Computational Problems

Debadatta Kar
Cryptography Research Lab
Indian Institute of Science Education and Research Bhopal

July 21, 2025

Lecture 3

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: $v \in \mathcal{L}$ such that

$$||v|| = \lambda_1$$

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 $t \in \mathbb{R}^n$ in the ambient space.
Output: $v \in \mathcal{L}$ such that

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

2.3 Shortest Integer vector Problem(SIVP)

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

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: $v \in \mathcal{L}(B)$ such that $0 < ||v|| \leq \gamma \cdot \lambda_1(\mathcal{L})$

Open Problem 3.1. *Prove or disprove* $SVP_\gamma \leq GapSVP_\gamma$

4 Basis Reduction

Given a lattice $\mathcal{L}$ and its basis B, if we can find a basis B' such that $\mathcal{L}(B) = \mathcal{L}(B')$ and B' contains comparatively smaller lattice vectors than B, we call B' a reduced basis. Minkowski gave an upper bound for the shortest lattice vector. However, in 1805, Gauss gave a working algorithm that solved the SVP exactly in 2 dimensions. During 1982, the LLL Basis Reduction algorithm was proposed by Arjen Lenstra, Hendrick Lenstra Jr. and László Lovász, which gives an approximation to the shortest vector and works on the technique of basis reduction. It is a generalisation of Gauss's Algorithm.

Definition 4.1. *A babis* $[b_1, b_2]$ *in* $\mathbb{R}^2$ *is said to be reduced if*

1. $||b_1|| \leq ||b_2||$
2. $|\mu_{2,1}| \leq 1/2$

Where, $\mu_{1,2} = \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle}$

The above reduced condition is also called the Gaussian reduced basis form.

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