CSE 206A: Lattice Algorithms and Applications Winter 2016

The Gaussians Distribution

Instructor: *Daniele Micciancio* UCSD CSE

1 The real fourier transform

Gaussian distributions and harmonic analysis play a fundamental role both in the design of lattice-based cryptographic functions, and the theoretical study of lattice problems. For any function $f\colon \mathbb{R}^n \to \mathbb{C}$ such that $\int_{\mathbf{x}\in\mathbb{R}} |f(\mathbf{x})| \, \mathrm{d}\mathbf{x} < \infty$, the fourier transform of f is defined as

$$\widehat{f}(\mathbf{y}) = \int_{\mathbf{x}\in\mathbb{R}^n} f(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{x},\mathbf{y}\rangle} \, \mathrm{d}\mathbf{x}$$

where $i = \sqrt{-1}$ is the imaginary unit and $e^{2\pi iz} = \cos(\frac{z}{2\pi}) + i\sin(\frac{z}{2\pi})$ the exponential function from the unit interval $z \in \mathbb{R}/\mathbb{Z} \approx [0,1)$ to the unit circle on the complex plane $e^{2\pi iz} \in \{c \in \mathbb{C} : |c| = 1\}$. So, the fourier transform is also a function $\widehat{f}\colon \mathbb{R}^n \to \mathbb{C}$ from the euclidean space $\mathbb{R}^n$ to the complex numbers. The gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$ naturally arises in harmonic analysis as an eigenfunction of the fourier transform operator.

Lemma 1 *The gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$ equals its fourier transform $\widehat{\rho}(\mathbf{x}) = \rho(\mathbf{x})$.*

Proof. It is enough to prove the statement in dimension $n = 1$, as the general statement follows by

$$\begin{aligned}
\widehat{\rho}(\mathbf{y}) &= \int_{\mathbf{x}\in\mathbb{R}^n} \rho(\mathbf{x}) e^{-2\pi i\langle \mathbf{x},\mathbf{y}\rangle} \, \mathrm{d}\mathbf{x} \\
&= \int_{\mathbf{x}\in\mathbb{R}^n} \prod_k \rho(x_k) e^{-2\pi i x_k y_k} \, \mathrm{d}\mathbf{x} \\
&= \prod_k \int_{x\in\mathbb{R}} \rho(x) e^{-2\pi i x y_k} \, \mathrm{d}x \\
&= \prod_k \widehat{\rho}(y_k) = \rho(\mathbf{y}).
\end{aligned}$$

So, let $\rho(x) = e^{-\pi x^2}$ the one-dimensional gaussian. We compute

$$\begin{aligned}
\widehat{\rho}(y) &= \int_{x\in\mathbb{R}} \rho(x) e^{-2\pi i x y} \, \mathrm{d}x \\
&= \int_{x\in\mathbb{R}} e^{-\pi(x^2+2ixy)} \, \mathrm{d}x \\
&= e^{-\pi y^2} \int_y e^{-\pi(x+iy)^2} \, \mathrm{d}x \\
&= \rho(y) \int_{x\in\mathbb{R}+iy} \rho(x) \, \mathrm{d}x.
\end{aligned}$$

Finally, we observe that $\int_{x\in\mathbb{R}+iy}\rho(x)\,\mathrm{d}x = \int_{x\in\mathbb{R}}\rho(x)\,\mathrm{d}x$ by Cauchy's theorem, and

$$\begin{aligned}\int_{x\in\mathbb{R}}\rho(x)\,\mathrm{d}x &= \sqrt{\int_{x_1\in\mathbb{R}}\rho(x_1)\,\mathrm{d}x_1\cdot\int_{x_2\in\mathbb{R}}\rho(x_2)\,\mathrm{d}x_2}\\ &= \sqrt{\int_{\mathbf{x}\in\mathbb{R}^2}\rho(\mathbf{x})\,\mathrm{d}\mathbf{x}} = \sqrt{\int_{r=0}^{\infty}2\pi r\rho(r)\,\mathrm{d}r} = 1\end{aligned}$$

where the last equality follows from the fact that $\rho'(r) = -2\pi r\cdot\rho(r)$. □

We note that in other settings the gaussian distribution is often defined as $g(x) = e^{-\frac{1}{2}x^2}$, which is the same as ρ, but with a different scaling factor. Using $g(x)$ corresponds to normalizing the standard deviation $\sqrt{\int_x g(x)^2\,\mathrm{d}x} = 1$, but introduces a scaling factor when taking the fourier transform of g. As we will make extensive use of the fourier transform, in lattice cryptography it is typically preferable to use $\rho(x) = e^{-\pi x^2}$ as the "standard" gaussian function, so that $\widehat{\rho} = \rho$. The standard deviation of ρ is $\sqrt{\int_{\mathbf{x}\in\mathbb{R}^n}\rho(\mathbf{x})^2\,\mathrm{d}\mathbf{x}} = \sqrt{\frac{n}{2\pi}}$.

The following properties of the fourier transform easily follow from the definition.

Lemma 2 *Any function f with $\int_{\mathbf{x}\in\mathbb{R}^n}|f(\mathbf{x})| < \infty$ satisfies the following properties:*

1. *for any nonsingular square matrix $\mathbf{T}$, if $h(\mathbf{Tx}) = f(\mathbf{x})$ then $\widehat{h}(\mathbf{y}) = \det(\mathbf{T})\cdot\widehat{f}(\mathbf{T}^t\mathbf{y})$.*
2. *if $h(\mathbf{x}) = f(\mathbf{x}+\mathbf{v})$, then $\widehat{h}(\mathbf{y}) = \widehat{f}(\mathbf{y})\cdot e^{2\pi i\langle\mathbf{v},\mathbf{y}\rangle}$.*
3. *if $h(\mathbf{x}) = f(\mathbf{x})\cdot e^{2\pi i\langle\mathbf{x},\mathbf{v}\rangle}$, then $\widehat{h}(\mathbf{y}) = \widehat{f}(\mathbf{y}-\mathbf{v})$.*

Proof. For the first property, we have

$$\widehat{h}(\mathbf{y}) = \int_{\mathbf{z}\in\mathbb{R}^n}h(\mathbf{z})\cdot e^{-2\pi i\langle\mathbf{z},\mathbf{y}\rangle}\,\mathrm{d}\mathbf{z} = \int_{\mathbf{z}\in\mathbb{R}^n}f(\mathbf{T}^{-1}\mathbf{z})\cdot e^{-2\pi i\langle\mathbf{z},\mathbf{y}\rangle}\,\mathrm{d}\mathbf{z}.$$

Making a change of variable $\mathbf{z} = \mathbf{Tx}$, the last expression equals

$$\det(\mathbf{T})\int_{\mathbf{x}\in\mathbb{R}^n}f(\mathbf{x})\cdot e^{-2\pi i\langle\mathbf{x},\mathbf{T}^t\mathbf{y}\rangle}\,\mathrm{d}\mathbf{x} = \det(\mathbf{T})\widehat{f}(\mathbf{T}^t\mathbf{y}).$$

The other two properties are proved similarly, using the definition of the fourier transform, and applying an appropriate change of variable. □

Less trivial to prove is the following result, known as Poisson summation formula. The theorem requires f to satisfy appropriate regularity conditions. We will apply the theorem only to the gaussian function $\rho(\mathbf{x})$, and other functions obtained from it by the simple change of variables described in Lemma 2. These functions behave in the nicest possible way with respect to the fourier transform, so we do not explicitly state necessary requirements on the function f.

Theorem 3 *If $f(\mathbb{Z}^n) = \sum_{\mathbf{x}\in\mathbb{Z}^n} f(\mathbf{x})$, and similarly for $\widehat{f}(\mathbb{Z}^n)$, then*

$$f(\mathbb{Z}^n) = \widehat{f}(\mathbb{Z}^n).$$

Proof. Let $f\colon \mathbb{R}^n \to \mathbb{C}$ and define the periodic function $\varphi(\mathbf{x}) = f(\mathbf{x}+\mathbb{Z}^n) = \sum_{\mathbf{y}\in\mathbb{Z}^n} f(\mathbf{x}+\mathbf{y})$. Notice that $\varphi(\mathbf{x}) = \varphi(\mathbf{x} \bmod \mathbf{y})$ for any $\mathbf{y} \in \mathbb{Z}^n$, i.e., φ is periodic modulo 1, and can be equivalently described as a function from $[0,1)^n$ to $\mathbb{C}$. The fourier series of a periodic function $\varphi\colon [0,1)^n \to \mathbb{C}$ is defined as

$$\widehat{\varphi}(\mathbf{z}) = \int_{\mathbf{x}\in[0,1)^n} \varphi(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{x},\mathbf{z}\rangle}\, \mathrm{d}\mathbf{x}$$

for any $\mathbf{z} \in \mathbb{Z}^n$. The fourier inversion theorem for periodic functions states that if φ is sufficiently nice, it can be recovered from its fourier series

$$\varphi(\mathbf{x}) = \sum_{\mathbf{z}\in\mathbb{Z}^n} \widehat{\varphi}(\mathbf{z}) \cdot e^{2\pi i\langle \mathbf{z},\mathbf{x}\rangle}.$$

We will need this inversion formula only to evaluate φ at 0, giving

$$f(\mathbb{Z}^n) = \varphi(\mathbf{0}) = \sum_{\mathbf{z}\in\mathbb{Z}^n} \widehat{\varphi}(\mathbf{z}) \cdot e^0 = \widehat{\varphi}(\mathbb{Z}^n).$$

Next we compute the fourier coefficients

$$\begin{aligned} \widehat{\varphi}(\mathbf{z}) &= \int_{\mathbf{x}\in[0,1)^n} \varphi(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{x},\mathbf{z}\rangle}\, \mathrm{d}\mathbf{x} \\ &= \int_{\mathbf{x}\in[0,1)^n} \sum_{\mathbf{w}\in\mathbb{Z}^n} f(\mathbf{x}+\mathbf{w}) \cdot e^{-2\pi i\langle \mathbf{x},\mathbf{z}\rangle}\, \mathrm{d}\mathbf{x}. \end{aligned}$$

Since $\mathbf{x} \mapsto e^{-2\pi i\langle \mathbf{x},\mathbf{z}\rangle}$ is also periodic modulo 1, the last expression equals

$$\int_{\mathbf{x}\in[0,1)^n} \sum_{\mathbf{w}\in\mathbb{Z}^n} f(\mathbf{x}+\mathbf{w}) \cdot e^{-2\pi i\langle \mathbf{x}+\mathbf{w},\mathbf{z}\rangle}\, \mathrm{d}\mathbf{x} = \int_{\mathbf{x}\in\mathbb{R}^n} f(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{x},\mathbf{z}\rangle}\, \mathrm{d}\mathbf{x} = \widehat{f}(\mathbf{z})$$

i.e., the fourier series of the periodic function φ equals the fourier tranform of f at integer points $\mathbf{z} \in \mathbb{Z}^n$. So, $f(\mathbb{Z}^n) = \widehat{\varphi}(\mathbb{Z}^n) = \widehat{f}(\mathbb{Z}^n)$. □

The theorem is easily generalized to arbitrary lattices.

Corollary 4 *For any lattice Λ,*

$$f(\Lambda) = \det(\Lambda^*)\widehat{f}(\Lambda^*)$$

where $f(\Lambda) = \sum_{\mathbf{x}\in\Lambda} f(\mathbf{x})$, and similarly for $\widehat{f}(\Lambda^*)$.

Proof. We may assume without loss of generality that Λ is a full dimensional lattice. Let $\mathbf{B}$ be a basis of Λ, so that the lattice can be written as $\mathbf{B}\mathbb{Z}^n$, and let $h(\mathbf{x}) = f(\mathbf{B}\mathbf{x})$. Then, using the previous theorem, we have

$$f(\Lambda) = h(\mathbb{Z}^n) = \hat{h}(\mathbb{Z}^n) = \det(\mathbf{B}^{-1})h(\mathbf{B}^{-t}\mathbb{Z}^n) = \det(\Lambda^*)h(\Lambda^*).$$

□

We know from the proof of Lemma 1 that $\int_{\mathbf{x}} \rho(\mathbf{x})\, \mathrm{d}\mathbf{x} = 1$. So, the gaussian function can be interpreted as a probability distribution over $\mathbb{R}^n$. Lattice cryptography uses a discrete version of this probability distribution which selects points from a lattice $\mathbf{x} \in \Lambda$ with probability proportional to $\rho(\mathbf{x})$.

Definition 5 *For any lattice Λ, the discrete gaussian probability distribution D_Λ is the probability distribution over Λ that selects each lattice point $\mathbf{x} \in \Lambda$ with probability $\Pr\{\mathbf{x}\} = \rho(\mathbf{x})/\rho(\Lambda)$, where $\rho(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho(\mathbf{x})$ is normalization factor.*

Informally (or even formally, with some effort) one can think of the discrete gaussian distribution D_Λ as the conditional distribution of the continuous gaussian distribution $\Pr\{\mathbf{x}\} = \rho(\mathbf{x})$ on $\mathbb{R}^n$, conditioned on the event that $\mathbf{x} \in \Lambda$ is a lattice point. The reason we state this informally is that the event of picking a lattice point $\mathbf{x} \in \Lambda$ when choosing $\mathbf{x}$ according to a continuous probability distribution has zero probability. So, giving a formal definition of conditional distribution can be tricky. Luckily, none of this is needed, as we will work only with discrete distributions.

2 Fourier analysis of finite groups

Harmonic analysis in $\mathbb{R}^n$ requires sensible assumptions on the function f to guarantee convergence and the validity of the fourier inversion formula. Fortunately, in lattice cryptography, we will deal primarity with discrete probability distributions and the fourier transform over finite groups. This allows for a much simpler treatment, using linear algebra.

We start with the simple case of a finite cyclic group $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ of the integers modulo q. It will be useful to think of $\mathbb{Z}_q$ in concrete terms as the quotient between $\mathbb{Z}$ and its subgroup $q\mathbb{Z}_q$, and think these two sets as two lattices. Any finite abelian group can be expressed as a quotient Λ/Λ', where Λ is a lattice and Λ' is a full rank sublattice of Λ. As we will see, much of what we will prove for $\mathbb{Z}_q$ applies also to the quotient Λ/Λ' between to lattices, and therefore holds for arbitrary abelian groups. Notice that the same group can be expressed as the quotiend of two lattices in different ways. For example the group $\mathbb{Z}_q$ can also be represented as the quotient between $\mathbb{Z}$ and $\frac{1}{q}\mathbb{Z}$, and sometimes it is convenient to use this other representation. Since $\mathbb{Z}/\frac{1}{q}\mathbb{Z}$ is obtained just by scaling both lattices in $\mathbb{Z}/q\mathbb{Z}$ by a factor $\frac{1}{q}$, we abbreviate it as $\frac{1}{q}\mathbb{Z}_q$. So, $\frac{1}{q}\mathbb{Z}_q$ is just the same group as $\mathbb{Z}_q$, but with the elements represented as multiples of $\frac{1}{q}$ in the range $[0, 1)$.

The set of functions $V = (\mathbb{Z}_q \to \mathbb{C})$ is a q-dimensional vector space over the field $\mathbb{C}$ of complex numbers. This vector space has an inner product defined as

$$\langle f, g \rangle = E_{x \in \mathbb{Z}_q}[f(x) \cdot \overline{g(x)}] = \frac{1}{q} \sum_{x \in \mathbb{Z}_q} f(x) \cdot \overline{g(x)}$$

where $\overline{a + ib} = a - ib \in \mathbb{C}$ is the complex conjugation operation, for $a, b \in \mathbb{R}$.

Consider the family of functions $\chi_x(y) = e^{2\pi xy}$. Notice that if $x \in \frac{1}{q}\mathbb{Z}_q = \mathbb{Z}/\frac{1}{q}\mathbb{Z}$, then $\chi_x(y)$ is periodic modulo q. So, it defines a function from $\mathbb{Z}_q$ to $\mathbb{C}$. The following lemma shows that this set of functions is an orthonormal basis for $\mathbb{Z}_q \to \mathbb{C}$.

Lemma 6 *For any $x, y \in \frac{1}{q}\mathbb{Z}$,*

$$\langle \chi_x, \chi_y \rangle = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

Proof. By definition $\langle \chi_x, \chi_y \rangle = \frac{1}{q} \sum_{z \in \mathbb{Z}_q} e^{2\pi i(x-y)z}$. If $x = y$, then $e^{2\pi i(x-y)z} = e^0 = 1$, and $\langle \chi_x, \chi_y \rangle = 1$. On the other hand, if $x \neq y$, then $e^{2\pi i(x-y)} \neq 1$ and

$$\sum_{z=0}^{q-1} e^{2\pi i(x-y)z} = \frac{e^{2\pi i(x-y)q} - 1}{e^{2\pi i(x-y)-1}} = 0$$

and $\langle \chi_x, \chi_y \rangle = 0$. □

The functions χ_x with $x \in \frac{1}{q}\mathbb{Z}_q$ are called the characters of the group $\mathbb{Z}_q$, and, since there are precisely q of them, they form an orthonormal basis for $V = \mathbb{Z}_q \to \mathbb{C}$. In particular, any function can be expressed as a linear combination of the characters

$$f(x) = \sum_y \langle f, \chi_y \rangle \cdot \chi_y(x).$$

Notice the similarity between the coefficients

$$\widehat{f}(y) = \langle f, \chi_y \rangle = \frac{1}{q} \sum_{x \in \mathbb{Z}_q} f(x) \cdot e^{-2\pi ixy}$$

and the definition of the real fourier transform of a function. The function $\widehat{f}(y)$ mapping each $y \in \frac{1}{q}\mathbb{Z}_q$ to the corresponding coefficient $\langle f, \chi_y \rangle$ is called the (discrete) fourier transform of f, and the set of characters χ_y is called the fourier basis. Expressing the function f with respect to the fourier basis can be rewritten as

$$f(x) = \sum_y \widehat{f}(y) e^{-2\pi ixy}$$

giving a fourier inversion formula.

Everything easily extends to arbitrary abelian groups, but before moving on, it is useful to pay some attention to the way we represented group elements for the index $\mathbf{y} \in \frac{1}{q}\mathbb{Z}_q$ and input $\mathbf{x} \in \mathbb{Z}_q$ of the group characters $\chi_{\mathbf{y}}(\mathbf{x})$. If we think of

$$G = \Lambda/\Gamma$$

as the quotient of two lattices $\Lambda = \mathbb{Z}$ and $\Gamma = q\mathbb{Z} \subseteq \Lambda$, then $\frac{1}{q}\mathbb{Z}_q$ is precisely the dual group of G, which can be formally defined as the quotient

$$\widehat{G} = \Gamma^*/\Lambda^*$$

between the dual lattices $\Gamma^* = \frac{1}{q}\mathbb{Z}$ and $\Lambda^* = \mathbb{Z}$. (Notice that in order to take the quotient we need also to reverse the position of the two lattices, so that $\Lambda^* \subseteq \Gamma^*$.)

Now let us move to the product of cyclic groups $G = \prod_k \mathbb{Z}_{q_k} = \mathbb{Z}^n/(\prod_k (q_k \cdot \mathbb{Z}))$, and the set of functions from G to $\mathbb{C}$. In this more general setting, the fourier basis is given by the characters

$$\chi_{\mathbf{y}}(\mathbf{x}) = e^{2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}$$

for $\mathbf{y} \in \widehat{G} = \prod_k (\frac{1}{q_k}\mathbb{Z}_q) = (\prod_k \frac{1}{q_k}\mathbb{Z})/\mathbb{Z}^n$. Here $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_k x_k \cdot y_k$ is just the usual dot product between vectors. It is only the inner product of functions $\langle f, g \rangle = E_{x \in G}[f(x) \cdot \overline{g(x)}]$ that is normalized by the group size $\prod_k q_k$, so that the characters have norm $\|\chi\|^2 = \langle \chi, \chi \rangle = 1$. As before, characters are mutually orthogonal because

$$\langle \chi_{\mathbf{x}}, \chi_{\mathbf{y}} \rangle = \prod_k \langle \chi_{x_k}, \chi_{y_k} \rangle$$

and the product vanishes as soon as $x_k = y_k$ for some k. So, we define the discrete fourier transform of a function $f \colon G \to \mathbb{C}$ as before

$$\widehat{f}(\mathbf{y}) = \langle f, \chi_{\mathbf{y}} \rangle = \frac{1}{q} \sum_{\mathbf{x} \in G} f(\mathbf{x}) \cdot e^{-2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}$$

giving the fourier inversion formula

$$f(\mathbf{x}) = \sum_{\mathbf{y} \in \widehat{G}} \langle f, \chi_{\mathbf{y}} \rangle \cdot \chi_{\mathbf{y}}(\mathbf{x}) = \sum_{\mathbf{y} \in \widehat{G}} \widehat{f}(\mathbf{y}) \cdot e^{-2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}.$$

Every quotient of two (full rank) lattices $G = \Lambda/\Gamma$ with $\Gamma \subseteq \Lambda$ is a finite abelian group, and any abelian group can be represented as a product of cyclic groups. So, this is all we need to deal with quotients between any two arbitrary (full rank) lattices $\Gamma \subseteq \Lambda$. But it is useful to give a general formulation of everything we have proved so far directly in terms of lattices. In the most general setting, we start from a lattice Λ and a full rank sublattice $\Gamma \subseteq \Lambda$, which define a finite abelian group $G = \Lambda/\Gamma$ and its dual $\widehat{G} = \Gamma^*/\Lambda^*$. The set of all functions $G \to \mathbb{C}$ is a $|G|$-dimensional vector space over $\mathbb{C}$ with an inner product

$$\langle f, g \rangle = E_{\mathbf{x} \in G}[f(\mathbf{x}) \cdot \overline{g(x)}] = \frac{1}{|G|} \sum_{x \in G} f(\mathbf{x}) \cdot \overline{g(x)}$$

and orthonormal basis $\chi_{\mathbf{y}}(\mathbf{x}) = e^{2\pi\langle \mathbf{x},\mathbf{y}\rangle}$ for $\mathbf{y} \in \widehat{G}$. The discrete fourier transform of $f: G \to \mathbb{C}$ is the function $\widehat{f}(\mathbf{y}) = \langle f, \chi_{\mathbf{y}}\rangle$ from $\widehat{G}$ to $\mathbb{C}$ and it satisfies the fourier inversion formula $f(\mathbf{x}) = \sum_{\mathbf{y}\in\widehat{G}} \widehat{f}(\mathbf{y}) \cdot \chi_{\mathbf{y}}(\mathbf{x})$.

3 Gaussian sums

Poisson summation formula can be used to prove several interesting bounds on gaussian sums over lattices.

Lemma 7 *For any lattice Λ and real $s \geq 1$,*

$$\rho(\Lambda/s) \leq s^n \rho(\Lambda)$$

Proof. By the Poisson summation formula, and using $\rho(s\mathbf{x}) \leq \rho(\mathbf{x})$, we get

$$\rho(\Lambda/s) = \det(s\Lambda^*)\rho(s\Lambda^*) \leq s^n \det(\Lambda^*)\rho(\Lambda^*) = s^n\rho(\Lambda).$$

□

Lemma 8 *For any lattice coset $\Lambda + \mathbf{u}$,*

$$\rho(\Lambda + \mathbf{u}) \leq \rho(\Lambda).$$

Proof. Recall that if $f(\mathbf{x}) = \rho(\mathbf{x}+\mathbf{v})$ then $\widehat{f}(\mathbf{y}) = e^{2\pi i\langle \mathbf{y},\mathbf{v}\rangle} \cdot \rho(\mathbf{y})$. Using Poisson summation formula and triangle inequality we get

$$\begin{aligned} \rho(\Lambda + \mathbf{u}) &= \left|\det(\Lambda^*) \sum_{\mathbf{y}\in\Lambda^*} \rho(\mathbf{y}) \cdot \exp(2\pi i \langle \mathbf{y}, \mathbf{u}\rangle)\right| \\ &\leq \det(\Lambda^*) \sum_{\mathbf{y}\in\Lambda^*} \rho(\mathbf{y}) = \rho(\Lambda). \end{aligned}$$

□

An immediate consequence of the above lemma is that for any lattices $\Lambda \subset \Lambda'$, the gaussian probability distribution ($D_{\Lambda'}$ mod Λ) over the quotient group Λ'/Λ is maximized at 0 mod Λ.

Using these bounds we can easily prove several tail inequalities on the norm of vectors chosen according to a discrete Gaussian distribution.

Lemma 9 *For any lattice coset $\Lambda + \mathbf{c}$ and halfspace $H = \{\mathbf{x} : \langle \mathbf{x}, \mathbf{h}\rangle \geq \|\mathbf{h}\|^2\}$,*

$$\rho((\Lambda + \mathbf{c}) \cap H) \leq \rho(\mathbf{h}) \cdot \rho(\Lambda + \mathbf{c} - \mathbf{h}).$$

Proof. If $I_H(\mathbf{x})$ the indicator function of H, then we have

$$\begin{aligned}
\rho((\Lambda + \mathbf{c}) \cap H) &= \sum_{\mathbf{x} \in \Lambda + \mathbf{c}} \rho(\mathbf{x}) \cdot I_H(\mathbf{x}) \\
&\leq \sum_{\mathbf{x} \in \Lambda + \mathbf{c}} \rho(\mathbf{x}) \cdot \frac{\exp(2\pi \langle \mathbf{x}, \mathbf{h} \rangle)}{\exp(2\pi \|\mathbf{h}\|^2)} \\
&= \rho(\mathbf{h}) \sum_{\mathbf{x} \in \Lambda + \mathbf{c}} \rho(\mathbf{x} - \mathbf{h}) \\
&= \rho(\mathbf{h}) \rho(\Lambda + \mathbf{c} - \mathbf{h})
\end{aligned}$$

□

Using a union bound over all standard unit vectors $\pm\mathbf{e}_i$, gives a tail inequality on the infinity norm of a vector chosen according to the discrete gaussian distribution from an n-dimensional lattice.

Corollary 10 *For any n-dimensional lattice Λ, if $x \leftarrow D_\Lambda$ then*

$$\Pr\{\|\mathbf{x}\|_\infty \geq t\} \leq 2n \exp(-\pi t^2).$$

As a special case, using the scaled integer lattice $\Lambda = \mathbb{Z}/s$, we get a tail bound for gaussian samples from $\mathbb{Z}$.

Corollary 11 *If $x \leftarrow D_{\mathbb{Z},s}$, then $\Pr\{|x| \geq st\} \leq 2\exp(-\pi t^2)$.*

Theorem 12 *For any lattice coset $\Lambda + \mathbf{c}$ and $\alpha \geq 1$,*

$$\rho((\Lambda + \mathbf{u}) \setminus B(\alpha\sqrt{n/(2\pi)})) \leq \left(\frac{\alpha^2}{\exp(\alpha^2 - 1)}\right)^{n/2} \rho(\Lambda)$$

where $B(r) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\}$.

Proof. If $I_r(\mathbf{x})$ is the characteristic function of $B(r)$, then for any $0 < t < \pi$ and $r = \alpha\sqrt{n/(2\pi)}$ we have

$$\begin{aligned}
\rho((\Lambda + \mathbf{u}) \setminus B(r)) &= \sum_{\mathbf{x} \in \Lambda + \mathbf{c}} \rho(\mathbf{x})(1 - I_r(\mathbf{x})) \\
&\leq \sum_{\mathbf{x} \in \Lambda + \mathbf{c}} \rho(\mathbf{x}) \frac{\exp(t\|\mathbf{x}\|^2)}{\exp(tr^2)} \\
&= \exp(-tr^2) \rho(\sqrt{1 - t/\pi} \cdot (\Lambda + \mathbf{c})) \\
&\leq \exp(-tr^2) \rho(\sqrt{1 - t/\pi} \cdot (\Lambda)) \\
&\leq \exp(-tr^2) \cdot (1 - t/\pi)^{-n/2} \cdot \rho(\Lambda))
\end{aligned}$$

This function is minimized at $t = \pi - n/(2r^2) \geq 0$, which gives the bound in the theorem. $\square$

Notice that the base $\alpha^2/\exp(\alpha^2 - 1)$ of the exponential factor in the above theorem is monotonically decreasing for $\alpha \geq 1$, and equals $\alpha^2/\exp(\alpha^2 - 1) = 1$ when $\alpha = 1$.

Corollary 13 *For any $\alpha \geq 1$, if $\mathbf{x} \leftarrow D_\Lambda$ then*

$$\Pr\left\{\|\mathbf{x}\| \geq \alpha\sqrt{\frac{n}{2\pi}}\right\} \leq \left(\frac{\alpha^2}{\exp(\alpha^2 - 1)}\right)^{n/2}.$$

Also this corollary can be used to bound the probability that $x \leftarrow D_{\mathbb{Z},s}$ is bigger than $|x| > st$.

4 The smoothing parameter

Definition 14 *For any lattice Λ, the ϵ-smoothing parameter of a lattice Λ is the smallest $s > 0$ such that $\rho(s\Lambda^*) \leq 1 + \epsilon$.*

Informally, the smoothing parameter is the amount of (gaussian) noise that needs to be added to a lattice to obtain a uniformly distributed point in space, as formalized in the next theorem.

Lemma 15 *For any lattice coset $\Lambda + \mathbf{u}$, if $\eta_\epsilon(\Lambda) \leq 1$ then*

$$\rho(\Lambda + \mathbf{u}) \in [1 \pm \epsilon] \cdot \det(\Lambda^*).$$

Proof. Assume $\eta_\epsilon(\Lambda) \leq 1$, or, equivalently, $\rho(\Lambda^*) \leq 1 + \epsilon$. Then

$$\begin{aligned}
|\rho(\Lambda + \mathbf{u}) - \det(\Lambda^*)| &= \det(\Lambda^*)\left|\sum_{\mathbf{y}\in\Lambda^*} \rho(\mathbf{y}) \cdot \exp(2\pi i \langle \mathbf{y}, \mathbf{u}\rangle) - 1\right| \\
&= \det(\Lambda^*)\left|\sum_{\mathbf{y}\in\Lambda^*\setminus\{\mathbf{0}\}} \rho(\mathbf{y}) \cdot \exp(2\pi i \langle \mathbf{y}, \mathbf{u}\rangle)\right| \\
&\leq \det(\Lambda^*) \sum_{\mathbf{y}\in\Lambda^*\setminus\{\mathbf{0}\}} \rho(\mathbf{y}) \\
&= \det(\Lambda^*) \cdot (\rho(\Lambda^*) - 1) \leq \epsilon \cdot \det(\Lambda^*).
\end{aligned}$$

$\square$

It is clear from the definition that for any lattice Λ and scalar $c > 0$, $\eta_\epsilon(c\Lambda) = c\eta_\epsilon(\Lambda)$. Next, we turn to evaluating the smoothing parameter of a lattice. We begin with the integer lattice.

Lemma 16 *For any $\epsilon > 0$, we have*

$$1 + \frac{2}{\exp(\pi s^2)} \leq \rho(s\mathbb{Z}) \leq 1 + \frac{2}{\exp(\pi s^2) - 1}$$

$$\sqrt{\frac{\ln(2/\epsilon)}{\pi}} \leq \eta_\epsilon(\mathbb{Z}) \leq \sqrt{\frac{\ln(1 + 2/\epsilon)}{\pi}}.$$

Proof. For the lower bound, we restrict the summation to the integers $\{-1, 0, 1\} \subset \mathbb{Z}$:

$$\rho(s\mathbb{Z}) \geq \rho(s\{-1, 0, 1\}) = 1 + 2\rho(s) = 1 + \frac{2}{\exp(\pi s^2)}.$$

For the upper bound, we extend the summation over $\sqrt{\mathbb{Z}} = \{\sqrt{n} : n \in \mathbb{Z}\} \supset \mathbb{Z}$:

$$\rho(s\mathbb{Z}) \leq \rho(s\sqrt{\mathbb{Z}}) = 1 + 2\sum_{k \geq 1} \exp(-\pi s^2)^k = 1 + \frac{2}{\exp(\pi s^2) - 1}.$$

Setting the bound to $1 + \epsilon$ and solving for s gives upper and lower bounds on $\eta_\epsilon(\mathbb{Z})$. □

In order to bound the smoothing parameter of arbitrary lattices, we look at how the smoothing parameter interacts with orthogonalization. Notice that for any mutually orthogonal lattice $\langle \Lambda_1, \Lambda_2 \rangle = \{\mathbf{0}\}$, the dual of the sum $(\Lambda_1 + \Lambda_2)^*$ equals the sum of the duals $\Lambda^* + \Lambda^*$, and therefore

$$\rho((\Lambda_1 + \Lambda_2)^*) = \rho(\Lambda_1^* + \Lambda_2^*) = \rho(\Lambda_1^*)\rho(\Lambda_2^*).$$

So, if $s = \eta_{\epsilon_1}(\Lambda_1) = \eta_{\epsilon_2}(\Lambda_2)$, then $s = \eta_\epsilon(\Lambda_1 + \Lambda_2)$ for $\epsilon = \epsilon_1 + \epsilon_2 + \epsilon_1\epsilon_2$. This already gives a way to bound the smoothing parameter of lattices that have an orthogonal basis. But most lattices do not have such a basis, so we need one more tool. For the general case, we use the fact that orthogonalizig a lattice can only increase its smoothing parameter.

Theorem 17 *For any lattice basis $\mathbf{B}$ with Gram-Schmidt orthogonalization $\mathbf{B}^*$ and $\epsilon > 0$,*

$$\eta_\epsilon(\mathcal{L}(\mathbf{B})) \leq \eta_\epsilon(\mathcal{L}(\mathbf{B}^*)).$$

The theorem is proved using Lemma 8, by induction on the dimension, using the relation between the orthogonalization of $\mathbf{B}$ and the orthogonalization (in reverse order) of its dual basis. The details of the proof are left as an exercise.