Cornell Bowers CIS
Computer Science

CHARM Seminar
Sep 8, 2024

Recursive Lattice Reduction

Spencer Peters
and

Divesh Aggarwal

Thomas Espitau

Noah S.D.

The Plan

- Introduction
- Preliminaries
- Warmup: SVP $\Rightarrow$ SVP (inefficient)
- DSP $\Rightarrow$ DSP
- DSP $\Rightarrow$ SVP
- Representing the lattices in our reductions
- Computer-Aided Search & Numerical Bounds

Introduction

Lattices

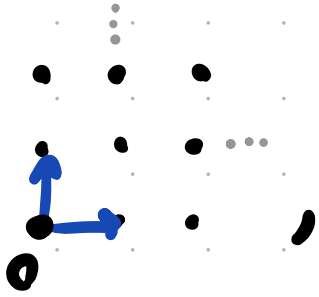
A *lattice* $\mathcal{L} = \mathcal{L}(B)$ is specified by a *basis* $B = (b_1, b_2, \ldots, b_n)$ of linearly independent vectors $b_i \in \mathbb{R}^d$:

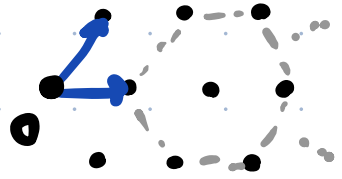
$$\mathcal{L}(B) := \left\{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid z_i \in \mathbb{Z} \right\}$$

Lattices

A *lattice* $\mathcal{L} = \mathcal{L}(B)$ is specified by a *basis* $B = (b_1, b_2, \ldots, b_n)$ of linearly independent vectors $b_i \in \mathbb{R}^d$:

$$\mathcal{L}(B) := \{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid z_i \in \mathbb{Z} \}$$

e.g., $\mathbb{Z}^2$: 

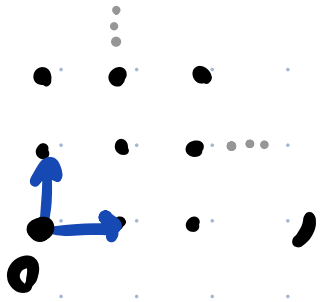
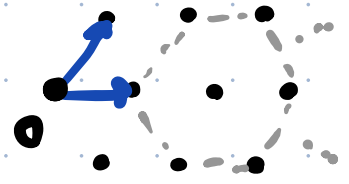
, $\mathbb{Z}^n$:  , Hexagonal: 

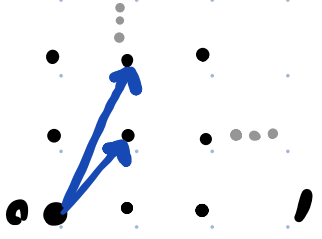
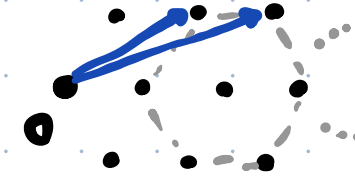
, ...

Lattices

A *lattice* $\mathcal{L} = \mathcal{L}(B)$ is specified by a *basis* $B = (b_1, b_2, \ldots, b_n)$ of linearly independent vectors $b_i \in \mathbb{R}^d$:

$$\mathcal{L}(B) := \left\{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid z_i \in \mathbb{Z} \right\}$$

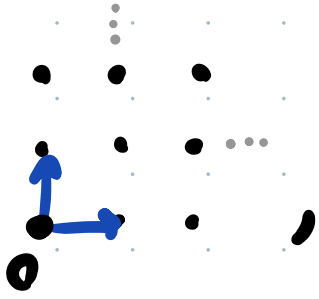
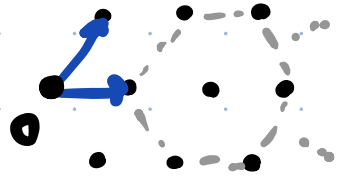
e.g., $\mathbb{Z}^2$:  , $\mathbb{Z}^n$:  , Hexagonal:  , ...

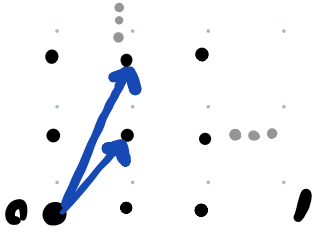
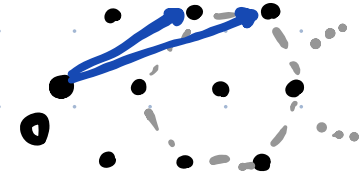
$\mathbb{Z}^2$:  , $\mathbb{Z}^n$:  , Hexagonal:  , ...

Lattices

A *lattice* $\mathcal{L} = \mathcal{L}(B)$ is specified by a *basis* $B = (b_1, b_2, \ldots, b_n)$ of linearly independent vectors $b_i \in \mathbb{R}^d$:

$$\mathcal{L}(B) := \{ z_1 b_1 + z_2 b_2 + \cdots + z_n b_n \mid z_i \in \mathbb{Z} \}$$

e.g., $\mathbb{Z}^2$:  , $\mathbb{Z}^n$:  , Hexagonal:  , ...

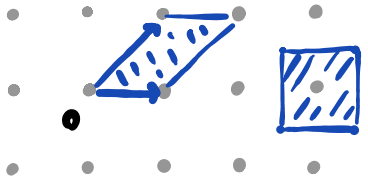
$\mathbb{Z}^2$:  , $\mathbb{Z}^n$:  , Hexagonal:  , ...

n is called the *rank* or *dimension* of $\mathcal{L}$.

Lattices

$$\lambda_1(\mathcal{L}) := \min_{\substack{y \in \mathcal{L} \\ y \neq \vec{0}}} \|y\|$$

Lattices

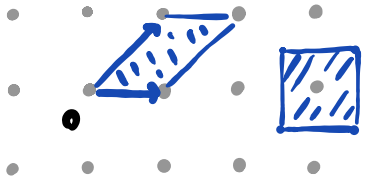


$$\lambda_1(\mathcal{L}) := \min_{\substack{y \in \mathcal{L} \\ y \neq \vec{0}}} \|y\|$$

$$\det(\mathcal{L}) := \sqrt{\det(B^T B)}$$

$$= \frac{\text{volume}}{\text{point}} = \frac{1}{\text{density}}.$$

Lattices



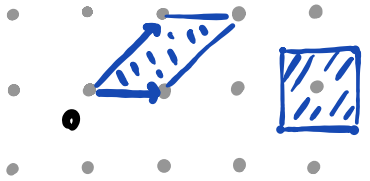
$$\lambda_1(\mathcal{L}) := \min_{\substack{y \in \mathcal{L} \\ y \neq \vec{0}}} \|y\|$$

$$\det(\mathcal{L}) := \sqrt{\det(B^T B)}$$

$$= \frac{\text{volume}}{\text{point}} = \frac{1}{\text{density}}.$$

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

Lattices



$$\lambda_1(\mathcal{L}) := \min_{\substack{y \in \mathcal{L} \\ y \neq \vec{0}}} \|y\|$$

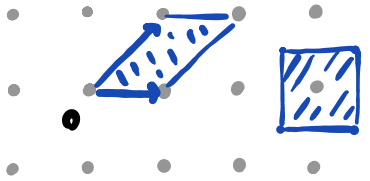
$$\det(\mathcal{L}) := \sqrt{\det(B^T B)}$$

$$= \frac{\text{volume}}{\text{point}} = \frac{1}{\text{density}}.$$

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

SVP: Find $v \in \mathcal{L}$ with $\|v\| = \lambda_1(\mathcal{L})$.

Lattices



$$\lambda_1(\mathcal{L}) := \min_{\substack{y \in \mathcal{L} \\ y \neq \vec{0}}} \|y\|$$

$$\det(\mathcal{L}) := \sqrt{\det(B^T B)}$$

$$= \frac{\text{volume}}{\text{point}} = \frac{1}{\text{density}}.$$

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

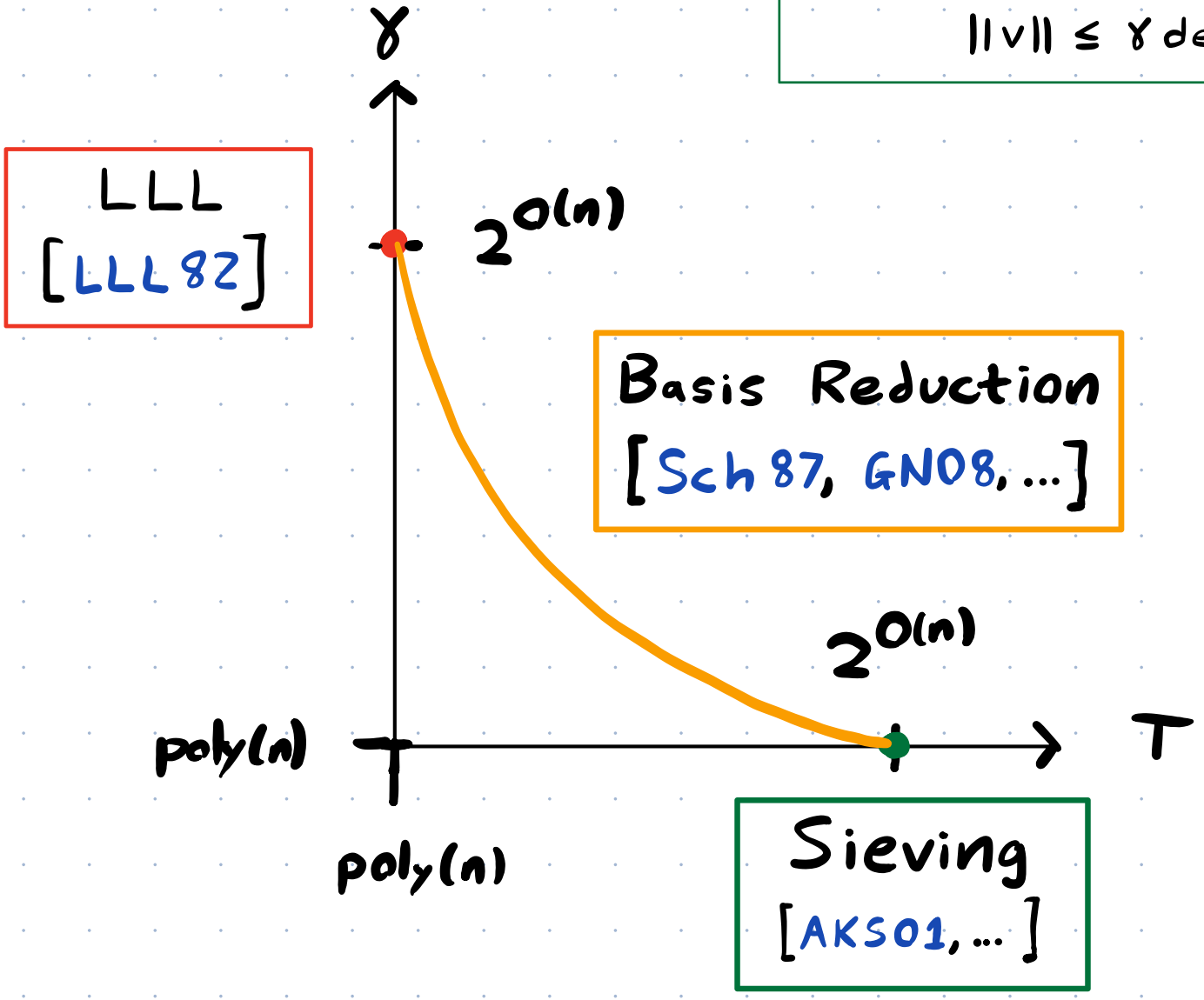
SVP: Find $v \in \mathcal{L}$ with $\|v\| = \lambda_1(\mathcal{L})$.

γ-approximate (H)SVP: Find $v \in \mathcal{L}$:

$$\|v\| \leq \gamma \det(\mathcal{L})^{1/n}$$

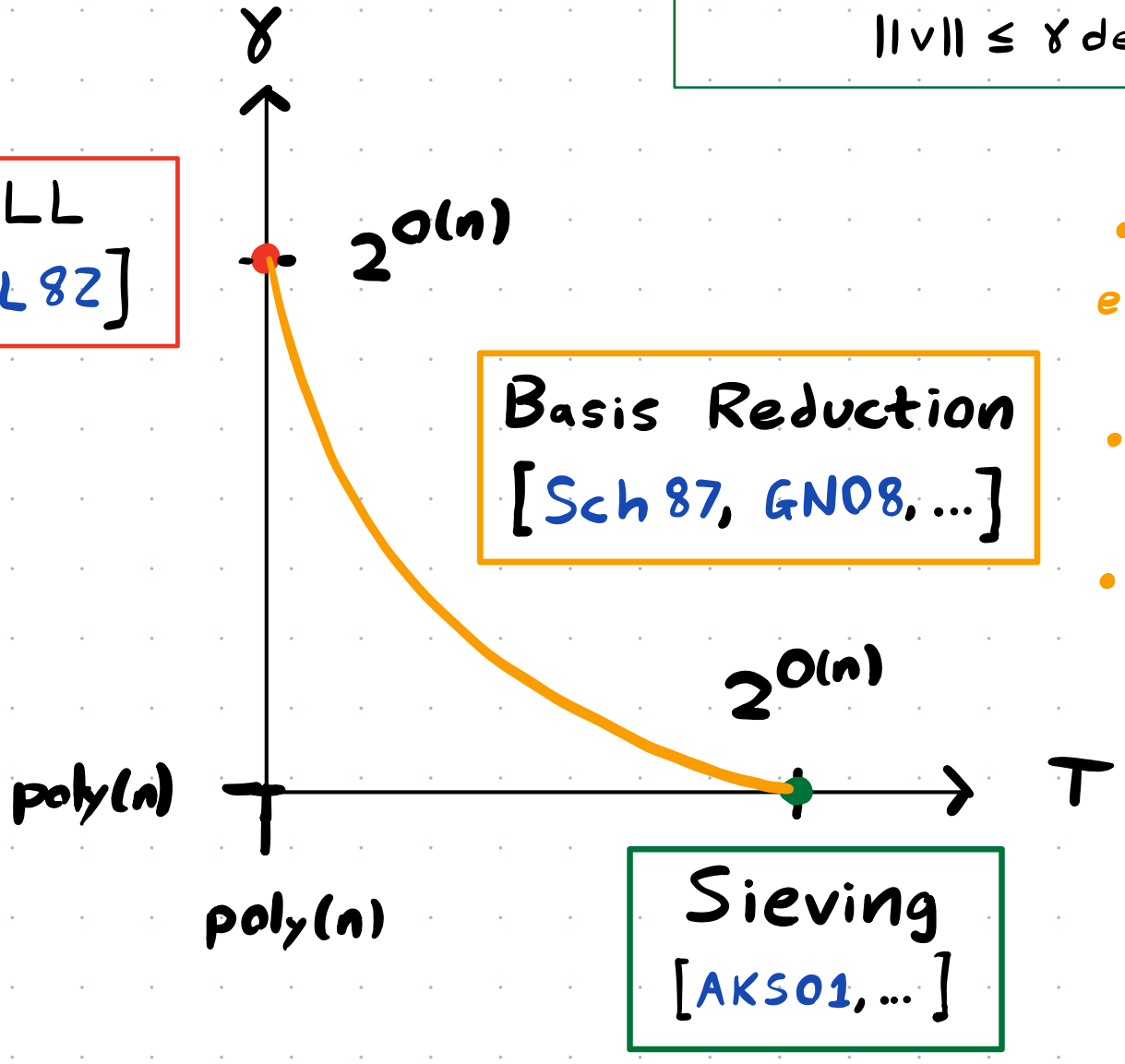
Time / Approximation Tradeoffs

γ-approximate (H)SVP: Find $v \in \mathcal{L}$:
$\|v\| \leq \gamma \det(\mathcal{L})^{1/n}$



Time / Approximation Tradeoffs

γ-approximate (H)SVP: Find $v \in \mathcal{L}$:
$\|v\| \leq \gamma \det(\mathcal{L})^{1/n}$



LLL
[LLL82]

Basis Reduction
[Sch87, GN08, ...]

Sieving
[AKS01, ...]

- Works by solving exact SVP in dimension κ
- $T = \text{poly}(n)\, 2^{O(\kappa)}$
- $\gamma = \kappa^{\frac{(n-1)}{2(\kappa-1)}} \approx \kappa^{\frac{n}{2\kappa}}$.

Basis Reduction Algorithms

- All basis reduction algorithms follow the basic approach of LLL: iteratively improve the basis by solving SVP exactly in smaller dimension.

- Analysis is intricate
  - Our best (practical) algorithms are *heuristic*

Basis Reduction Algorithms

- All basis reduction algorithms follow the basic approach of LLL: iteratively improve the basis by solving SVP exactly in smaller dimension.

- Analysis is intricate
  - Our best (practical) algorithms are *heuristic*

- This talk: match Basis Reduction tradeoff with an "Algorithms 101"-style recursive algorithm.
  - "Recurse on a smaller-dimensional lattice!"

Basis Reduction Algorithms

- All basis reduction algorithms follow the basic approach of LLL: iteratively improve the basis by solving SVP exactly in smaller dimension.

- Analysis is intricate
  - Our best (practical) algorithms are *heuristic*

- This talk: match Basis Reduction tradeoff with an "Algorithms 101"-style recursive algorithm.
  - "Recurse on a smaller-dimensional lattice!"
  - Should be a *sublattice*

Basis Reduction Algorithms

- All basis reduction algorithms follow the basic approach of LLL: iteratively improve the basis by solving SVP exactly in smaller dimension.

- Analysis is intricate
  - Our best (practical) algorithms are *heuristic*

- This talk: match Basis Reduction tradeoff with an "Algorithms 101"-style recursive algorithm.
  - "Recurse on a smaller-dimensional lattice!"
  - Should be a *sublattice*
  - But should still have *short vectors*
    - —i.e., small determinant
    - —i.e. should be a <u>dense</u> sublattice.

An approach for solving SVP

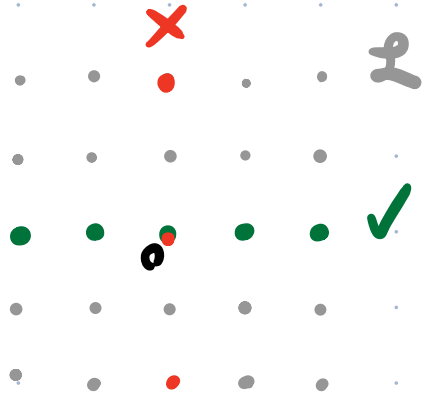
$A(\mathcal{L})$:

1. Find dense sublattice $\mathcal{L}' \subset \mathcal{L}$ (somehow)
2. Return $A(\mathcal{L}')$.

- For the base case, when $\text{rank}(\mathcal{L}) = \kappa$, output $SVP(\mathcal{L})$ — that is, use an exact algorithm.

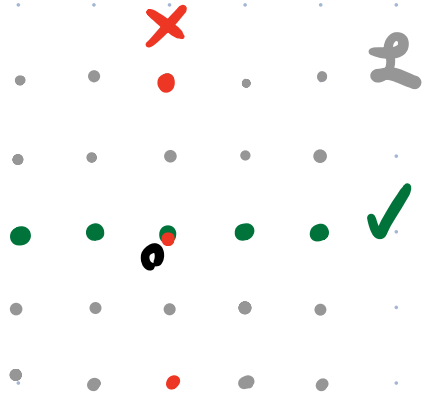
The Densest Sublattice Problem

A (primitive) sublattice $\mathcal{L}'$ of $\mathcal{L}$ is the intersection of $\mathcal{L}$ with a subspace.



The Densest Sublattice Problem

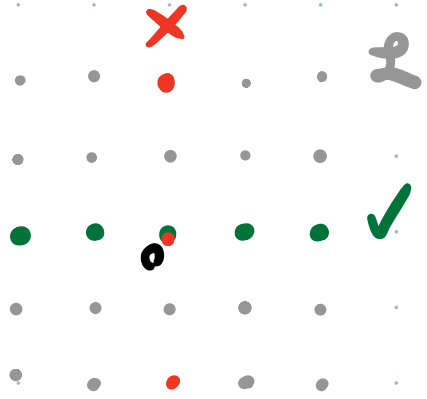
A *(primitive)* sublattice $\mathcal{L}'$ of $\mathcal{L}$ is the intersection of $\mathcal{L}$ with a subspace.



γ-$DSP_\ell(\mathcal{L})$: Find $\mathcal{L}' \subset \mathcal{L}$ of rank ℓ such that $\det(\mathcal{L}') \leq \gamma \cdot \det(\mathcal{L})^{\ell/n}$.

The Densest Sublattice Problem

A (*primitive*) sublattice $\mathcal{L}'$ of $\mathcal{L}$ is the intersection of $\mathcal{L}$ with a subspace.



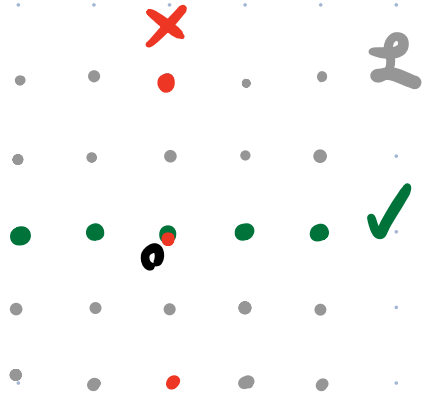
γ-$\mathrm{DSP}_\ell(\mathcal{L})$: Find $\mathcal{L}' \subset \mathcal{L}$ of rank ℓ such that $\det(\mathcal{L}') \le \gamma \cdot \det(\mathcal{L})^{\ell/n}$.

$$\gamma(\mathcal{L}', \mathcal{L}) := \frac{\det(\mathcal{L}')}{\det(\mathcal{L})^{\ell/n}}$$

$\sqrt{\delta_{n,\ell}}$ is the best γ possible in general (for worst-case $\mathcal{L}$)

The Densest Sublattice Problem

A (*primitive*) sublattice $\mathcal{L}'$ of $\mathcal{L}$ is the intersection of $\mathcal{L}$ with a subspace.



γ-$\mathrm{DSP}_\ell(\mathcal{L})$: Find $\mathcal{L}' \subset \mathcal{L}$ of rank ℓ such that $\det(\mathcal{L}') \le \gamma \cdot \det(\mathcal{L})^{\ell/n}$.

$$\gamma(\mathcal{L}', \mathcal{L}) := \frac{\det(\mathcal{L}')}{\det(\mathcal{L})^{\ell/n}}$$

$\sqrt{\delta_{n,\ell}}$ is the best γ possible in general (for worst-case $\mathcal{L}$)

γ-DSP with $\ell = 1$ is exactly γ-SVP.

Main Result

For any $\kappa = \kappa(n) \geq 10$, $1 \leq \ell = \ell(n) \leq n - \kappa + 1$,

there is an efficient reduction

from γ-DSP$_\ell$ on lattices of rank n

to HSVP on lattices of rank κ,

for $\gamma = (1 + o(1)) \cdot \kappa^{\frac{\ell(n-\ell)}{2(\kappa-1)}}$.

- The $\ell = 1$ case is a HSVP to HSVP reduction which asymptotically matches state-of-the-art basis reduction algorithms.
- The $\ell > 1$ case gives, to the best of our knowledge, the fastest known γ-DSP$_\ell$ algorithm for $\ell > \kappa$ for all $\gamma << 2^{O(n\ell)}$, in the cryptographically most relevant regime $\kappa = \Omega(n)$.

Preliminaries

γ-DSP is Composable

Consider $\mathcal{L}'' \subset \mathcal{L}' \subset \mathcal{L}$.

rank: $\ell < m < n$

γ-DSP is Composable

Consider $\mathcal{L}'' \subset \mathcal{L}' \subset \mathcal{L}$.

rank: $\ell < m < n$

$\mathcal{L}'' \in \gamma_1\text{-DSP}_\ell(\mathcal{L}')$ AND $\mathcal{L}' \in \gamma_2\text{-DSP}_m(\mathcal{L})$

γ-DSP is Composable

Consider $\mathcal{L}'' \subset \mathcal{L}' \subset \mathcal{L}$.

rank: $\ell < m < n$

$$\mathcal{L}'' \in \gamma_1\text{-DSP}_\ell(\mathcal{L}') \text{ AND } \mathcal{L}' \in \gamma_2\text{-DSP}_m(\mathcal{L})$$

$$\Rightarrow \mathcal{L}'' \in (\gamma_1 \cdot \gamma_2^{\ell/m})\text{-DSP}_\ell(\mathcal{L})$$

γ-DSP is Composable

Consider $\mathcal{L}'' \subset \mathcal{L}' \subset \mathcal{L}$.

rank: $\ell \leq m \leq n$

$$\mathcal{L}'' \in \gamma_1\text{-DSP}_\ell(\mathcal{L}') \text{ AND } \mathcal{L}' \in \gamma_2\text{-DSP}_m(\mathcal{L})$$

$$\Rightarrow \mathcal{L}'' \in (\gamma_1 \cdot \gamma_2^{\ell/m})\text{-DSP}_\ell(\mathcal{L})$$

Proof. $\det(\mathcal{L}'') \leq \gamma_1 \cdot \det(\mathcal{L}')^{\ell/m}$

$= \gamma_1 \cdot (\gamma_2 \det(\mathcal{L})^{\ell/m})^{m/n} = \gamma_1 \cdot \gamma_2^{\ell/m} \det(\mathcal{L})^{\ell/m}$.

γ-DSP is Self-Dual

$$\mathcal{L}^* := \{ w \in \mathrm{span}(\mathcal{L}) : \forall y \in \mathcal{L}, \langle w, y \rangle \in \mathbb{Z} \}$$

γ-DSP is Self-Dual

$$\mathcal{L}^* := \{ w \in \mathrm{span}(\mathcal{L}) : \forall y \in \mathcal{L}, \langle w, y \rangle \in \mathbb{Z} \}$$

$$(\mathcal{L}^*)^* = \mathcal{L}$$

$$\det(\mathcal{L}^*) = 1 / \det(\mathcal{L})$$

γ-DSP is Self-Dual

$$\mathcal{L}^* := \{ w \in \mathrm{span}(\mathcal{L}) : \forall y \in \mathcal{L}, \langle w, y \rangle \in \mathbb{Z} \}$$

$$(\mathcal{L}^*)^* = \mathcal{L}$$

$$\det(\mathcal{L}^*) = 1 / \det(\mathcal{L})$$

- There is a bijection from rank ℓ sublattices of $\mathcal{L}$ to rank $(n-\ell)$ sublattices of $\mathcal{L}^*$, preserving the approximation factor!

$$\mathcal{L}' \in \gamma\text{-DSP}_\ell(\mathcal{L})$$

$$\Leftrightarrow$$

$$\mathcal{L}^* \cap (\mathcal{L}')^\perp \in \gamma\text{-DSP}_{n-\ell}(\mathcal{L}^*)$$

γ-DSP is Self-Dual

$$\mathcal{L}^* := \{ w \in \mathrm{span}(\mathcal{L}) : \forall y \in \mathcal{L}, \langle w, y \rangle \in \mathbb{Z} \}$$

$$(\mathcal{L}^*)^* = \mathcal{L}$$

$$\det(\mathcal{L}^*) = 1 / \det(\mathcal{L})$$

- There is a bijection from rank ℓ sublattices of $\mathcal{L}$ to rank $(n-\ell)$ sublattices of $\mathcal{L}^*$, preserving the approximation factor!

$$\mathcal{L}' \in \gamma\text{-DSP}_\ell(\mathcal{L})$$

$$\Leftrightarrow$$

$$\mathcal{L}^* \cap (\mathcal{L}')^\perp \in \gamma\text{-DSP}_{n-\ell}(\mathcal{L}^*)$$

Important Special Case:

$$w \in \gamma\text{-SVP}(\mathcal{L}^*)$$

$$\Leftrightarrow$$

$$\mathcal{L} \cap w^\perp \in \gamma\text{-DSP}_{n-1}(\mathcal{L}).$$

Warmup

Warm-up: $\ell = 1$ (SVP $\Rightarrow$ SVP)

- Plan:
  1. $w \leftarrow A(\mathcal{L}^*)$
  2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$
  3. Output $A(\mathcal{L}')$.

- Base case: if $\text{rank}(\mathcal{L}) = \kappa$, output $\text{SVP}(\mathcal{L})$.

Warm-up: $\ell = 1$ (SVP $\Rightarrow$ SVP)

- Plan:

1. $w \leftarrow A(\mathcal{L}^*)$

    1. $w \leftarrow A(\mathcal{L})$

        1. $w \leftarrow A(\mathcal{L}^*)$

            ...

Warm-up: $\ell = 1$ (SVP $\Rightarrow$ SVP)

- Plan:
  - Choose initial "depth parameter"

$$\tau = \tau(n) \geq 0.$$

1. $w \leftarrow A(\mathcal{L}^*, \tau - 1)$ "Right child"
2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$
3. Output $A(\mathcal{L}', \tau)$ "Left child"

- Base cases:

if $\tau = 0$, output $LLL(\mathcal{L}, 1)$

if $\text{rank}(\mathcal{L}) = \kappa$, output $SVP(\mathcal{L})$.

Analysis

1. $w \leftarrow A(\mathcal{L}^*, \tau - 1)$
2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$ (Dual)
3. Output $y \leftarrow A(\mathcal{L}', \tau)$ (Composition)

Analysis

1. $w \leftarrow A(\mathcal{L}^*, \tau - 1)$
2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$ (Dual)
3. Output $y \leftarrow A(\mathcal{L}', \tau)$ (Composition)

$$\gamma(y, \mathcal{L}) \leq \gamma(y, \mathcal{L}') \cdot \gamma(\mathcal{L}', \mathcal{L})^{\frac{1}{n-1}}$$ (Compositionality)

$\ell = 1, \; m = n-1$

Analysis

1. $w \leftarrow A(\mathcal{L}^*, \tau - 1)$
2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$ (Dual)
3. Output $y \leftarrow A(\mathcal{L}', \tau)$ (Composition)

$$\gamma(y, \mathcal{L}) \le \gamma(y, \mathcal{L}') \cdot \gamma(\mathcal{L}', \mathcal{L})^{\frac{1}{n-1}}$$ (Compositionality) $\ell = 1,\ m = n-1$

$$= \gamma(y, \mathcal{L}') \cdot \gamma(w, \mathcal{L}^*)^{\frac{1}{n-1}}$$ (Duality)

Analysis

1. $w \leftarrow A(\mathcal{L}^*, \tau - 1)$
2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$ (Dual)
3. Output $y \leftarrow A(\mathcal{L}', \tau)$ (Composition)

$$\gamma(y, \mathcal{L}) \le \gamma(y, \mathcal{L}') \cdot \gamma(\mathcal{L}', \mathcal{L})^{\frac{1}{n-1}}$$ (Compositionality, $\ell = 1$, $m = n-1$)

$$= \gamma(y, \mathcal{L}') \cdot \gamma(w, \mathcal{L}^*)^{\frac{1}{n-1}}$$ (Duality)

$$\Rightarrow \boxed{\gamma(n, \tau) \le \gamma(n-1, \tau) \cdot \gamma(n, \tau-1)^{\frac{1}{n-1}}.}$$

Analysis

1. $w \leftarrow A(\mathcal{L}^*, \tau - 1)$
2. $\mathcal{L}' := \mathcal{L} \cap w^\perp$ (Dual)
3. Output $y \leftarrow A(\mathcal{L}', \tau)$ (Composition)

$$\gamma(y, \mathcal{L}) \le \gamma(y, \mathcal{L}') \cdot \gamma(\mathcal{L}', \mathcal{L})^{\frac{1}{n-1}}$$ (Compositionality) $\ell = 1,\ m = n-1$

$$= \gamma(y, \mathcal{L}') \cdot \gamma(w, \mathcal{L}^*)^{\frac{1}{n-1}}$$ (Duality)

$$\Rightarrow \boxed{\gamma(n, \tau) \le \gamma(n-1, \tau) \cdot \gamma(n, \underline{\tau - 1})^{\frac{1}{n-1}}.}$$

Analysis

$$\gamma(n, \tau) \leq \gamma(n-1, \tau) \cdot \gamma(n, \tau-1)^{\frac{1}{n-1}}$$

$$\gamma(n, 0) = 2^n \qquad \gamma(\kappa, \tau) = \sqrt{\kappa}$$

- Can check that by induction

$$\gamma(n, \tau) \leq \kappa^{\frac{n-1}{2(\kappa-1)}} \cdot \exp\left(n^3 / 2^\tau\right)$$

- Taking $\tau = O(\log n)$ recovers basis reduction tradeoff:

$$\gamma = (1 + o(1))\, \kappa^{\frac{n-1}{2(\kappa-1)}}$$

Analysis

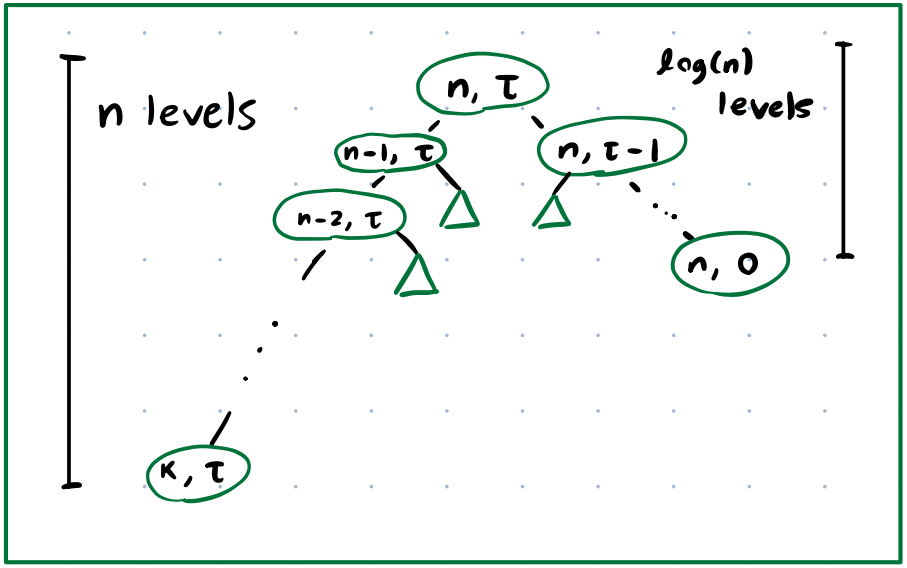
- SVP oracle calls dominate runtime.

$$C(n, \tau) = C(n-1, \tau) + C(n, \tau-1)$$

$$C(\kappa, \tau) = 1 \qquad C(n, 0) = 0$$

$$C(n, \tau) = \binom{n - \kappa + \tau - 1}{\tau} \approx n^{\tau} = n^{O(\log n)}$$

- Issue: Call tree highly unbalanced.



DSP ⇒ DSP

Take Two: $\ell > 1$ (DSP $\Rightarrow$ DSP)

- Plan:
  - Choose initial $\tau = O(\log n)$, $0 < \varepsilon < 1$.
  1. $\hat{\mathcal{L}} \leftarrow A(\mathcal{L}^*, \varepsilon n, \tau - 1)$
  2. $\mathcal{L}' := \mathcal{L} \cap (\hat{\mathcal{L}})^\perp$ // $\text{rank}(\mathcal{L}') = (1-\varepsilon)n$
  3. Output $A(\mathcal{L}', \ell, \tau)$

- Base cases:
  - if $\tau = 0$, output $\text{LLL}(\mathcal{L}, \ell)$
  - if $\text{rank}(\mathcal{L}) = \kappa$, output $\text{DSP}(\mathcal{L}, \ell)$.

Take Two: $\ell > 1$ (DSP $\Rightarrow$ DSP)

- Plan:
  - Choose initial $\tau = O(\log n)$, $0 < \varepsilon \ll 1$.
  1. $\hat{\mathcal{L}} \leftarrow A(\mathcal{L}^*, \varepsilon n, \tau - 1)$
  2. $\mathcal{L}' := \mathcal{L} \cap (\hat{\mathcal{L}})^\perp$ // $\text{rank}(\mathcal{L}') = (1-\varepsilon)n$
  3. Output $A(\mathcal{L}', \ell, \tau)$

What if $\text{rank}(\mathcal{L}') = (1-\varepsilon)n < \ell$?

Can't find a larger-rank sublattice!

Take Two: $\ell > 1$ (DSP $\Rightarrow$ DSP)

- Plan:
  - Choose initial $\tau = O(\log n)$, $0 < \varepsilon \ll 1$.

0. If $\ell > n/2$,
   output $\mathcal{L} \cap (A(\mathcal{L}^*, n-\ell, \tau))^\perp$.

1. $\hat{\mathcal{L}} \leftarrow A(\mathcal{L}^*, \lceil \varepsilon n \rceil, \tau - 1)$
2. $\mathcal{L}' := \mathcal{L} \cap (\hat{\mathcal{L}})^\perp$ // $\text{rank}(\mathcal{L}') = (1-\varepsilon)n$
3. Output $A(\mathcal{L}', \ell, \tau)$

- Base cases:
  - if $\tau = 0$, output $LLL(\mathcal{L}, \ell)$.
  - if $\text{rank}(\mathcal{L}) = \kappa$, output $DSP(\mathcal{L}, \ell)$.

Analysis

- C = poly(n) oracle calls!

Analysis

- C = poly(n) oracle calls!
- Recurrence becomes

$$\gamma(n, \ell, \tau) \leq \gamma((1-\varepsilon)n, \ell, \tau) \cdot \gamma(n, \varepsilon n, \tau)^{\frac{\ell}{(1-\varepsilon)n}}$$

Analysis

- C = poly(n) oracle calls!
- Recurrence becomes

$$\gamma(n, \ell, \tau) \leq \gamma((1-\varepsilon)n, \ell, \tau) \cdot \gamma(n, \varepsilon n, \tau)^{\frac{\ell}{(1-\varepsilon)n}}$$

$$\gamma(n, \ell, 0) = 2^{n\ell}$$

$$\gamma(K, \ell, \tau) = \sqrt{\delta_{K,\ell}} = K^{\Theta\left(\frac{\ell(K-\ell)}{2(K-1)}\right)}$$

Analysis

- C = poly(n) oracle calls!
- Recurrence becomes

$$\gamma(n, \ell, \tau) \le \gamma((1-\varepsilon)n, \ell, \tau) \cdot \gamma(n, \varepsilon n, \tau)^{\frac{\ell}{(1-\varepsilon)n}}$$

$$\gamma(n, \ell, 0) = 2^{n\ell}$$

$$\gamma(K, \ell, \tau) = \sqrt{\delta_{K,\ell}} = K^{\Theta\left(\frac{\ell(K-\ell)}{2(K-1)}\right)}$$

- Can check

$$\gamma(n, \ell, \tau) \le K^{O\left(\frac{\ell(n-\ell)}{2(K-1)}\right)} \cdot \exp\left(O\left(n^2 \ell(n-\ell)/2^{\tau}\right)\right)$$

Analysis

- C = poly(n) oracle calls!
- Recurrence becomes

$$\gamma(n, \ell, \tau) \leq \gamma((1-\varepsilon)n, \ell, \tau) \cdot \gamma(n, \varepsilon n, \tau)^{\frac{\ell}{(1-\varepsilon)n}}$$

$$\gamma(n, \ell, 0) = 2^{n\ell}$$

$$\gamma(K, \ell, \tau) = \sqrt{\delta_{K,\ell}} = K^{\Theta\left(\frac{\ell(K-\ell)}{2(K-1)}\right)}$$

- Can check $\gamma(n, \ell, \tau) \leq K^{O\left(\frac{\ell(n-\ell)}{2(K-1)}\right)} \cdot \exp\left(O\left(n^2 \ell(n-\ell)/2^\tau\right)\right)$

(To handle the duality step, note that the guess is symmetric under $\ell \mapsto (n-\ell)$.)

Analysis

- C = poly(n) oracle calls!
- Recurrence becomes

$$\gamma(n, \ell, \tau) \leq \gamma((1-\varepsilon)n, \ell, \tau) \cdot \gamma(n, \varepsilon n, \tau)^{\frac{\ell}{(1-\varepsilon)n}}$$

$$\gamma(n, \ell, 0) = 2^{n\ell}$$

$$\gamma(K, \ell, \tau) = \sqrt{\delta_{K,\ell}} = K^{\Theta\left(\frac{\ell(K-\ell)}{2(K-1)}\right)}$$

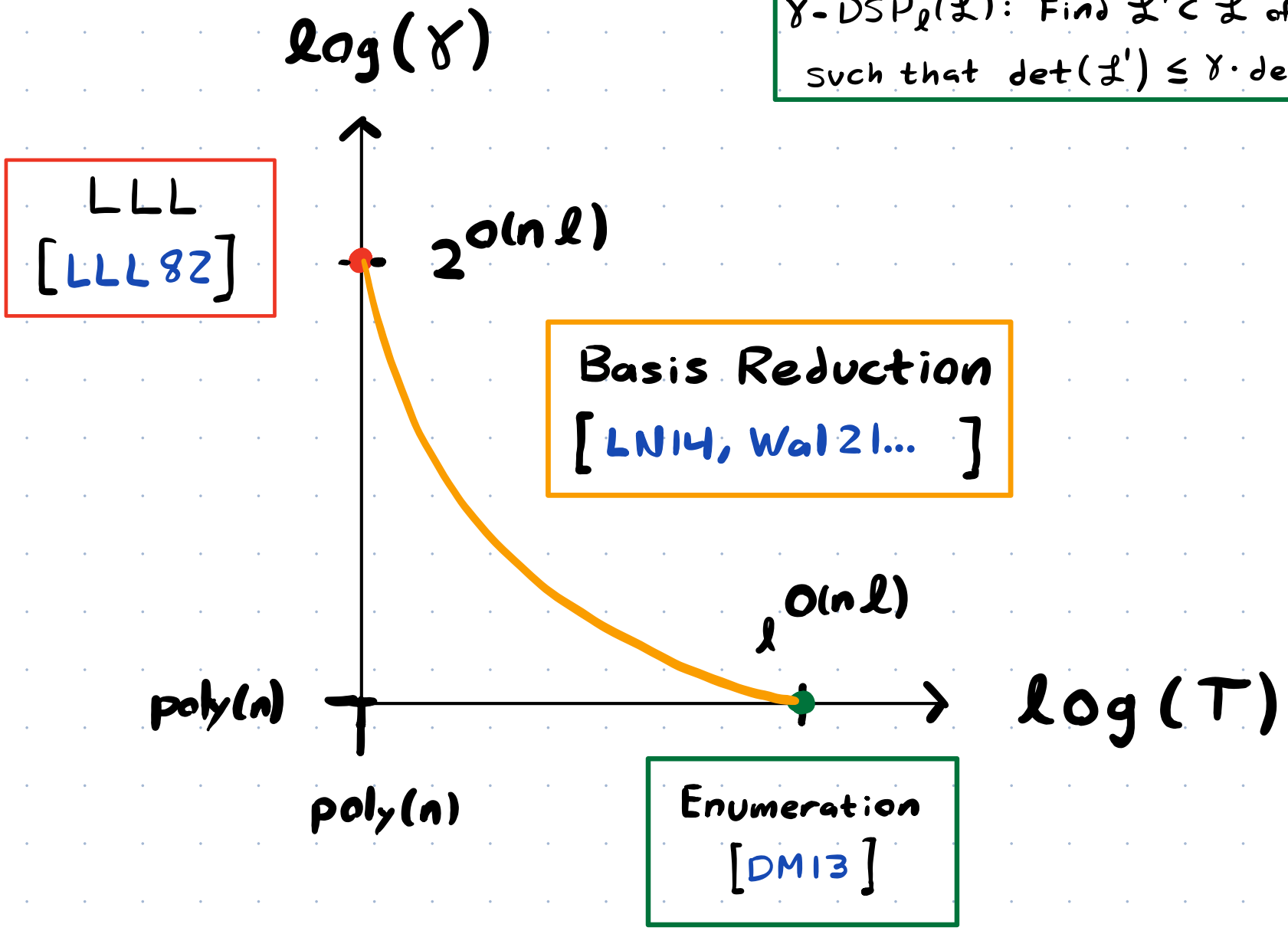
- Can check $$\gamma(n, \ell, \tau) \leq K^{O\left(\frac{\ell(n-\ell)}{2(K-1)}\right)} \cdot \exp\left(O\left(n^2 \ell(n-\ell)/2^\tau\right)\right)$$

(To handle the duality step, note that the guess is symmetric under $\ell \mapsto (n-\ell)$.)

$$\gamma = K^{O\left(\frac{\ell(n-\ell)}{2(K-1)}\right)}$$

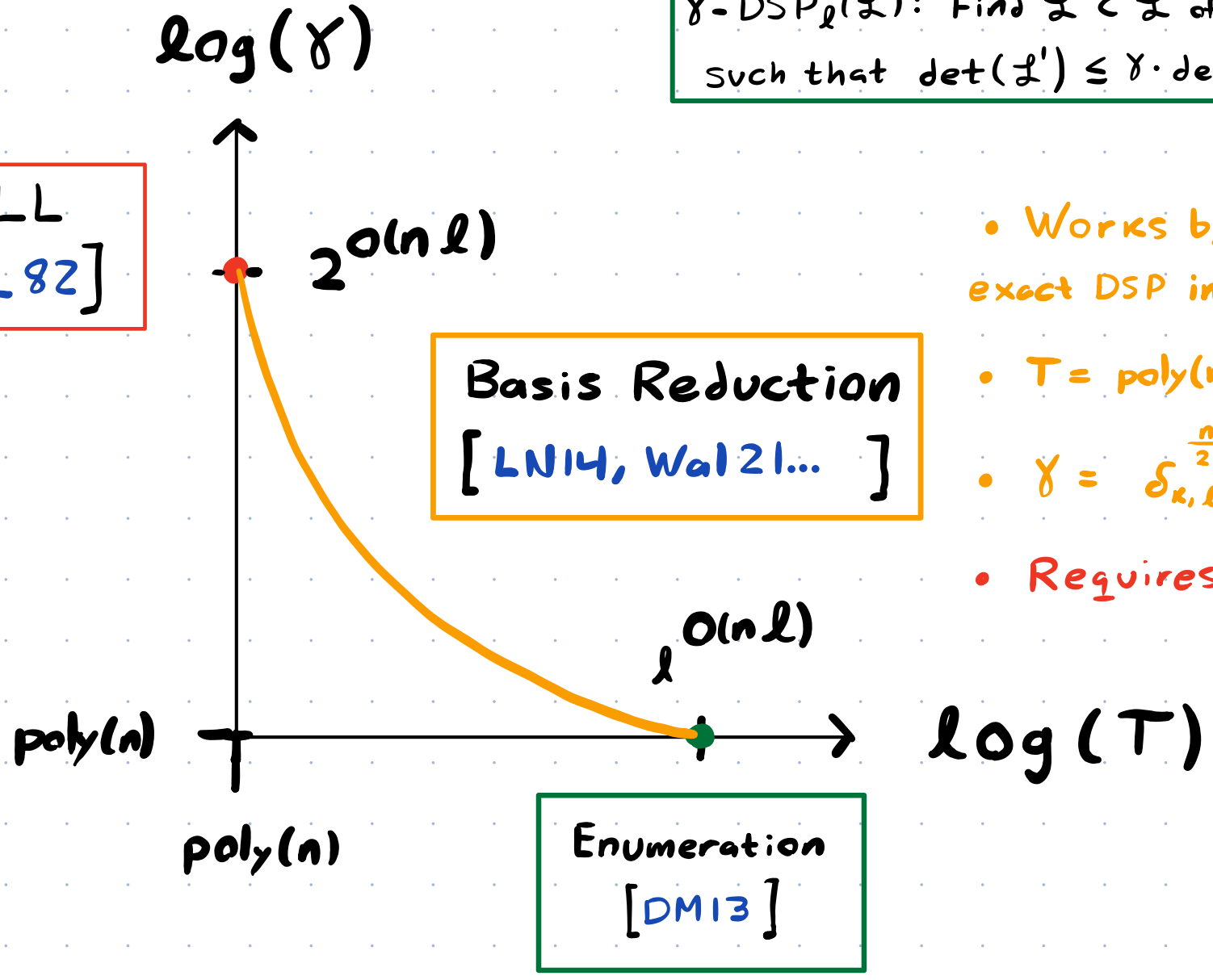
Time / γ Tradeoffs for γ-DSP$_\ell$

γ-DSP$_\ell(\mathcal{L})$: Find $\mathcal{L}' \subset \mathcal{L}$ of rank ℓ such that $\det(\mathcal{L}') \le \gamma \cdot \det(\mathcal{L})^{\ell/n}$.



Time / γ Tradeoffs for γ-DSP$_\ell$

γ-DSP$_\ell(\mathcal{L})$: Find $\mathcal{L}' \subset \mathcal{L}$ of rank ℓ such that $\det(\mathcal{L}') \le \gamma \cdot \det(\mathcal{L})^{\ell/n}$.



- Works by solving exact DSP in dimension κ
- $T = \text{poly}(n)\, \ell^{O(\kappa \ell)}$
- $\gamma = \delta_{\kappa,\ell}^{\frac{n-\ell}{2(\kappa-\ell)}} = \kappa^{\Theta\left(\frac{\ell(n-\ell)}{(\kappa-1)}\right)}$.
- Requires $\ell \le \kappa$.

Analysis

- C = poly(n) oracle calls!
- Recovers basis reduction, even for $\ell > k$!

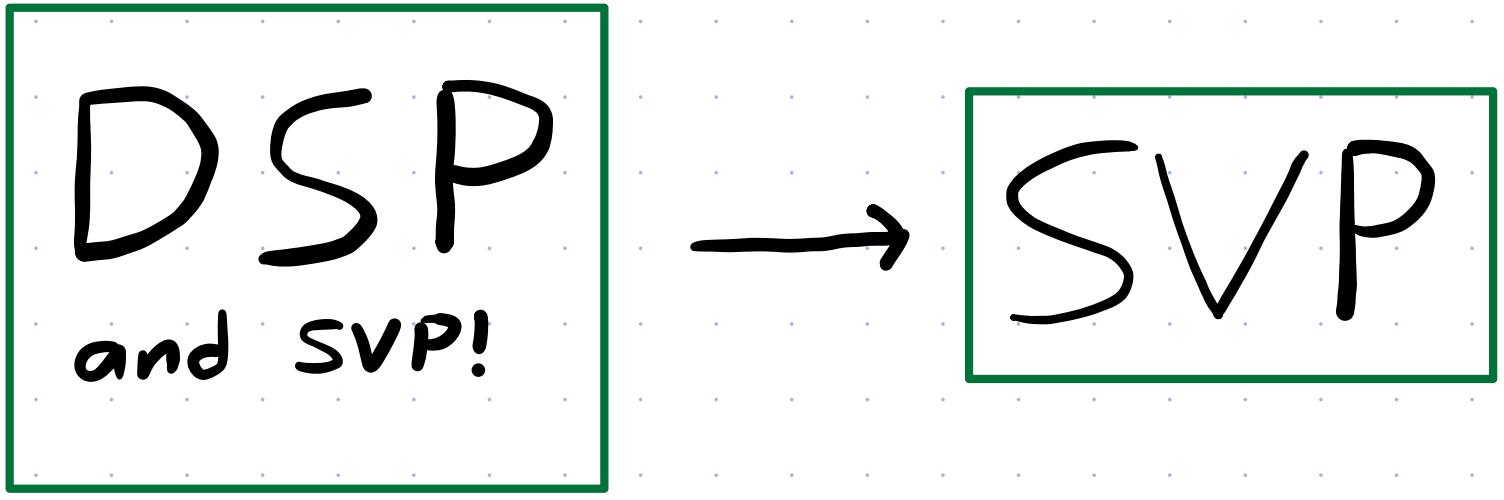
$$\gamma = (1 + o(1))\, K^{\frac{\ell(n-\ell)}{2(k-1)}}$$

Analysis

- $C = \text{poly}(n)$ oracle calls!
- Recovers basis reduction, even for $\ell > k$!

$$\gamma = (1 + o(1))\, k^{\frac{\ell(n-\ell)}{2(k-1)}}$$

- DSP oracle calls are expensive.


DSP
and SVP!
SVP

Challenges

- The big challenge: make sure that

$$n = k \Rightarrow \ell = 1 \quad (\text{or } \ell = n - 1)$$

Challenges

- The big challenge: make sure that

$$n = \kappa \Rightarrow \ell = 1 \quad (\text{or } \ell = n - 1)$$

- Solution idea: maintain the invariant that

$$\hat{\ell} := \min\{\ell, n - \ell\} \leq n - \kappa + 1$$

  - Squeeze ℓ to the extremes!

Challenges

- The big challenge: make sure that

$$n = \kappa \Rightarrow \ell = 1 \quad (\text{or } \ell = n-1)$$

- Solution idea: maintain the invariant that

$$\hat{\ell} := \min\{\ell, n-\ell\} \leq n - \kappa + 1$$

  - Squeeze ℓ to the extremes!

- Problem: Recurrence not favorable when ℓ is large.

Challenges

- The big challenge: make sure that

$$n = \kappa \Rightarrow \ell = 1 \quad (\text{or } \ell = n-1)$$

- Solution idea: maintain the invariant that

$$\hat{\ell} := \min\{\ell, n-\ell\} \leq n - \kappa + 1$$

  - Squeeze ℓ to the extremes!

- Problem: Recurrence not favorable when ℓ is large.

- Solution idea: When ℓ is large, be patient:
  don't reduce the depth parameter τ.

The Reduction

Start with $\ell \le n - \kappa + 1$.

- Duality: if $\max\{1, \frac{(n-\kappa)}{5}\} < \ell < \frac{n}{2}$

  OR $\ell \ge n - \max\{1, \frac{(n-\kappa)}{10}\}$:

  output $\mathcal{L} \cap A(\mathcal{L}^*, n-\ell, \tau)^\perp$.

- Recursive step:

  $\hat{\mathcal{L}} \leftarrow A(\mathcal{L}^*, \lceil \frac{(n-\kappa)}{20} \rceil, \tau - b)$

  Output $A(\mathcal{L} \cap (\hat{\mathcal{L}})^\perp, \ell, \tau)$.

  $b = \begin{cases} 1, & \ell < \frac{n}{2} \\ 0, & \ell \ge \frac{n}{2} \end{cases}$

- Base cases:

  if $\tau = 0$, output $\mathrm{LLL}(\mathcal{L}, \ell)$.

  if $\mathrm{rank}(\mathcal{L}) = \kappa$ AND $\ell = 1$, return $\mathrm{SVP}(\mathcal{L})$.

Analysis: Key Lemmas

Lemma 1. All recursive calls satisfy $\min\{\ell, n-\ell\} \le n-\kappa+1$.

All can be verified directly from local checks!

↳ Algorithm does not get "stuck"!

Lemma 2. The potential $\Phi(n,\tau) := \tau + 20\log(n-\kappa+1)$ drops by at least 1 from parent to grandchild.

↳ poly(n) runtime (oracle calls).

Lemma 3. The guess $f(n,\ell,\tau) := \kappa^{\frac{\ell(n-\ell)}{2(\kappa-1)}} \cdot \exp(n^3/2^\tau)$ satisfies the recurrence induced by Λ.

↳ Achieve basis reduction tradeoff $\kappa^{\frac{\ell(n-\ell)}{2(\kappa-1)}}$.

Lattice Representations and Concrete Runtime

- We've described our reductions as operating on abstract lattices.
- To bound concrete running time we must specify a representation.
  - How is $\mathcal{L}$ represented in bits?
  - How are duality $\mathcal{L} \mapsto \mathcal{L}^*$ and intersection $(\mathcal{L}, M) \mapsto \mathcal{L} \cap M^\perp$ computed?
- This matters as repeated duality and intersection steps may blow up the representation size.

Lattice Representations and Concrete Runtime

- We present two possible representations.
- Using **LLL-reduced bases** we can show that the representation size stays bounded by $n^{O(\log n)}$.
- However, this is likely tight.
- To achieve polynomial size (and thus polynomial-time reductions) we devise an *approximate* representation.
- Specifically, we show how to "round" any lattice (basis) to fixed poly(n) bit length, such that dense sublattices in the rounded lattice correspond to equally* dense sublattices of the original.

Computer-Aided Search

- Our DSP → SVP involved tricky parameter choices.

  Why not let the computer do it?

Computer-Aided Search

- Our DSP → SVP involved tricky parameter choices.

  Why not let the computer do it?

Duality: if CONDITION(n, ℓ, τ), output $\mathcal{L} \cap A(\mathcal{L}^*, n-\ell, c)^\perp$

Recursive step: $\hat{\mathcal{L}} \leftarrow A(\mathcal{L}^*, \ell^*, c^*)$

Output $A(\mathcal{L} \cap (\hat{\mathcal{L}})^\perp, \ell, c-c^*)$.

Base cases: $\tau = 0$, output $\mathrm{LLL}(\mathcal{L}, 1)$; if $n = \kappa$ AND $\ell = 1$, output $\mathrm{SVP}(\mathcal{L})$.

Computer-Aided Search

- Our DSP → SVP involved tricky parameter choices.

  Why not let the computer do it?

Duality: if CONDITION(n, ℓ, τ), output $\mathcal{L} \cap A(\mathcal{L}^*, n-\ell, c)^\perp$

Recursive step: $\hat{\mathcal{L}} \leftarrow A(\mathcal{L}^*, \ell^*, c^*)$

Output $A(\mathcal{L} \cap (\hat{\mathcal{L}})^\perp, \ell, c-c^*)$.

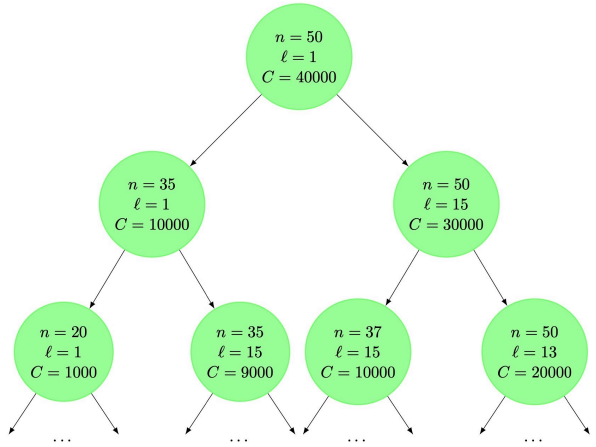
Base cases: $\tau = 0$, output $\mathrm{LLL}(\mathcal{L}, 1)$; if $n = \kappa$ AND $\ell = 1$, output $\mathrm{SVP}(\mathcal{L})$.

- Using dynamic programming, solve

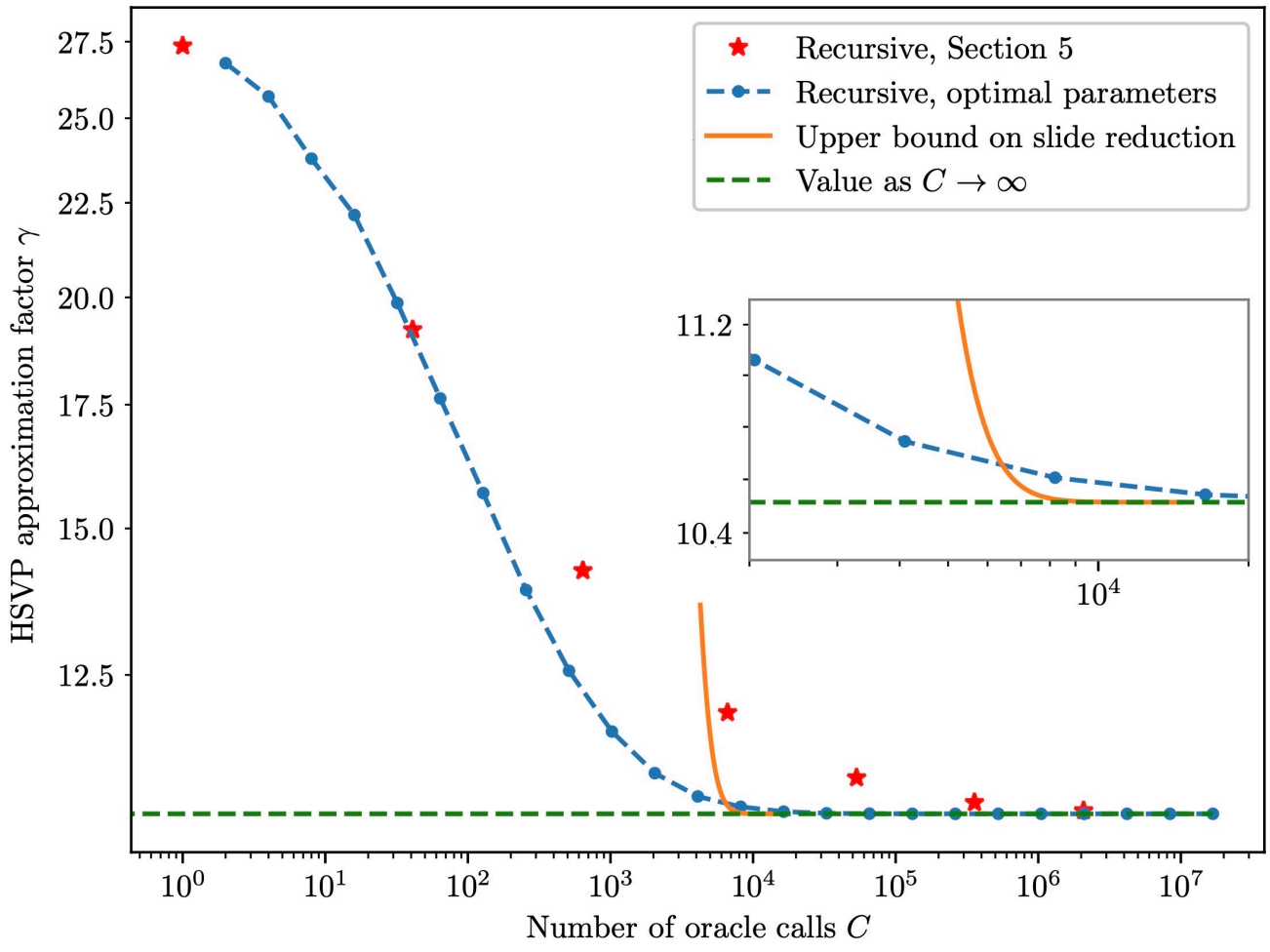
$$\gamma(n, \ell, C) := \min \left\{ \gamma(n, n-\ell, C), \min_{1 \le \ell^* \le n-\kappa} \min_{c^* \le C} \gamma(n-\ell^*, \ell, C-c^*)\, \gamma(n, \ell^*, c^*)^{\frac{\ell}{n-\ell^*}} \right\}$$

Results

- **Optimal DP solution bounds**
  rather massively improve on
  DSP → SVP guarantee.

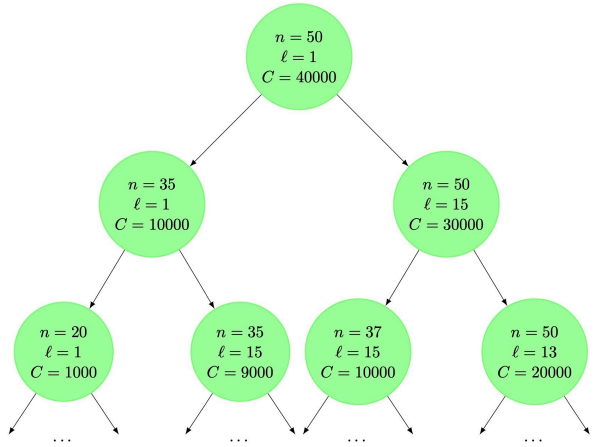


$n = 50,\ \kappa = 10$



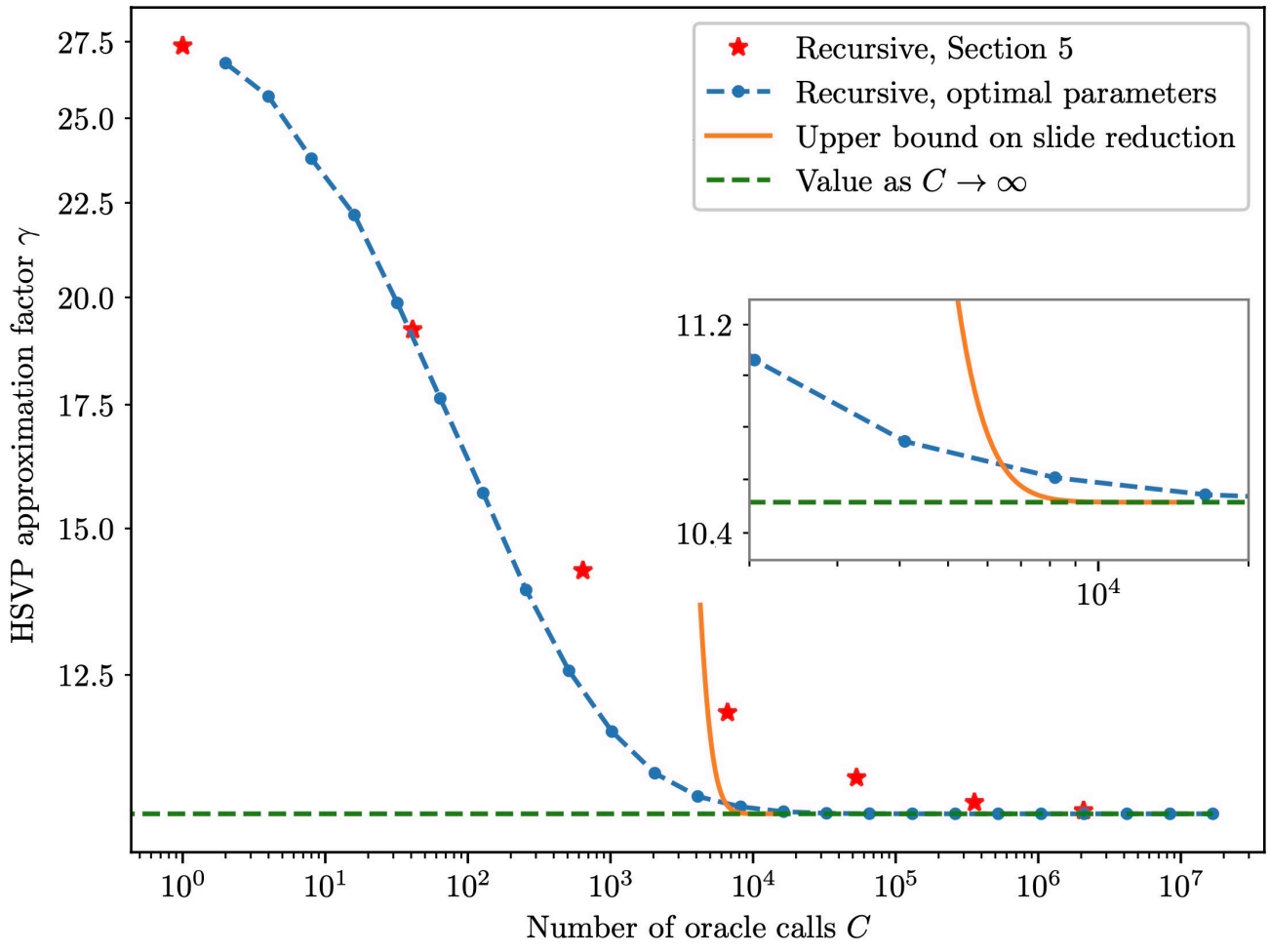
Results

- **Optimal DP solution bounds** rather massively improve on **DSP → SVP guarantee.**



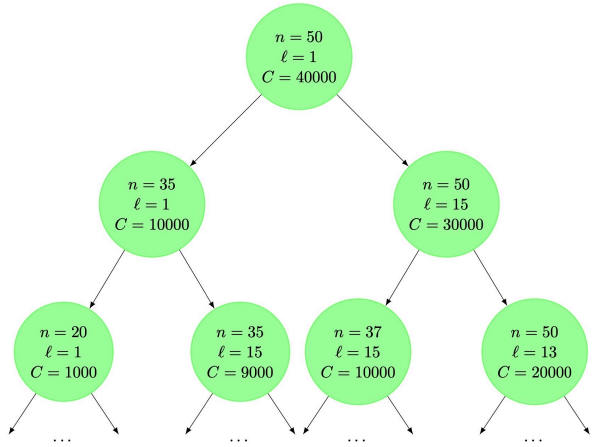
- **Comparable to provable bounds on slide reduction.**

$n = 50,\ \kappa = 10$



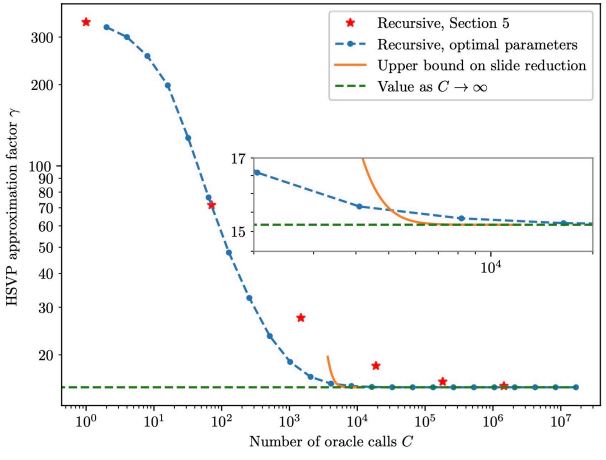
Results

- **Optimal DP solution bounds** rather massively improve on **DSP → SVP guarantee.**

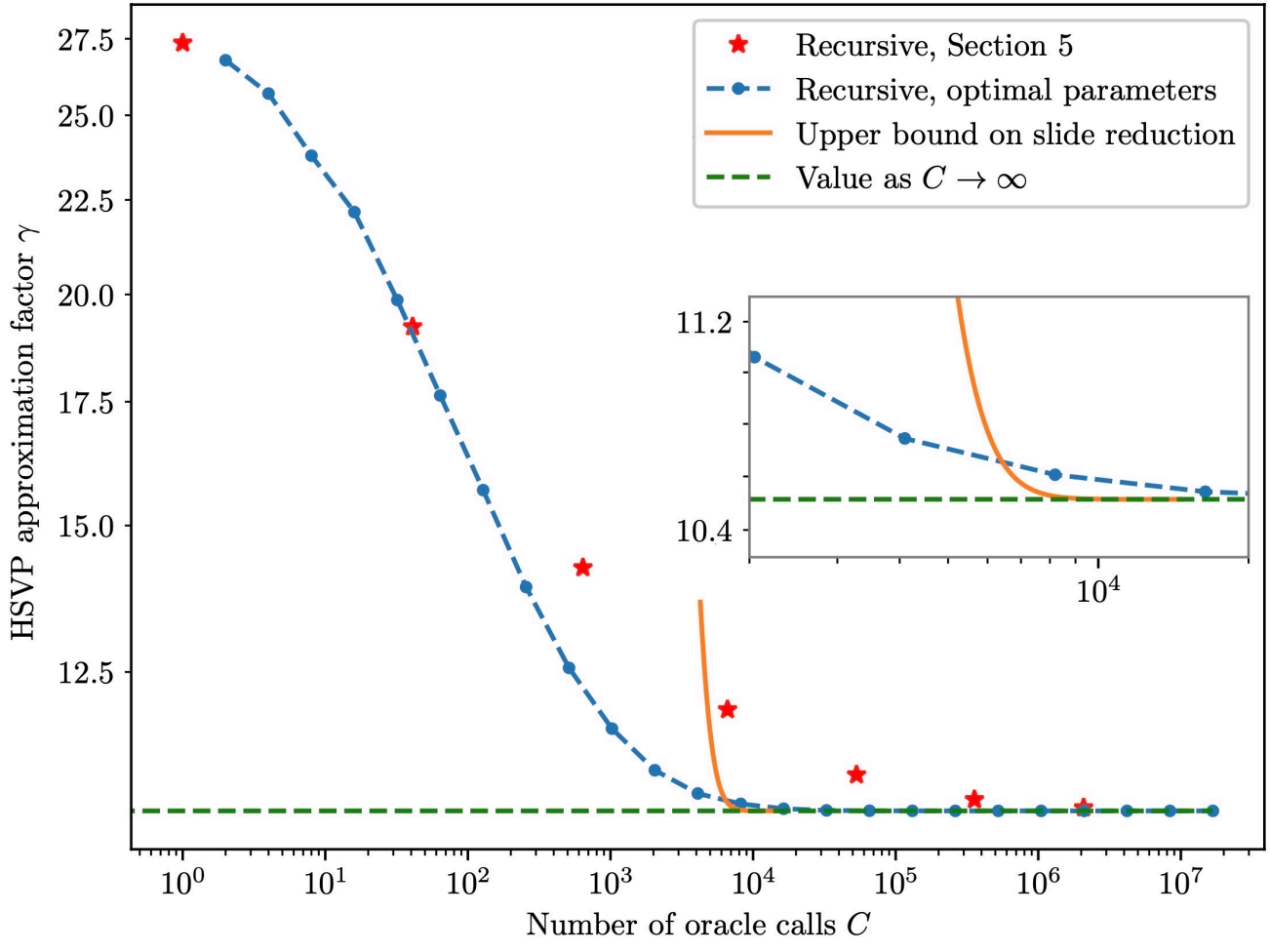


- **Comparable to provable bounds on slide reduction.**

$n = 100$, $\kappa = 30$



$n = 50$, $\kappa = 10$



Mixing and Matching Oracles

- Rough estimate: solving SVP in dimension n takes time 2^n.

> Optional Base Case: For all $T \geq 2^n$,
>
> $$\gamma(n, 1, T) = \sqrt{n}.$$

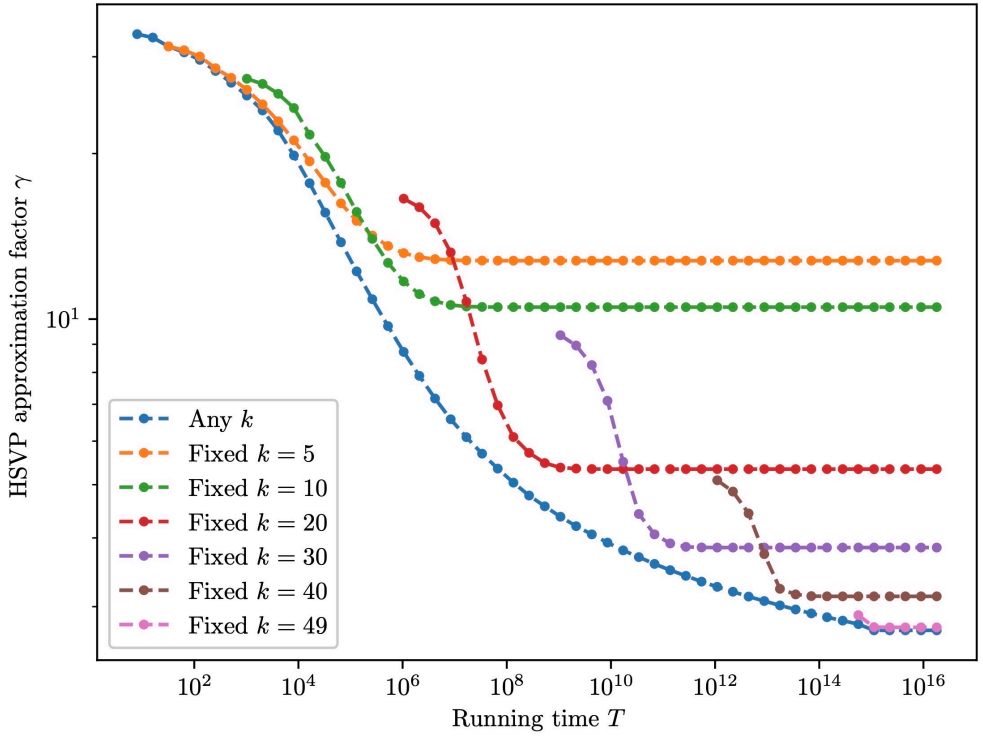
Mixing and Matching Oracles

- Rough estimate: solving SVP in dimension n takes time 2^n.

Optional Base Case: For all $T \geq 2^n$,

$$\gamma(n, 1, T) = \sqrt{n}.$$

$n = 50$, $\kappa = 10$



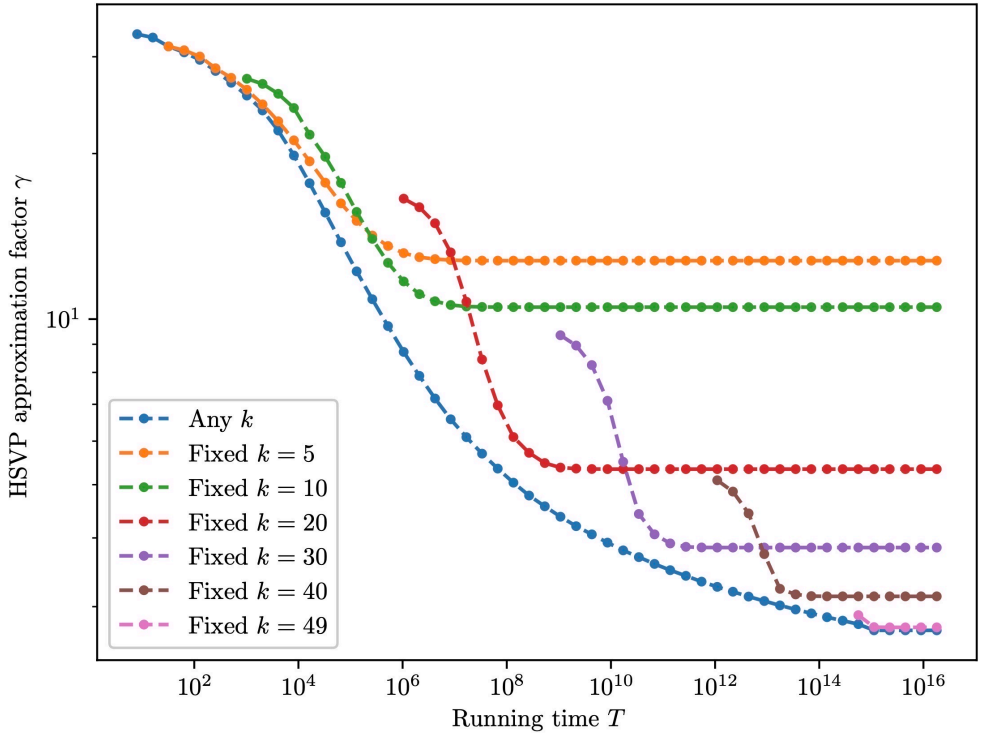
Mixing and Matching Oracles

- Rough estimate: solving SVP in dimension n takes time 2^n.

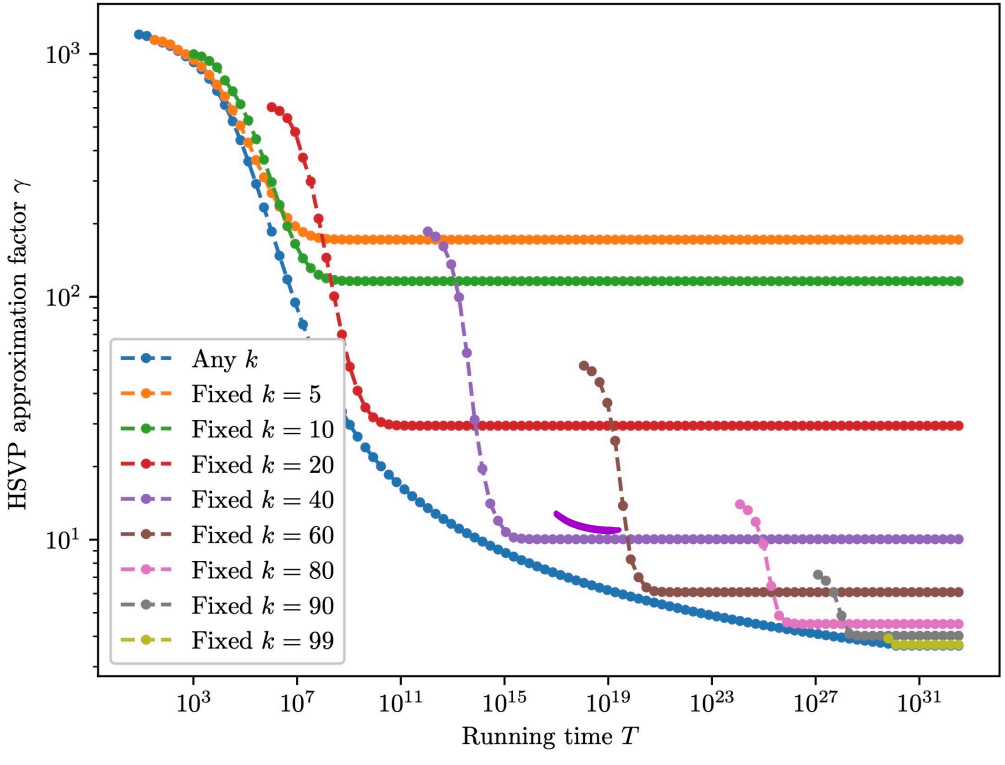
Optional Base Case: For all $T \geq 2^n$,

$$\gamma(n, 1, T) = \sqrt{n}.$$

$n = 50,\ k = 10$



$n = 100,\ k = 30$



Future Directions

- Explore the design space
  - Tuning parameters to exploit structure
  - Trees of higher arity?

Future Directions

- Explore the design space
  - Tuning parameters to exploit structure
  - Trees of higher arity?
- Basis Reduction and Recursive Lattice Reduction
  - Is there a formal relationship?
  - Can recursive lattice reduction capture LLL?
  - Mix and match?

Future Directions

- Explore the design space
  - Tuning parameters to exploit structure
  - Trees of higher arity?
- Basis Reduction and Recursive Lattice Reduction
  - Is there a formal relationship?
  - Can recursive lattice reduction capture LLL?
  - Mix and match?
- Practical behavior: Implementation and heuristic analysis

Thanks for listening!