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

Chris Peikert\textsuperscript{1}  Alon Rosen\textsuperscript{2}

\textsuperscript{1}SRI International

\textsuperscript{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:

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

Let $B = \{b_1, \ldots, b_n\} \subset \mathbb{R}^n$ be linearly independent.
The $n$-dim lattice $L$ having basis $B$ is:

$$L = \sum_{i=1}^{n} (\mathbb{Z} \cdot b_i)$$

Fundamental region: Parallelepiped $P$ spanned by $b_i$'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:

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

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

**Minimum distance:** $\lambda_1 = \text{length of shortest nonzero } \mathbf{v} \in \mathcal{L}$. 
Lattices

Let $\mathcal{B} = \{b_1, \ldots, b_n\} \subset \mathbb{R}^n$ be linearly independent. The $n$-dim lattice $\mathcal{L}$ having basis $\mathcal{B}$ is:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot b_i)$$

**Fundamental region:** Parallelepiped $\mathcal{P}$ spanned by $b_i$s.

**Minimum distance:** $\lambda_1 = \text{length of shortest nonzero } v \in \mathcal{L}$.

**Minkowski’s Theorem**

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

(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 $v \in \mathcal{L}$ such that $\|v\| \leq \gamma \cdot \lambda_1$. 
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 \( v \in \mathcal{L} \) such that \( \|v\| \leq \gamma \cdot \lambda_1 \).

**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 $v \in \mathcal{L}$ such that $\|v\| \leq \gamma \cdot \lambda_1$.

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

$\text{SVP}_{\gamma}$ hard in the worst case

\[\Downarrow\]

problems hard on the average
Worst-Case/Average-Case Connections [Ajtai,…]

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

$\text{SVP}_\gamma$ 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 \([\text{Ajtai,} \ldots]\)

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 \([\text{Ajtai,GGH,} \ldots]\)
- Public-key encryption \([\text{AjtaiDwork,Regev}]\)

---

**Optimizing the Connection Factor \(\gamma\)**

- Interesting to characterize complexity
- Important for crypto due to time/accuracy tradeoff
- Current best \(\gamma(n) \sim n\) \([\text{MicciancioRegev}]\)
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 $\ell_p$ 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.
   - For SVP in any $\ell_p$ norm.

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 [Ajtai Dwork, Regev]

2. Cyclic lattices:
   - Efficient & compact OWFs [Micciancio]
   - Collision-resistant hashing [Peikert Rosen, Lyubashevsky Micciancio]
Other Special Classes of Lattices

1. “Unique” shortest vector:
   - One-way/CR functions [Ajtai, GGH]
   - Public-key encryption [Ajtai Dwork, Regev]

2. Cyclic lattices:
   - Efficient & compact OWFs [Micciancio]
   - Collision-resistant hashing [Peikert Rosen, Lyubashevsky Micciancio]

Structure used for functionality & efficiency.
Connection factors $\gamma \sim n$ or more.
Worst-to-Average Reduction [Ajtai,…]

**Average-Case Problem**

For uniform $a_1, \ldots, a_m \leftarrow \mathbb{Z}^n \mod q$, find short nonzero $z \in \mathbb{Z}^m$:

$$\sum z_i a_i = 0 \mod q.$$
**Worst-to-Average Reduction** [Ajtai,…]

**Average-Case Problem**

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

\[
\sum z_i \mathbf{a}_i = 0 \mod q.
\]

**Reduction**

1. Sample offset vectors \( \mathbf{i}_i \in \mathbb{R}^n \), derive uniform \( \mathbf{a}_i \)’s
2. Get short solution \( \mathbf{z} \in \mathbb{Z}^m \)
3. Output \( (\sum z_i \cdot \mathbf{i}_i) \in \mathcal{L} \)
Worst-to-Average Reduction [Ajtai,…]

**Average-Case Problem**

For uniform \( a_1, \ldots, a_m \leftarrow \mathbb{Z}^n \mod q \), find short nonzero \( z \in \mathbb{Z}^m \):

\[
\sum z_i a_i = 0 \mod q.
\]

**Reduction**

1. Sample offset vectors \( \vec{i} \in \mathbb{R}^n \), derive uniform \( a_i \)'s
2. Get short solution \( z \in \mathbb{Z}^m \)
3. Output \( (\sum z_i \cdot \vec{i}) \in \mathcal{L} \)
Worst-to-Average Reduction [Ajtai,...]

**Average-Case Problem**

For uniform $a_1, \ldots, a_m \leftarrow \mathbb{Z}^n \mod q$, find short nonzero $z \in \mathbb{Z}^m$:

$$\sum z_i a_i = 0 \mod q.$$

**Reduction**

1. Sample offset vectors $i \in \mathbb{R}^n$, derive uniform $a_i$'s
2. Get short solution $z \in \mathbb{Z}^m$
3. Output $(\sum z_i \cdot i) \in \mathcal{L}$
Worst-to-Average Reduction [Ajtai,…]

Average-Case Problem

For uniform \( a_1, \ldots, a_m \leftarrow \mathbb{Z}^n \mod q \), find short nonzero \( z \in \mathbb{Z}^m \):

\[
\sum z_i a_i = 0 \mod q.
\]

Reduction

1. Sample offset vectors \( \vec{\eta}_i \in \mathbb{R}^n \), derive uniform \( a_i \)'s
2. Get short solution \( z \in \mathbb{Z}^m \)
3. Output \( (\sum z_i \cdot \vec{\eta}_i) \in \mathcal{L} \)
Worst-to-Average Reduction [Ajtai,…]

### Average-Case Problem

For uniform $a_1, \ldots, a_m \leftarrow \mathbb{Z}^n \mod q$, find short nonzero $z \in \mathbb{Z}^m$:

$$
\sum z_i a_i = 0 \mod q.
$$

### Reduction

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

### Connection Factor

- Size of solution $z \in \mathbb{Z}^m$
- Lengths of offset vectors $i$
Our Approach

- Replace “1-dim” integers \( \mathbb{Z} \) with “\( n \)-dim integers” \( \mathcal{O}_K \).

\[ \mathcal{O}_K = \text{ring of algebraic integers in number field } K \text{ of degree } n. \]
Our Approach

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

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

- Has $+$ and $\times$, “absolute value” $|\cdot|$, . . .
Our Approach

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

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

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

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Worst-case object</strong></td>
<td><strong>ideal in $\mathcal{O}_K$:</strong></td>
</tr>
<tr>
<td>lattice in $\mathbb{R}^n$:</td>
<td>$\sum (\mathcal{O}_K \cdot b_i)$ for $b_i \in \mathcal{O}_K$</td>
</tr>
<tr>
<td>$\sum (\mathbb{Z} \cdot b_i)$ for $b_i \in \mathbb{R}^n$</td>
<td>$\sum (\mathcal{O}_K \cdot b_i)$ for $b_i \in \mathcal{O}_K$</td>
</tr>
</tbody>
</table>
Our Approach

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

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

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

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Worst-case object</strong></td>
<td><strong>Ideal in $\mathcal{O}_K$:</strong></td>
</tr>
<tr>
<td>$lattice$ in $\mathbb{R}^n$:</td>
<td>$\sum (\mathcal{O}_K \cdot b_i)$ for $b_i \in \mathcal{O}_K$</td>
</tr>
<tr>
<td>$\sum (\mathbb{Z} \cdot b_i)$ for $b_i \in \mathbb{R}^n$</td>
<td>for $a_i \leftarrow \mathcal{O}_K \ mod \ q$</td>
</tr>
<tr>
<td><strong>Avg-case problem</strong></td>
<td><strong>find “small” $z_i \in \mathcal{O}_K$:</strong></td>
</tr>
<tr>
<td>find small $z_i \in \mathbb{Z}$:</td>
<td>$\sum z_i a_i = 0 \ mod \ q$</td>
</tr>
<tr>
<td>$\sum z_i a_i = 0 \ mod \ q$</td>
<td>for $a_i \leftarrow \mathcal{O}_K \ mod \ q$</td>
</tr>
</tbody>
</table>
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 $O_K$.
- Use $K$ having constant root discriminant (as function of dim $n$).

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Size of solution $z$</td>
<td>$\sqrt{n \log n}$</td>
<td>$\sqrt{\log n}$</td>
</tr>
<tr>
<td>2. Length of offsets</td>
<td>$\geq \sqrt{n \cdot \lambda_1}$</td>
<td>$\lambda_1$</td>
</tr>
</tbody>
</table>
Improving the Reduction

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

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Size of solution $z$</td>
<td>$\sqrt{n \log n}$</td>
</tr>
<tr>
<td>2. Length of offsets</td>
<td>$\geq \sqrt{n \cdot \lambda_1}$</td>
</tr>
</tbody>
</table>

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 \( n \)).

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Size of solution ( z )</td>
<td>( \sqrt{n \log n} )</td>
<td>( \sqrt{\log n} )</td>
</tr>
<tr>
<td>2. Length of offsets</td>
<td>( \geq \sqrt{n} \cdot \lambda_1 )</td>
<td>( \lambda_1 )</td>
</tr>
</tbody>
</table>

Why shorter solutions?
- \( \mathcal{O}_K \) is much “denser” than \( \mathbb{Z} \).

Why shorter offsets?
- Ideal lattice primal & dual have (optimally) large \( \lambda_1 \).
Pretty Pictures: Ideal Lattices
Pretty Pictures: Ideal Lattices
Pretty Pictures: Ideal Lattices

- Root discriminant $D_K = \frac{\text{(fundamental volume)}}{n}$
- Minimum distance $\lambda_1$ easy to estimate
- Same for dual lattice $\Rightarrow$ short offsets
Pretty Pictures: Ideal Lattices

- Root discriminant $D_K = (\text{fundamental volume})^{2/n}$
Pretty Pictures: Ideal Lattices

- Root discriminant $D_K = (\text{fundamental volume})^{2/n}$
Pretty Pictures: Ideal Lattices

- Root discriminant $\mathcal{D}_K = (\text{fundamental volume})^{2/n}$
Pretty Pictures: Ideal Lattices

- Root discriminant $D_K = (\text{fundamental volume})^{2/n}$
- Minimum distance $\lambda_1$ easy to estimate
Pretty Pictures: Ideal Lattices

- Root discriminant $D_K = (\text{fundamental volume})^{2/n}$
- Minimum distance $\lambda_1$ easy to estimate
- Same for dual lattice $\Rightarrow$ short offsets
Shorter Average-Case Solutions

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

- \(|z| \leq \beta\)

- \(\sim 2\beta\) elements

- \(\sim \beta^n\) elements!
Shorter Average-Case Solutions

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

\[
|z| \leq \beta
\]

\( \mathbb{Z} \)

\sim 2\beta \text{ elements}

\( \mathcal{O}_K \)

\sim \beta^n \text{ elements!}
Shorter Average-Case Solutions

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

$|z| \leq \beta$

$\sim 2\beta$ 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.

\[ |z| \leq \beta \]

\[ \sim 2\beta \text{ elements} \]

\[ \mathbb{Z} \]

\[ \mathcal{O}_K \]

\[ \sim \beta^n \text{ elements!} \]
Open Problems

Good families of number fields $K$ are crucial!

1. Need small root discriminant $D_K$ (as function of dim $n$).
   Families with $D_K < 100$ exist & are easy to verify.

2. Concrete good $K$ known up to $n \sim 85$.
   Even $D_K \sim n^{2/3}$ is useful.

3. Reductions are non-uniform: need short basis for $O_K$.

Q1: Are there efficient asymptotic constructions?

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

Q3: Can this be done efficiently?

Crypto is tricky: must map \{0, 1\} $\ast$ to short elts of $O_K$. 
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?

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

Q3: Can this be done efficiently?
Open Problems

Good families of number fields $K$ are crucial!

1. Need small root discriminant $D_K$ (as function of dim $n$).

Families with $D_K < 100$ exist & are easy to verify.

Q1: Are there efficient asymptotic constructions?

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

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

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

Q3: Can this be done efficiently?
Open Problems

Good families of number fields $K$ are crucial!

1. Need small root discriminant $D_K$ (as function of dim $n$).
   
   Families with $D_K < 100$ exist & are easy to verify.

   Q1: Are there efficient asymptotic constructions?
   
   - Concrete good $K$ known up to $n \sim 85$
   - Even $D_K \sim n^{2/3}$ 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 $D_K$ (as function of dim $n$).
   Families with $D_K < 100$ exist & are easy to verify.
   Q1: Are there efficient asymptotic constructions?
   - Concrete good $K$ known up to $n \sim 85$
   - Even $D_K \sim n^{2/3}$ 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?