Intro

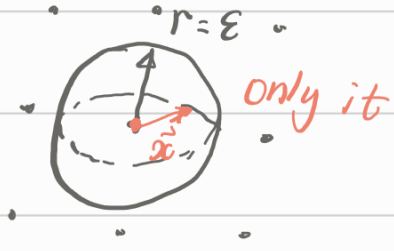
- History
- Adv & Disadv
- General concept

Part I : Euclidean lattices

1. Definition

Def 1 An n-dim Eu lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$

- Additive subgroup: $\vec{0} \in \Lambda$. for all $\vec{x}, \vec{y} \in \Lambda$, $\vec{x}+\vec{y}$, $-\vec{x} \in \Lambda$
- Discrete: $\forall \vec{x} \in \Lambda$, $\exists \varepsilon > 0$, st. $\mathcal{B}(\vec{x}, \varepsilon) \cap \Lambda = \{\vec{x}\}$



$\mathcal{B}(\vec{x}, \varepsilon)$: open ball of radius ε around $\vec{x}$.

Exp $\mathbb{Z}^n$ is a n-dim lattice (integer lattice)

scale it by $\forall c \in \mathbb{R}$, $c\mathbb{Z}^n$.

rotate it by $\perp$ matrix $R \in \mathbb{R}^{n \times n}$ $(R^T \cdot R = I_n)$

$\Rightarrow R\mathbb{Z}^n$

- Minima

1st minimum

$$\lambda_1(\Lambda) := \min_{\vec{v} \in \Lambda \setminus \{0\}} \|\vec{v}\|$$

i^{th} minimum $\lambda_i(\Lambda)$ smallest r such that Λ ...

i^{th} minimum $\lambda_i(\Lambda)$ smallest r such that Λ contains i linearly independent vectors of norm at most r

More formally:

$$\lambda_i(\Lambda) := \min_{r \in \mathbb{N}} \{ \dim(\text{span}(\Lambda \cap \bar{B}(\vec{0}, r))) \geq i \}$$

$\bar{B}(\vec{0}, r)$: closed ball of radius r around $\vec{0}$.

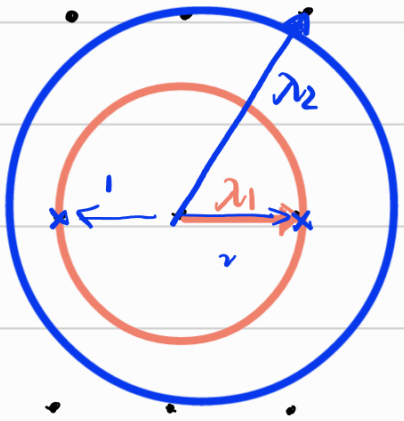


fig 2.

e.g. $1^{st} \rightarrow$ 1 discrete pt

$2^{nd} \rightarrow$ 2 dis pts

Bases

$B = (\vec{b_1}, \cdots, \vec{b_k}) \in \mathbb{R}^n, \quad k \leq n$

$\Lambda(B) = \mathcal{L}(B) = \{ \sum_{i=1}^{k} z_i \vec{b_i} : z_i \in \mathbb{Z} \}$ → linear comb of the basis vectors

$= \{ B\vec{z} : \vec{z} \in \mathbb{Z}^n \}$ → matrix form.

k : rank

n : dim

$k = n$: full rank / dimensional.

e.g. $B = \begin{pmatrix} b_{11} & \cdots & b_{k1} \\ \vdots & & \vdots \\ b_{1n} & & b_{kn} \end{pmatrix}$

span

$$\text{Span}(\Lambda(B)) := \text{Span}(B) = \{ B\vec{x} : \vec{x} \in \mathbb{R}^n \}$$

- for $k=n$, $\text{span}(B) = \mathbb{R}^n$.
- lattice basis B not unique.

$\forall$ unimodular matrix $U \in \mathbb{Z}^{n \times n}$, $\mathcal{L}(B \cdot U) = \mathcal{L}(B)$

↳ $\det(U) = \pm 1$ $\quad B \cdot U \cdot \mathbb{Z}^n \overset{\Uparrow}{=} B \cdot \mathbb{Z}^n$

($B \cdot \mathbb{Z}^n$ can be seen as a linear transform of integer lattice $\mathbb{Z}^n$, thus any $\mathcal{L}(B)$ can be seen this way)

Exp

$\mathbb{Z}^n$ basis I_n.

$c\mathbb{Z}^n$ basis cI_n

$R\mathbb{Z}^n$ basis R

Fundamental Parallelepiped

(origin-centered)

$$\mathcal{P}(B) := \left\{ \sum_{i=1}^{n} c_i \vec{b}_i : c_i \in [-1/2, 1/2) \right\}$$

Note:

- every coset $\vec{x} + \Lambda$ with $\vec{x} \in \mathbb{R}^n$ has exact one representative in $\mathcal{P}(B)$

Volume

$$V = \det(\Lambda) := |\det(B)|$$
$$= V(\mathcal{P}(B))$$

Dual lattice

A dual of a lattice $\Lambda \subset \mathbb{R}^n$:

$$\Lambda^\vee := \{\vec{w} \in \text{span}(\Lambda) : \langle \vec{w}, \vec{x} \rangle \in \mathbb{Z}, \forall \vec{x} \in \Lambda\}$$

- $\Lambda = \mathcal{L}(B) \Rightarrow \Lambda^\vee = \mathcal{L}((B^T)^{-1})$

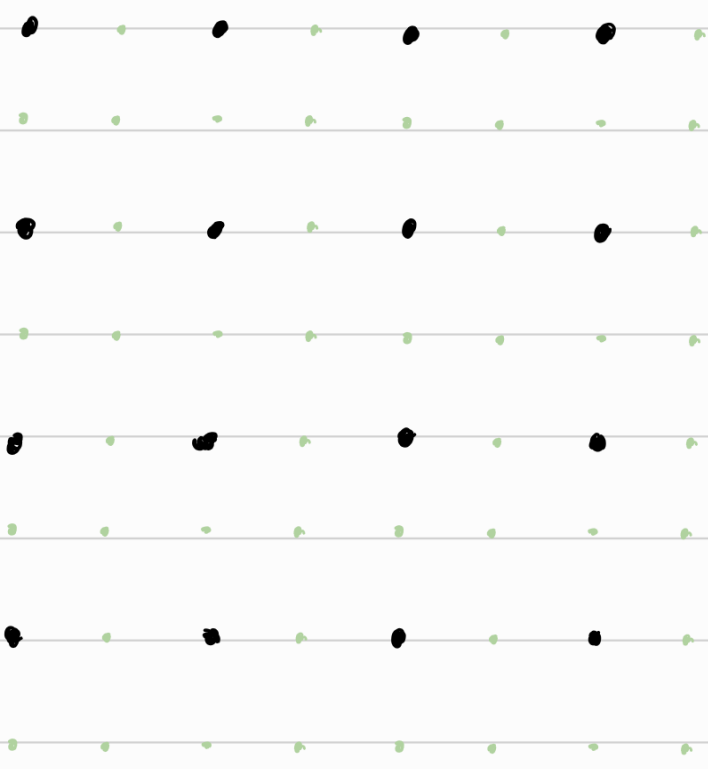
$$\Rightarrow \det(\Lambda^\vee) = \det(\Lambda)^{-1}$$

$$\det(\Lambda^\vee) = |\det((B^T)^{-1})|$$
$$= |\det(B^T)^{-1}| = |\det(B)^{-1}| = |\det(B)|^{-1}$$
$$= \det(\Lambda)^{-1}$$

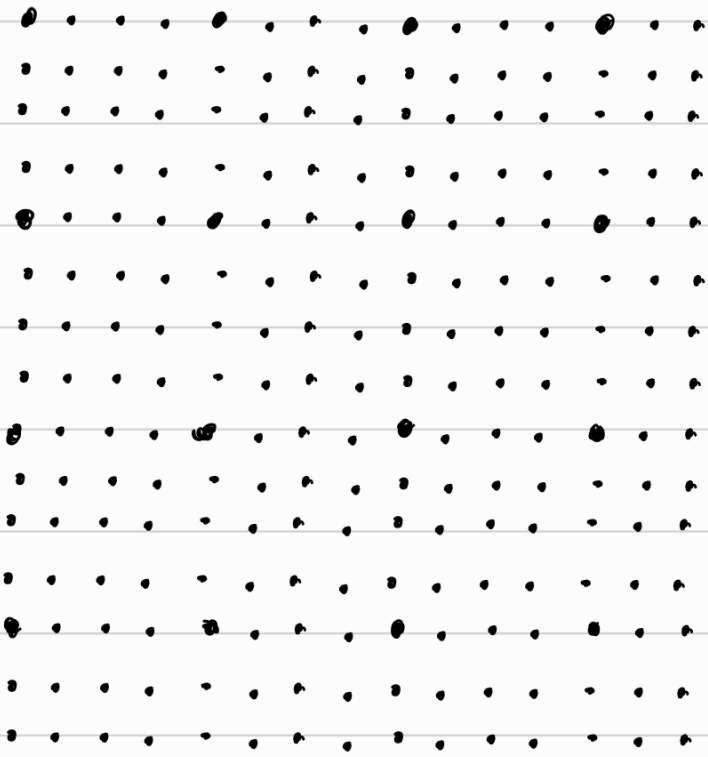
Exp4 $\Lambda = \mathbb{Z}^n$ and $R\mathbb{Z}^n$ are self-dual ($\Lambda^\vee = \Lambda$)

$(c\mathbb{Z}^n)^\vee = \frac{1}{c}\mathbb{Z}^n$

Eg.



$2\mathbb{Z}^2$



↓ dual Λ

$\frac{1}{2}\mathbb{Z}^2$

Minkowski

- first minimum of a lattice ✓

$$\lambda_1(\Lambda) := \min_{\vec{v} \in \Lambda \setminus \{0\}} \|\vec{v}\|$$

  - how small is it for a given lattice ?

- Minkowski : upper bound

  lattice Λ . dim n. determinant $\det(\Lambda)$

  $\Rightarrow$

$$\lambda_1(\Lambda) \leq \sqrt{n}\, \det(\Lambda)^{1/n}$$

Exp5 For $\mathbb{Z}^n$ any unit vector is a shortest vec and thus :

$$\lambda_1(\mathbb{Z}^n) = 1$$

lemma 6

let Λ be an n-dim lattice. it yiels:

1) $\lambda_1(\Lambda) \cdot \lambda_1(\Lambda^\vee) \leq n$

2) $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^\vee) \geq 1$

Theorem 7, Banaszczyk's transference theorem

Λ. n-dim. →

$$1 \leq \lambda_1(\Lambda) \cdot \lambda_n(\Lambda^\vee) \leq n.$$

Gaussian heuristic

n-dim Λ. $\det(\Lambda)$. we expect:

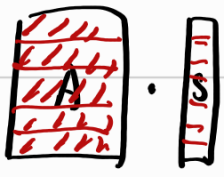
$$\lambda_1(\Lambda) \approx \sqrt{\frac{n}{2\pi e}} \cdot \det(\Lambda)^{1/n}$$

q-ary lattices

Given a matrix $A \in \mathbb{Z}_q^{m \times n}$, we can define 2 lattices:

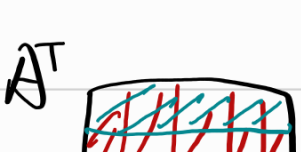
1) $\Lambda_q(A) = \{\vec{y} \in \mathbb{Z}^m : \vec{y} = A\vec{s} \bmod q \text{ for some } \vec{s} \in \mathbb{Z}^n\}$

- generated by rows of A



2) $\Lambda_q^\perp(A^T) = \{\vec{y} \in \mathbb{Z}^m : A^T\vec{y} = \vec{0} \bmod q\}$

- contains all vectors that orth to rows of A^T



→ Is there an

nxm

mx1

$= 0$

error in the note ?

- Duality:

$$\begin{cases} \Lambda_q^{\perp}(A^T) = q \cdot \Lambda_q(A)^V \\ \Lambda_q(A) = q \cdot \Lambda_q^{\perp}(A^T)^V \end{cases}$$