Computational Problems

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

July, 2025

$\boxed{III}$

---

1 Introduction

This article will cover the computational problems involved in the Lattices. We will look at the Shortest Vector Problem in detail and a way to solve it computationally. In the first part, we will define the problems, and subsequently, we will look at the way the mechanism to solve them evolved.

2 Exact Computational Problems

2.1 Shortest Vector problem(SVP)

Input: Basis of lattice B
Output: $\mathbf{v} \in \mathcal{L}$ such that

$$||\mathbf{v}|| = \lambda_1$$

2.1.1 Optimisation Version of SVP

Input: Basis of lattice B
Output: $\lambda_1(\mathcal{L}(B))$

2.1.2 Decision Version of SVP

Input: Basis of lattice B and $d \in \mathbb{R}$
Output: Yes if $\lambda_1 \leq d$ else No

2.2 Closest vector Problem(CVP)

Input: Basis of lattice B and a target vector $\mathbf{t} \in \mathbb{R}^n$ in the ambient space.
Output: $\mathbf{v} \in \mathcal{L}$ such that

$$\|\mathbf{v}\| = \min_{\mathbf{u} \in \mathcal{L}} ||\mathbf{u} - \mathbf{t}||$$

2.3 Shortest Integer vector Problem(SIVP)

Input: Basis of lattice B
Output: $||\mathbf{v_1}|| \leq ||\mathbf{v_2}|| \leq \cdots \leq ||\mathbf{v_d}|| \leq \lambda_d$

3 Approximation Computational Problems

The $\gamma-$approximate shortest vector problem, where $\gamma = \gamma(n) \geq 1$ is a function of dimension n. It has the following variants

3.1 Decision(GapSVP$_\gamma$)

Input: Basis of lattice B and $d \in \mathbb{Z}^+$
Output: $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > \gamma \cdot d$

3.2 Estimation(EstSVP$_\gamma$)

Input: Basis of lattice B
Output: $\lambda_1(\mathcal{L})$ up to a factor γ and return $d \in [\lambda_1(\mathcal{L}), \gamma \cdot \lambda_1(\mathcal{L})]$

3.3 Search(SVP$_\gamma$)

Input: Basis of lattice B
Output: $\mathbf{v} \in \mathcal{L}(B)$ such that $0 < ||\mathbf{v}|| \leq \gamma \cdot \lambda_1(\mathcal{L})$

Open Problem: Prove or disprove SVP$_\gamma \leq$ GapSVP$_\gamma$

References

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

[2] Vinod Vaikuntanathan, *Advanced Topics in Cryptography: From Lattices to Program Obfuscation*, MIT, Fall 2024.

[3] Chris Peikert, *Lattices in Cryptography*, University of Michigan, 2015

[4] Deng, Xinyue *An Introduction to Lenstra-Lenstra-Lovasz Lattice Basis Reduction Algorithm*, Massachusetts Institute of Technology, 2016