PROVING THETA FUNCTION BY USING INTEGRALS

Gaddam Venkat Reddy
,Department of Mathematics,College of Natural and Computational Sciences,
JIGJIGA UNIVERSITY,ETHIOPIA
Mail Id: gvreddy16673@gmail.com

ABSTRACT

Let f : $R^n \longrightarrow R$ be a positive definite quadratic form and let $y \in R^n$ be point. We present a fully polynomial randomized approximation scheme (FPRAS) for computing ,$\sum_{x\varepsilon z^n} e^{-f(x)}$, provided the eigenvalues of f lie in the interval roughly between s and e^s and for computing $\sum_{x\varepsilon z^n} e^{-f(x-y)}$ 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 Rn, and to compute the second sum, we use the reciprocity relation for theta functions. Choosing s ∼ log n, we apply the results to test the existence of sufficiently many short integer vectors in a given subspace L ⊂ Rn or in the vicinity of L.

1.INTRODUCTION AND MAIN RESULTS:

(1.1) Theta function. Let f : $R^n \longrightarrow R+$ be a positive definite quadratic form, so

$$f(x) = (Bx,x) \qquad \text{for} \qquad x \in R^n,$$

where B is an $n \times n$ positive definite matrix and h·,·i is the standard scalar product in R^n. We consider the problem of efficient computing (approximating) the sum

$$\text{(1.1.1)} \qquad \Theta(B) = \sum_{x\varepsilon z^n} e^{-f(x)} = \sum_{x\varepsilon z^n} e^{-(Bx,x)} \quad ,$$

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

$$\text{(1.1.2)} \qquad \Theta(B,y) = \sum_{x\varepsilon z^n} e^{-f(x,y)} = \sum_{x\varepsilon z^n} e^{-(B(x-y),x-y)} \quad ,$$

Together with (1.1.1) and (1.1.2), we also compute the sum $\sum_{x\varepsilon z^n} e$

$$\text{(1.1.3)} \qquad \sum_{x\varepsilon z^n} exp\{-(Bx,x)+i(b,x)\} \quad ,$$

where $b \in R^n$ and $i^2 = -1$. 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]. The reciprocity relation states that

$$\sum_{x \varepsilon z^n} exp\{-\pi(B(x-y), x-y)\}$$

(1.1.4) $$\frac{1}{\sqrt{det}} \sum_{u\varepsilon z_n} \exp\{-\Pi(B^{-1}x, x) + 2\Pi i(x, y)\}$$

see, for example, [BL61].

One motivation to study (1.1.1) and (1.1.2) from the computational point of view comes from connections with algorithmic problems on lattices.

(1.2) Connections to algorithmic problems on lattices. Let $\Lambda \subset R^n$ be a lattice, that is a discrete additive subgroup of R n such that span(Λ) = R^n. Equivalently, $\Lambda = S(Z^n)$, where $S : R^n \longrightarrow R^n$ is an invertible linear transformation. Let A be the matrix of S in the standard basis. Then, for $B = A^T A$, we can write

(1.2.1) $$\theta(B) = \sum_{x\varepsilon\Lambda} e^{-\|x\|^2} \quad \text{and} \quad \theta(B) = \sum_{x\varepsilon\Lambda} e^{-\|x-y\|^2} \quad ,$$

where $||x||=\sqrt{(x,x)}$ is the standard Euclidean norm in R^n.

Two algorithmic problems have been of considerable interest for quite some time. One is finding the length of a shortest non-zero vector in Λ,

$$\lambda(\Lambda) = \min \min_{x\varepsilon\Lambda/\{0\}} ||x|| \ ,$$

where kxk = p hx, xi is the standard Euclidean norm in R n. Two algorithmic problems have been of considerable interest for quite some time. One is finding the length of a shortest non-zero vector in Λ, ,

and the other is finding the distance from a given point y ∈ R n to the lattice:

$$\text{dist}(y,\Lambda) = \min_{x\varepsilon\Lambda} ||x-y|| \ .$$

In the breakthrough paper [Ba93], Banaszczyk used theta series to sharpen structural results, "transference theorems", relating, in particular, the length of a shortest non-zero vector in Λ and the largest distance from a point y ∈ R n to the dual (reciprocal) lattice

$$\Lambda^* = \{Z \in R^n : (x,z) \in Z \text{ for all } x \in \Lambda\}$$

The main tool is the reciprocity relation (1.1.4), which is written in the form

$$\sum_{x\in\Lambda} exp\{-\pi|\|x-y\|^2\} = \frac{1}{\det\Lambda}\sum_{x\in\Lambda} exp\{-\pi\|x\|^2 + 2\pi i(y,x)\} \ ,$$

where det Λ = | det S| for an invertible linear transformation S such that $\Lambda = S(Z^n)$.

Using theta functions, Aharonov and Regev [AR05] showed that the problems of approximating within a factor O(√n) the length of a shortest non-zero vector in Λ and the distance to Λ from a given point lie in NP ∩ coNP. This is in contrast to the fact that the existing polynomial time algorithms are guaranteed to approximate the desired quantities only within a $2^{O(n)}$ factor, see [G+93] (both problems are NP hard to solve exactly).

We note the following inequalities from [Ba93] and [AR05]:

(1.2.2) $$e^{dist^{2(y,\Lambda)}} \quad \le \quad \frac{\sum_{x\in\Lambda} e^{-\|x-y\|^2}}{\sum_{x\in\Lambda} e^{-\|x\|^2}} \quad \le \ 1,$$

so by computing (1.2.1), one can provide a lower bound for $dist^2(y,\Lambda)$.

Another concept that turned out to be quite useful is that of the "discrete Gaussian measure", that is the probability measure on Λ defined b

$$\mathbf{P}(x) = \frac{e^{-\|x\|^2}}{\sum_{u\in\Lambda} e^{-\|u\|^2}} \quad \text{for } x\in\Lambda \ ,$$

see [Ba93], [AR05], [MR07], [A+15], [RS17] for its applications and properties. Just to compute P (x) for a single point x, we need to be able to compute (1.2.1). One particularly useful inequality due to Banaszczyk [Ba93] states that

(1.2.3) $$\sum_{x\in\Lambda:||x-y||>\sqrt{\pi n}} e^{-\|x-y\|^2} \quad \le \ 5^{-n} \sum_{x\in\Lambda} e^{-\|x\|^2} \quad \text{for any } y\in R^n \ .$$

Choosing y = 0, we conclude from (1.2.3) that the bulk of the measure is concentrated within √ πn distance from 0.

Finally, we note that the shortest non-zero vector and nearest lattice point problems for general lattices in R^n reduce to those for lattices of the type $\Lambda = L\cap Z^{n+1}$, where $L \subset R^{n+1}$ is a hyperplane spanned by integer points [S+11].

In what follows, we write A ≤ B for n × n real symmetric matrices A and B if B − A is a positive semidefinite matrix. We denote by I the n × n identity matrix. Computing Θ(B) and Θ(B, y) for matrices B that are too small or too big in the "≤" order is not interesting: if (ω ln n)I≤ B for some fixed ω > 1 then Θ(B) = 1 + o(1), since only x = 0 contributes a substantial amount in (1.1.1), see Lemma 4.1. On the other hand, if B ≤ (ω/ ln n)I for some fixed ω < π then

$$\Theta(B, y) = \frac{\pi^{n/2}}{\sqrt{\det B}} \quad (1+o(1)) \ .$$

This follows from the reciprocity relation (1.1.4). In this case, the series (1.1.2) that is just a Riemann sum for the integral

$$\int e^{-f(x-y)}\mathrm{dx} = \frac{\pi^{n/2}}{\sqrt{\det \mathrm{B}}}$$

approximates the integral very well.

(1.3) Results. Our main result is a fully polynomial randomized approximation scheme (FPRAS) for computing (1.1.1) and (1.1.3) provided

(1.3.1) $$\mathrm{sI} \leq \mathrm{B} \leq (\mathrm{s}+\frac{e^{s}}{4}(1\text{-}\mathrm{e}^{-\mathrm{s}})^2\ (1\text{-}\mathrm{e}^{-2\mathrm{s}}))\mathrm{I} \text{ for some } \mathrm{s}\geq 1,$$

see Section 2. It turns out that in that case we can write (1.1.1) and (1.1.3) as an integral of some explicit log-concave function G : $\mathrm{R}^n \rightarrow \mathrm{R}_+$ and hence we can use any of the efficient algorithms for integrating log-concave functions as a blackbox [AK91], [F+94], [FK99], [LV07]. The most interesting case is that of s in (1.3.1) slowly growing with n (certainly not faster than ln n). From (1.3.1) we obtain an easier to parse condition

(1.3.2) $$\mathrm{sI} \leq \mathrm{B} \leq (\mathrm{s}+\frac{e^{s}}{5})\ \mathrm{I} \ \text{ for } \mathrm{s} \geq 3,$$

which is sufficient for Θ(B) and, more generally (1.1.3), to be efficiently computable. From the reciprocity relation (1.1.4) it immediately follows that there is an FPRAS for Θ(B, y) provided

$$\pi^2(\mathrm{s}+\frac{e^{s}}{4}(1\text{-}\mathrm{e}^{-\mathrm{s}})^2\ (1\text{-}\mathrm{e}^{-2\mathrm{s}}))^{-1}\ \mathrm{I} \leq \mathrm{B} \leq\ \pi^2\mathrm{s}^{-1}\ \mathrm{I} \text{ for some } \mathrm{s} \geq 1.$$

An easier to parse sufficient condition is

(1.3.3) $$\pi^2(\mathrm{s}+\frac{e^{s}}{5})^{1}\ \mathrm{I} \leq \mathrm{B} \leq (\ \pi^2\mathrm{s}^{-1)}\ \mathrm{I} \text{ for some } \mathrm{s} \geq 3\ .$$

We note that any positive definite matrix B can be scaled B → αB so that (1.3.3) is satisfied for some s. Hence via (1.2.2) one can get a lower bound (not necessarily interesting) for dist(y,Λ) for arbitrary $\Lambda \subset \mathrm{R}^n$ and $\mathrm{y} \in \mathrm{R}^n$. Applying successive conditioning on the coordinate affine subspaces, one can efficiently sample points $\mathrm{x} \in \mathrm{Z}^n$ from the discrete Gaussian distribution associated with matrix B satisfying (1.3.3), a question of independent interest, cf. [A+15]. It is not clear, however, whether one can efficiently sample if B satisfies (1.3.2).

(1.4) Short integer vectors near a subspace. Given a proper subspace $\mathrm{L} \subset \mathrm{R}^n$, we are interested in finding out whether there are vectors $\mathrm{x} \in \mathrm{Z}^n \setminus \{0\}$ that are reasonably short and also reasonably close to L. In analytic terms, when L is defined by a system of homogeneous linear equations Ax = 0, we are interested in non-trivial short integer "near solutions" x to the system or, equivalently, in small integer "near linear dependencies" among the columns of matrix A, cf. Chapter 5 of [G+93] for related problems of Diophantine approximation.

Let us fix 0 < ω < 1 (all implied constants in the "O" notation in this section depend on ω only). Given a proper subspace $\mathrm{L} \subset \mathrm{R}^n$, let us construct an n × n positive definite matrix B = B(L, ω) as follows. The eigenvectors of B lie in $\mathrm{L} \cup \mathrm{L}^{\perp}$, the eigenvectors in L all have eigenvalue ω ln n and the eigenvectors in $\mathrm{L}^{\perp}$ all have eigenvalue ω ln n + $\frac{1}{5}\mathrm{n}^{\omega}$. Hence (1.3.2) is satisfied for all sufficiently large n with

$$s = \omega \ln n$$

and Θ(B) as well as Θ(sI) can be approximated in randomized polynomial time. Let us consider the discrete Gaussian probability measure on Z n where

(1.4.1) $$P(x) = \frac{e^{-w||x||^2}}{\sum_{u \in Zn} e^{-s||u||^2}} = \frac{n^{-w||x||^2}}{\sum_{u \in Zn} n^{-w||u||^2}} .$$

Then

(1.4.2) $$\frac{\Theta(B)}{\Theta(sI)} = E \exp\{-\tfrac{1}{5} n^{w}\, dist^2(x, L)\}$$

Where

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

is the Euclidean distance from x to L.

It turns out that the probability measure defined by (1.4.1) is concentrated on vectors $x \in Z^n$ with $||x|| \approx \sqrt{}\,2n1-\omega$. In particular, in Theorem 4.2 we prove that

(1.4.3) $$\mathbf{P}(2n^{1-w}\ (1-\epsilon) \le ||x||^2 \le 2n^{1-w}\ (1+\epsilon)\ \ge 1\text{-}2 \exp\{-\frac{e^2\, n^{1-w}}{2} + O(n^{1-2w})\}$$ for all $0<\epsilon<1$

.

We also note that

$$\mathbf{P}(x = 0) = \exp\{-2n^{1-w} + \ +0n^{1-2w}\}$$

and that, more generally, if L is a coordinate subspace of codimension k then

$$\mathbf{P}(x \in L) = \exp\{-2kn^{w}(kn^{2w})\},$$

see Lemma 4.1.

By computing the expectation (1.4.2) we can furnish a guarantee that there is a reasonably short integer vector $x \neq 0$ that has a small angle with L. Suppose, for example, that the value of (1.4.2) is at least $\exp\{-\alpha n^{1-\omega}\}$ for some $0 < \alpha < 0.1$, which happens, for example, when

$$\mathbf{P}\,(x \in L) \ge \exp\{-\alpha n^{1-\omega}\}$$

Let us choose = 0.5 in (1.4.3) and let

$$X = \{x \in Z^n : n^{1-\omega} \le ||x||^2 \le 3n^{1-\omega}\}.$$

Then, for the conditional expectation we have

$$E \exp\left\{-\frac{1}{5} n^{w}\, dist^2(x, L) \middle| x \in X\right\} \ \ge\ \frac{1}{2} \exp\{-\alpha n^{1-w}\}$$

for all sufficiently large n.

Hence we conclude that there is a vector $x \in X$ with

$$dist^2(x, L) \le 5\alpha n^{1-2\omega} + O(n^{-w}).$$

In particular, we conclude that there is an $x \in Z^n \setminus \{0\}$ such that $||x|| = O(n^{(1-w)/2})$ and such that the angle between x and L is $O(\sqrt{\alpha n^{-w/2}})$ (it is not clear how to construct such an x efficiently). For example, if L contains sufficiently many short integer vectors, by computing (1.4.2) we can ascertain that there is a short non-zero integer vector forming a small angle with L, even when the probability to hit such a vector at random is exponentially small.

Suppose now that the subspace $L \subset R\, n$ is defined by a system of linear equations $Ax = 0$ where A is an $m \times n$ integer matrix of rank $m < n$. Then

$$\text{dist}(x, L) \geq (||A||_{op})^{-1} \quad \text{for all } x \in Z^n \setminus L,$$

where $(||A||_{op})$ is the operator norm of A, that is the largest singular value of A, see Theorem 4.3. Let us fix $0.5 < \omega < 1$ and $0 < \delta < \omega - 0.5$ and consider the class of integer matrices A and corresponding subspaces $L = \ker A$ such that $(||A||_{op}) \leq n\, \delta$. Then the contribution of the vectors $x \in Z^n \setminus L$ to (1.4.2) does not exceed

$$\exp\{-\frac{1}{5}n^{w-2\delta}\}$$

and hence is exponentially small compared to

$$\mathbf{P}(x \in L) \geq \mathbf{P}(x = 0) = \exp\{-2n^{1-\omega} + O(n^{1-\omega})\}$$

Summarizing, in this case

$$|\frac{\Theta(B)}{\Theta(sI)} - P(x \in L)| \leq \exp\{-\frac{1}{5}n^{w-2\delta}\}$$

and the expectation (1.4.2) approximates the discrete Gaussian measure of L up to an exponentially small in $n\, \omega-2\delta$ relative error.

2. THE ALGORITHM

A function $G : R^n \to R_+$ is called log-concave if

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

Equivalently, $G = e^{\psi}$ where $\psi : R^n \to R \cup \{-\infty\}$ is concave, that is $\psi(\alpha x + (1-\alpha y) \geq \alpha\psi(x) + (1-\alpha)\psi(y)$ for all $x, y \in R^n$ and all $0 \leq \alpha \leq 1$.

Recall that by $||A||_{op}$ we denote the operator norm of a matrix A, that is the largest singular value of A. Our main result is as follows.

(2.1) Theorem. *Let $A = (aij)$ 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 $F_{A,b,s} : R_m \to R_+$ by

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

Then (1) We have

$$2\pi^{-m/2}\prod_{k=1}^{\infty}(1-q^{2k})^{n}\int_{Rm} F_{a,b,s}(t)\, e^{-||t||2/2}dt$$
$$=\sum_{x\varepsilon z^{n}} exp\{-(Bx,x)+\ i(b,x)\}$$

(2) Suppose that

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

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

$G(t)=\ e^{-||t||2/2}\prod_{j=1}^{n}\prod_{k=1}^{\infty}(1+2q^{2k-1}\cos(ß_j+\sum_{i=1}^{m} a_{ij}T_i)+q^{4k-2}))$, *where* $t = (\tau1, \ldots, \tau m)$,

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

We note that

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

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

$$||A^{T}A||_{op}\leq\frac{1}{2}e^{s}\,(1-e^{-s})^{2}\ \ (1-e^{-2s})$$

We prove Theorem 2.1 in Section 3.

Theorem 2.1 allows us to approximate Θ(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]. Since the most interesting case is that of B with a gap between the smallest and the largest eigenvalues, we will assume that $s \geq 1$.

(2.2) Algorithm for computing theta function. We present an algorithm for computing (1.1.3). Input: An $n \times n$ positive definite matrix B such that

$$S\preccurlyeq B\preccurlyeq s+\frac{e^{s}}{4}((1-e^{-s})^{2}\ \ 1-e^{-2s}))I \text{ for some } S\geq 1$$

a vector $b \in R^{n}$, $b = (\beta1, \ldots, \beta n)$, and a number $0 < \epsilon < 1$. Output: A positive real number approximating

$$\sum_{x\varepsilon z^{n}} exp\{-\ (\text{-}Bx,X)+i(b,x)\}$$

within relative error ϵ.

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

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

Next, we write

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

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

$$||A||_{op}=\leq\frac{1}{2}\ \ e^{s}\ (1-e^{-s})^{2}\ \ 1-e^{-2s})\ .$$

Let q = e –^{s} For an integer K = K(∊) > 0, to be specified in a moment, we define F˜ : R ^{m} → R by

$$\prod_{j=1}^{n}\prod_{k=1}^{k}(1+2q^{2k-1}\cos(ß_j+\sum_{i=1}^{m}a_{ij}T_i)+q^{4k-2}))$$

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

$$2\pi^{-m/2}\prod_{k=1}^{k}(1-q^{2k})^{n}\int_{Rm}\mathscr{F}_{a,b,s}(t)\, e^{-\|t\|2/2}dt$$

within relative error ∊/3. We choose K so that the relative error acquired by replacing infinite product

$$\prod_{k=1}^{\infty}(1-q^{2k})^{n} \text{ and } \prod_{k=1}^{k}(1+2q^{2k-1}\cos(ß_j+\sum_{i=1}^{m}a_{ij}T_i)+q^{4k-2})$$

in Theorem 2.1 by finite ones does not exceed ∊/3. Since

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

Similarly,

$$|f(x) = \sum_{k=K}^{\infty}\ln 1+q^{2k-1}\cos(ß_j+\sum_{i=1}^{m}a_{ij}T_i)+q^{4k-2})|$$

$$\le |\sum_{k=K}^{\infty}\ln(1-2q^{2k-1}+q^{4k-2})| \le 4\sum_{k=K}^{\infty}q^{2k-1} = \frac{4q^{2K-1}}{1-q^2} \le 5q^{2k-1}.$$

Consequently, to approximate the infinite products in Theorem 2.1 by finite ones within relative error ∊/3, we can choose K = O (ln(n/∊)). The complexity of the resulting algorithm is polynomial in n, $∊^{-1}$ and s.

3. PROOF OF THEOREM 2.1

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

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

$$\prod_{k\ge1}(1-q^{2k})(1+wq^{2k-1})(1+w^{-1}q^{2k-1}) = \sum_{\xi\epsilon Z}w^{\xi}q^{\xi^2}.$$

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

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

Then

$$\prod_{j=1}^{n}\prod_{k\ge1}^{k}(1-q^{2k})(1+w_j q^{2k-1})(1+w_j^{-1}q^{2k-1})$$

$$(3.1.1)\quad = \sum_{\substack{x\varepsilon z^n \\ x=\xi n}} q^{\|x\|\xi^2}\prod_{j=1}^{n}w^{\xi}w_j^{\xi j}.$$

(3.2) Proof of Part (1). For t = (τ1, . . . , τm), we choose

$$wj(t) = \exp\{i(\beta j+\sum_{i=1}^{m}a_{ij}T_i)\} \quad \text{for } j=1,\ldots\ldots,n.$$

in (3.1.1). Using that

$$(1+w_j(t)\,q^{2k-1})\,(1+w_j(t)\,q^{2k-1}) = 1+w_j(t) + w_j^{-1}(t))\,q^{2k-1}+ q^{4k-2})$$
$$=1+2\cos(ß_j+ \textstyle\sum_{i=1}^{m} a_{ij}T_i) + q^{2k-1}+q^{4k-2})$$

and that

$$\prod_{j=1}^{n} w_j^{\xi j} = \exp\{\mathbf{i}\textstyle\sum_{j=1}^{n} ßj\,\xi j + \mathbf{i}\sum_{j=1}^{m} \tau 1(\sum_{i=1}^{m} a_{ij}\,\xi j)\},$$

$F_{a,b,t}(t)= \prod_{k=1}^{n}(1- q^{2k-1})^n$

$$= \sum_{\substack{x\varepsilon z^n \\ x=\xi n}} q^{||x||\xi^2} \exp\{\mathbf{i}\textstyle\sum_{j=1}^{n} ßj\ \xi j + \mathbf{i}\sum_{j=1}^{m} \tau 1(\sum_{i=1}^{n} a\,\text{ij}\,\xi j)\}.$$

Since

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty} \exp\{i\,T_i \textstyle\sum_{j=1}^{n} a_{ij}\,\xi_i\}\,(e^{-Ti2/2}\,d\,T_i = \exp(-\frac{1}{2}(\sum_{j=1}^{n} a_{ij}\,\xi_i)^2\},$$

We get

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

$$=\sum_{x\varepsilon z^n} q^{||x||^2} \exp\{-\tfrac{1}{2}||Ax||^2+ i\,(b,x)\} = \textstyle\sum_{n=1}^{\infty} \exp\{-(Bx,x) + i(b,x)\},$$

and the proof follows.

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

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

$$\frac{d^{\,2}}{dT^{\,2}} \ln(1 + 2q\cos(\alpha\tau + \beta) + q^2) < \frac{2\alpha^2 q}{(1-q)^2}$$

Proof , We have

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

and

$$\frac{d}{dr}\ln(1 + 2q\cos(\alpha\tau + \beta) + q^2$$

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

$$= -\frac{2\alpha^2 q cos(\alpha T+\beta)\left(1+q^{\,2}\right)+4\alpha^2 q^{\,2}}{(1+2q cos(\alpha T+\beta)+q^{\,2})^2}$$

Now,

$$(1 + 2q cos(\alpha T + \beta) + q^{\,2})^2 \geq (1-2q + q^2)^2 = 1-q^4.$$

Also

$$2\alpha^2 cos(\alpha T + \beta)\,(1+q^2)+ 4\alpha^2 q^{\,2} \geq -2\alpha^2 q(1+q^2)+ 4\alpha^2 q^{\,2}$$
$$= 2\alpha^2 q(2q-1-q^2) = -2\alpha^2 q(1-q)^2 .$$

The proof now follows.

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

$$T_l = \gamma_i T + \delta_i \text{ for } i=1,....,m \quad \text{where } \sum_{i=1}^{m} \gamma^{2} = 1$$

is log-concave. Indeed, let g(τ) be that restriction. From Lemma 3.3, we get

$$\frac{d^{2}}{dT^{2}} \ln g(T) \leq -1+2 \sum_{K=1}^{K} \left(\frac{q^{2k-1}}{(1-q^{2k-1})^2}\right) \sum_{j=1}^{m} \left(\sum_{j=1}^{m} a_{ij}\, \gamma_i \right)^2$$

$$= -1+2\|A^{T}A\|_{op} \sum_{K=1}^{K} \left(\frac{q^{2k-1}}{(1-q^{2k-1})^2}\right) \leq 0$$

and hence ln g(τ) is concave. The proof now follows.

4. ESTIMATES FOR THE DISCRETE GAUSSIAN MEASURE

In this section, we prove some supporting estimates for Section 1.4. Let $s \geq 1$ and let $q = e^{-s}$. We consider the discrete Gaussian probability measure on Z^n defined by

$$\mathbf{P}(x) = \frac{e^{-s\|x\|^2}}{\sum_{x\varepsilon z^n} e^{-s\|u\|^2}} = \frac{q^{\|x\|^2}}{\sum_{x\varepsilon z^n} q^{\|u\|^2}} \quad \text{for} \quad x \in Z^n$$

We note that the coordinates of a random point $x \in Z^n$, $x = (\xi 1, \ldots, \xi n)$, are independent.

All implied constants in the "O" notation are absolute, as long as the constraint $s \geq 1$ is imposed.

Our main result is that for a random vector $x \in Z^n$, we have $\|x\| \approx \sqrt{2qn}$ with high probability. Towards this goal, we first prove a general estimate.

(4.1) Lemma . *For $0 < q \leq 0.9$, we have*

$$\sum_{x \in Zn} q^{\|x\|^2} = \exp\{2qn+O(q^2 n)\}.$$

In particular, for $x \in Z_n$, $x=(\xi_1, \ldots \xi_n)$, we have

$$\mathbf{P}(\xi_j = 0) = \exp\{-2q+O(q^2)\} \quad \text{for} \quad j=1,....,n$$

Proof. By Jacobi's formula ,we have

$$\sum_{x\varepsilon z^n} q^{\|x\|^2} = \left(\prod_{k\geq 1}(1-q^{2k})(1+q^{2k-1})^2\right)^2$$

See section 3.1 we have

$$\ln\left(\prod_{k\geq 1}(1-q^{2k})(1+q^{2k-1})^2\right) = \sum_{k\geq 1} \ln(1-q^{2k}) + 2(1+q^{2k-1}) = 2q+O(q^2),$$

and proof follows

(4.2)Theorem. *Suppose that $0 \leq q \leq e^{-1}$.Then for any $0 \leq \epsilon \leq 1$, we have*

$$P(\|x\|^2 \geq 2qn(1+\epsilon)) \leq \exp\{-\frac{\epsilon 2qn}{2} + O(q^2 n)\} \text{ and}$$

$$P(\|x\|^2 \geq 2qn(1-\epsilon)) \leq \exp\{-\frac{\epsilon 2qn}{2} + O(q^2 n)\}$$

Proof ,We have

$$\mathbf{P}(\|x\|^2 \geq 2qn(1+\epsilon)) = P(e^{\varepsilon\|x\|^2/2} \geq e^{qn\epsilon(1+\epsilon)}) \leq e^{-qn\epsilon(1+\epsilon)}\, \mathrm{E}e^{\varepsilon\|x\|^2/2}$$

by Markov Inquality Now

$$\mathrm{E}e^{\varepsilon\|x\|^2/2} = \frac{\sum_{x\varepsilon z^n} \left(e^{\varepsilon/2}q\right)^{\|x\|^2}}{\sum_{x\varepsilon z^n} q^{\|x\|^2}}$$

Since

$$2e^{\epsilon/2}q \leq e^{0.5}\, e^{-1=}\, e^{-0.5} < 0.9,$$

by Lemma 4.1 we have

$$\sum_{x\varepsilon z^n} \left(e^{\varepsilon/2}q\right)^{\|x\|^2} = \exp\{\ 2e^{\epsilon/2}qn + O(q^2n)\}\ .$$

and similarly

$$\sum_{x\varepsilon z^n} q^{\|x\|^2} = \exp(\{2qn + O(q^2n)\},$$

Hence

$$\mathbf{E}e^{\varepsilon\|x\|^2/2} = \exp\{2qn(e^{\epsilon/2}-1) + O(q^2n))$$

and

$$\mathbf{P}(\|x\|^2 \leq 2qn(1-\epsilon)) \leq \exp\{\ qn(2e^{-\epsilon/2}-2+\epsilon)) + O(q^2n))$$

Since

$$e^{-\epsilon/2}-1+\frac{\epsilon}{2} \leq \frac{\epsilon 2}{4} \ \text{ for } 0 \leq \epsilon \leq 1\ ,$$

the proof of the second inequality follows.

The following result is most certainly known, but we give its proof for completeness.

(4.3) Theorem. Let A be an m × n integer matrix with rank A = m < n and let L = ker A, L ⊂ R ^{n}. Then

$$\mathrm{dist}(x, L) \geq (\|A\|op)^{-1} \text{ for all } x \in Z^n \setminus L.$$

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

$$\mathrm{dist}^2(x,L) = \|P(x)\|^2 = (A^T(AA^T)^{-1}Ax, A^T(AA)^{-1}Ax) = ((AA^T)^{-1}Ax, Ax).$$

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

$$((AA^T)^{-1}Ax, Ax) \geq \lambda$$

and hence

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

On the other hand,

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

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.

[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, 19

[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.

[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+93] M. Gr¨otschel, L. Lov´asz and A. Schrijver, Geometric Algorithms and Combinatorial Optimization. Second edition, Algorithms and Combinatorics, 2, Springer-Verlag, Berlin, 1993.

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

[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.

[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 Birkh¨auser Classics, Birkh¨auser 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 Birkh¨auser Classics, Birkh¨auser 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 Birkh¨auser Classics, Birkh¨auser Boston Inc., Boston, MA, 2007

[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.