

Exercise 1 (Diameter of the Torus)

Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. For $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, define

$$d(\mathcal{L}, \mathbf{x}) := \min_{\mathbf{w} \in \mathcal{L}} \|\mathbf{x} - \mathbf{w}\| \quad \text{and} \quad d_{\mathcal{L}}(\mathbf{x}, \mathbf{y}) := d(\mathcal{L}, \mathbf{y} - \mathbf{x}).$$

Let \mathbf{X} be uniformly distributed on $\mathbb{R}^n / \mathcal{L}$. Prove the following statements.

1. Show that $d_{\mathcal{L}}$ induces a metric on the torus: i.e. $d_{\mathcal{L}}(\mathbf{x}, \mathbf{z}) \leq d_{\mathcal{L}}(\mathbf{x}, \mathbf{y}) + d_{\mathcal{L}}(\mathbf{y}, \mathbf{z})$, $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$.
2. Show that $\max_{\mathbf{x}, \mathbf{y} \in \mathbb{R}^n} d_{\mathcal{L}}(\mathbf{x}, \mathbf{y}) = \mu(\mathcal{L})$.
3. For any $\mathbf{t} \in \mathbb{R}^n$, show that $\mathbf{X} + \mathbf{t}$ is also uniformly distributed on $\mathbb{R}^n / \mathcal{L}$.
4. Show that $\mu(\mathcal{L}) \leq 2 \mathbb{E}[d(\mathcal{L}, \mathbf{X})]$.

Exercise 2 (Smoothing Parameter of \mathbb{Z}^n)

Recall that $\rho_s(A) := \sum_{\mathbf{x} \in A} e^{-\pi \|\mathbf{x}/s\|^2}$. Prove the following statements.

1. For $s > 0$, show that

$$\begin{aligned} \max\left\{1 + 2e^{-\pi s^2}, \frac{1}{s}\right\} \leq \rho(s\mathbb{Z}) \leq \min\left\{\left(1 + 2\frac{e^{-\frac{\pi}{s^2}}}{1 - e^{-\frac{\pi}{s^2}}}\right) \cdot \frac{1}{s}, 1 + 2\frac{e^{-\pi s^2}}{1 - e^{-\pi s^2}}\right\} \\ \leq 1.01(1 + 1/s). \end{aligned}$$

2. Use the above to show that $\eta_\varepsilon(\mathbb{Z}^n) \leq O(\sqrt{\ln(n/\varepsilon)/\pi})$.

Exercise 3 (Orthogonalizing Gaussian Sums)

Let $\mathcal{L} \subset \mathbb{R}^n$ be an n -dimensional lattice, $W \subseteq \mathbb{R}^n$ be a linear subspace such that $\dim(W \cap \mathcal{L}) = \dim(W)$, $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ be a basis for \mathcal{L} and $s > 0$.

Prove the following statements.

1. Show that $\rho_s(\mathcal{L}) \leq \rho_s(\mathcal{L} \cap W) \rho_s(\mathcal{L}/W)$, where $\mathcal{L}/W := \pi_{W^\perp}(\mathcal{L})$.
(Hint: Use the fact $\rho_s(\Lambda + \mathbf{t})$ is maximized at $\mathbf{t} = 0$ for any lattice Λ and apply this to the fibers of $\pi_{W^\perp}(\mathcal{L})$.)
2. Use the first part to show that $\rho_s(\mathcal{L}) \leq \prod_{i=1}^n \rho_s(\|\tilde{\mathbf{b}}_i\| \mathbb{Z})$.
3. Show that

$$|\mathcal{L} \cap r\mathcal{B}_2^n| \leq e^{n/2} \prod_{i=1}^n \rho_{\sqrt{\frac{2\pi}{n}} r}(\|\tilde{\mathbf{b}}_i\| \mathbb{Z}) \leq (1.03e)^{n/2} \prod_{i=1}^n \left(1 + \sqrt{\frac{2\pi}{n}} \frac{r}{\|\tilde{\mathbf{b}}_i\|}\right).$$