Notes for Math 669

Yiwei Fu, Instructor: Alexander Barvinok

FA 2022

Contents

Office hours:

Chapter 1

1.1 Lattice and Its Basis

Definition 1.1.1. A lattice $\Lambda \subset V$ is a discrete additive group.

Last time: $L \in V$ is a subspace if $L = \mathrm{span}(L \cap \Lambda)$

Theorem 1.1.1. *If L is a lattice subspace, $L \neq V$, then $\exists u \in L \setminus \Lambda$ such that $d(u, L) \leq d(x, L)$ for all $x \in L \setminus \Lambda$.*

Say $L \in \mathrm{span}\{u_1, \ldots, u_m\}$ linearly independent vectors, $\Pi = \{\}$ There is $u \in \Lambda \setminus L$ such that $\mathrm{dist}(u, \Pi) \leq \mathrm{dist}(x, \Pi)$ for all $x \in \Lambda \setminus L$.

Proof. Take $\rho > 0$ large enough. Consider $\Pi_\rho = \{y, d(y, \Pi) \leq \rho\}$. It contains points from $\Lambda \setminus L$, choose the one in $\Pi_\rho \cap (\Lambda \setminus L)$ closet to Π. ∎

<u>CLAIM</u> $u \in \Lambda \setminus L$ is what we need. Why? Pick any $x \in \Lambda \setminus L$. Let $y \in L$ be the closest to x.

$$\mathrm{dist}(x, L) = \|x - y\| = \|(x - w) - (y - w)\|.$$

$$y = \sum_{i=1}^{m} d_i u_i$$

Let $w = \sum_{i=1}^{m} \lfloor \alpha_i \rfloor u_i \in \Lambda \setminus L, y - w = \sum_{i=1}^{m} \{\alpha_i\} u_i \in \Pi$.

Theorem 1.1.2. *Every lattice has a basis.*

Proof. By induction on $n = \dim V$.

Base case: for $n = 1$, we have $V = \mathbb{R}$.

Let $u > 0$ be the lattice vector closet to 0, among all positive vectors in Λ.

Then u is a basis of Λ. Pick any $v \in \Lambda$. Assume $v > 0$ WLOG. Then $v = \alpha u$ for $\alpha > 0$. If

$\alpha \in \mathbb{Z}$ then we are done. If not, consider $w = \alpha u - \lfloor \alpha \rfloor u = \{\alpha\} u$, this is closer to 0 than u, a contradiction.

Induction hypothesis: suppose any lattice of dimension $n-1$ has a basis.

Induction step: pick a lattice hyperplane H (lattice subspace with $\dim = n-1$). Then $\Lambda_1 = H \cap \Lambda$ has a basis $u_1, \dots, u_{n-1}$. Pick u_n such that $u_n \notin H$ and $\operatorname{dist}(u_n, H)$ is the smallest. We claim that $u_1, \dots, u_{n-1}, u_n$ is a basis of Λ.

Let $u \in \Lambda$, $u = \sum_{i=1}^n \alpha_i u_i$ with $\alpha_i \in \mathbb{R}$. If $\alpha_n = 0$ then $u \in \Lambda_1$, then $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{Z}$. Suppose $\alpha_n \neq 0$. Consider $w = u - \lfloor \alpha_n \rfloor u_n$. $w \in \Lambda$ and $w = \{\alpha_n\} u_n + \sum_{i=1}^{n-1} \alpha_i u_i$. So

$$\operatorname{dist}(w, H) = \operatorname{dist}(\{\alpha_n\} u_n, H) = \{\alpha_n\} \operatorname{dist}(u_n, H)$$

If $\{\alpha_n\} > 0$ then $0 < \operatorname{dist}(w, H) < \operatorname{dist}(u_n, H)$, a contradiction.

So $\{\alpha_n\} = 0 \implies \alpha_n \in \mathbb{Z}$. Then $w = \sum_{i=1}^{n-1} \alpha_i u_i \implies \alpha_1, \dots, \alpha_{n-1} \in \mathbb{Z}$.

So we have constructed a basis for lattice of dimension n, thus finishing the proof. ■

This is called A.N.Korkin(e)-Zolotarev(öff) basis.

<u>EXERCISE</u> Suppose $u_1, \dots, u_n \in V$ is a basis of subspace. The integer combinations form a lattice.

<u>EXERCISE</u> Suppose a 2-dimensional lattice. Then there exists a lattice basis u, v such that the angle α between u, v satisfies $\frac{\pi}{3} \leq \alpha \leq \frac{\pi}{2}$.

<u>EXERCISE</u> If Λ is a lattice and L is a lattice subspace. The orthogonal projection $\mathrm{PR} : V \to L^{\perp}$. Then $\mathrm{PR}(\Lambda) \subset L^{\perp}$ is a lattice.

Definition 1.1.2. Suppose $u_1, \dots, u_n$ be a basis of Λ.

$$\Pi = \left\{ \sum_{i=1}^{n} \alpha_i u_i : 0 \leq \alpha_i < 1, i = 1, \dots, n \right\}$$

is the *fundamental parallelepiped* of a fundamental parallelepiped of Λ.

Theorem 1.1.3. *The volume of a fundamental parallelepiped Π doesn't depend on Π. The volume is called the determinant of Λ. Furthermore, if $B_\tau = \{x : \|x\| \leq \tau\}$, then*

$$\lim_{\tau \to \infty} = \frac{|B_\tau \cap \Lambda|}{\operatorname{vol} B_\tau} = \frac{1}{\det \Lambda}.$$

We start with a lemma:

Lemma 1.1.1. *Let Π be a fundamental parallelepiped of $\Lambda \subset V$. Then every vector $x \in V$ is* *uniquely written as* $x = u + y$ *where* $u \in \Lambda, y \in \Pi$.

Proof. Existence: Π is the fundamental parallelepiped for $u_1, \ldots, u_n$. If $x = \sum_{i=1}^{n} \alpha_i u_i$ then $u = \sum_{i=1}^{n} \lfloor \alpha_i \rfloor u_i$ and $y = \sum_{i=1}^{n} \{\alpha_i\} u_i$

Uniqueness: suppose $x = u_1 + y_1 = u_2 + y_2$ then $u_1 - u_2 = y_2 - y_1$. Since $u_1 - u_2 \in \Lambda$ we have $y_2 - y_1 = \sum_{i=1}^{n} (\alpha_i - \beta_i)\mathbf{u}_i$. We have $(\alpha_i - \beta_i) \in \mathbb{Z}$. Since $-1 < \alpha_i - \beta_i < 1$, it has to be 0. ■

A geometry interpretation is that we can cover the whole space with fundamental parallelepipeds without overlaps.