Lattices that Admit Logarithmic Worst-Case to Average-Case Connection Factors

Chris Peikert[1] Alon Rosen[2]

[1]SRI International

[2]Harvard SEAS → IDC Herzliya

STOC 2007

Worst-case versus average-case complexity

Lattices are an intriguing case study:

- Believed hard in the worst case
- Worst-case / average-case reductions

Worst-case versus average-case complexity

Lattices are an intriguing case study:

- Believed hard in the worst case
- Worst-case / average-case reductions

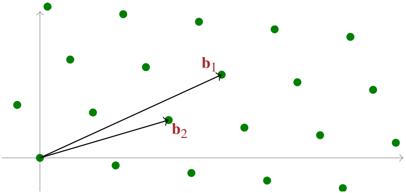
This Talk...

- Not (exactly) about crypto
- Special, natural class of algebraic lattices
- Very tight worst-case/average-case reductions
  - Much tighter than known for general lattices
- Distinctions between decision and search
- Many open problems

Lattices

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.
The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

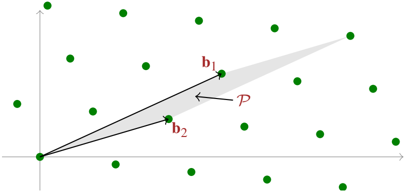
$$\mathcal{L} \quad = \quad \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Lattices

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.
The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} \quad = \quad \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$

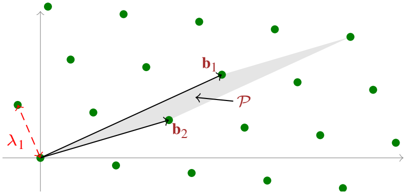


Fundamental region: Parallelepiped $\mathcal{P}$ spanned by $\mathbf{b}_i$s.

Lattices

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.
The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} \quad = \quad \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



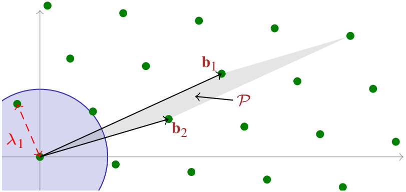
Fundamental region: Parallelepiped $\mathcal{P}$ spanned by $\mathbf{b}_i$s.

Minimum distance: λ_1 = length of shortest nonzero $\mathbf{v} \in \mathcal{L}$.

Lattices

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.
The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} \quad = \quad \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Fundamental region: Parallelepiped $\mathcal{P}$ spanned by $\mathbf{b}_i$s.

Minimum distance: λ_1 = length of shortest nonzero $\mathbf{v} \in \mathcal{L}$.

Minkowski's Theorem

$$\lambda_1 \quad \leq \quad \sqrt{n} \cdot \mathrm{vol}(\mathcal{P})^{1/n}$$

(Non-constructive, non-algorithmic proof. . .)

Shortest Vector Problem (SVP)

Approximation factor $\gamma = \gamma(n)$.

Decision: Given basis, distinguish $\lambda_1 \leq 1$ from $\lambda_1 > \gamma$.

Shortest Vector Problem (SVP)

Approximation factor $\gamma = \gamma(n)$.

Decision: Given basis, distinguish $\lambda_1 \leq 1$ from $\lambda_1 > \gamma$.

Search: Given basis, find nonzero $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1$.

Shortest Vector Problem (SVP)

Approximation factor $\gamma = \gamma(n)$.

Decision: Given basis, distinguish $\lambda_1 \leq 1$ from $\lambda_1 > \gamma$.

Search: Given basis, find nonzero $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1$.

Hardness

- Almost-polynomial factors $\gamma(n)$ [Ajt,Mic,Kho,HaRe]

Shortest Vector Problem (SVP)

Approximation factor $\gamma = \gamma(n)$.

Decision: Given basis, distinguish $\lambda_1 \leq 1$ from $\lambda_1 > \gamma$.

Search: Given basis, find nonzero $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1$.

Hardness

- Almost-polynomial factors $\gamma(n)$ [Ajt,Mic,Kho,HaRe]

Algorithms for SVP$_\gamma$

- $\gamma(n) \sim 2^n$ approximation in poly-time [LLL]
- Can trade-off running time/approximation [Sch,AKS]

Worst-Case/Average-Case Connections [Ajtai,...]

For some $\gamma(n) = \mathrm{poly}(n)$ ("connection factor"):

SVP$_\gamma$ hard in the worst case

$\Downarrow$

problems hard on the average

Worst-Case/Average-Case Connections [Ajtai,...]

For some $\gamma(n) = \mathrm{poly}(n)$ ("connection factor"):

SVP$_\gamma$ hard in the worst case

$\Downarrow$

problems hard on the average

Cryptographic Applications

- One-way & collision-resistant functions [Ajtai,GGH,...]
- Public-key encryption [AjtaiDwork,Regev]

Worst-Case/Average-Case Connections [Ajtai,...]

For some $\gamma(n) = \text{poly}(n)$ ("connection factor"):

SVP$_\gamma$ hard in the worst case

$\Downarrow$

problems hard on the average

Cryptographic Applications

- One-way & collision-resistant functions [Ajtai,GGH,...]
- Public-key encryption [AjtaiDwork,Regev]

Optimizing the Connection Factor γ

- Interesting to characterize complexity
- Important for crypto due to time/accuracy tradeoff
- Current best $\gamma(n) \sim n$ [MicciancioRegev]

This Work: Ideal Lattices

- Ideal lattices: special class from algebraic number theory.
  Ideals in the ring of integers of a number field.

This Work: Ideal Lattices

- Ideal lattices: special class from algebraic number theory.
  Ideals in the ring of integers of a number field.
- Our interest: number fields with small root discriminant.

This Work: Ideal Lattices

- Ideal lattices: special class from algebraic number theory.
  Ideals in the ring of integers of a number field.
- Our interest: number fields with small root discriminant.

SVP on Ideal Lattices

- Well-known bottleneck in number theory algorithms:

  Ideal reduction, unit & class group computation, ...

This Work: Ideal Lattices

- Ideal lattices: special class from algebraic number theory.
  Ideals in the ring of integers of a number field.
- Our interest: number fields with small root discriminant.

SVP on Ideal Lattices

- Well-known bottleneck in number theory algorithms:
  Ideal reduction, unit & class group computation, . . .
- Decision-SVP is *easy* to approximate: $\lambda_1 \approx$ Minkowski bound.
  Not NP-hard!

This Work: Ideal Lattices

- Ideal lattices: special class from algebraic number theory.
  Ideals in the ring of integers of a number field.
- Our interest: number fields with small root discriminant.

SVP on Ideal Lattices

- Well-known bottleneck in number theory algorithms:
  Ideal reduction, unit & class group computation, …
- Decision-SVP is *easy* to approximate: $\lambda_1 \approx$ Minkowski bound.
  Not NP-hard!
- Search-SVP appears hard, despite structure.
  Best known algorithms [LLL,Sch,AKS].

Our Results

Complexity of Ideal Lattices

1. Connection factors as low as $\gamma = \sqrt{\log n}$.
   - Based on search-SVP. (Decision is *easy*.)
   - For SVP in any ℓ_p norm. (Stay for CCC.)

   Classic *win-win* situation.
2. Relations among problems on ideal lattices (SVP, CVP).

Our Results

Complexity of Ideal Lattices

1. Connection factors as low as $\gamma = \sqrt{\log n}$.
   - Based on search-SVP. (Decision is *easy*.)
   - For SVP in any ℓ_p norm. (Stay for CCC.)

   Classic *win-win* situation.
2. Relations among problems on ideal lattices (SVP, CVP).

Subtleties

No *efficient* constructions of best number fields (yet).

⇒ Non-uniformity (preprocessing) in reductions.

⇒ Crypto is tricky.

⇒ Many interesting open problems!

Other Special Classes of Lattices

1. **"Unique" shortest vector:**
   - One-way/CR functions [Ajtai,GGH]
   - Public-key encryption [AjtaiDwork,Regev]

Other Special Classes of Lattices

1. **“Unique” shortest vector:**
   - One-way/CR functions [Ajtai,GGH]
   - Public-key encryption [AjtaiDwork,Regev]
2. **Cyclic lattices:**
   - Efficient & compact OWFs [Micciancio]
   - Collision-resistant hashing [PeikertRosen,LyubashevskyMicciancio]

Other Special Classes of Lattices

1. **"Unique" shortest vector:**
   - One-way/CR functions [Ajtai,GGH]
   - Public-key encryption [AjtaiDwork,Regev]
2. **Cyclic lattices:**
   - Efficient & compact OWFs [Micciancio]
   - Collision-resistant hashing [PeikertRosen,LyubashevskyMicciancio]

Structure used for functionality & efficiency.

Connection factors $\gamma \sim n$ or more.

Worst-to-Average Reduction [Ajtai,...]

Average-Case Problem

For uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow \mathbb{Z}^n \bmod q$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$:

$$\sum z_i \mathbf{a}_i = \mathbf{0} \bmod q.$$

Worst-to-Average Reduction [Ajtai,...]

Average-Case Problem

For uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow \mathbb{Z}^n \bmod q$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$:

$$\sum z_i \mathbf{a}_i = \mathbf{0} \bmod q.$$

Reduction

1. Sample offset vectors $\nearrow_i \in \mathbb{R}^n$, derive uniform $\mathbf{a}_i$'s
2. Get short solution $\mathbf{z} \in \mathbb{Z}^m$
3. Output $(\sum z_i \cdot \nearrow_i) \in \mathcal{L}$

Worst-to-Average Reduction [Ajtai,…]

Average-Case Problem

For uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow \mathbb{Z}^n \bmod q$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$:

$$\sum z_i \mathbf{a}_i = \mathbf{0} \bmod q.$$

Reduction

1. Sample offset vectors $\nearrow_i \in \mathbb{R}^n$, derive uniform $\mathbf{a}_i$'s
2. Get short solution $\mathbf{z} \in \mathbb{Z}^m$
3. Output $(\sum z_i \cdot \nearrow_i) \in \mathcal{L}$

Worst-to-Average Reduction [Ajtai,...]

Average-Case Problem

For uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow \mathbb{Z}^n \bmod q$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$:

$$\sum z_i \mathbf{a}_i = \mathbf{0} \bmod q.$$

Reduction

1. Sample offset vectors $\nearrow_i \in \mathbb{R}^n$, derive uniform $\mathbf{a}_i$'s
2. Get short solution $\mathbf{z} \in \mathbb{Z}^m$
3. Output $(\sum z_i \cdot \nearrow_i) \in \mathcal{L}$

Worst-to-Average Reduction [Ajtai,...]

Average-Case Problem

For uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow \mathbb{Z}^n \bmod q$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$:

$$\sum z_i \mathbf{a}_i = \mathbf{0} \bmod q.$$

Reduction

1. Sample offset vectors $\nearrow_i \in \mathbb{R}^n$, derive uniform $\mathbf{a}_i$'s
2. Get short solution $\mathbf{z} \in \mathbb{Z}^m$
3. Output $(\sum z_i \cdot \nearrow_i) \in \mathcal{L}$

Worst-to-Average Reduction [Ajtai,...]

Average-Case Problem

For uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow \mathbb{Z}^n \bmod q$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$:

$$\sum z_i \mathbf{a}_i = \mathbf{0} \bmod q.$$

Reduction

1. Sample offset vectors $\nearrow_i \in \mathbb{R}^n$, derive uniform $\mathbf{a}_i$'s
2. Get short solution $\mathbf{z} \in \mathbb{Z}^m$
3. Output $(\sum z_i \cdot \nearrow_i) \in \mathcal{L}$

Connection Factor

- Size of solution $\mathbf{z} \in \mathbb{Z}^m$
- Lengths of offset vectors $\nearrow_i$

Our Approach

- Replace "1-dim" integers $\mathbb{Z}$ with "n-dim integers" $\mathcal{O}_K$.

  $\mathcal{O}_K =$ ring of algebraic integers in number field K of degree n.

Our Approach

- Replace "1-dim" integers $\mathbb{Z}$ with "n-dim integers" $\mathcal{O}_K$.

  $\mathcal{O}_K =$ ring of algebraic integers in number field K of degree n.

  - Has $+$ and $\times$, "absolute value" $|\cdot|$, $\ldots$

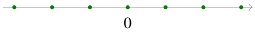
Our Approach

- Replace "1-dim" integers $\mathbb{Z}$ with "n-dim integers" $\mathcal{O}_K$.

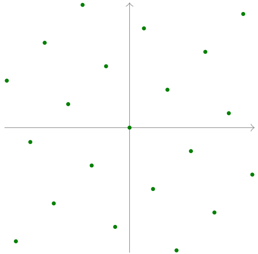
  $\mathcal{O}_K =$ ring of algebraic integers in number field K of degree n.

  - Has $+$ and $\times$, "absolute value" $|\cdot|$, ...
  - Is an n-dim lattice under K's canonical embedding.

$\mathbb{Z}$



$\mathcal{O}_K$



Our Approach

- Replace "1-dim" integers $\mathbb{Z}$ with "n-dim integers" $\mathcal{O}_K$.

  $\mathcal{O}_K =$ ring of algebraic integers in number field K of degree n.

  - Has $+$ and $\times$, "absolute value" $|\cdot|$, ...
  - Is an n-dim lattice under K's canonical embedding.

	Before	**After**
Worst-case object	*lattice* in $\mathbb{R}^n$: $\sum(\mathbb{Z} \cdot \mathbf{b}_i)$ for $\mathbf{b}_i \in \mathbb{R}^n$	*ideal* in $\mathcal{O}_K$: $\sum(\mathcal{O}_K \cdot b_i)$ for $b_i \in \mathcal{O}_K$

Our Approach

- Replace "1-dim" integers $\mathbb{Z}$ with "n-dim integers" $\mathcal{O}_K$.

  $\mathcal{O}_K =$ ring of algebraic integers in number field K of degree n.

  - Has $+$ and $\times$, "absolute value" $|\cdot|$, ...
  - Is an n-dim lattice under K's canonical embedding.

	Before	**After**
Worst-case object	*lattice* in $\mathbb{R}^n$: $\sum(\mathbb{Z} \cdot \mathbf{b}_i)$ for $\mathbf{b}_i \in \mathbb{R}^n$	*ideal* in $\mathcal{O}_K$: $\sum(\mathcal{O}_K \cdot b_i)$ for $b_i \in \mathcal{O}_K$
Avg-case problem	for $\mathbf{a}_i \leftarrow \mathbb{Z}^n \bmod q$ find small $z_i \in \mathbb{Z}$: $\sum z_i \mathbf{a}_i = 0 \bmod q$	for $a_i \leftarrow \mathcal{O}_K \bmod q$ find "small" $z_i \in \mathcal{O}_K$: $\sum z_i a_i = 0 \bmod q$

Improving the Reduction

- Replace $\mathbb{Z}$ with $\mathcal{O}_K$.
- Use K having constant root discriminant (as function of dim n).

Improving the Reduction

- Replace $\mathbb{Z}$ with $\mathcal{O}_K$.
- Use K having constant root discriminant (as function of dim n).

	Before	**After**
1. Size of solution z	$\sqrt{n \log n}$	$\sqrt{\log n}$
2. Length of offsets $\nearrow$	$\geq \sqrt{n} \cdot \lambda_1$	λ_1

Improving the Reduction

- Replace $\mathbb{Z}$ with $\mathcal{O}_K$.
- Use K having constant root discriminant (as function of dim n).

	Before	**After**
1. Size of solution z	$\sqrt{n \log n}$	$\sqrt{\log n}$
2. Length of offsets $\nearrow$	$\geq \sqrt{n} \cdot \lambda_1$	λ_1

1. Why shorter solutions?
    - $\mathcal{O}_K$ is much "denser" than $\mathbb{Z}$.

Improving the Reduction

- Replace $\mathbb{Z}$ with $\mathcal{O}_K$.
- Use K having constant root discriminant (as function of dim n).

	Before	After
1. Size of solution z	$\sqrt{n \log n}$	$\sqrt{\log n}$
2. Length of offsets $\nearrow$	$\geq \sqrt{n} \cdot \lambda_1$	λ_1

1. Why shorter solutions?
   - $\mathcal{O}_K$ is much "denser" than $\mathbb{Z}$.
2. Why shorter offsets?
   - Ideal lattice primal & dual have (optimally) large λ_1.

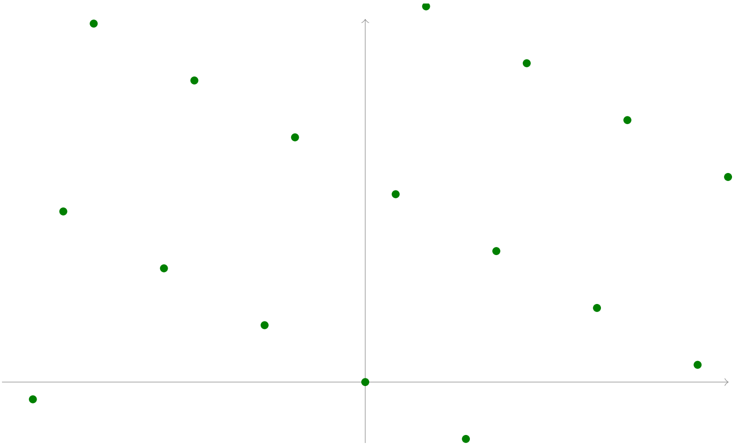
Crash Course in Algebraic Number Theory

Crash Course in Algebraic Number Theory

Pretty Pictures: Ideal Lattices

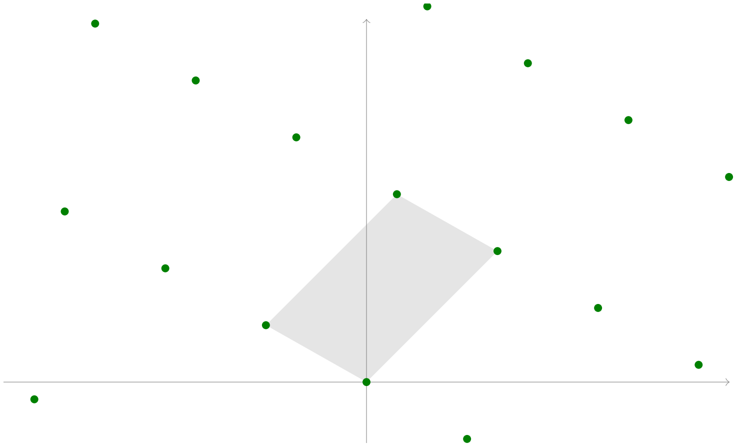
Pretty Pictures: Ideal Lattices

Pretty Pictures: Ideal Lattices



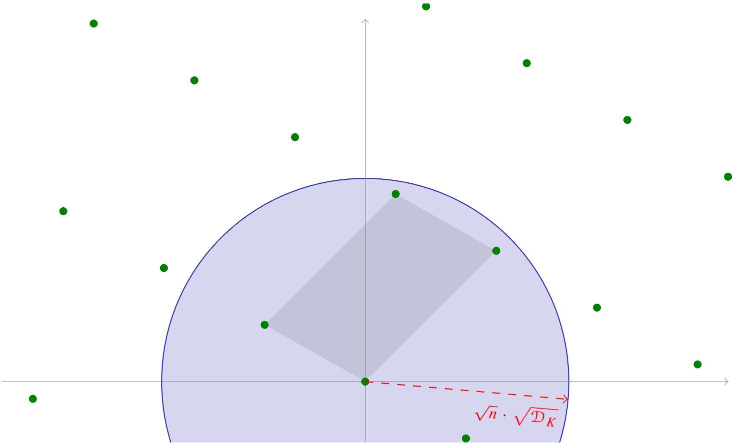
Pretty Pictures: Ideal Lattices

- Root discriminant $\mathcal{D}_K$ = (fundamental volume)$^{2/n}$



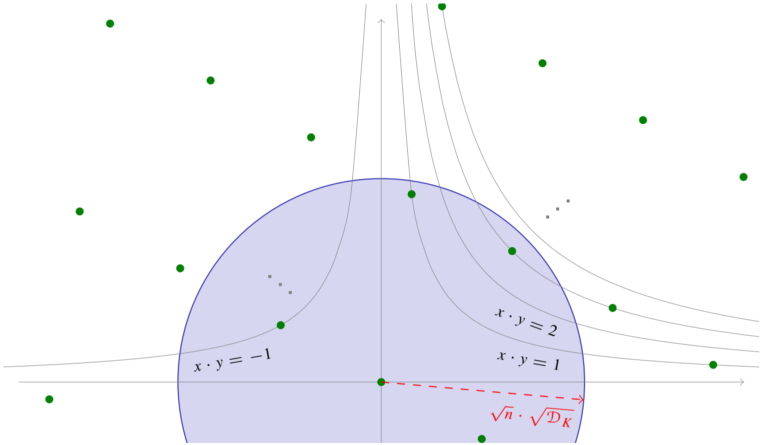
Pretty Pictures: Ideal Lattices

- Root discriminant $\mathcal{D}_K$ = (fundamental volume)$^{2/n}$



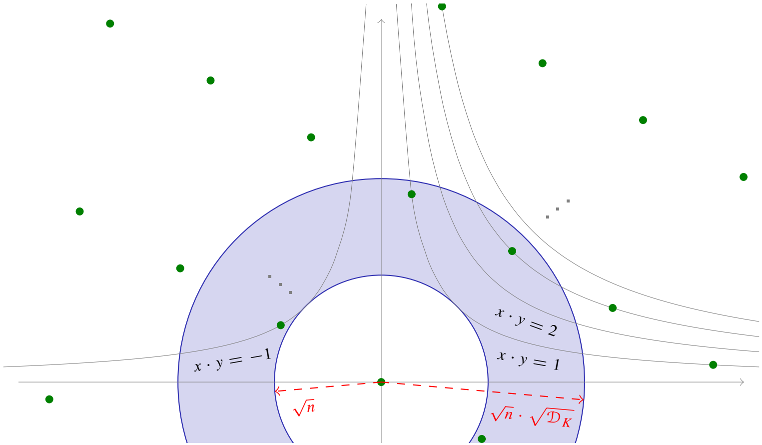
Pretty Pictures: Ideal Lattices

- Root discriminant $\mathcal{D}_K$ = (fundamental volume)$^{2/n}$



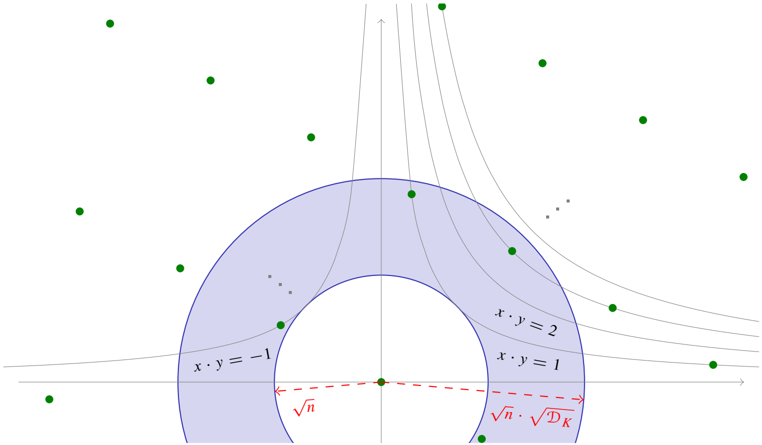
Pretty Pictures: Ideal Lattices

- Root discriminant $\mathcal{D}_K$ = (fundamental volume)$^{2/n}$
- Minimum distance λ_1 easy to estimate



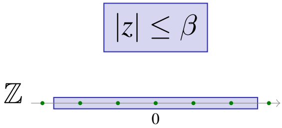
Pretty Pictures: Ideal Lattices

- Root discriminant $\mathcal{D}_K$ = (fundamental volume)$^{2/n}$
- Minimum distance λ_1 easy to estimate
- Same for dual lattice $\Rightarrow$ short offsets $\nearrow$

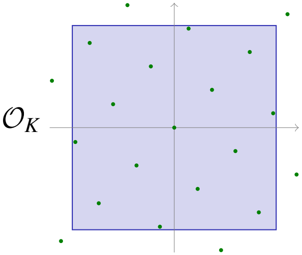


Shorter Average-Case Solutions

- $\mathcal{O}_K$ is much denser than $\mathbb{Z}$.



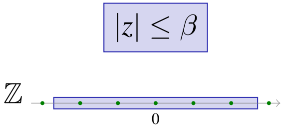
$\sim 2\beta$ elements



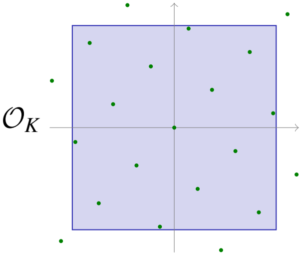
$\sim \beta^n$ elements!

Shorter Average-Case Solutions

- $\mathcal{O}_K$ is much denser than $\mathbb{Z}$.



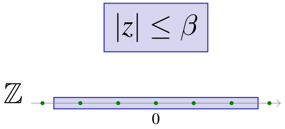
$\sim 2\beta$ elements



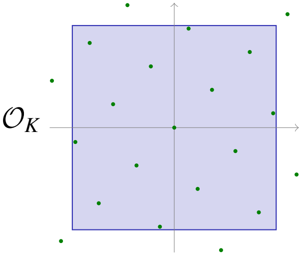
$\sim \beta^n$ elements!

Shorter Average-Case Solutions

- $\mathcal{O}_K$ is much denser than $\mathbb{Z}$.



$\sim 2\beta$ elements

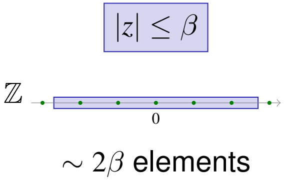


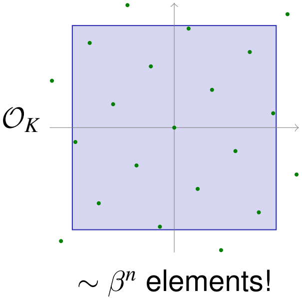
$\sim \beta^n$ elements!

- Solutions taken over $\mathcal{O}_K$ instead of $\mathbb{Z}$.

Shorter Average-Case Solutions

- $\mathcal{O}_K$ is much denser than $\mathbb{Z}$.





- Solutions taken over $\mathcal{O}_K$ instead of $\mathbb{Z}$.
- Denser $\mathcal{O}_K \Rightarrow$ denser, shorter solutions.

Open Problems

Good families of number fields K are crucial!

Open Problems

Good families of number fields K are crucial!

1. Need small root discriminant $\mathcal{D}_K$ (as function of dim n).

   Families with $\mathcal{D}_K < 100$ exist & are easy to verify.

   Q1: Are there efficient asymptotic constructions?

Open Problems

Good families of number fields K are crucial!

1. Need small root discriminant $\mathcal{D}_K$ (as function of dim n).

   Families with $\mathcal{D}_K < 100$ exist & are easy to verify.

   Q1: Are there efficient asymptotic constructions?

   - Concrete good K known up to $n \sim 85$
   - Even $\mathcal{D}_K \sim n^{2/3}$ is useful

Open Problems

Good families of number fields K are crucial!

1. Need small root discriminant $\mathcal{D}_K$ (as function of dim n).

   Families with $\mathcal{D}_K < 100$ exist & are easy to verify.

   Q1: Are there efficient asymptotic constructions?

   - Concrete good K known up to $n \sim 85$
   - Even $\mathcal{D}_K \sim n^{2/3}$ is useful

2. Reductions are non-uniform: need short basis for $\mathcal{O}_K$.

   Q2: Can explicit constructions yield this advice “for free”?

Open Problems

Good families of number fields K are crucial!

1. Need small root discriminant $\mathcal{D}_K$ (as function of dim n).

   Families with $\mathcal{D}_K < 100$ exist & are easy to verify.

   Q1: Are there efficient asymptotic constructions?

   - Concrete good K known up to $n \sim 85$
   - Even $\mathcal{D}_K \sim n^{2/3}$ is useful

2. Reductions are non-uniform: need short basis for $\mathcal{O}_K$.

   Q2: Can explicit constructions yield this advice "for free"?

3. Crypto is tricky: must map $\{0,1\}^*$ to short elts of $\mathcal{O}_K$.

   Q3: Can this be done efficiently?