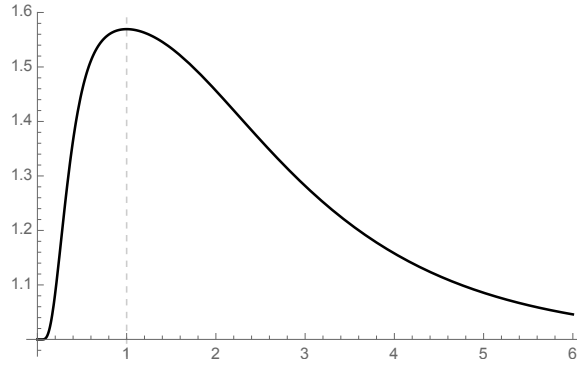


FIGURE 2. The function $g(y)$ of Theorem 3 with $\kappa = 2$ and $\lambda = 5$.

Proof. Let us first observe that by the modularity relation satisfied by ϑ_3 , we have

$$\vartheta_3\left(\frac{1}{y}\right) = \sqrt{y} \vartheta_3(y)$$

for all $y \in \mathbb{R}_+$, and that this implies easily that

$$g\left(\frac{1}{y}\right) = g(y)$$

for all $y \in \mathbb{R}_+$. The function g is also clearly real-analytic. Thus, it is enough to prove that g is strictly decreasing in $]1, \infty[$.

Let us write $f(x) = \log \vartheta_3(e^x)$, $x = \log y$, $h = \log \lambda$ and $k = \log \kappa$. Then

$$\log g(y) = \log \frac{\vartheta_3(\lambda y) \vartheta_3(y/\lambda)}{\vartheta_3(\kappa y) \vartheta_3(y/\kappa)} = f(x+h) - f(x+k) - f(x-k) + f(x-h),$$

and we need to prove that the last expression is strictly decreasing for $x \in \mathbb{R}_+$. By Lemma 1, we may rewrite this expression as a convolution against $T(\cdot; k, h)$ as

$$f(x+h) - f(x+k) - f(x-k) + f(x-h) = \int_{-\infty}^{\infty} f''(u) T(u-x; k, h) du.$$

Since f'' is infinitely smooth and $T(\cdot; k, h)$ is continuous and compactly supported, the last integral is differentiable with derivative

$$\frac{d}{dx} \int_{-\infty}^{\infty} f''(u) T(u-x; k, h) du = \int_{-\infty}^{\infty} f'''(u) T(u-x; k, h) du,$$

and the problem is reduced to proving that the last integral is strictly negative for $x \in \mathbb{R}_+$. Before embarking on this, let us invoke Lemma 12 which says that the third derivative f''' is an odd function on \mathbb{R} and strictly negative in \mathbb{R}_+ .

Let us now start treating the integral by observing that the function $T(\cdot - x; k, h)$ is supported on $[x - h, x + h]$, and so

$$\int_{-\infty}^{\infty} f'''(u) T(u - x; k, h) du = \int_{x-h}^{x+h} f'''(u) T(u - x; k, h) du.$$

In particular, if $x \geq h$, then the integrand is strictly negative in $]x - h, x + h[$. Thus, we may assume that $x \in]0, h[$.

We now split the integral into pieces and rearrange them, remembering that $f'''(\cdot)$ is an odd function, and that $T(\cdot; k, h)$ is an even function, to get

$$\begin{aligned} & \int_{x-h}^{x+h} f'''(u) T(u - x; k, h) du \\ &= \int_{x-h}^0 f'''(u) T(u - x; k, h) du + \int_0^{h-x} f'''(u) T(u - x; k, h) du + \int_{h-x}^{h+x} f'''(u) T(u - x; k, h) du \\ &= - \int_0^{h-x} f'''(u) T(u + x; k, h) du + \int_0^{h-x} f'''(u) T(u - x; k, h) du + \int_{h-x}^{h+x} f'''(u) T(u - x; k, h) du \\ &= \int_0^{h-x} f'''(u) (T(u - x; k, h) - T(u + x; k, h)) du + \int_{h-x}^{h+x} f'''(u) T(u - x; k, h) du. \end{aligned}$$

Here the last integral is again strictly negative since the integrand is, and so it is enough to prove that the second to the last integral is nonnegative. Since f''' is again strictly negative in the integrand in $]0, h - x[$, it is enough to prove that $T(u + x; k, h) \leq T(u - x; k, h)$ for $u \in]0, h - x[$. But this last inequality is geometrically obvious, and we are done. \square

Let us now look at the original conjecture. Assume that $a, b \in \mathbb{R}_+$ with $a \leq b$. If $a = 1$ or $b = 1$ then the ϑ_3 -expression reduces to a constant, so let us assume that $a \neq 1$ and $b \neq 1$. We can write the expression as

$$\frac{\vartheta_3(y) \vartheta_3(aby)}{\vartheta_3(ay) \vartheta_3(by)} = \frac{\vartheta_3\left(\frac{1}{\sqrt{ab}}(\sqrt{ab}y)\right) \vartheta_3\left(\sqrt{ab}(\sqrt{ab}y)\right)}{\vartheta_3\left(\sqrt{\frac{a}{b}}(\sqrt{ab}y)\right) \vartheta_3\left(\sqrt{\frac{b}{a}}(\sqrt{ab}y)\right)}.$$

Clearly $\sqrt{b/a} \geq 1 \geq \sqrt{a/b}$. If $1 < a \leq b$, then

$$\sqrt{ab} > \sqrt{\frac{b}{a}} \geq \sqrt{\frac{a}{b}} > \frac{1}{\sqrt{ab}},$$

and Conjecture 2 holds by Theorem 3. Similarly, if $a \leq b < 1$, then

$$\frac{1}{\sqrt{ab}} > \sqrt{\frac{b}{a}} \geq \sqrt{\frac{a}{b}} > \frac{1}{\sqrt{ab}},$$

and again Conjecture 2 holds by Theorem 3. Finally, if $a < 1 < b$, then

$$\sqrt{\frac{b}{a}} > \sqrt{ab} > \sqrt{\frac{a}{b}}, \quad \text{and} \quad \sqrt{\frac{b}{a}} > \frac{1}{\sqrt{ab}} > \sqrt{\frac{a}{b}},$$

and the conjecture is not true, because, by Theorem 3, the function obtains a minimum instead of a maximum at the points $1/\sqrt{ab}$.

4. COUNTEREXAMPLES

We would like to start this section by giving very elementary counterexamples for the original conjecture. Let $\ell \in \mathbb{Z}_+$ and $\ell \geq 2$, and let us consider the ℓ -modular lattice

$$D^\ell = \mathbb{Z} \oplus \sqrt{\ell} \mathbb{Z}.$$

The secrecy function attached to this lattice is

$$\Xi_{D^\ell}(y) = \frac{\Theta_{(\ell^{1/4}\mathbb{Z})^2}(y)}{\Theta_{D^\ell}(y)} = \frac{\vartheta_3^2(y\sqrt{\ell})}{\vartheta_3(y)\vartheta_3(y\ell)},$$

defined for $y \in \mathbb{R}_+$. The secrecy function conjecture states that the function Ξ_{D^ℓ} should have a global maximum at the natural symmetry point $1/\sqrt{\ell}$. Our goal here is to prove that this is not the case.

Theorem 4. *Let $\ell \in \mathbb{Z}_+$ and $\ell \geq 2$. Then the lattice D^ℓ does not satisfy the secrecy function conjecture. More precisely, the secrecy function Ξ_{D^ℓ} does not have a global maximum at the point $1/\sqrt{\ell}$.*

Proof. On the one hand,

$$\Xi_{D^\ell}(y) \longrightarrow 1 \quad \text{as} \quad y \longrightarrow \infty.$$

On the other hand, Lemma 5 below tells us that

$$\Xi_{D^\ell}\left(\frac{1}{\sqrt{\ell}}\right) < 1.$$

Thus, clearly the secrecy function cannot have a global maximum at the point $1/\sqrt{\ell}$. \square

Lemma 5. *Let $\ell \in \mathbb{Z}_+$ and $\ell \geq 2$. Then we have*

$$\Xi_{D^\ell}\left(\frac{1}{\sqrt{\ell}}\right) < 1.$$

Proof. We need to prove that

$$\vartheta_3^2(1) < \vartheta_3\left(\frac{1}{\sqrt{\ell}}\right)\vartheta_3(\sqrt{\ell}).$$

We recall that the ϑ -function ϑ_3 satisfies the modularity relation

$$\vartheta_3\left(\frac{1}{y}\right) = \sqrt{y} \vartheta_3(y)$$

for all $y \in \mathbb{R}_+$. Given this modularity relation, and the fact that $\vartheta_3(y) > 1$ for all $y \in \mathbb{R}_+$, we have

$$\vartheta_3\left(\frac{1}{\sqrt{\ell}}\right) \vartheta_3(\sqrt{\ell}) = \ell^{1/4} \vartheta_3^2(\sqrt{\ell}) > \ell^{1/4}.$$

On the other hand, it is easy to compute numerically that

$$\vartheta_3^8(1) \approx 1.9410 \dots < 2 \leq \ell,$$

and so $\vartheta_3^2(1) < \ell^{1/4}$, and we are done. \square

We can use the more advanced Theorem 3 to prove the following counterexamples. The purpose of the condition $a_1 < \sqrt{\ell}$ in the following theorem is just to exclude the uninteresting case $L = (\sqrt{\ell} \mathbb{Z})^{n+1}$ in which the secrecy function Ξ_L is a constant function. The requirement that $1 < a_k < \ell$ for some k in Theorem 7 serves the same purpose.

Theorem 6. *Let $\ell, n \in \mathbb{Z}_+$ with $\ell \geq 2$, and let us be given integers*

$$1 \leq a_1 \leq a_2 \leq a_3 \leq \dots \leq a_n \leq \ell,$$

such that $a_1 < \sqrt{\ell}$ and $a_k a_{n+1-k} = \ell$ for each $k \in \{1, 2, \dots, n\}$. Then the secrecy function Ξ_L of the ℓ -modular lattice

$$L = \bigoplus_{k=1}^n \sqrt{a_k} \mathbb{Z}$$

has a unique global minimum at the point $1/\sqrt{\ell}$, is strictly decreasing in $]0, 1/\sqrt{\ell}]$ and strictly increasing in $[1/\sqrt{\ell}, \infty[$.

Proof. Since Ξ_L only takes positive values, we may consider its square which may be written in the form

$$\Xi_L^2\left(\frac{y}{\sqrt{\ell}}\right) = \prod_{k=1}^n \frac{\vartheta_3^2(y)}{\vartheta_3(a_k y / \sqrt{\ell}) \vartheta_3(a_{n+1-k} y / \sqrt{\ell})},$$

and the desired properties of Ξ_L follow from Theorem 3. \square

Remark 1. In [7] Faulhuber and Steinerberger proved that the function $\log \vartheta_3(e^x)$ is strictly convex for $x \in \mathbb{R}$, which is actually enough to see that the above lattices L are counterexamples, as Jensen's inequality directly gives the weaker conclusion $\Xi_L(y) < 1$ for all $y \in \mathbb{R}_+$.

Theorem 7. *Let $\ell, n \in \mathbb{Z}_+$ with $\ell \geq 2$, and let us be given integers*

$$1 \leq a_1 \leq a_2 \leq a_3 \leq \dots \leq a_n \leq \ell,$$

such that $a_k a_{n+1-k} = \ell$ for each $k \in \{1, 2, \dots, n\}$ and that $1 < a_k < \ell$ for at least one $k \in \{1, 2, \dots, n\}$. Then the modified secrecy function $\tilde{\Xi}_L$ of the ℓ -modular lattice

$$L = \bigoplus_{k=1}^n \sqrt{a_k} \mathbb{Z}$$

has a unique global maximum at the point $1/\sqrt{\ell}$, is strictly increasing in $]0, 1/\sqrt{\ell}]$, and strictly decreasing in $[1/\sqrt{\ell}, \infty[$.

Proof. Since $\tilde{\Xi}_L$ takes only positive values, we may consider its square which may be written in the form

$$\tilde{\Xi}_L^2\left(\frac{y}{\sqrt{\ell}}\right) = \prod_{k=1}^n \frac{\vartheta_3(y\sqrt{\ell}) \vartheta_3(y/\sqrt{\ell})}{\vartheta_3(a_k y/\sqrt{\ell}) \vartheta_3(a_{n+1-k} y/\sqrt{\ell})},$$

and the desired properties of $\tilde{\Xi}_L$ follow from Theorem 3. \square

Example 1. For example, let us consider the lattice

$$C^\ell = \bigoplus_{d|n} \sqrt{d} \mathbb{Z},$$

where $d | n$ means taking a term for each positive divisor d of ℓ , and where $\ell \in \mathbb{Z}_+$ with $\ell \geq 2$. By Theorem 6 this lattice is a counterexample to the original ℓ -modular secrecy function conjecture, but by Theorem 7 it does satisfy the modified ℓ -modular secrecy function conjecture.

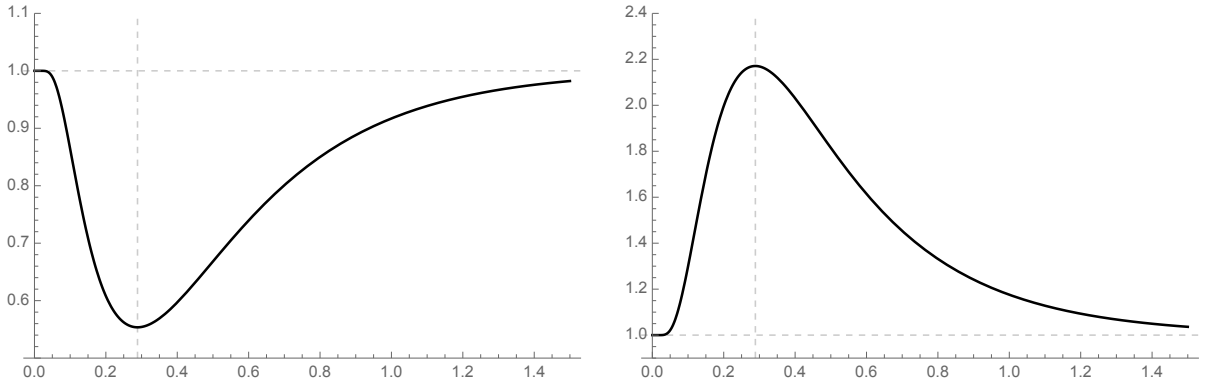


FIGURE 3. The secrecy function $\Xi_{C^{12}}$ and the modified secrecy function $\tilde{\Xi}_{C^{12}}$.

5. POLYNOMIZATION

The classical Dedekind η -function is defined by setting

$$\eta(y) = e^{-\pi y/12} \prod_{n=1}^{\infty} (1 - e^{-2\pi n y})$$

for $y \in \mathbb{R}_+$, where we have again simplified notation by writing $\eta(y)$ for $\eta(yi)$, as usual. We recall that this satisfies the modularity relation

$$\eta\left(\frac{1}{y}\right) = \sqrt{y} \eta(y)$$

for all $y \in \mathbb{R}_+$.

Let $\ell \in \mathbb{Z}_+$. For the polynomization we need to understand η -quotients involving the function $\eta^{(\ell)}: \mathbb{R}_+ \rightarrow \mathbb{R}_+$ defined by

$$\eta^{(\ell)}(y) = \prod_{d|\ell} \eta(dy)$$

for all $y \in \mathbb{R}_+$, where the product $\prod_{d|\ell}$ is taken over all positive divisors d of ℓ . When ℓ is odd, we also define

$$g_\ell(y) = \left(\frac{\eta^{(\ell)}(y/2) \eta^{(\ell)}(2y)}{(\eta^{(\ell)}(y))^2} \right)^{D_\ell / \dim C^\ell}$$

for $y \in \mathbb{R}_+$, and when ℓ is even, we define

$$g_\ell(y) = \left(\frac{\eta^{(\ell/2)}(y/2) \eta^{(\ell/2)}(4y)}{\eta^{(\ell/2)}(y) \eta^{(\ell/2)}(2y)} \right)^{D_\ell / \dim C^\ell},$$

again for $y \in \mathbb{R}_+$. Here

$$D_\ell = \frac{24 d(\ell)}{\prod_{p|\ell} (p+1)},$$

where $d(\ell)$ is the number of positive divisors of ℓ and the product $\prod_{p|\ell}$ is over the positive prime divisors p of ℓ . Naturally, we have

$$\dim C^\ell = \dim \bigoplus_{d|\ell} \sqrt{d} \mathbb{Z} = d(\ell).$$

The following theorem is the first half of Corollary 3 from [17]. We recall that two lattices $\Lambda \subset \mathbb{R}^n$ and $\Lambda' \subset \mathbb{R}^n$ of dimension $n \in \mathbb{Z}_+$ are called rationally equivalent if $\Lambda = A \Lambda'$ for some invertible matrix $A \in \mathbb{Q}^{n \times n}$.

We also recall that an integral lattice Λ is strongly ℓ -modular for $\ell \in \mathbb{Z}_+$ if the smallest $\ell' \in \mathbb{Z}_+$, for which $\sqrt{\ell'} \Lambda^*$ is integral, satisfies $\ell' \mid \ell$, and if Λ has a modularity of level m for each positive divisor $m \mid \ell$ such that m and ℓ/m are coprime. A modularity σ of level $m \in \mathbb{Z}_+$ of an n -dimensional integral lattice Λ is a similarity of \mathbb{R}^n multiplying norms by m and mapping $\Lambda^{*\Pi}$ to Λ where Π is the set of primes dividing m . Finally, given a set of primes Π the Π -dual $\Lambda^{*\Pi}$ of an integral lattice Λ consists of those vectors $v \in \Lambda \otimes \mathbb{Q}$ such that $v \cdot \Lambda \subseteq \mathbb{Z}_p$ for $p \in \Pi$ and $v \cdot \Lambda^* \subseteq \mathbb{Z}_p$ for primes $p \notin \Pi$. In particular, if ℓ is a prime, then an ℓ -modular integral lattice is also strongly ℓ -modular.

Theorem 8. *Assume that $\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$, and let Λ be a strongly ℓ -modular lattice that is rationally equivalent to $(C^\ell)^k$, where $k \in \mathbb{Z}_+$. Then its theta series can be written in the form*

$$\Theta_\Lambda = \Theta_{C^\ell}^k \sum_{i=0}^N c_i g_2^i,$$

where $N \in \mathbb{Z}_+$ and the coefficients c_0, c_1, \dots, c_N are real numbers.

Remark 2. We remark here that one may use the beautiful theory of rational quadratic forms (see e.g. Chapter IV in [18]) to check the rational equivalence, similarly to how the 2-modular case was considered in [5]. More precisely, if we consider the lattice $(C^\ell)^k$ and a given ℓ -modular lattice Λ of the same dimension, where $\ell, k \in \mathbb{Z}_+$, then the two lattices are rationally equivalent if and only if the corresponding quadratic forms have the same discriminants, signatures and Hasse–Witt invariants. Since they have the same determinants, namely ℓ^k , the discriminants must also be the same, and since the quadratic forms are strictly positive-definite, this easily implies that also the signatures are the same and that the Hasse–Witt invariants at ∞ are both equal to $+1$. The argument used in the appendix of [5] shows that the Hasse–Witt invariants at p are both equal to $+1$ for any odd prime p not dividing ℓ . This only leaves finitely many Hasse–Witt invariants ε_p to compute and to compare. More detailed discussions can be found in [18, 5].

We can now state the theorems that we are going to prove.

Theorem 9. *Let $\ell \in \{3, 5, 7, 11, 23\}$, let Λ be an ℓ -modular lattice, which is rationally equivalent to $(C^\ell)^k$, where $k \in \mathbb{Z}_+$, and let*

$$\Theta_\Lambda = \Theta_{C^\ell}^k \sum_{i=0}^N c_i g_\ell^i,$$

where $N \in \mathbb{Z}_+$ and the coefficients c_0, c_1, \dots, c_N are real numbers. Then the modified secrecy function $\tilde{\Xi}_\Lambda$ has a unique global maximum at the natural symmetry point $1/\sqrt{\ell}$ if and only if

$$\sum_{i=0}^N c_i x^i > \sum_{i=0}^N c_i g_\ell^i \left(\frac{1}{\sqrt{\ell}} \right)$$

for all $x \in]0, g_\ell(1/\sqrt{\ell})[$.

Proof. Since $C^\ell = \mathbb{Z} \oplus \sqrt{\ell}\mathbb{Z} = D^\ell$ as ℓ is a prime, we have

$$\frac{1}{\tilde{\Xi}_\Lambda} = \frac{\Theta_\Lambda}{\Theta_{D^\ell}^k(y)} = \sum_{i=0}^N c_i g_\ell^i.$$

Hence, it suffices to consider the expression $\sum_{i=0}^N c_i g_\ell^i$. Let us now analyse the behaviour of the function g_ℓ . By Theorem 11 below the function g_ℓ is strictly increasing in $]0, 1/\sqrt{\ell}[$, and strictly decreasing in $[1/\sqrt{\ell}, \infty[$, with $g_\ell(y) \rightarrow 0+$ as $y \rightarrow 0+$ or $y \rightarrow \infty$. Thus, the conjecture holds for Λ if and only if the polynomial $\sum_{i=0}^N c_i x^i$ has in the interval $]0, g_\ell(1/\sqrt{\ell})]$ a strict global minimum at the point $g_\ell(1/\sqrt{\ell})$, and we are done. \square

Example 2. The ϑ -function of the strongly 3-modular 12-dimensional Coxeter–Todd lattice K_{12} is of the form

$$\Theta_{K_{12}}(y) = 1 + 756 e^{-4\pi y} + 4032 e^{-6\pi y} + 20412 e^{-8\pi y} + 60480 e^{-10\pi y} + \dots$$

It can be written in the form

$$(\vartheta_3(y) \vartheta_3(3y))^6 (1 - 12 g_3(y) + 12 g_3^2(y) - 64 g_3^3(y)).$$

The modified secrecy function of this lattice is thus

$$\begin{aligned} \tilde{\Xi}_{K_{12}}(y) &= \frac{(\vartheta_3(y) \vartheta_3(3y))^6}{(\vartheta_3(y) \vartheta_3(3y))^6 (1 - 12 g_3(y) + 12 g_3^2(y) - 64 g_3^3(y))} \\ &= (1 - 12 g_3(y) + 12 g_3^2(y) - 64 g_3^3(y))^{-1} \end{aligned}$$

Let us now look at the polynomial $P(x) = 1 - 12x + 12x^2 - 64x^3$. Since $P'(x) = -12 + 24x - 192x^2 < 0$ on real numbers, the polynomial $P(x)$ is decreasing. Hence, the lattice K_{12} satisfies the modified conjecture.

Example 3. The ϑ -function of the strongly 5-modular 8-dimensional icosean lattice $H4$, also known as $Q_8(1)$, is of the form

$$\Theta_{H4}(y) = 1 + 120 e^{-4\pi y} + 240 e^{-6\pi y} + 600 e^{-8\pi y} + 1440 e^{-10\pi y} + \dots$$

It can be written in the form

$$(\vartheta_3(y) \vartheta_3(5y))^4 (1 - 8 g_5(y) + 8 g_5^2(y) - 16 g_5^3(y)).$$

The modified secrecy function of this lattice is thus

$$\begin{aligned} \tilde{\Xi}_{H4}(y) &= \frac{(\vartheta_3(y) \vartheta_3(5y))^4}{(\vartheta_3(y) \vartheta_3(5y))^4 (1 - 8 g_5(y) + 8 g_5^2(y) - 16 g_5^3(y))} \\ &= (1 - 8 g_5(y) + 8 g_5^2(y) - 16 g_5^3(y))^{-1} \end{aligned}$$

Let us now look at the polynomial $P(x) = 1 - 8x + 8x^2 - 16x^3$. Since $P'(x) = -8 + 16x - 48x^2 < 0$ on real numbers, the polynomial $P(x)$ is decreasing. Hence, the lattice $H4$ satisfies the modified conjecture.

The proof of Theorem 9 also works in the case $\ell = 2$ which has been treated in [5]. In the case that ℓ is a composite number, we can prove the following theorem which is weaker than the theorem above.

Theorem 10. *Let $\ell \in \{6, 14, 15\}$, let Λ be a strongly ℓ -modular lattice, which is rationally equivalent to $(C^\ell)^k$, where $k \in \mathbb{Z}_+$, and let*

$$\Theta_\Lambda = \Theta_{C^\ell}^k \sum_{i=0}^N c_i g_\ell^i,$$

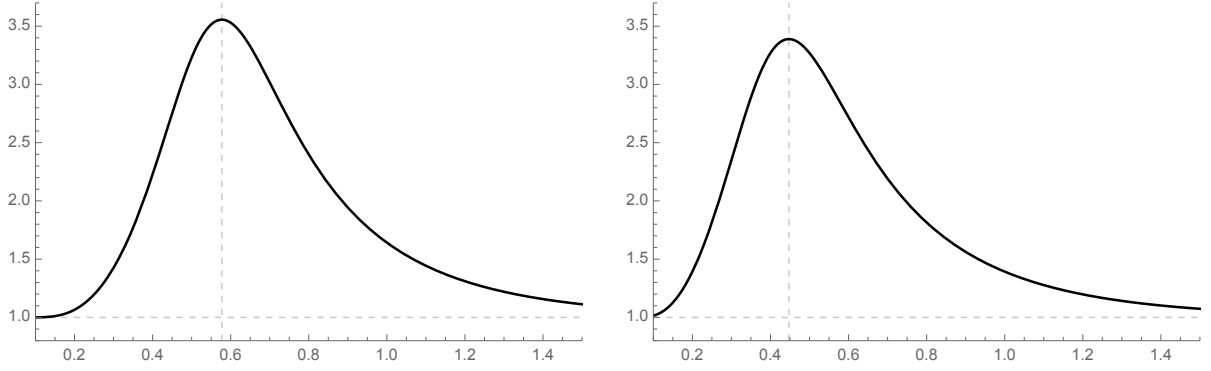


FIGURE 4. The modified secrecy functions $\tilde{\Xi}_{K_{12}}$ and $\tilde{\Xi}_{H_4}$ of Examples 2 and 3.

where $N \in \mathbb{Z}_+$ and the coefficients c_0, c_1, \dots, c_N are real numbers. Assume that

$$\sum_{i=0}^N c_i x^i \geq \sum_{i=0}^N c_i g_\ell^i \left(\frac{1}{\sqrt{\ell}} \right)$$

for all $x \in]0, g_\ell(1/\sqrt{\ell})]$. Then the modified secrecy function $\tilde{\Xi}_\Lambda$ has a unique global maximum at the natural symmetry point $1/\sqrt{\ell}$.

Remark 3. This theorem has only one direction: even if the polynomial does not attain its minimum in the interval at the given point, it might happen that the lattice satisfies the conjecture.

Proof of Theorem 10. We start by factoring the modified secrecy function into two parts

$$\tilde{\Xi}_\Lambda = \frac{\Theta_{D^\ell}^{n/2}}{\Theta_\Lambda} = \frac{\Theta_{D^\ell}^{n/2}}{\Theta_{C^\ell}^k} \cdot \frac{\Theta_{C^\ell}^k}{\Theta_\Lambda}.$$

The first factor $\Theta_{D^\ell}^{n/2}/\Theta_{C^\ell}^k$ has a unique global maximum at the point $1/\sqrt{\ell}$ by Theorem 7, and so it is enough to prove that the second quotient has a global maximum at the point $1/\sqrt{\ell}$. But this factor is

$$\frac{\Theta_{C^\ell}^k}{\Theta_\Lambda} = \left(\sum_{i=0}^N c_i g_\ell^i \right)^{-1}.$$

Hence, it suffices to consider the expression $\sum_{i=0}^N c_i g_\ell^i$. Let us now analyse the behaviour of the function g_ℓ . By Theorem 11 below the function g_ℓ is strictly increasing in $]0, 1/\sqrt{\ell}]$, and strictly decreasing in $[1/\sqrt{\ell}, \infty[$, with $g_\ell(y) \rightarrow 0+$ as $y \rightarrow 0+$ or $y \rightarrow \infty$. Thus, the conjecture holds for Λ , provided that the polynomial $\sum_{i=0}^N c_i x^i$ has in the interval $]0, g_\ell(1/\sqrt{\ell})]$ a global minimum at the point $g_\ell(1/\sqrt{\ell})$, and we are done. \square

The following theorem is crucial for understanding the behaviour of g_ℓ in the above theorems. It depends on a technical lemma on some finer properties of the function $\log \eta(\exp)$. The lemma is stated and proved in Section 7 below.

ℓ	$g_\ell(1/\sqrt{\ell})$
3	0.0625000
5	0.0954915
6	0.133975
7	0.125000
11	0.176101
14	0.228788
15	0.250000
23	0.284920

FIGURE 5. Numerical values for the expressions $g_\ell(1/\sqrt{\ell})$ appearing in Theorems 9 and 10.

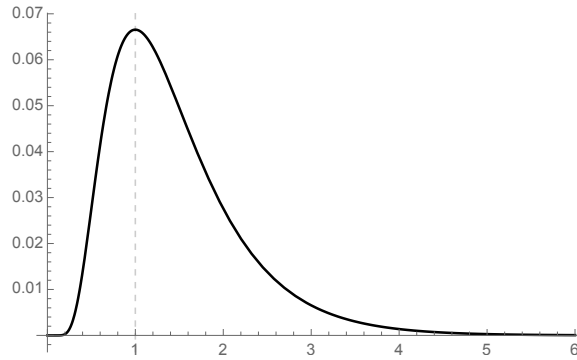


FIGURE 6. The function $g(y)$ of Theorem 11 with $\kappa = 2$, $\lambda = 5$ and $\ell = 3$.

Theorem 11. Let $\kappa, \lambda \in \mathbb{R}_+$ with $1 \leq \kappa < \lambda$, and let $\ell \in \mathbb{Z}_+$. Let us define a function $g: \mathbb{R}_+ \rightarrow \mathbb{R}_+$ by setting

$$g(y) = \frac{\eta^{(\ell)}\left(\frac{\lambda y}{\sqrt{\ell}}\right) \eta^{(\ell)}\left(\frac{y}{\lambda \sqrt{\ell}}\right)}{\eta^{(\ell)}\left(\frac{\kappa y}{\sqrt{\ell}}\right) \eta^{(\ell)}\left(\frac{y}{\kappa \sqrt{\ell}}\right)}$$

for all $y \in \mathbb{R}_+$.

This function g is a real-analytic function satisfying the modularity relation

$$g\left(\frac{1}{y}\right) = g(y)$$

for all $y \in \mathbb{R}_+$. Furthermore, it is strictly increasing in $]0, 1]$, strictly decreasing in $[1, \infty[$, has a strict global maximum at the point 1, its image set is $]0, g(1)]$, and furthermore, $g(y) \rightarrow 0$ as $y \rightarrow \infty$ or $y \rightarrow 0+$.

Proof. The real-analyticity of g follows from the real-analyticity of all the functions involved in its definition. The modularity relation is an immediate consequence of the modularity relation

$$\eta\left(\frac{1}{y}\right) = \sqrt{y} \eta(y),$$

which holds for all $y \in \mathbb{R}_+$. The conclusion about the image set will follow from the other remaining claims and the continuity of g . Of the limits of $g(y)$ as $y \rightarrow 0+$ or $y \rightarrow \infty$ only one needs to be considered as the other case follows from the modularity relation. The limit $y \rightarrow \infty$ is easily dealt with as $\eta(y) \sim e^{-\pi y/12}$ as $y \rightarrow \infty$ and so $\eta^{(\ell)}(y) \sim e^{-\pi \sigma(\ell)y/12}$ as $y \rightarrow \infty$, where $\sigma(N)$ denotes the sum of the positive divisors of N , and consequently,

$$g(y) \sim \exp\left(-\frac{\pi \sigma(\ell)}{12 \sqrt{\ell}} \left(\lambda + \frac{1}{\lambda} - \kappa - \frac{1}{\kappa}\right) y\right)$$

as $y \rightarrow \infty$, and the conclusion $g(y) \rightarrow 0$ as $y \rightarrow \infty$ follows from the simple observation that $\lambda + 1/\lambda > \kappa + 1/\kappa$.

Finally, the claims about the global maximum at 1 follows from the claimed monotonicity properties in $]0, 1]$ and $[1, \infty[$, and by the modularity relation, it only remains to prove that $g(y)$ is strictly decreasing for $y \in]1, \infty[$. It is enough to prove that $\log g(e^x)$ is strictly decreasing for $x \in \mathbb{R}_+$. In terms of the function $f(x)$, given by $\log \eta(e^x)$ for $x \in \mathbb{R}$, and the parameters $h = \log \lambda$ and $k = \log \kappa$, this logarithm is, applying Lemma 1,

$$\begin{aligned} \log g(e^x) &= \sum_{d|\ell} \left(f(x + \log d - \log \sqrt{\ell} + h) - f(x + \log d - \log \sqrt{\ell} + k) \right. \\ &\quad \left. - f(x + \log d - \log \sqrt{\ell} - k) + f(x + \log d - \log \sqrt{\ell} - h) \right) \\ &= \sum_{d|\ell} \int_{-\infty}^{\infty} f''(u + \log d - \log \sqrt{\ell}) T(u - x; k, h) du = \int_{-\infty}^{\infty} f''(u) K(u - x) du, \end{aligned}$$

where the kernel K is given by

$$K(u) = \sum_{d|\ell} T(u - \log d + \log \sqrt{\ell}; k, h)$$

for $u \in \mathbb{R}$. It is easily seen that this is an even continuous compactly supported function taking only nonnegative values.

Since f'' is real-analytic and K is continuous and compactly supported, the last integral is differentiable with derivative

$$\frac{d}{dx} \log g(e^x) = \int_{-\infty}^{\infty} f'''(u) K(u - x) du.$$

We only need to prove that this is strictly negative for $x \in \mathbb{R}_+$. But since f''' is a strictly decreasing odd function in \mathbb{R} by Theorem 16, and K takes only nonnegative values and is

even and not identically zero, we may estimate simply

$$\int_{-\infty}^{\infty} f'''(u) K(u-x) du < \int_{-\infty}^{\infty} f'''(u) K(u) du = 0,$$

and we are done. \square

6. TECHNICAL LEMMAS ON ϑ_3

We now state and prove the technical lemmas that are needed to prove Theorem 3. It turns out that the following lemma has appeared as Proposition 5.14 in Faulhuber's dissertation [6], but this section is nonetheless self-contained.

Lemma 12. *The second derivative of the function $\log \vartheta_3(e^x)$, defined for $x \in \mathbb{R}$, is an even function which is strictly decreasing for $x \in [0, \infty[$, and strictly increasing for $x \in]-\infty, 0]$.*

Proof. Let us simplify notation by writing $f(x) = \log \vartheta_3(e^x)$ for $x \in \mathbb{R}$. By the modularity relation of ϑ_3 we have

$$\vartheta_3\left(\frac{1}{y}\right) = \sqrt{y} \vartheta_3(y),$$

for $y \in \mathbb{R}_+$, so that

$$\log \vartheta_3(e^{-x}) = \frac{x}{2} + \log \vartheta_3(e^x),$$

for $x \in \mathbb{R}$, so that the second derivative f'' is an even function of x , and it is enough to prove that it is strictly decreasing for $x \in [0, \infty[$.

The second derivative is

$$f''(x) = \frac{e^x \vartheta_3'(e^x) \vartheta_3(e^x) + e^{2x} \vartheta_3''(e^x) \vartheta_3(e^x) - e^{2x} (\vartheta_3'(e^x))^2}{\vartheta_3^2(e^x)}.$$

We will prove the claim first for $x \in [0, \log(3/2)]$. Since $f''(-x) = f''(x)$ for all $x \in \mathbb{R}$, it is enough to prove that the function f'' is strictly concave in $[0, \log(3/2)]$, or equivalently, that the fourth derivative $f''''(x)$ is strictly negative for $x \in [0, \log(3/2)]$, but this is established in Lemma 13 below.

Thus it remains to prove that the function

$$\frac{y \vartheta_3'(y) \vartheta_3(y) + y^2 \vartheta_3''(y) \vartheta_3(y) - y^2 (\vartheta_3'(y))^2}{\vartheta_3^2(y)}$$

is strictly decreasing for $y \in [3/2, \infty[$. To do so, we will prove that its derivative, given by the expression

$$\begin{aligned} & \frac{\vartheta_3'(y) \vartheta_3^2(y) + 3y \vartheta_3''(y) \vartheta_3^2(y) - 3y (\vartheta_3'(y))^2 \vartheta_3(y)}{\vartheta_3^3(y)} \\ & + \frac{y^2 \vartheta_3'''(y) \vartheta_3^2(y) - 3y^2 \vartheta_3''(y) \vartheta_3'(y) \vartheta_3(y) + 2y^2 (\vartheta_3'(y))^3}{\vartheta_3^3(y)}, \end{aligned}$$

takes only strictly negative values for $y \in [3/2, \infty[$. Since the denominator takes only strictly positive values, we may focus solely on the numerator. But the strict negativity of the numerator for $y \in [3/2, \infty[$ is shown in Lemma 14 below. \square

Lemma 13. *Let $f(x) = \log \vartheta_3(e^x)$ for $x \in \mathbb{R}$. Then*

$$f''''(x) < 0$$

for $x \in [0, \log(3/2)]$.

Proof. Let us write $g(y) = \log \vartheta_3(y)$ for $y \in \mathbb{R}_+$. The first derivative of this expression is

$$\frac{d}{dy} g(y) = \frac{\vartheta_3'(y)}{\vartheta_3(y)},$$

its second derivative is

$$\frac{d^2}{dy^2} g(y) = \frac{\vartheta_3''(y)}{\vartheta_3(y)} - \frac{(\vartheta_3'(y))^2}{\vartheta_3^2(y)},$$

its third derivative is

$$\frac{d^3}{dy^3} g(y) = \frac{\vartheta_3'''(y)}{\vartheta_3(y)} - \frac{3 \vartheta_3''(y) \vartheta_3'(y)}{\vartheta_3^2(y)} + \frac{2 (\vartheta_3'(y))^3}{\vartheta_3^3(y)},$$

and its fourth derivative is

$$\frac{d^4}{dy^4} g(y) = \frac{\vartheta_3''''(y)}{\vartheta_3(y)} - \frac{4 \vartheta_3'''(y) \vartheta_3'(y)}{\vartheta_3^2(y)} - \frac{3 (\vartheta_3''(y))^2}{\vartheta_3^2(y)} + \frac{12 \vartheta_3''(y) (\vartheta_3'(y))^2}{\vartheta_3^3(y)} - \frac{6 (\vartheta_3'(y))^4}{\vartheta_3^4(y)},$$

and the fourth derivative f'''' is

$$\frac{d^4}{dx^4} f(x) = \frac{d^4}{dx^4} g(e^x) = g''''(e^x) e^{4x} + 6 g'''(e^x) e^{3x} + 7 g''(e^x) e^{2x} + g'(e^x) e^x.$$

Thus, we need to prove that the expression

$$h(y) = y^4 g''''(y) + 6 y^3 g'''(y) + 7 y^2 g''(y) + y g'(y)$$

is strictly negative for $y \in [1, 3/2]$.

Let $m, M \in [1, \infty[$ with $m < M$. Then, for $y \in [m, M]$, we may use Lemma 15 to rewrite and estimate the expression as follows:

$$\begin{aligned}
h(y) &= y^4 \left(\frac{\vartheta_3''''(y)}{\vartheta_3(y)} - \frac{4 \vartheta_3'''(y) \vartheta_3'(y)}{\vartheta_3^2(y)} - \frac{3 (\vartheta_3''(y))^2}{\vartheta_3^2(y)} + \frac{12 \vartheta_3''(y) (\vartheta_3'(y))^2}{\vartheta_3^3(y)} - \frac{6 (\vartheta_3'(y))^4}{\vartheta_3^4(y)} \right) \\
&\quad + 6 y^3 \left(\frac{\vartheta_3'''(y)}{\vartheta_3(y)} - \frac{3 \vartheta_3''(y) \vartheta_3'(y)}{\vartheta_3^2(y)} + \frac{2 (\vartheta_3'(y))^3}{\vartheta_3^3(y)} \right) \\
&\quad + 7 y^2 \left(\frac{\vartheta_3''(y)}{\vartheta_3(y)} - \frac{(\vartheta_3'(y))^2}{\vartheta_3^2(y)} \right) + y \frac{\vartheta_3'(y)}{\vartheta_3(y)} \\
&< \left(\frac{M^4 \Theta_{3,4}(m)}{\vartheta_{3,0}(M)} - \frac{4 m^4 \vartheta_{3,3}(M) \vartheta_{3,1}(M)}{\Theta_{3,0}^2(m)} - \frac{3 m^4 (\vartheta_{3,2}(M))^2}{\Theta_{3,0}^2(m)} \right. \\
&\quad \left. + \frac{12 M^4 \Theta_{3,2}(m) (\Theta_{3,1}(m))^2}{\vartheta_{3,0}^3(M)} - \frac{6 m^4 (\vartheta_{3,1}(M))^4}{\Theta_{3,0}^4(m)} \right) \\
&\quad + 6 \left(-\frac{m^3 \vartheta_{3,3}(M)}{\Theta_{3,0}(m)} + \frac{3 M^3 \Theta_{3,2}(m) \Theta_{3,1}(m)}{\vartheta_{3,0}^2(M)} - \frac{2 m^3 (\vartheta_{3,1}(M))^3}{\Theta_{3,0}^3(m)} \right) \\
&\quad + 7 \left(\frac{M^2 \Theta_{3,2}(m)}{\vartheta_{3,0}(M)} - \frac{m^2 (\vartheta_{3,1}(M))^2}{\Theta_{3,0}^2(m)} \right) - \frac{m \vartheta_{3,1}(M)}{\Theta_{3,0}(m)}.
\end{aligned}$$

Using this upper bound, it is easy to check numerically, that $h(y) < -0.16$ for all

$$y \in \left[1 + \frac{k-1}{1000}, 1 + \frac{k}{1000} \right]$$

for each $k \in \{1, 2, \dots, 500\}$ separately. □

Lemma 14. *Let $y \in [3/2, \infty[$. Then*

$$\begin{aligned}
&\vartheta_3'(y) \vartheta_3^2(y) + 3 y \vartheta_3''(y) \vartheta_3^2(y) - 3 y (\vartheta_3'(y))^2 \vartheta_3(y) \\
&\quad + y^2 \vartheta_3'''(y) \vartheta_3^2(y) - 3 y^2 \vartheta_3''(y) \vartheta_3'(y) \vartheta_3(y) + 2 y^2 (\vartheta_3'(y))^3 < 0.
\end{aligned}$$

Proof. Using Lemma 15 below, the left-hand side is

$$\begin{aligned}
&< -\vartheta_{3,1}(y) \vartheta_{3,0}^2(y) + 3 y \Theta_{3,2}(y) \Theta_{3,0}^2(y) - 3 y (\vartheta_{3,1}(y))^2 \vartheta_{3,0}(y) \\
&\quad - y^2 \vartheta_{3,3}(y) \vartheta_{3,0}^2(y) + 3 y^2 \Theta_{3,2}(y) \Theta_{3,1}(y) \Theta_{3,0}(y) - 2 y^2 (\vartheta_{3,1}(y))^3.
\end{aligned}$$

We may further absorb the terms involving $e^{-9\pi y}$ into those involving $e^{-4\pi y}$, remembering that $e^{-\pi y} < 1/100$ for $y \geq 3/2$, leading to the upper bound

$$\begin{aligned} &< - (2\pi e^{-\pi y} + 8\pi e^{-4\pi y}) (1 + 2e^{-\pi y} + 2e^{-4\pi y})^2 \\ &\quad + 3y (2\pi^2 e^{-\pi y} + 33\pi^2 e^{-4\pi y}) (1 + 2e^{-\pi y} + 3e^{-4\pi y})^2 \\ &\quad - 3y (2\pi e^{-\pi y} + 8\pi e^{-4\pi y})^2 (1 + 2e^{-\pi y} + 2e^{-4\pi y}) \\ &\quad - y^2 (2\pi^3 e^{-\pi y} + 128\pi^3 e^{-4\pi y}) (1 + 2e^{-\pi y} + 2e^{-4\pi y})^2 \\ &\quad + 3y^2 (2\pi^2 e^{-\pi y} + 33\pi^2 e^{-4\pi y}) (2\pi e^{-\pi y} + 9\pi e^{-4\pi y}) (1 + 2e^{-\pi y} + 3e^{-4\pi y}) \\ &\quad - 2y^2 (2\pi e^{-\pi y} + 8\pi e^{-4\pi y})^3. \end{aligned}$$

The last expression turns out to be

$$\begin{aligned} &= - (2\pi^3 y^2 - 6\pi^2 y + 2\pi) e^{-\pi y} + (4\pi^3 y^2 + 12\pi^2 y - 8\pi) e^{-2\pi y} - 8\pi e^{-3\pi y} \\ &\quad - (128\pi^3 y^2 - 99\pi^2 y + 8\pi) e^{-4\pi y} - (268\pi^3 y^2 - 336\pi^2 y + 40\pi) e^{-5\pi y} \\ &\quad - (180\pi^3 y^2 - 252\pi^2 y + 48\pi) e^{-6\pi y} + (379\pi^3 y^2 + 402\pi^2 y - 32\pi) e^{-8\pi y} \\ &\quad + (738\pi^3 y^2 + 666\pi^2 y - 72\pi) e^{-9\pi y} + (1137\pi^3 y^2 + 507\pi^2 y - 32\pi) e^{-12\pi y}. \end{aligned}$$

Here the contribution from the terms involving $e^{-3\pi y}$, $e^{-4\pi y}$, $e^{-5\pi y}$ and $e^{-6\pi y}$ are clearly strictly negative for $y \in [3/2, \infty[$. Similarly, we may forget those terms not involving a power of y , since all of them are strictly negative as well. Thus, we may continue our estimations

$$\begin{aligned} &< - (2\pi^3 y^2 - 6\pi^2 y) e^{-\pi y} + (4\pi^3 y^2 + 12\pi^2 y) e^{-2\pi y} \\ &\quad + (379\pi^3 y^2 + 402\pi^2 y) e^{-8\pi y} + (738\pi^3 y^2 + 666\pi^2 y) e^{-9\pi y} \\ &\quad + (1137\pi^3 y^2 + 507\pi^2 y) e^{-12\pi y}. \end{aligned}$$

Now we extract a common factor $-y^2 e^{-\pi y}$, and use the lower bound $y \geq 3/2$ to continue

$$\begin{aligned} &\leq y^2 e^{-\pi y} (-2\pi^3 + 4\pi^2 + 4\pi^3 e^{-3\pi/2} + 8\pi^2 e^{-3\pi/2} \\ &\quad + 379\pi^3 e^{-21\pi/2} + 268\pi^2 e^{-21\pi/2} + 738\pi^3 e^{-24\pi/2} + 444\pi^2 e^{-24\pi/2} \\ &\quad + 1137\pi^3 e^{-33\pi/2} + 338\pi^2 e^{-33\pi/2}). \end{aligned}$$

Finally, this last expression is easily seen to be $< -20y^2 e^{-\pi y}$, and we are done. \square

Lemma 15. *Let $y \in [1, \infty[$. Then the ϑ_3 -function and its derivatives satisfy*

$$0 < \vartheta_{3,\nu}(y) < (-1)^\nu \vartheta_3^{(\nu)}(y) < \Theta_{3,\nu}(y)$$

for all $y \in [1, \infty[$, for each $\nu \in \{0, 1, 2, 3, 4\}$, where

$$\begin{cases} \vartheta_{3,0}(y) = 1 + 2e^{-\pi y} + 2e^{-4\pi y} + 2e^{-9\pi y}, \\ \vartheta_{3,1}(y) = 2\pi e^{-\pi y} + 8\pi e^{-4\pi y} + 18\pi e^{-9\pi y}, \\ \vartheta_{3,2}(y) = 2\pi^2 e^{-\pi y} + 32\pi^2 e^{-4\pi y} + 162\pi^2 e^{-9\pi y}, \\ \vartheta_{3,3}(y) = 2\pi^3 e^{-\pi y} + 128\pi^3 e^{-4\pi y} + 1458\pi^3 e^{-9\pi y}, \\ \vartheta_{3,4}(y) = 2\pi^4 e^{-\pi y} + 512\pi^4 e^{-4\pi y} + 13122\pi^4 e^{-9\pi y}, \end{cases}$$

and

$$\begin{cases} \Theta_{3,0}(y) = 1 + 2e^{-\pi y} + 2e^{-4\pi y} + 3e^{-9\pi y}, \\ \Theta_{3,1}(y) = 2\pi e^{-\pi y} + 8\pi e^{-4\pi y} + 19\pi e^{-9\pi y}, \\ \Theta_{3,2}(y) = 2\pi^2 e^{-\pi y} + 32\pi^2 e^{-4\pi y} + 163\pi^2 e^{-9\pi y}, \\ \Theta_{3,3}(y) = 2\pi^3 e^{-\pi y} + 128\pi^3 e^{-4\pi y} + 1459\pi^3 e^{-9\pi y}, \\ \Theta_{3,4}(y) = 2\pi^4 e^{-\pi y} + 512\pi^4 e^{-4\pi y} + 13123\pi^4 e^{-9\pi y}. \end{cases}$$

Proof. Let $y \in [1, \infty[$ and $\nu \in \{0, 1, 2, 3, 4\}$. The lower bounds $0 < \vartheta_{3,\nu}(y) < (-1)^\nu \vartheta_3^{(\nu)}(y)$ hold trivially as $\vartheta_{3,\nu}(y)$ are just the beginning of the Fourier series representation of $(-1)^\nu \vartheta_3^{(\nu)}(y)$. Thus, it is enough to prove the upper bounds involving $\Theta_{3,\nu}(y)$. This is achieved by estimating

$$0 < (-1)^\nu \vartheta_3^{(\nu)}(y) - \vartheta_{3,\nu}(y) = 2\pi^\nu \sum_{n=4}^{\infty} n^{2\nu} e^{-\pi n^2 y} < 2\pi^\nu \sum_{n=16}^{\infty} n^\nu e^{-\pi n y} < 2\pi^\nu \int_{15}^{\infty} t^\nu e^{-\pi t y} dt,$$

where we apply the simple fact that the function $t^\nu e^{-\pi t y}$ is strictly decreasing in t for $t \in [15, \infty[$ for each fixed $y \in [1, \infty[$ and for each $\nu \in \{0, 1, 2, 3, 4\}$.

The proof is finished by showing that the expression $2\pi^\nu \int_{15}^{\infty} \dots$ is smaller than $\pi^\nu e^{-9\pi y}$. In the case $\nu = 4$ we get

$$\begin{aligned} 2\pi^4 \int_{15}^{\infty} t^4 e^{-\pi t y} dt &= \left(\frac{101250}{\pi y} + \frac{27000}{\pi^2 y^2} + \frac{5400}{\pi^3 y^3} + \frac{720}{\pi^4 y^4} + \frac{48}{\pi^5 y^5} \right) \pi^4 e^{-15\pi y} \\ &\leq \left(\frac{101250}{\pi} + \frac{27000}{\pi^2} + \frac{5400}{\pi^3} + \frac{720}{\pi^4} + \frac{48}{\pi^5} \right) e^{-6\pi} \pi^4 e^{-9\pi y} < \pi^4 e^{-9\pi y}. \end{aligned}$$

The other cases $\nu \in \{0, 1, 2, 3\}$ are similar but slightly simpler. \square

7. A TECHNICAL LEMMA ON η

Proofs of the polynomization results in Section 5 are based on some good properties of the function $\log \eta(\exp)$ on the real line. The crucial features of this function are listed in the following theorem.

Theorem 16. *Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = \log \eta(e^x)$ for all $x \in \mathbb{R}$. The function f is a real-analytic strictly concave function, and the second derivative f'' is a strictly*

concave even function. Furthermore, the third derivative f''' is a strictly decreasing odd function.

Proof. It is clear that f is real-analytic. Taking logarithms in the modularity relation of η gives

$$f(-x) = \frac{x}{2} + f(x)$$

for all $x \in \mathbb{R}$. Differentiating two, three and four times gives

$$f''(-x) = f''(x), \quad f'''(-x) = -f'''(x), \quad \text{and} \quad f''''(-x) = f''''(x),$$

respectively, for all $x \in \mathbb{R}$. Furthermore, the desired properties of f''' follow immediately from the desired properties of f'' . Thus, it only remains to prove that f and f'' are both strictly concave functions. Furthermore, since f'' and f'''' are even, it is enough to prove that $f''(x) < 0$ and $f''''(x) < 0$ for all $x \in [0, \infty[$.

We will start with the series representation

$$f(x) = -\frac{\pi e^x}{12} + \sum_{n=1}^{\infty} \log(1 - e^{-2\pi n e^x}),$$

which converges absolutely for all $x \in \mathbb{R}$, and uniformly in any bounded interval of \mathbb{R} . We recall the Taylor expansion

$$\log(1 - z) = -\sum_{m=1}^{\infty} \frac{z^m}{m},$$

which holds for all $z \in]-1, 1[$, and where the series on the right converges absolutely for all such z , and uniformly when z is restricted to a closed subinterval of $]-1, 1[$. Using this expansion we may continue by writing

$$f(x) = -\frac{\pi e^x}{12} - \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{m} e^{-2\pi m n e^x}.$$

To prove that f is strictly concave, it is enough to show that the expression $\exp(-2\pi m n e^x)$ gives a strictly convex function for $x \in [0, \infty[$. The second derivative of the expression is

$$\frac{d^2}{dx^2} (e^{-2\pi m n e^x}) = 2\pi m n e^x e^{-2\pi m n e^x} (-1 + 2\pi m n e^x),$$

and this is strictly positive since $2\pi m n e^x \geq 2\pi > 1$ for all $x \in [0, \infty[$, $m \in \mathbb{Z}_+$ and $n \in \mathbb{Z}_+$.

To prove that f'''' is strictly concave, it is enough to prove that the above expression $\exp(-2\pi m n e^x)$ has a strictly positive fourth derivative for $x \in [0, \infty[$. Its fourth derivative is

$$\frac{d^4}{dx^4} (e^{-2\pi m n e^x}) = (-1 + 14\pi m n e^x - 24\pi^2 m^2 n^2 e^{2x} + 8\pi^3 m^3 n^3 e^{3x}) 2\pi m n e^x e^{-2\pi m n e^x}.$$

But this last expression is easily seen to be strictly positive, since for all $x \in [0, \infty[$, $m \in \mathbb{Z}_+$ and $n \in \mathbb{Z}_+$ we may easily estimate

$$14\pi m n e^x \geq 14\pi > 1$$

as well as

$$8\pi^3 m^3 n^3 e^{3x} > 24\pi^2 m^3 n^3 e^{3x} \geq 24\pi^2 m^2 n^2 e^{2x},$$

and we are done. \square

REFERENCES

- [1] J.-C. Belfiore and F. E. Oggier. Secrecy gain: a wiretap lattice code design. In *ISITA*, 174–178, 2010.
- [2] J.-C. Belfiore and P. Solé. Unimodular lattices for the gaussian wiretap channel. In *ITW*, 2010.
- [3] A.-M. Ernvall-Hytönen. On a conjecture by Belfiore and Solé on some lattices. *IEEE Transactions on Information Theory*, 58(9), 5950–5955.
- [4] A.-M. Ernvall-Hytönen and C. Hollanti. On the eavesdropper’s correct decision in Gaussian and fading wiretap channels using lattice codes. In *ITW*, 210–214, 2011.
- [5] A.-M. Ernvall-Hytönen and B. A. Sethuraman. Counterexample to the generalized Belfiore-Solé secrecy function conjecture for l -modular lattices. *IEEE Transactions on Information Theory*, 62(8), 4514–4522.
- [6] M. Faulhuber. *Extremal Bounds of Gaussian Gabor Frames and Properties of Jacobi’s Theta Functions*. Doctoral dissertation. University of Vienna, 2016.
- [7] M. Faulhuber and S. Steinerberger. Optimal Gabor frame bounds for separable lattices and estimates for Jacobi theta functions. *Journal of Mathematical Analysis and Applications*, 445, 407–422, 2017.
- [8] X. Hou, F. Lin, and F. Oggier. Construction and Secrecy Gain of a Family of 5-modular Lattices. In *ITW*, 117–121, 2014.
- [9] B. Hernandez. *Results on the Secrecy Function Conjecture on the Theta Function of Lattices*. Master’s thesis. California State University, Northridge, 2016.
- [10] F. Lin. *Lattice Coding for the Gaussian Wiretap Channel — A Study of the Secrecy Gain*. Doctoral dissertation. Nanyang Technical University, Singapore, 2013.
- [11] F. Lin and F. Oggier. Secrecy gain of Gaussian wiretap codes from unimodular lattices. In *ITW*, 718–722, 2011.
- [12] F. Lin and F. Oggier. A classification of unimodular lattice wiretap codes in small dimensions. *IEEE Transactions on Information Theory*, 59(6), 3295–3303.
- [13] F. Lin, F. Oggier, and P. Solé. 2- and 3-Modular lattice wiretap codes in small dimensions. *Applicable Algebra in Engineering, Communication and Computing*, 26(6), 571–590.
- [14] F. Oggier, P. Solé, and J.-C. Belfiore. Lattice codes for the wiretap gaussian channel: Construction and analysis. *IEEE Transactions on Information Theory*, 62(10), 5690–5708.
- [15] J. Pinchak. Wiretap codes: families of lattices satisfying the Belfiore-Solé secrecy function conjecture. In *ISIT*, 2617–2620, 2013.
- [16] J. Pinchak and B. A. Sethuraman. The Belfiore-Solé conjecture and a certain technique for verifying it for a given lattice. In *ITA*, 486–488, 2014.
- [17] E. M. Rains and N. J. A. Sloane. The shadow theory of modular and unimodular lattices. *Journal of Number Theory*, 73, 359–389, 1998.
- [18] J.-P. Serre. *Cours d’arithmétique*. Le Mathématicien, Presses Universitaires de France, 2007.
- [19] B. A. Sethuraman, personal communication.
- [20] G. R. D. A. S. Strey. *A série teta e a função de sigilo de um reticulado*. Master’s thesis. University of Campinas, 2016.
- [21] A. D. Wyner. The wire-tap channel. *Bell. Syst. Tech. Journal*, 54(October), 1355–1387, 1975.