Logarithmic Lattices

Léo Ducas

Centrum Wiskunde & Informatica, Amsterdam, The Netherlands

Workshop: Computational Challenges in the Theory of Lattices
ICERM, Brown University, Providence, RI, USA,
April 23-27, 2018
2 Settings

Continuous setting:
Λ ⊂ C^n: a lattice,
⊙: component-wise product on C^n.

\[ \text{Exp}_\Lambda : \vec{v} \in \mathbb{C}^n \mapsto (\exp(v_1), \ldots, \exp(v_n)) \circ \Lambda \]
\[ \mathcal{L} = \{ \vec{v} \in \mathbb{C}^n \text{ s.t. } \text{Exp}_\Lambda(\vec{v}) = \Lambda \}. \]

Discrete setting:
\[ \mathcal{B} = \{p_1, \ldots, p_n\} \subset K^\times: \text{ a set of primes of a field } K. \]
[·]: K^\times → G, a multiplicative morphism to a finite abelian group G.

\[ \text{Exp}_\mathcal{B} : \vec{v} \in \mathbb{Z}^n \mapsto \left[ \prod p_i^{v_i} \right] \]
\[ \mathcal{L} = \{ \vec{v} \in \mathbb{Z}^n \text{ s.t. } \text{Exp}_\mathcal{B}(\vec{v}) = \text{Id}_G \}. \]
Logarithm Problem

Logarithms are only defined mod $\mathcal{L}$:

$$\text{Exp}_B(x) = \text{Exp}_B(y) \iff x \in y + \mathcal{L}$$

$$\text{Log}_B(g) := \text{Exp}_B^{-1}(g) = x + \mathcal{L} \text{ s.t. } \text{Exp}_B(x) = g$$

Hidden Subgroup Problem

Find the lattice $\mathcal{L}$ (a set of generators of $\mathcal{L}$).
(typically: find one non-zero vector $\Rightarrow$ find the whole lattice)
Classically: Index Calculus Methods,
Quantumly: [Eisentrger Hallgren Kitaev Song 14]

Discrete Logarithm Problem mod $p$

$R = \mathbb{Z}, g, h \in (\mathbb{Z}/p\mathbb{Z})^\times$, \([\cdot] : x \mapsto x \mod p, \mathcal{L} = (p - 1)\mathbb{Z} \text{ is known.}
DLP: Find a representative $x \in \text{Log}(g)$
Short Logarithm Problems?

... non-zero vector in a lattice (coset) ... 

Non-zero vector in a lattice, you said?

How short can it be? Can it be found efficiently?

Fair question, but why would that matter?
Short Logarithm Problems?

... non-zero vector in a lattice (coset) ...

Non-zero vector in a lattice, you said?

How short can it be? Can it be found efficiently?

Fair question, but why would that matter?
Short Logarithm Problems?

... non-zero vector in a lattice (coset) ...

Non-zero vector in a lattice, you said?

How short can it be? Can it be found efficiently?

Fair question, but why would that matter?
Short Logarithm Problems?

... non-zero vector in a lattice (coset) ...

Non-zero vector in a lattice, you said?

How short can it be? Can it be found efficiently?

Fair question, but why would that matter?
Example (DLP over $(\mathbb{Z}/p\mathbb{Z})^\times$)

$\dim \mathcal{L} = 1$: Shortest solution trivially found...

Example (Inside Index Calculus)

Step 1 (relation collection) find many vectors $M = (v_1 \ldots v_m) \in \mathcal{L}$.
Step 2 (linear algebra) Solve the linear system $Mx = y$.

Step 2 is faster if $M$ is sparse: we want to make $M$ “shorter”!
But $\dim \mathcal{L} =$ HUGE: limited to ad-hoc micro improvements.

More interesting cases for lattice theoretician and algorithmicians?
3 encounters with *Logarithmic Lattices*

**[Cramer D. Peikert Regev 16]**: Dirichlet’s Unit lattice  
**[Cramer D. Wesolowsky 17]**: Stickelberger’s Class-relation lattice

**Summary**: These lattices admits a known almost-orthogonal basis  
⇒ Can use lattice algorithm to solve ‘short-DLP’  
⇒ Break some crypto

**[Chor Rivest ’89]**: Logarithmic lattices over $(\mathbb{Z}/p\mathbb{Z})^\times$  
**Summary**: Make certain ‘short-DLP’ easy by design, get an efficiently decodable lattice, hide it for Crypto.

**[D. Pierrot ’18]**: Logarithmic lattices over $(\mathbb{Z}/p\mathbb{Z})^\times$  
**Summary**: Remove crypto from Chor-Rivest. Optimize asymptotically. Get close to Minkowski’s bound.
3 encounters with \textit{Logarithmic Lattices}

\[\text{[Cramer D. Peikert Regev 16]}: \text{Dirichlet’s Unit lattice}\]
\[\text{[Cramer D. Wesolowsky 17]}: \text{Stickelberger’s Class-relation lattice}\]

\textbf{Summary:} These lattices admits a known almost-orthogonal basis
\[\Rightarrow \text{Can use lattice algorithm to solve ‘short-DLP’}\]
\[\Rightarrow \text{Break some crypto}\]

\[\text{[Chor Rivest ’89]}: \text{Logarithmic lattices over } (\mathbb{Z}/p\mathbb{Z})^\times\]
\textbf{Summary:} Make certain ‘short-DLP’ easy by design, get an efficiently decodable lattice, hide it for Crypto.

\[\text{[D. Pierrot ’18]}: \text{Logarithmic lattices over } (\mathbb{Z}/p\mathbb{Z})^\times\]
\textbf{Summary:} Remove crypto from Chor-Rivest. Optimize asymptotically. Get close to Minkowski’s bound.
3 encounters with \textit{Logarithmic Lattices}

[Cramer D. Peikert Regev 16]: Dirichlet’s Unit lattice
[Cramer D. Wesolowsky 17]: Stickelberger’s Class-relation lattice

\textbf{Summary:} These lattices admits a known almost-orthogonal basis
\[\Rightarrow\] Can use lattice algorithm to solve ‘short-DLP’
\[\Rightarrow\] Break some crypto

\[\text{Chor Rivest '89}\]: Logarithmic lattices over \((\mathbb{Z}/p\mathbb{Z})^\times\)
\textbf{Summary:} Make certain ‘short-DLP’ easy by design, get an efficiently decodable lattice, hide it for Crypto.

\[\text{D. Pierrot '18}\]: Logarithmic lattices over \((\mathbb{Z}/p\mathbb{Z})^\times\)
\textbf{Summary:} Remove crypto from Chor-Rivest. Optimize asymptotically. Get close to Minkowski’s bound.
Part 1:
The Logarithmic Lattice of cyclotomic units

Part 2:
Short Stickelberger’s Class relations

Part 3:
Chor-Rivest dense Sphere-Packing with efficient decoding

For a Survey on 1 and 2, see [D. ’17],
Part 1:
The logarithmic lattice of cyclotomic units
Cyclotomic number field: $K(= \mathbb{Q}(\omega_m))$, ring of integer $R = \mathcal{O}_K(= \mathbb{Z}[\omega_m])$.

**Definition (Ideals)**

- An **integral ideal** is a subset $\mathfrak{h} \subset \mathcal{O}_K$ closed under addition, and by multiplication by elements of $\mathcal{O}_K$,

- A **(fractional) ideal** is a subset $\mathfrak{f} \subset K$ of the form $\mathfrak{f} = \frac{1}{x} \mathfrak{h}$, where $x \in \mathbb{Z}$,

- A **principal ideal** is an ideal $\mathfrak{f}$ of the form $\mathfrak{f} = g \mathcal{O}_K$ for some $g \in K$.

In particular, ideals are lattices.

We denote $\mathcal{F}_K$ the set of fractional ideals, and $\mathcal{P}_K$ the set of principal ideals.
The Problem

Short generator recovery

Given $h \in R$, find a small generator $g$ of the ideal $(h)$.

Note that $g \in (h)$ is a generator iff $g = u \cdot h$ for some unit $u \in \mathbb{R}^\times$. We need to explore the (multiplicative) unit group $R^\times$. 
The Problem

Short generator recovery

Given \( h \in R \), find a small generator \( g \) of the ideal \((h)\).

Note that \( g \in (h) \) is a generator iff \( g = u \cdot h \) for some unit \( u \in \mathbb{R}^\times \).

We need to explore the (multiplicative) unit group \( R^\times \).

Translation an to additive problem

Take logarithms:

\[
\text{Log} : g \mapsto (\log |\sigma_1(g)|, \ldots, \log |\sigma_n(g)|) \in \mathbb{R}^n
\]

where the \( \sigma_i \)'s are the canonical embeddings \( \mathbb{K} \to \mathbb{C} \).
Let $R^\times$ denotes the multiplicative group of units of $R$. Let

$$\Lambda = \text{Log } R^\times.$$  

Theorem (Dirichlet unit Theorem)

$\Lambda \subset \mathbb{R}^n$ is a lattice (of a given rank).
The Unit Group and the log-unit lattice

Let $R^\times$ denotes the multiplicative group of units of $R$. Let

$$\Lambda = \text{Log } R^\times.$$

**Theorem (Dirichlet unit Theorem)**

$\Lambda \subset \mathbb{R}^n$ is a lattice (of a given rank).

**Reduction to a Close Vector Problem**

Elements $g$ is a generator of $(h)$ if and only if

$$\text{Log } g \in \text{Log } h + \Lambda.$$

Moreover the map Log preserves some geometric information: $g$ is the “smallest” generator iff Log $g$ is the “smallest” in Log $h + \Lambda$. 

Cramer, D., Peikert, Regev (Leiden, CWI, NYU) Recovering Short Generators Eurocrypt, May 2016 7 / 21
Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

- **x-axis:** $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$
- **y-axis:** $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$
- component-wise additions and multiplications
Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

- $x$-axis: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$
- $y$-axis: $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$
- Component-wise additions and multiplications

- "Orthogonal" elements
- Units (algebraic norm 1)
- "Isonorms" curves
Example: Logarithmic Embedding $\log \mathbb{Z}[\sqrt{2}]$

$\{\bullet\}, +$ is a sub-monoid of $\mathbb{R}^2$
Example: Logarithmic Embedding $\log \mathbb{Z}[\sqrt{2}]$

\[ \Lambda = (\{\bullet\}, +) \cap \text{ is a lattice of } \mathbb{R}^2, \text{ orthogonal to } (1, 1) \]
Example: Logarithmic Embedding $\text{Log } \mathbb{Z}[\sqrt{2}]$

\{ • \} \cap \text{ are shifted finite copies of } \Lambda
Reduction modulo $\Lambda = \log \mathbb{Z}[\sqrt{2}]^\times$

The reduction mod\(\Lambda\) for various fundamental domains.
Reduction modulo $\Lambda = \log \mathbb{Z}[\sqrt{2}]^\times$

The reduction mod $\Lambda$ for various fundamental domains.
Reduction modulo $\Lambda = \log \mathbb{Z}[\sqrt{2}]^\times$

The reduction mod $\Lambda$ for various fundamental domains.
Reduction modulo $\Lambda = \log \mathbb{Z}[\sqrt{2}]^\times$

The reduction mod $\Lambda$ for various fundamental domains.
A two-step approach was suggested in [Bernstein ’14, Cambell Groves Shepherd ’14]:

- Use fancy quantum algorithm to recover any generator $h$
  [Eisenträger Hallgren Kitaev Song ’14, Biasse Song ’16]
- Reduce modulo units to obtain a short generator
  [Cramer D. Peikert Regev ’16]

For the analysis of the second step we need an explicit basis of the units of $\mathbb{Z}[^\omega]$. It is (almost) given by the set

$$u_i = \frac{1 - \omega^i}{1 - \omega} \text{ for } i \in (\mathbb{Z}/m\mathbb{Z})^\times$$
Almost Orthogonal

Using techniques from Analytic Number Theory (bounds on Dirichlet $L$-series), we can prove that the basis $(\log u_i)_i$ is almost orthogonal. Implies efficient algorithms for

- Bounded Distance Decoding problem (BDD)
- Approximate Close Vector Problem (approx-CVP)

for interesting parameters.

### Short Generator Recovery, BDD setting

If there exists an unusually short generator $g$ (as in certain crypto settings), we can recover it in classical poly-time from any generator $h = ug$.

### Short Generator Recovery, worst-case

For any generator $h$, we can recover a generator $g$ of length at most $\exp(\tilde{O}(\sqrt{n}))$ larger than the shortest vector of $(h)$. 
Can we remove the Principality condition?
Comparison with General lattices

General Lattices

Crypto

Time

$e^{\tilde{\Theta}(n)}$

$e^{\tilde{\Theta}(\sqrt{n})}$

poly$(n)$

polyn$(n)$

$e^{\tilde{\Theta}(\sqrt{n})}$

$e^{\tilde{\Theta}(n)}$

Principal Ideal lattices

Crypto

Time

$e^{\tilde{\Theta}(n)}$

$e^{\tilde{\Theta}(\sqrt{n})}$

poly$(n)$

polyn$(n)$

$e^{\tilde{\Theta}(\sqrt{n})}$

$e^{\tilde{\Theta}(n)}$

Can we remove the **Principality** condition?
Part 2:
Short Stickelberger’s Class relations
The obstacle: the Class Group

Ideals can be multiplied, and remain ideals:

\[ ab = \left\{ \sum_{\text{finite}} a_i b_i, \quad a_i \in a, \ b_i \in b \right\}. \]

The product of two principal ideals remains principal:

\[ (a\mathcal{O}_K)(b\mathcal{O}_K) = (ab)\mathcal{O}_K. \]

\(\mathcal{F}_K\) form an abelian group\(^1\), \(\mathcal{P}_K\) is a subgroup of it.

**Definition (Class Group)**

Their quotient forms the **class group** \(\text{Cl}_K = \mathcal{F}_K/\mathcal{P}_K\).

An ideal \(\alpha \in \mathcal{F}_K\) is denoted \([\alpha] \in \text{Cl}_K\).

An ideal \(\alpha\) is principal iff \([\alpha] = [\mathcal{O}_K]\).

---

\(^1\)with neutral element \(\mathcal{O}_K\)
The obstacle: the Class Group

Ideals can be multiplied, and remain ideals:

$$ab = \left\{ \sum_{\text{finite}} a_i b_i, \quad a_i \in a, b_i \in b \right\}.$$  

The product of two principal ideals remains principal:

$$(aO_K)(bO_K) = (ab)O_K.$$  

$\mathcal{F}_K$ form an abelian group\(^1\), $\mathcal{P}_K$ is a subgroup of it.

**Definition (Class Group)**

Their quotient forms the **class group** $\text{Cl}_K = \mathcal{F}_K / \mathcal{P}_K$.

The class of an ideal $a \in \mathcal{F}_K$ is denoted $[a] \in \text{Cl}_K$.

An ideal $a$ is principal iff $[a] = [O_K]$.

\(^1\)with neutral element $O_K$
The problem: Reducing to the principal case

Definition (The Close Principal Multiple problem)

- Given an ideal \( a \), and an factor \( F \)
- Find a **small integral** ideal \( b \) such that \([ab] = [\mathcal{O}_K]\) and \( Nb \leq F \)

**Note:** Smallness with respect to the Algebraic Norm \( N \) of \( b \), (essentially the **volume** of \( b \) as a lattice).

Choose a factor basis \( \mathcal{B} = \{p_1 \ldots p_n\} \) and restrict the search to \( b \) of the form \( b = \prod p_i^{\nu_i} \). i.e. solve the **short discrete-logarithm problem**

\[ \vec{v} \in \text{Log}_\mathcal{B}([a]^{-1}). \]
How to solve it?

Again, two steps:

- Find an arbitrary solution $\vec{v} \in \text{Log}_B([a]^{-1})$
  
  [Eisentrager Kitaev Hallgren Song ’14, Biasse Song ’16]

- Reduce it modulo $L$ ?

But do we even know $L = \text{Log}_B([\mathcal{O}_K])$ ?
Yes, we know $\mathcal{L}$ ! (Well Almost)

For a well chosen factor basis, e.g. $\{\sigma(p), \sigma \in G := \text{Gal}(K/\mathbb{Q})\}$, $\mathcal{L}$ is almost given by Stickelberger:

**Definition (The Stickelberger ideal)**

The **Stickelberger element** $\theta \in \mathbb{Q}[G]$ is defined as

$$\theta = \sum \left( \frac{a}{m} \mod 1 \right) \sigma_a^{-1}$$

where $G \ni \sigma_a : \omega \mapsto \omega^a$.

The **Stickelberger ideal** is defined as $S = \mathbb{Z}[G] \cap \theta \mathbb{Z}[G]$.

**Theorem (Stickelberger’s theorem)**

*The Stickelberger ideal annihilates* $\text{Cl}$: $\forall e \in S, a \subset K$: $[a^e] = [\mathcal{O}_K]$. *In particular, if* $\mathcal{B} = \{p^\sigma, \sigma \in G\}$, *then* $S \subset \mathcal{L}$.

**Turn-out**: the natural basis of $S$ is almost orthogonal... Again !
For a well chosen factor basis, e.g. $\mathcal{L} = \{\sigma(p), \sigma \in G := \text{Gal}(K/\mathbb{Q})\}$, $\mathcal{L}$ is almost given by Stickelberger:

**Definition (The Stickelberger ideal)**

The **Stickelberger element** $\theta \in \mathbb{Q}[G]$ is defined as

$$\theta = \sum \left(\frac{a}{m} \mod 1\right) \sigma^{-1}$$

where $G \ni \sigma_a : \omega \mapsto \omega^a$.

The **Stickelberger ideal** is defined as $S = \mathbb{Z}[G] \cap \theta \mathbb{Z}[G]$.

**Theorem (Stickelberger’s theorem)**

The Stickelberger ideal annihilates $\text{Cl}$: $\forall e \in S, a \subset K: [\alpha^e] = [\mathcal{O}_K]$.

*In particular, if $\mathcal{B} = \{p^\sigma, \sigma \in G\}$, then $S \subset \mathcal{L}$.**

**Turn-out:** the natural basis of $S$ is almost orthogonal... Again!
Approx-Ideal-SVP in poly-time for large $\alpha$

[Cramer D. Wesolowsky '17] CPM via Stickelberger Short Class Relation

$\Rightarrow$ Approx-Ideal-SVP solvable in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

General Lattices

Ideal lattices

Time

Crypto

\[ e^{\tilde{\Theta}(\sqrt{n})} \]

\[ e^{\tilde{\Theta}(n)} \]

\[ \alpha \]

\[ \text{poly}(n) \]

\[ \text{poly}(n) \]

\[ e^{\tilde{\Theta}(\sqrt{n})} \]

\[ e^{\tilde{\Theta}(n)} \]

\[ \alpha \]

\[ \text{poly}(n) \]

\[ \text{poly}(n) \]
Approx-Ideal-SVP in poly-time for large $\alpha$

[Cramer D. Wesolowsky '17] CPM via Stickelberger Short Class Relation

$\Rightarrow$ Approx-Ideal-SVP solvable in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

General Lattices

Ideal lattices

L. Ducas (CWI)
Takeaway: Dual viewpoint (Caley-Graphs and Lattices)

\[
\mu : \vec{v} \in \mathbb{Z}^2 \mapsto v_1 + 2v_2 \mod 5, \quad \Lambda = \ker \mu,
\]
then \(\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}^2/\Lambda\)

Cayley-Graph(\(\mathbb{Z}/5\mathbb{Z}, \{1, 2\}\))

\[\mathbb{Z}^{\{1,2\}}/\Lambda\]

\(\ell_1\)-distance mod \(\Lambda\)
Covering radius
Minimal vector
Smoothing parameter

Distance
Diameter
Shortest loop
Mixing time
Part 3:
Chor-Rivest dense Sphere-Packing with efficient decoding
Dense Lattice with Efficient Decoding

Construct a lattice $\mathcal{L}$ together with an efficient decoding algorithm for $\mathcal{L}$

**Bounded Distance Decoding with radius $r$**

- Given $t = v + e$ where $v \in \mathcal{L}$ and $\|e\| \leq r$
- Recover $v$ and/or $e$

The problem can only be solved up to half the minimal distance:

$$r \leq \lambda_1(\mathcal{L})/2$$

(otherwise solution are not uniques). We would like to find a lattice for which the above can be done efficiently up to $r$ close to Minkowsky’s bound:

$$\lambda_1^{(1)}(\mathcal{L}) \leq O(n) \cdot \det(\mathcal{L})^{-1/n}$$

$$\lambda_1^{(2)}(\mathcal{L}) \leq O(\sqrt{n}) \cdot \det(\mathcal{L})^{-1/n}.$$
Chor-Rivest Cryptosystem and Friends

[Chor Rivest ’89]: First knapsack-based cryptosystem that was not devastated. Idea:

- Subset-sums is hard
- Subset-product is easy (factoring numbers knowing potential factors)
- Take logarithm to disguise the later as the former, get crypto.

Variants of the cryptosystem by [Lenstra ’90, Li Ling Xing Yeo ’17].

Originally over finite-field polynomials $\mathbb{F}_p[X]$, but variants also exists over the integers: [Naccache Stern ’97, Okamoto Tanaka Uchiyama ’00].

[Brier Coron Geraud Maimut Naccache ’15]: Remove crypto from [NS’97], get a good decodable binary code.

[D. Pierrot ’18]: Remove crypto from [OTU ’00], get a good decodable lattice.
[Chor Rivest ’89]: First knapsack-based cryptosystem that was not devastated. Idea:

- Subset-sums is hard
- Subset-product is easy (factoring numbers knowing potential factors)
- Take logarithm to disguise the later as the former, get crypto.

Variants of the cryptosystem by [Lenstra ’90, Li Ling Xing Yeo ’17].

Originally over finite-field polynomials \( \mathbb{F}_p[X] \), but variants also exists over the integers: [Naccache Stern ’97, Okamoto Tanaka Uchiyama ’00].

[Brier Coron Geraud Maimut Naccache ’15]: Remove crypto from [NS’97], get a good decodable binary code.

[D. Pierrot ’18]: Remove crypto from [OTU ’00], get a good decodable lattice.
[Chor Rivest '89]: First knapsack-based cryptosystem that was not devastated. Idea:

- Subset-sums is hard
- Subset-product is easy (factoring numbers knowing potential factors)
- Take logarithm to disguise the later as the former, get crypto.

Variants of the cryptosystem by [Lenstra '90, Li Ling Xing Yeo '17].

Originally over finite-field polynomials \( \mathbb{F}_p[X] \), but variants also exists over the integers: [Naccache Stern '97, Okamoto Tanaka Uchiyama '00].

[Brier Coron Geraud Maimut Naccache '15]: Remove crypto from [NS’97], get a good decodable binary code.

[D. Pierrot '18]: Remove crypto from [OTU '00], get a good decodable lattice.
Chor-Rivest Cryptosystem and Friends

[Chor Rivest ’89]: First knapsack-based cryptosystem that was not devastated. Idea:

▶ Subset-sums is hard
▶ Subset-product is easy (factoring numbers knowing potential factors)
▶ Take logarithm to disguise the later as the former, get crypto.

Variants of the cryptosystem by [Lenstra ’90, Li Ling Xing Yeo ’17].

Originally over finite-field polynomials \( \mathbb{F}_p[X] \), but variants also exists over the integers: [Naccache Stern ’97, Okamoto Tanaka Uchiyama ’00].

[Brier Coron Geraud Maimut Naccache ’15]: Remove crypto from [NS’97], get a good decodable binary code.

[D. Pierrot ’18]: Remove crypto from [OTU ’00], get a good decodable lattice.
Choose a factor basis of \textbf{small} primes, coprimes to $Q = 3^k$: \hspace{1cm} 

$$\mathcal{B} = \{2, 5, 7, 11, 13, \ldots, p_n\} \subset \mathbb{Z}, \quad [\cdot] : x \mapsto x \mod Q.$$  

$$\mathcal{L} = \{v \in \mathbb{Z}^n \text{ s.t. } \prod p_i^{v_i} = 1 \mod Q\}.$$  

\hspace{1cm} 

$\dim \mathcal{L} = n$, $\det \mathcal{L} \leq \phi(Q) \leq Q$. Note that $p_n \sim n \log n$. 

\hspace{1cm}
If \( p_n^r < Q \) then one can decode integral positive errors up to \( \ell_1 \) radius \( r \) in the lattice \( \mathcal{L} \). That is:

- given \( t = v + e \), for \( v \in \mathcal{L} \) and \( e \in \mathbb{Z}_{\geq 0}^n \), \( \|e\|_1 \leq r \)
- we can efficiently recover \( v \) and \( e \).

Compute

\[
\prod p_i^{t_i} \mod Q = \prod p_i^{v_i} \prod p_i^{e_i} \mod Q = \prod p_i^{e_i} \mod Q
\]

The last product is in fact known over \( \mathbb{Z} \), not just \( \mod Q \), since \( \prod p_i^{e_i} < Q \). Factorize \( f \) (efficient trial division by 2, 5, ..., \( p_n \)), recover \( e \), then \( v \).
Decoding Chor-Rivest Lattice

Now assume $2 \cdot p_n^r < \sqrt{Q}$.

$$f = \prod_{i \text{ s.t. } e_i > 0} p_i^{e_i} \cdot \prod_{i \text{ s.t. } e_i < 0} p_i^{e_i} = u/v \mod Q.$$ 

To recover $u = \prod_{i \text{ s.t. } e_i > 0} p_i^{e_i}$ and $v = \prod_{i \text{ s.t. } e_i < 0} p_i^{-e_i}$ not only modulo $Q$ but in $\mathbb{Z}$, we use the following lemma.

**Lemma (Rational reconstruction mod $Q$)**

*If $u, v$ are positive coprime integers and invertible modulo $m$ such that $u, v < \sqrt{m/2}$, and if $f = u/v \mod m$, then $\pm(u, v)$ are the shortests vector of the 2-dimensional lattice

$$L = \{(x, y) \in \mathbb{Z}^2 | x - fy = 0 \mod Q\}.$$*

*In particular, given $f$ and $m$, one can recover $(u, v)$ in polynomial time.*
Choose $k = n$. This gives

$$r^{(1)} = \Theta(n/ \log n) = \Theta(n/ \log n) \det(L)^{-1/n}.$$ 

Compare to Minkowsky’s bound in $\ell_1$ norm:

$$\lambda_1^{(1)}(L) \leq O(n) \cdot \det(L)^{-1/n}$$

By norm inequality this directly imply decoding in $\ell_2$-norm for a radius

$$r^{(2)} = \Theta(\sqrt{n}/ \log n) = \Theta(\sqrt{n}/ \log n) \det(L)^{-1/n}.$$ 

Compare to Minkowsky’s bound in $\ell_2$ norm:

$$\lambda_1^{(2)}(L) \leq O(\sqrt{n}) \cdot \det(L)^{-1/n}.$$
Asymptotic parameters

Choose \( k = n \). This gives

\[
r^{(1)} = \Theta(n / \log n) = \Theta(n / \log n) \det(L)^{-1/n}.
\]

Compare to Minkowsky’s bound in \( \ell_1 \) norm:

\[
\lambda_1^{(1)}(L) \leq O(n) \cdot \det(L)^{-1/n}
\]

By norm inequality this directly imply decoding in \( \ell_2 \)-norm for a radius

\[
r^{(2)} = \Theta(\sqrt{n} / \log n) = \Theta(\sqrt{n} / \log n) \det(L)^{-1/n}.
\]

Compare to Minkowsky’s bound in \( \ell_2 \) norm:

\[
\lambda_1^{(2)}(L) \leq O(\sqrt{n}) \cdot \det(L)^{-1/n}.
\]
A paradoxical result?

To the best of our knowledge, the best lattice with efficient BDD was Barnes-Wall, with BDD up to a radius $O(\sqrt[4]{n})$ away from Minkowsky’s bound [Micciancio Nicolesi ’08] ($\ell_2$ norm).

We are only $O(\log n)$ away from Minkowsky’s bound, but this result is strange:

- We can construct $\mathcal{L}$ efficiently.
- We can solve BDD efficiently in $\mathcal{L}$
- We don’t know how to find short vectors in $\mathcal{L}$...
We are still $O(\log n)$ away from Minkowsky’s bound...
The issue is that we do not have enough small primes.
To get down to $O(1)$ away from Minkowsky’s bound, we need

$$n \text{ primes of ‘size’ } O(1).$$

- Switching back from $\mathbb{Z}$ to $\mathbb{F}_p[X]$ does not solve improve this loss
- Elliptic curves could ?
- Connection with Mordel-Weil lattices ? [Shioda ’91, Elkies ’94]
Thanks for your interest.

Questions?

Other Logarithmic Lattices of interest?
Thanks for your interest.

Questions?

Other Logarithmic Lattices of interest?