CS758: Advanced Tools from Modern Cryptography (Lattices) Spring 2026

Lecture 3.14

15/Aug/1947

Instructor: Chethan Kamath Scribe: Your name (Roll no)

1 Motivation

In this course we will study lattices.

2 Notation

Let's try to use the following notation for the objects we will use in our course.

- Sets: $\mathcal{S}_1 \cup \mathcal{S}_2$
- Complexity classes: **NP**, **coNP**
- Problems: SVP, CVP
- Matrices and vectors: $\overline{A}$, $\bar{x}$
- Algorithms: GramSchmidt, LLL
- Algebraic objects: $\mathbb{G}$, $\mathbb{N}$ (natural numbers), $\mathbb{Z}$ (integers), $\mathbb{F}$ (finite fields)

3 Environments: Definitions, Lemmata, Proofs etc

Definition 1 (Lattice, Definition 1)**.** Write your definition of lattice here.

Definition 2 (Lattice, Definition 2)**.** Write your alternative definition of lattice here.

Lemma 1 (Unimodularity and inverses)**.** If a matrix $\overline{A}$ is unimodular, then so is its inverse.

Proof. Prove using Cramer's rule. □

Open Problem 1. Can we construct one-way function from SVP?

You can use `\cref` to refer to the above (do give meaningful label names).

Homework 1. Prove that Definition 1 implies Definition 2.

You can use `\href` to refer to articles or papers online (e.g., StackExchange or Wikipedia)

- We will rely on two courses:
  1. CS206A, Lattices Algorithms and Applications (Spring 2007) by Daniele Micciancio, for Module I

2. CS294: Lattices, Learning with Errors and Post-Quantum Cryptography by Vinod Vaikuntanathan, for Modules II and III

- Cramer's rule has a very cool geometric interpretation: see this 3Blue1Brown video.

4 Misc.

Do feel free to use the other macros defined, such as $|-1|$, $[1, n]$, $\{1, 2, 3\}$, $\{1, \ldots, 3\}$, $s \leftarrow \mathcal{S}$ etc