Notes for

Yiwei Fu, Instructor: Chris Peikert

FA 2022

Contents

Office hours:

Chapter 1

Introduction

1.1 Brief History of Lattices in Cryptography

In late to mid 18th century the concept of lattice is start to be formally defined by Gauss, Laplace, etc. It was used in number theory to give proofs such as quadratic reciprocity and the four square theorem. Minkowski went all in "Geometry of Numbers", generalizing to higher dimensions.

In early 1980s, Lenstra-Lenstra-Lovasz: 'LLL' algorithm for lattice basis reduction. Other applications include breaking many proposed cryptosystems.

In mid 1990s (1996), Ajtai proves "worse-case to average-case" reduction for lattices. This gives a secure crypto primitive, assuming certain lattice problems are hard.

NTRU(Hoffstein, Pipher, Silverman) cryptosystem (no theoretical soundness found yet): seems secure!

From 2000s onward, a better, faster, stronger, smaller, cleaner, simpler, . . .

2016-, NIST, Goggle, Cloudfare: 'post-quantum' secure proposals, deployments of lattice based cryptography.

1.2 Lattice

Definition 1.2.1. An n-dimentional lattice is a discrete additive subgroup of $\mathbb{R}^n$.

Every lattice (except the degenerate case) is infinite. But it has a finite representation through basis.

Definition 1.2.2. A basis B is a set of vectors $\{b_1, \ldots, b_n\}$ of a lattice $\mathcal{L}$ is a set of linearly independent vectors whose integer linear combinations generates $\mathcal{L}$.

Equivalently, view B as a nonsingular matrix whose i-th column is b_i, then $\mathcal{L} = B \cdot \mathbb{Z}^n = \{Bz : z \in \mathbb{Z}^n\}$.

Theorem 1.2.1. *Every lattice has a basis. (not unique)*

Lemma 1.2.1. *Suppose bases B_1, B_2 generate the same lattice $\mathcal{L}$ if and only if there exists an unimodular matrix $U \in \mathbb{Z}^{n\times n}, \det U = \pm 1$ such that $B_1 = B_2 \cdot U$.*

Corollary 1.2.1. *The bases of Z^n are exactly the unimodular matrices $U \in \mathbb{Z}^{n\times n}$.*

Corollary 1.2.2. *Given two sets B_1, B_2 we can efficiently test whether they generate the same lattice by check is B_2^{-1}, B_1 is unimodular.*

Proof of Lemma 1.2.1. Suppose B_1, B_2 generates the same lattice $\mathcal{L}$ i.e. $B_1 \cdot \mathbb{Z}^n = B_2 \cdot \mathbb{Z}^n$. So each column of B_1 is an integer linear combination of B_2's columns: $B_1 = B_2 \cdot X$ for some $X \in \mathbb{Z}^{n\times n}$.

Similarly, we have $B_2 = B_1 \cdot Y$. So $B_2 = B_2(X \cdot Y) \implies X \cdot Y = \mathrm{id} \implies \det(X)\det(Y) = 1$.

Suppose $B_1 = B_2 \cdot U$ for unimodular U. Then $B_1 \cdot \mathbb{Z}^n = B_2 \cdot U \cdot Z^n = B_2 \cdot \mathbb{Z}^n$. (for any $z \in Z^n$, we have $U(U^{-1}z) = z$. $U^{-1}z$ is an integral vector since U^{-1} is an integer matrix.) ■