Generalized Theta Series of a Lattice

Maiara F. Bollauf
University of Tartu
Narva mnt 18, 51009, Tartu, Estonia
Email: maiara.bollauf@ut.ee

Hsuan-Yin Lin
Simula UiB
N–5006 Bergen, Norway
Email: lin@simula.no

***Abstract*—Mimicking the idea of the generalized Hamming weight of linear codes, we introduce a new lattice invariant, the *generalized theta series*. Applications range from identifying stable lattices to the lattice isomorphism problem. Moreover, we provide counterexamples for the *secrecy gain conjecture* on isodual lattices, which claims that the ratio of the theta series of an isodual (and more generally, formally unimodular) lattice by the theta series of the integer lattice $\mathbb{Z}^n$ is minimized at a (unique) symmetry point.**

I. Introduction

In coding theory, the generalized Hamming weight [1] serves as a structural parameter that provides additional information beyond the minimum Hamming weight of a linear code. It has applications in the type II wiretap channel, where an eavesdropper taps s out of n bits of a sent message and is supposed to get the least information from it. It can also be used as a code invariant to guarantee two linear codes are not equivalent or assist in finding an equivalence if it exists.

The theta series characterizes the (Euclidean) distance spectrum of an n-dimensional lattice Λ. A lattice property is said to be *audible* if it can be determined by the lattice theta series, as, for example, the theta series of the dual lattice Λ^* is related to the theta series of Λ via the Jacobi's formula [2, p. 103]. Conway and Fung [3] asked the following question: *Can you hear the shape of a lattice?* In other words, in which dimensions there can be two non-isomorphic lattices with the same theta series? It was demonstrated that one can hear the shape of $n = 2$ [3, pp. 44–45] and $n = 3$-dimensional lattices [4], but cannot for $n \geq 4$ [3, pp. 42–44].

This paper contributes to the solution of this problem by providing a refined notion of audible given by a new lattice geometric invariant, the *generalized theta series*. It is inspired by the generalized Hamming weight of linear codes and connects two other lattice invariants, the determinant and the theta series. In more mathematical terms, the r-th generalized theta series of a lattice Λ counts the number of r-dimensional sublattices $\Lambda' \subseteq \Lambda$ that have the same volume.

The first application of the generalized theta series is in finding *stable lattices*, i.e., lattices such that all of its sublattices have a volume larger than or equal to one. Stable lattices have recently gained a lot of interest in connection with the *reverse Minkowski theorem* [5], [6]. Given the *theta series ratio* $\Delta_\Lambda(\tau) \triangleq {}^{\Theta_\Lambda(i\tau)}/_{\Theta_{\mathbb{Z}^n}(i\tau)}$ of a lattice Λ, a key result in this theory is that $\Delta_\Lambda(\tau) \leq 1$ for all stable lattices Λ, when τ is either very small or very large [5]. However, whether this inequality holds *for all* $\tau > 0$ remains an open problem.

In the context of wiretap channel communication, Belfiore and Solé [7] have conjectured that the global minimum of the theta series ratio of unimodular lattices is achieved at $\tau = 1$. This result is not completely demonstrated, but it is known to be true for extremal unimodular lattices [8], several unimodular lattices and even-dimensional Construction A unimodular lattices from binary self-dual codes in small dimensions [9], [10], many unimodular lattices constructed via *direct-sum* [11], and Construction A and A_4 unimodular lattices satisfying a numerical sufficient condition [12], [13]. The conjecture was further extended to isodual [14] and formally unimodular lattices [12].

Using techniques from the generalized theta series, we demonstrate that there exist isodual lattices such that $\Delta_\Lambda(\tau) > 1$, and moreover, such that $\tau = 1$ is not the global minimum of the theta series ratio $\Delta_\Lambda(\tau)$, invalidating the conjectures [14, Conj. 1] and [12, Conj. 37], since isodual lattices are also formally unimodular.

Moreover, the contributions of this paper are:

i) An original lattice invariant, the *generalized theta series* of a lattice Λ, which can assist in *hearing the shape of a lattice*, that is, distinguishing between two non-isomorphic lattices that share the same theta series, provided their generalized theta series can be determined. Moreover, we define the *r-th generalized Euclidean norms* of a lattice, which reflects the concept of the generalized Hamming weight of a linear code.

ii) A connection between the generalized theta series and the r-th densest sublattice problem [15], which asks to find the r linearly independent vectors in a lattice Λ that yields to the smallest volume.

iii) We verify the stability of lattices via the generalized theta series.

iv) We show that conjectures concerning secure communication in a Gaussian wiretap channel *do not hold* for isodual lattices, as well as for formally unimodular lattices, by providing explicit counterexamples.

II. Preliminaries

A. Notation

We denote by $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ the set of naturals, integers, and reals, respectively. $[i : j] \triangleq \{i, i+1, \ldots, j\}$ for $i, j \in \mathbb{Z}$,

$i \le j$. Vectors are *row* vectors and boldfaced, e.g., $\boldsymbol{x}$. The all-zero vector is denoted by $\mathbf{0}$. Matrices and sets are represented by capital sans serif letters and calligraphic uppercase letters, respectively, e.g., X and $\mathcal{X}$. An identity matrix $n \times n$ is denoted by I_n. The inner product of two vectors is denoted by $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$. The natural embedding $\phi_q \colon \mathbb{Z}_q^n \to \mathbb{Z}^n$ is such that $\phi_q(x)$ maps each element $x \in \mathbb{Z}_q$ to the corresponding integer.

B. Lattices and Linear Codes

A *lattice* $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$. A (full rank) lattice can also be seen as $\Lambda = \{\boldsymbol{\lambda} = \boldsymbol{u}\mathsf{L}_{n\times n} \colon \boldsymbol{u} \in \mathbb{Z}^n\}$, where the n rows of the *generator matrix* L form a lattice basis in $\mathbb{R}^n$. If a lattice Λ has generator matrix L, then the lattice $\Lambda^\star \subset \mathbb{R}^n$ generated by $\left(\mathsf{L}^{-1}\right)^\mathsf{T}$ is called the *dual lattice* of Λ. The *volume* of a lattice Λ is $\mathrm{vol}(\Lambda) = |\det(\mathsf{L})|$. A *sublattice* Λ' of a lattice Λ is a lattice such that $\Lambda' \subseteq \Lambda$.

Next, we define the theta series of a lattice Λ.

Definition 1 (Theta series): Let Λ be a lattice. Its theta series is given by

$$\Theta_\Lambda(z) = \sum_{\boldsymbol{\lambda}\in\Lambda} q^{\|\boldsymbol{\lambda}\|^2} = \sum_{\boldsymbol{\lambda}\in\Lambda} \mathrm{e}^{i\pi z\|\boldsymbol{\lambda}\|^2},$$

where $q \triangleq \mathrm{e}^{i\pi z}$ and $\mathrm{Im}\{z\} > 0$.

Here, we will consider z to be purely imaginary. Then, the theta series of Λ reduces to

$$\Theta_\Lambda(i\tau) = \sum_{\boldsymbol{\lambda}\in\Lambda} \mathrm{e}^{-\pi\tau\|\boldsymbol{\lambda}\|^2}.$$

A lattice Λ is said to be *integral* if the inner product of any two lattice vectors is an integer or equivalently if and only if $\Lambda \subseteq \Lambda^\star$. An integral lattice such that $\Lambda = \Lambda^\star$ is a *unimodular* lattice. A lattice that can be obtained from its dual by a rotation or reflection is called *isodual*. We say that a lattice Λ is *formally unimodular* if and only if $\Theta_\Lambda(z) = \Theta_{\Lambda^\star}(z)$. It is worth mentioning that unimodular, isodual, and formally unimodular lattices all have volume equal to 1. A lattice Λ is said to be *stable* if $\mathrm{vol}(\Lambda) = 1$ and $\mathrm{vol}(\Lambda') \ge 1$ for all sublattice $\Lambda' \subseteq \Lambda$. Unimodular lattices are stable [16, Cor., p. 407].

Analogous to the theta series of a lattice, a binary $[n,k]$ linear code[1] $\mathscr{C} \subseteq \mathbb{F}_2^n$ has a *weight enumerator*

$$\begin{aligned} W_{\mathscr{C}}(x,y) &= \sum_{\boldsymbol{c}\in\mathscr{C}} x^{n-w_{\mathrm{H}}(\boldsymbol{c})} y^{w_{\mathrm{H}}(\boldsymbol{c})} \\ &= \sum_{w=0}^{n} A_w(\mathscr{C})\, x^{n-w} y^w, \end{aligned}$$

where $A_w(\mathscr{C}) \triangleq |\{\boldsymbol{c} \in \mathscr{C} \colon w_{\mathrm{H}}(\boldsymbol{c}) = w\}|$, $w \in [0:n]$.

Next, we define the *generalized Hamming weight* of linear codes, a quantity that characterizes the weights of subcodes of a given linear code $\mathscr{C}$.

[1]A binary $[n,k]$ code $\mathscr{C}$ is a k-dimensional linear subspace of $\mathbb{F}_2^n$. In general, codes can be defined over a Galois field $\mathbb{F}_q$.

Definition 2 (Generalized Hamming weight [1]): The r-th generalized Hamming weight of an $[n,k]$ code $\mathscr{C}$ is the size of the smallest support of an r-dimensional subcode of $\mathscr{C}$, i.e.,

$$d_r(\mathscr{C}) = \min\{w(\mathscr{C}_r) \colon \mathscr{C}_r \text{ is an } [n,r] \text{ subcode of } \mathscr{C}\},$$

considering $w(\mathscr{C}) = \bigl|\{i \in [1:n] \colon \exists\, \boldsymbol{c} = (c_1,\ldots,c_n) \in \mathscr{C} \text{ s.t. } c_i \neq 0\}\bigr|$, and $r \in [1:k]$. We define $\boldsymbol{d}(\mathscr{C}) \triangleq \{d_1(\mathscr{C}),\ldots,d_k(\mathscr{C})\}$ as the *weight hierarchy* of a code $\mathscr{C}$ and $d_r(\mathscr{C})$ denotes the r-th generalized Hamming weight of $\mathscr{C}$.

We remark that, in the literature, most results on generalized Hamming weights are established for binary $[n,k]$ codes. However, there also exist several results concerning linear codes over $\mathbb{F}_q$. See, for example, [17].

The generalized Hamming weight is monotonic.

Theorem 1: [1, Thm. 1] For an $[n,k]$ linear code $\mathscr{C}$ with $k > 0$, we have that

$$1 \le d_1(\mathscr{C}) < d_2(\mathscr{C}) < \cdots < d_k(\mathscr{C}) \le n.$$

Example 1: Consider two non-isometric $[6,3]$ binary codes $\mathscr{C}_1$ and $\mathscr{C}_2$ in [3, pp. 40–42], with respective generator matrices $\mathsf{G}^{\mathscr{C}_1} = (\mathsf{I}_3\ \mathsf{B}_1)$ and $\mathsf{G}^{\mathscr{C}_2} = (\mathsf{I}_3\ \mathsf{B}_2)$, where

$$\mathsf{B}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \mathsf{B}_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The weight hierarchies of $\mathscr{C}_1$ and $\mathscr{C}_2$ are

$$\boldsymbol{d}(\mathscr{C}_1) = \{2,4,6\} \text{ and } \boldsymbol{d}(\mathscr{C}_2) = \{2,3,6\}.$$

The distinct weight hierarchies indicate that the two codes are indeed non-isometric. However, they have the same weight enumerator

$$W_{\mathscr{C}_1}(x,y) = W_{\mathscr{C}_2}(x,y) = x^6 + 3x^4y^2 + 3x^2y^4 + y^6,$$

and thus, are said to be *isospectral*. ◊

Lattices can be constructed from linear codes through Construction A [2], [18]. A $\mathbb{Z}_q$ linear code $\mathscr{C}$ of length n is an additive subgroup of $\mathbb{Z}_q^n$.

Definition 3 (Construction A [18, p. 31]): Let $\mathscr{C}$ be a $\mathbb{Z}_q$ linear code, then $\Lambda_{\mathsf{A}_q}(\mathscr{C}) \triangleq \frac{1}{\sqrt{q}}(\phi_q(\mathscr{C}) + q\mathbb{Z}^n)$ is a lattice.

C. Conjectures on the Theta Series

Characterizing the theta series of a general lattice is a hard task. It has applications in many fields, being used to bound the success probability of eavesdropping a message in communication channels [7], or in theoretical computer science, where it is believed that the theta series of the integer lattice $\mathbb{Z}^n$ maximizes the theta series of stable lattices [19].

We start by defining a particular quotient of the theta series.

Definition 4 (Theta series ratio [20]): Let Λ be a lattice with volume $\mathrm{vol}(\Lambda) = 1$. The theta series ratio of Λ is defined by

$$\Delta_\Lambda(\tau) \triangleq \frac{\Theta_\Lambda(i\tau)}{\Theta_{\mathbb{Z}^n}(i\tau)}, \quad \tau \triangleq -iz > 0.$$

Regev and Stephen-Davidowitz conjectured that $\Delta_\Lambda(\tau) \le 1$ for all stable lattices [19].

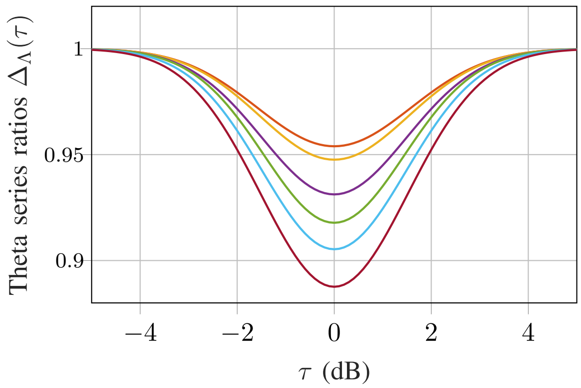

Fig. 1. Theta series ratios as a function of $\tau > 0$ for several *isodual* lattices that both satisfy Conjectures 1 and 2. Observe that $\Delta_\Lambda(\tau) \leq 1$ for all $\tau > 0$ and $\operatorname{argmin}_{\tau>0} \Delta_\Lambda(\tau) = 1$.

Conjecture 1 (Upper bound on the theta series ratio for stable lattices): For all stable lattices $\Lambda \subset \mathbb{R}^n$ and *for all* $\tau > 0$, it holds that

$$\Theta_\Lambda(i\tau) \leq \Theta_{\mathbb{Z}^n}(i\tau) \text{ or equivalently } \Delta_\Lambda(\tau) \leq 1.$$

In the context of Gaussian wiretap channel communication, the theta series ratio is also of fundamental importance since it upper bounds the error probability of an eavesdropper guessing a sent message once lattice coset encoding is performed [7]. The original conjecture was stated for unimodular lattices.

Conjecture 2 (Global minimum of the theta series ratio for unimodular lattices): The theta series ratio of a unimodular lattice Λ achieves its global minimum at $\tau = 1$, i.e.,

$$\operatorname*{argmin}_{\tau>0} \Delta_\Lambda(\tau) = 1.$$

Later on, the same conjecture was extended to isodual [14, Conj. 1] and formally unimodular lattices [12, Conj. 37]. Given that formally unimodular lattices are also isodual, we will focus on isodual lattices from this point onward. Nevertheless, the same conclusions apply to formally unimodular lattices.

Fig. 1 illustrates several *typical* isodual lattices that simultaneously satisfy Conjectures 1 and 2.

The argument for the minimization of the theta series ratio, relies on the concept of *weak secrecy gain*, which is simply the theta series ratio evaluated at a symmetry point τ_0, i.e., $\Delta_\Lambda(\tau_0)$, where τ_0 is such that for all $\tau > 0$,

$$\Delta_\Lambda(\tau_0 \cdot \tau) = \Delta_\Lambda({}^{\tau_0}\!/\!{}_{\tau}).$$

In [14, Conj. 1], the claim is that, given an isodual lattice Λ, the global minimum of its theta series ratio is achieved at the symmetry point $\tau_0 = 1$. We will refer to this formulation as the *secrecy gain conjecture* for isodual lattices.

III. Generalized Theta Series

Inspired by the concept of generalized Hamming weight, we define an equivalent notion for lattices.

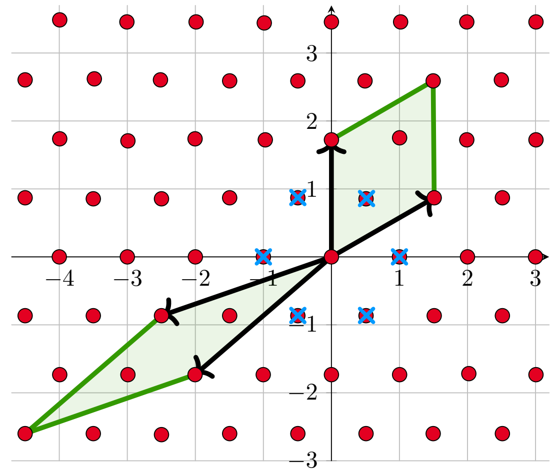

Fig. 2. Geometric interpretation of the generalized theta series.

Definition 5 (Generalized Theta Series): Consider a lattice $\Lambda \subset \mathbb{R}^n$. Its r-th generalized theta series is

$$\Theta_\Lambda^{(r)}(z) = \sum_{\substack{\{\boldsymbol{a}_i\}_{i=1}^r \subseteq \Lambda: \\ \operatorname{rank}(\mathsf{A})=r,}} q^{\det(\mathsf{A}\mathsf{A}^\mathsf{T})}, \tag{1}$$

where $\mathsf{A}^\mathsf{T} = [\boldsymbol{a}_1^\mathsf{T}, \ldots, \boldsymbol{a}_r^\mathsf{T}]$, $r \in [1:n]$, $q \triangleq \mathrm{e}^{i\pi z}$ and $\operatorname{Im}\{z\} > 0$.

Observe that, the definition of generalized theta series does not take into account the ordering. In other words, the lattice generated by any permutation of the vectors $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r\}$ is considered just once in the exponent of (1).

Due to the connection with the r-dimensional densest sublattice problem (r-DSP) [15] to be further discussed in Section V-A, it is known that the minimum determinant is uniquely determined and therefore, Definition 5 is well-defined. Moreover, the following holds.

Remark 1:

1) $\Theta_\Lambda(z) = 1 + \Theta_\Lambda^{(1)}(z)$.
2) The set $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r\} \subseteq \Lambda$ consisting of r linearly independent lattices vectors generates an r-dimensional sublattice $\Lambda' \subseteq \Lambda \subset \mathbb{R}^n$. Its volume is $\operatorname{vol}(\Lambda') = \sqrt{\det(\mathsf{A}\mathsf{A}^\mathsf{T})}$ where $\mathsf{A}^\mathsf{T} = [\boldsymbol{a}_1^\mathsf{T}, \ldots, \boldsymbol{a}_r^\mathsf{T}]$, $r \in [1:n]$.

Example 2: Consider the hexagonal lattice A_2, with basis $\{(1,0), ({}^1\!/\!{}_2, {}^{\sqrt{3}}\!/\!{}_2)\}$. From Definition 5, we get that

$$\Theta_{\mathsf{A}_2}^{(1)}(z) = 6q + 6q^3 + 6q^4 + 12q^7 + 6q^9 + \cdots$$
$$\Theta_{\mathsf{A}_2}^{(2)}(z) = 12q^{3/4} + 24q^{27/4} + 12q^{12} + 24q^{75/4} + \cdots$$

Geometrically, given a term $N_m q^m$ in the generalized theta series $\Theta_\Lambda^{(r)}(z)$, the exponent m corresponds to the volume of the fundamental region of a lattice generated by any combination of r linearly independent vectors; the integer N indicates how many set of r linearly independent vectors are there yielding the same volume. The blue crosses in Fig. 2 illustrate the six vectors with squared norm one in the first term of $\Theta_{\mathsf{A}_2}^{(1)}(z)$, while the green fundamental regions (with the same area) are generated by two sets of vectors that contribute to the term $24q^{27/4}$ in $\Theta^{(2)}_{\mathrm{A}_2}(z)$. $\Diamond$

Apart from enumerating the r-dimensional volumes for Λ, we adopt the concept of r-th generalized Hamming weights of codes [1], [21] and define the corresponding *generalized Euclidean norm* for a lattice Λ.

Definition 6 (r-th Generalized Euclidean Norm/r-Dimensional Minimum Sublattice Volume): The r-th generalized Euclidean norms are the minimum exponents defined in (1) for all $r \in [1:n]$ and,

$$\nu_r(\Lambda) = \min\{\det(\mathsf{A}\mathsf{A}^\mathsf{T}) : \{\boldsymbol{a}_i\}_{i=1}^r \subseteq \Lambda \text{ and } \operatorname{rank}(\mathsf{A}) = r\}.$$

Moreover, the norm hierarchy is defined as $\boldsymbol{\nu}(\Lambda) = \{\nu_r(\Lambda) \colon r \in [1:n]\}$.

Remark 2: Let λ_1 be the length of the shortest nonzero vector of a lattice Λ. It follows from Definition 6 that we have $\nu_1(\Lambda) = \lambda_1^2$ of the lattice Λ and $\nu_n(\Lambda) = \operatorname{vol}(\Lambda)^2$.

IV. Properties of the r-th Generalized Euclidean Norm

We now present a property related to the r-th generalized Euclidean norm for equivalent lattices.

Proposition 1: Consider two equivalent lattices $\Lambda, \overline{\Lambda} \subseteq \mathbb{R}^n$, i.e., $\mathsf{L}_{\overline{\Lambda}} = \alpha \mathsf{L}_\Lambda \mathsf{Q}$ for some $\alpha \neq 0$ and an orthogonal matrix $\mathsf{Q} \in \mathbb{R}^{n\times n}$. Then, $\nu_r(\overline{\Lambda}) = \alpha^{2r}\nu_r(\Lambda)$ for all $r \in [1:n]$.

Proof: Consider $\{\overline{\boldsymbol{a}}_i\}_{i=1}^r \subseteq \overline{\Lambda}$, $\overline{\mathsf{A}}^\mathsf{T} = [\overline{\boldsymbol{a}}_1^\mathsf{T}, \ldots, \overline{\boldsymbol{a}}_r^\mathsf{T}]$, $r \in [1:n]$, and $\operatorname{rank}(\overline{\mathsf{A}}) = r$. Observe that for a fixed i and $\overline{\boldsymbol{a}}_i \in \overline{\Lambda}$, we have $\overline{\boldsymbol{a}}_i = \boldsymbol{u}_i \mathsf{L}_{\overline{\Lambda}} = \alpha \boldsymbol{u}_i \mathsf{L}_\Lambda \mathsf{Q}$, where $\boldsymbol{u}_i \in \mathbb{Z}^n$. Therefore, the *Gram matrix* $\overline{\mathsf{A}}\overline{\mathsf{A}}^\mathsf{T}$ [2, p. 101] will have elements of the form

$$\begin{aligned}\langle \overline{\boldsymbol{a}}_i, \overline{\boldsymbol{a}}_j\rangle &= \langle \alpha\boldsymbol{u}_i\mathsf{L}_\Lambda\mathsf{Q}, \alpha\boldsymbol{u}_j\mathsf{L}_\Lambda\mathsf{Q}\rangle = \alpha^2\langle \boldsymbol{u}_i\mathsf{L}_\Lambda, \boldsymbol{u}_j\mathsf{L}_\Lambda\rangle \\ &= \alpha^2\langle \boldsymbol{a}_i, \boldsymbol{a}_j\rangle,\end{aligned}$$

for $i, j \in [1:r]$, $\boldsymbol{a}_i, \boldsymbol{a}_j \in \Lambda$. Since $\overline{\mathsf{A}}\overline{\mathsf{A}}^\mathsf{T}$ and $\mathsf{A}\mathsf{A}^\mathsf{T}$ are $r \times r$ matrices for a fixed rank r, we can conclude that

$$\det(\overline{\mathsf{A}}\overline{\mathsf{A}}^\mathsf{T}) = \alpha^{2r}\det(\mathsf{A}\mathsf{A}^\mathsf{T}).$$

This completes the proof. ∎

Example 3: Consider the D_4 lattice [2, p. 9] generated by the following generator matrix

$$\mathsf{L}_{\mathrm{D}_4} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

and another lattice $\overline{\mathrm{D}}_4$ with generator matrix $\mathsf{L}_{\overline{\mathrm{D}}_4} = \frac{1}{\sqrt{2}}\mathsf{L}_{\mathrm{D}_4}\mathsf{Q}$, which is equivalent to D_4 and

$$\mathsf{Q} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

is an orthogonal matrix. As a result, we numerically compute the norm hierarchy $\boldsymbol{\nu}(\mathrm{D}_4) = (2, 3, 4, 4)$ based on Definition 6, and Proposition 1 indicates that $\boldsymbol{\nu}(\overline{\mathrm{D}}_4) = (1, 3/4, 1/2, 1/4)$. $\Diamond$

V. Applications

A. Stability of Lattices

The generalized theta series naturally can identify whether a lattice is stable, which we address next.

A generalization of the the *shortest vector problem* (SVP) in a lattice Λ is the *r-DSP* [15].

Definition 7 (r-dimensional Densest Sublattice Problem (r-DSP)): Consider a lattice $\Lambda \subseteq \mathbb{R}^n$. Find r linearly independent lattice vectors $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_r\} \subseteq \Lambda$ such that it generates a sublattice achieving the smallest possible volume $\det(\mathsf{A}\mathsf{A}^\mathsf{T})$, where $\mathsf{A}^\mathsf{T} = [\boldsymbol{a}_1^\mathsf{T}, \ldots, \boldsymbol{a}_r^\mathsf{T}]$, $r \in [1:n]$.

Note that the first term of the generalized theta series $\Theta^{(r)}_\Lambda(z)$ resolves the r-DSP problem.

To the best of our knowledge, the most efficient algorithm to compute the r-DSP has running time at most $r^{\mathcal{O}(rn)}$, which is presented in [15]. Its main theoretical finding is the realization that the r-DSP solution either contains the lattice shortest vectors or one can efficiently generate a short list of $\mathcal{O}(r)^n$ lattice vectors that contains the solution to r-DSP.

Lemma 1 ([15, Lemma 3.1]): Consider an n-dimensional lattice Λ. A minimum-volume sublattice either contains all lattice vectors of length λ_1, or it contains a set of r linearly independent vectors, each of length at most $r\lambda_1$.

To verify whether a lattice is stable, one must ensure that for any $\Lambda' \subseteq \Lambda$, $\operatorname{vol}(\Lambda') \geq 1$. Thus, Lemma 1 can be used to verify the stability of a lattice computationally. In the following examples, we provide three concrete evidence demonstrating the fact that Construction A lattices obtained from codes over $\mathbb{Z}_q$ are not necessarily stable. We begin with an example based on the binary Construction A lattice, building upon Example 1.

Example 4: Consider the corresponding Construction A lattices $\Lambda_{\mathrm{A}_2}(\mathscr{C}_1)$ and $\Lambda_{\mathrm{A}_2}(\mathscr{C}_2)$, obtained from $\mathscr{C}_1$ and $\mathscr{C}_2$ as in Example 1, respectively. Using [15, Algorithm 1] we get

$$\boldsymbol{\nu}(\Lambda_1) = \{1, 1, 1, 1, 1, 1\},\ \boldsymbol{\nu}(\Lambda_2) = \{1, 3/4, 1/2, 3/4, 1, 1\},$$

which shows that $\Lambda_{\mathrm{A}_2}(\mathscr{C}_2)$ is not stable as there exists an 2-dimensional $\Lambda' \subseteq \Lambda_{\mathrm{A}_2}(\mathscr{C}_2)$ with $\operatorname{vol}(\Lambda') < 1$.

In fact, using Definition 5, with an extensive computation, we get

$$\begin{aligned}&\Theta^{(1)}_{\Lambda_{\mathrm{A}_2}(\mathscr{C}_1)}(z) = 12q^1 + 60q^2 + 160q^3 + 252q^4 + \cdots,\\ &\Theta^{(2)}_{\Lambda_{\mathrm{A}_2}(\mathscr{C}_1)}(z) = 300q^1 + \mathbf{1968}q^3 + \mathbf{3840}q^4 + \cdots,\\ &\Theta^{(2)}_{\Lambda_{\mathrm{A}_2}(\mathscr{C}_2)}(z) = 80q^{3/4} + \mathbf{44}q^1 + \mathbf{768}q^{7/4} + \cdots.\end{aligned}$$

It is worth mentioning that the boldfaced coefficients cannot be guaranteed by Lemma 1, as they do not correspond to the minimum sublattice volume. Here, we simply obtained the values numerically.

Furthermore, our findings indicate that the two Construction A lattices $\Lambda_{\mathrm{A}_2}(\mathscr{C}_1)$ and $\Lambda_{\mathrm{A}_2}(\mathscr{C}_2)$ are non-isometric, which partially addresses the question raised in [3]: "Can one can hear the shape of a lattice?" Thus, it appears that we can indeed "hear" the shapes of lattices through this newly introduced definition of the *generalized theta series* for lattices. $\Diamond$

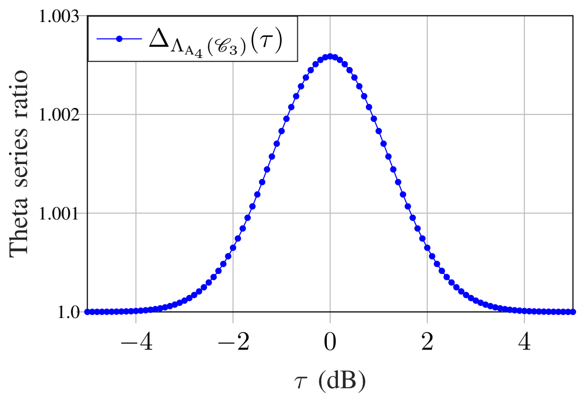

Fig. 3. Theta series ratio as a function of $\tau > 0$ in Example 5. Observe that $\Delta_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)}(\tau) > 1$ for all $\tau > 0$.

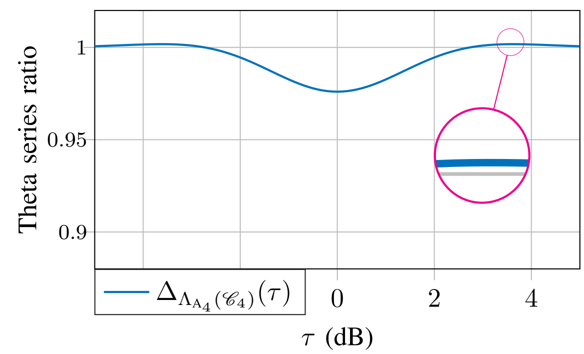

Fig. 4. Theta series ratio as a function of $\tau > 0$ for a $\Lambda_{\mathrm{A}_4}(\mathscr{C}_4)$ lattices that satisfy Conjecture 2. However, it can be observed that it does not satisfy Conjecture 1; that is, there exists some $\tau > 0$ such that $\Delta_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_4)}(\tau) > 1$.

Similarly, as the generalized Hamming weight can be used to distinguish equivalent codes, the generalized theta series serves as a geometric invariant that can help determine whether two lattices are isometric, which is the hard problem behind the *Lattice Isomorsphim Problem* (LIP) [22]. We emphasize, however, that this does not necessarily pose a threat to cryptographic schemes based on the LIP, since computing the r-th generalized Euclidean norm or generalized theta series remains computationally expensive and, therefore, impractical for general lattices.

B. Conjectures Do Not Hold for Isodual Lattices!

We provide next a counterexample which proves the secrecy gain conjecture for isodual lattices [14, Conj. 1] not to be true.

Example 5: Consider a $\mathbb{Z}_4$-linear code $\mathscr{C}_3$ with generator matrix

$$\mathsf{G}^{\mathscr{C}_3} = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 2 & 2 & 0 \end{pmatrix}.$$

Applying [15, Algorithm 1] we obtain

$$\boldsymbol{\nu}\big(\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)\big) = \{1, {}^3/_4, {}^1/_2, {}^3/_4, 1, 1\},$$

and thus the lattice $\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)$ is *not stable*. Moreover, its generalized theta series is given by

$$\Theta^{(1)}_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)}(z) = 12q^1 + 16q^{7/4} + 8q^2 + 32q^{9/4} + \cdots,$$
$$\Theta^{(2)}_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)}(z) = 144q^{3/4} + 8q^1 + 16q^{3/2} + \cdots.$$

Note that $\Lambda_{\mathrm{A}_4}(\mathscr{C}_3) = \frac{1}{2}(\phi_4(\mathscr{C}_3) + 4\mathbb{Z}^n)$ and $\mathscr{C}$ is an isodual bordered double circulant code [23, Lemma 2.4], thus $\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)$ is isodual, [24, p. 378], [13, Sec. III-B]. Its theta series ratio is illustrated in Fig. 3, and $\Delta_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_3)}(1) \approx 1.0026 > 1$, which demonstrates that Conjecture 1 is not true for isodual lattices. However, this does not disprove the conjecture since isodual lattices are not necessarily to be stable, as shown in this example. We also observe that, although its theta series ratio exhibits one symmetry point, it attains its *maximum* at $\tau = 1$, rather than the minimum. Therefore, Conjecture 2 does not hold as well. This invalidates the current formulation of the secrecy gain conjecture for isodual lattices [14, Conj. 1], and consequently, its generalization to formally unimodular lattices presented in [12, Conj. 37]. ♢

Next, we provide another compelling example that violates Conjecture 1 while satisfying Conjecture 2.

Example 6: Consider a $\mathbb{Z}_4$-linear code $\mathscr{C}_4$ with generator matrix

$$\mathsf{G}^{\mathscr{C}_4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}.$$

Applying [15, Algorithm 1] we get

$$\boldsymbol{\nu}\big(\Lambda_{\mathrm{A}_4}(\mathscr{C}_4)\big) = \{0.75, 0.88, 0.77, 0.88, 0.75, 1\},$$

which indicates that $\Lambda_{\mathrm{A}_4}(\mathscr{C}_4)$ is not stable.

We demonstrate the theta series ratio in Fig. 4. As shown, the theta series ratio clearly reaches its minimum at $\tau = 1$, thereby satisfying Conjecture 2. Nevertheless, there exist regions of τ where the theta series ratio remains strictly greater than 1, revealing that Conjecture 1 does not hold for this isodual lattice.

VI. Conclusion

We have presented a new lattice invariant, the generalized theta series. It characterizes the volume of lattices generated by r linearly independent lattice vectors, with $r \in [1:n]$. In terms of applications, calculating the generalized theta series of a lattice solves the r-dimensional densest sublattice problem, serves as an auxiliary tool to decide whether two lattices are isomorphic, and can be used to find stable lattices. In this work, we have applied this new lattice property to find counterexamples for a decade-long conjecture about the secrecy gain of isodual (and more recently, formally self-dual) lattices. Moving forward, we want to demonstrate further properties of the generalized theta series, find relations through the Jacobi theta functions [2, pp. 102–105] to speed up its rather costly calculations. We also aim to further investigate the relationship between the r-th generalized Hamming weights of a code and the r-th generalized Euclidean norms of the corresponding lattices derived from the code.

REFERENCES

[1] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer, 1999.

[3] J. H. Conway and F. Y. C. Fung, *The Sensual (quadratic) Form*. Mathematical Association of America, 2009.

[4] A. Schiemann, "Ternary positive definite quadratic forms are determined by their theta series," *Math. Ann.*, vol. 308, no. 3, pp. 507–517, Jul. 1997.

[5] O. Regev and N. Stephens-Davidowitz, "A reverse Minkowski theorem," in *Proc. 49th Annu. ACM Symp. Theory Comput. (STOC)*, Montreal, QC, Canada, June 19–23, 2017, pp. 941–953.

[6] ——, "A simple proof of a reverse Minkowski theorem for integral lattices," Jun. 2023, arXiv:2306.03697v1 [math.MG].

[7] J.-C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian wiretap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Dublin, Ireland, Aug. 30 – Sep. 3, 2010.

[8] A.-M. Ernvall-Hytonen, "On a conjecture by Belfiore and Solé on some lattices," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5950–5955, Sep. 2012.

[9] F. Lin and F. Oggier, "Gaussian wiretap lattice codes from binary self-dual codes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Lausanne, Switzerland, Sep. 3–7, 2012.

[10] ——, "A classification of unimodular lattice wiretap codes in small dimensions," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3295–3303, Jun. 2013.

[11] J. Pinchak and B. A. Sethuraman, "The Belfiore-Solé conjecture and a certain technique for verifying it for a given lattice," in *Proc. Inf. Theory Appl. Workshop (ITA), Univ. California*, San Diego, CA, USA, Feb. 9–14, 2014.

[12] M. F. Bollauf, H.-Y. Lin, and Ø. Ytrehus, "Formally unimodular packings for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 69, no. 12, pp. 7755–7776, Dec. 2023.

[13] ——, "Secrecy gain of formally unimodular lattices from codes over the integers modulo 4," *IEEE Trans. Inf. Theory*, vol. 70, no. 5, pp. 3309–3329, May 2024.

[14] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.

[15] D. Dadush and D. Micciancio, "Algorithms for the densest sub-lattice problem," in *Proc. Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, New Orleans, LA, USA, Jan. 6–8, 2013, pp. 1103–1122.

[16] L. Weng, "Stability and new non-abelian zeta functions," in *Number Theoretic Methods*, S. Kanemitsu and C. Jia, Eds. New York, NY, USA: Springer, 2002, pp. 405–419.

[17] R. Jurrius and R. Pellikaan, "Extended and generalized weight enumerators," in *Proc. Int. Workshop Coding Cryptography (WCC)*, Ullensvang, Norway, May 10–15, 2009, pp. 76–91.

[18] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge, U.K.: Cambridge University Press, 2014.

[19] O. Regev and N. Stephens-Davidowitz, "A reverse Minkowski theorem," *Ann. Math.*, vol. 199, no. 1, Jan. 2024.

[20] M. F. Bollauf and H.-Y. Lin, "On the maximum theta series over unimodular lattices," Mar. 2024, arXiv:2403.16932v2 [math.MG].

[21] T. Helleseth, T. Klve, and Ø. Ytrehus, "Generalized Hamming weights of linear codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 1133–1140, May 1992.

[22] L. Ducas and W. van Woerden, "On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography," in *Proc. 41st Annu. Int. Conf. Theory Appl. Crypto. Techn. (EUROCRYPT)*, Trondheim, Norway, May 30 – Jun. 3, 2022, pp. 643–673.

[23] C. Bachoc, T. A. Gulliver, and M. Harada, "Isodual codes over $\mathbb{Z}_{2k}$ and isodual lattices," *J. Algebraic Combinatorics*, vol. 12, no. 3, pp. 223–240, 2000.

[24] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge University Press, 2003.