Gaussian and Smoothness

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

November, 2025

XI

---

1 Introduction

So far, we have built the tools and basics in lattice. We looked at basis reduction, solving the shortest vector problem, and solving the closest vector problem. We touched on concepts that we would use as tools, such as Fourier analysis and algebra in mathematics, among others. Now, as we move forward, we will examine a more advanced version of what we have seen so far. In this article, we will discuss of solving the Closest vector problem in a randomized way within a polynomial error bound.

2 Revisiting Some Results

1. $f(x+\mathcal{L}) = det(\mathcal{L}^*) \cdot \sum_{w\in\mathcal{L}^*} \hat{f}(w) \cdot e^{2\pi i\langle w,x\rangle}$
2. **Poission Summasion Formula**

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

3. $\hat{\rho}(y) = s^n\rho_{1/s}(y)$
4. $e^{-x} + e^x \geq 2$

3 The Problem

We are given a lattice $\mathcal{L}$, and we want to process advice that would efficiently provide us with some answer of the form either $\text{dist}(x,\mathcal{L}) \leq 1$ or $\text{dist}(x,\mathcal{L}) \geq \sqrt{n}$. In particular, we are solving the $GapCVP_{\sqrt{n}}$ on the preprocessed lattice.

4 CVP with Preprocessing

The strategy is to use a $\mathcal{L}$ periodic function $g(x)$ such that

(i) $g(x) \geq 1/1000$ whenever $\text{dist}(x,\mathcal{L}) \leq 1$

(ii) $g(x) \leq 2^{-n}$ whenever $\text{dist}(x,\mathcal{L}) \geq \sqrt{n}$

(iii) $g(x)$ is efficiently computable every time with negligible error.

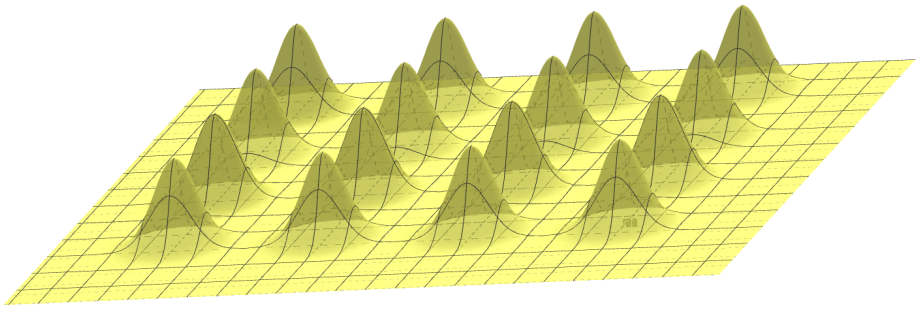

Figure 1: Gaussian Function in 3D

To determine if a point $\mathbf{x}$ is close to or far from the lattice, we just need to estimate the value of g.

Definition 4.1. **($\mathcal{L}$ periodic scaled Gaussian)**
We define the function $\rho_s : \mathbb{R}^n \to \mathbb{R}^+$ *as*

$$\rho_s(\mathbf{x}) := e^{-\pi\|\mathbf{x}/s\|^2}$$

From this we define the $\mathcal{L}$ *periodic Gaussian* $g : \mathbb{R}^n \to \mathbb{R}^+$ *as*

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

Then we define $\mathcal{L}$ *periodic scaled Gaussian* $g : \mathbb{R}^n \to \mathbb{R}^+$ *as*

$$g(x) = \frac{f(x)}{f(\mathbf{0})} = \frac{\sum_{\mathbf{v}\in\mathcal{L}} \rho(x+\mathbf{v})}{\sum_{\mathbf{v}\in} \rho(\mathbf{v})} = \frac{\rho(\mathbf{x}+\mathcal{L})}{\rho(\mathcal{L})}$$

$\rho(\mathbf{x}+\mathcal{L}) \leq \rho(\mathcal{L})$ for any $\mathbf{x} \in \mathbb{R}^n$.

Recall the following result

(a) Fourier time shift

For a function shifted by c, i.e. if a function $h(x) = f(x+c)$, then its Fourier Transform is given as $\hat{h}(w) = \hat{f}(w)e^{2\pi ixw}$
Equivalently, for a lattice shift (a shift by $\mathbf{v} \in \mathcal{L}$) if we have $h(\mathbf{x}) = f(\mathbf{x}+\mathbf{v})$, then the function's Fourier Transform is given as $\hat{h}(\mathbf{w}) = \hat{f}(\mathbf{w})e^{2\pi i\langle \mathbf{x},\mathbf{w}\rangle}$

(b) Poisson Summation Formula

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

Proof.

$$\rho(\mathbf{x}+\mathcal{L}) = \sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{x}+\mathbf{v}) = \det(\mathcal{L}^*) \sum_{\mathbf{w}\in\mathcal{L}^*} \hat{\rho}(\mathbf{w}) e^{2\pi i\langle \mathbf{x},\mathbf{w}\rangle}$$
$$\leq \det(\mathcal{L}^*) \sum_{\mathbf{w}\in\mathcal{L}^*} \rho(\mathbf{w}) = \rho(\mathcal{L})$$

□

The claim states that the maximum value of the function ρ_s is attained at points $\mathbf{x} \in \mathcal{L}$.

Result 4.2. *For any $s \geq 1$ we have $\rho_s(\mathcal{L}) \leq s^n \cdot \rho(\mathcal{L})$ where $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$ for any $\mathbf{x} \in \mathbb{R}^n$.*

Proof. **Recall Fourier time scaling**
For a function scaled by s, i.e. if a function $h(x) = f(sx)$, then its Fourier Transform is given as $\hat{h}(w) = 1/s\hat{f}(w/s)$

$$\rho_s = e^{-\pi\|\mathbf{x}/s\|^2} \text{ then, } \hat{\rho}_s = s^n \cdot \rho_{1/s}$$

$$\rho_s(\mathcal{L}) = \det(\mathcal{L}^*) \cdot \hat{\rho}_s(\mathcal{L}^*) = \det(\mathcal{L}^*) \cdot s^n \cdot \rho_{1/s}(\mathcal{L}^*) \leq s^n \cdot \det(\mathcal{L}^*) \cdot \rho(\mathcal{L}^*) = s^n \cdot \rho(\mathcal{L})$$

□

Lemma 4.3. *For any $\mathbf{x} \in \mathbb{R}^n$ we have $g(\mathbf{x}) \geq e^{-\pi dist(\mathbf{x},\mathcal{L})^2}$.*

Proof. We know that $\mathbf{x}+\mathcal{L} = \mathbf{x}-\mathcal{L}$ and $e^x + e^{-x} \geq 2$ so we proceed as,

$$\begin{aligned}
\rho(\mathbf{x}+\mathcal{L}) &= \frac{\rho(\mathbf{x}+\mathcal{L}) + \rho(\mathbf{x}-\mathcal{L})}{2} \\
&= \frac{1}{2}\sum_{\mathbf{v}\in\mathcal{L}} \left(e^{-\pi\|\mathbf{x}+\mathbf{v}\|^2} + e^{-\pi\|\mathbf{x}-\mathbf{v}\|^2}\right) \\
&= \frac{1}{2}\sum_{\mathbf{v}\in\mathcal{L}} e^{-\pi\|\mathbf{x}\|^2-\pi\|\mathbf{v}\|^2-2\pi\langle\mathbf{x},\mathbf{v}\rangle} \cdot e^{-\pi\|\mathbf{x}\|^2-\pi\|\mathbf{v}\|^2+2\pi\langle\mathbf{x},\mathbf{v}\rangle} \\
&= \frac{1}{2}\sum_{\mathbf{v}\in\mathcal{L}} e^{-\pi\|\mathbf{x}\|^2} \cdot e^{-\pi\|\mathbf{v}\|^2} \cdot \left(e^{-2\pi\langle\mathbf{x},\mathbf{v}\rangle} + e^{2\pi\langle\mathbf{x},\mathbf{v}\rangle}\right) \\
&= \frac{1}{2} \cdot e^{-\pi\|\mathbf{x}\|^2} \sum_{\mathbf{v}\in\mathcal{L}} e^{-\pi\|\mathbf{v}\|^2} \cdot \left(e^{-2\pi\langle\mathbf{x},\mathbf{v}\rangle} + e^{2\pi\langle\mathbf{x},\mathbf{v}\rangle}\right) \\
&\geq e^{-\pi\|\mathbf{x}\|^2} \sum_{\mathbf{v}\in\mathcal{L}} e^{-\pi\|\mathbf{v}\|^2} = e^{-\pi\|\mathbf{x}\|^2} \cdot \rho(\mathcal{L})
\end{aligned}$$

Now we normalize $\rho(\mathbf{x}+\mathcal{L})$ to obtain,

$$g(x) = \frac{\rho(\mathbf{x}+\mathcal{L})}{\rho(\mathcal{L})} \geq e^{-\pi\|\mathbf{x}\|^2}$$

□

Observation: When $\text{dist}(\mathbf{x},\mathcal{L}) \leq 1$ then $g(x) \geq e^{-\pi} \approx 0.043$, so our first requirement is met.

(i) ✓ $g(x) \geq 1/1000$ whenever $\text{dist}(x,\mathcal{L}) \leq 1$

(ii) $g(x) \leq 2^{-n}$ whenever $\text{dist}(x,\mathcal{L}) \geq \sqrt{n}$

(iii) $g(x)$ is efficiently computable every time with negligible error.

Now we will prove a lemma which we would call a **tail bound** (a tail bound is a mathematical inequality that provides an upper limit on the probability that a random variable will have a value far from its mean).

Lemma 4.4. (Ban93) *For any coset* $\mathbf{x}+\mathcal{L}$ *we have* $\rho((\mathbf{x}+\mathcal{L})-\sqrt{n}\mathcal{B}) \leq 2^{-n}\cdot\rho(\mathcal{L})$ *where* $\mathcal{B}$ *is the open unit ball.*

Proof. Let $\mathcal{D} = (\mathbf{x}+\mathcal{L})-\sqrt{n}\mathcal{B}$

We already have two important results,

1. $\rho_s(\mathcal{L}) \leq s^n\cdot\rho(\mathcal{L}) \implies \rho_2(\mathcal{L}) \leq 2^n\cdot\rho(\mathcal{L})$
2. $\rho(\mathbf{x}+\mathcal{L}) \leq \rho(\mathcal{L}) \implies \rho_2(\mathbf{x}+\mathcal{L}) \leq \cdot\rho_2(\mathcal{L})$

They provide us with the inequality,

$$\rho_2(\mathbf{x}+\mathcal{L}) \leq 2^n\cdot\rho(\mathcal{L})$$

$$\begin{aligned}
2^n\cdot\rho(\mathcal{L}) &\geq \rho_2(\mathbf{x}+\mathcal{L}) \\
&= \sum_{\mathbf{v}\in\mathbf{x}+\mathcal{L}} e^{-\pi\|\frac{\mathbf{v}}{2}\|^2} \geq \sum_{\mathbf{v}\in\mathcal{D}} e^{-\pi\|\frac{\mathbf{v}}{2}\|^2} \\
&= \sum_{\mathbf{v}\in\mathcal{D}} e^{3\pi\|\frac{\mathbf{v}}{2}\|^2}\cdot e^{-\pi\|\mathbf{v}\|^2} \\
&\geq e^{3\pi n/4}\cdot\sum_{\mathbf{v}\in\mathcal{D}} e^{-\pi\|\mathbf{v}\|^2} \geq 4^n\cdot\rho(\mathcal{D})
\end{aligned}$$

$$\pi \geq 3 \implies 3\pi/4 \geq 9/4 \geq 2$$
$$e \geq 2 \implies e^{3\pi/4} \geq 2^{3\pi/4} \geq 2^2$$

So,

$$e^{(3\pi/4)n} \geq 4^n$$

□

Lemma 4.5. *If* $dist(\mathbf{x},\mathcal{L}) \geq \sqrt{n}$ *then* $g(x) \leq 2^{-n}$.

Proof.

$$g(\mathbf{x}+\mathcal{L}) = \frac{\rho(\mathbf{x}+\mathcal{L})}{\rho(\mathcal{L})} = \frac{\rho((\mathbf{x}+\mathcal{L})-\sqrt{n}\mathcal{B})}{\rho(\mathcal{L})} \leq 2^{-n}$$

□

Observation: When $\text{dist}(\mathbf{x},\mathcal{L}) \leq 1$ then $g(x) \geq e^{-\pi} \approx 0.043$, so our first requirement is met.

(i) ✓ $g(x) \geq 1/1000$ whenever $\text{dist}(x,\mathcal{L}) \leq 1$

(ii) $g(x) \leq 2^{-n}$ whenever $\text{dist}(x, \mathcal{L}) \geq \sqrt{n}$

(iii) $g(x)$ is efficiently computable every time with negligible error.

Result 4.6. *Given a polynomial-time advice about $\mathcal{L}$, the function g can be computed efficiently within a small error.*

$$\hat{g}(\mathbf{w}) = \frac{\det(\mathcal{L}^*) \cdot \hat{\rho}(\mathbf{w})}{\rho(\mathcal{L})} = \frac{\det(\mathcal{L}^*) \cdot \hat{\rho}(\mathbf{w})}{\det(\mathcal{L}^*) \cdot \hat{\rho}(\mathcal{L}^*)} = \frac{\rho(\mathbf{w})}{\rho(\mathcal{L}^*)} \in [0, 1]$$

Now we have,

$$g(x) = \sum_{\mathbf{w} \in \mathcal{L}^*} \hat{g}(\mathbf{w}) e^{2\pi i \langle \mathbf{x}, \mathbf{w} \rangle} = \mathop{\mathbb{E}}_{\mathbf{w} \leftarrow \hat{g}} [\cos(2\pi \langle \mathbf{x}, \mathbf{w} \rangle)]$$

Observation: When $\text{dist}(\mathbf{x}, \mathcal{L}) \leq 1$ then $g(x) \geq e^{-\pi} \approx 0.043$, so our first requirement is met.

(i) $g(x) \geq 1/1000$ whenever $\text{dist}(x, \mathcal{L}) \leq 1$

(ii) $g(x) \leq 2^{-n}$ whenever $\text{dist}(x, \mathcal{L}) \geq \sqrt{n}$

(iii) $g(x)$ is efficiently computable every time with negligible error.

To approximate g all we need is a random sampling of $\mathbf{w} \in \mathcal{L}^*$ in the probability distribution of $\hat{g}$. Doing this we can get the average value of $\cos(2\pi \langle \mathbf{x}, \mathbf{w} \rangle)$. Thus we can take enough sample to make it more accurate, to estimate g. Applying probability theory we can always bound it within a sum of polynomial error.

5 Smoothing

We will try to define gaussian on $\mathcal{L}$ that would behave very much same as uniform distribution.

Lemma 5.1. *Let $\mathcal{L}$ be a lattice with basis B, then the statistical distance between the uniform distribution defined on $\mathcal{P}(B)$ and the discrete Gaussian sampling with modulo $\mathcal{P}(B)$ is at-most $\frac{1}{2}\rho_{1/s}(\mathcal{L}^* - \mathbf{0})$*

Proof. The uniform distribution over $\mathcal{P}(B)$ is

$$U(x) = \frac{1}{\det(\mathcal{L})} = \det(\mathcal{L}^*)$$

Now, define the discrete gaussian as

$$\frac{\rho_s(\mathbf{x})}{s^n}$$

The distribution function for modulo $\mathcal{P}(B)$ is

$$\begin{aligned} Y(x) = \sum_{\mathbf{x} \in \mathcal{L}} \frac{\rho_s(\mathbf{x})}{s^n} &= \frac{\rho_s(\mathbf{x} + \mathcal{L})}{s^n} \\ &= \frac{1}{s^n} \det(\mathcal{L}^*) s^n \sum_{\mathbf{w} \in \mathcal{L}^*} \rho_{1/s} e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} \\ &= \det(\mathcal{L}^*) \left(1 + \sum_{\mathbf{w} \in \mathcal{L}^* - \{\mathbf{0}\}} \rho_{1/s} e^{-2\pi i \langle \mathbf{w}, \mathbf{x} \rangle} \right) \end{aligned}$$

Now we calculate the statistical distance as

$$\begin{aligned}
\Delta(Y,U) &= \frac{1}{2}\int_{\mathcal{P}(B)} |Y(x)-U(x)| \\
&\leq \frac{1}{2}\det(\mathcal{L}) \max_{\mathbf{x}\in\mathcal{P}(B)} |Y(x)-U(x)| \\
&\leq \frac{1}{2}\det(\mathcal{L}) \max_{\mathbf{x}\in\mathcal{P}(B)} \left|\det\left(\mathcal{L}^*\right)\left(1+\sum_{\mathbf{w}\in\mathcal{L}^*-\{\mathbf{0}\}} \rho_{1/s}e^{-2\pi i\langle \mathbf{w},\mathbf{x}\rangle}\right) - \det\left(\mathcal{L}^*\right)\right| \\
&\leq \frac{1}{2}\det(\mathcal{L})\det\left(\mathcal{L}^*\right) \max_{\mathbf{x}\in\mathcal{P}(B)} \left|1+\sum_{\mathbf{w}\in\mathcal{L}^*-\{\mathbf{0}\}} \rho_{1/s}e^{-2\pi i\langle \mathbf{w},\mathbf{x}\rangle} - 1\right| \\
&\leq \frac{1}{2} \max_{\mathbf{x}\in\mathcal{P}(B)} \left|\sum_{\mathbf{w}\in\mathcal{L}^*-\{\mathbf{0}\}} \rho_{1/s}e^{-2\pi i\langle \mathbf{w},\mathbf{x}\rangle}\right| \leq \frac{1}{2}\sum_{\mathbf{w}\in\mathcal{L}^*-\{\mathbf{0}\}} |\rho_{1/s}| \leq \frac{1}{2}\rho_{1/s}(\mathcal{L}^*-\{\mathbf{0}\})
\end{aligned}$$

□

Definition 5.2. *For an $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ of a lattice $\mathcal{L}$ is the smallest value $s > 0$ such that $\rho_{1/s}(\mathcal{L}^* - \{0\}) \leq \varepsilon$*

Definition 5.3. **(Smoothing Parameter)** *For a full rank lattice $\mathcal{L} \subset \mathbb{R}$ an $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ of a lattice $\mathcal{L}$ is the smallest value $s > 0$ such that $\rho_{1/s}(\mathcal{L}^*) = 1 + \varepsilon$*

$$\eta_\varepsilon(\mathcal{L}) := \min\{s > 0 \mid \rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) \leq \varepsilon\}$$

Change in value of s affects the function $\rho_{1/s}$ as

(i) $\rho_{1/s}(\mathcal{L}^*) \to 0$ as $s \to \infty$

(i) $\rho_{1/s}(\mathcal{L}^*) \to 1$ as $s \to 0$

From the plots in the figure we observe that, given any value of s we want a function that has value as small as we please except for the origin $\mathbf{O}$.

We will look at the motivation behind this definition step by step

1. $\forall\ s > 0$ and $\mathbf{x} \in \mathbb{R}^n$ we define the gaussian mass function

$$\rho_s(\mathbf{x}+\mathcal{L}) = \sum_{\mathbf{v}\in\mathcal{L}} \rho_s(\mathbf{x}+\mathbf{v}) = \sum_{\mathbf{v}\in\mathcal{L}} e^{-\pi\|\mathbf{x}+\mathbf{v}\|^2/s^2}$$

2. Applying summasion formula we get,

$$\rho_s(\mathbf{x}+\mathcal{L}) = \det(\mathcal{L}^*)\cdot s^n \cdot \sum_{\mathbf{w}\in\mathcal{L}^*} \rho_{1/s}(\mathbf{w})e^{-2\pi i\langle \mathbf{x},\mathbf{w}\rangle}$$

3. For the term $\mathbf{w} = \mathbf{0}$ we have constant value of $\rho_{1/s}(\mathbf{w})$ and rest terms do change if we change the value of $\mathbf{x}$. For making it smooth these terms need to negligible/bounded/constant.

4. The rest terms are bounded only when

$$\sum_{\mathbf{w}\in\mathcal{L}^*-\mathbf{0}} \rho_{1/s}(\mathbf{w}) \leq \varepsilon$$

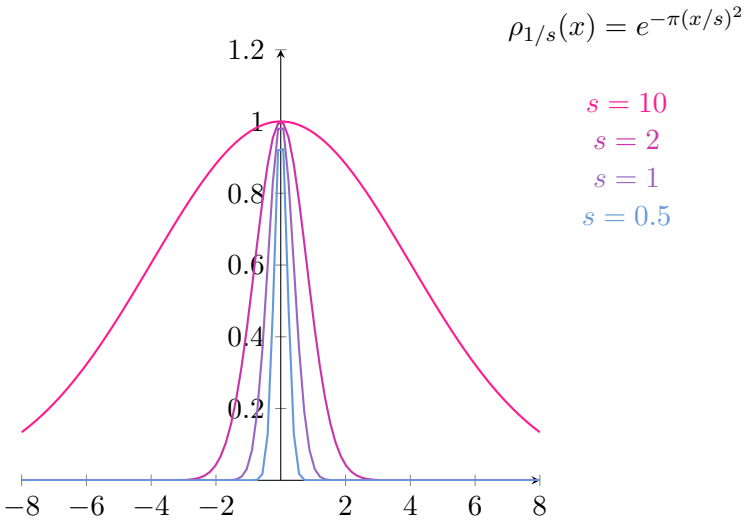

Figure 2: Variability of $\rho_{1/s}(x)$ across different values of s

which turns out to be,

$$\rho_{1/s}(\mathcal{L}^* - \mathbf{0}) \leq \varepsilon$$

Theorem 5.4. *If* $\rho(\mathcal{L}^* - \{\mathbf{0}\}) \leq \varepsilon$ *then* $\rho(\mathbf{x} + \mathcal{L}) \geq \frac{1-\varepsilon}{1+\varepsilon} \cdot \rho(\mathcal{L})$

Proof.

$$\begin{aligned}
\rho(\mathbf{x} + \mathcal{L}) &= \det(\mathcal{L}^*) \sum_{\mathbf{w} \in \mathcal{L}^*} \rho(\mathbf{w}) \cdot e^{2\pi i \langle \mathbf{x}, \mathbf{w} \rangle} \\
&= \det(\mathcal{L}^*) \left(1 + \sum_{\mathbf{w} \in \mathcal{L}^* - \{\mathbf{0}\}} \rho(\mathbf{w}) \cdot e^{2\pi i \langle \mathbf{x}, \mathbf{w} \rangle} \right) \\
&\geq \det(\mathcal{L}^*) \left(1 - \sum_{\mathbf{w} \in \mathcal{L}^* - \{\mathbf{0}\}} \rho(\mathbf{w}) \right) \\
&\geq \det(\mathcal{L}^*) \cdot (1 - \varepsilon) \qquad \text{[using the hypothesis]} \\
&= \frac{\rho(\mathcal{L})}{1 + \varepsilon} \cdot (1 - \varepsilon) = \frac{1 - \varepsilon}{1 + \varepsilon} \cdot \rho(\mathcal{L})
\end{aligned}$$

Now we show that $\det(\mathcal{L}^*) = \frac{\rho(\mathcal{L})}{1+\varepsilon}$ as,

$$\begin{aligned}\rho(\mathcal{L}) &= \det(\mathcal{L}^*) \sum_{\mathbf{w}\in\mathcal{L}^*} \rho(\mathbf{w}) \\ &= \det(\mathcal{L}^*) \left(1 + \sum_{\mathbf{w}\in\mathcal{L}^*-\{\mathbf{0}\}} \rho(\mathbf{w})\right) \\ &= \det(\mathcal{L}^*)(1+\varepsilon)\end{aligned}$$

or,

$$\det(\mathcal{L}^*) = \frac{\rho(\mathcal{L})}{1+\varepsilon}$$

□

Above theorem says that the occurrence of small Gaussian mass in the dual lattice has weak effect in changing the Gaussian mass of the primal lattice with any shift.

Result 5.5. *If* $\rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) \leq \frac{\varepsilon}{1+\varepsilon} \cdot \rho_{1/s}(\mathcal{L}^*)$ *then* $\rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) \leq \varepsilon$ *and hence* $s \geq \eta_\varepsilon(\mathcal{L})$

Proof.

$$\begin{aligned}\rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) &= \frac{\varepsilon}{1+\varepsilon} \cdot \rho_{1/s}(\mathcal{L}^*) \\ &= \frac{\varepsilon}{1+\varepsilon} \cdot \left(1 + \rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\})\right) \\ (1+\varepsilon) \cdot \rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) &\leq \varepsilon + \varepsilon \cdot \rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) \\ \rho_{1/s}(\mathcal{L}^* - \{\mathbf{0}\}) &\leq \varepsilon\end{aligned}$$

□

Lemma 5.6. *For any full rank lattice* $\mathcal{L} \in \mathbb{R}^n$ *and* $\varepsilon = 4^{-n}$*, we have that*

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

Lemma 5.7. *For any lattice* $\mathcal{L}$ *and* $\varepsilon \leq 2e^{-\pi}$*, we have that*

$$\eta_\varepsilon(\mathcal{L}) \geq \frac{1}{\lambda_1(\mathcal{L}^*)}$$

Definition 5.8. *For a lattice* $\mathcal{L}$ *the* $i-th$ *successive minima is defined as*

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

Theorem 5.9. *For any* $\varepsilon > 0$ *and full rank lattice* $\mathcal{L}$ *we have*

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

Definition 5.10. *For a unit vector* $\mathbf{u} \in \mathbb{R}^n$ *and* $t \in \mathbb{R}^+ \cup \{0\}$ *the open half space is defined as*

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

Lemma 5.11. *For any lattice* $\mathcal{L}$ *and unit vector* $\mathbf{u} \in \mathbb{R}^n$*,* $t \in \mathbb{R}^+ \cup \{0\}$ *and* $\mathbf{x} \in \mathbb{R}^n$ *we have*

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

$$\mathcal{D}_{\mathbb{Z}^n,\sigma} = \prod_{i=1}^{n} \mathcal{D}_{\mathbb{Z},\sigma}$$

References

[DD18] Daniel Dadush and Léo Ducas. *Short Integer Solution (SIS) problem, Collision resistant functions, One way functions*. Introduction to Lattice Algorithms and Cryptography. Lecture 9, Scribed by K. de Boer. Spring 2018. URL: `https://homepages.cwi.nl/~dadush/teaching/lattices-2018/notes/`.

[Pei13] Chris Peikert. "Lecture Notes on Lattices in Cryptography". Georgia Tech, Fall 2013. 2013. URL: `https://github.com/cpeikert/LatticesInCryptography`.

[Reg09] Regev. *Lecture Notes on Lattices in Computer Science*. Tel Aviv University, 2009.