§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.

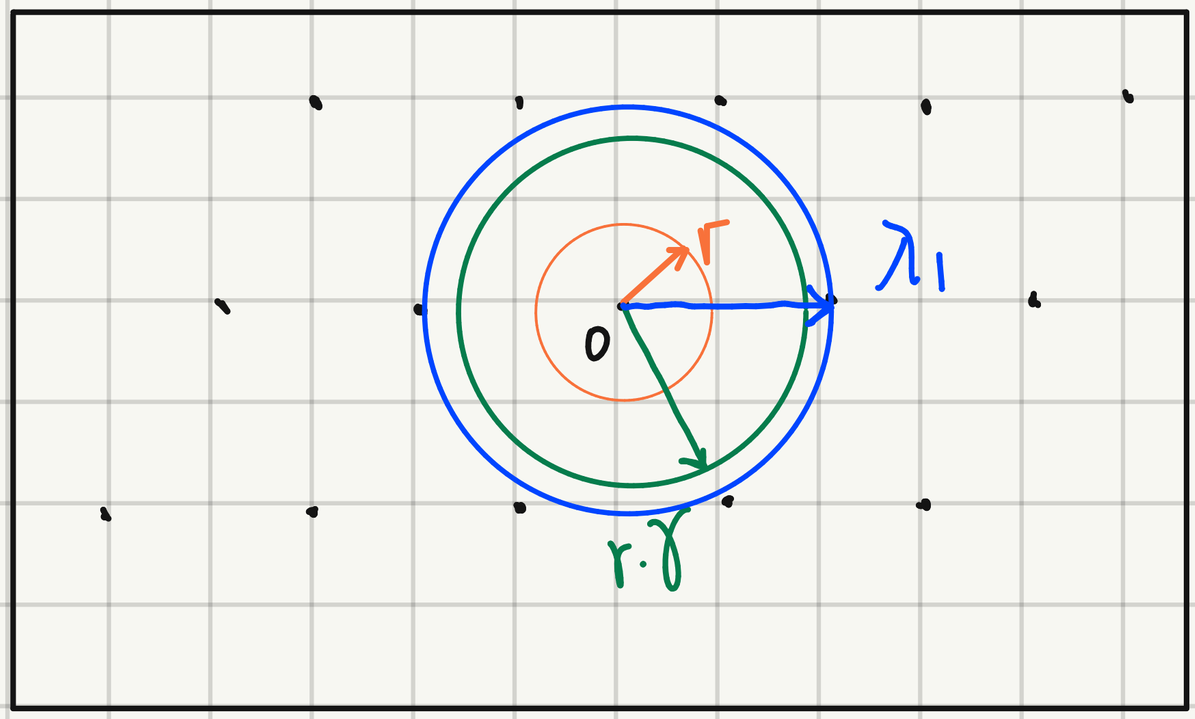
(B, r) : B basis. n-dim Λ

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

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

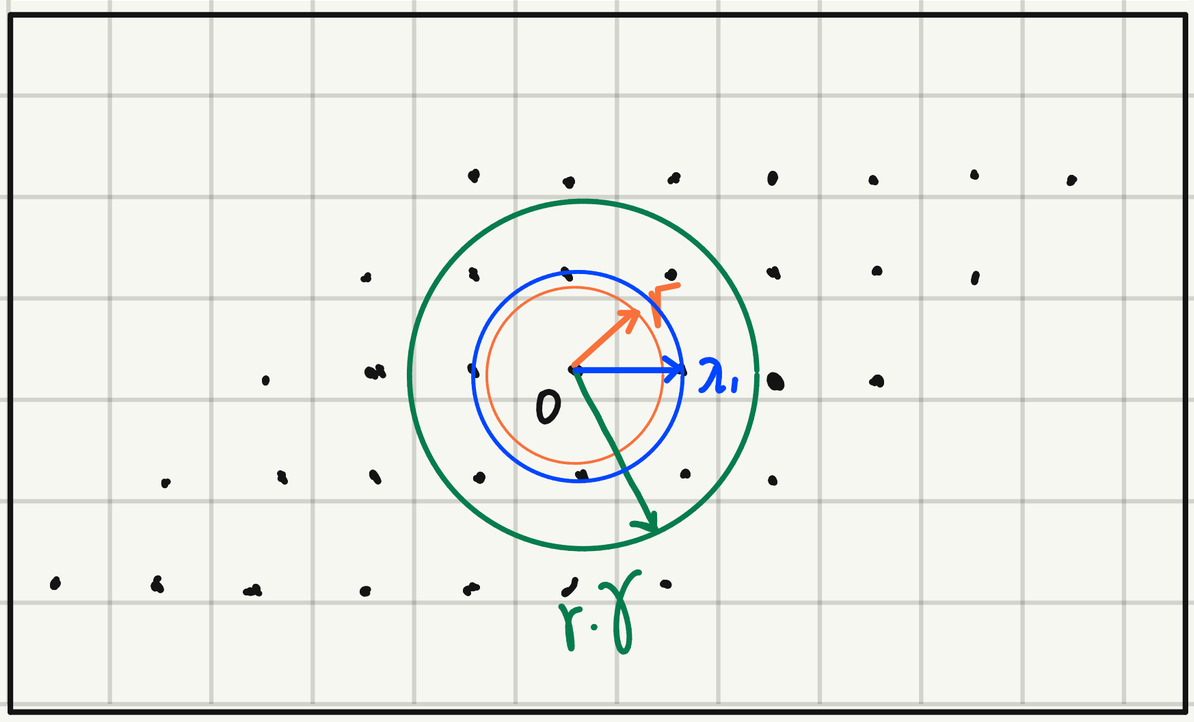
goal: distinguish YES / NO

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.

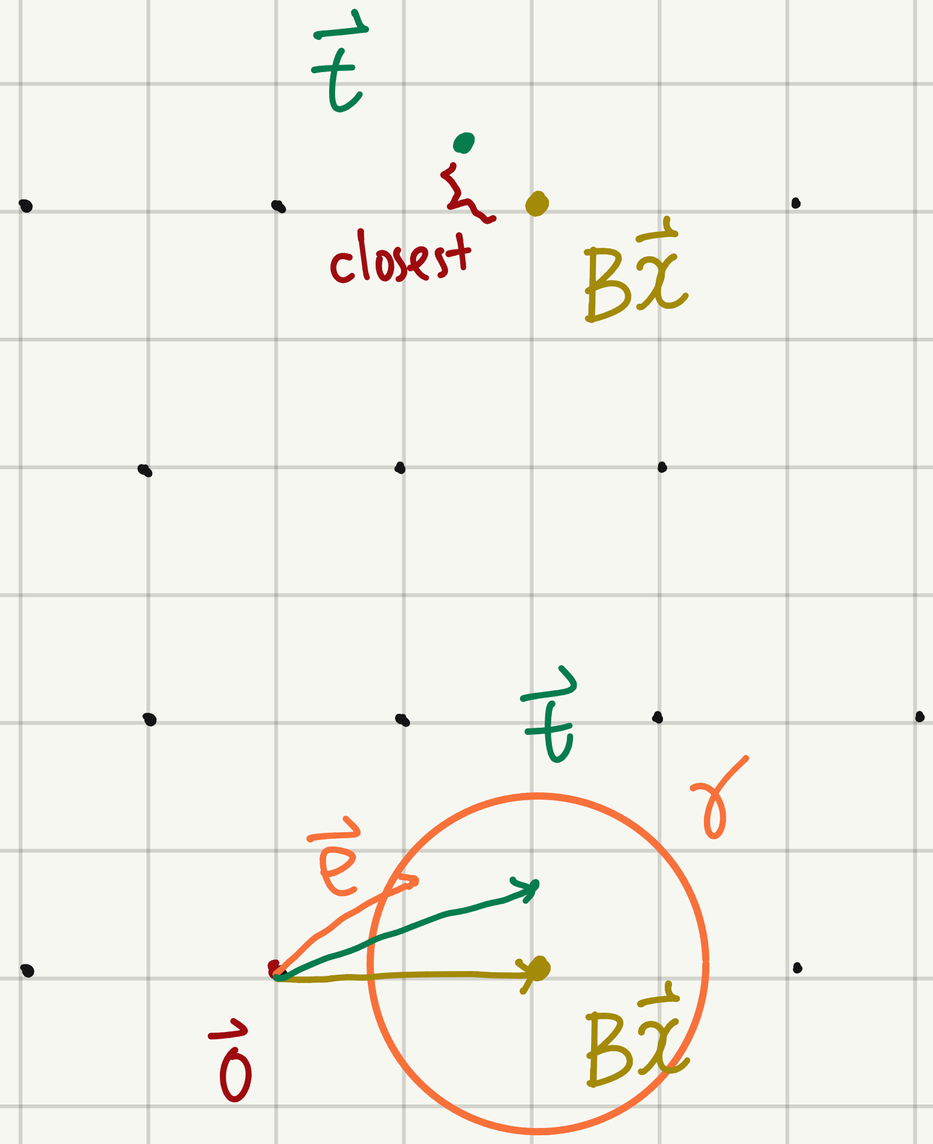
B. n-dim. Λ. γ.

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

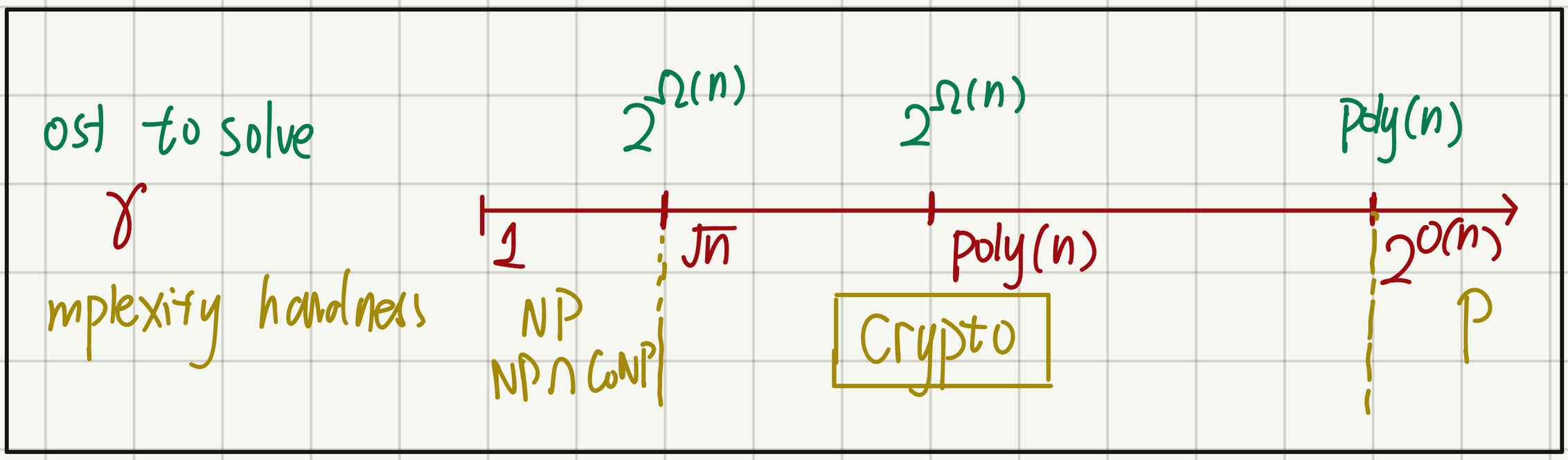
Reduction (next page)

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