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:
$\Lambda \subset \mathbb{C}^n$: a lattice,
$\odot$: component-wise product on $\mathbb{C}^n$.

$$\mathrm{Exp}_\Lambda : \vec{v} \in \mathbb{C}^n \mapsto (\exp(v_1), \dots, \exp(v_n)) \odot \Lambda$$
$$\mathscr{L} = \{v \in \mathbb{C}^n \text{ s.t. } \mathrm{Exp}_\Lambda(v) = \Lambda\}.$$

Discrete setting:
$\mathfrak{B} = \{\mathfrak{p}_1, \dots \mathfrak{p}_n\} \subset K^\times$: a set of primes of a field K.
$[\cdot] : K^\times \to G$, a multiplicative morphism to a finite abelian group G.

$$\mathrm{Exp}_\mathfrak{B} : \vec{v} \in \mathbb{Z}^n \mapsto \left[\prod \mathfrak{p}_i^{v_i}\right]$$
$$\mathscr{L} = \{v \in \mathbb{Z}^n \text{ s.t. } \mathrm{Exp}_\mathfrak{B}(v) = Id_G\}.$$

Logarithm Problem

Logarithms are only defined $\bmod \mathscr{L}$:

$$\mathrm{Exp}_{\mathfrak{B}}(x) = \mathrm{Exp}_{\mathfrak{B}}(y) \Leftrightarrow x \in y + \mathscr{L}$$
$$\mathrm{Log}_{\mathfrak{B}}(g) := \mathrm{Exp}_{\mathfrak{B}}^{-1}(g) = x + \mathscr{L} \text{ s.t. } \mathrm{Exp}_{\mathfrak{B}}(x) = g$$

Hidden Subgroup Problem

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

Discrete Logarithm Problem $\bmod p$

$R = \mathbb{Z}$, $g, h \in (\mathbb{Z}/p\mathbb{Z})^\times$, $[\cdot] : x \mapsto x \bmod p$, $\mathscr{L} = (p-1)\mathbb{Z}$ is known.
DLP: Find a representative $x \in \mathrm{Log}(g)$

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 ?

Short Logarithm Problems ?

Example (DLP over $(\mathbb{Z}/p\mathbb{Z})^\times$)

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

Example (Inside Index Caculus)

Step 1 (relation collection) find many vectors $M = (v_1 \ldots v_m) \in \mathscr{L}$.
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 $\dim \mathscr{L} =$ HUGE: limited to ad-hoc micro improvements.

More interesting cases for lattice theoretician and algorithmicians ?

3 encounters with $\mathscr{L}$ogarithmic $\mathscr{L}$attices

[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
$\Rightarrow$ Can use lattice algorithm to solve 'short-DLP'
$\Rightarrow$ 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 $\mathscr{L}$ogarithmic $\mathscr{L}$attices

[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
$\Rightarrow$ Can use lattice algorithm to solve 'short-DLP'
$\Rightarrow$ 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 $\mathscr{L}$ogarithmic $\mathscr{L}$attices

[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
$\Rightarrow$ Can use lattice algorithm to solve 'short-DLP'
$\Rightarrow$ 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.

Part 1:
The $\mathscr{L}$ogarithmic $\mathscr{L}$attice of cyclotomic units

$\sim$

Part 2:
Short Stickelberger's $\mathscr{C}\ell$ass relations

$\sim$

Part 3:
Chor-Rivest dense $\mathscr{S}$phere-$\mathscr{P}$acking
with efficient decoding

For a Survey on 1 and 2, see **[D. '17]**,
`http://www.nieuwarchief.nl/serie5/pdf/naw5-2017-18-3-184.pdf`

Part 1:
The $\mathscr{L}$ogarithmic $\mathscr{L}$attice of cyclotomic units

Ideals and Principal Ideals

Cyclotomic number field: $K(= \mathbb{Q}(\omega_m))$, ring of integer $R = \mathscr{O}_K(= \mathbb{Z}[\omega_m])$.

Definition (Ideals)

- An **integral ideal** is a subset $\mathfrak{h} \subset \mathscr{O}_K$ closed under addition, and by multiplication by elements of $\mathscr{O}_K$,
- 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 $\mathfrak{f} = g\mathscr{O}_K$ for some $g \in K$.

In particular, ideals are lattices.

We denote $\mathscr{F}_K$ the set of fractional ideals,
and $\mathscr{P}_K$ 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:

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

where the σ_i's are the canonical embeddings $\mathbb{K} \to \mathbb{C}$.

The Unit Group and the log-unit lattice

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

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

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

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

Theorem (Dirichlet unit Theorem)

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

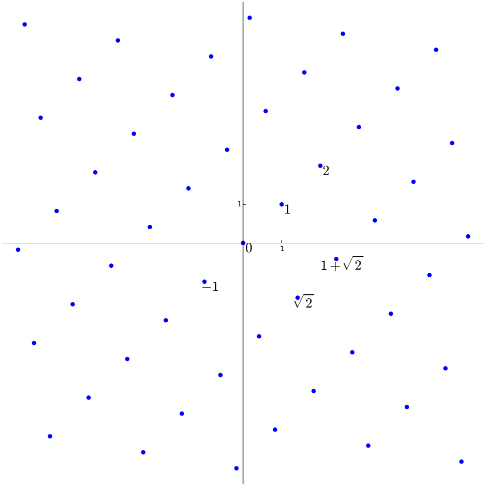
Reduction to a Close Vector Problem

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

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

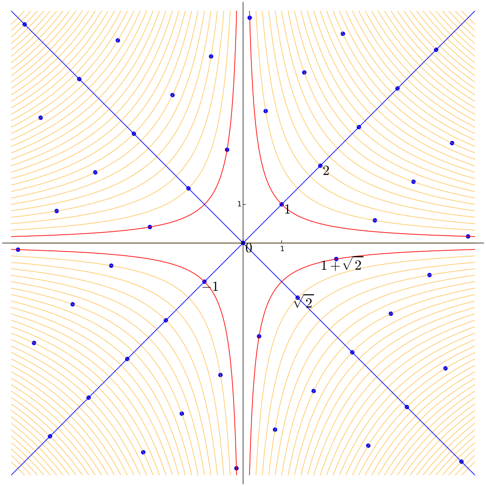
Moreover the map Log preserves some geometric information:
g is the "smallest" generator iff $\operatorname{Log} g$ is the "smallest" in $\operatorname{Log} h + \Lambda$.

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

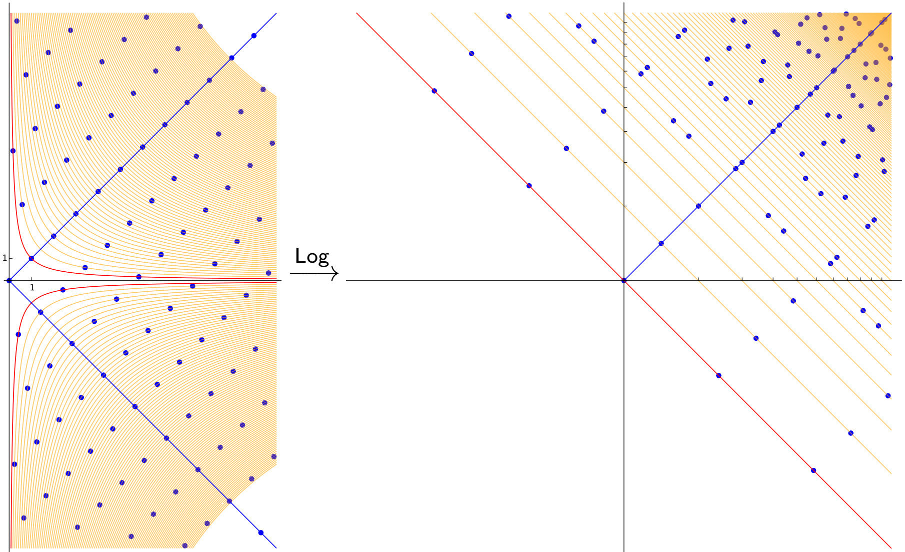
"Orthogonal" elements

Units (algebraic norm 1)

"Isonorms" curves

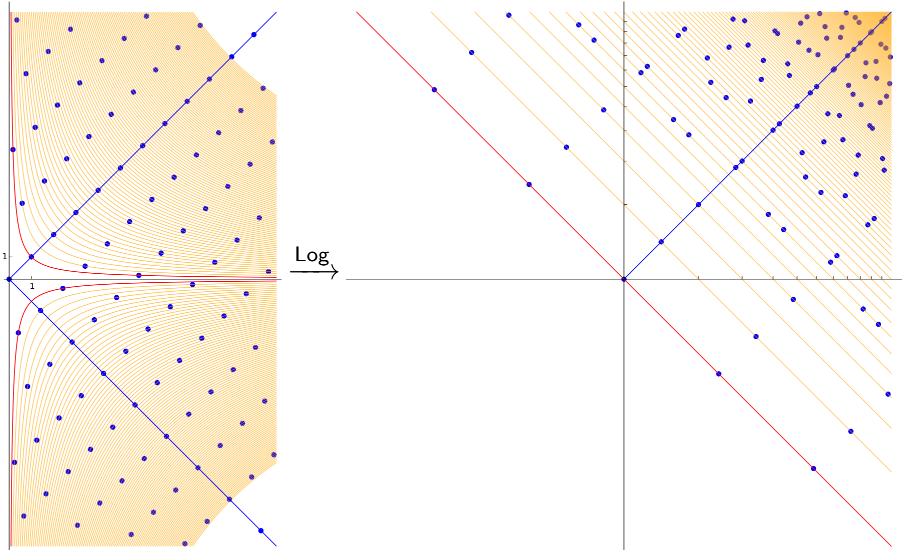
Example: Logarithmic Embedding $\mathrm{Log}\,\mathbb{Z}[\sqrt{2}]$

$(\{\bullet\}, +)$ is a sub-monoid of $\mathbb{R}^2$



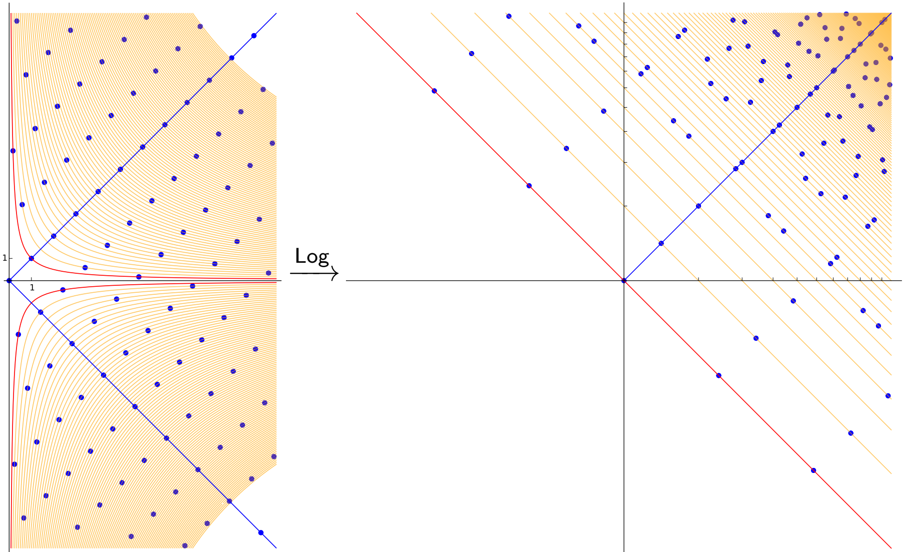
Example: Logarithmic Embedding Log $\mathbb{Z}[\sqrt{2}]$

$\Lambda = (\{\bullet\}, +) \cap$ ╲ is a lattice of $\mathbb{R}^2$, orthogonal to $(1, 1)$



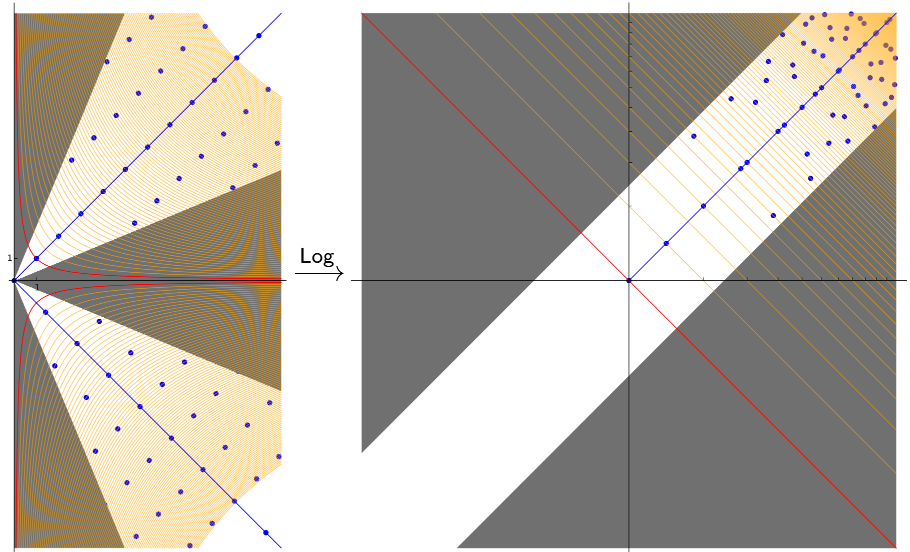
Example: Logarithmic Embedding $\operatorname{Log} \mathbb{Z}[\sqrt{2}]$

$\{\bullet\} \cap$ ╲ are shifted finite copies of Λ



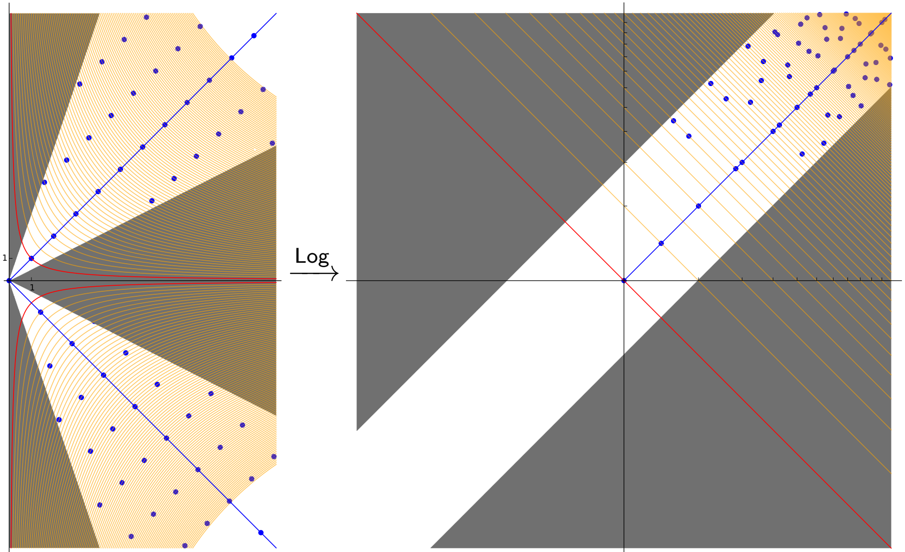
Reduction modulo $\Lambda = \mathrm{Log}\, \mathbb{Z}[\sqrt{2}]^\times$

The reduction modΛ for various fundamental domains.



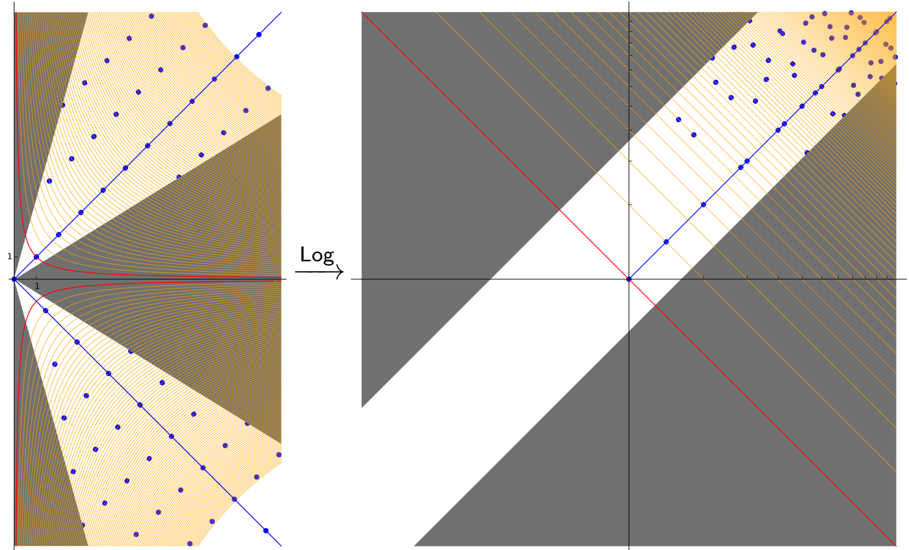
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

The reduction $\bmod \Lambda$ for various fundamental domains.



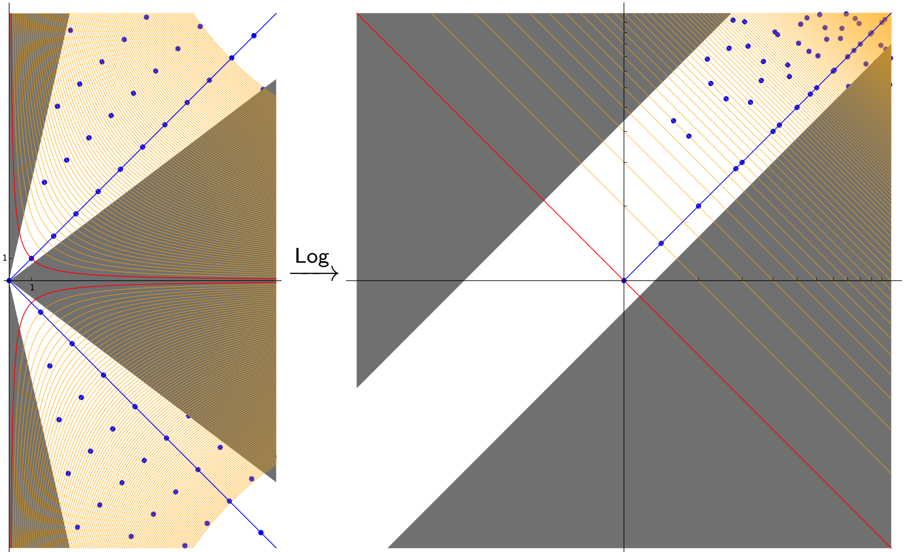
Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^\times$

The reduction $\bmod \Lambda$ for various fundamental domains.



Reduction modulo $\Lambda = \operatorname{Log} \mathbb{Z}[\sqrt{2}]^{\times}$

The reduction $\bmod \Lambda$ for various fundamental domains.



Strategy

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 $(\mathrm{Log}\, u_i)_i$ 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

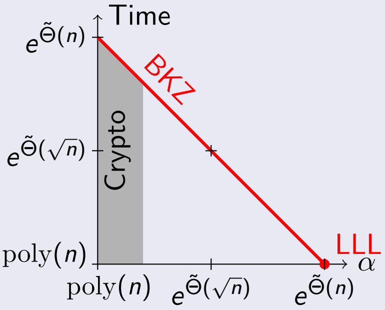
If there exists an unusually short generator g (as in certain crypto settings), we can recover it in classical poly-time from any generator $h = ug$.

Short Generator Recovery, worst-case

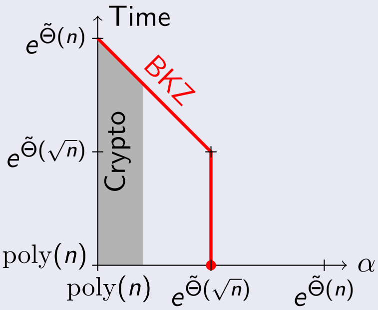
For any generator h, we can recover a generator g of length at most $\exp(\tilde{O}(\sqrt{n}))$ larger than the shortest vector of (h).

Comparison with General lattices

General Lattices



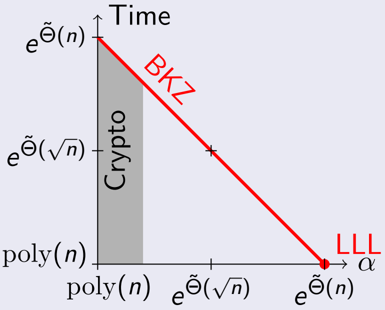
Principal Ideal lattices



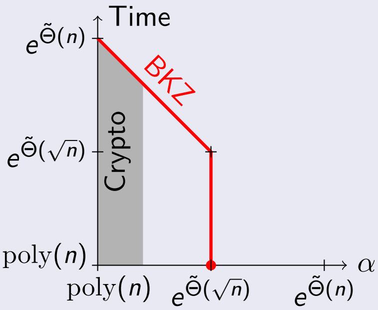
Can we remove the **Principality** condition ?

Comparison with General lattices

General Lattices



Principal Ideal lattices



Can we remove the **Principality** condition ?

Part 2:
Short Stickelberger's $\mathscr{C}\!\!\!\ell$ass relations

The obstacle: the Class Group

Ideals can be multiplied, and remain ideals:

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

The product of two principal ideals remains principal:

$$(a\mathscr{O}_K)(b\mathscr{O}_K) = (ab)\mathscr{O}_K.$$

$\mathscr{F}_K$ form an **abelian group**[1], $\mathscr{P}_K$ is a **subgroup** of it.

Definition (Class Group)

Their quotient forms the **class group** $\mathrm{Cl}_K = \mathscr{F}_K / \mathscr{P}_K$.
The class of an ideal $\mathfrak{a} \in \mathscr{F}_K$ is denoted $[\mathfrak{a}] \in \mathrm{Cl}_K$.

An ideal $\mathfrak{a}$ is principal iff $[\mathfrak{a}] = [\mathscr{O}_K]$.

[1] with neutral element $\mathscr{O}_K$

The obstacle: the Class Group

Ideals can be multiplied, and remain ideals:

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

The product of two principal ideals remains principal:

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

$\mathscr{F}_K$ form an **abelian group**[1], $\mathscr{P}_K$ is a **subgroup** of it.

Definition (Class Group)

Their quotient forms the **class group** $\mathrm{Cl}_K = \mathscr{F}_K / \mathscr{P}_K$.
The class of an ideal $\mathfrak{a} \in \mathscr{F}_K$ is denoted $[\mathfrak{a}] \in \mathrm{Cl}_K$.

An ideal $\mathfrak{a}$ is principal iff $[\mathfrak{a}] = [\mathcal{O}_K]$.

[1] with neutral element $\mathcal{O}_K$

The problem: Reducing to the principal case

Definition (The Close Principal Multiple problem)

- Given an ideal $\mathfrak{a}$, and an factor F
- Find a **small integral** ideal $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathscr{O}_K]$ and $N\mathfrak{b} \leq F$

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

Choose a factor basis $\mathfrak{B} = \{\mathfrak{p}_1 \dots \mathfrak{p}_n\}$ and restrict the search to $\mathfrak{b}$ of the form $\mathfrak{b} = \prod \mathfrak{p}_i^{v_i}$. I.e. solve the **short discrete-logarithm problem**

$$\vec{v} \in \mathrm{Log}_{\mathfrak{B}}([\mathfrak{a}]^{-1}).$$

How to solve it ?

Again, two steps:

- Find an arbitrary solution $\vec{v} \in \mathrm{Log}_{\mathfrak{B}}([\mathfrak{a}]^{-1})$
  [Eisentrager Kitaev Hallgren Song '14, Biasse Song '16]
- Reduce it modulo $\mathscr{L}$?

But do we even know $\mathscr{L} = \mathrm{Log}_{\mathfrak{B}}([\mathscr{O}_K])$?

Yes, we know $\mathscr{L}$! (Well Almost)

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

Definition (The Stickelberger ideal)

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

$$\theta = \sum \left(\frac{a}{m} \bmod 1 \right) \sigma_a^{-1} \qquad \text{where } G \ni \sigma_a : \omega \mapsto \omega^a.$$

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

Theorem (Stickelberger's theorem)

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

Turn-out: the natural basis of S is almost orthogonal... Again !

Yes, we know $\mathscr{L}$! (Well Almost)

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

Definition (The Stickelberger ideal)

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

$$\theta = \sum \left(\frac{a}{m} \bmod 1 \right) \sigma_a^{-1} \qquad \text{where } G \ni \sigma_a : \omega \mapsto \omega^a.$$

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

Theorem (Stickelberger's theorem)

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

Turn-out: the natural basis of S is almost orthogonal... Again !

Approx-Ideal-SVP in poly-time for large α

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

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

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

General Lattices

Ideal lattices

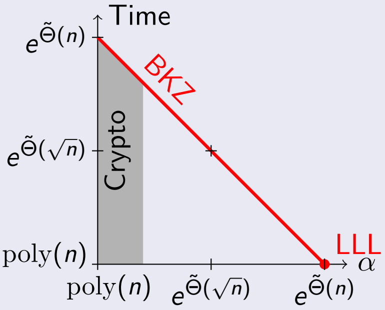
Approx-Ideal-SVP in poly-time for large α

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

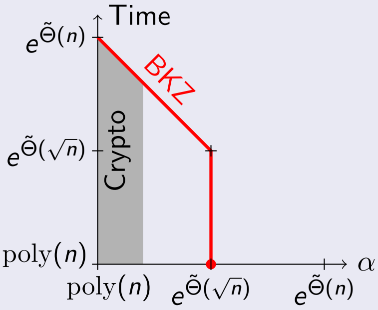
$\Rightarrow$ Approx-Ideal-SVP **solvable** in Quantum poly-time, for

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

General Lattices



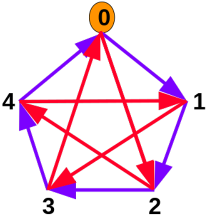
Ideal lattices



Takeaway: Dual viewpoint (Caley-Graphs and Lattices)

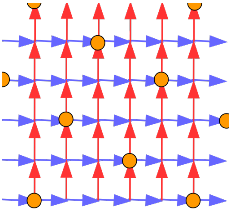
$$\mu : \vec{v} \in \mathbb{Z}^2 \mapsto v_1 + 2v_2 \bmod 5,\ \Lambda = \ker \mu,$$
$$\text{then } \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}^2/\Lambda$$

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



Distance
Diameter
Shortest loop
Mixing time

$\mathbb{Z}^{\{1,2\}}/\Lambda$



ℓ_1-distance mod Λ
Covering radius
Minimal vector
Smoothing parameter

Part 3:
Chor-Rivest dense $\mathscr{S}$phere-$\mathscr{P}$acking
with efficient decoding

Dense Lattice with Efficient Decoding

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

Bounded Distance Decoding with radius r

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

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

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

(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:

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

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

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 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 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 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 Lattice

Choose a factor basis of **small** primes, coprimes to $Q = 3^k$:
$\mathfrak{B} = \{2, 5, 7, 11, 13, \dots, p_n\} \subset \mathbb{Z}$, $[\cdot] : x \mapsto x \bmod Q$.

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

.

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

Decoding Chor-Rivest Lattice (positive errors)

If $p_n^r < Q$ then one can decode integral positive errors up to ℓ_1 radius r in the lattice $\mathscr{L}$. That is:

- given $t = v + e$, for $v \in \mathscr{L}$ and $e \in \mathbb{Z}^n_{\geq 0}$, $\|e\|_1 \leq r$
- we can efficiently recover v and e.

Compute

$$f = \prod p_i^{t_i} \bmod Q = \prod p_i^{v_i} \prod p_i^{e_i} \bmod Q = \prod p_i^{e_i} \bmod Q$$

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

Decoding Chor-Rivest Lattice

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

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

To recover $u = \prod_{i \text{ s.t. } e_i > 0}^{n} p_i^{e_i}$ 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 $f = u/v \bmod m$, then $\pm(u, v)$ are the shortests vector of the 2-dimensional lattice

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

In particular, given f and m, one can recover (u, v) in polynomial time.

Asymptotic parameters

Choose $k = n$. This gives

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

Compare to Minkowsky's bound in ℓ_1 norm:

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

By norm inequality this directly imply decoding in ℓ_2-norm for a radius

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

Compare to Minkowsky's bound in ℓ_2 norm:

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

Asymptotic parameters

Choose $k = n$. This gives

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

Compare to Minkowsky's bound in ℓ_1 norm:

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

By norm inequality this directly imply decoding in ℓ_2-norm for a radius

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

Compare to Minkowsky's bound in ℓ_2 norm:

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

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]** (ℓ_2 norm).

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

- We can construct $\mathscr{L}$ efficiently.
- We can solve BDD efficiently in $\mathscr{L}$
- We don't know how to find short vectors in $\mathscr{L}$...

The last mile ?

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]**

$\mathscr{T}$hanks for your interest.

$\mathscr{Q}$uestions ?

$\mathscr{O}$ther $\mathscr{L}$ogarithmic $\mathscr{L}$attices of interest ?

$\mathscr{T}$hanks for your interest.

$\mathscr{Q}$uestions ?

$\mathscr{O}$ther $\mathscr{L}$ogarithmic $\mathscr{L}$attices of interest ?