COMPUTING THE THETA FUNCTION

Alexander Barvinok

June 4, 2023

Abstract. Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a positive definite quadratic form and let $y \in \mathbb{R}^n$ be a point. We present a fully polynomial randomized approximation scheme (FPRAS) for computing $\sum_{x \in \mathbb{Z}^n} e^{-f(x)}$, provided the eigenvalues of f lie in the interval roughly between s and e^s and for computing $\sum_{x \in \mathbb{Z}^n} e^{-f(x-y)}$, provided the eigenvalues of f lie in the interval roughly between e^{-s} and s^{-1} for some $s \geq 3$. To compute the first sum, we represent it as the integral of an explicit log-concave function on $\mathbb{R}^n$, and to compute the second sum, we use the reciprocity relation for theta functions. We then apply our results to test the existence of many short integer vectors in a given subspace $L \subset \mathbb{R}^n$, to estimate the distance from a given point to a lattice, and to sample a random lattice point from the discrete Gaussian distribution.

1. Introduction

(1.1) The theta function. Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}_+$ be a positive definite quadratic form, so

$$f(x) = \langle Bx, x \rangle \quad \text{for} \quad x \in \mathbb{R}^n,$$

where B is an $n \times n$ positive definite matrix and $\langle \cdot, \cdot \rangle$ is the standard scalar product in $\mathbb{R}^n$. We consider the problem of efficient computing (approximating) the sum

$$\Theta(B) = \sum_{x \in \mathbb{Z}^n} e^{-f(x)} = \sum_{x \in \mathbb{Z}^n} e^{-\langle Bx, x \rangle}, \tag{1.1.1}$$

where $\mathbb{Z}^n \subset \mathbb{R}^n$ is the standard integer lattice. More generally, for a given point $y \in \mathbb{R}^n$, we want to efficiently compute (approximate) the sum

$$\Theta(B, y) = \sum_{x \in \mathbb{Z}^n} e^{-f(x-y)} = \sum_{x \in \mathbb{Z}^n} e^{-\langle B(x-y), x-y \rangle}. \tag{1.1.2}$$

1991 *Mathematics Subject Classification.* 52C07, 11H55, 68R01, 68W25.
Key words and phrases. theta function, integer point, approximation algorithms, lattice.
This research was partially supported by NSF Grant DMS 1855428.

Together with (1.1.1) and (1.1.2), we also compute the sum

$$\sum_{x\in\mathbb{Z}^n} \exp\left\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\right\}, \tag{1.1.3}$$

where $b \in \mathbb{R}^n$ and $\mathbf{i}^2 = -1$.

Of course, the sums (1.1.1) – (1.1.3) are examples of the (multivariate) theta function, an immensely popular object, see, for example, [M07a], [M07b] and [M07c]. Theta functions satisfy the *reciprocity relation*

$$\begin{aligned} &\sum_{x\in\mathbb{Z}^n} \exp\left\{-\pi\langle B(x-y), x-y\rangle\right\} \\ =&\frac{1}{\sqrt{\det B}} \sum_{x\in\mathbb{Z}^n} \exp\left\{-\pi\langle B^{-1}x, x\rangle + 2\pi\mathbf{i}\langle x, y\rangle\right\}, \end{aligned} \tag{1.1.4}$$

see, for example, [BL61].

One motivation to study (1.1.1)–(1.1.3) from the computational point of view comes from connections with algorithmic problems on lattices, such as approximating the length of a shortest non-zero vector in the lattice and estimating the distance from a given point to a given lattice, see [Sc87], [G+93], [Ba93], [Aj96], [A+01], [MG02], [D+03], [AR05], [Kh05], [MR07], [A+15], [M+21], as well as lattice-based cryptography, see [MG02], [MR07], [G+08], [MR09], [Pe10].

(1.2) Lattices. A *lattice* $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup which spans $\mathbb{R}^n$. Equivalently, Λ is the set of all integer linear combinations of some linearly independent vectors $u_1, \ldots, u_n$, called a *basis* of Λ,

$$\Lambda = \left\{ \sum_{i=1}^n \xi_i u_i : \quad \xi_i \in \mathbb{Z} \quad \text{for} \quad i = 1, \ldots, n \right\}.$$

We say that $\operatorname{rank}\Lambda = n$.

For $n > 1$, the same lattice Λ has many different bases, and some of those bases are more convenient to work with than others, see, for example, [G+93] and [MG02]. Given a vector $u \in \Lambda$, $u = \xi_1 u_1 + \ldots + \xi_n u_n$, we have

$$\|u\|^2 = \langle Bx, x\rangle \quad \text{where} \quad x = (\xi_1, \ldots, \xi_n)$$

and B is the Gram matrix of the vectors $u_1, \ldots, u_n$, so that

$$B = (\beta_{ij}) \quad \text{where} \quad \beta_{ij} = \langle u_i, u_j\rangle.$$

Similarly, if $v \in \mathbb{R}^n$ is an arbitrary point, $v = \eta_1 u_1 + \ldots + \eta_n u_n$, then

$$\|u - v\|^2 = \langle B(x-y), x-y\rangle \quad \text{for} \quad y = (\eta_1, \ldots, \eta_n).$$

Consequently, the theta functions (1.1.1) and (1.1.2) are written as

$$\Theta(B) = \sum_{u \in \Lambda} e^{-\|u\|^2} \qquad \text{and} \qquad \Theta(B, y) = \sum_{u \in \Lambda} e^{-\|u-v\|^2}. \tag{1.2.1}$$

We see from (1.2.1) that the theta functions do not depend on the choice of a basis of the lattice: choosing a different basis corresponds to replacing the Gram matrix B with a Gram matrix of the form $A^T B A$, where $A \in GL(n, \mathbb{Z})$ is an integer matrix such that $\det A = \pm 1$. It follows that the value of $\det B$ does not depend on the choice of a basis. The number $\sqrt{\det B}$ is called the *determinant* of Λ and denoted $\det \Lambda$, see, for example, Chapter I of [Ca97].

The following two optimization problems have attracted a lot of attention due to their importance for optimization and cryptography. One is finding (or approximating) the minimum length of a non-zero vector from a given lattice,

$$\lambda(\Lambda) = \min_{u \in \Lambda \setminus \{0\}} \|u\|$$

and the other is finding (or approximating) the distance from a given point $v \in \mathbb{R}^n$ to a given lattice,

$$\operatorname{dist}(v, \Lambda) = \min_{u \in \Lambda} \|u - v\|,$$

see [Sc87], [G+93], [Ba93], [Aj96], [A+01], [MG02], [D+03], [AR05], [Kh05], [A+15]. We assume that Λ is defined by its basis. In a breakthrough paper [Ba93], Banaszczyk used theta functions to obtain structural results (known as "transference theorems") for $\lambda(\Lambda)$ and a host of related quantities (successive minima, covering radius, etc.) Using results of [Ba93], Aharonov and Regev [AR05] showed that the problems of approximating $\lambda(\Lambda)$ and $\operatorname{dist}(v, \Lambda)$ within a factor $O(\sqrt{n})$ lie in NP $\cap$ co-NP. This is in contrast to the fact that the existing polynomial time algorithms are guaranteed to approximate the desired quantities roughly within a $2^{O(n)}$ factor, more precisely within a factor of $2^{O(n(\log\log n)^2/\log n)}$ in deterministic polynomial time [Sc87] and within a factor $2^{O(n \log\log n/\log n)}$ in randomized polynomial time [A+01]. Computing $\lambda(\Lambda)$ exactly is NP-hard, and approximating $\lambda(\Lambda)$ within a factor of $2^{(\log n)^{\frac{1}{2}-\epsilon}}$ is hard modulo some plausible computational complexity assumptions [Kh05], while approximating $\operatorname{dist}(v, \Lambda)$ within a factor of $n^{c/\log\log n}$ is NP-hard for some absolute constant $c > 0$ [D+03].

Given a lattice $\Lambda \subset \mathbb{R}^n$ and a point $v \in \mathbb{R}^n$, one can define a probability measure on Λ, called the *discrete Gaussian distribution*, where the probability of $u \in \Lambda$ is proportional to $e^{-\|u-v\|^2}$,

$$\mathbf{P}(u) \sim e^{-\|u-v\|^2} \quad \text{for all} \quad u \in \Lambda. \tag{1.2.2}$$

Efficient approximate sampling from the distribution (1.2.2) has attracted a lot of attention, in connection with optimization and cryptography, see [G+08], [MR07], [MR09], [Pe10], [A+15], [RS17].

2. Results

(2.1) Approximating the theta function. In what follows, we write $A \preceq B$ for $n \times n$ real symmetric matrices A and B if $B - A$ is a positive semidefinite matrix. We denote by I the $n \times n$ identity matrix. Our main result is a fully polynomial randomized approximation scheme (FPRAS) for computing (1.1.1) and (1.1.3) provided

$$sI \;\preceq\; B \;\preceq\; \left(s + \frac{e^s}{4}\left(1 - e^{-s}\right)^2\left(1 - e^{-2s}\right)\right) I \quad \text{for some} \quad s \geq 1. \tag{2.1.1}$$

Thus we present a randomized algorithm that for any B satisfying (2.1.1) and for any $\epsilon > 0$ approximates the value of $\Theta(B)$ and that of (1.1.3) within relative error ϵ in time polynomial in n, ϵ^{-1} and s. It turns out that when (2.1.1) is satisfied, we can write (1.1.1) and (1.1.3) as an integral of some explicit log-concave function $G : \mathbb{R}^n \longrightarrow \mathbb{R}_+$ and hence we can use any of the efficient algorithms for integrating log-concave functions as a blackbox [AK91], [F+94], [FK99], [LV07]. From (2.1.1) we obtain an easier to parse condition

$$sI \;\preceq\; B \;\preceq\; \left(s + \frac{e^s}{5}\right) I \quad \text{for} \quad s \geq 3, \tag{2.1.2}$$

which is sufficient for $\Theta(B)$ and, more generally, for (1.1.3) to be efficiently computable. We describe the algorithm is Section 3 and prove the main structural result (Theorem 3.1) underlying the algorithm in Section 4.

From the reciprocity relation (1.1.4) it immediately follows that there is an FPRAS for $\Theta(B, y)$ provided

$$\pi^2\left(s + \frac{e^s}{4}\left(1 - e^{-s}\right)^2\left(1 - e^{-2s}\right)\right)^{-1} I \;\preceq\; B \;\preceq\; \pi^2 s^{-1} I \quad \text{for some} \quad s \geq 1. \tag{2.1.3}$$

That is, there is a randomized algorithm that for any B satisfying (2.1.3), for any $y \in \mathbb{R}^n$ and any $0 < \epsilon < 1$ approximates the value of $\Theta(B, y)$ within relative error ϵ in time polynomial in n, ϵ^{-1} and s. An easier to parse sufficient condition is

$$\pi^2\left(s + \frac{e^s}{5}\right)^{-1} I \;\preceq\; B \;\preceq\; \left(\pi^2 s^{-1}\right) I \quad \text{for} \quad s \geq 3. \tag{2.1.4}$$

(2.1.5) The smooth range.

Let us fix $\gamma > 1$ and let $s = \gamma \ln n$. It is not hard to check that if $sI \preceq B$ then the value of $\Theta(B)$, and, more generally, of (1.1.3) is $1 + O\left(n^{1-\gamma}\right)$, since only $x = 0$ contributes significantly to the sum. Furthermore, a straightforward algorithm approximates $\Theta(B)$ and (1.1.3) within relative error ϵ in time polynomial in n and

ϵ^{-1}, provided n is sufficiently large, $n \geq n_0(\gamma)$. For the sake of completeness, we present the algorithm along with some technical estimates in Section 8.

Applying the reciprocity relation (1.1.4), we have

$$\Theta(B, y) = \frac{\pi^{n/2}}{\sqrt{\det B}} \left(1 + O\left(n^{1-\gamma}\right)\right) \quad \text{provided} \quad B \preceq \left(\frac{\pi^2}{\gamma \ln n}\right) I \quad \text{for} \quad \gamma > 1.$$

Furthermore, as long as $\gamma > 1$ is fixed, for any $\epsilon > 0$ the value of $\Theta(B, y)$ can be approximated within relative error ϵ in time polynomial in n and ϵ^{-1}. Hence if B is sufficiently small in the "$\preceq$" order, the discrete sum (1.1.2) is well-approximated by the integral

$$\int_{\mathbb{R}^n} \exp\left\{-\langle B(x-y), x-y\rangle\right\} \, dx = \frac{\pi^{n/2}}{\sqrt{\det B}}.$$

This phenomenon is described by the *smoothing parameter* of a lattice introduced in [MR07]. Our constraints (2.1.1) and (2.1.3) correspond to the "non-smooth" range when $s \leq \gamma \ln n$ for some fixed $0 < \gamma < 1$. Apart from some straightforward situations (for example, when the matrix B is diagonal), the condition (2.1.3) appears to be the first one when $\Theta(B, y)$ can be efficiently approximated in a non-smooth, that is genuinely discrete, case.

(2.2) Integer points in a subspace. Let A be an $m \times n$ integer matrix of $\operatorname{rank} A = m < n$ and let

$$\Lambda = \{x \in \mathbb{Z}^n : \; Ax = 0\}. \tag{2.2.1}$$

Then Λ is a lattice in the ambient space $\operatorname{span}(\Lambda) = \ker A$. We remark that even when $m = 1$, the class of such lattices (2.2.1) is quite rich: it is shown in [S+11] that any lattice Λ' of rank n can be arbitrarily closely approximated by a proper scaling $\alpha\Lambda$ of a lattice Λ that is a hyperplane section of $\mathbb{Z}^{n+1}$.

For $s > 0$, we consider the theta function

$$\Theta_\Lambda(s) = \sum_{u \in \Lambda} e^{-s\|u\|^2}.$$

We denote by $\|A\|_{\text{op}}$ the operator norm of A, that is the largest singular value of A. Let us fix $\delta > 0$. In what follows, we consider asymptotics as n grows.

In Section 5, we show that if $\|A\|_{\text{op}} = o\left(n^\delta\right)$, then for

$$s = \left(\frac{1}{2} + \delta\right) \ln n$$

and any $\epsilon > 0$, the value of $\Theta_\Lambda(s)$ can be approximated within relative error $\epsilon + o(1)$ in randomized polynomial time. This is based on the observation that $\Theta_\Lambda(s)$ is

approximated within an additive error $o(1)$ by the function $\Theta(B)$ of (1.1.1), where B is an $n \times n$ matrix with the eigenvectors in $\ker A$ with eigenvalue s and in $(\ker A)^{\perp} = \operatorname{im} A^T$ with eigenvalue $s + e^s/5$ so that B satisfies (2.1.2) when $s \geq 3$.

Note that as long as $\delta < 1/2$, we are in a "non-smooth" range, cf. Section 2.1.5.

This result is then applied to testing the existence of short non-zero vectors in Λ. We show that if

$$\min_{u \in \Lambda \setminus \{0\}} \|u\| \ \gg \ n^{\frac{1}{2} - \delta}$$

then $\Theta_{\Lambda}(s) = 1 + o(1)$, while $\Theta_{\Lambda}(s) \gg 1$, if Λ contains many short vectors, which allows us to separate these two cases in randomized polynomial time.

Using a different approach, in [M+21], the authors present a polynomial time algorithm to find a lattice vector closest to a given point, when A is a totally unimodular matrix.

(2.3) Estimating the distance to the lattice. In Section 6, we consider the problem of estimating the distance from a given point $v \in \mathbb{R}^n$ to a given lattice $\Lambda \subset \mathbb{R}^n$, provided $\mathbb{Z}^n \subset \Lambda$. Such lattices Λ appear in a few natural ways. If $\Lambda_0 \subset \mathbb{Z}^n$ is a lattice with an integer basis, then the *dual* or *reciprocal* lattice $\Lambda = \Lambda_0^*$ defined by

$$\Lambda_0^* = \{u \in \mathbb{R}^n : \quad \langle u, w \rangle \in \mathbb{Z} \quad \text{for all} \quad w \in \Lambda_0\}$$

contains $\mathbb{Z}^n$. The *q-ary* lattices Λ satisfying $(q\mathbb{Z})^n \subset \Lambda \subset \mathbb{Z}^n$ for an integer $q > 1$ play a prominent role in lattice-based cryptography, see [Aj96], [MG02], [MR09]. Typically, they are defined as the sets of solutions to systems of integer linear equations $\mod q$. Clearly, if Λ is a q-ary lattice then the lattice $q^{-1}\Lambda$ contains $\mathbb{Z}^n$.

For a lattice $\Lambda \subset \mathbb{R}^n$ and $\tau > 0$, we define

$$\Theta_{\Lambda}(\tau, v) = \sum_{u \in \Lambda} \exp\left\{-\tau \|u - v\|^2\right\}.$$

In particular, if $\Lambda = \mathbb{Z}^n$, then $\Theta_{\mathbb{Z}^n}(\tau, v) = \Theta(\tau I, v)$ and $\Theta_{\mathbb{Z}^n}(\tau, 0) = \Theta(\tau I)$ in the notation of Section 1.1.

In Section 6, we prove that if $\mathbb{Z}^n \subset \Lambda$ then for any $0 < \tau \leq 1$, we have

$$41e^{-\pi^2/\tau} \operatorname{dist}^2(v, \Lambda) \ \geq \ \ln \frac{\Theta(\tau I)}{\Theta_{\Lambda}(\tau, v)} \ \geq \ 13e^{-\pi^2/\tau} \operatorname{dist}^2(v, \Lambda) + \ln \det \Lambda. \tag{2.3.1}$$

As n grows, under some conditions the additive term of $\ln \det \Lambda$ becomes asymptotically negligible and (2.3.1) provides an approximation of $\operatorname{dist}(v, \Lambda)$ within a constant factor of $\sqrt{41/13} \approx 1.8$, computable in randomized polynomial time. We provide an example to that effect in Section 6.

(2.4) Sampling from the discrete Gaussian distribution. Given a lattice $\Lambda \subset \mathbb{R}^n$ and a point $v \in \mathbb{R}^n$, we consider the discrete Gaussian probability distribution (1.2.2). Suppose that Λ has a basis whose Gram matrix B satisfies

$$\lambda I \ \preceq \ B \tag{2.4.1}$$

for some $\lambda > 0$. Assume further that for any given $y \in \mathbb{R}^n$, the value of $\Theta(B, y)$ can be approximated in randomized polynomial time (for example, if B satisfies (2.1.3)). We present an algorithm which for any given $0 < \epsilon < 1$ samples a random point $u \in \Lambda$ from a probability distribution μ which is ϵ-close to (1.2.2) in the total variation distance, that is,

$$\frac{1}{2} \sum_{u \in \Lambda} |\mathbf{P}(u) - \mu(u)| \ \leq \ \epsilon.$$

The complexity of the algorithm is polynomial in n, ϵ^{-1} and λ^{-1}.

It appears that previously polynomial time sampling algorithms, apart from some simple cases (such as when B is a diagonal matrix), were known only in the smooth range, when the discrete Gaussian measure is well-approximated by its classical continuous version [G+08], [Pe10]. Our algorithm follows the general logic of Peikert's algorithm [Pe10], except that we are able to extend it to non-smooth cases, since we are able to approximate the value of the theta function in those cases. Apart from that, the price we apparently have to pay is the dependence of the computational complexity on λ in (2.4.1), which is absent in the smooth case.

We discuss the algorithm in Section 7.

(2.5) The plan of the paper. Summarizing, the plan of the paper is as follows.

In Section 3, we present our main algorithm for approximating the theta functions (1.1.1) and (1.1.3).

In Section 4, we prove the main structural result, underlying the algorithm.

In Section 5, we compute theta functions associated with integer points in a subspace.

In Section 6, we estimate the distance from a given point to a lattice containing $\mathbb{Z}^n$.

In Section 7, we present an algorithm for sampling from a discrete Gaussian distribution.

In Section 8, we discuss the smooth case.

3. The main algorithm

A function $G : \mathbb{R}^n \longrightarrow \mathbb{R}_+$ is called *log-concave* if

$$G(\alpha x + (1-\alpha)y) \ \geq \ G^{\alpha}(x) G^{1-\alpha}(y) \quad \text{for all} \quad x, y \in \mathbb{R}^n \quad \text{and all} \quad 0 \leq \alpha \leq 1.$$

Equivalently, $G = e^{\psi}$ where $\psi : \mathbb{R}^n \longrightarrow \mathbb{R} \cup \{-\infty\}$ is concave, that is

$$\psi\big(\alpha x + (1-\alpha)y\big) \ \geq \ \alpha\psi(x) + (1-\alpha)\psi(y) \quad \text{for all} \quad x, y \in \mathbb{R}^n \quad \text{and all} \quad 0 \leq \alpha \leq 1.$$

Recall that by $\|A\|_{\text{op}}$ we denote the operator norm of a matrix A, that is the largest singular value of A.

Our main result is as follows.

(3.1) Theorem. *Let $A = (a_{ij})$ be an $m \times n$ real matrix, let $b = (\beta_1, \ldots, \beta_n)$ be a real n-vector and let $s > 0$ be a real number. Let*

$$B = sI + \frac{1}{2}A^T A$$

be an $n \times n$ positive definite matrix.

Let $q = e^{-s}$ and let us define a function $F_{A,b,s} : \mathbb{R}^m \longrightarrow \mathbb{R}_+$ by

$$F_{A,b,s}(t) = \prod_{j=1}^{n} \prod_{k=1}^{\infty} \left(1 + 2q^{2k-1} \cos\left(\beta_j + \sum_{i=1}^{m} a_{ij}\tau_i\right) + q^{4k-2}\right),$$
$$\text{where} \quad t = (\tau_1, \ldots, \tau_m).$$

Then

(1) *We have*

$$(2\pi)^{-m/2} \prod_{k=1}^{\infty} \left(1 - q^{2k}\right)^n \int_{\mathbb{R}^m} F_{A,b,s}(t) e^{-\|t\|^2/2} \, dt$$
$$= \sum_{x \in \mathbb{Z}^n} \exp\left\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\right\}.$$

(2) *Suppose that*

$$\|A^T A\|_{\mathrm{op}} \sum_{k=1}^{\infty} \frac{q^{2k-1}}{\left(1 - q^{2k-1}\right)^2} \ \leq \ \frac{1}{2}.$$

Then for every integer $K > 0$ the function $G(t) = G_{A,b,s,K}(t)$ defined by

$$G(t) = e^{-\|t\|^2/2} \prod_{j=1}^{n} \prod_{k=1}^{K} \left(1 + 2q^{2k-1} \cos\left(\beta_j + \sum_{i=1}^{m} a_{ij}\tau_i\right) + q^{4k-2}\right),$$
$$\text{where} \quad t = (\tau_1, \ldots, \tau_m),$$

is log-concave. In particular, the function $F_{A,b,s}(t)e^{-\|t\|^2/2}$ is log-concave.

We note that

$$\sum_{k=1}^{\infty} \frac{q^{2k-1}}{(1 - q^{2k-1})^2} \ \leq \ \frac{1}{(1-q)^2} \sum_{k=1}^{\infty} q^{2k-1} = \frac{q}{(1-q)^2(1-q^2)} = \frac{e^{-s}}{(1 - e^{-s})^2(1 - e^{-2s})}.$$

Consequently, to satisfy the constraint in Part (2), we are allowed to choose A so that

$$\|A^T A\|_{\mathrm{op}} \ \leq \ \frac{1}{2} e^s \left(1 - e^{-s}\right)^2 \left(1 - e^{-2s}\right).$$

We prove Theorem 3.1 in Section 4.

Theorem 3.1 allows us to approximate $\Theta(B)$ and, more generally the sum (1.1.3), by using any of the efficient algorithms for integrating log-concave functions [AK91], [F+94], [FK99], [LV07].

(3.2) Algorithm for computing the theta function. We present an algorithm for computing (1.1.3).

Input: An $n \times n$ positive definite matrix B such that

$$sI \preceq B \preceq \left(s + \frac{e^s}{4} \left(1 - e^{-s}\right)^2 \left(1 - e^{-2s}\right) \right) I \quad \text{for some} \quad s \geq 1,$$

a vector $b \in \mathbb{R}^n$, $b = (\beta_1, \ldots, \beta_n)$, and a number $0 < \epsilon < 1$.

Output: A positive real number approximating

$$\sum_{x \in \mathbb{Z}^n} \exp\left\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\right\}$$

within relative error ϵ.

Algorithm: Let $C = B - sI$. Hence C is a positive definite matrix with

$$\|C\|_{\text{op}} \leq \frac{e^s}{4} \left(1 - e^{-s}\right)^2 \left(1 - e^{-2s}\right).$$

Next, we write

$$C = \frac{1}{2} A^T A \quad \text{so that} \quad B = sI + \frac{1}{2} A^T A$$

for an $m \times n$ matrix A. We can always choose $m = n$ or $m = \operatorname{rank} A$. Hence

$$\left\|A^T A\right\|_{\text{op}} \leq \frac{1}{2} e^s \left(1 - e^{-s}\right)^2 \left(1 - e^{-2s}\right).$$

Let $q = e^{-s}$. For an integer $K = K(\epsilon) > 0$, to be specified in a moment, we define $\widehat{F} : \mathbb{R}^m \longrightarrow \mathbb{R}$ by

$$\widehat{F}(t) = \prod_{j=1}^{n} \prod_{k=1}^{K} \left(1 + 2q^{2k-1} \cos\left(\beta_j + \sum_{i=1}^{m} a_{ij} \tau_i \right) + q^{4k-2} \right)$$
$$\text{for} \quad t = (\tau_1, \ldots, \tau_m)$$

and use any of the efficient algorithms of integration log-concave functions to compute

$$(2\pi)^{-m/2} \prod_{k=1}^{K} \left(1 - q^{2k}\right)^n \int_{\mathbb{R}^m} \widehat{F}(t) e^{-\|t\|^2/2} \, dt$$

within relative error $\epsilon/3$.

We choose K so that the relative error acquired by replacing infinite products

$$\prod_{k=1}^{\infty} \left(1 - q^{2k}\right)^n \quad \text{and} \quad \prod_{k=1}^{\infty} \left(1 + 2q^{2k-1} \cos\left(\beta_j + \sum_{i=1}^{m} a_{ij} \tau_i \right) + q^{4k-2} \right)$$

in Theorem 3.1 by finite ones does not exceed $\epsilon/3$. Since

$$|\ln(1+x)| \ \le \ 2|x| \quad \text{for} \quad -0.5 \ \le \ x \ \le \ 0.5,$$

and $q = e^{-s} \le e^{-1}$, we have

$$\left| \sum_{k=K}^{\infty} \ln\left(1-q^k\right) \right| \ \le \ 2 \sum_{k=K}^{\infty} q^k = \frac{2q^K}{1-q} \ \le 4q^K.$$

Similarly,

$$\begin{aligned} &\left| \sum_{k=K}^{\infty} \ln\left(1 + 2q^{2k-1}\cos\left(\beta_j + \sum_{i=1}^{m} a_{ij}\tau_i\right) + q^{4k-2}\right) \right| \\ &\qquad \le \ \left| \sum_{k=K}^{\infty} \ln\left(1 - 2q^{2k-1} + q^{4k-2}\right) \right| = 2 \left| \sum_{k=K}^{\infty} \ln\left(1-q^{2k-1}\right) \right| \\ &\qquad \le 4 \sum_{k=K}^{\infty} q^{2k-1} = \frac{4q^{2K-1}}{1-q^2} \ \le \ 5q^{2K-1}. \end{aligned}$$

Consequently, to approximate the infinite products in Theorem 3.1 by finite ones within relative error $\epsilon/3$, we can choose $K = O\left(\ln(n/\epsilon)\right)$. We summarize the result as a theorem.

(3.3) Theorem. *Given an $n \times n$ positive definite matrix B satisfying (2.1.1), a vector $b \in \mathbb{R}^n$ and $0 < \epsilon \le 1$, the algorithm of Section 3.2 approximates*

$$\sum_{x \in \mathbb{Z}^n} \exp\left\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\right\}$$

within relative error ϵ in time polynomial in n, s and ϵ^{-1}.

□

4. Proof of Theorem 3.1

The proof of Part (1) is based on the Jacobi identity.

(4.1) Jacobi's formula. For any $0 \le q < 1$ and any $w \in \mathbb{C} \setminus 0$, we have

$$\prod_{k \ge 1} \left(1-q^{2k}\right)\left(1+wq^{2k-1}\right)\left(1+w^{-1}q^{2k-1}\right) = \sum_{\xi \in \mathbb{Z}} w^{\xi} q^{\xi^2}.$$

This is Jacobi's triple product identity, see for example, Section 2.2 of [An98]. Suppose now that

$$w_j \in \mathbb{C} \setminus \{0\} \quad \text{for} \quad j = 1, \ldots, n.$$

Then

$$\prod_{j=1}^{n}\prod_{k\geq 1}\left(1-q^{2k}\right)\left(1+w_jq^{2k-1}\right)\left(1+w_j^{-1}q^{2k-1}\right)$$

$$= \sum_{\substack{x\in\mathbb{Z}^n:\\ x=(\xi_1,\dots,\xi_n)}} q^{\|x\|^2}\prod_{j=1}^{n} w_j^{\xi_j}. \tag{4.1.1}$$

(4.2) Proof of Part (1). For $t=(\tau_1,\dots,\tau_m)$, we choose

$$w_j(t)=\exp\left\{\mathbf{i}\left(\beta_j+\sum_{i=1}^{m}a_{ij}\tau_i\right)\right\}\quad\text{for}\quad j=1,\dots,n$$

in (4.1.1). Using that

$$\left(1+w_j(t)q^{2k-1}\right)\left(1+w_j^{-1}(t)q^{2k-1}\right)=1+\left(w_j(t)+w_j^{-1}(t)\right)q^{2k-1}+q^{4k-2}$$

$$=1+2\cos\left(\beta_j+\sum_{i=1}^{m}a_{ij}\tau_i\right)q^{2k-1}+q^{4k-2}$$

and that

$$\prod_{j=1}^{n}w_j^{\xi_j}=\exp\left\{\mathbf{i}\sum_{j=1}^{n}\beta_j\xi_j+\mathbf{i}\sum_{i=1}^{m}\tau_i\left(\sum_{j=1}^{n}a_{ij}\xi_j\right)\right\},$$

we conclude that

$$F_{A,b,s}(t)\prod_{k=1}^{\infty}\left(1-q^{2k}\right)^n$$

$$=\sum_{\substack{x\in\mathbb{Z}^n:\\ x=(\xi_1,\dots,\xi_n)}} q^{\|x\|^2}\exp\left\{\mathbf{i}\sum_{j=1}^{n}\beta_j\xi_j+\mathbf{i}\sum_{i=1}^{m}\tau_i\left(\sum_{j=1}^{n}a_{ij}\xi_j\right)\right\}.$$

Since

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty}\exp\left\{\mathbf{i}\tau_i\sum_{j=1}^{n}a_{ij}\xi_j\right\}e^{-\tau_i^2/2}\,d\tau_i=\exp\left\{-\frac{1}{2}\left(\sum_{j=1}^{n}a_{ij}\xi_j\right)^2\right\},$$

we get

$$(2\pi)^{-m/2}\prod_{k=1}^{\infty}\left(1-q^{2k}\right)^n\int_{\mathbb{R}^m}F_{A,b,s}(t)e^{-\|t\|^2/2}\,dt$$

$$=\sum_{\substack{x\in\mathbb{Z}^n:\\ x=(\xi_1,\dots,\xi_n)}} q^{\|x\|^2}\exp\left\{-\frac{1}{2}\sum_{i=1}^{m}\left(\sum_{j=1}^{n}a_{ij}\xi_j\right)^2+\mathbf{i}\sum_{j=1}^{n}\beta_j\xi_j\right\}$$

$$=\sum_{x\in\mathbb{Z}^n}q^{\|x\|^2}\exp\left\{-\frac{1}{2}\|Ax\|^2+\mathbf{i}\langle b,x\rangle\right\}=\sum_{x\in\mathbb{Z}^n}\exp\left\{-\langle Bx,x\rangle+\mathbf{i}\langle b,x\rangle\right\},$$

and the proof follows. □

To prove Part (2), we need one technical estimate.

(4.3) Lemma. *Let $0 < q < 1$ and α, β be reals. Then*

$$\frac{d^2}{d\tau^2} \ln\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right) \;\le\; \frac{2\alpha^2 q}{(1-q)^2}.$$

Proof. We have

$$\frac{d}{d\tau} \ln\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right) = -\frac{2\alpha q \sin(\alpha\tau + \beta)}{1 + 2q\cos(\alpha\tau + \beta) + q^2}$$

and

$$\begin{aligned}
&\frac{d^2}{d\tau^2} \ln\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right) \\
= &\quad - \frac{2\alpha^2 q\cos(\alpha\tau + \beta)\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right) + \left(2\alpha q \sin(\alpha\tau + \beta)\right)^2}{\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right)^2} \\
= &- \frac{2\alpha^2 q(1+q^2)\cos(\alpha\tau + \beta) + 4\alpha^2 q^2}{\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right)^2}.
\end{aligned}$$

Now,

$$\left(1 + 2q\cos(\alpha\tau + \beta) + q^2\right)^2 \;\ge\; \left(1 - 2q + q^2\right)^2 = (1-q)^4.$$

Also,

$$\begin{aligned}
2\alpha^2 q(1+q^2)\cos(\alpha\tau + \beta) + 4\alpha^2 q^2 \;&\ge\; -2\alpha^2 q(1+q^2) + 4\alpha^2 q^2 \\
&= 2\alpha^2 q\left(2q - 1 - q^2\right) = -2\alpha^2 q(1-q)^2.
\end{aligned}$$

The proof now follows. □

(4.4) Proof of Part (2). It suffices to prove that the restriction of $G(t)$ onto any affine line

$$\tau_i = \gamma_i \tau + \delta_i \quad \text{for} \quad i = 1, \ldots, m \quad \text{where} \quad \sum_{i=1}^{m} \gamma_i^2 = 1$$

is log-concave. Indeed, let $g(\tau)$ be that restriction. From Lemma 4.3, we get

$$\begin{aligned}
\frac{d^2}{d\tau^2} \ln g(\tau) \;&\le\; -1 + 2\sum_{k=1}^{K} \frac{q^{2k-1}}{\left(1 - q^{2k-1}\right)^2} \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij}\gamma_i\right)^2 \\
&\le -1 + 2\|A^T\|_{\mathrm{op}}^2 \sum_{k=1}^{K} \frac{q^{2k-1}}{\left(1 - q^{2k-1}\right)^2} \\
&= -1 + 2\|A^T A\|_{\mathrm{op}} \sum_{k=1}^{K} \frac{q^{2k-1}}{\left(1 - q^{2k-1}\right)^2} \;\le\; 0
\end{aligned}$$

and hence $\ln g(\tau)$ is concave. The proof now follows. □

5. Integer points in a subspace

Let A be an $m \times n$ integer matrix of $\operatorname{rank} A = m < n$ and let $L = \ker A$ be a subspace, $L \subset \mathbb{R}^n$. Then $\Lambda = \mathbb{Z}^n \cap L$ is a lattice in L. Note that in this case, we do not define Λ by its basis. For $s > 0$, we consider the theta function

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

Our main result is as follows.

(5.1) Theorem. *Suppose that $\|A\|_{\text{op}} \leq \gamma$ for some $\gamma \geq 1$. For $s > 0$ and $t > 0$, let $B = B_{s,t}$ be an $n \times n$ positive definite matrix with the eigenvectors in $L \cup L^\perp$, where $L = \ker A$, and such that the eigenvectors in L have eigenvalue s while the eigenvectors in $L^\perp$ have eigenvalue $s + t$. Then*

$$|\Theta(B) - \Theta_\Lambda(s)| \ \leq \ \exp\left\{-\frac{t}{\gamma^2} + \frac{2ne^{-s}}{1 - e^{-s}}\right\}.$$

(5.2) Example. Let us fix $\delta > 0$ and let

$$s = \left(\frac{1}{2} + \delta\right) \ln n \quad \text{and} \quad t = \frac{e^s}{5} = \frac{n^{\frac{1}{2}+\delta}}{5}. \tag{5.2.1}$$

From Theorem 5.1, we have

$$|\Theta(B) - \Theta_\Lambda(s)| \ \leq \ \exp\left\{-\frac{n^{\frac{1}{2}+\delta}}{5\gamma^2} + \frac{2n^{\frac{1}{2}-\delta}}{1 - n^{-\frac{1}{2}-\delta}}\right\}.$$

As long as $\gamma = o\left(n^\delta\right)$, we get

$$|\Theta(B) - \Theta_\Lambda(s)| = o(1). \tag{5.2.2}$$

When $s \geq 3$, the matrix $B = B_{s,t}$ satisfies (2.1.2) and hence $\Theta(B)$ can be efficiently approximated. Since $\Theta(B) \geq 1$, from (5.2.2) and Theorem 3.3, we obtain a randomized polynomial time algorithm that approximates $\Theta_\Lambda(s)$ within a relative error of $o(1)$ as $n \longrightarrow \infty$.

The proof of Theorem 5.1 is based on the following two lemmas. In the first lemma, we bound from below the distance of a point $x \in \mathbb{Z}^n \setminus \Lambda$ to the subspace L.

(5.3) Lemma. *Let A be an $m \times n$ integer matrix with $\operatorname{rank} A = m < n$ and let $L = \ker A$. For a point $x \in \mathbb{R}^n$, let*

$$\operatorname{dist}(x, L) = \min_{y \in L} \|x - y\|$$

be the Euclidean distance from x to L. Then

$$\operatorname{dist}(x, L) \;\geq\; (\|A\|_{\mathrm{op}})^{-1} \quad \textit{for all} \quad x \in \mathbb{Z}^n \setminus L.$$

Proof. Suppose that $x \in \mathbb{Z}^n \setminus L$. Let $P : \mathbb{R}^n \longrightarrow L^{\perp} = \operatorname{image} A^T$ be the orthogonal projection. Then the matrix of P in the standard coordinates is $A^T(AA^T)^{-1}A$ and hence

$$\operatorname{dist}^2(x, L) = \|P(x)\|^2 = \big\langle A^T(AA^T)^{-1}Ax,\; A^T(AA^T)^{-1}Ax\big\rangle = \big\langle (AA^T)^{-1}Ax,\; Ax\big\rangle.$$

Since A is an integer matrix, x is an integer vector and $Ax \neq 0$, we have $\|Ax\| \geq 1$. Let $\lambda > 0$ be the smallest eigenvalue of the matrix $(AA^T)^{-1}$. Then

$$\big\langle (AA^T)^{-1}Ax,\; Ax\big\rangle \;\geq\; \lambda\|Ax\|^2 \;\geq\; \lambda$$

and hence

$$\operatorname{dist}^2(x, L) \;\geq\; \lambda.$$

On the other hand,

$$\lambda = \big(\|AA^T\|_{\mathrm{op}}\big)^{-1} = (\|A\|_{\mathrm{op}})^{-2},$$

from which the proof follows. □

The next lemma provides some technical estimates for the theta function. For the proof of Theorem 5.1 we need Part (1) only, while Part (2) will be used later.

(5.4) Lemma.

(1) *For $s > 0$, we have*

$$\Theta(sI) = \sum_{x \in \mathbb{Z}^n} e^{-s\|x\|^2} \;\leq\; \exp\left\{\frac{2ne^{-s}}{1 - e^{-s}}\right\}.$$

(2) *For $s > 0$ and*

$$4ne^{-1} \;\geq\; k \;\geq\; 30ne^{-s},$$

we have

$$\sum_{\substack{x \in \mathbb{Z}^n: \\ \|x\|^2 \geq k}} e^{-s\|x\|^2} \;\leq\; e^{-k}.$$

Proof. For $s > 0$, we have

$$\begin{aligned}\Theta(sI) = \left(\sum_{\xi \in \mathbb{Z}} e^{-s\xi^2}\right)^n \;\leq\; \left(1 + 2\sum_{\xi=1}^{\infty} e^{-s\xi}\right)^n &= \left(1 + \frac{2e^{-s}}{1 - e^{-s}}\right)^n \\ = \exp\left\{n \ln\left(1 + \frac{2e^{-s}}{1 - e^{-s}}\right)\right\} \;\leq\; \exp\left\{\frac{2ne^{-s}}{1 - e^{-s}}\right\},&\end{aligned}$$

which proves Part (1).

To prove Part (2), for any $0 < \tau < s$, using Part (1), we get

$$\sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} e^{-s\|x\|^2} \;\leq e^{-\tau k} \sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} e^{-s\|x\|^2} e^{\tau\|x\|^2} \;\leq\; e^{-\tau k}\Theta\big((s-\tau)I\big)$$
$$\leq\; \exp\left\{-\tau k + \frac{2ne^{-(s-\tau)}}{1-e^{-(s-\tau)}}\right\}.$$

Optimizing on τ, we choose

$$\tau = s + \ln\frac{k}{4n}.$$

Since $k \geq 30ne^{-s}$, we have

$$\tau \;\geq\; \ln\frac{30}{4} \;>\; 2$$

and since $k \leq 4ne^{-1}$, we have

$$s - \tau = -\ln\frac{k}{4n} \;\geq\; 1.$$

Therefore,

$$\sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} e^{-s\|x\|^2} \;\leq\; \exp\left\{-\tau k + 4ne^{-(s-\tau)}\right\} = \exp\left\{-(\tau-1)k\right\} \;\leq\; e^{-k},$$

as required. □

Now we are ready to prove Theorem 5.1.

(5.5) Proof of Theorem 5.1.

Applying Lemma 5.3 and Part(1) of Lemma 5.4, we obtain

$$\begin{aligned}
|\Theta(B) - \Theta_\Lambda(s)| &= \sum_{x\in\mathbb{Z}^n\setminus L} \exp\left\{-\langle Bx, x\rangle\right\} \\
&= \sum_{x\in\mathbb{Z}^n\setminus L} \exp\left\{-t\,\mathrm{dist}^2(x,L)\right\} \exp\left\{-s\|x\|^2\right\} \\
&\leq\; \exp\left\{-\frac{t}{\gamma^2}\right\} \sum_{x\in\mathbb{Z}^n} \exp\left\{-s\|x\|^2\right\} \\
&\leq\; \exp\left\{-\frac{t}{\gamma^2} + \frac{2ne^{-s}}{1-e^{-s}}\right\}.
\end{aligned}$$

□

As in Example 5.2, let us fix $0 < \delta < \frac{1}{2}$, define s and t by (5.2.1) and assume that $\|A\|_{\mathrm{op}} = o\left(n^{\delta}\right)$, so that $\Theta_\Lambda(s)$ can be approximated in randomized polynomial time within a relative error of $o(1)$. If there are no points $x \in \Lambda \setminus \{0\}$ with $\|x\|^2 \leq 30n^{\frac{1}{2}-\delta}$ then by Part (2) of Lemma 5.4, we have $\Theta_\Lambda(s) = 1 + o(1)$. On the other hand, if Λ contains many short vectors, then $\Theta_\Lambda(s)$ can be large. For example, if L is a coordinate subspace, $\dim L \geq \alpha n$ for some $0 < \alpha < 1$, so that Λ is identified with $\mathbb{Z}^{\dim L}$, then

$$\Theta_\Lambda(s) \ \geq \ \left(\sum_{\xi \in \mathbb{Z}} e^{-s\xi^2}\right)^{\alpha n} \ \geq \ \left(1 + 2e^{-s}\right)^{\alpha n} = \left(1 + \frac{2}{n^{\frac{1}{2}+\delta}}\right)^{\alpha n} \ \geq \ \exp\left\{\alpha n^{\frac{1}{2}-\delta}\right\}$$

is exponentially large in n. Hence computing $\Theta_\Lambda(s)$ allows us to distinguish the case of L having no short non-zero integer vectors from the case of L having sufficiently many short integer vectors.

6. Lattices containing $\mathbb{Z}^n$

As in Section 5, for a lattice $\Lambda \subset \mathbb{R}^n$, a point $v \in \mathbb{R}^n$ and a number $\tau > 0$, we denote

$$\Theta_\Lambda(\tau, v) = \sum_{u \in \Lambda} \exp\left\{-\tau\|u - v\|^2\right\}.$$

In agreement with our notation in Sections 1-4, when $\Lambda = \mathbb{Z}^n$, we still denote $\Theta_{\mathbb{Z}^n}(\tau, v)$ just by $\Theta(\tau I, v)$ and $\Theta_{\mathbb{Z}^n}(\tau, 0)$ just by $\Theta(\tau I)$, so

$$\Theta(\tau I, v) = \sum_{x \in \mathbb{Z}^n} e^{-\tau\|x-v\|^2} \quad \text{and} \quad \Theta(\tau I) = \sum_{x \in \mathbb{Z}^n} e^{-\tau\|x\|^2}.$$

In this section we prove the following main result.

(6.1) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice such that $\mathbb{Z}^n \subset \Lambda$. Then for $0 < \tau \leq 1$, we have*

$$41e^{-\pi^2/\tau}\operatorname{dist}^2(v, \Lambda) \ \geq \ \ln\frac{\Theta(\tau I)}{\Theta_\Lambda(\tau, v)} \ \geq \ 13e^{-\pi^2/\tau}\operatorname{dist}^2(v, \Lambda) + \ln\det\Lambda.$$

Apart from the additive term of $\ln\det\Lambda$, the formula of Theorem 6.1 provides an estimate of $\operatorname{dist}(v, \Lambda)$ within a constant factor of $\sqrt{41/13} \approx 1.8$. It may happen that as n grows, the additive term becomes asymptotically negligible, and hence the formula of Theorem 6.1 provides an approximation of $\operatorname{dist}(v, \Lambda)$ within a constant factor.

(6.2) Example. A lattice $\Lambda \subset \mathbb{R}^n$ containing $\mathbb{Z}^n$ can be constructed as follows: let $w_1, \ldots, w_n$ be a basis of $\mathbb{Z}^n$ and let $\lambda_1, \ldots, \lambda_n$ be positive integers. Then

$$u_i = \frac{1}{\lambda_i} w_i \quad \text{for} \quad i = 1, \ldots, n \tag{6.2.1}$$

is a basis of a lattice Λ containing $\mathbb{Z}^n$. Moreover, any lattice containing $\mathbb{Z}^n$ can be constructed this way, cf., for example, Chapter I of [Ca97] for the Smith normal form. We have

$$\ln \det \Lambda = -\sum_{i=1}^{n} \ln \lambda_i.$$

Let us consider the case when $\operatorname{dist}^2(v, \Lambda) \geq n^\alpha$ for some $0 < \alpha < 1$. We let

$$\tau = \frac{10\pi^2}{\alpha \ln n},$$

so that

$$e^{-\pi^2/\tau} \operatorname{dist}^2(v, \Lambda) = n^{-0.1\alpha} \operatorname{dist}^2(v, \Lambda) \ \geq \ n^{0.9\alpha}.$$

To make sure that the term $\ln \det \Lambda$ is asymptotically negligible, we choose not more than $n^{0.8\alpha}$ of λ_i in (6.2.1) satisfying $\lambda_i \leq \gamma$ for a constant $\gamma > 1$, fixed in advance, while the rest of λ_i are equal to 1.

Let B be the Gram matrix of the basis $u_1, \ldots, u_n$. In the trivial case, if $w_1, \ldots, w_n$ in (6.2.1) is the standard basis $e_1, \ldots, e_n$, then for large n, the matrix τB satisfies (2.1.4) and hence the ratio $\Theta(\tau I)/\Theta_\Lambda(\tau, v)$ can be approximated in randomized polynomial time. However, the matrix τB would still satisfy (2.1.4) in a less trivial situation, when $w_1, \ldots, w_n$ are close enough to the standard basis, for example, when $w_i = Ae_i$ for some matrix $A \in GL(n, \mathbb{Z})$ where

$$\|A\|_{\text{op}} \ \leq \ \gamma \quad \text{and} \quad \|A^{-1}\|_{\text{op}} \ \leq \ n^{\alpha/21\gamma^2},$$

for a constant $\gamma > 1$, fixed in advance.

It appears essential that we are able to choose τ in the non-smooth range, see Section 2.1.5. Indeed, choosing $\tau \leq \pi^2/\gamma \ln n$ for some $\gamma > 1$ leads to

$$e^{-\pi^2/\tau} \operatorname{dist}^2(v, \Lambda) = o(1)$$

and hence the $\ln \det \Lambda$ additive term cannot be discarded.

We note that the ratio $\Theta_\Lambda(\tau, v)/\Theta_\Lambda(\tau, 0)$ was crucially used by Aharonov and Regev to show that estimating $\operatorname{dist}(v, \Lambda)$ within a factor of $O(\sqrt{n})$ for any lattice $\Lambda \subset \mathbb{R}^n$ lies in NP $\cap$ co-NP [AR05].

To prove Theorem 6.1, we first consider the case of $\Lambda = \mathbb{Z}^n$.

(6.3) Lemma. *For $y \in \mathbb{R}^n$ and $0 < \tau \le 1$, we have*

$$\exp\left\{-41e^{-\pi^2/\tau}\operatorname{dist}^2(y,\mathbb{Z}^n)\right\} \le \frac{\Theta(\tau I, y)}{\Theta(\tau I)} \le \exp\left\{-13e^{-\pi^2/\tau}\operatorname{dist}^2(y,\mathbb{Z}^n)\right\}.$$

Proof. Let $y = (\eta_1, \dots, \eta_n)$. We have

$$\Theta(\tau I, y) = \sum_{x\in\mathbb{Z}^n} \exp\left\{-\tau\|x-y\|^2\right\} = \prod_{i=1}^{n}\sum_{\xi\in\mathbb{Z}} \exp\left\{-\tau(\xi-\eta_i)^2\right\}$$

and similarly,

$$\Theta(\tau I) = \sum_{x\in\mathbb{Z}^n} \exp\left\{-\tau\|x\|^2\right\} = \prod_{i=1}^{n}\sum_{\xi\in\mathbb{Z}} \exp\left\{-\tau\xi^2\right\}.$$

Translating y by an integer vector, without loss of generality we assume that $y = (\eta_1, \dots, \eta_n)$ where

$$|\eta_i| \le \frac{1}{2} \quad \text{for} \quad i = 1, \dots, n.$$

Then

$$\operatorname{dist}^2(y,\mathbb{Z}^n) = \|y\|^2 = \sum_{i=1}^{n}\eta_i^2.$$

By the reciprocity relation (1.1.4), we get

$$\Theta(\tau I, y) = \frac{\pi^{n/2}}{\tau^{n/2}}\prod_{i=1}^{n}\sum_{\xi\in\mathbb{Z}} \exp\left\{-\pi^2\tau^{-1}\xi^2 + 2\pi\mathbf{i}\xi\eta_i\right\} \quad \text{and}$$

$$\Theta(\tau I) = \frac{\pi^{n/2}}{\tau^{n/2}}\prod_{i=1}^{n}\sum_{\xi\in\mathbb{Z}} \exp\left\{-\pi^2\tau^{-1}\xi^2\right\}.$$

Denoting

$$q = e^{-\pi^2/\tau},$$

from the Jacobi identity (4.1), we get

$$\begin{aligned}
&\sum_{\xi\in\mathbb{Z}} \exp\left\{-\pi^2\tau^{-1}\xi^2 + 2\pi\mathbf{i}\xi\eta_i\right\} \\
&\quad= \prod_{k=1}^{\infty}\left(1-q^{2k}\right)\left(1+\exp\left\{2\pi\mathbf{i}\eta_i\right\}q^{2k-1}\right)\left(1+\exp\left\{-2\pi\mathbf{i}\eta_i\right\}q^{2k-1}\right) \\
&\quad= \prod_{k=1}^{\infty}\left(1-q^{2k}\right)\left(1+2q^{2k-1}\cos(2\pi\eta_i)+q^{4k-2}\right)
\end{aligned}$$

and, similarly,

$$\sum_{\xi\in\mathbb{Z}} \exp\left\{-\pi^2\tau^{-1}\xi^2\right\} = \prod_{k=1}^{\infty}\left(1-q^{2k}\right)\left(1+2q^{2k-1}+q^{4k-2}\right).$$

Summarizing,

$$\begin{aligned}\frac{\Theta(\tau I, y)}{\Theta(\tau I)} =& \prod_{i=1}^{n}\prod_{k=1}^{\infty}\frac{1+2q^{2k-1}\cos(2\pi\eta_i)+q^{4k-2}}{1+2q^{2k-1}+q^{4k-2}}\\ =& \prod_{i=1}^{n}\prod_{k=1}^{\infty}\left(1-\frac{2q^{2k-1}\left(1-\cos(2\pi\eta_i)\right)}{\left(1+q^{2k-1}\right)^2}\right).\end{aligned}$$

We have

$$7\eta^2 \;\le\; 1-\cos(2\pi\eta) \;\le\; 20\eta^2 \quad \text{for} \quad -\frac{1}{2}\le\eta\le\frac{1}{2}.$$

Since

$$q = e^{-\pi^2/\tau} \;\le\; e^{-\pi^2} \;<\; 10^{-4} \quad \text{and} \quad |\eta_i| \;\le\; \frac{1}{2},$$

we have

$$\frac{\eta_i^2 q^{2k-1}}{\left(1+q^{2k-1}\right)^2} \;\le\; \frac{1}{4}10^{-4}$$

and we can further write

$$\prod_{i=1}^{n}\prod_{k=1}^{\infty}\left(1-\frac{40\eta_i^2q^{2k-1}}{\left(1+q^{2k-1}\right)^2}\right) \;\le\; \frac{\Theta(\tau I,y)}{\Theta(\tau I)} \;\le\; \prod_{i=1}^{n}\prod_{k=1}^{\infty}\left(1-\frac{14\eta_i^2q^{2k-1}}{\left(1+q^{2k-1}\right)^2}\right) \tag{6.3.1}$$

(note that all factors in the products are positive).

Using that

$$\ln(1-\alpha) \;\le\; -\alpha \quad \text{for} \quad 0\le\alpha<1,$$

we conclude that

$$\begin{aligned}\prod_{k=1}^{\infty}\left(1-\frac{14\eta_i^2q^{2k-1}}{(1+q^{2k-1})^2}\right) &= \exp\left\{\sum_{k=1}^{\infty}\ln\left(1-\frac{14\eta_i^2q^{2k-1}}{(1+q^{2k-1})^2}\right)\right\}\\ &\le\; \exp\left\{-\sum_{k=1}^{\infty}\frac{14\eta_i^2q^{2k-1}}{(1+q^{2k-1})^2}\right\} \;\le\; \exp\left\{-13\eta_i^2\sum_{k=1}^{\infty}q^{2k-1}\right\}\\ &= \exp\left\{-\frac{13\eta_i^2q}{1-q^2}\right\} \;\le\; \exp\left\{-13\eta_i^2q\right\}.\end{aligned} \tag{6.3.2}$$

Similarly, using that

$$\ln(1-\alpha) \;\ge\; -1.01\alpha \quad \text{for} \quad 0\le\alpha\le 0.001,$$

we conclude that

$$\begin{aligned}\prod_{k=1}^{\infty}\left(1-\frac{40\eta_i^2q^{2k-1}}{(1+q^{2k-1})^2}\right) &= \exp\left\{\sum_{k=1}^{\infty}\ln\left(1-\frac{40\eta_i^2q^{2k-1}}{(1+q^{2k-1})^2}\right)\right\}\\ &\geq\ \exp\left\{-\sum_{k=1}^{\infty}\frac{40.5\eta_i^2q^{2k-1}}{(1+q^{2k-1})^2}\right\}\ \geq\ \exp\left\{-40.5\eta_i^2\sum_{k=1}^{\infty}q^{2k-1}\right\}\\ &= \exp\left\{-\frac{40.5\eta_i^2q}{1-q^2}\right\}\ \geq\ \exp\left\{-41\eta_i^2q\right\}.\end{aligned} \tag{6.3.3}$$

Summarizing, from (6.3.1)–(6.3.3) we infer that

$$\frac{\Theta(\tau I,y)}{\Theta(\tau I)}\ \leq\ \prod_{i=1}^{n}\exp\left\{-13\eta_i^2q\right\}=\exp\left\{-13q\sum_{i=1}^{n}\eta_i^2\right\}=\exp\left\{-13q\,\mathrm{dist}^2\left(y,\mathbb{Z}^n\right)\right\}$$

and

$$\frac{\Theta(\tau I,y)}{\Theta(\tau I)}\ \geq\ \prod_{i=1}^{n}\exp\left\{-41\eta_i^2q\right\}=\exp\left\{-41q\sum_{i=1}^{n}\eta_i^2\right\}=\exp\left\{-41q\,\mathrm{dist}^2\left(y,\mathbb{Z}^n\right)\right\},$$

which concludes the proof. □

Now we are ready to prove Theorem 6.1.

(6.4) Proof of Theorem 6.1. Let $u_i, i\in I$ be the coset representatives of the quotient $\Lambda/\mathbb{Z}^n$, so that Λ is represented as a disjoint union

$$\Lambda=\bigcup_{i\in I}(u_i+\mathbb{Z}^n)\quad\text{and}\quad|I|=\frac{1}{\det\Lambda}. \tag{6.4.1}$$

Then

$$\begin{aligned}\Theta_\Lambda(\tau,v)&=\sum_{u\in\Lambda}\exp\left\{-\tau\|u-v\|^2\right\}=\sum_{i\in I}\sum_{x\in\mathbb{Z}^n}\exp\left\{-\tau\|u_i+x-v\|^2\right\}\\ &=\sum_{i\in I}\Theta(\tau I,v-u_i).\end{aligned} \tag{6.4.2}$$

On the other hand,

$$\mathrm{dist}(v,\Lambda)=\min_{i\in I}\mathrm{dist}\left(v,u_i+\mathbb{Z}^n\right)=\min_{i\in I}\mathrm{dist}\left(v-u_i,\mathbb{Z}^n\right).$$

By Lemma 6.3, we have

$$\Theta(\tau I,v-u_i)\ \leq\ \exp\left\{-13e^{-\pi^2/\tau}\,\mathrm{dist}^2\left(v-u_i,\mathbb{Z}^n\right)\right\}\Theta(\tau I)$$

and hence

$$\Theta(\tau I, v - u_i) \;\le\; \exp\Big\{-13e^{-\pi^2/\tau}\operatorname{dist}^2(v,\Lambda)\Big\}\,\Theta(\tau I).$$

Therefore, by (6.4.2) we have

$$\Theta_\Lambda(\tau, v) \;\le\; |I|\exp\Big\{-13e^{-\pi^2/\tau}\operatorname{dist}^2(v,\Lambda)\Big\}\,\Theta(\tau I)$$

and from (6.4.1) we obtain

$$\frac{\Theta_\Lambda(\tau, v)}{\Theta(\tau I)} \;\le\; (\det\Lambda)^{-1}\exp\Big\{-13e^{-\pi^2/\tau}\operatorname{dist}^2(v,\Lambda)\Big\}. \tag{6.4.3}$$

We have

$$\operatorname{dist}(v,\Lambda) = \operatorname{dist}(v - u_{i_0}, \mathbb{Z}^n) \quad \text{for some} \quad i_0 \in I.$$

Therefore, by Lemma 6.3,

$$\Theta(\tau I, v - u_{i_0}) \;\ge\; \exp\Big\{-41e^{-\pi^2/\tau}\operatorname{dist}^2(v,\Lambda)\Big\}\,\Theta(\tau I).$$

Hence by (6.4.2)

$$\frac{\Theta_\Lambda(\tau, v)}{\Theta(\tau I)} \;\ge\; \exp\Big\{-41e^{-\pi^2/\tau}\operatorname{dist}^2(v,\Lambda)\Big\}. \tag{6.4.4}$$

Combining (6.4.3)–(6.4.4), we complete the proof. □

7. Sampling from the discrete Gaussian measure

(7.1) Gaussian measure on lattices. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $v \in \mathbb{R}^n$. In this section, we use the shorthand

$$\Theta_\Lambda(v) = \sum_{u\in\Lambda} e^{-\|u-v\|^2} \quad \text{and} \quad \Theta_\Lambda(0) = \sum_{u\in\Lambda} e^{-\|u\|^2}.$$

We consider the discrete Gaussian probability measure on Λ defined by

$$\mathbf{P}(u) = \frac{\exp\{-\|u-v\|^2\}}{\Theta_\Lambda(v)} \quad \text{for} \quad u \in \Lambda. \tag{7.1.1}$$

Our goal is to sample a point $u \in \Lambda$ from a probability distribution that is ϵ-close in the total variation distance to (7.1.1).

Let $u_1, \ldots, u_n$ be a basis of Λ, so that every point $u \in \mathbb{R}^n$ can be uniquely written as

$$u = \xi_1 u_1 + \ldots + \xi_n u_n \quad \text{for some} \quad \xi_1, \ldots, \xi_n \in \mathbb{R}, \tag{7.1.2}$$

and $u \in \Lambda$ if and only if $\xi_1, \dots, \xi_n$ are integer.

The general design of the algorithm is the same as in [G+08] and [Pe10]: we consecutively sample the coordinates $\xi_n, \xi_{n-1}, \dots, \xi_1$ of u. For that, we compute the conditional distribution of ξ_{n-k} for fixed $\xi_n, \dots, \xi_{n-k+1}$.

For $\alpha \in \mathbb{Z}$, let $H_\alpha \subset \mathbb{R}^n$ be the affine hyperplane defined by the equation $\xi_n = \alpha$ in (7.1.2). Let $\Lambda_\alpha = \Lambda \cap H_\alpha$. We identify H_α with $\mathbb{R}^{n-1}$ by choosing the origin at a point of Λ_α, so that $\Lambda_\alpha \subset H_\alpha$ becomes a lattice. The general idea of the algorithm is to compute $\mathbf{P}(u \in H_\alpha)$, sample $\alpha \in \mathbb{Z}$ from the computed probability distribution, assign $\xi_n = \alpha$ and then iterate, until all coordinates are sampled.

We will use the following inequality from [Ba03] and [AR05]:

$$\Theta_\Lambda(v) \;\le\; \Theta_\Lambda(0) \;\le\; \exp\left\{\operatorname{dist}^2(v,\Lambda)\right\} \Theta_\Lambda(v) \quad \text{for all} \quad v \in \mathbb{R}^n. \tag{7.1.3}$$

The following lemma summarizes various technical estimates that we need.

(7.2) Lemma. *Let v_α be the orthogonal projection of v onto H_α, so that*

$$\|v - v_\alpha\| = \operatorname{dist}(v, H_\alpha).$$

(1) *We have*

$$\mathbf{P}(\xi_n = \alpha) = \mathbf{P}(u \in H_\alpha) = \exp\left\{-\|v - v_\alpha\|^2\right\} \frac{\Theta_{\Lambda_\alpha}(v_\alpha)}{\Theta_\Lambda(v)};$$

(2) *We have*

$$\mathbf{P}(\xi_n = \alpha) \;\le\; \exp\left\{\operatorname{dist}^2(v,\Lambda) - \|v - v_\alpha\|^2\right\};$$

(3) *Let B be the Gram matrix of $u_1, \dots, u_n$ and suppose that*

$$\lambda_{\min} I \;\preceq\; B \;\preceq\; \lambda_{\max} I$$

for some $\lambda_{\max} \ge \lambda_{\min} > 0$. Let

$$v = \eta_1 u_1 + \ldots + \eta_n u_n$$

for some real $\eta_1, \dots, \eta_n$. Then

$$\mathbf{P}(\xi_n = \alpha) \;\le\; \exp\left\{\frac{n\lambda_{\max}}{4} - \lambda_{\min}(\eta_n - \alpha)^2\right\}.$$

(4) *Suppose that the Gram matrix B of $u_1, \dots, u_n$ satisfies the condition of Part (3) for some $\lambda_{\max} \ge \lambda_{\min} > 0$. Then the Gram matrix B' of $u_1, \dots, u_{n-1}$ satisfies the condition with the same $\lambda_{\max}$ and $\lambda_{\min}$.*

Proof. For every $u \in H_\alpha$, by the Pythagoras Theorem, we have

$$\|u - v\|^2 = \|v - v_\alpha\|^2 + \|v_\alpha - u\|^2.$$

Hence

$$\sum_{u \in \Lambda_\alpha} \exp\left\{-\|u - v\|^2\right\} = \exp\left\{-\|v - v_\alpha\|^2\right\} \sum_{u \in \Lambda_\alpha} \exp\left\{-\|u - v_\alpha\|^2\right\},$$

and the proof of Part (1) follows.

To prove Part (2), by applying (7.1.3) we get

$$\Theta_{\Lambda_\alpha}(v_\alpha) \ \le \ \Theta_{\Lambda_\alpha}(0) = \Theta_{\Lambda_0}(0) \ \le \ \Theta_\Lambda(0) \ \le \ \Theta_\Lambda(v) \exp\left\{\mathrm{dist}^2(v, \Lambda)\right\},$$

and the proof follows from Part (1).

Next, we prove Part (3). For $i = 1, \ldots, n$, let ν_i be the integer nearest to η_i, so that $|\eta_i - \nu_i| \le \frac{1}{2}$ and let $u = \nu_1 u_1 + \ldots + \nu_n u_n$, so that $u \in \Lambda$. Let

$$y = (\eta_1 - \nu_1, \ldots, \eta_n - \nu_n).$$

Then

$$\mathrm{dist}^2(v, \Lambda) \ \le \ \|v - u\|^2 = \langle By, y\rangle \ \le \ \lambda_{\max}\|y\|^2 \ \le \ \frac{\lambda_{\max} n}{4}. \tag{7.2.1}$$

Let w be a unit vector orthogonal to $u_1, \ldots, u_{n-1}$. Then

$$\|v - v_\alpha\|^2 = \mathrm{dist}^2(v, H_\alpha) = (\langle v, w\rangle - \langle v_\alpha, w\rangle)^2 = \langle u_n, w\rangle^2 (\eta_n - \alpha)^2. \tag{7.2.2}$$

To bound $\langle u_n, w\rangle^2$, we consider the $n \times n$ matrix A having vectors $u_1, \ldots, u_n$ as rows. Then $B = AA^T$ and since the eigenvalues of the matrices AA^T and $A^T A$ coincide (the matrices are similar), we also have

$$\lambda_{\min} I \ \preceq \ A^T A, \tag{7.2.3}$$

Now, $Aw = \langle u_n, w\rangle e_n$, where e_n is the n-th standard basis vector and hence $A^T A w = \langle u_n, w\rangle u_n$. From (7.2.3), we obtain that

$$\langle A^T A w, w\rangle = \langle u_n, w\rangle^2 \ \ge \ \lambda_{\min}. \tag{7.2.4}$$

Combining (7.2.1), (7.2.2), (7.2.4) and Part (2), we complete the proof of Part (3).

To prove Part (4), we identify $\mathbb{R}^{n-1}$ with the coordinate subspace of $\mathbb{R}^n$, consisting of the points $x = (\xi_1, \ldots, \xi_n)$ where $\xi_n = 0$. The condition on the matrix B says that

$$\lambda_{\min}\|x\|^2 \ \le \ \langle Bx, x\rangle \ \le \ \lambda_{\max}\|x\|^2 \quad \text{for} \quad x \in \mathbb{R}^n,$$

while the same condition for B' says that the above inequality holds for $x \in \mathbb{R}^{n-1} \subset \mathbb{R}^n$. □

Now we are ready to present the sampling algorithm.

(7.3) Algorithm for sampling from the discrete Gaussian distribution.

Input: A basis $u_1, \dots, u_n$ of a lattice Λ such that the Gram matrix B of $u_1, \dots, u_n$ satisfies

$$\lambda_{\min} I \preceq B \preceq \lambda_{\max} I$$

for some $\lambda_{\max} \geq \lambda_{\min} > 0$ such that

$$\lambda_{\min} \geq \pi^2 \left(s + \frac{e^s}{4} \left(1 - e^{-s}\right) \left(1 - e^{-2s}\right) \right)^{-1} \quad \text{and} \quad \lambda_{\max} \leq \pi^2 s^{-1}$$

for some $s \geq 1$, a point $v \in \mathbb{R}^n$ and $0 < \epsilon \leq 1$.

Output: A random point u from a distribution μ on Λ such that

$$\frac{1}{2} \sum_{u \in \Lambda} |\mu(u) - \mathbf{P}(u)| \leq \epsilon, \quad \text{where} \quad \mathbf{P}(u) = \frac{\exp\left\{-\|u - v\|^2\right\}}{\Theta_\Lambda(v)}.$$

Algorithm:

Step 0: Let

$$v = \eta_1 u_1 + \ldots + \eta_n u_n.$$

From Part (3) of Lemma 7.2, compute an integer $l \geq 1$,

$$l = O\left(\frac{n}{\lambda_{\min}} \ln \frac{n}{\epsilon} \right),$$

such that for $u = \xi_1 u_1 + \ldots + \xi_n u_n$, $u \in \Lambda$, one has

$$\mathbf{P}\Big(|\xi_i - \eta_i| > l \quad \text{for some} \quad i = 1, \dots, n \Big) < \frac{\epsilon}{10n}.$$

For $k = 1, \dots, n$ perform the following steps.

Step k: The input of Step k is the lattice $\Lambda^{(k)} \subset \mathbb{R}^{n-k+1}$ with basis $u_1, \dots, u_{n-k+1}$, where $\mathbb{R}^{n-k+1}$ is identified with span $(u_1, \dots, u_{n-k+1})$, and a point $v^{(k)} \in \mathbb{R}^{n-k+1}$,

$$v^{(k)} = \eta_1^{(k)} u_1^{(k)} + \ldots + \eta_{n-k+1}^{(k)} u_{n-k+1}.$$

When $k = 1$, we have $\Lambda^{(1)} = \Lambda$ and $v^{(1)} = v$. For $\alpha \in \mathbb{Z}$ such that

$$|\alpha - \eta_{n-k+1}| \leq l,$$

compute the probabilities that $\xi_{n-k+1} = \alpha$ within relative error $\epsilon/10n$ as in Part (1) of Lemma 7.2. To compute theta functions, use the algorithm of Section 3.2 and the reciprocity relation (1.1.4). Sample a value $\xi_{n-k+1} = \alpha$ from the resulting probability distribution. If $k < n$, let $v^{(k+1)} = v_\alpha^{(k)}$ and go to Step $k + 1$.

At the end of Step n, we have integers $\xi_1, \dots, \xi_n$. Output

$$u = \xi_1 u_1 + \ldots + \xi_n u_n.$$

We state the result as a theorem.

(7.4) Theorem. *The algorithm of Section 7.3 samples a point $u \in \Lambda$ from a distribution which is ϵ-close in the total variation distance to the discrete Gaussian distribution (7.1.1) in time polynomial in n, ϵ^{-1} and $\lambda_{\min}^{-1}$.*

□

(7.5) The smooth case. As we mentioned in Section 2.4, the algorithm follows the general scheme of Peikert [Pe10]. The difference is that [Pe10] deals with the smooth range, when $B \preceq sI$ with $s \ll (\ln n)^{-1}$ so that the value of $\Theta_\Lambda(v)$ does not significantly depend on the choice of $v \in \mathbb{R}^n$. Hence there is no need to compute values of the theta function, and one needs to sample α from the distribution where

$$\mathbf{P}\left(\xi_{n-k+1} = \alpha\right) \sim \exp\left\{-\|v^{(k)} - v_\alpha^{(k)}\|^2\right\}. \tag{7.5.1}$$

Another computational advantage of the smooth case in that the distribution (7.5.1) is well-approximated by a continuous Gaussian distribution. As a result, the complexity of sampling ξ_{n-k+1} does not depend badly on the length of an interval for ξ_{n-k+1} and so there is no dependence on $\lambda_{\min}$ that we have in Theorem 7.4. It appears that once we leave the smooth range, we do need to compute theta functions, and the dependence on $\lambda_{\min}$ appears to be unavoidable.

8. The smooth range

Let us fix $\gamma > 1$. In this section, we present a fully polynomial time approximation scheme (FPTAS) for computing (1.1.3) when B is an $n \times n$ positive definite matrix of a sufficiently large size $n \geq n_0(\gamma)$ satisfying

$$sI \ \preceq \ B \quad \text{where} \quad s \ \geq \ \gamma \ln n.$$

Thus we present a deterministic algorithm that for any $0 < \epsilon \leq 1$ approximates (1.1.3) within relative error ϵ in time polynomial in ϵ^{-1} and n. From the reciprocity relation (1.1.4), we immediately get an FPTAS for approximating $\Theta(B, y)$ provided

$$B \ \preceq \ sI \quad \text{where} \quad s \ \leq \ \frac{\pi^2}{\gamma \ln n} I$$

as long as $n \geq n_0(\gamma)$. The results of this section are likely to be known in some form, but since we are unable to provide a reference, we summarize them here for completeness.

The algorithm is based on the following simple result.

(8.1) Theorem. *Fix $\gamma > 1$ and let B be an $n \times n$ be positive definite matrix such that*

$$sI \ \preceq \ B \quad \textit{where} \quad s \ \geq \ \gamma \ln n.$$

(1) *For $n \geq 2$ and for all integer $k \geq 1$, we have*

$$\sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} \exp\{-\langle Bx, x\rangle\} \;\leq\; 60n^{(1-\gamma)k}.$$

(2) *Let*

$$n_0(\gamma) = \exp\left\{\frac{5}{\gamma-1}\right\}.$$

Then for any $n \geq n_0(\gamma)$ and any $b \in \mathbb{R}^n$, we have

$$\left|-1 + \sum_{x\in\mathbb{Z}^n} \exp\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\}\right| \;\leq\; \frac{1}{2}.$$

(3) *For any integer $k \geq 1$, we have*

$$\left|x \in \mathbb{Z}^n :\; \|x\|^2 \leq k \;\right| \;\leq\; (2n+2)^k.$$

Proof. The proof of Part (1) is similar to that of Lemma 5.4. For $0 < \tau < s$, we have

$$\sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} \exp\{-\langle Bx, x\rangle\} \;\leq\; \sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} e^{-s\|x\|^2} \;\leq\; e^{-\tau k} \sum_{\substack{x\in\mathbb{Z}^n:\\ \|x\|^2\geq k}} e^{-s\|x\|^2} e^{\tau\|x\|^2}$$

$$\leq\; e^{-\tau k}\Theta\big((s-\tau)I\big) \;\leq\; \exp\left\{-\tau k + \frac{2ne^{-(s-\tau)}}{1-e^{-(s-\tau)}}\right\},$$

where the last inequality is from Part (1) of Lemma 5.4. We choose

$$\tau = (\gamma-1)\ln n.$$

Since $s - \tau \geq \ln n$, we obtain

$$\exp\left\{-\tau k + \frac{2ne^{-(s-\tau)}}{1-e^{-(s-\tau)}}\right\} \leq \exp\left\{-\tau k + \frac{2}{1-n^{-1}}\right\} \;\leq\; 60n^{(1-\gamma)k},$$

which completes the proof of Part (1).

Part (2) follows from Part (1) for $k = 1$, since for $n \geq n_0(\gamma)$ we have $60n^{1-\gamma} \leq \frac{1}{2}$.

To prove Part (3), letting $x = (\xi_1, \ldots, \xi_n)$ and $\eta_i = \xi_i^2$, we observe that the number non-negative integer solutions to the inequality $\eta_1 + \ldots + \eta_n \leq k$ is

$$\binom{n+k}{k} = \frac{(n+k)(n+k-1)\cdots(n+1)}{k(k-1)\cdots 1} \;\leq\; (n+1)^k.$$

Since each of at most k positive η_i correspond to at most two values $\pm\xi_i$, the bound follows.

□

Now we are ready to present the algorithm.

(8.2) The algorithm. Fix $\gamma > 1$ and

$$n_0 = \exp\left\{\frac{5}{\gamma - 1}\right\}.$$

Input: For $n \geq n_0(\gamma)$, an $n \times n$ positive definite matrix B such that $sI \preceq B$ for some $s \geq \gamma \ln$, a vector $b \in \mathbb{R}^n$ and $0 < \epsilon < 1$.

Output: A number approximating

$$\sum_{x \in \mathbb{Z}^n} \exp\left\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\right\} \tag{8.2.1}$$

within relative error ϵ.

Algorithm: From Parts (1) and (2) of Theorem 1, choose

$$k = O\left(\frac{\ln(1/\epsilon)}{(\gamma - 1)\ln n}\right),$$

so that

$$\sum_{\substack{x \in \mathbb{Z}^n: \\ \|x\|^2 \leq k}} \exp\left\{-\langle Bx, x\rangle + \mathbf{i}\langle b, x\rangle\right\} \tag{8.2.2}$$

approximates (8.2.1) within relative error ϵ, and compute (8.2.2).

From Part (3) of Theorem 8.1, the sum (8.2.2) contains $(1/\epsilon)^{O\left(\frac{1}{\gamma-1}\right)}$ terms.

Acknowledgment

The author is grateful to the anonymous referees for their criticism and suggestions.

References

[A+15] D. Aggarwal, D. Dadush, O. Regev and N. Stephens-Davidowitz, *Solving the shortest vector problem in 2^n time via discrete Gaussian sampling (extended abstract)*, STOC'15–Proceedings of the 2015 ACM Symposium on Theory of Computing, ACM, New York, 2015, pp. 733–742.

[Aj96] M. Ajtai, *Generating hard instances of lattice problems (extended abstract)*, Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996), ACM, New York, 1996, pp. 99–108.

[A+01] M. Ajtai, R. Kumar and D. Sivakumar, *A sieve algorithm for the shortest lattice vector problem*, Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, ACM, New York, 2001, pp. 601–610.

[AK91] D. Applegate and R. Kannan, *Sampling and integration of near log-concave functions*, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, ACM, New York, 1991, pp. 156–163.

[An98] G.E. Andrews, *The Theory of Partitions. Reprint of the 1976 original*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1998.

[AR05] D. Aharonov and O. Regev, *Lattice problems in NP ∩ coNP*, Journal of the ACM **52** (2005), no. 5, 749–765.

[Ba93] W. Banaszczyk, *New bounds in some transference theorems in the geometry of numbers*, Mathematische Annalen **296** (1993), no. 4, 625–635.

[BL61] R. Bellman and L. R. Sherman, *The reciprocity formula for multidimensional theta functions*, Proceedings of the American Mathematical Society **12** (1961), 954–961.

[Ca97] J.W.S. Cassels, *An Introduction to the Geometry of Numbers. Corrected reprint of the 1971 edition*, Classics in Mathematics, Springer-Verlag, Berlin, 1997.

[D+03] I. Dinur, G. Kindler, R. Raz and S. Safra, *Approximating CVP to within almost-polynomial factors is NP-hard*, Combinatorica **23** (2003), no. 2, 205–243.

[FK99] A. Frieze and R. Kannan, *Log-Sobolev inequalities and sampling from log-concave distributions*, The Annals of Applied Probability **9** (1999), no. 1, 14–26.

[F+94] A. Frieze, R. Kannan, and N. Polson, *Sampling from log-concave distributions*, The Annals of Applied Probabability **4** (1994), no. 3, 812–837.

[G+08] C. Gentry, C. Peikert and V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions [extended abstract]*, STOC'08, ACM, New York, 2008, pp. 197–206.

[G+93] M. Grötschel, L. Lovász and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization. Second edition*, Algorithms and Combinatorics, **2**, Springer-Verlag, Berlin, 1993.

[Kh05] S. Khot, *Hardness of approximating the shortest vector problem in lattices*, Journal of the ACM **52** (2005), no. 5, 789–808.

[LV07] L. Lovász and S. Vempala, *The geometry of logconcave functions and sampling algorithms*, Random Structures & Algorithms **30** (2007), no. 3, 307–358.

[M+21] S.T. McCormick, B. Peis, R. Scheidweiler and F. Vallentin, *A polynomial time algorithm for solving the closest vector problem in zonotopal lattices*, SIAM Journal on Discrete Mathematics **35** (2021), no. 4, 2345–2356.

[MG02] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems. A cryptographic perspective*, The Kluwer International Series in Engineering and Computer Science, **671**, Kluwer Academic Publishers, Boston, MA, 2002.

[MR07] D. Micciancio and O. Regev, *Worst-case to average-case reductions based on Gaussian measures*, SIAM Journal on Computing **37** (2007), no. 1, 267–302.

[MR09] D. Micciancio and O. Regev, *Lattice-based cryptography*, Post-Quantum Cryptography, Springer, Berlin, 2009, pp. 147–191.

[M07a] D. Mumford, *Tata Lectures on Theta. I. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman*, Reprint of the 1983 edition, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007.

[M07b] D. Mumford, *Tata Lectures on Theta. II. Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura*, Reprint of the 1984 original, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007.

[M07c] D. Mumford, *Tata Lectures on Theta. III. With collaboration of Madhav Nori and Peter Norman*, Reprint of the 1991 original, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2007.

[Pe10] C. Peikert, *An efficient and parallel Gaussian sampler for lattices*, Advances in cryptology–CRYPTO 2010, Lecture Notes in Computer Science, vol. 6223, Springer, Berlin, 2010, pp. 80–97.

[RS17] O. Regev and N. Stephens-Davidowitz, *An inequality for Gaussians on lattices*, SIAM Journal on Discrete Mathematics **31** (2017), no. 2, 749–757.

[S+11] N.J.A. Sloane, V.A. Vaishampayan and S.I.R. Costa, *A note on projecting the cubic lattice*, Discrete & Computational Geometry **46** (2011), no. 3, 472–478.

[Sc87] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoretical Computer Science **53** (1987), no. 2-3, 201–224.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA

E-mail address: barvinok@umich.edu