Intro

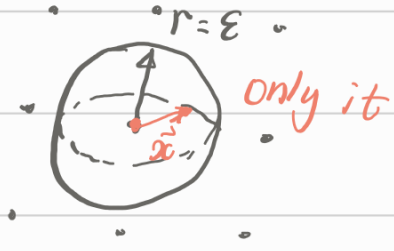
- History
- Adv & Disadv
- General concept

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 $\vec{0}$.

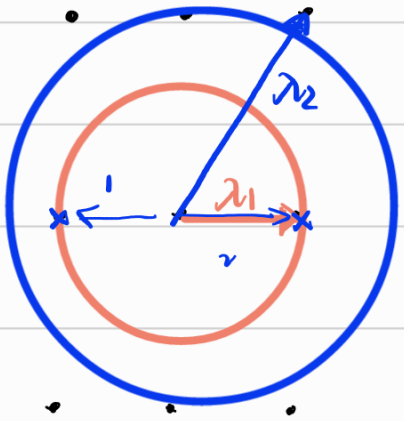


fig 2.

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 $\Lambda \subset \mathbb{R}^n$:

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

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

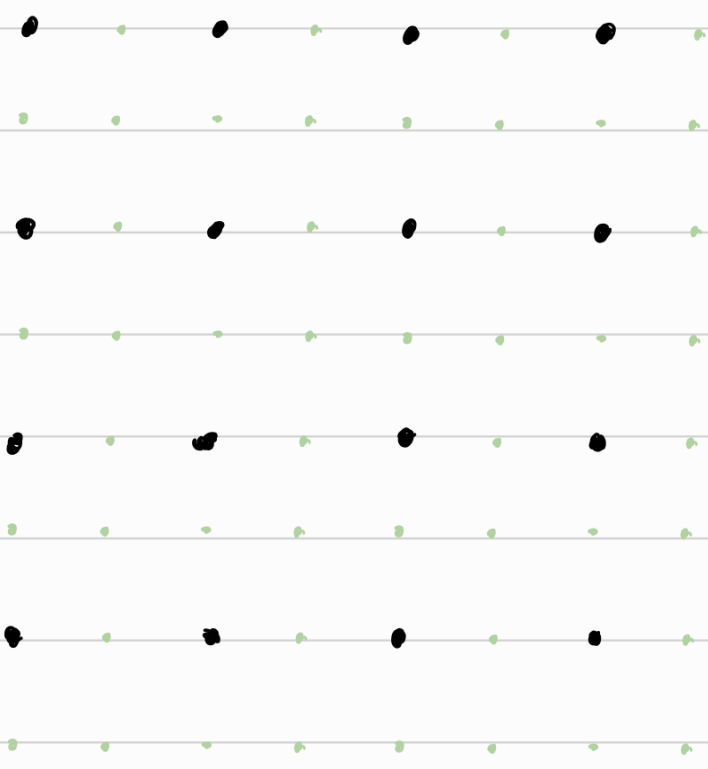
$$\Rightarrow \det(\Lambda^\vee) = \det(\Lambda)^{-1}$$

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

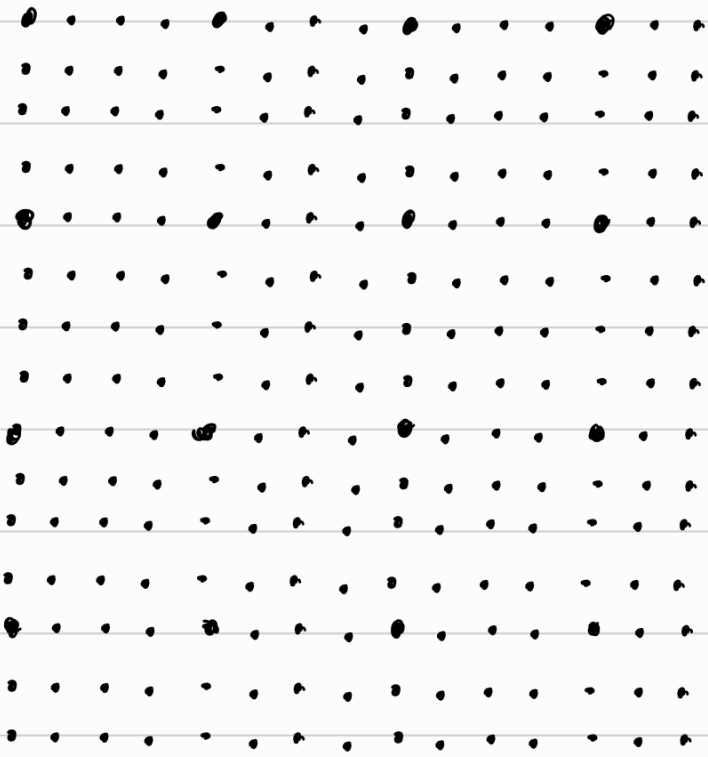
Exp4 $\Lambda = \mathbb{Z}^n$ and $R\mathbb{Z}^n$ are self-dual ($\Lambda^\vee = \Lambda$)

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

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:

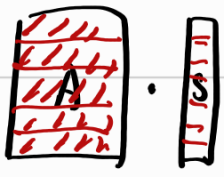
$$\lambda_1(\Lambda) \approx \sqrt{\frac{n}{2\pi e}} \cdot \det(\Lambda)^{1/n}$$

q-ary lattices

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

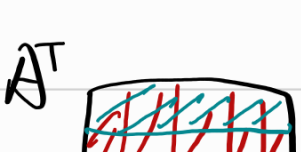
1) $\Lambda_q(A) = \{\vec{y} \in \mathbb{Z}^m : \vec{y} = A\vec{s} \bmod q \text{ for some } \vec{s} \in \mathbb{Z}^n\}$

- 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:

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

§2. Computational Problems

2.1. Shortest Vector Problem

Def 8: SVP

basis B. n-dim. Λ.

goal: find a vector $\vec{z} \neq \vec{0}$ st. $\|\vec{z}\| = \lambda_1(\Lambda)$

In cryptography: approx. factor γ ← relaxed

⇓

Def 9: SVP_γ

Let $\gamma = \gamma(n) \geq 1$ be a fcn in dim n.

B. n-dim. Λ.

goal: $\vec{z} \neq \vec{0}$, st. $\|\vec{z}\| \leq \gamma \cdot \lambda_1(\Lambda)$

- the larger γ, the easier the prob.
- $\gamma \geq 1 \Rightarrow$ SVP.
- find → search variant of SVP_γ
- We build crypto schemes on: { decision variant of SVP_γ / more general search

- general search SVP_γ:
  not only one short vec of (approx.) $\lambda_1(\Lambda)$ norm
  but also n linearly indep vecs norm at most $\lambda_n(\Lambda)$

Def 10. $SIVP_\gamma$ Approx. Shortest Independent Vec Prob

γ as before. B. n-dim Λ.

goal: find n linearly indep vecs $\vec{s}_1, \cdots, \vec{s}_n$

st. $\|\vec{s}_i\| \leq \gamma \cdot \lambda_n(\Lambda)$ for all i

The next: 2 cases to distinguish.

Def 11. $GapSVP_\gamma$ decision SVP $GapsVP_\gamma$

γ as before.

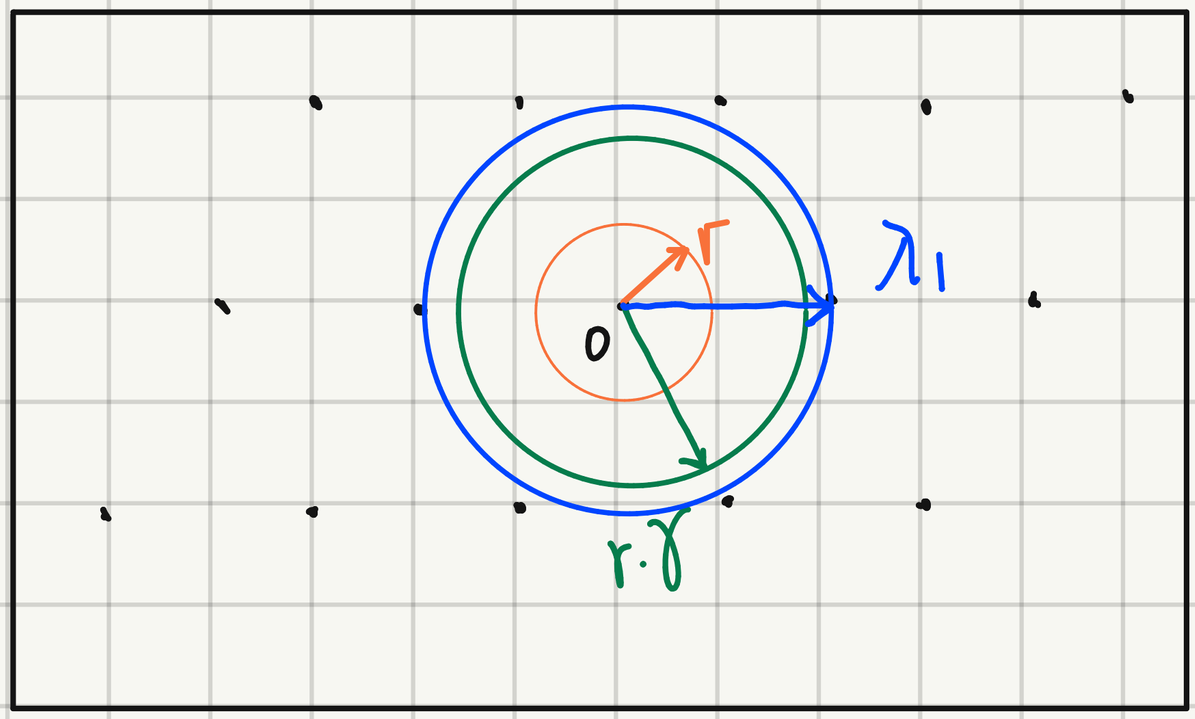
(B, r) : B basis. n-dim Λ

$r > 0 \in \mathbb{R}$

$\begin{cases} \text{YES instance} \leftarrow \lambda_1(\Lambda) \leq \gamma \cdot r \\ \text{NO instance} \leftarrow \lambda_1(\Lambda) > \gamma \cdot r \end{cases}$

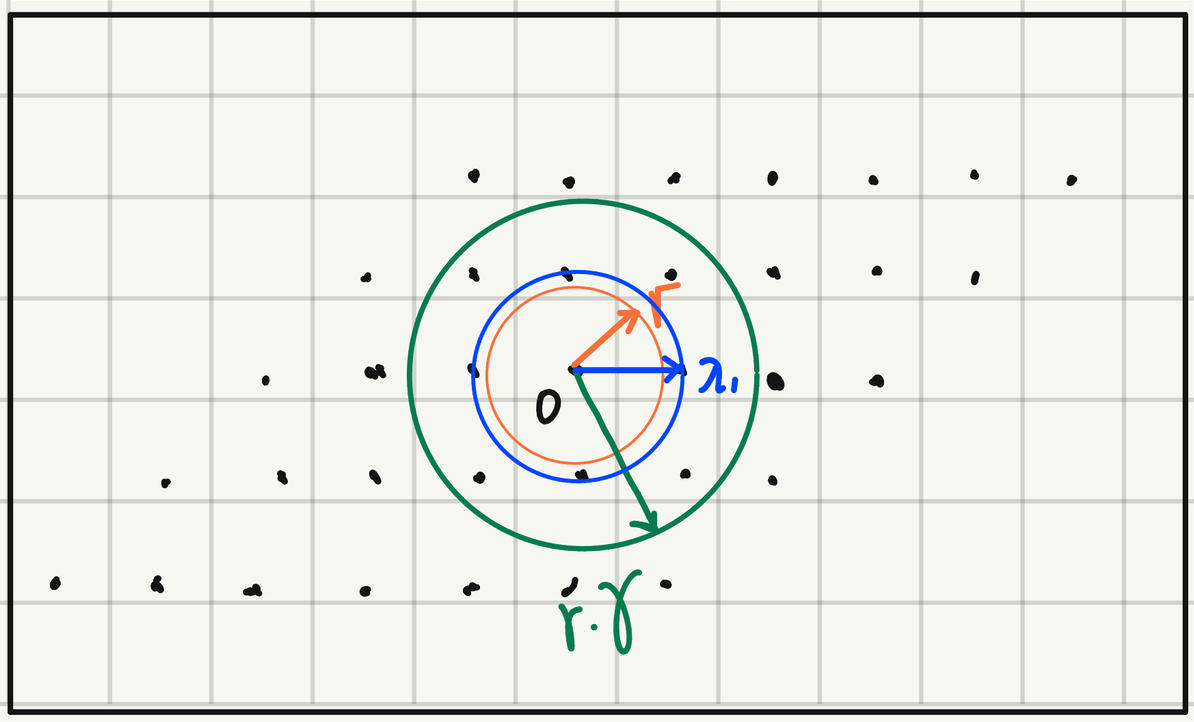
goal: distinguish YES / NO

e.g.



NO instance.

$\lambda_1 > \gamma \cdot r$



YES instance.

$\lambda_1 \leq r \cdot \gamma$

2.2. Closest Vector Problem.

CVP: Given a point in span. find a vec closest to it. we def approx. ver

Def 12. CVP$_\gamma$

B. n-dim. Λ γ.

Input: a point $\vec{t} \in \text{span}(\Lambda)$

goal: find $\vec{x} \in \Lambda$

st. $\|\vec{t} - \vec{x}\| = \min_{\vec{y} \in \Lambda} \gamma \cdot \|\vec{t} - \vec{y}\|$

Def 13. GapCVP$_\gamma$ (search)

γ. B. n-dim. Λ.

input: $(B, \vec{t}, r)$

- B basis.
- $\vec{t} \in \text{span}(\Lambda)$
- $r > 0 \in \mathbb{R}$

- YES: $\text{dist}(\vec{t}, \Lambda) \leq \gamma \cdot r$
- NO: $\text{dist}(\vec{t}, \Lambda) > \gamma \cdot r$

goal: distinguish.

- CVP$_\gamma$ has not been proved secure for cryptosystem.
  → a promise ver of CVP$_\gamma$

Def 14 BDD_γ Bounded Distance Decoding problem.

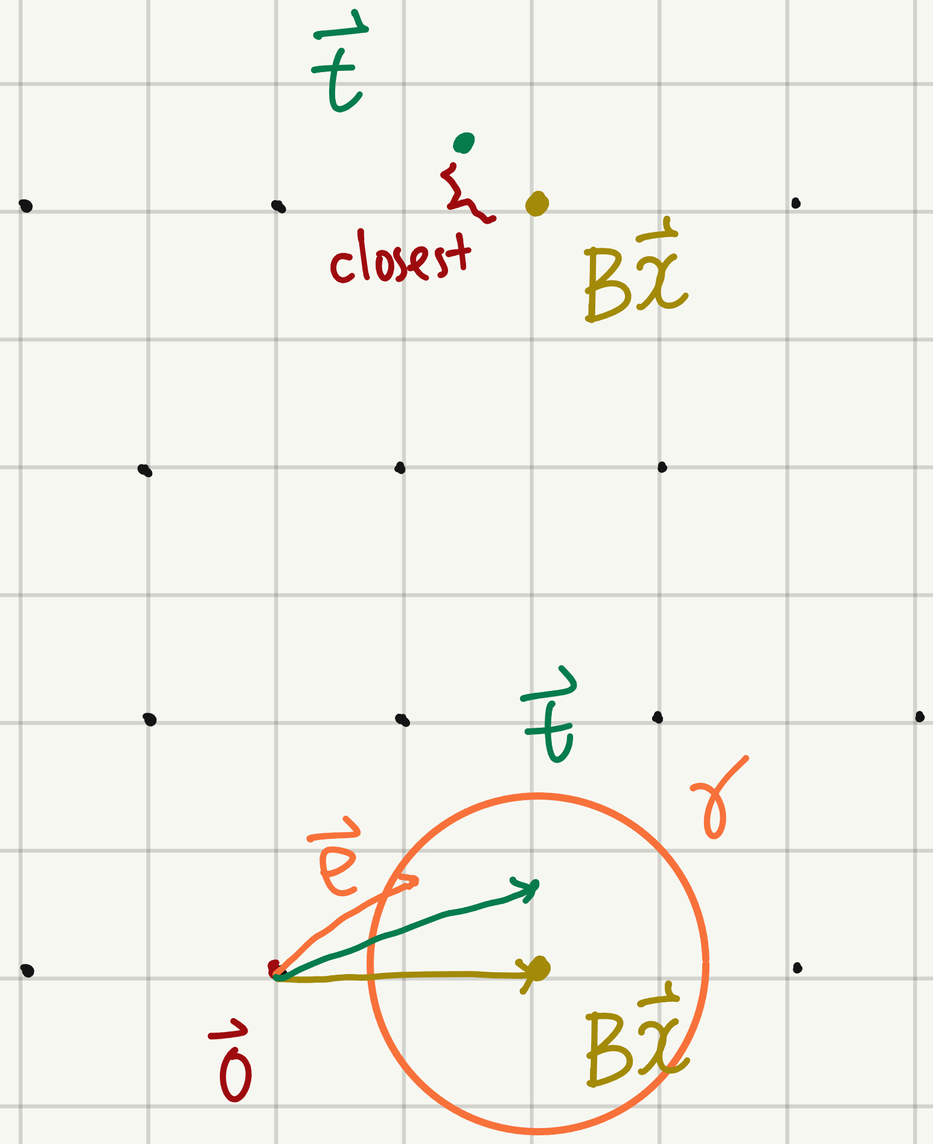
B. n-dim. Λ. γ.

input: $\vec{t} \in \mathbb{R}^n$ of the form $\vec{t} = \vec{x} + \vec{e}$
where $\vec{x} \in \Lambda$, $\|\vec{e}\| \leq \gamma$.

goal: find $\vec{x}$ (or $\vec{e}$)

- SVP is like CVP with $\vec{t} = \vec{0}$ but CVP allows sol to be $\vec{0}$, SVP not.
- possible: $SVP_\gamma \xrightarrow{rd} CVP_\gamma$
  $CVP_\gamma \xrightarrow{rd}$ (in this dir, γ increases to $\sqrt{n}\gamma^2$)

e.g.



2.3 Easy Computational Problem.

SVP. CVP: difficult.
still some easy probs.

Def 15. Membership.

B. n-dim Λ. $\vec{v} \in \mathbb{R}^n$.
goal: decide if $\vec{v} \in \Lambda(B)$.

Def 16: Equivalence

$B, B' \in \mathbb{R}^{n \times n}$
goal: decide if $\Lambda(B) = \Lambda(B')$

2.4. Reductions

Exp $\quad \text{GapSVP}_\gamma \rightarrow \text{GapCVP}_\gamma$

Thm 17.

There is a <u>polynomial-time reduction</u> from GapSVP_γ to GapCVP_γ for any input lattice B and any approx. factor γ.

- strategy: take a target $\vec{w} + \vec{v}$
  input a modified basis $\setminus \{\vec{w}\}$.

Proof

for every $j \in [n]$, def basis

$$B^{(j)} := [\vec{b}_1, \cdots, \vec{b}_{j-1}, 2\vec{b}_j, \vec{b}_{j+1}, \cdots, \vec{b}_n]$$

($B^{(j)}$ does not contain $\vec{b}_j$)

e.g.

$B^{(1)} = [2\vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n]$

$B^{(2)} = [\vec{b}_1, 2\vec{b}_2, \cdots, \vec{b}_n]$

$B^{(3)} = [\vec{b}_1, \vec{b}_2, 2\vec{b}_3, \cdots, \vec{b}_n]$

...

claim 1. let $\vec{v} = \sum_i c_i \vec{b}_i$ be a short vector.

$\exists$ an index j st. $c_j = 1 \mod 2$.

claim 2 let $\vec{v} = \sum_i c_i \vec{b}_i$ be a vec in $\Lambda(B)$

st. $\exists j$ st. $c_j = 1 \mod 2$

Then:

$$\vec{u} := \frac{c_j + 1}{2}(2\vec{b}_j) + \sum_{i \neq j} c_i \vec{b}_i \in \Lambda(B^{(j)})$$

and:

$$\| \vec{u} - \vec{b}_j \| = \| \vec{v} \|$$

claim 3. let $\vec{u} = c_j' \cdot 2\vec{b}_j + \sum_i c_i \vec{b}_i \in \Lambda(B^{(j)})$

Then:

$$\vec{v} := (2c_j' - 1)\vec{b}_j + \sum_{i \neq j} c_i \vec{b}_i$$

is non-zero, lies in $\Lambda(B)$. yiels $\|\vec{v}\| = \|\vec{u} - \vec{b}_j\|$

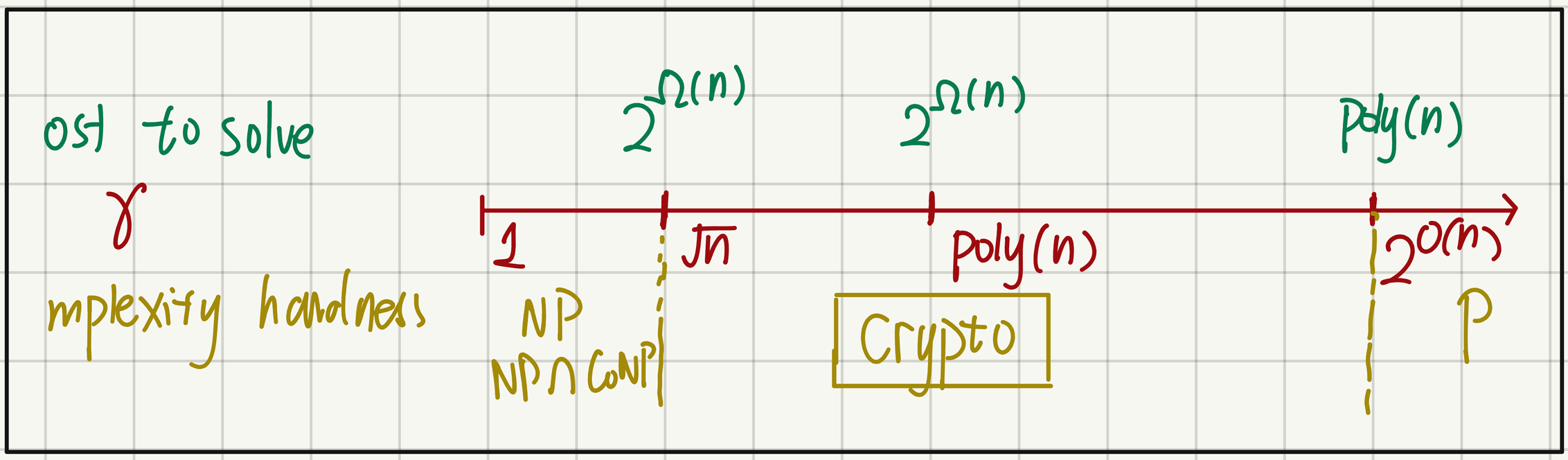
Reduction (next page)

Reduction

(B, r) : GapSVP$_\gamma$

↳ $(B^{(j)}, \vec{b}_j, r)$ for $j \in [n]$: GapCVP$_\gamma$

- if (B, r) is a YES, then $\exists j$ st $(B^{(j)}, \vec{b}_j, r)$ is a YES.
- if (B, r) NO. $(B^{(j)}, \vec{b}_j, r)$ every NO



- hardness SVP$_\gamma$ ≥ SIVP$_\gamma$ ≥ GapSVP$_\gamma$

($\sqrt{n}\gamma \leftarrow r$) ($n\gamma \leftarrow \gamma$)

2.5. Complexity & Algorithm

- crypto need : $\gamma = poly(n)$
- 1982, LLL : Solves SVP$_\gamma$. γ exponentially large in n-dim.
- 1987. Schnorr : runtime & γ tradeoff.
  → BKZ, 1994. [SE94]
- → Solving SVP$_\gamma$.
  - γ poly(n) → runtime ~ $2^{\tilde{O}(n)}$
  - rt poly(n) → $\gamma \sim 2^{\tilde{O}(n)}$

Conjecture 18.

There is no poly time classical / quantum alg that approx. SVP_γ, $GapSVP_\gamma$, or $SIVP_\gamma$ to within poly γ (for all possible input lattices)

↳ LBC starts!

§3. Crypto Dilemma

- Worst-case problem
  - { hard to solve in worst case
    but not in any case
  - ⇒ not very feasible for crypto
- average-case problem ← what we need
  - random instances
  - e.g. LWE, SIS.
    - at least as hard as w-c p → params
- Also: crypto on w-c p, but: { no sec proof
  params choices