Lattices in Cryptography
University of Michigan, Fall 2022

Lecture 10
Smoothing Parameter

Instructor: Chris Peikert
Scribe: Hank Carter

Here we introduce a fundamental lattice quantity called the *smoothing parameter*, which is essentially the amount of Gaussian noise needed to completely "smooth out" the discrete structure of a lattice.

1 Background

Recall the following material from previous lectures.

Definition 1.1 (Dual lattice). For a (full-rank) lattice $\mathcal{L} \subset \mathbb{R}^n$, its *dual lattice* is

$$\mathcal{L}^* := \{\mathbf{w} \in \mathbb{R}^n : \langle \mathbf{w}, \mathcal{L} \rangle \subseteq \mathbb{Z}\}.$$

Last time we showed several basic facts about the dual lattice, e.g., $(\mathcal{L}^*)^* = \mathcal{L}$, $\det(\mathcal{L}^*) = \det(\mathcal{L})^{-1}$, and $\mathbf{B}$ is a basis of $\mathcal{L}$ if and only if $\mathbf{B}^{-t}$ is a basis of $\mathcal{L}^*$.

Lemma 1.2 (Poisson Summation Formula (PSF)). *For any "nice enough" $f \colon \mathbb{R}^n \to \mathbb{C}$ having Fourier transform $\hat{f}$, we have*

$$f(\mathcal{L}) = \det(\mathcal{L}^*) \cdot \hat{f}(\mathcal{L}^*). \tag{1.1}$$

Lemma 1.3 (Periodization). *For any full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ and "nice enough" function $f \colon \mathbb{R}^n \to \mathbb{C}$, the induced $\mathcal{L}$-periodic function $g \colon \mathbb{R}^n/\mathcal{L} \to \mathbb{C}$ defined as*

$$g(\mathbf{x} + \mathcal{L}) = f(\mathbf{x} + \mathcal{L}) = \sum_{\mathbf{v} \in \mathbf{x} + \mathcal{L}} f(\mathbf{v})$$

has Fourier series $\hat{g}(\mathbf{w}) = \det(\mathcal{L}^*) \cdot \hat{f}(\mathbf{w})$ for all $\mathbf{w} \in \mathcal{L}^*$.

The *Gaussian function* $\rho \colon \mathbb{R}^n \to \mathbb{R}^+$ is defined as

$$\rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|^2) = \exp(-\pi \langle \mathbf{x}, \mathbf{x} \rangle), \tag{1.2}$$

and its scaling with parameter $s > 0$ is $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s) = \exp(-\pi \|\mathbf{x}\|^2/s^2)$. Recall that $\hat{\rho} = \rho$, and $\hat{\rho_s} = s^n \cdot \rho_{1/s}$.

2 Smoothing Parameter

Last time, we considered the $\mathcal{L}$-periodic Gaussian function $\rho(\mathbf{x} + \mathcal{L})$, and showed that it can be "lumpy," in the sense that:

1. $\rho(\mathbf{x} + \mathcal{L}) \geq \frac{1}{1000} \cdot \rho(\mathcal{L})$ when $\operatorname{dist}(\mathbf{x}, \mathcal{L}) \leq 1$
2. $\rho(\mathbf{x} + \mathcal{L}) \leq 2^{-n} \cdot \rho(\mathcal{L})$ when $\operatorname{dist}(t, \mathcal{L}) \geq \sqrt{n}$, which is equivalent to $(\mathbf{x} + \mathcal{L}) \cap \sqrt{n}\mathcal{B} = \emptyset$.

Today, we consider sufficient conditions that make this function "smooth," i.e., nearly equal on every coset $\mathbf{x} + \mathcal{L}$. First, recall that by the shift rule for the Fourier transform and the PSF (twice),

$$\begin{aligned} \rho(\mathbf{x} + \mathcal{L}) &= \det(\mathcal{L}^*) \cdot \sum_{\mathbf{w} \in \mathcal{L}^*} \rho(\mathbf{w}) \cdot \exp(2\pi i \langle \mathbf{w}, \mathbf{x} \rangle) \\ &\leq \det(\mathcal{L}^*) \cdot \rho(\mathcal{L}^*) = \rho(\mathcal{L}), \end{aligned} \tag{2.1}$$

where the inequality follows because $\exp(2\pi i \langle \mathbf{w}, \mathbf{x} \rangle) \in \mathbb{C}$ is on the complex unit circle and $\rho(\mathbf{w}) > 0$.

When is this upper bound essentially tight, i.e., when do we have near-equality? The following important theorem gives a sufficient condition.

Theorem 2.1. *If $\rho(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \varepsilon$ for some $\varepsilon > 0$, then $\rho(\mathbf{x} + \mathcal{L}) \geq \frac{1-\varepsilon}{1+\varepsilon} \cdot \rho(\mathcal{L})$ for all $\mathbf{x} \in \mathbb{R}^n$.*

Proof. Continuing from Equation (2.1), and separating out the case $\mathbf{w} = \mathbf{0}$, we have

$$\begin{aligned}
\rho(\mathbf{x} + \mathcal{L}) &= \det(\mathcal{L}^*) \cdot (1 + \sum_{\mathbf{w} \in \mathcal{L}^* \setminus \{\mathbf{0}\}} \rho(\mathbf{w}) \cdot \exp(2\pi i \langle \mathbf{w}, \mathbf{x} \rangle)) \\
&\geq \det(\mathcal{L}^*) \cdot (1 - \sum_{\mathbf{w} \in \mathcal{L}^* \setminus \{0\}} \rho(\mathbf{w})) \\
&\geq \det(\mathcal{L}^*) \cdot (1 - \varepsilon) \\
&\geq \frac{1-\varepsilon}{1+\varepsilon} \cdot \det(\mathcal{L}^*) \cdot \rho(\mathcal{L}^*) \\
&= \frac{1-\varepsilon}{1+\varepsilon} \cdot \rho(\mathcal{L}),
\end{aligned}$$

where the first inequality (again) uses the fact that $|\exp(2\pi i \langle \mathbf{w}, \mathbf{x} \rangle)| = 1$ and $\rho(\mathbf{w}) > 0$, and the second and third inequalities uses the hypothesis. □

Theorem 2.1 says that if the dual lattice has small Gaussian mass, then shifting the (primal) lattice has little effect on its Gaussian mass. The mass is maximized on the lattice's zero coset, but the mass changes only slightly as one shifts the lattice around. This fact motivates the following definition.

Definition 2.2 (Smoothing parameter [MR04]). For an $\varepsilon > 0$, the *smoothing parameter* $\eta_\varepsilon(\mathcal{L})$ of a lattice $\mathcal{L}$ is the smallest $s > 0$ such that $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \varepsilon$.

Note that as s increases, $1/s$ decreases, so $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\})$ decreases. So for any $s \geq \eta_\varepsilon(\mathcal{L})$, we have $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \varepsilon$. This in turn means that

$$\rho_s(\mathbf{x} + \mathcal{L}) \geq \frac{1-\varepsilon}{1+\varepsilon} \cdot \rho_s(\mathcal{L})$$

for any $\mathbf{x} \in \mathbb{R}^n$, simply by scaling and applying Theorem 2.1.

The following small claim will be useful for bounding the smoothing parameter by bounding the *fraction* of Gaussian mass on the non-zero points of the dual lattice.

Claim 2.3. *If $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \frac{\varepsilon}{1+\varepsilon} \cdot \rho_{1/s}(\mathcal{L}^*)$, then $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \varepsilon$, and hence $s \geq \eta_\varepsilon(\mathcal{L})$.*

Proof. We have $\rho_{1/s}(\mathcal{L}^*) = 1 + \rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq 1 + \frac{\varepsilon}{1+\varepsilon} \cdot \rho_{1/s}(\mathcal{L}^*)$. Rearranging proves the claim. □

We can relate $\eta_\varepsilon(\mathcal{L})$ to "standard" lattice quantities. We first connect it to the minimum distance of the dual lattice.

Lemma 2.4. *For any (full-rank) lattice $\mathcal{L} \in \mathbb{R}^n$ and $\varepsilon = 4^{-n}$, we have that*

$$\eta_\varepsilon(\mathcal{L}) \leq \frac{\sqrt{n}}{\lambda_1(\mathcal{L}^*)}.$$

Proof. For notational convenience, by scaling $\mathcal{L}$ (and its dual) we can assume that $s = \sqrt{n}/\lambda_1(\mathcal{L}^*) = 1$, so $\lambda_1(\mathcal{L}^*) = \sqrt{n}$. We then need to show that $\rho(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \varepsilon = 2^{-n}$.

Recall from the previous lecture that the Gaussian mass of any lattice (coset) outside the radius-$\sqrt{n}$ ball is a tiny fraction of the lattice's total Gaussian mass: $\rho((\mathbf{x}+\mathcal{L}^*)\setminus\sqrt{n}\mathcal{B}) \leq 5^{-n}\cdot\rho(\mathcal{L}^*)$.[1] Since $\lambda_1(\mathcal{L}^*) \geq \sqrt{n}$, we have that

$$\begin{aligned}\rho(\mathcal{L}^*\setminus\{\mathbf{0}\}) &= \rho(\mathcal{L}^*\setminus\sqrt{n}\mathcal{B}) \\ &\leq 5^{-n}\cdot\rho(\mathcal{L}^*) \\ &\leq \frac{1}{4^n+1}\cdot\rho(\mathcal{L}^*).\end{aligned}$$

The lemma then follows from Claim 2.3. □

Lemma 2.5. *For any lattice $\mathcal{L}$ and $\varepsilon \leq 2\exp(-\pi)$, we have that $\eta_\varepsilon(\mathcal{L}) \geq 1/\lambda_1(\mathcal{L}^*)$.*

Proof. Again, by scaling we can assume that $s = 1/\lambda_1(\mathcal{L}^*) = 1$, so $\lambda_1(\mathcal{L}^*) = 1$. Then $\rho(\mathcal{L}^*\setminus\{\mathbf{0}\}) \geq 2\exp(-\pi)$, by considering just the Gaussian mass on any shortest nonzero vector and its negation. □

We next relate the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ to quantities of the primal lattice $\mathcal{L}$ itself. For intuition, consider the possibility that $\eta(\mathcal{L}) \leq \lambda_1(\mathcal{L})$, which intuitively could hold in many cases. However, this is false in general. As a counterexample, consider the lattice with basis $(1,0),(0,100)$. While the sum of the lattice-centered Gaussians on the x-axis is fairly "smooth," the lattice points on the y-axis are too far separated, making the Gaussians "lumpy" in that direction.

This can be seen in another way—which corresponds to the actual definition of the smoothing parameter—by looking at the dual lattice, which has basis $(1,0),(0,1/100)$. The Gaussian mass of nonzero dual points on the x-axis is very small, but the mass of those on the y-axis is fairly large, because they are so tightly spaced together. Indeed, Lemma 2.5 says that $\eta_\varepsilon \geq 1/\lambda_1(\mathcal{L}^*) = 100 \gg \lambda_1(\mathcal{L}) = 1$ even for a moderately small constant $\varepsilon > 0$.

Below we will give a general smoothing-parameter bound which shows that, in this particular example (and as one might expect), to get "smoothness" we need to use Gaussians of width approximately 100, times small extra factor.

Definition 2.6. The *ith successive minimum* of a lattice $\mathcal{L}$ is defined as

$$\begin{aligned}\lambda_i(\mathcal{L}) &= \min\{r : (\mathcal{L}\cap r\mathcal{B}) \text{ contains at least } i \text{ linearly independent vectors}\} \\ &= \min\{r : \dim(\operatorname{span}(\mathcal{L}\cap r\mathcal{B})) \geq i\}.\end{aligned}$$

Thus, for a (full-rank) n-dimensional lattice, $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.

Theorem 2.7 ([MR04]). *For any $\varepsilon > 0$ and (full-rank) n-dimensional lattice $\mathcal{L}$, we have*

$$\eta_\varepsilon(\mathcal{L}) \leq \lambda_n(\mathcal{L})\cdot\sqrt{\ln(2n(1+1/\varepsilon))/\pi} = \lambda_n(\mathcal{L})\cdot O(\sqrt{\ln(2n/\varepsilon)}).$$

For example, if we use an exponentially small $\varepsilon = \exp(-n)$, then $\sqrt{\ln(2n/\varepsilon)} \approx \sqrt{n}$. Or, we can use an inverse-quasipolynomial $\varepsilon = 1/n^{\log n}$ to get $\sqrt{\ln(2n/\varepsilon)} \approx \log n$. To prove Theorem 2.7, we will use a new discrete tail bound for Gaussians.

[1] We previously stated the claim with only a 2^{-n} factor, but a 5^{-n} factor can be obtained from the same proof and the fact that $\exp(3\pi/4) > 10$.

Definition 2.8. For a unit vector $\mathbf{u} \in \mathbb{R}^n$ and real $t \geq 0$, define the (open) *halfspace*

$$H_{\mathbf{u},t} = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{u} \rangle < t\}.$$

In words, $H_{\mathbf{u},t}$ is the set of points in $\mathbb{R}^n$ that are at most t from the origin in the direction of $\mathbf{u}$.

Lemma 2.9 ([Ban95]). *For any lattice $\mathcal{L}$, unit vector $\mathbf{u} \in \mathbb{R}^n$, real $t \geq 0$, and $\mathbf{x} \in \mathbb{R}^n$, we have that*

$$\rho((\mathbf{x} + \mathcal{L}) \setminus H_{\mathbf{u},t}) \leq \exp(-\pi t^2) \cdot \rho(\mathcal{L}).$$

The proof works somewhat similarly to the proof of the tail bound from the previous lecture. That is, we consider multiplying the Gaussian mass of the coset points that are *outside* the halfspace by some very large factor. Then we show that the resulting mass is upper bounded by a not-too-large multiple of the Gaussian mass on the lattice. The only way this can be possible is if the (original) Gaussian mass outside the halfspace is a small fraction of the lattice's total mass.

Proof. Because $\langle \mathbf{v}, \mathbf{u} \rangle \geq t$ for every $\mathbf{v} \notin H_{\mathbf{u},t}$, and by completing the square, we have

$$\begin{aligned}
\exp(2\pi t^2) \cdot \rho((\mathbf{x} + \mathcal{L}) \setminus H_{\mathbf{u},t}) &\leq \sum_{\mathbf{v} \in \mathbf{x} + \mathcal{L}} \rho(\mathbf{v}) \cdot \exp(2\pi \langle \mathbf{v}, t\mathbf{u} \rangle) \\
&= \sum_{\mathbf{v} \in \mathbf{x} + \mathcal{L}} \exp(-\pi(\langle \mathbf{v}, \mathbf{v} \rangle - 2\langle \mathbf{v}, t\mathbf{u} \rangle)) \\
&= \sum_{\mathbf{v} \in \mathbf{x} + \mathcal{L}} \exp(-\pi \langle \mathbf{v} - t\mathbf{u}, \mathbf{v} - t\mathbf{u} \rangle) \cdot \exp(\pi \langle t\mathbf{u}, t\mathbf{u} \rangle) \\
&= \exp(\pi t^2) \cdot \sum_{\mathbf{w} \in \mathbf{x} - t\mathbf{u} + \mathcal{L}} \exp(-\pi \langle \mathbf{w}, \mathbf{w} \rangle) \\
&= \exp(\pi t^2) \cdot \rho(\mathbf{x} - t\mathbf{u} + \mathcal{L}) \\
&\leq \exp(\pi t^2) \cdot \rho(\mathcal{L}).
\end{aligned}$$

Dividing both sides of the inequality by $\exp(2\pi t^2)$ proves the claim. □

(An interesting fact related to Lemma 2.9 is that a *continuous* Gaussian has the same kind of tail behavior: the tail probability outside $H_{\mathbf{u},t}$ is upper bounded by $\exp(-\pi t^2)$. This can be shown by a similar argument using integrals.)

Proof of Theorem 2.7. By Claim 2.3, it suffices to show that $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \frac{\varepsilon}{1+\varepsilon} \cdot \rho(\mathcal{L}^*)$. As usual, by scaling the lattice we can assume that $s = \lambda_n(\mathcal{L}) \cdot \sqrt{\ln(2n(1 + 1/\varepsilon))/\pi} = 1$.

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathcal{L}$ be such that $\|\mathbf{v}_i\| = \lambda_i := \lambda_i(\mathcal{L})$ for all i. (Actually, it will be enough that $\|\mathbf{v}_i\| \leq \lambda_n$.) Observe that any $\mathbf{w} \in \mathcal{L}^* \setminus \{\mathbf{0}\}$ has *nonzero integer* inner product with at least one of the $\mathbf{v}_i$, because they span $\mathbb{R}^n$ and $\mathbf{w}$ is in the dual lattice. So, $|\langle \mathbf{w}, \mathbf{v}_i \rangle| \geq 1$, which implies that

$$|\langle \mathbf{w}, \mathbf{u}_i \rangle| \geq 1/\|\mathbf{v}_i\| \geq 1/\lambda_n = \sqrt{\ln(2n(1 + 1/\varepsilon))/\pi},$$

where $\mathbf{u}_i = \mathbf{v}_i / \|\mathbf{v}_i\|$ is the unit vector in the direction of $\mathbf{v}_i$. Therefore, every $\mathbf{w} \in \mathcal{L}^* \setminus \{\mathbf{0}\}$ is outside *at least one* halfspace $H_{\pm\mathbf{u}_i, 1/\lambda_n}$, so we have

$$\rho(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \sum_{i=1}^{n} \rho(\mathcal{L}^* \setminus H_{\mathbf{u}_i, 1/\lambda_n}) + \rho(\mathcal{L}^* \setminus H_{-\mathbf{u}_i, 1/\lambda_n}).$$

We complete the proof by invoking Lemma 2.9: it says that each term in the above sum is at most

$$\exp(-\pi/\lambda_n^2) \cdot \rho(\mathcal{L}^*) = \exp(-\ln(2n(1+1/\varepsilon))) \cdot \rho(\mathcal{L}^*) = \frac{\varepsilon}{2n(1+\varepsilon)} \cdot \rho(\mathcal{L}^*).$$

The sum has $2n$ such terms, so we have shown that $\rho(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \frac{\varepsilon}{1+\varepsilon} \cdot \rho(\mathcal{L}^*)$, as desired. □

References

[Ban95] W. Banaszczyk. Inequalites for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$. *Discrete & Computational Geometry*, 13:217–231, 1995. Page 4.

[MR04] D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007. Preliminary version in FOCS 2004. Pages 2 and 3.