Barreal, Amaro; Damir, Mohamed Taoufiq; Freij-Hollanti, Ragnar; Hollanti, Camilla

An approximation of theta functions with applications to communications

Published in:
SIAM Journal on Applied Algebra and Geometry

DOI:
10.1137/19M1275334

Published: 01/01/2020

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Barreal, A., Damir, M. T., Freij-Hollanti, R., & Hollanti, C. (2020). An approximation of theta functions with applications to communications. *SIAM Journal on Applied Algebra and Geometry*, *4*(4), 471-501. https://doi.org/10.1137/19M1275334

SIAM J. APPL. ALGEBRA GEOMETRY
Vol. 4, No. 4, pp. 471–501

An Approximation of Theta Functions with Applications to Communications*

Amaro Barreal†, Mohamed Taoufiq Damir‡, Ragnar Freij-Hollanti‡, and Camilla Hollanti‡

Abstract. Computing the theta series of an arbitrary lattice, and more specifically a related quantity known as the flatness factor, has been recently shown to be important for lattice code design in various wireless communication setups. However, the theta series is in general not known in closed form, excluding a small set of very special lattices. In this article, motivated by the practical applications as well as the mathematical problem itself, a simple approximation of the theta series of a lattice is derived. A rigorous analysis of its accuracy is provided. In relation to this, maximum-likelihood decoding in the context of compute-and-forward relaying is studied. Following previous work, it is shown that the related metric can exhibit a flat behavior, which can be characterized by the flatness factor of the decoding function. Contrary to common belief, we note that the decoding metric can be rewritten as a sum over a random lattice only when at most two sources are considered. Using a particular matrix decomposition, a link between the random lattice and the code lattice employed at the transmitter is established, which leads to an explicit criterion for code design, in contrast to implicit criteria derived previously. Finally, candidate lattices are examined with respect to the proposed criterion using the derived theta series approximation.

Key words. arbitrary lattices, compute-and-forward protocol, flatness factor, geometry of lattices, lattice codes, theta series approximation, wireless communications, wiretap channels

AMS subject classifications. 11H06, 11P21, 11F27, 11H71

DOI. 10.1137/19M1275334

1. Introduction.

Lattices are mathematical objects which have become indispensable for code design in many areas of wireless communications, as many design criteria for reliable performance rely on the discrete and algebraic structure of lattices. Despite their deceptively simple structure, many computational problems related to lattices are extremely challenging, such as the famous *shortest vector problem* or related *closest vector problem*. In particular, as the same lattice can be generated by distinct bases, a natural problem is to find a basis consisting of shortest vectors, a problem so hard that cryptographic protocols have been developed around it. Moreover, even enumerating vectors of certain lengths is very difficult. The generating function for the number of elements in a lattice of a given norm is known as the *theta series* of the lattice. This is an interesting object in its own right, and it is not surprising that it is known only in closed form for a very small set of highly structured lattices.

*Received by the editors July 16, 2019; accepted for publication (in revised form) September 1, 2020; published electronically December 3, 2020.
https://doi.org/10.1137/19M1275334
Funding: This work was supported by Academy of Finland grants 276031, 282938, and 303819.
†Coop IT Digital Analytics and AI, Basel, 4002, Switzerland (am.barreal@gmail.com).
‡Department of Mathematics and Systems Analysis, Aalto University, 00076 Aalto (Espoo), Finland (mohamed.damir@aalto.fi, ragnar.freij@aalto.fi, camilla.hollanti@aalto.fi).

From an applications perspective, it has been recently shown that code design in various areas of wireless communications and cryptography can profit from studying the theta series of certain involved lattices, e.g., for *wiretap code design* [1, 2], *dither avoidance in lattice noise quantization* [3], or *compute-and-forward relaying* [4]. Compute-and-forward relaying is a promising physical layer network coding protocol proposed in the award-winning paper [4] and exploits the natural effects of interference by decoding linear combinations of the transmitted messages at the intermediate relays to achieve high computation rates. It will be the main applicational focus in this paper. For more details, see section 4.

Originally, a relay operating under the compute-and-forward protocol would first scale the received signal before applying a minimum-distance decoder to obtain an estimate of the desired linear combination of the codewords. The decoding error probability for this decoding procedure was studied in [5]. It was later in [6] where *maximum-likelihood* (ML) decoding at the relay was first considered. An approach to lattice code design for compute-and-forward was simultaneously derived therein, as well as in [10], and the first efficient decoding algorithm was proposed in dimension 1. The subsequent work [12] builds upon those innovative articles and continues the investigation toward efficient decoding algorithms, an example of which is derived for Gaussian channels without fading. The fundamental work carried out in [6, 10] is essential for code design considerations, as it introduces the notion of the *flatness factor* of a lattice and utilizes it to derive an implicit lattice code design criterion. This criterion is indirect in the sense that it relates to an uncontrollable sum of random lattices and not to the code lattices themselves, where the randomness is enabled by the physical channel. It is also noteworthy that following the work [6], the common belief has been that this sum can be rewritten as a sum over elements of a lattice for any number of transmitters. This is, as shown in this article, the case only if at most two sources are considered, the case studied empirically in [6, 10]. More recently, the compute-and-forward protocol has been extended to more general rings of algebraic integers [13].

The article is structured as follows. We start by recalling the most important results related to lattices in section 2. The concepts of theta series and flatness factor are subsequently introduced in section 3, wherein we derive a simple but accurate approximation of the theta series and, consequently, the flatness factor of a lattice (cf. Definition 17 and the equations beneath). We provide a rigorous study on the accuracy of the approximation, along with some illustrating plots and discussion. In section 4, we summarize the compute-and-forward protocol and, following [6, 10], investigate the behavior of the ML decoding metric in terms of its flatness factor. Adopting certain restrictions, we establish a link between the resulting random lattice and the code lattice, allowing for an explicit lattice code design criterion. Namely, we show that in order to maximize the flatness factor of the random lattice, it suffices to maximize that of the code lattice. We then make use of the derived theta series approximation to investigate different lattices in varying dimensions with respect to the design criterion. The main contributions are the following.

- In Theorem 4 we derive a simple but accurate approximation of the theta series of a lattice. For a fixed dimension, the approximation is merely a rational function and in most cases significantly outperforms a mere series truncation approximation. Such an easy-to-compute approximation is important, as approximating the theta series is crucial in many lattice related applications as closed form expressions are unknown

even for most deterministic lattices. In particular, the approximation also yields an approximation of the lattice flatness factor via Definition 17, which relates to, e.g., compute-and-forward decoding, wiretap coset code design, smoothing parameter in cryptography, and dither avoidance in lattice noise quantization as mentioned above.

- We provide a rigorous analysis on the accuracy of the approximation as well as some intuition and discussion on its qualities (sections 3.1 and 3.2.). More precisely,
  - we show that our approximation is, on average (over the space of all lattices), below the value of the complete theta series, and furthermore, we show that the error term, on average, goes to zero both when $q \to 1$ (resp., $\sigma \to \infty$) and when $q \to 0$ (resp., $\sigma \to 0$);
  - we show that for any fixed j, there is a threshold σ_j such that our approximation is larger than Θ_j (the jth term truncation) for any $\sigma > \sigma_j$;
  - we show that we are better than the first term truncation, except possibly for some small values of σ for some lattices, depending on the kissing number of the lattice.

  Combining these results as well as our numerical examples, we are convinced that there is a very strong basis for using this approximation.
- We provide a simple explicit formula for computing the approximation for even dimensions. An explicit formula can be also derived for odd dimensions.
- We provide an alternative description of the error term that now more explicitly depends on the first minimum and not on the Lipschitz constant.
- As a special case, we motivate the accuracy by a heuristic on the minimality of the error term when the lattice is chosen to be well-rounded of dimension 2 or 3. This case is of particular interest for wireless communications.
- The compute-and-forward ML decoding framework is slightly generalized in Proposition 20 to allow for more general lattices than in previous work. While the analysis of the function can become more difficult depending on the matrix decomposition used, the decoding procedure can nonetheless be executed by the relay also in this more general setting.
- In Lemma 21, we note that the decoding metric can be rewritten as a sum over elements of a lattice only for two sources, rectifying the common belief that this holds for any number of transmitting sources.
- Theorem 23 establishes a link between the code lattice and the random lattice involved in the ML-decoding metric, allowing us to state an explicit design criterion for the code lattice, in contrast to previous implicit criteria.
- Finally, various lattices are examined using the explicit design criterion and derived theta series approximation.

2. Lattices.

This section is dedicated to acquainting the reader with basic concepts in lattice theory. In this article, a vector is labeled in bold, $\mathbf{v}$, and is always represented as a column vector.

Definition 1. *A* lattice $\Lambda \subset \mathbb{R}^n$ *is a discrete subgroup of* $\mathbb{R}^n$ *with the property that there exists a basis* $\{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$ *of* $\mathbb{R}^n$ *such that*

$$\Lambda = \bigoplus_{i=1}^{t} \mathbf{b}_i \mathbb{Z}. \tag{1}$$

We say that $\{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$ *is a* $\mathbb{Z}$-basis *of* Λ*, thus* $\Lambda \cong \mathbb{Z}^t$ *as Abelian groups. We call* $t = \mathrm{rk}(\Lambda) \leq n$ *the* rank*, and* n *the* dimension *of* Λ*. A lattice* $\Lambda' \subset \mathbb{R}^n$ *such that* $\Lambda' \subset \Lambda$ *is called a* sublattice *of* Λ*.*

By discrete we mean that the metric on $\mathbb{R}^n$ defines the discrete topology on Λ. Note also that if $\dim(\Lambda) = \dim(\Lambda')$, then the index $|\Lambda/\Lambda'|$ is finite.

More conveniently, we can define a *generator matrix* $M_\Lambda := \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_t \end{bmatrix}$, so that every point $\mathbf{x} \in \Lambda$ can be expressed as $\mathbf{x} = M\mathbf{z}$ for some vector $\mathbf{z} \in \mathbb{Z}^t$. Henceforth we will only consider *full* lattices, that is, where $t = n$.

Remark 1. Given a pair of full lattices $\Lambda_1 \subseteq \Lambda_2$, we will say that Λ_1 is *nested* in Λ_2. We refer to Λ_2 as the *fine* lattice and to Λ_1 as the *coarse* lattice. Similarly, a sequence $\Lambda_1, \ldots, \Lambda_s$ of lattices is *nested* if $\Lambda_1 \subseteq \Lambda_2 \subseteq \cdots \subseteq \Lambda_s$.

Given a full lattice $\Lambda \subset \mathbb{R}^n$, the ith *successive minimum* of Λ, for $i = 1, \ldots, n$, is defined as

$$\lambda_i = \lambda_i(\Lambda) := \left(\inf\left\{r \middle| \dim(\mathrm{span}(\Lambda \cap \mathcal{B}_{\mathbf{0}}(r))) \geq i\right\}\right)^2, \tag{2}$$

where $\mathcal{B}_{\mathbf{0}}(r)$ is the sphere of radius r centered at the origin. The first minimum, $\lambda_1 = \min_{\mathbf{x}\in\Lambda} ||\mathbf{x}||^2$ is referred to as the (square) *minimal norm* of Λ, which exists due to the discreteness property of the lattice. If all successive minima are equal, $\lambda_1 = \cdots = \lambda_n$, the lattice is called *well-rounded*.

Consider now a lattice Λ with generator matrix $M_\Lambda = [\mathbf{b}_i]_{1\leq i\leq n}$. The *fundamental parallelotope* of Λ is defined as

$$\mathcal{P}_\Lambda := \left\{ \sum_{i=1}^{n} \mathbf{b}_i z_i \middle| \, 0 \leq z_i < 1 \right\}, \tag{3}$$

and we define the *volume* of Λ to be the volume of $\mathcal{P}_\Lambda$,

$$\mathrm{vol}\,\Lambda := \mathrm{vol}\,\mathcal{P}_\Lambda = |\det(M_\Lambda)|\,. \tag{4}$$

Note that $\mathrm{vol}\,\Lambda$ is independent of the choice of the generator matrix M_Λ. We can easily compute the volume of a sublattice $\Lambda' \subset \Lambda$ as $\mathrm{vol}\,\Lambda' = \mathrm{vol}\,\Lambda\,|\Lambda/\Lambda'|$.

A further useful function, not only for coding-theoretic purposes, is a *lattice quantizer* Q_Λ, a function that maps every point $\mathbf{y} \in \mathbb{R}^n$ to its closest point in the lattice. This function allows us to define a *modulo-lattice* operation, $\mathbf{y} \pmod{\Lambda} := \mathbf{y} - Q_\Lambda(\mathbf{y})$. Given a lattice Λ and a lattice quantizer Q_Λ, we can associate to each lattice point $\mathbf{x} \in \Lambda$ its *Voronoi cell*, the set

$$\mathcal{V}_\Lambda(\mathbf{x}) := \{\mathbf{y} \in \mathbb{R}^n | \, Q_\Lambda(\mathbf{y}) = \mathbf{x}\}\,. \tag{5}$$

The Voronoi cell around the origin, $\mathcal{V}(\Lambda) := \mathcal{V}_\Lambda(\mathbf{0})$, is called the *basic Voronoi cell* of Λ.

With the above definitions, we can now define the notion of a *nested lattice code*, an object widely used for code construction in different communications scenarios.

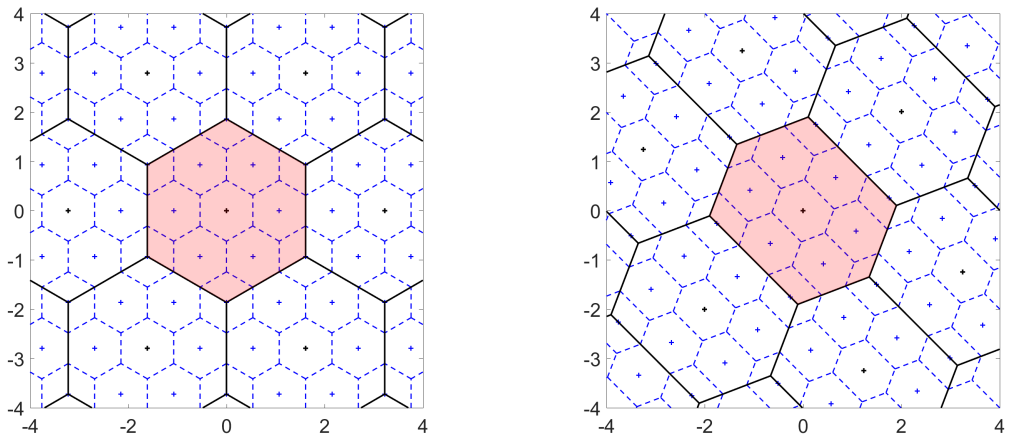

Figure 1. *Nested lattices $\Lambda_C \subset \Lambda_F = 3\Lambda_C$ with the Voronoi cells around each lattice point of the coarse (solid) and fine (dashed) lattices. On the left figure we fix $\Lambda_C = A_2$, the hexagonal lattice, and on the right figure $\Lambda_C = \Psi(\mathcal{O}_{\mathbb{Q}(\sqrt{5})})$, the lattice obtained via the canonical embedding Ψ of the ring of integers of the algebraic number field $\mathbb{Q}(\sqrt{5})$. The centered Voronoi cell $\mathcal{V}(\Lambda_C)$ (red) contains a set of representatives for a nested lattice code $\mathcal{C}(\Lambda_C, \Lambda_F)$ of cardinality $|\mathcal{C}(\Lambda_C, \Lambda_F)| = |\Lambda_F/\Lambda_C| = 9$.*

Definition 2. *Let $\Lambda_C \subset \Lambda_F$ be a pair of nested lattices. We define a* nested lattice code *$\mathcal{C}(\Lambda_C, \Lambda_F)$ as the set of representatives*

$$\mathcal{C}(\Lambda_C, \Lambda_F) := \{[\mathbf{x}] \in \Lambda_F \pmod{\Lambda_C} \,|\, \mathbf{x} \in \Lambda_F\} = \Lambda_F \cap \mathcal{V}(\Lambda_C). \tag{6}$$

The code rate *of $\mathcal{C}(\Lambda_C, \Lambda_F)$ in bits per dimension is*

$$\mathcal{R} = \frac{1}{n}\log_2 |\mathcal{C}(\Lambda_C, \Lambda_F)| = \frac{1}{n}\log_2 \frac{\operatorname{vol}\Lambda_C}{\operatorname{vol}\Lambda_F} = \frac{1}{n}\log_2 |\Lambda_F/\Lambda_C|. \tag{7}$$

Note that some coset representatives fall on the boundary of $\mathcal{V}(\Lambda_C)$ and need to be selected systematically. We illustrate the introduced concepts in Figure 1.

3. The theta series and flatness factor of a lattice.

In this section, we introduce the objects of main interest for this article: the *theta series*, and a related quantity, the *flatness factor* of a lattice.

Definition 3. *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice. For each $r \in \mathbb{R}$, define*

$$\Omega_\Lambda(r) := \left|\left\{\mathbf{x} \in \Lambda \mid ||\mathbf{x}||^2 = r\right\}\right|, \tag{8}$$

$$\Sigma_\Lambda(r) := \left|\left\{\mathbf{x} \in \Lambda \mid ||\mathbf{x}||^2 \leq r\right\}\right| = \sum_{0<i\leq r} \Omega_\Lambda(i). \tag{9}$$

The theta series *of Λ is the generating function*

$$\Theta_\Lambda(q) := 1 + \sum_{r>0} \Omega_\Lambda(r) q^r = \sum_{\mathbf{x}\in\Lambda} q^{||\mathbf{x}||^2}. \tag{10}$$

Remark 2. The theta series converges absolutely if $0 \leq q < 1$. We further note that

$$\arg\min_{r>0} \{\Omega_\Lambda(r) > 0\} = \lambda_1, \qquad \min_{r>0} \{\Omega_\Lambda(r) > 0\} = \kappa(\Lambda), \tag{11}$$

where $\kappa(\Lambda)$ is the kissing number of Λ. It is thus clear that $\Theta_\Lambda(q)$ encodes important features of Λ.

More generally, the theta series is defined in terms of a complex variable $q = e^{\pi i z}$, where $z \in \mathbb{C}$. In this case, $\Theta_\Lambda(q)$ is a holomorphic function for $\Im(z) \geq 0$. For the purposes of this article, however, it suffices to view $\Theta_\Lambda(q)$ as a formal power series in a real variable q.

Although of great importance, the theta series is unfortunately known only in closed form for a handful of lattices, for example, those tabulated in Table 1, and is usually given in terms of the *Jacobi theta functions*

$$\theta_2(q) = \sum_{k=-\infty}^{\infty} q^{\left(k+\frac{1}{2}\right)^2}, \quad \theta_3(q) = \sum_{k=-\infty}^{\infty} q^{k^2}, \quad \theta_4(q) = \sum_{k=-\infty}^{\infty} (-q)^{k^2}. \tag{12}$$

Even so, the Jacobi theta functions are by no means simple functions, but rather hard. The reason for this small set of lattices with known closed form theta series is that efficient counting of lattice points in domains in arbitrary dimensions is still an open problem. While many results have been obtained over the last two decades, such as the results in [15, 16, 18], the settings are so general that the upper bounds on the number of lattice points in bounded domains are far from being tight, even for very simple lattices and domains. Thus, being able to efficiently compute even an approximated version of the theta series of an arbitrary lattice is a problem which is interesting in its own right.

As additional motivation, and as we shall see in later parts of this article, recent work on lattice code design in different wireless communication scenarios [1, 3, 6, 10] has led to considering the *flatness factor* of a lattice, which itself is directly related to the theta series of the lattice—see Definition 17 and the equations beneath in section 3.4.

Table 1
Various important lattices and their basic attributes.

Lattice	Dim	λ_1	$\operatorname{vol}\Lambda$	$\Theta_\Lambda(q)$
$\mathbb{Z}^n$ Integer	$n \geq 1$	1	1	$\theta_3^n(q)$
D_n Checkerboard	$n \geq 3$	2	2	$\frac{1}{2}(\theta_3^n(q) + \theta_4^n(q))$
A_2 Hexagonal	2	1	$\sqrt{\frac{3}{4}}$	$\theta_2(q)\theta_2(q^3) + \theta_3(q)\theta_3(q^3)$
E_8 Gosset	8	2	1	$\frac{1}{2}(\theta_2^8(q) + \theta_3^8(q) + \theta_4^8(q))$
K_{12} Coxeter-Todd	12	4	27	$\frac{9}{32}\theta_2^6(q)\theta_2^6(q^3) + \left(\theta_2(q^4)\theta_2(q^{12}) + \theta_3(q^4)\theta_3(q^{12})\right)^6$ $+\frac{45}{16}\theta_2^4(q)\theta_2^4(q^3)\left(\theta_2(q^4)\theta_2(q^{12}) + \theta_3(q^4)\theta_3(q^{12})\right)^2$
L_{24} Leech	24	4	1	$\frac{1}{2}(\theta_2^8(q) + \theta_3^8(q) + \theta_4^8(q))^3 - \frac{45}{16}(\theta_2(q)\theta_3(q)\theta_4(q))^8$

We define the *gamma function* and the *incomplete gamma function* for $a \in \mathbb{R}, x > 0$, respectively, as

$$\Gamma(a) := \int_0^\infty t^{a-1}e^{-t}dt, \quad \Gamma(a,x) := \int_x^\infty t^{a-1}e^{-t}dt.$$

For an integer argument $a = n \in \mathbb{N}$, we have $\Gamma(n) = (n-1)!$.

Theorem 4. *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice with volume $\operatorname{vol}\Lambda$ and minimal norm λ_1. The theta series $\Theta_\Lambda(q)$, where $0 \le q < 1$, can be expressed as*

$$\Theta_\Lambda(q) = (1-q^{\lambda_1}) - \frac{\log(q)\lambda_1^{\frac{n}{2}+1}\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)\operatorname{vol}\Lambda}\int_1^\infty t^{\frac{n}{2}}q^{\lambda_1 t}dt + \Xi(\Lambda,n,L,q), \tag{13}$$

where

$$\Xi(\Lambda,n,L,q) = -C(\Lambda,n,L)\log(q)\lambda_1\int_1^\infty t^{\frac{n-1}{2}}q^{\lambda_1 t}dt. \tag{14}$$

The constant $C(n,\Lambda,L)$ depends on n, Λ, and a Lipschitz constant L.

We will build up the proof using a series of propositions.

Proposition 5. *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice with minimal norm λ_1. Then,*

$$\Theta_\Lambda(q) = \left(1-q^{\lambda_1}\right) - \log(q)\lambda_1\int_1^\infty \Sigma_\Lambda(\lambda_1 t)q^{\lambda_1 t}dt. \tag{15}$$

Proof. Using the elementary fact $\int_a^\infty q^t dt = -\frac{q^a}{\log(q)}$ for $a \ge 0$, we write

$$\Theta_\Lambda(q) = \sum_{\mathbf{x}\in\Lambda} q^{||\mathbf{x}||^2} = \sum\nolimits_{\mathbf{x}\in\Lambda}\int_{||\mathbf{x}||^2}^\infty -\log(q)q^t dt \tag{16}$$

$$= -\int_0^\infty \left|\left\{\mathbf{x}\in\Lambda \,|\, ||\mathbf{x}||^2 \le t\right\}\right|\log(q)q^t dt \tag{17}$$

$$= -\int_0^\infty \Sigma_\Lambda(t)\log(q)q^t dt. \tag{18}$$

We observe that $\Sigma_\Lambda(\lambda_1 t) \equiv 1$ for $t \in [0,1)$; thus by substituting $t \mapsto \lambda_1 t$ and splitting the integration range, we have

$$\Theta_\Lambda(q) = -\int_0^1 \Sigma_\Lambda(\lambda_1 t)\log(q)\lambda_1 q^{\lambda_1 t}dt - \int_1^\infty \Sigma_\Lambda(\lambda_1 t)\log(q)\lambda_1 q^{\lambda_1 t}dt \tag{19}$$

$$= \left(1-q^{\lambda_1}\right) - \log(q)\lambda_1\int_1^\infty \Sigma_\Lambda(\lambda_1 t)q^{\lambda_1 t}dt. \tag{20}$$

∎

The next step is to estimate the quantity $\Sigma_\Lambda(r)$, which counts the number of lattice points in an n-sphere of radius $\sqrt{r}$. To that end, we first need the following technical definition and a related lemma.

Definition 6. *Let $S \subset \mathbb{R}^n$ be a bounded convex set. We say that S is $(n-1)$-*Lipschitz parametrizable*, and write $S \in \mathrm{Lip}(n, T, L)$, if there are T maps $\phi_1, \ldots, \phi_T : [0,1]^{n-1} \to S$, the union of images of which cover S, and satisfying for all $1 \leq i \leq T$ the Lipschitz condition*

$$|\phi_i(\mathbf{x}) - \phi_i(\mathbf{y})| \leq L\,|\mathbf{x} - \mathbf{y}|\,. \tag{21}$$

Lemma 7 (see [19, Thm. 2, p. 128]). *Let $D \subset \mathbb{R}^n$ be such that ∂D is $(n-1)$-Lipschitz parametrizable, that is, $\partial D \in \mathrm{Lip}(n, T, L)$, and let $\Lambda \subset \mathbb{R}^n$ be a full lattice of volume $\mathrm{vol}\,\Lambda$. Then,*

$$|\{\mathbf{x} |\, \mathbf{x} \in \Lambda \cap rD\}| = \frac{\mathrm{vol}\, D}{\mathrm{vol}\,\Lambda} r^n + O(r^{n-1}), \tag{22}$$

where the error term $O(r^{n-1})$ depends on Λ, n, and the Lipschitz constant L.

Using the above lemma, we can now prove the next result.

Proposition 8. *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice with minimal norm λ_1 and volume $\mathrm{vol}\,\Lambda$. Let $\Sigma_\Lambda(r) := \left|\left\{\mathbf{x} \in \Lambda |\, ||\mathbf{x}||^2 \leq r\right\}\right|$, $r \in \mathbb{R}_{>0}$ sufficiently large. Then,*

$$|\Sigma_\Lambda(\lambda_1 r) - \frac{(\pi\lambda_1 r)^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)\mathrm{vol}\,\Lambda}| \leq C(\Lambda, n, L) r^{\frac{n-1}{2}} \tag{23}$$

for some constant $C(\Lambda, n, L)$ that depends on the lattice, dimension, and a Lipschitz constant L.

Proof. We use Lemma 7 with $D_{\lambda_1} := \mathcal{B}_{\mathbf{0}}(\sqrt{\lambda_1})$, a sphere of radius $\sqrt{\lambda_1}$ centered at the origin. Since D_{λ_1} is bounded and convex, by [15, Thm. 2.6] we have $\partial D_{\lambda_1} \in \mathrm{Lip}(n, 1, L)$.

We can now write

$$\Sigma_\Lambda(\lambda_1 r) = \left|\left\{\mathbf{x} \in \Lambda |\, ||\mathbf{x}||^2 \leq \lambda_1 r\right\}\right| \tag{24}$$

$$= \left|\left\{\mathbf{x} \in \left(\Lambda \cap \mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)\right)\right\}\right| \tag{25}$$

$$= \left|\left\{\mathbf{x} \in \Lambda \cap \left(\sqrt{r} D_{\lambda_1}\right)\right\}\right|. \tag{26}$$

Using the relation $\mathrm{vol}\, D_{\lambda_1} = \mathrm{vol}\,\mathcal{B}_{\mathbf{0}}(\sqrt{\lambda_1}) = \frac{(\pi\lambda_1)^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)}$, we have

$$\Sigma_\Lambda(\lambda_1 r) = \frac{(\pi\lambda_1 r)^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)\mathrm{vol}\,\Lambda} + O(r^{\frac{n-1}{2}}), \tag{27}$$

where by Lemma 7, the error term $O(r^{\frac{n-1}{2}})$ is bounded by $C(\Lambda, n, L) r^{\frac{n-1}{2}}$ for some constant $C(\Lambda, n, L)$ that depends on the lattice, dimension, and a Lipschitz constant L. ∎

We can now prove Theorem 4 using the above results.

Proof of Theorem 4. By Proposition 5 we start by writing

$$\Theta_\Lambda(q) = (1 - q^{\lambda_1}) - \log(q)\lambda_1 \int_1^\infty \Sigma_\Lambda(\lambda_1 t) q^{\lambda_1 t} dt. \tag{28}$$

Using the estimate for $\Sigma_\Lambda(r)$ derived in Proposition 8, we can now further manipulate the expression to read

$$\Theta_\Lambda(q) + q^{\lambda_1} - 1 = -\log(q)\lambda_1 \int_1^\infty \Sigma_\Lambda(\lambda_1 t) q^{\lambda_1 t} dt \tag{29}$$

$$= -\log(q)\lambda_1 \int_1^\infty \left(\frac{(\pi\lambda_1 t)^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)\operatorname{vol}\Lambda} + C(\Lambda, n, L) t^{\frac{n-1}{2}} \right) q^{\lambda_1 t} dt \tag{30}$$

$$= -\frac{\log(q)\pi^{\frac{n}{2}}\lambda_1^{\frac{n}{2}+1}}{\Gamma\left(\frac{n}{2}+1\right)\operatorname{vol}\Lambda} \int_1^\infty t^{\frac{n}{2}} q^{\lambda_1 t} dt - C(\Lambda, n, L)\log(q)\lambda_1 \int_1^\infty t^{\frac{n-1}{2}} q^{\lambda_1 t} dt \tag{31}$$

$$= -\frac{\log(q)\pi^{\frac{n}{2}}\lambda_1^{\frac{n}{2}+1}}{\Gamma\left(\frac{n}{2}+1\right)\operatorname{vol}\Lambda} \int_1^\infty t^{\frac{n}{2}} q^{\lambda_1 t} dt + \Xi(\Lambda, n, L, q). \tag{32}$$

■

We will henceforth write $\Theta_\Lambda^{\mathfrak{A}}(q)$ for the approximation $\Theta_\Lambda(q) - \Xi(\Lambda, n, L, q)$. The following corollary will be of use later.

Corollary 9. *Let $\sigma^2 \in \mathbb{R}_{>0}$, and $q(\sigma^2) := e^{-\frac{1}{2\sigma^2}}$. Then, as a function of σ^2, we have*

$$\Theta_\Lambda^{\mathfrak{A}}(q(\sigma^2)) = \left(1 - e^{-\frac{\lambda_1}{2\sigma^2}}\right) + \frac{(\lambda_1\pi)^{\frac{n}{2}}\lambda_1}{2\sigma^2\Gamma\left(\frac{n}{2}+1\right)\operatorname{vol}\Lambda} \int_1^\infty t^{\frac{n}{2}} e^{-\frac{\lambda_1 t}{2\sigma^2}} dt. \tag{33}$$

Let $q = q(\sigma) = e^{-1/2\sigma^2}$. An elementary change of variable $t = \frac{\lambda_1}{2\sigma^2} z$ yields

$$\Gamma\left(\frac{n}{2}+1, x\right) = \left(\frac{\lambda_1}{2\sigma^2}\right)^{\frac{n}{2}+1} \int_{\frac{2\sigma^2 x}{\lambda_1}}^\infty z^{\frac{n}{2}} e^{-\frac{\lambda_1}{2\sigma^2} z} dz.$$

Let $x = \frac{\lambda_1}{2\sigma^2}$. Then

$$\int_1^\infty z^{n/2} e^{-\frac{\lambda_1}{2\sigma^2} z} dz = \left(\frac{2\sigma^2}{\lambda_1}\right)^{\frac{n}{2}+1} \Gamma\left(\frac{n}{2}+1, \frac{\lambda_1}{2\sigma^2}\right). \tag{34}$$

Thus, the approximation in Theorem 4 becomes

$$\Theta(q) = \Theta(e^{-1/2\sigma^2}) = 1 - e^{-\lambda_1/2\sigma^2} + \frac{\left(\sqrt{2\sigma^2\pi}\right)^n}{\operatorname{vol}(\Lambda)} \frac{\Gamma\left(n/2+1, \frac{\lambda_1}{2\sigma^2}\right)}{\Gamma\left(n/2+1, 0\right)} + \Xi = \Theta_\Lambda^{\mathfrak{A}}(q) + \Xi, \tag{35}$$

where $\Xi = \frac{\lambda_1}{2\sigma^2} C(n, \Lambda, L)\Gamma(\frac{n}{2}+\frac{1}{2}, \lambda_1)$.

The following corollary provides a recursive formula for calculating the main term $\Theta_\Lambda^{\mathfrak{A}}(q)$ in Theorem 4 whenever the dimension n is even.

Corollary 10. *Let $q = e^{\frac{-1}{2\sigma^2}}$ and n even. Then $\Theta_\Lambda^{\mathfrak{A}}(q(\sigma))$ in (35) becomes*

$$\Theta_\Lambda^{\mathfrak{A}}(q) = 1 + q^{\lambda_1}\left(-1 + \frac{\pi^{\frac{n}{2}}}{\operatorname{vol}(\Lambda)} \sum_{i=0}^{\frac{n}{2}} \frac{\lambda_1^i 2^{\frac{n}{2}-i}\sigma^{n-2i}}{i!}\right).$$

Proof.

$$\begin{aligned}\Theta_\Lambda^{\mathfrak{A}}(q) &= 1 - q^{\lambda_1} + \frac{\pi^{\frac{n}{2}}}{\mathrm{vol}(\Lambda)}\left(\frac{-1}{\log(q)}\right)^{\frac{n}{2}} q^{\lambda_1}\left(\sum_{i=0}^{\frac{n}{2}} \frac{(-\lambda_1 \log(q))^i}{i!}\right)\\ &= 1 - q^{\lambda_1} + \frac{\pi^{\frac{n}{2}}}{\mathrm{vol}(\Lambda)} 2^{\frac{n}{2}} \sigma^n q^{\lambda_1} \sum_{i=0}^{\frac{n}{2}} \frac{\lambda_1^i}{i! 2^i \sigma^{2i}}\\ &= 1 + q^{\lambda_1}\left(-1 + \frac{\pi^{\frac{n}{2}} 2^{\frac{n}{2}} \sigma^n}{\mathrm{vol}(\Lambda)} \sum_{i=0}^{\frac{n}{2}} \frac{\lambda_1^i}{i! 2^i \sigma^{2i}}\right)\\ &= 1 + q^{\lambda_1}\left(-1 + \frac{\pi^{\frac{n}{2}}}{\mathrm{vol}(\Lambda)} \sum_{i=0}^{\frac{n}{2}} \frac{\lambda_1^i 2^{\frac{n}{2}-i} \sigma^{n-2i}}{i!}\right).\end{aligned}$$

■

3.1. Analysis for the accuracy of $\Theta_\Lambda^{\mathfrak{A}}$. From Corollary 10, we get the following result, showing that $\Theta_\Lambda^{\mathfrak{A}}$ is indeed larger than any truncation of the theta series for values of σ sufficiently large.

Proposition 11. *Let Λ be a lattice of even dimension n, and let j be a positive integer. Then there is a threshold value $\sigma_j \geq 0$ such that $\Theta_\Lambda^{\mathfrak{A}}(q(\sigma)) \geq \Theta_{j,\Lambda}(q(\sigma))$ for all $\sigma \geq \sigma_j$. If the lattice Λ satisfies $(\kappa+1)\,\mathrm{vol}(\Lambda) \leq \lambda_1^{\frac{n}{2}}\,\mathrm{vol}(\mathcal{B}_{\mathbf{0}}(1))$, then $\Theta_\Lambda^{\mathfrak{A}}(q(\sigma)) \geq \Theta_{1,\Lambda}(q(\sigma))$ for all $\sigma \geq 0$.*

Proof. For simplicity, we only present the proof for even n. For odd n, it goes analogously but will look messier due to the more complicated form of the gamma function.

Let λ_i be the ith successive minimum norm of Λ, and let κ_i be the number of vectors in Λ of norm λ_i. By definition, we then have

$$\Theta_{j,\Lambda}(q(\sigma)) = 1 + \sum_{i=1}^{j} q^{\lambda_i}\kappa_i \leq 1 + q^{\lambda_1}\sum_{i=1}^{j}\kappa_i.$$

By Corollary 10, it thus suffices to show that

$$-1 + \frac{\pi^{\frac{n}{2}}}{\mathrm{vol}(\Lambda)} \sum_{i=0}^{\frac{n}{2}} \frac{\lambda_1^i 2^{\frac{n}{2}-i} \sigma^{n-2i}}{i!} \geq \sum_{i=1}^{j}\kappa_i \tag{36}$$

for large enough σ. But the left-hand side (lhs) of (36) is a continuous and strictly increasing function in $\sigma \geq 0$ and tends to infinity as $\sigma \to \infty$. As $\sum_{i=1}^{j}\kappa_i$ is constant, the inequality (36) holds for all large enough σ.

To prove the second part of the theorem, it is now enough to show that (36) holds for $\sigma = 0$, $j = 0$. But when $\sigma = 0$, the only nonvanishing term in the sum is when $i = \frac{n}{2}$, so (36) is equivalent to

$$\frac{\pi^{\frac{n}{2}}\lambda_1^{\frac{n}{2}}}{\mathrm{vol}(\Lambda)\frac{n}{2}!} \geq \kappa + 1.$$

Observing that

$$(\kappa+1)\operatorname{vol}(\Lambda) \le \lambda_1^{\frac{n}{2}} \operatorname{vol}(\mathcal{B}_{\mathbf{0}}(1))) = \frac{\pi^{\frac{n}{2}}}{\frac{n}{2}!},$$

the statement of the proposition follows. ∎

It is worth noting that there is a nice geometric interpretation of the above inequality,

$$(\kappa+1)\operatorname{vol}(\Lambda) \le \lambda_1^{\frac{n}{2}} \operatorname{vol}(\mathcal{B}_{\mathbf{0}}(1)). \tag{37}$$

Namely, the rhs of (37) is the volume of the ball centered around the origin with the shortest vectors of Λ on its boundary. The lhs of (37) is the volume of the union of the $\kappa+1$ Voronoi cells centered at the origin and at the shortest vectors of Λ. Depending on which of these volumes is the largest, the inequality $\Theta_\Lambda^{\mathfrak{A}} \ge \Theta_1$ holds either for all q or only for large enough q.

To prove that the approximation $\Theta_\Lambda^{\mathfrak{A}}$ is indeed closer to the actual theta function Θ than the jth truncation Θ_j for $\sigma > \sigma_j$, it would be enough to show that $\Theta_\Lambda^{\mathfrak{A}}(q) \le \Theta_\Lambda(q)$ holds for all lattices Λ and all $0 \le q < 1$. While this inequality holds for all lattices for which we can do explicit calculations, we are not able to prove it in full generality. However, it holds on average in the sense of the following theorem.

Theorem 12. *Let Λ be a random lattice with distribution given by the Haar measure on $\mathrm{SL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{Z})$. Then, for every $0 \le q < 1$, it holds that*

$$\mathbb{E}[\Theta_\Lambda^{\mathfrak{A}}(q)] \le \mathbb{E}[\Theta_\Lambda(q)].$$

Proof. A straightforward application of Siegel's mean value theorem [8] implies that for any $t > 0$, we have

$$\mathbb{E}(\Sigma_\Lambda(t)) = 1 + \operatorname{vol}(\mathcal{B}_{\mathbf{0}}(t)),$$

where $\mathcal{B}_{\mathbf{0}}(1)$ is the Euclidean ball of radius r. For any fixed lattice Λ, we can thus write

$$\Theta_\Lambda^{\mathfrak{A}}(q) = (1-q^\ell) - \log q \int_\ell^\infty q^t \mathbb{E}[\Sigma_\Lambda(t) - 1]dt \tag{38}$$

$$= -\log q \int_0^\ell q^t dt - \log q \int_\ell^\infty q^t \mathbb{E}[\Sigma_\Lambda(t) - 1]dt \tag{39}$$

$$= -\log q \int_0^\infty q^t \left(I_{t\le\ell} + I_{t>\ell}\mathbb{E}[\Sigma_\Lambda(t) - 1]\right) dt, \tag{40}$$

where ℓ is the (deterministic) shortest norm of Λ, and I_E denotes the indicator function of the event E. Observing that

$$\Theta_\Lambda(q) = -\log(q) \int_0^\infty \Sigma_\Lambda(t) q^t dt,$$

we get by linearity of the expectation and by Fubini's theorem that

$$\begin{aligned}
\mathbb{E}[\Theta_\Lambda(q)] - \mathbb{E}[\Theta_\Lambda^{\mathfrak{A}}(q)] &= -\log q\, \mathbb{E}\left[\int_0^\infty \Sigma_\Lambda(t) q^t dt - \int_0^\infty q^t \left(I_{t\le\lambda} + I_{t>\lambda}\mathbb{E}\left[\Sigma_\Lambda(t) - 1\right]\right) dt\right] \\
&= -\log q \int_0^\infty q^t \mathbb{E}\left[\Sigma_\Lambda(t) - \left(I_{t\le\lambda} + I_{t>\lambda}(\mathbb{E}(\Sigma_\Lambda(t)) - 1)\right)\right] dt \\
&= -\log q \int_0^\infty q^t \mathbb{E}\left[\mathbb{E}\left[\Sigma_\Lambda(t)\right] - \left(I_{t\le\lambda} + I_{t>\lambda}(\mathbb{E}(\Sigma_\Lambda(t)) - 1)\right)\right] dt \\
&= -\log q \int_0^\infty q^t \left(\mathbb{E}\left[\mathbb{E}\left[\Sigma_\Lambda(t)\right](1 - I_{t>\lambda})\right] - \mathbb{E}\left[I_{t\le\lambda} - I_{t>\lambda}\right]\right) dt \\
&= -\log q \int_0^\infty q^t \left(\mathbb{E}\left[\Sigma_\Lambda(t)\right]\mathbb{P}[t \le \lambda] - \mathbb{P}[t \le \lambda] + \mathbb{P}[t > \lambda]\right) dt \\
&= -\log q \int_0^\infty q^t (\mathbb{P}[t \le \lambda]\mathbb{E}\left[\Sigma_\Lambda(t) - 1\right] + \mathbb{P}[t > \lambda]) dt,
\end{aligned}$$

where λ is the (random) shortest norm of Λ. The integrand is now readily seen to be a nonnegative real function, wherefore we get

$$\mathbb{E}[\Theta_\Lambda(q)] \ge \mathbb{E}[\Theta_\Lambda^{\mathfrak{A}}(q)]. \qquad \blacksquare$$

3.2. Error term analysis for the point counting function. The proof of Theorem 4 relied on an estimate (Proposition 8) of the number of lattice points in $\mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)$. For the sake of completeness, we sketch an alternative proof of Proposition 8 with a slightly different error term.

Let $\Lambda = M \cdot \mathbb{Z}^n$ for some $M \in \mathrm{GL}_n(\mathbb{R})$. Then

$$\Sigma_\Lambda(\lambda_1 r) = \left|M \cdot \mathbb{Z}^n \cap \mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)\right| \tag{41}$$

$$= \left|\mathbb{Z}^n \cap M^{-1}\mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)\right|, \tag{42}$$

where $M^{-1}\mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right) = \left\{M^{-1}\mathbf{x} \ : \ \mathbf{x} \in \mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)\right\}$.

Consider the tiling of $\mathbb{R}^n$ with unit cubes centered at the points of $\mathbb{Z}^n$. We interpret $\Sigma_\Lambda(\lambda_1 r)$ as the number of unit cubes in this tiling with centers lying inside $M^{-1}\mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)$. Hence,

$$\Sigma_\Lambda(\lambda_1 r) = \mathrm{vol}\left(M^{-1}\mathcal{B}_{\mathbf{0}}\left(\sqrt{\lambda_1 r}\right)\right) + \mathcal{E}_\Lambda(\sqrt{\lambda_1 r}) \tag{43}$$

$$= \frac{(\pi\lambda_1 r)^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)\mathrm{vol}\,\Lambda} + \mathcal{E}_\Lambda(\sqrt{\lambda_1 r}), \tag{44}$$

where $\mathcal{E}_\Lambda(\sqrt{\lambda_1 r})$ is bounded by the volumes of cubes that intersect the boundary $\partial M^{-1}\mathcal{B}_{\mathbf{0}}(\sqrt{\lambda_1 r})$. This volume is proportional to the (Hausdorff) surface measure of $M^{-1}\mathcal{B}_{\mathbf{0}}(\sqrt{\lambda_1 r})$. Thus, for r large enough, the dominant term in $\Sigma_\Lambda(\lambda_1 r)$ is $\mathrm{vol}(M^{-1}\mathcal{B}_{\mathbf{0}}(\sqrt{\lambda_1 r}))$.

Let

$$\Sigma_\Lambda(t) = \mathrm{vol}\left(M^{-1}\mathcal{B}_{\mathbf{0}}\left(\sqrt{t}\right)\right) + \mathcal{E}_\Lambda(\sqrt{t}).$$

In the following, we will consider the order of magnitude of $\mathcal{E}_\Lambda(\sqrt{t})$ and its relation with the error term in Theorem 4.

Let C be a positive constant, f a real valued (integrable) function, and t_0 a positive real number such that

$$|\mathcal{E}_\Lambda(\sqrt{t})| < Cf(t) \text{ for all } t \geq t_0,$$

i.e., $\mathcal{E}_\Lambda(\sqrt{t}) = O(f(t))$.

With the notation above, we rewrite the error term in Theorem 4 in the following form:

$$\Xi(\Lambda, n, q) = O\left(\log(q)\lambda_1 \int_1^\infty f(\lambda_1 r) q^{\lambda_1 r} dr\right) \tag{45}$$

$$= O\left(\log(q) \int_{\lambda_1}^\infty f(t) q^t dt\right) \tag{46}$$

$$\leq O\left(\log(q) \int_{\lambda_1}^{t_0} f(t) q^t dt\right) + C\log(q) \int_{t_0}^\infty f(t) q^t dt. \tag{47}$$

Note that in the proof of Theorem 4 we implicitly assume that $t \geq \lambda_1$. Thus, $t_0 \geq \lambda_1$. Equation (45) shows that any improvement on the order of magnitude of $\mathcal{E}_\Lambda(\sqrt{\lambda_1 r})$ will necessarily imply an improved error term $\Xi(\Lambda, n, q)$.

Remark 3. With this new interpretation of $\Sigma_\Lambda(t)$, the main term in Theorem 4 remains the same, but the term $\Xi(\Lambda, n, q)$ depends on λ_1 rather than the Lipschitz constant L.

In [9], Götze showed that $\mathcal{E}_\Lambda(\sqrt{t}) = O(t^{\frac{n-2}{2}})$ for every lattice $\Lambda \subset \mathbb{R}^n$ with $n \geq 5$. This bound is tight in the sense that $\mathcal{E}_\Lambda(\sqrt{t}) \neq o(t^{\frac{n-2}{2}})$ for $\Lambda = \mathbb{Z}^n$.

Assuming that $n \geq 5$, we get

$$\Xi(\Lambda, n, q) \leq O\left(\log(q) \int_{\lambda_1}^{t_0} t^{\frac{n-2}{2}} q^t dt\right) + C\log(q) \int_{t_0}^\infty t^{\frac{n-2}{2}} q^t dt. \tag{48}$$

Let $q = e^{\frac{-1}{2\sigma^2}}$. Then inequality (48) becomes

$$\Xi\left(\Lambda, n, e^{\frac{-1}{2\sigma^2}}\right) \leq O\left(\log(q) \int_{\lambda_1}^{t_0} t^{\frac{n-2}{2}} q^t dt\right) - \frac{C}{2\sigma^2} \int_{t_0}^\infty t^{\frac{n-2}{2}} e^{-\frac{t}{2\sigma^2}} dt. \tag{49}$$

Thus, using the same argument as in (34) we get

$$\Xi\left(\Lambda, n, e^{\frac{-1}{2\sigma^2}}\right) = O\left((2\sigma^2)^{\frac{n}{2}-1} \Gamma\left(\frac{n}{2}, \frac{t_0}{2\sigma^2}\right)\right). \tag{50}$$

Finally, we write the approximation in Theorem 4 as

$$\Theta\left(e^{-1/2\sigma^2}\right) - 1 + e^{-\lambda_1/2\sigma^2} = \frac{\left(\sqrt{2\sigma^2\pi}\right)^n}{\text{vol}(\Lambda)} \frac{\Gamma\left(n/2+1, \frac{\lambda_1}{2\sigma^2}\right)}{\Gamma\left(n/2+1, 0\right)} + \Xi\left(\Lambda, n, e^{\frac{-1}{2\sigma^2}}\right). \tag{51}$$

Using integration by parts, one can prove that the incomplete gamma function satisfies the following recurrence relation:

$$\Gamma\left(\frac{n}{2}+1, \frac{\lambda_1}{2\sigma^2}\right) = \frac{n}{2}\Gamma\left(\frac{n}{2}, \frac{\lambda_1}{2\sigma^2}\right) + \left(\frac{\lambda_1}{2\sigma^2}\right)^{\frac{n}{2}} e^{-\frac{\lambda_1}{2\sigma^2}}. \tag{52}$$

Assume, for instance, that $t_0 = \lambda_1$; then using (52), the ratio of the main and error terms in (51) is

$$\mathcal{R} = \frac{\left(\sqrt{2\sigma^2\pi}\right)^n}{\mathrm{vol}(\Lambda)} \frac{\Gamma\left(n/2+1, \frac{\lambda_1}{2\sigma^2}\right)}{\Gamma\left(n/2+1, 0\right)} \times \frac{1}{\left((2\sigma^2)^{\frac{n}{2}-1}\Gamma\left(\frac{n}{2}, \frac{t_0}{2\sigma^2}\right)\right)} \tag{53}$$

$$= n\sigma^2 \frac{\mathrm{vol}(\mathcal{B}_0(1))}{\mathrm{vol}(\Lambda)} + h(\lambda_1, n, \sigma), \tag{54}$$

where $h(\lambda_1, n, \sigma)$ is a positive constant depending on n, λ_1, and σ.

The last equality shows that under the above assumptions, the ratio $\mathcal{R}$ is greater than one whenever $\sigma > \sqrt{\frac{\mathrm{vol}(\Lambda)}{n\,\mathrm{vol}(\mathcal{B}_0(1))}}$.

As a last part of this section, we mention further results on the magnitude of $\mathcal{E}_\Lambda(\sqrt{t})$.

Let $\mathcal{L}_n$ be the set of determinant 1 lattices with Haar measure μ_n. We call a random variable sampled from $\mathcal{L}_n$ with respect to μ_n a random lattice.

Let $\delta > 0$ be a small arbitrary constant. Schmidt [17] proved that $\mathcal{E}_\Lambda(\sqrt{t}) = O(t^{\frac{n}{4}+\delta})$ for almost every lattice.

It is conjectured [7] that $\mathcal{E}_\Lambda(\sqrt{t}) = O(t^{\frac{n-1}{4}+\delta/2})$. In [11], the author showed that the bound $\mathcal{E}_\Lambda(\sqrt{t}) = O(t^{\frac{n-1}{4}+\delta/2})$ holds in average for lattices of dimensions $n = 2, 3$, where the average is taken over any compact subset Y of the space of all lattices (not necessarily of volume 1).

In the following, we will give an example of a compact subset of $\mathcal{L}_n$. Compact subsets of $\mathcal{L}_n$ can be obtained by the so-called Mahler's compactness criterion.

Theorem 13 (Mahler). *The set of lattices $\Lambda \in \mathcal{L}_n$ whose shortest vector is of a fixed length $\geq r > 0$ is compact.*

Definition 14. *A lattice $\Lambda \subset \mathbb{R}^n$ is* well-rounded *(abbreviated WR) if*

$$\mathrm{span}_{\mathbb{R}}(S(L)) = \mathbb{R}^n.$$

We denote by $\mathcal{WR}_n$ the set of well-rounded lattices in $\mathcal{L}_n$.

Proposition 15. *The set $\mathcal{WR}_n$ is compact in $\mathcal{L}_n$.*

Proof. Let Λ be a lattice in $\mathcal{WR}_n$, and let $v_i \in \Lambda$ such that $||v_i|| = \lambda_i(\Lambda)$ for $1 \leq i \leq n$. Taking $\Lambda' = \mathrm{span}_{\mathbb{Z}}(v_i \mid 1 \leq i \leq n)$, then Λ' is a full-rank sublattice of Λ. Hence, $\mathrm{vol}(\Lambda') = [\Lambda : \Lambda'] \geq 1$.

On the other hand

$$\prod_{i=1}^{n} ||v_i|| = \prod_{i=1}^{n} \lambda_i(\Lambda) = \lambda_1(\Lambda)^n.$$

Recalling the Hadamard's inequality $\prod_{i=1}^{n} ||v_i|| \geq \mathrm{vol}(\Lambda')$, we conclude that

$$\lambda_1(\Lambda) \geq 1.$$

The result follows from Mahler's compactness criterion. ∎

Combining Proposition 15 with the main result in [11], we get the following result.

Proposition 16. *The bound*

$$\Xi\left(\Lambda, n, e^{\frac{-1}{2\sigma^2}}\right) = O\left((2\sigma^2)^{\frac{n-5}{4}+\delta/2}\Gamma\left(\frac{n-1}{4}+\delta/2, \frac{t_0}{2\sigma^2}\right)\right)$$

holds on average over $\mathcal{WR}_2$ *and* $\mathcal{WR}_3$.

Landau [25] proved that $\mathcal{E}_\Lambda(\sqrt{t}) \neq o(t^{\frac{n-1}{4}})$ for any lattice of dimension $n \geq 3$. Consequently, for $n \geq 3$ we have

$$\Xi\left(\Lambda, n, e^{\frac{-1}{2\sigma^2}}\right) \neq o\left((2\sigma^2)^{\frac{n-5}{4}+}\Gamma\left(\frac{n-1}{4}, \frac{t_0}{2\sigma^2}\right)\right).$$

Proposition 16 shows that heuristically, the error term in Theorem 4 achieves the conjectured bound over the sets $\mathcal{WR}_2$ and $\mathcal{WR}_3$.

In the next section, we analyze the accuracy of our approximation for some well-rounded lattices, i.e., $\mathbb{Z}^2$, D_3, D_4, E_8, and K_{12}. In fact, most of the known lattices are well-rounded. To name just a few, we mention the local maxima of the sphere packing problem, the lattices D_n, A_n, and the orthogonal lattice $\mathbb{Z}^n$.

3.3. Empirical study and discussion. We first depict the accuracy of the approximation $\Theta_\Lambda^{\mathfrak{A}}(q)$ for some of the well-known lattices tabulated in Table 1. We choose $q = e^{-\frac{1}{2\sigma^2}}$ and interpret $\Theta_\Lambda^{\mathfrak{A}}(e^{-\frac{1}{2\sigma^2}})$ as a function in the variable σ^2. The choice of this specific indeterminate q will be clarified in the subsequent sections of this article.

From Figure 2 it is visible that the approximation is accurate in the considered cases, even as the dimension increases. A naive way of approximating the theta series is by simply considering the first term in the power series expression, that is, $\Theta_\Lambda(q) \approx 1 + \kappa(\Lambda)q^{\lambda_1}$. In Figure 3, we compare the derived approximation $\Theta_\Lambda^{\mathfrak{A}}(q)$ with this truncated sum on the Leech lattice Λ_{24}. While our approximation accurately approximates the theta series $\Theta_{\Lambda_{24}}(q)$, the truncated sum very quickly diverges from the actual function, as is to be expected.

Remark 4. The error term in the expression from Theorem 4 arises from the estimation of lattice points in an n-sphere, *i.e.*, the estimation of $\Sigma_\Lambda(r)$. In its full generality, this is a

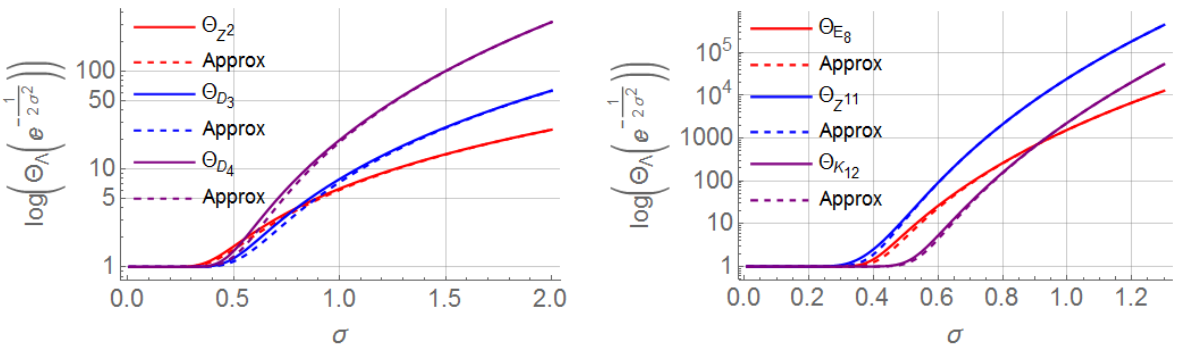

Figure 2. *Comparison of the theta function of various lattices and the derived approximation. The lhs picture depicts the theta series of low-dimensional, the rhs picture higher-dimensional lattices as a function of* σ^2.

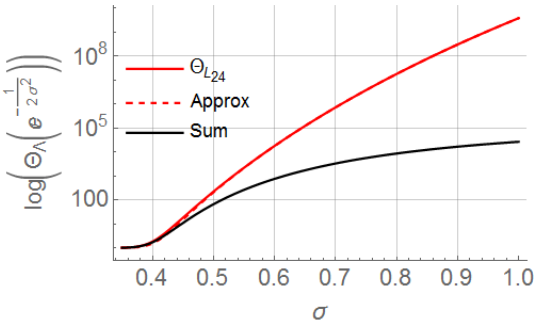

Figure 3. *Comparison of* $\Theta_\Lambda^{\mathfrak{A}}(q)$ *and a truncated sum* $1+\kappa(\Lambda)q^{\lambda_1}$ *of the Leech lattice* $\Lambda = L_{24}$.

hard problem. For instance, the original proof of Lemma 7 in [19] is not constructive and does not offer any insight into the involved constant. Accurately counting lattice points in more general domains is a topic of the utmost interest in lattice theory. In [18], an upper bound on the quantity $|\Lambda \cap P|$, where $\Lambda \subset \mathbb{R}^n$ is a full lattice and $P \subset \mathbb{R}^n$ an arbitrary polytope of dimension $n' \leq n$, is given. Further, [15] gives an upper bound on $|\Lambda \cap S|$, where $S \subset \mathbb{R}^n$ is a bounded domain, of general *narrow class* $s \geq 1$. Both mentioned results are, however, so general that the upper bounds are not tight, even for low-dimensional, well-conditioned lattices.

3.4. The flatness factor. Having introduced the theta series $\Theta_\Lambda(q)$ of a lattice, we now define a related quantity—the flatness factor $\varepsilon_\Lambda(q)$ of Λ. Consider the usual n-dimensional zero-mean Gaussian PDF with variance σ^2, given by

$$f(\mathbf{t}, \sigma^2) = \frac{1}{(\sqrt{2\pi\sigma^2})^n} e^{-\frac{||\mathbf{t}||^2}{2\sigma^2}}. \tag{55}$$

We are interested in the case where the variable $\mathbf{t}$ ranges over points over a (possibly shifted) full lattice Λ, yielding for $\mathbf{y} \in \mathbb{R}^n$ the sum of Gaussian functions

$$f(\Lambda + \mathbf{y}, \sigma^2) := \sum_{\mathbf{x}\in\Lambda} f(\mathbf{x} + \mathbf{y}, \sigma^2). \tag{56}$$

As a function of $\mathbf{y}$, $f(\Lambda + \mathbf{y}, \sigma^2)$ is a Λ-periodic function and defines a PDF on the basic Voronoi cell $\mathcal{V}(\Lambda)$ of Λ, which we refer to as the *lattice Gaussian PDF*. For the centered sum $f(\Lambda, \sigma^2)$, we have the useful identity

$$f(\Lambda, \sigma^2) = \sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}, \sigma^2) = \frac{1}{(\sqrt{2\pi\sigma^2})^n} \sum_{\mathbf{x}\in\Lambda} e^{-\frac{||\mathbf{x}||^2}{2\sigma^2}} \tag{57}$$

$$= \frac{1}{(\sqrt{2\pi\sigma^2})^n} \Theta_\Lambda\left(e^{-\frac{1}{2\sigma^2}}\right). \tag{58}$$

Introduced in [1] as an information theoretic tool in the context of fading wiretap channels, the *flatness factor* is a quantity which measures the deviation of the lattice Gaussian PDF from the uniform distribution on the Voronoi cell $\mathcal{V}(\Lambda)$. Formally, it can be defined as follows.

Definition 17. *Let $\Lambda \subset \mathbb{R}^n$ be a full lattice, and for $\mathbf{y} \in \mathbb{R}^n$, let $f(\Lambda + \mathbf{y}, \sigma^2)$ denote the lattice Gaussian PDF of the lattice $\Lambda + \mathbf{y}$. The* flatness factor *of Λ is defined as*

$$\varepsilon_\Lambda(\sigma^2) := \max_{\mathbf{y}\in\mathbb{R}^n} \left| \frac{f(\Lambda+\mathbf{y},\sigma^2)}{1/\operatorname{vol}\Lambda} - 1 \right|. \tag{59}$$

It is easy to show (see [20]) that the maximum of $f(\Lambda + \mathbf{y}, \sigma^2)$ is achieved for $\mathbf{y} \in \Lambda$. Hence, an explicit representation of $\varepsilon_\Lambda(\sigma^2)$ is immediate,

$$\varepsilon_\Lambda(\sigma^2) = \frac{\operatorname{vol}\Lambda}{(\sqrt{2\pi\sigma^2})^n}\Theta_\Lambda\left(e^{-\frac{1}{2\sigma^2}}\right) - 1. \tag{60}$$

If we define the *volume-to-noise ratio*[1] (VNR) $\gamma_\Lambda(\sigma^2) := \frac{\operatorname{vol}\Lambda^{\frac{2}{n}}}{2\pi\sigma^2}$, then we can equivalently express the flatness factor as [6]

$$\varepsilon_\Lambda(\sigma^2) = \gamma_\Lambda(\sigma^2)^{\frac{n}{2}}\Theta_\Lambda\left(e^{-\frac{1}{2\sigma^2}}\right) - 1. \tag{61}$$

From the definition of the flatness factor, it is clear that a small flatness factor implies a more uniform distribution.

4. Theta series and the compute-and-forward relaying strategy. In this section, we consider a protocol known as *compute-and-forward* relaying [4]. This protocol was proposed to harness the interference in an advantageous way. Namely, in wireless communications, a single transmission is heard by all near-enough receivers. Similarly, a receiver will hear all signals transmitted in the vicinity, not only the signals intended for them. This is referred to as interference, which degrades the reception quality. Several protocols have been proposed in the literature to remedy this degradation. The most prominent ones are *decode-and-forward, compress-and-forward*, and *amplify-and-forward*. For more details on these protocols, we refer to [4] and references therein. The compute-and-forward strategy simultaneously aims at protection against noise and exploitation of interference for cooperative gains. In contrast to compress-and-forward and amplify-and-forward, which can be seen as converting a network into a set of *noisy* linear equations, the compute-and-forward converts it into a set of *reliable* linear equations. The compute-and-forward protocol has been shown to be superior at moderate signal quality levels, where both noise and interference play a nonnegligible role.

Analyzing the ML metric in the compute-and-forward context, we show how the flatness factor of a certain lattice enters the picture [6], and we relate this random lattice to the code lattice at the transmitter. We then utilize the derived theta series approximation to analyze the performance of various lattices with respect to an explicit design criterion. Namely, we show that in order to maximize the flatness factor of the random lattice, it suffices to maximize that of the code lattice.

In this article we will only consider real valued channels, which are also studied in the original article [4] and additionally assumed in [6, 10]. We refer to [4] for the complex alternative.[2] Assume that $K > 1$ transmitters want to communicate to a single destination, aided

[1] The VNR is usually defined without the term 2π in the denominator. Here, the definition is chosen to agree with [6].

[2] As shown in [4], a complex channel output can be treated as two separate real equations.

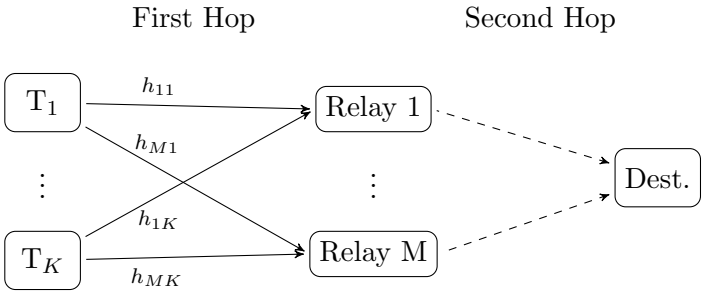

Figure 4. *System model with $K > 1$ transmitters and $M > K$ relays connected to a destination.*

by M intermediate relays which, operating under the original compute-and-forward strategy, attempt to decode an integer linear combination of the transmitted messages. We assume that each user, relay, and destination is equipped with one antenna only. The model is depicted in Figure 4.

The first hop from the transmitters to the relays is modeled as a Gaussian fading channel, while it is usually assumed that the relays are connected to a destination with error-free bit pipes with unlimited capacities. We will henceforth focus on the first hop.

The sources want to communicate messages $\mathbf{w}_k \in \mathbb{F}_p^s$ to the destination, which are encoded into n-dimensional codewords $\mathbf{x}_k \in \Lambda_{k,F} \subset \mathbb{R}^n$ before transmission. Here, $\Lambda_{k,F}$ is a full-rank lattice employed by transmitter k, acting as the fine lattice in the nested code $\mathcal{C}_k(\Lambda_C, \Lambda_{k,F}) = \{[\mathbf{x}] \in \Lambda_{k,F} \,(\mathrm{mod}\ \Lambda_C) \mid \mathbf{x} \in \Lambda_{k,F}\}$. We impose the usual symmetric power constraint $\frac{1}{n}E\left[||\mathbf{x}_k||^2\right] \leq P$ for all k. We can interpret the coarse lattice Λ_C as the structure imposing the power constraint on the codewords, which allows us to ignore the specific definition of Λ_C in the remainder of this section. The observed signal at relay m can be expressed as

$$\mathbf{y}_m = \sum_{k=1}^{K} h_{mk}\mathbf{x}_k + \mathbf{n}_m, \tag{62}$$

where $\mathbf{n}_m$ is additive white Gaussian noise with variance σ^2, and the channel coefficients h_{mk} are independent and identically distributed with normalized unit variance $\sigma_h^2 = 1$. Here, the *signal-to-noise ratio* (SNR) is $\rho = P/\sigma^2$. The compute-and-forward strategy involves transforming the above random linear combination into a deterministic one and treating the rest of the equation as noise. We will describe this process next, leading to (63).

Channel state information is available only at the relays; more specifically, each relay only knows the channel $\mathbf{h}_m^t = (h_{m1}, \ldots, h_{mK})$ to itself. Operating under the original compute-and-forward protocol, a fixed relay selects a scalar $\alpha_m \in \mathbb{R}$, as well as an integer vector $\mathbf{a}_m^t = (a_{m1}, \ldots, a_{mK})$, and attempts to decode a linear combination of the received codewords with coefficients a_{mk}. For $\tilde{\mathbf{y}}_m := \alpha_m \mathbf{y}_m$, the channel output is modified to read

$$\tilde{\mathbf{y}}_m = \sum_{k=1}^{K} a_{mk}\mathbf{x}_k + \sum_{k=1}^{K} (\alpha_m h_{mk} - a_{mk})\mathbf{x}_k + \alpha_m \mathbf{n}_m. \tag{63}$$

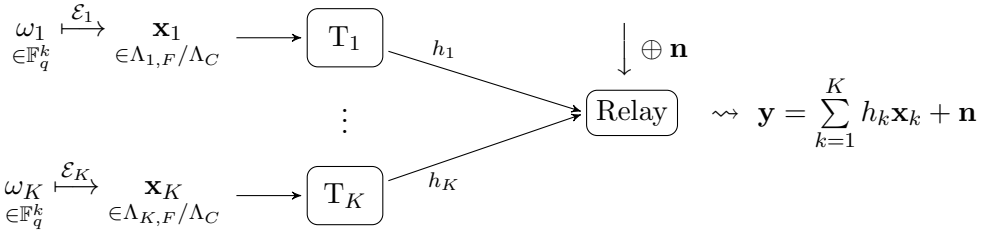

Figure 5. *System model focused on the first hop, with $K > 1$ transmitters and a fixed relay.*

The so-called effective noise

$$\mathbf{n}_{\text{eff}} := \sum_{k=1}^{K} (\alpha_m h_{mk} - a_{mk})\mathbf{x}_k + \alpha_m \mathbf{n}_m \tag{64}$$

is no longer Gaussian.

Upon observing the faded superposition of transmitted codewords, each relay proceeds in the same fashion in order to decode a linear combination. We can hence focus on a single relay and, for ease of notation, drop the subscript m henceforth. The focused system model, now resembling a K-user multiple-access channel, is illustrated in Figure 5.

An important performance metric of the compute-and-forward protocol is the so-called computation rate. If $\mathcal{R}_M(k) = \frac{s}{n} \log p$ denotes the *message rate* at transmitter k, then the relay is able to decode a linear combination involving the codewords whose corresponding message rates are smaller than the computation rate $\mathcal{R}_C(\mathbf{h}, \mathbf{a})$ achieved by the relay, that is, which satisfy $\mathcal{R}_M \leq \mathcal{R}_C$. The main results on the computation rate are briefly summarized below.

Lemma 18 (see [4, 21]). *For a relay employing the original compute-and-forward strategy under a real valued channel model, the computation rate region is maximized by choosing α as the minimum mean square error estimate*

$$\alpha_{\text{MMSE}} = \frac{\rho \mathbf{h}^t \mathbf{a}}{1 + \rho ||\mathbf{h}||^2}, \tag{65}$$

resulting in the computation rate region

$$\mathcal{R}_C(\mathbf{h}, \mathbf{a}) = \frac{1}{2} \log^+ \left(\left(||\mathbf{a}||^2 - \frac{\rho (\mathbf{h}^t \mathbf{a})^2}{1 + \rho ||\mathbf{h}||^2} \right)^{-1} \right). \tag{66}$$

Moreover, the optimal coefficient vector is the solution to the minimization problem

$$\mathbf{a}_{\text{opt}} = \underset{\mathbf{a} \in \mathbb{Z}^K \setminus \{\mathbf{0}\}}{\arg\min}\ \mathbf{a}^t G \mathbf{a}, \tag{67}$$

where $G = I_K - \frac{\rho \mathbf{h}\mathbf{h}^t}{1+\rho||\mathbf{h}||^2}$. Hence, $\mathbf{a}_{\text{opt}}$ corresponds to the coefficient vector of the shortest vector in the lattice with Gram matrix G.

Remark 5. The lattice shortest vector problem is in general a computationally hard problem. However, it has been shown recently that in certain instances in the context of compute-and-forward, e.g., for solving (67), it can be solved in polynomial time [22].

A low-complexity approach assuming no cooperation between the relays has also been proposed in [23].

4.1. Decoding linear equations. For each k, let $\mathcal{C}_k := \mathcal{C}_k(\Lambda_C, \Lambda_{k,F})$ denote the nested lattice code employed by transmitter k. Assume that the fine lattices, possibly after reordering the indexes, are nested, $\Lambda_{1,F} \supseteq \Lambda_{2,F} \supseteq \cdots \supseteq \Lambda_{K,F}$. Since the codebook is finite for each transmitter, the codewords can be assumed to be equiprobable in $\mathcal{C}_k$.

A relay attempts to decode

$$\mathbf{y} = \sum_{k=1}^{K} h_k \mathbf{x}_k + \mathbf{n}$$

to a lattice point

$$[\lambda] = \sum_{k=1}^{K} a_k \mathbf{x}_k \pmod{\Lambda_C}$$

in two steps:

(i) Scale the received signal by a scalar α, compute an equation coefficient vector $\mathbf{a}^t = (a_1, \ldots, a_K)$ by solving (67), and decode an estimate $\hat{\lambda}$ of

$$\lambda = \sum_{k=1}^{K} a_k \mathbf{x}_k \in \Lambda_F := \sum_{k=1}^{K} a_k \Lambda_{k,F}. \tag{68}$$

(ii) Apply the modulo-lattice operation to shift the received signal back into $\mathcal{V}(\Lambda_C)$,

$$[\lambda] = \lambda \pmod{\Lambda_C}. \tag{69}$$

The requirement $\Lambda_{1,F} \supseteq \Lambda_{2,F} \cdots \supseteq \Lambda_{K,F}$ guarantees[3] that

$$\Lambda_F = \sum_{k=1}^{K} a_k \Lambda_{k,F} \tag{70}$$

is a lattice. The crucial step is the first one, estimating $\hat{\lambda} \in \Lambda_F$. Originally, a nearest neighbor decoder is used for this estimation. As this method is optimal only at high SNR, we employ ML decoding at the relay instead.

4.2. The ML decoding metric. Let $\Lambda_F = \sum_{k=1}^{K} a_k \Lambda_k$ be the lattice defined above. By the imposed norm constraint on the codewords, the desired lattice point $\lambda = \sum_{k=1}^{K} a_k \mathbf{x}_k$ is contained in a finite subset $L_F \subset \Lambda_F$, which is determined by the norm restriction of the original codewords as well as the coefficient vector $\mathbf{a}$. Thus, a relay can restrict its search space to L_F. We make this more precise in the following straightforward proposition.

[3]Note that nesting is not necessary, but sufficient; more generally, it suffices to fix a common superlattice for all transmitters. We adopt the nested assumption to be consistent with [4].

Proposition 19. *For a fixed coefficient vector* $\mathbf{a}^t = (a_1, \dots, a_K)$*, the lattice point* λ *is contained in the set*

$$L_F = \left\{ \lambda \in \Lambda_{k_{\min},F} \,\middle|\, ||\lambda|| \leq \sum_{k=1}^{K} |a_k| \max_{\mathbf{x} \in \mathcal{C}_{k_{\min}}} \{||\mathbf{x}||\} \right\}, \tag{71}$$

where $k_{\min} := \arg\min_{1 \leq k \leq K} \{a_k \neq 0\}$.

Proof. By definition, $k_{\min}$ is the index of the first nonzero entry in the coefficient vector $\mathbf{a}$, hence the index of the first codeword to be included in the targeted linear combination. As $\Lambda_{1,F} \supseteq \cdots \supseteq \Lambda_{K,F}$, we have that $\mathbf{x}_k \in \mathcal{C}_{k_{\min}}$ for all $k \geq k_{\min}$. Consequently, each of the codewords involved in the linear combination satisfies $||\mathbf{x}_k|| \leq \max_{\mathbf{x} \in \mathcal{C}_{k_{\min}}} \{||\mathbf{x}||\}$. We conclude

$$||\lambda|| = \left|\left| \sum_{k=1}^{K} a_k \mathbf{x}_k \right|\right| \leq \sum_{k=1}^{K} |a_k| ||\mathbf{x}_k|| \tag{72}$$

$$\leq \sum_{k=1}^{K} |a_k| \max_{\mathbf{x} \in \mathcal{C}_{k_{\min}}} \{||\mathbf{x}||\}. \tag{73}$$

■

In this context, ML decoding amounts to maximizing the conditional probability

$$\hat{\lambda} = \arg\max_{\lambda \in L_F} \mathbb{P}\left[\alpha \mathbf{y} \mid \lambda\right] \tag{74}$$

$$= \arg\max_{\lambda \in L_F} \sum_{\substack{(\mathbf{x}_i)_i \in (\mathcal{C}_i)_i \\ \sum_{k=1}^{K} a_k \mathbf{x}_k = \lambda}} \mathbb{P}\left[\alpha \mathbf{y} | (\mathbf{x}_1, \dots, \mathbf{x}_K)\right] \mathbb{P}\left[(\mathbf{x}_1, \dots, \mathbf{x}_K)\right]. \tag{75}$$

The former factor in the above expression behaves as

$$\mathbb{P}\left[\alpha \mathbf{y} | (\mathbf{x}_1, \dots, \mathbf{x}_K)\right] \propto \exp\left\{ -\frac{1}{2\sigma^2} \left|\left| \mathbf{y} - \sum_{k=1}^{K} h_k \mathbf{x}_k \right|\right|^2 \right\}. \tag{76}$$

Note that this is independent of α. We define the function

$$\varphi(\lambda) := \sum_{\substack{(\mathbf{x}_i)_i \in (\mathcal{C}_i)_i \\ \sum_{k=1}^{K} a_k \mathbf{x}_k = \lambda}} \exp\left\{ -\frac{1}{2\sigma^2} \left|\left| \mathbf{y} - \sum_{k=1}^{K} h_k \mathbf{x}_k \right|\right|^2 \right\}, \tag{77}$$

and using the assumption that the codewords are equiprobable in $(\mathcal{C}_1, \dots, \mathcal{C}_K)$, we conclude that the estimate $\hat{\lambda}$ of λ can be computed by solving

$$\hat{\lambda} = \arg\max_{\lambda \in L_F} \varphi(\lambda). \tag{78}$$

Remark 6. We are not proposing a decoding algorithm but rather elucidating the behavior of the decoding metric and deriving a code design criterion. It has been shown in [10] that in dimension $n = 1$ decoding based on Diophantine approximation is optimal, and in the same article it was conjectured to be optimal for $n \geq 2$ as well. However, how to treat simultaneous Diophantine equations is a mathematically open problem, which would be needed for implementing the Diophantine decoder in higher dimensions. While other optimal decoding methods may be derived, related work, such as [12], has to date only proposed efficient decoding algorithms in arbitrary dimensions for Gaussian channels.

Our goal in the remainder of this section is to study the behavior of $\varphi(\lambda)$. To analyze the decoding metric, we first need to express the function $\varphi(\lambda)$ in terms of the lattice point λ. This is achieved in the following proposition, whose proof we include as important quantities will be defined within. We follow a similar procedure described in [6, 10], but in more generality.

Proposition 20. *Let $\varphi(\lambda)$ be the decoding metric defined in (77). Then, $\varphi(\lambda)$ can be expressed in terms of the lattice point λ as*

$$\varphi(\lambda) = \sum_{\mathbf{t} \in S \subset \mathbb{Z}^{nK}} \exp\left\{ -\frac{1}{2\sigma^2} \left|\left| \omega(\lambda) - M_{\mathcal{L}} \hat{U} \mathbf{t} \right|\right|^2 \right\}, \tag{79}$$

where $S \subset \mathbb{Z}^{nK}$ is finite, $\omega(\lambda)$ is explicitly given in terms of λ, $\hat{U} \in \mathrm{Mat}(n(K-1) \times nK, \mathbb{R})$, and $M_{\mathcal{L}} \in \mathrm{Mat}(n \times n(K-1), \mathbb{R})$.

Proof. For each transmitter $1 \leq k \leq K$, let $M_k \in \mathrm{Mat}(n, \mathbb{R})$ denote the generator matrix of $\Lambda_{k,F}$, and write $\mathbf{x}_k = M_k \mathbf{z}_k$ for some $\mathbf{z}_k \in \mathbb{Z}^n$. We define the matrix $M := \left[a_1 M_1 \ \cdots \ a_K M_K \right] \in \mathrm{Mat}(n \times nK, \mathbb{R})$, where $\mathbf{a}^t = (a_1, \ldots, a_K)$ is the solution to (67) and express λ as

$$\lambda = \sum_{k=1}^{K} a_k \mathbf{x}_k = \sum_{k=1}^{K} a_k M_k \mathbf{z_k} \tag{80}$$

$$= \begin{bmatrix} a_1 M_1 & \cdots & a_K M_K \end{bmatrix} \begin{bmatrix} \mathbf{z}_1 \\ \vdots \\ \mathbf{z}_K \end{bmatrix} = M\mathbf{z}. \tag{81}$$

Let now[4] $U \in \mathrm{GL}_{nK}(\mathbb{R})$ be an invertible matrix such that

$$\tilde{B} := MU = \left[0_{n \times n(K-1)} \ \middle| \ B \right], \tag{82}$$

where $B \in \mathrm{Mat}(n, \mathbb{R})$ is invertible. We proceed by decomposing the matrix U into blocks $V_i \in \mathrm{Mat}(n, \mathbb{R})$ and $U_i \in \mathrm{Mat}(n \times n(K-1), \mathbb{R})$, as

$$U = \begin{bmatrix} U_1 & V_1 \\ \vdots & \vdots \\ U_K & V_K \end{bmatrix}. \tag{83}$$

[4] We will later choose a specific decomposition. However, any decomposition of this form suffices for decoding purposes.

Let now $\tilde{\mathbf{r}} := U^{-1}\mathbf{z} = (\mathbf{r}^t, \mathbf{r}_n^t)^t$, where $\mathbf{r}_n$ denotes the last n components of $\tilde{\mathbf{r}}$, and write

$$\lambda = M\mathbf{z} = \tilde{B}U^{-1}\mathbf{z} = \tilde{B}\tilde{\mathbf{r}} = B\mathbf{r}_n. \tag{84}$$

Note that $\mathbf{r}_n = B^{-1}\lambda$. To describe $\mathbf{r}$, the first $n(K-1)$ components of $\tilde{\mathbf{r}}$, let $\hat{U}$ be composed of the first $n(K-1)$ rows of U^{-1}. Then $\mathbf{r} = \hat{U}\mathbf{z}$. We can now write

$$\begin{bmatrix} \mathbf{z}_1 \\ \vdots \\ \mathbf{z}_K \end{bmatrix} = \begin{bmatrix} U_1 & V_1 \\ \vdots & \vdots \\ U_K & V_K \end{bmatrix} \begin{bmatrix} \mathbf{r} \\ B^{-1}\lambda \end{bmatrix} = \begin{bmatrix} U_1\mathbf{r} + V_1 B^{-1}\lambda \\ \vdots \\ U_K\mathbf{r} + V_K B^{-1}\lambda \end{bmatrix} \tag{85}$$

and consequently rewrite the codewords $\mathbf{x}_k$ in terms of λ as

$$\mathbf{x}_k = M_k\mathbf{z}_k = M_kU_k\mathbf{r} + M_kV_kB^{-1}\lambda \tag{86}$$

$$= M_kU_k(\hat{U}\mathbf{z}) + \mu_k(\lambda), \tag{87}$$

where $\mu_k(\lambda) := M_kV_kB^{-1}\lambda$. For $\nu_k := M_kU_k(\hat{U}\mathbf{z})$, the exponent of $\varphi(\lambda)$ now takes the form

$$\left|\left|\mathbf{y} - \sum_{k=1}^{K} h_k\mathbf{x}_k\right|\right|^2 = \left|\left|\mathbf{y} - \sum_{k=1}^{K} h_k(\mu_k(\lambda) + \nu_k)\right|\right|^2 \tag{88}$$

$$= \left|\left|\left(\mathbf{y} - \sum_{k=1}^{K} h_k\mu_k(\lambda)\right) - \sum_{k=1}^{K} h_k\nu_k\right|\right|^2. \tag{89}$$

To further simplify the expression, define the matrix

$$M_{\mathcal{L}} := \sum_{k=1}^{K} h_kM_kU_k, \tag{90}$$

which allows us to rewrite $\varphi(\lambda)$ explicitly in terms of λ as

$$\varphi(\lambda) = \sum_{\mathbf{t}\in S\subset\mathbb{Z}^{nK}} \exp\left\{-\frac{1}{2\sigma^2}\left|\left|\omega(\lambda) - M_{\mathcal{L}}\hat{U}\mathbf{t}\right|\right|^2\right\}. \tag{91}$$

Here $S \subset \mathbb{Z}^{nK}$ is finite and we have defined

$$\omega(\lambda) := \mathbf{y} - \sum_{k=1}^{K} h_k\mu_k(\lambda). \tag{92}$$

■

We state a lemma related to the structure defined by the matrix $M_{\mathcal{L}}$ for future reference and quickly discuss the consequences.

Lemma 21. *Let $M_{\mathcal{L}} = \sum_{k=1}^{K} h_kM_kU_k$ be the matrix defined in (90). Then $M_{\mathcal{L}}$ defines a subgroup $\mathcal{L}$ of $\mathbb{R}^n$ of rank $n(K-1)$, which can only be discrete for $K = 2$. Hence, for $K \geq 3$, $\mathcal{L}$ is not a lattice almost surely, i.e., with probability one.*

Remark 7. We remark that the authors in [6, 10] are not aiming at analyzing the behavior of $\varphi(\lambda)$ for actual resulting lattice sums $\mathcal{L}$. The structure of $\mathcal{L}$ has been studied only in the case $K = 2$, and consequently $\mathcal{L}$ has been commonly believed to be a lattice for any number of transmitters. By Lemma 21, $\mathcal{L}$ is a lattice for $K = 2$ but lacks a discrete structure when $K > 2$. The main problem is the effect of the random channel coefficients h_k and, as an important implication, the function $\varphi(\lambda)$ does not converge if the sum ranges over all of $\mathcal{L}$. This fact has dramatic consequences, as it implies that the tools developed in [6] for analyzing the behavior of $\mathcal{L}$ can be applied only in the case $K = 2$.

In general $\mathcal{L} = \sum_{i=1}^{K-1} \mathcal{L}_i$ is a sum of $(K-1)$ lattices, i.e., consists of vectors of the form $\mathbf{q} = \sum_{i=1}^{K-1} \mathbf{q}_i$, where $\mathbf{q}_i \in \mathcal{L}_i$. An example of a finite subset $\overline{\mathcal{L}} \subset \mathcal{L}$ for a sum of two lattices $\mathcal{L} = \mathcal{L}_1 + \mathcal{L}_2$ $(K = 3)$ for $n = 2$ and a fixed channel vector is depicted in Figure 6 for illustrative purposes.

In the proof of Proposition 20, we assumed the existence of a matrix $U \in \mathrm{GL}_{nK}(\mathbb{R})$ which yields the desired decomposition (82). For a general matrix $U \in \mathrm{GL}_{nK}(\mathbb{R})$, its inverse is a matrix with coefficients in $\mathbb{R}$, and hence $\mathbf{r} = \hat{U}\mathbf{z}$ is not an integer vector. Thus, $M_{\mathcal{L}}\hat{U}\mathbf{z}$ cannot be interpreted as an element of the lattice sum $\mathcal{L}$.

In [6, 10, 12], the authors propose a decomposition based on the *Hermite normal form* (HNF) of M. While the use of this specific decomposition has certain disadvantages, for example, it only allows us to consider integer lattices at the transmitter, it also allows us to further simplify the decoding expression. Using the HNF, the matrix U is unimodular, i.e., $U \in \mathrm{GL}_{nK}(\mathbb{Z})$. In this special situation, we have that $\hat{U} \in \mathrm{Mat}(n(K-1) \times nK, \mathbb{Z})$, and consequently $\mathbf{r} = \hat{U}\mathbf{z} \in \mathbb{Z}^{n(K-1)}$. This allows us to further simplify the ML decoding decision (91) to read

$$\hat{\lambda} = \arg\max_{\lambda \in L_F} \sum_{\mathbf{q} \in \overline{\mathcal{L}}} \exp\left\{ \frac{1}{2\sigma^2} \left|\left|\omega(\lambda) - \mathbf{q}\right|\right|^2 \right\}, \tag{93}$$

where $\mathbf{q} = M_{\mathcal{L}}\mathbf{z}$ with $\mathbf{z} \in \mathbb{Z}^{n(K-1)}$ ranges over a finite subset $\overline{\mathcal{L}} \subset \mathcal{L}$.

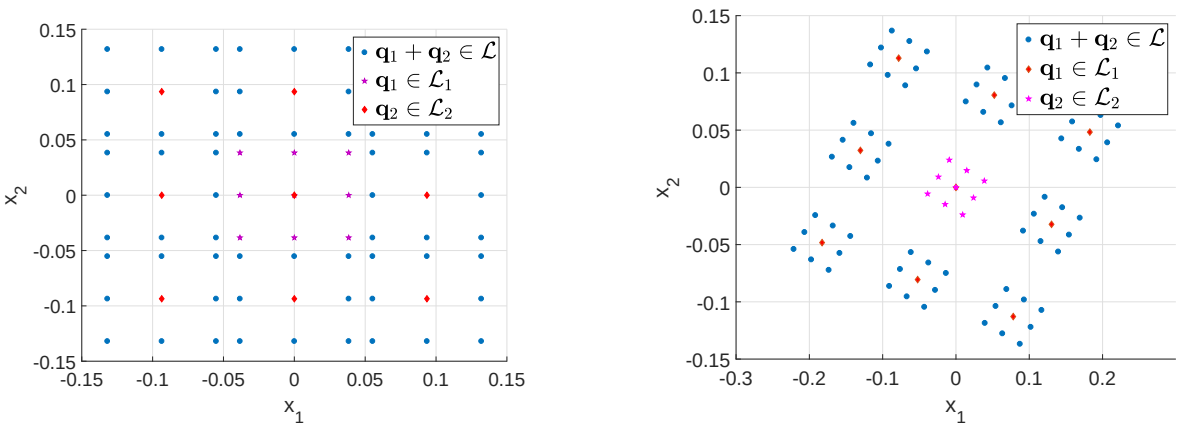

Figure 6. *Sum of $(K-1) = 2$ lattices $\mathcal{L} = \mathcal{L}_1 + \mathcal{L}_2$ in dimension $n = 2$. The depicted points correspond to coefficient vectors $\mathbf{z} \in [-p, p]^4$ with $p = 1$, and the density increases rapidly as p grows. The employed code lattices are $\mathbb{Z}^2$ on the left and $\Psi(\mathcal{O}_{\mathbb{Q}(\sqrt{5})})$ on the right figure.*

Nonetheless, any decomposition yielding a matrix in the form (82) allows for ML decoding at the relay.

4.3. The behavior of $\varphi(\lambda)$. We move on to analyze the behavior of the function

$$\varphi(\lambda) = \sum_{\mathbf{t}\in S\subset\mathbb{Z}^{nK}} \exp\left\{\frac{1}{2\sigma^2}\left|\left|\omega(\lambda) - M_{\mathcal{L}}\hat{U}\mathbf{t}\right|\right|^2\right\}, \tag{94}$$

which, as indicated in [6], can be *flat* for certain parameters leading to ambiguous decoding decisions and ultimately resulting in decoding errors. We begin by illustrating the behavior of $\varphi(\lambda)$ in Figure 7 for dimensions $n = 1$ and 2. In order to show that the flatness behavior of $\varphi(\lambda)$ prevails when using a decomposition other than the HNF, as well as when employing noninteger lattices, we use the LQ-decomposition of M. Here $M = LQ$, where L is lower triangular and Q unitary, and we choose $U := Q$; cf. (82).

In order to decode the lattice point λ, the relay needs to solve the maximization problem (78). We adopt two necessary restrictions.

(i) The definition of the flatness factor involves the volume of the considered lattice. Hence, the analysis of $\varphi(\lambda)$ in terms of this quantity makes sense only when the volume $\operatorname{vol}\mathcal{L}$ is defined. We thus require that $\mathcal{L}$ is a lattice, i.e., $K = 2$ (cf. Lemma 21).

(ii) Second, while any decomposition yielding the desired form allows the relay to solve (78), the matrix $\hat{U}$ may not be an integer matrix. The fractional part $\operatorname{frac}(\hat{U}\mathbf{t}) = \hat{U}\mathbf{t} - \operatorname{int}(\hat{U}\mathbf{t})$ may complicate the analysis of $\varphi(\lambda)$. To overcome this problem, we henceforth restrict to integer lattices, i.e., lattices with an integer generator matrix. This allows us to choose the HNF as the employed decomposition and consider the simplified expression (93).

Remark 8. An extension to the case $K > 2$ seems necessary, as numerical results suggest that the flat behavior prevails for more than two transmitters. A natural first step is to study the average flatness factor restricted to finite sets of the lattices constituting $\mathcal{L}$, as a straightforward generalization of the flatness factor for a sum of lattices $\mathcal{L}$ is not obvious. This was considered in a preliminary version of this article. However, the relevance of such an approach needs to be verified, and numerical simulations are currently too expensive.

If the intermediate relay aims to decode a linear combination of $K = 2$ codewords, the ML decoding metric (91) is a sum over lattice points, as repeatedly remarked previously. This

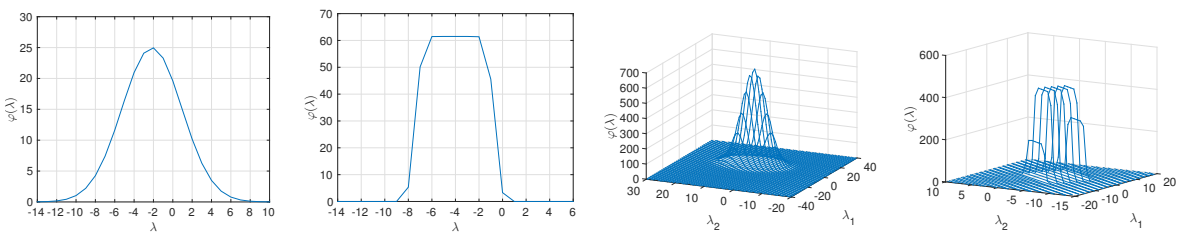

Figure 7. *Behavior of $\varphi(\lambda)$ for $K = 2$ transmitters in dimension $n = 1$ (left) with $\Lambda = \mathbb{Z}$, and $n = 2$ (right) with $\Lambda = \Psi(\mathcal{O}_{\mathbb{Q}(\sqrt{5})})$.*

allows us to characterize the behavior of $\varphi(\lambda)$ in terms of the flatness factor of the lattice $\mathcal{L}$ (cf. (61)).

Definition 22. *Let $K = 2$. The* flatness factor *of $\varphi(\lambda)$ is defined as the flatness factor of $\mathcal{L}$,*

$$\varepsilon_{\varphi(\lambda)}(\sigma^2) := \varepsilon_{\mathcal{L}}(\sigma^2). \tag{95}$$

Remark 9. The description of $\varepsilon_{\Lambda}(\sigma^2)$ in (61) allows us to study the flatness factor as a function of the noise variance σ^2. In the context of compute-and-forward, we need $\varepsilon_{\varphi(\lambda)}(\sigma^2)$ to be as large as possible, as by the definition large values imply a distinctive maximum, which inhibits a flat behavior of the related function $\varphi(\lambda)$.

Initially, studying the lattice flatness factor $\varepsilon_{\varphi(\lambda)}(\sigma^2)$ boils down to studying the flatness factor of the random lattice $\mathcal{L}$ which results at the relays. In order to have a reliable performance in the considered setting, we should choose lattices at the transmitter which are good for reliable communications, i.e., protect against noise and fading, while maximizing the flatness factor of the resulting lattice $\mathcal{L}$. By adopting the two restrictions listed above, it turns out that $\mathcal{L}$ can be related to the lattices employed at the transmitter, a link which we make explicit in Theorem 23 below. The consequences of the theorem are that maximizing the flatness factor of $\mathcal{L}$ amounts to maximizing the flatness factor of the original lattice.

Theorem 23. *Let $K = 2$, and let $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ be full integer lattices such that if M_Λ is the generator matrix of Λ_1, then there exists $c \in \mathbb{Z}\backslash\{0\}$ such that cM_Λ is the generator matrix for Λ_2. Hence, $\Lambda_1 \supseteq \Lambda_2$ are nested. Then, employing the HNF decomposition, the lattices $\mathcal{L}$ and Λ_1 are equivalent.*

Proof. We determine the generator matrix $M_{\mathcal{L}}$ of the lattice $\mathcal{L}$. Assume that $\mathbf{a}^t = (a_1, a_2)$ is the coefficient vector determining the linear combination to be decoded. As $\mathbf{a}$ is the solution to a shortest vector problem, we have $\gcd(a_1, a_2) = 1$. Define the matrix

$$M := \begin{bmatrix} a_1 M_\Lambda & a_2 c M_\Lambda \end{bmatrix}. \tag{96}$$

Since we have $\mathbf{a}^t \neq (0, 0)$, the matrix M has full-rank. Hence, there always exist $U \in \mathrm{GL}_{2n}(\mathbb{Z})$ and $B \in \mathrm{Mat}(n, \mathbb{Z})$ invertible, such that $MU = \begin{bmatrix} 0_n & B \end{bmatrix}$ is in HNF. If we write $A_1 := \mathrm{diag}\,\{a_1\}_{i=1}^n$, $A_2 := \mathrm{diag}\,\{ca_2\}_{i=1}^n$, and decompose the matrix U into $n \times n$ blocks as

$$U = \begin{bmatrix} U_1 & V_1 \\ U_2 & V_2 \end{bmatrix}, \tag{97}$$

we can write

$$MU = \begin{bmatrix} a_1 M_\Lambda & a_2 c M_\Lambda \end{bmatrix} U \tag{98}$$

$$= \begin{bmatrix} M_\Lambda & M_\Lambda \end{bmatrix} \begin{bmatrix} A_1 & 0_n \\ 0_n & A_2 \end{bmatrix} \begin{bmatrix} U_1 & V_1 \\ U_2 & V_2 \end{bmatrix} \tag{99}$$

$$= \begin{bmatrix} M_\Lambda & M_\Lambda \end{bmatrix} \begin{bmatrix} A_1 U_1 & A_1 V_1 \\ A_2 U_2 & A_2 V_2 \end{bmatrix} = \begin{bmatrix} 0_n & B \end{bmatrix}. \tag{100}$$

As M_Λ generates a full lattice, it is invertible. We multiply by M_Λ^{-1} from the left to get

$$M_\Lambda^{-1}\begin{bmatrix} M_\Lambda & M_\Lambda \end{bmatrix}\begin{bmatrix} A_1U_1 & A_1V_1 \\ A_2U_2 & A_2V_2 \end{bmatrix} \tag{101}$$

$$= \begin{bmatrix} I_n & I_n \end{bmatrix}\begin{bmatrix} A_1U_1 & A_1V_1 \\ A_2U_2 & A_2V_2 \end{bmatrix} \tag{102}$$

$$= \begin{bmatrix} (A_1U_1 + A_2U_2) & (A_1V_1 + A_2V_2) \end{bmatrix} \tag{103}$$

$$= \begin{bmatrix} 0_n & M_\Lambda^{-1}B \end{bmatrix}, \tag{104}$$

which yields the equations $A_1U_1 + A_2U_2 = 0_n$ and $A_1V_1 + A_2V_2 = M_\Lambda^{-1}B$. We can rewrite the first equation to read

$$\begin{bmatrix} A_1 & A_2 \end{bmatrix}\begin{bmatrix} U_1 \\ U_2 \end{bmatrix} \tag{105}$$

$$= \begin{bmatrix} a_1 & 0 & \cdots & 0 & ca_2 & 0 & \cdots & 0 \\ 0 & a_1 & & 0 & 0 & ca_2 & & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & & a_1 & 0 & & \cdots & ca_2 \end{bmatrix}\begin{bmatrix} U_1 \\ U_2 \end{bmatrix} = 0_n. \tag{106}$$

This equation is satisfied if and only if

$$\operatorname{colspan}\left(\begin{bmatrix} U_1 \\ U_2 \end{bmatrix}\right) \subseteq \ker\left(\begin{bmatrix} A_1 & A_2 \end{bmatrix}\right) \tag{107}$$

$$= \operatorname{span}\left\{\begin{bmatrix} ca_2 \cdot e_i \\ -a_1 \cdot e_i \end{bmatrix}\right\}_{i=1}^{n}, \tag{108}$$

where e_i is the ith standard vector. In particular, we can always choose

$$U_1 = -\operatorname{diag}\{ca_2\}_{i=1}^n; \quad U_2 = \operatorname{diag}\{a_1\}_{i=1}^n. \tag{109}$$

With this choice, the generator matrix of $\mathcal{L}$ simplifies to

$$M_\mathcal{L} = h_1 M_\Lambda U_1 + h_2 c M_\Lambda U_2 \tag{110}$$

$$= -h_1 M_\Lambda \operatorname{diag}\{ca_2\}_{i=1}^n + h_2 c M_\Lambda \operatorname{diag}\{a_1\}_{i=1}^n \tag{111}$$

$$= (h_2 c \operatorname{diag}\{a_1\}_{i=1}^n - h_1 \operatorname{diag}\{ca_2\}_{i=1}^n) M_\Lambda = r M_\Lambda \tag{112}$$

for some $r \in \mathbb{R}$. ∎

This result motivates the study of the flatness factor of the code lattices. As these should be picked to be well-conditioned for coding purposes, we only need to compute the flatness factor of reasonably conditioned lattices. Thus, the derived approximation $\Theta_\Lambda^{\mathfrak{A}}(q)$ will suffice for that purpose. We consider the lattices $\Lambda_i^{(3)}$ and $\Lambda_i^{(4)}$, $1 \le i \le 4$, tabulated in Table 2 in Appendix 5. As the well-known lattices $\mathbb{Z}^n$, D_n and the dual D_n^* are all examples of well-rounded lattices, we consider additional lattices $\Lambda_4^{(3)}$, $\Lambda_3^{(4)}$, and $\Lambda_4^{(4)}$ which are well-rounded as well, for sake of consistency. These are found via computer search.

Remark 10. Note that, as it should be, the flatness factor of $\varphi(\lambda)$ is independent of the size of constellation, as it is simply the flatness factor of the unconstrained lattice $\mathcal{L}$. For a meaningful comparison, however, we fix a finite codebook for each of the considered lattices and illustrate their flatness factor with respect to the power-dependent SNR, $\rho = P/\sigma^2$.

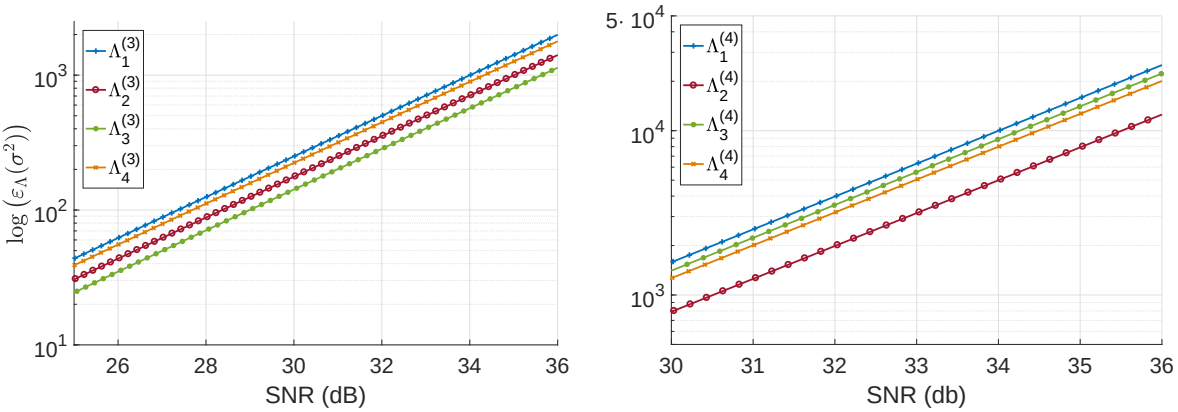

Figure 8. *Flatness factors of* Λ *for lattices of dimensions* $n = 3$ *(left) and* $n = 4$ *(right).*

The average power P for the employed constellation is also found in Table 2. We compare the considered lattices in Figure 8.

In both dimensions $n = 3$ and $n = 4$, it is visible that the integer lattice $\Lambda_1^{(n)} = \mathbb{Z}^n$ performs best among the considered lattices with respect to the flatness factor criterion. This is in agreement with the observation in [10] that the lattice $\mathcal{L}$ should not be dense. However, the density is not the only factor that plays a role, as visible from the plot in dimension $n = 3$. There, the best quantizer, $\Lambda_3^{(3)} = D_3^*$, exhibits the smallest flatness factor, even below the densest packing $\Lambda_2^{(3)} = D_3$. In dimension $n = 4$, the lattice $\Lambda_2^{(4)} = D_4$ is both the best quantizer and densest packing and exhibits the smallest flatness factor.

The quintessential statement, however, is not that the lattice $\mathbb{Z}^n$ is the one that should always be used. Indeed, the code lattice should first be chosen to perform well in compute-and-forward, and additionally exhibit a large flatness factor. This yields a potential trade-off in code design.

5. Conclusions. The main goal of this article was to derive a simple approximation of the theta series of a lattice. Our approximation can be shown to be a simple rational function.

We then studied maximum-likelihood decoding in the context of compute-and-forward relaying and showed that partial code design criteria can be derived based on the so-called flatness factor of certain involved lattices. Using a particular matrix decomposition for manipulating the decoding metric, and adopting two important restrictions, we further prove that the code lattice at the transmitter and the random lattice at the relay are similar. This allows for a direct design criterion for the code lattice, rather than for the random lattice. Namely, the flatness factor of the code lattice should be maximized.

As the flatness factor is directly related to the theta series of a lattice, it is hence crucial to be able to efficiently compute the latter quantity. Hence, for the purposes of empirically analyzing different lattices at the transmitter, the theta series approximation proves to be crucial, both in this context as well as in the context of wiretap coset code design, e.g., the results obtained in [27].

This work allows extending the framework in a variety of directions. First, as noted in this article, the decoding metric is only a sum over lattice points for $K = 2$ transmitters,

and the analysis of its behavior becomes more complicated when $K \geq 3$, though numerical results show that the flatness behavior prevails. On the other hand, the used decomposition only allows for integer lattices and integer linear combinations. Following related work [24, 26] where the linear combinations are allowed to be over the ring of integers of an algebraic number field, it would be of benefit to examine the decoding metric in this generalized setting. The HNF decomposition over the integers $\mathbb{Z}$ is only a special case, and the algorithm has been extended to arbitrary Dedekind domains. Thus using this generalized decomposition would allow studying algebraic lattices for code construction at the transmitters.

Appendix. Table 2 serves as a summary of the characteristics of the lattices used for simulations and introduces the employed notation.

Table 2

Summary of the lattices employed for simulation results.

$\mathbf{n=3}$	Notation	M_Λ	λ_1	$\mathrm{vol}\,\Lambda$	$\Theta_\Lambda(q)$	P ($\lvert\mathcal{C}\rvert = 343$)
	$\Lambda_1^{(3)} = \mathbb{Z}^3$	I_3	1	1	$\theta_3^3(q)$	4
	$\Lambda_2^{(3)} = D_3 \cong A_3$	$\begin{bmatrix} -1 & 1 & 0 \\ -1 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix}$	2	2	$\frac{1}{2}(\theta_3^3(q) + \theta_4^3(q))$	8
	$\Lambda_3^{(3)} = D_3^* \cong A_3^*$	$\begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$	3	4	$\theta_2(4q)^3 + \theta_3(4q)^3$	16.6667
	$\Lambda_4^{(3)}$	$\begin{bmatrix} 2 & 0 & 0 \\ 1 & -2 & 1 \\ 0 & -1 & -2 \end{bmatrix}$	5	10	-	20
$\mathbf{n=4}$						P ($\lvert\mathcal{C}\rvert = 2401$)
	$\Lambda_1^{(4)} = \mathbb{Z}^4$	I_4	1	1	$\theta_3^4(q)$	4
	$\Lambda_2^{(4)} = D_4$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	2	2	$\frac{1}{2}(\theta_3^4(q) + \theta_4^4(q))$	8
	$\Lambda_3^{(4)}$	$\begin{bmatrix} 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	3	8	-	12
	$\Lambda_4^{(4)}$	$\begin{bmatrix} -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 1 & 1 & -2 & 1 \\ 0 & 2 & 1 & 0 \end{bmatrix}$	5	20	-	20

Acknowledgments. The authors would like to thank Dr. David Karpuk and Dr. Laia Amorós for their help toward this article.

REFERENCES

[1] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehle, *Semantically secure lattice codes for the Gaussian wiretap channel*, IEEE Trans. Inform. Theory, 60 (2014), pp. 6399–6416.
[2] A. Campello, C. Ling, and J.-C. Belfiore, *Semantically Secure Lattice Codes for Compound MIMO Channels*, https://arxiv.org/abs/1903.09954, 2019.
[3] C. Ling and L. Gan, *Lattice quantization noise revisited*, in proceedings of the IEEE Information Theory Workshop, Sevilla, 2013, pp. 1–5.
[4] B. Nazer and M. Gastpar, *Compute-and-forward: Harnessing interference through structured codes*, IEEE Trans. Inform. Theory, 57 (2011) pp. 6463–6486.
[5] C. Feng, D. Silva, and F. R. Kschischang, *An algebraic approach to physical-layer network coding*, IEEE Trans. Inform. Theory, 59 (2013), pp. 7576–7596.
[6] J.-C. Belfiore, *Lattice codes for the compute-and-forward protocol: The flatness factor*, Presented at the IEEE Information Theory Workshop, 2011.
[7] A. Ivic, E. Krätzel, M. Kühleitner, and W. G. Nowak, *Lattice Points in Large Regions and Related Arithmetic Functions: Recent Developments in a Very Classic Topic*, https://arxiv.org/abs/math/0410522, 2004.
[8] C. L. Siegel, *A mean value theorem in geometry of numbers*, Ann. of Math., 46 (1945), pp. 340–347.
[9] F. Götze, *Lattice point problems and values of quadratic forms*, Invent. Math., 157 (2004), pp. 195–226.
[10] J.-C. Belfiore and C. Ling, *The flatness factor in lattice network coding: Design criterion and decoding algorithm*, presented at the Zurich Seminar on Communications, 2012.
[11] S. Holmin, *The Number of Points from a Random Lattice that Lie Inside a Ball*, preprint, https://arxiv.org/abs/1311.2865, 2013.
[12] A. Mejri and G. Rekaya-Ben Othman, *Efficient decoding algorithms for the compute-and-forward strategy*, IEEE Trans. Comm., 63 (2015), pp. 2475–2485.
[13] S. Lyu, A. Campello, and C. Ling, *Ring compute-and-forward over block-fading channels*, IEEE Trans. Inform. Theory, 65 (2019), pp. 6931–6949.
[14] D. Micciancio and O. Regev, *Worst-case to average-case reductions based on Gaussian measures*, SIAM J. Comput., 37 (2007), pp. 267–302.
[15] M. Widmer, *Lipschitz class, narrow class, and counting lattice points*, Proc. Amer. Math. Soc., 140 (2011), pp. 677–689.
[16] M. Henk, *Successive minima and lattice points*, Rend. Circ. Mat. Palermo (2) Suppl., 70 (2002), pp. 377–384.
[17] W. Schmidt, *A metrical theorem in geometry of numbers*, Trans. Amer. Math. Soc., 95 (1960), pp. 516–529.
[18] L. Fukshansky and A. Schürmann, *Bounds on generalized Frobenius numbers*, European J. Combin., 42 (2011), pp. 361–368.
[19] S. Lang, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1970.
[20] D. Micciancio and O. Regev, *Worst-case to average-case reductions based on Gaussian measures*, SIAM J. Comput., 37 (2007), pp. 267–302.
[21] A. Osmane and J.-C. Belfiore, *The Compute-and-Forward Protocol: Implementation and Practical Aspects*, https://arxiv.org/abs/1107.0300v1, 2011.
[22] S. Sahraei and M. Gastpar, *Polynomially solvable instances of the shortest and closest vector problems with applications to compute-and-forward*, IEEE Trans. Inform. Theory, 63 (2017), pp. 7780–7792.
[23] A. Barreal, J. Pääkkönen, D. Karpuk, C. Hollanti, and O. Tirkkonen, *A low-complexity message recovery method for Compute-and-Forward relaying*, presented at the IEEE Information Theory Workshop, 2015.
[24] N. E. Tunali, K. R. Narayanan, J. J. Boutros, and Y. Huang, *Lattices over Eisenstein integers for compute-and-forward*, presented at the 50th Annual Allerton Conference on Communication, Control, and Computing, 2012.

[25] E. Landau, *Über die anzahl der gitterpunkte in gewissen bere-ichen. Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, Mathematisch-Physikalische Klasse, vol. 1924, 1924, pp. 137–150.
[26] Y. Huang, K. R. Narayanan, and P. Wang, *Adaptive compute-and-forward with lattice codes over algebraic integers*, presented at the IEEE International Symposium on Information Theory, 2012.
[27] A. Barreal, A. Karrila, D. Karpuk, and C. Hollanti, *Information bounds and flatness factor approximation for fading wiretap MIMO channels*, presented at the International Telecommunication Networks and Applications Conference, 2016.