CSE 206A: Lattice Algorithms and Applications Fall 2019

The Gaussians Distribution

Instructor: *Daniele Micciancio* UCSD CSE

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.

1 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 deal primarily with discrete probability distributions and the fourier transform over finite groups. This allows for a much simpler treatment, using linear algebra.

For any lattice Λ and full rank sublattice $\Gamma \subseteq \Lambda$, the quotient

$$\mathbf{G} = \Lambda/\Gamma = \{\mathbf{x} + \Gamma \mid \mathbf{x} \in \Lambda\}$$

is a finite (additive) group of order $|\mathbf{G}| = \det(\Gamma)/\det(\Lambda)$. (In fact, any finite additive group can be represented this way.)

Exercise 1 *Show that any finite additive group* $\mathbf{G}$ *can be represented as the quotient* Λ/Γ *of two lattices, with* $\Gamma \subseteq \Lambda$. Hint: Let $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$ a set of group elements that generate $\mathbf{G} = \sum_i \mathbf{g}_i \cdot \mathbb{Z}$, and consider the lattices $\Lambda = \mathbb{Z}^n$ and $\Gamma = \{\mathbf{x} \in \mathbb{Z}^n \mid \sum_i x_i \cdot \mathbf{g}_i = 0\}$.

The dual of the group $\mathbf{G} = \Lambda/\Gamma$ is defined as the quotient

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

where Λ^* and Γ^* are the dual lattices of Λ and Γ. Since $\Gamma \subseteq \Lambda$, we also have $\Lambda^* \subseteq \Gamma^*$ and the quotient Γ^*/Λ^* is well defined. Moreover, it is easy to see that the dual group has exactly the same size as the original group:

$$|\widehat{\mathbf{G}}| = \frac{\det(\Lambda^*)}{\det(\Gamma^*)} = \frac{1/\det(\Lambda)}{1/\det(\Gamma)} = \frac{\det(\Gamma)}{\det(\Lambda)} = |\mathbf{G}|.$$

In fact, $\mathbf{G}$ and $\widehat{\mathbf{G}}$ are also isomorphic, though this is harder to see, and it is not even true for arbitrary (possibly infinite) groups.

Exercise 2 *Show that the dual of the dual of a group* $\mathbf{G} = \Lambda/\Gamma$ *equals the original group* $\widehat{\widehat{\mathbf{G}}} = \mathbf{G}$.

The set of functions $V = (\mathbf{G} \to \mathbb{C})$ is a $|\mathbf{G}|$-dimensional vector space over the field $\mathbb{C}$ of complex numbers, where each function $f\colon \mathbf{G} \to \mathbb{C}$ may be identified with the vector $(f(\mathbf{x}))_{\mathbf{x}\in\mathbf{G}} \in \mathbb{C}^{|\mathbf{G}|}$. This vector space has an inner product defined as

$$\langle f, g\rangle = \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[f(\mathbf{x}) \cdot \overline{g(\mathbf{x})}\right] = \frac{1}{|\mathbf{G}|}\sum_{\mathbf{x}\in\mathbf{G}} f(\mathbf{x}) \cdot \overline{g(\mathbf{x})}$$

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

Exercise 3 *Show that $\langle,\rangle$ is indeed an inner product, i.e., it satisfies the following properties: $\langle a\mathbf{x}, \mathbf{y}\rangle = a \cdot \langle \mathbf{x}, \mathbf{y}\rangle$, $\langle \mathbf{x} + \mathbf{z}, \mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle + \langle \mathbf{z}, \mathbf{y}\rangle$, $\langle \mathbf{x}, \mathbf{y}\rangle = \overline{\langle \mathbf{y}, \mathbf{x}\rangle}$, and $\langle \mathbf{x}, \mathbf{x}\rangle \geq 0$, with equality $\langle \mathbf{x}, \mathbf{x}\rangle = 0$ if and only if $\mathbf{x} = \mathbf{0}$.*

Consider the family of functions

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

indexed by $\mathbf{y} \in \widehat{\mathbf{G}}$, mapping $\mathbf{x} \in \mathbf{G}$ to $\mathbb{C}$. Notice that these functions are well defined, because for any representatives $\mathbf{x} \in \Lambda$ and $\mathbf{y} \in \Gamma^*$, the inner product

$$\langle \mathbf{x} + \Gamma, \mathbf{y} + \Lambda^*\rangle = \langle \mathbf{x}, \mathbf{y}\rangle + \langle \mathbf{x}, \Lambda^*\rangle + \langle \Gamma, \mathbf{y}\rangle + \langle \Gamma, \Lambda^*\rangle \subseteq \langle \mathbf{x}, \mathbf{y}\rangle + \mathbb{Z}$$

is well defined modulo $\mathbb{Z}$, and for any integer $z \in \mathbb{Z}$

$$e^{2\pi i(\langle \mathbf{x}, \mathbf{y}\rangle + z)} = e^{2\pi i\langle \mathbf{x}, \mathbf{y}\rangle} \cdot e^{2\pi i z} = e^{2\pi i\langle \mathbf{x}, \mathbf{y}\rangle}.$$

The following lemma shows that this set of functions is an orthonormal basis for V.

Lemma 1 *For any $\mathbf{v}, \mathbf{w} \in \widehat{\mathbf{G}} = \Gamma^*/\Lambda^*$,*

$$\langle \chi_{\mathbf{v}}, \chi_{\mathbf{w}}\rangle = \begin{cases} 1 & \text{if } \mathbf{v} = \mathbf{w} \\ 0 & \text{otherwise} \end{cases}$$

Proof. If $\mathbf{v} = \mathbf{w}$, then $\langle \mathbf{v} - \mathbf{w}, \mathbf{x}\rangle = \langle \mathbf{0}, \mathbf{x}\rangle = 0$, and

$$\langle \chi_{\mathbf{v}}, \chi_{\mathbf{w}}\rangle = \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[e^{2\pi i\langle \mathbf{v}-\mathbf{w}, \mathbf{x}\rangle}\right] = \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[e^{0}\right] = 1.$$

On the other hand, if $\mathbf{v} \neq \mathbf{w}$ (in $\widehat{\mathbf{G}} = \Gamma^*/\Lambda^*$), then $\mathbf{u} = \mathbf{v} - \mathbf{w} \notin \Lambda^*$, and there must exist a vector $\mathbf{y} \in \Lambda$ such that $\langle \mathbf{u}, \mathbf{y}\rangle \notin \mathbb{Z}$. It follows that $e^{2\pi i\langle \mathbf{u}, \mathbf{y}\rangle} \neq 1$. Let $f\colon \mathbf{G} \to \mathbf{G}$ be the function $f(\mathbf{x}) = \mathbf{x} + \mathbf{y}$, and notice that $f(\mathbf{G}) = \mathbf{G}$ because f if bijective. It follows that

$$\begin{aligned}
\langle \chi_{\mathbf{v}}, \chi_{\mathbf{w}}\rangle &= \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[\chi_{\mathbf{v}}(\mathbf{x}) \cdot \overline{\chi_{\mathbf{w}}(\mathbf{x})}\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[e^{2\pi i\langle \mathbf{u}, \mathbf{x}\rangle}\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[e^{2\pi i\langle \mathbf{u}, f(\mathbf{x})\rangle}\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[e^{2\pi i\langle \mathbf{u}, \mathbf{x}\rangle} \cdot e^{2\pi i\langle \mathbf{u}, \mathbf{y}\rangle}\right] \\
&= \langle \chi_{\mathbf{v}}, \chi_{\mathbf{w}}\rangle \cdot e^{2\pi i\langle \mathbf{u}, \mathbf{y}\rangle}.
\end{aligned}$$

Since $e^{2\pi i\langle \mathbf{u},\mathbf{y}\rangle} \neq 1$, it must be $\langle \chi_{\mathbf{v}}, \chi_{\mathbf{w}}\rangle = 0$. $\square$

The functions $\chi_{\mathbf{v}}$ with $\mathbf{v} \in \widehat{\mathbf{G}}$, are called the characters of the group $\mathbf{G}$, and, since there are precisely $|\widehat{\mathbf{G}}| = |\mathbf{G}|$ of them, they form an orthonormal basis for $V = \mathbf{G} \to \mathbb{C}$. In particular, any function can be expressed as a linear combination of the characters

$$f(\mathbf{x}) = \sum_{\mathbf{v}} \langle f, \chi_{\mathbf{v}}\rangle \cdot \chi_{\mathbf{v}}(x).$$

The function $\widehat{f}(\mathbf{v})$ mapping each $\mathbf{v} \in \widehat{\mathbf{G}}$ to the corresponding coefficient $\langle f, \chi_{\mathbf{v}}\rangle$ is called the (discrete) fourier transform of f, and it is defined by the formula

$$\widehat{f}(\mathbf{v}) = \langle f, \chi_{\mathbf{v}}\rangle = \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}}\left[f(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})}\right] = \frac{1}{|\mathbf{G}|}\sum_{\mathbf{x}\in\mathbf{G}} f(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{x},\mathbf{y}\rangle}. \tag{1}$$

Using this linear algebra interpretation, we see that the Fourier transform of a function f is simply the set of coefficients of f with respect to the fourier basis given by the group characters $\chi_{\mathbf{v}}$. Expressing the function f with respect to the fourier basis can be rewritten as

$$f(\mathbf{x}) = \sum_{\mathbf{v}\in\widehat{\mathbf{G}}} \widehat{f}(\mathbf{v}) \cdot e^{2\pi i\langle \mathbf{x},\mathbf{v}\rangle} \tag{2}$$

giving the fourier inversion formula.

Exercise 4 *Give special cases of the fourier transform and inversion formula for the groups* $\mathbf{G} = \mathbb{Z}_q = \mathbb{Z}/(q\mathbb{Z})$*, and* $\mathbf{G}^n = \mathbb{Z}_q^n = \mathbb{Z}^n/(q\mathbb{Z}^n)$*.*

2 Lattices and periodic functions

As we are interested in lattices, it is natural to consider functions $f\colon \Lambda \to \mathbb{C}$ defined over a lattice Λ, as well as functions that are periodic modulo a lattice Λ, i.e., $\varphi(\mathbf{t}+\mathbf{v}) = \varphi(\mathbf{t})$ for every $\mathbf{v} \in \Lambda$. The canonical example of a periodic function is the distance $\varphi(\mathbf{t}) = \inf_{\mathbf{x}\in\Lambda} \|\mathbf{t}-\mathbf{x}\|$ of a target point $\mathbf{t}$ to the lattice Λ. Clearly, shifting the target $\mathbf{t}$ by a lattice point $\mathbf{v}$, does not affect the distance of $\mathbf{t}+\mathbf{v}$ to the lattice.

Let $\Lambda \subset \mathbb{R}^n$ be a full rank lattice, and $\varphi\colon \mathbb{R}^n/\Lambda \to \mathbb{C}$ a periodic function modulo Λ. (All this can be easily extended to lattices that are not full rank by using $\mathrm{span}(\Lambda)$ instead of $\mathbb{R}^n$.) Assume φ is a sufficiently nice function, in the sense that it can be reasonably approximated by the values of $\varphi(\mathbf{x})$ on a fine grid $\mathbf{x} \in \epsilon\Lambda$, as $\epsilon \to 0$. We will use scaling factors $\epsilon = 1/q$ for $q \in \mathbb{Z}$ a large integer, so that Λ is a sublattice of $\epsilon\Lambda = q^{-1}\Lambda$, and restricting φ to $q^{-1}\Lambda$ gives a function $\varphi_q\colon \mathbf{G} \to \mathbb{C}$ defined over a finite group $\mathbf{G}_q = q^{-1}\Lambda/\Lambda \equiv \mathbb{Z}_q^n$ of size $|\mathbf{G}_q| = q^n$. In particular, we can apply the fourier transform over finite groups, to obtain the function

$$\widehat{\varphi}_q(\mathbf{v}) = \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbf{G}_q}\left[\varphi_q(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})}\right] = \frac{1}{q^n}\sum_{\mathbf{x}\in\mathbf{G}_q} \varphi_q(\mathbf{x}) e^{-2\pi i\langle \mathbf{v},\mathbf{x}\rangle} \tag{3}$$

where $\mathbf{v} \in \widehat{G} = \Lambda^*/(q\Lambda^*)$. By the fourier inversion formula (over finite groups), this function satisfies

$$\varphi(\mathbf{x}) = \varphi_q(\mathbf{x}) = \sum_{\mathbf{v}\in\widehat{\mathbf{G}}_q} \widehat{\varphi}_q(\mathbf{v}) \cdot \chi_{\mathbf{v}}(\mathbf{x}) \tag{4}$$

for every $\mathbf{x} \in q^{-1} \cdot \Lambda$. For any $\mathbf{v} \in \Lambda^*$, if φ is continuous, the limit of (3) for $q \to \infty$ is well defined, and it is equals, by definition, to the integral

$$\widehat{\varphi}(\mathbf{v}) = \lim_{q\to\infty} \widehat{\varphi}_q(\mathbf{v}) = \frac{1}{\det(\Lambda)} \cdot \int_{\mathbf{x}\in\mathbb{R}^n/\Lambda} \varphi(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{v},\mathbf{x}\rangle} = \mathop{\mathbb{E}}_{\mathbf{x}\in\mathbb{R}^n/\Lambda} \left[\varphi(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})}\right]. \tag{5}$$

We call this function $\widehat{\varphi}\colon \Lambda^* \to \mathbb{C}$ the fourier transform of the periodic function $\varphi\colon \mathbb{R}^n/\Lambda \to \mathbb{C}$. Taking the limit (4) for $q \to \infty$, gives the corresponding inversion formula:

$$\varphi(\mathbf{x}) = \sum_{\mathbf{v}\in\Lambda^*} \widehat{\varphi}(\mathbf{v}) \cdot \chi_{\mathbf{v}}(\mathbf{x}). \tag{6}$$

Notice the similarity between the fourier transform and inversion formulas (1) (2) for finite groups, and those for periodic function (5) (6). The latter ones are a natural generalization of the finite group formulas to arbitrary (possibly infinite) compact groups. In this context, the dual group of $\mathbf{G} = \mathbb{R}^n/\Lambda$ is defined as $\widehat{\mathbf{G}} = \Lambda^*$. This may seem peculiar at first, but it can be understood by interpreting $\mathbf{G}$ as the limit of $\mathbf{G}_q = q^{-1}\Lambda/\Lambda$ for $q \to \infty$. For each finite q, the dual group is $\widehat{\mathbf{G}}_q = \Lambda^*/(q\Lambda^*)$. But as $q \to \infty$, this quotient gives the entire dual lattice Λ^*, without reduction modulo q.

In a similar fashion, one can define the fourier transform of a function $f\colon \Lambda \to \mathbb{C}$, which will be a function $\hat{f}\colon \mathbb{R}^n/\Lambda \to \mathbb{C}$. However, since Λ is a countable infinite set, we cannot define a uniform distribution over Λ and the expected value of $f(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})}$ for a "randomly chosen" $\mathbf{x} \in \Lambda$. So, in this case, we normalize the fourier transform by the determinant of the lattice rather than the group size, and define

$$\widehat{f}(\mathbf{v}) = \det(\Lambda) \cdot \sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})}$$

where $\mathbf{v} \in \mathbb{R}^n/\Lambda$ is any element of the dual group. Notice that as $\det(\Lambda)$ decreases, the lattice gets denser, and it has more points per unit volume. So, multiplying by $\det(\Lambda)$ is somehow analogous to dividing by the number of points in the lattice. Also, for the summation to be defined, it must be the case that $f(\mathbf{x})$ vanishes at infinity, i.e., $\lim_{\mathbf{x}\to\infty} f(\mathbf{x}) = 0$. As one may expect, the corresponding inversion formula is

$$f(\mathbf{x}) = \int_{\mathbf{v}\in\mathbb{R}/\Lambda^*} \widehat{f}(\mathbf{v}) \cdot \chi_{\mathbf{v}}(\mathbf{x})\, d\mathbf{v}.$$

3 The real fourier transform

We can take this one step forward by considering functions $f\colon \mathbb{R}^n \to \mathbb{C}^n$ of real random variables. This time we regard $\mathbb{R}^n$ as the "limit" of $\epsilon\Lambda$ for an arbitrary lattice Λ and $\epsilon \to 0$.

If we let f_ϵ be the restriction of f to $\epsilon\Lambda$, then we get

$$\widehat{f_\epsilon}(\mathbf{v}) = \det(\epsilon\Lambda) \cdot \sum_{\mathbf{x}\in\epsilon\Lambda} f(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})} \quad \text{and} \quad f_\epsilon(\mathbf{x}) = \int_{\mathbf{v}\in\mathbb{R}/(\epsilon^{-1}\Lambda^*)} \widehat{f_\epsilon}(\mathbf{v}) \cdot \chi_{\mathbf{v}}(\mathbf{x})\, d\mathbf{v}.$$

Taking the limit for $\epsilon \to 0$, we get the fourier transform and inversion formulas for functions of real variables:

$$\begin{aligned} \widehat{f}(\mathbf{v}) &= \int_{\mathbf{x}\in\mathbb{R}^n} f(\mathbf{x}) \cdot \overline{\chi_{\mathbf{v}}(\mathbf{x})}\, d\mathbf{x} = \int_{\mathbf{x}\in\mathbb{R}^n} f(\mathbf{x}) \cdot e^{-2\pi i\langle \mathbf{v},\mathbf{x}\rangle}\, d\mathbf{x} \\ f(\mathbf{x}) &= \int_{\mathbf{v}\in\mathbb{R}^n} \widehat{f_\epsilon}(\mathbf{v}) \cdot \chi_{\mathbf{v}}(\mathbf{x})\, d\mathbf{v} = \int_{\mathbf{v}\in\mathbb{R}^n} \widehat{f_\epsilon}(\mathbf{v}) \cdot e^{2\pi i\langle \mathbf{v},\mathbf{x}\rangle}\, d\mathbf{v}. \end{aligned}$$

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 2 *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 3 *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. □

We know from the proof of Lemma 2 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 4 *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.

4 Poisson summation formula

Theorem 5 *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 6 *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

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

□

5 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. □

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 $|x| > st$.

6 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

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

□

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 orthogonalizing 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.