SCIENCE
PASSION
TECHNOLOGY

Lattices

Lukas Helminger

Mathematical Foundations of Cryptography – WT 2019/20

Outline

Literature

The slides are based on the following sources

- **An Introduction to Mathematical Cryptography**, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
- **A Decade of Lattice Cryptography**, Chris Peikert
- **The LLL Algorithm**, Phong Q. Nguyen, Brigitte Vallée (Eds.)

Many graphics are based on graphics from Maria Eichlseder.

Lattice-Based Cryptography

- Conjectured security against quantum attacks:

  One half of the 2nd round candidates for NIST Post-Quantum Cryptography Standardization are lattice-based (in the category PKE).
- Algorithmic simplicity, efficiency, and parallelism.
- Strong security guarantees from worst-case hardness.
- Construction of versatile and powerful cryptographic objects
  - Fully Homomorphic Encryption
  - Attribute-Based Encryption

Vector Spaces

Vector Spaces

- A vector space V is a subset of $\mathbb{R}^m$ that is closed under addition and under scalar multiplication by elements of $\mathbb{R}$.
- A linear combination of the vectors $v_1, \ldots, v_k$ is any vector of the form

  $$w = \alpha_1 v_1 + \cdots + \alpha_k v_k, \text{ with } \alpha_1, \ldots, \alpha_k \in \mathbb{R}.$$

  The collection of all such linear combinations is called the span of $\{v_1, \ldots, v_k\}$.
- A set of vectors $v_1, \ldots, v_k \in V$ is linearly dependent

  $$\alpha_1 v_1 + \cdots + \alpha_k v_k = 0 \Rightarrow \alpha_1 = \cdots = \alpha_k = 0.$$

- A basis for V is a set of linearly independent vectors $v_1, \ldots, v_k$ that span V.

Length and Angle

- The dot product of $v = (x_1, \ldots, x_m), w = (y_1, \ldots, y_m) \in V$ is the quantity
$$v \cdot w = x_1 y_1 + \cdots + x_m y_m.$$
- v and w are orthogonal if $v \cdot w = 0$.
- The length, or Euclidean norm, of v is the quantity
$$\|v\| = \sqrt{x_1^2 + \cdots + x_m^2}.$$
- A basis $v_1, \ldots, v_n$ is an orthogonal basis if
$$v_i \cdot v_j = 0 \quad \forall i \neq j.$$
- Let α be the angle between v and w, then
$$v \cdot w = \|v\| \|w\| \cos(\alpha).$$

Gram Matrix

Let $v_1, \ldots, v_n$ be vectors in $\mathbb{R}^m$. The entries of the Gram matrix are given by $G_{ij} = v_i \cdot v_j$. The determinant of G is called the Gram determinant.

- $\det G \neq 0 \Rightarrow v_1, \ldots, v_n$ linearly independent.
- $\sqrt{\det G}$ is the n-dimensional volume spanned by $v_1, \ldots, v_n$.

Example: Let $v_1 = (2, 3), v_2 = (1, 4)$.

$$G = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 13 & 14 \\ 14 & 17 \end{pmatrix}$$

$\mathrm{vol}(v_1, v_2) = \sqrt{\det G} = \sqrt{25} = 5$

Gram-Schmidt Algorithm

Theorem (Gram-Schmidt Algorithm)

Let $v_1, \ldots, v_n$ be a basis for a vector space $V \subset \mathbb{R}^m$. The following algorithm creates an orthogonal basis $v_1^*, \ldots, v_n^*$ for V:

$v_1^* \leftarrow v_1$

for $i = 2..n$ **do**

  for $j = 1..i-1$

$$\mu_{i,j} \leftarrow \frac{v_i \cdot v_j^*}{\|v_j^*\|^2}$$

$$v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{i,j} v_j^*$$

Definition and Properties

Lattices

Definition (Lattice)

An n-dimensional lattice L is any subset of $\mathbb{R}^n$ that is both:

- an additive subgroup
- discrete

A basis for L is any set of independent vectors that generates L.

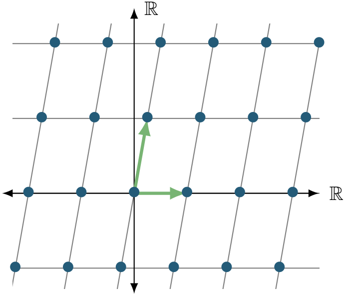
Lattice: Example

In other words, let $v_1, \ldots, v_n \in \mathbb{R}^n$ be a set of linearly independent vectors. The lattice generated by $v_1, \ldots, v_n$ is the set of linear combinations of $v_1, \ldots, v_n$ with coefficients in $\mathbb{Z}$,

$$L = \{a_1 v_1 + \cdots + a_n v_n \; : \; a_1, \ldots, a_n \in \mathbb{Z}\}.$$

Example:

$$\boldsymbol{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 1/4 \\ \sqrt{2} \end{pmatrix}$$

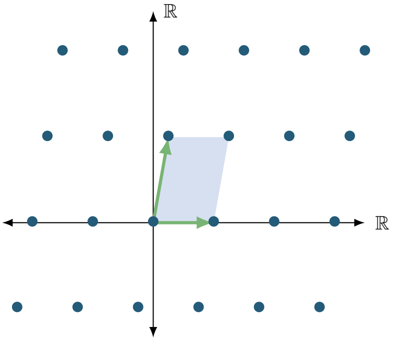


Fundamental Domains

Definition (Fundamental Domain)

Let L be a lattice of dimension n and let $v_1, \ldots, v_n$ be a basis for L. The fundamental domain is the set

$$F = [0,1)v_1 + \cdots + [0,1)v_n.$$



Volumes

Definition (Volume)

Let L be a lattice of dimension n and let F be a fundamental domain of L. Then the n-dimensional volume of F is called the volume of L (or sometimes the determinant of L).

Example: Let L be generated by the vectors

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1/4 \\ \sqrt{2} \end{pmatrix}.$$

First, compute Gram matrix:

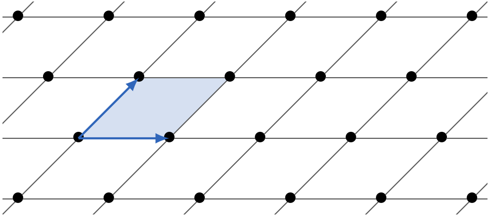
$$G = \begin{pmatrix} 1 & 0 \\ \frac{1}{4} & \sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{4} \\ 0 & \sqrt{2} \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{4} \\ \frac{1}{4} & \frac{33}{16} \end{pmatrix}$$

Therefore,

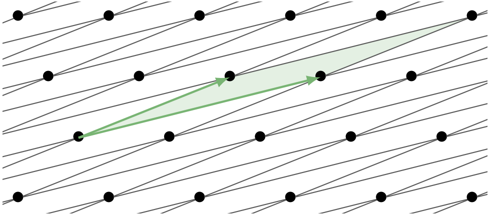
$$\mathrm{vol}(L) = \sqrt{\det G} = \sqrt{2}$$

Same Lattice?

$$\boldsymbol{v}_1 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \boldsymbol{v}_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$



$$\boldsymbol{v}_1' = \begin{pmatrix} 8 \\ 2 \end{pmatrix}, \boldsymbol{v}_2' = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$



Volume: Task

Task: Compute the volumes V resp. V' of the fundamental domains corresponding to v_1, v_2 respectively v_1', v_2'.

$$G = \begin{pmatrix} 3 & 0 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 9 & 6 \\ 6 & 8 \end{pmatrix}.$$

$$G' = \begin{pmatrix} 8 & 2 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 68 & 44 \\ 44 & 29 \end{pmatrix}.$$

Therefore $V = \sqrt{G} = \sqrt{36} = 6 = \sqrt{36} = \sqrt{G'} = V'$.

Proposition

Every fundamental domain for a given lattice L has the same volume.

Short Vectors in Lattices

Computational Problems

$\lambda_1(L)$... length of shortest nonzero vector in L.

- **Shortest Vector Problem (SVP):** Find a shortest nonzero vector v in L, i.e. $\|v\| = \lambda_1(L)$.
- **Closest Vector Problem (CVP):** Given a vector w, find closest vector to w in L.

Example: Given the lattice generated by v_1, v_2

$$v_1 = \begin{pmatrix} 8 \\ 2 \end{pmatrix}, v_2 = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$

and given the vector $w = (-1, 3)^T$. What is a shortest nonzero vector of L? Which vector is closest to w?

$$\begin{pmatrix} -1 \\ 2 \end{pmatrix} \text{ and } \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

How long is the shortest vector?

Theorem (Minkowski's Theorem)

Let $L \subset \mathbb{R}^n$ be a lattice of dimension n. Let $S \subset \mathbb{R}^n$ be convex, closed and symmetric. Suppose that $\text{vol}(S) \geq 2^n \text{vol}(L)$, then

$$S \cap L \supsetneq \{0\}.$$

S... hypercube in $\mathbb{R}^n$ centered at 0 with length $2\,\text{vol}(L)^{1/n}$, then $\text{vol}(S) = 2^n \text{vol}(L)$. Applying Minkowski's theorem leads to:

Corollary (Hermite's Theorem)

Every lattice L of dimension n contains a nonzero $v \in L$ satisfying

$$\|v\| \leq \sqrt{n}\,\text{vol}(L)^{\frac{1}{n}}.$$

Lattice Reduction Algorithms

Babai's Closest Vertex Algorithm

Input: Basis $v_1, \ldots, v_n$ and $w \in \mathbb{R}^n$.

1. Write $w = t_1 v_1 + \cdots, t_n v_n$, with $t_1, \ldots, t_n \in \mathbb{R}$.
2. Set $a_i = \lfloor t_i \rceil$ for $i = 1, \ldots, n$.
3. Return $v = a_1 v_1 + \cdots + a_n v_n$.

Try out the algorithm for

$$v_1 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, w = \begin{pmatrix} -1 \\ 3 \end{pmatrix}.$$

Orthogonality Defects

Definition (Hadamard Ratio)

We define the Hadamard ratio of the basis $B = \{v_1, \ldots, v_n\}$. to be the quantity

$$H(B) = \left(\frac{\mathrm{vol}(L)}{\|v_1\| \cdots \|v_n\|} \right)^{\frac{1}{n}} \in (0, 1].$$

(the closer to 1, the more orthogonal)

Example: $v_1 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$

$$H(B) = \left(\frac{6}{\sqrt{9}\sqrt{8}} \right)^{\frac{1}{2}} \approx 0.84.$$