A Quantum Algorithm for Finding Midly Short Vectors in Cyclotomic Ideal Lattices

Léo Ducas
Based on Joint Work with
R. Cramer, O. Regev. C. Peikert, B. Wesolowski

Cryptology Group, CWI, Amsterdam, The Netherlands

Mathematics of Public Key Cryptography
Aussois, FR, March 2019

Lattice-Based Crypto

Lattice problems provide a strong fundation for Post-Quantum Crypto

Worst-case to average-case reduction [Ajt99, Reg09]

$$\text{Worst-case Approx-SVP} \leq \begin{cases} \text{SIS} & \text{(Short Intreger Solution)} \\ \text{LWE} & \text{(Learning With Errors)} \end{cases}$$

How hard is Approx-SVP ? Depends on the Approximation factor α.

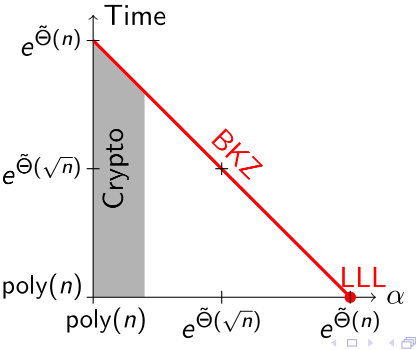
Lattice-Based Crypto

Lattice problems provide a strong fundation for Post-Quantum Crypto

Worst-case to average-case reduction [Ajt99, Reg09]

$$\text{Worst-case Approx-SVP} \leq \begin{cases} \text{SIS} & \text{(Short Intreger Solution)} \\ \text{LWE} & \text{(Learning With Errors)} \end{cases}$$

How hard is Approx-SVP ? Depends on the Approximation factor α.



Lattices over Rings (Ideals, Modules)

Generic lattices are cumbersome! Key-size $= \tilde{O}(n^2)$.

NTRU Cryptosystems [HPS98, HHGP+03]

Use the convolution ring $\mathcal{R} = R[X]/(X^p - 1)$, and module-lattices:

$$\mathcal{L}_h = \{(x, y) \in \mathcal{R}^2, \quad hx + y \equiv 0 \bmod q\}.$$

Same lattice dimension, Key-Size $= \tilde{O}(n)$. Later came variants with worst-case fundations:

wc-to-ac reduction [Mic07, LPR13]

$$\text{Worst-case Approx-Ideal-SVP} \leq \begin{cases} \text{Ring-SIS} \\ \text{Ring-LWE} \end{cases}$$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\zeta_m]$ (ζ_m a primitive m-th root of unity).

Denote $n = \deg \mathcal{R}$. In our cyclotomic cases: $n = \phi(m) \sim m$.

Lattices over Rings (Ideals, Modules)

Generic lattices are cumbersome! Key-size $= \tilde{O}(n^2)$.

NTRU Cryptosystems [HPS98, HHGP+03]

Use the convolution ring $\mathcal{R} = R[X]/(X^p - 1)$, and module-lattices:

$$\mathcal{L}_h = \{(x, y) \in \mathcal{R}^2, \quad hx + y \equiv 0 \bmod q\}.$$

Same lattice dimension, Key-Size $= \tilde{O}(n)$. Later came variants with worst-case fundations:

wc-to-ac reduction [Mic07, LPR13]

$$\text{Worst-case Approx-Ideal-SVP} \leq \begin{cases} \text{Ring-SIS} \\ \text{Ring-LWE} \end{cases}$$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\zeta_m]$ (ζ_m a primitive m-th root of unity).

Denote $n = \deg \mathcal{R}$. In our cyclotomic cases: $n = \phi(m) \sim m$.

Lattices over Rings (Ideals, Modules)

Generic lattices are cumbersome! Key-size $= \tilde{O}(n^2)$.

NTRU Cryptosystems [HPS98, HHGP+03]

Use the convolution ring $\mathcal{R} = R[X]/(X^p - 1)$, and module-lattices:

$$\mathcal{L}_h = \{(x, y) \in \mathcal{R}^2, \quad hx + y \equiv 0 \bmod q\}.$$

Same lattice dimension, Key-Size $= \tilde{O}(n)$. Later came variants with worst-case fundations:

wc-to-ac reduction [Mic07, LPR13]

$$\text{Worst-case Approx-Ideal-SVP} \leq \begin{cases} \text{Ring-SIS} \\ \text{Ring-LWE} \end{cases}$$

Applicable for cyclotomic rings $\mathcal{R} = \mathbb{Z}[\zeta_m]$ (ζ_m a primitive m-th root of unity).

Denote $n = \deg \mathcal{R}$. In our cyclotomic cases: $n = \phi(m) \sim m$.

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

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

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

Better tradeoffs

Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

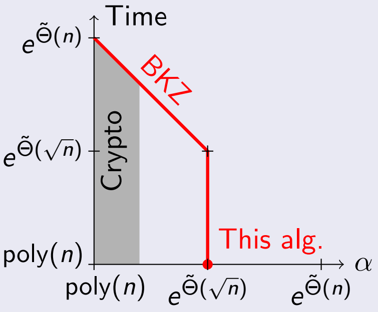
$\Rightarrow$ start favoring **weaker assumptions** ? e.g. Module-LWE

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

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

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

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

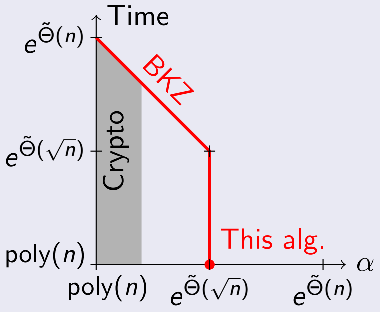
$\Rightarrow$ start favoring **weaker assumptions** ? e.g. Module-LWE

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

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

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

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

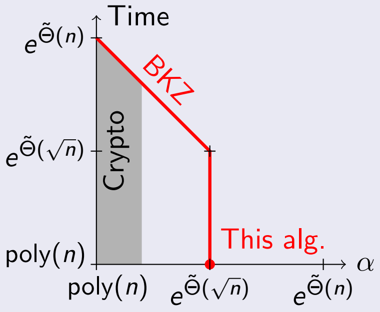
$\Rightarrow$ start favoring **weaker assumptions** ? e.g. Module-LWE

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

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

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

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

$\Rightarrow$ start favoring **weaker assumptions** ?
e.g. Module-LWE

Algebraic Number Theory

Ideals and Principal Ideals

Cyclotomic number field: $K(= \mathbb{Q}(\zeta_m))$, ring of integer $\mathcal{O}_K(= \mathbb{Z}[\zeta_m])$, where ζ_m is a formal m-th root of unity. The degree of K is $n = \varphi(m)$

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.

Ideals as Lattices

There is a Ring morphism (the empeddings):

$$K \to \mathbb{C}^n$$
$$\zeta \mapsto (\omega^i)_{i \in \mathbb{Z}_m^\times}$$

where $\omega \in \mathbb{C}$ is a complex m-th root of unity. This allows to view ideal as lattices.

- One can therefore view Ideal as lattices
- In the empedding space, multiplication is component-wise $\quad (\simeq \text{FFT})$

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:

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

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

Definition (Class Group)

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

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

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

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:

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

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

Definition (Class Group)

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

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

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

Lattice of Class Relations

Choose a factor basis: a set $\mathfrak{B} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ such that $\{[\mathfrak{p}_1], \dots, [\mathfrak{p}_k]\}$ generates Cl_K.
Consider the morphism

$$\phi : \mathbb{Z}^k \to \mathrm{Cl}_K$$
$$(x_1, \dots x_k) \mapsto \left[\prod \mathfrak{p}_i^{x_i}\right]$$

- The kernel $\Lambda = \ker \phi$ is the lattice of class relation over $\mathfrak{B}$.
- Reducing x_i modulo Λ : finding a small representative in the same class

Unit Group and Principal Ideals

- An element $g \in K^\times$ generates an ideal $g\mathcal{O}_K$ $(\approx GL_n(\mathbb{R}))$
- The unit group $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \text{ s.t. } x^{-1} \in \mathcal{O}_K\}$. $(\approx GL_n(\mathbb{Z}))$
- g and h generates the same ideal iff $g = uh$ for some unit $u \in \mathcal{O}_K$

$$\mathcal{P}_K \simeq K^\times / \mathcal{O}_K^\times$$

$$(\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z}))$$

- Unlike $\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z})$, the groups are *commutative* : reduction should be much easier...
- Spoiler: take the log and $\mathcal{O}_K^\times$ becomes a lattice !

Unit Group and Principal Ideals

- An element $g \in K^\times$ generates an ideal $g\mathcal{O}_K$ $(\approx GL_n(\mathbb{R}))$
- The unit group $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \text{ s.t. } x^{-1} \in \mathcal{O}_K\}$. $(\approx GL_n(\mathbb{Z}))$
- g and h generates the same ideal iff $g = uh$ for some unit $u \in \mathcal{O}_K$

$$\mathcal{P}_K \simeq K^\times / \mathcal{O}_K^\times$$

$$(\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z}))$$

- Unlike $\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z})$, the groups are *commutative* : reduction should be much easier...
- Spoiler: take the log and $\mathcal{O}_K^\times$ becomes a lattice !

Unit Group and Principal Ideals

- An element $g \in K^\times$ generates an ideal $g\mathcal{O}_K$ $\quad (\approx GL_n(\mathbb{R}))$
- The unit group $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \text{ s.t. } x^{-1} \in \mathcal{O}_K\}$. $\quad (\approx GL_n(\mathbb{Z}))$
- g and h generates the same ideal iff $g = uh$ for some unit $u \in \mathcal{O}_K$

$$\mathcal{P}_K \simeq K^\times / \mathcal{O}_K^\times$$

$$(\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z}))$$

- Unlike $\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z})$, the groups are *commutative* : reduction should be much easier...
- Spoiler: take the log and $\mathcal{O}_K^\times$ becomes a lattice !

Unit Group and Principal Ideals

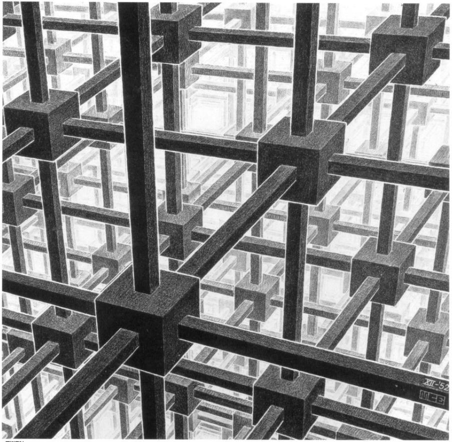
- An element $g \in K^\times$ generates an ideal $g\mathcal{O}_K$ $\qquad (\approx GL_n(\mathbb{R}))$
- The unit group $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \text{ s.t. } x^{-1} \in \mathcal{O}_K\}$. $\qquad (\approx GL_n(\mathbb{Z}))$
- g and h generates the same ideal iff $g = uh$ for some unit $u \in \mathcal{O}_K$

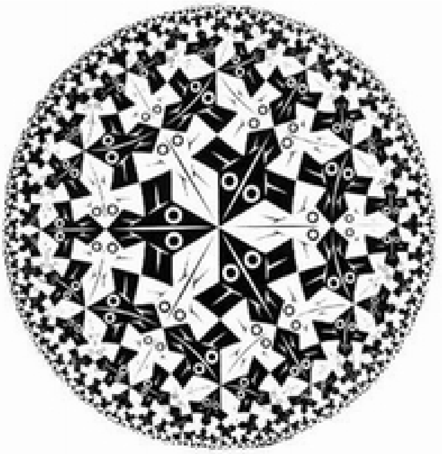
$$\mathcal{P}_K \simeq K^\times / \mathcal{O}_K^\times$$

$$(\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z}))$$

- Unlike $\{\text{lattices}\} \simeq GL_n(\mathbb{R})/GL_n(\mathbb{Z})$, the groups are *commutative* : reduction should be much easier...
- Spoiler: take the log and $\mathcal{O}_K^\times$ becomes a lattice !

Tesselation: commutative v.s. non-commutative





Overview

4 Steps to Ideal-SVP

The Close Principal Multiple Problem

Given an ideal $\mathfrak{a}$, find $\mathfrak{c} \subset \mathfrak{a}$ that is principal, and not much sparser

1. Find a representative $\prod \mathfrak{p}_i^{x_i}$ of $[\mathfrak{a}^{-1}]$ [EHKS14, BS15]
2. Make the x_i small by reducing modulo class relations [CDW17]

$\Rightarrow$ Output $\mathfrak{c} = \mathfrak{a} \cdot \prod \mathfrak{p}_i^{x_i}$

Short Generator Problem

Given a principal ideal $\mathfrak{c}$, find a short generator g of $\mathfrak{c}$

3. Find any generator g of $\mathfrak{c}$ [EHKS14, BS15]
4. Reduce g modulo the unit group $\mathcal{O}_K^\times$ [CDPR16]

$\Rightarrow$ Output g

This talk

Working Hypothesis

$$|\text{Quantum}\rangle = \mathfrak{Magic}$$

We will focus on the following steps:

2. Make the x_i small by reducing modulo class relations [CDW17]
4. Reduce g modulo the unit group $\mathcal{O}_K^\times$ [CDPR16]

For a survey covering all the steps, refer to [Duc17].

The Close Principal Multiple Problem

From CPM to Ideal-SVP

Definition (The Close Principal Multiple problem)

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

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

Factor Basis, Class-Group Discrete-Log

Choose a **factor basis** $\mathfrak{B}$ of integral ideals and search $\mathfrak{b}$ of the form:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{e_\mathfrak{p}}.$$

We choose $|\mathfrak{B}|$ small (say n) and $\mathfrak{p} \in \mathfrak{B}$ small as well $N\mathfrak{p} = \mathrm{poly}(n)$.

Corollary (Quantum Cl-Discrete Logarithm,[BS15])

Assume $\mathfrak{B}$ generates the class-group. Given $\mathfrak{a}$ and $\mathfrak{B}$, one can find in quantum polynomial time a vector $\mathbf{e} \in \mathbb{Z}^{\mathfrak{B}}$ such that:

$$\prod_{\mathfrak{p} \in \mathfrak{B}} [\mathfrak{p}^{e_\mathfrak{p}}] = [\mathfrak{a}^{-1}].$$

This finds a $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$, yet:

- $\mathfrak{b}$ may not be integral (negative exponents, yet easy to solve)
- $N\mathfrak{b} \approx \exp(\|\mathbf{e}\|_1)$ may be huge (unbounded $\mathbf{e}$, want $\|\mathbf{e}\|_1 = \tilde{O}(n^{3/2})$).

Factor Basis, Class-Group Discrete-Log

Choose a **factor basis** $\mathfrak{B}$ of integral ideals and search $\mathfrak{b}$ of the form:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{e_\mathfrak{p}}.$$

We choose $|\mathfrak{B}|$ small (say n) and $\mathfrak{p} \in \mathfrak{B}$ small as well $N\mathfrak{p} = \mathrm{poly}(n)$.

Corollary (Quantum Cl-Discrete Logarithm,[BS15])

Assume $\mathfrak{B}$ generates the class-group. Given $\mathfrak{a}$ and $\mathfrak{B}$, one can find in quantum polynomial time a vector $\mathbf{e} \in \mathbb{Z}^{\mathfrak{B}}$ such that:

$$\prod_{\mathfrak{p} \in \mathfrak{B}} \left[\mathfrak{p}^{e_\mathfrak{p}}\right] = \left[\mathfrak{a}^{-1}\right].$$

This finds a $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$, yet:

- $\mathfrak{b}$ may not be integral (negative exponents, yet easy to solve)
- $N\mathfrak{b} \approx \exp(\|\mathbf{e}\|_1)$ may be huge (unbounded $\mathbf{e}$, want $\|\mathbf{e}\|_1 = \tilde{O}(n^{3/2})$).

Factor Basis, Class-Group Discrete-Log

Choose a **factor basis** $\mathfrak{B}$ of integral ideals and search $\mathfrak{b}$ of the form:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}^{e_\mathfrak{p}}.$$

We choose $|\mathfrak{B}|$ small (say n) and $\mathfrak{p} \in \mathfrak{B}$ small as well $N\mathfrak{p} = \mathrm{poly}(n)$.

Corollary (Quantum Cl-Discrete Logarithm,[BS15])

Assume $\mathfrak{B}$ generates the class-group. Given $\mathfrak{a}$ and $\mathfrak{B}$, one can find in quantum polynomial time a vector $\mathbf{e} \in \mathbb{Z}^{\mathfrak{B}}$ such that:

$$\prod_{\mathfrak{p} \in \mathfrak{B}} \left[\mathfrak{p}^{e_\mathfrak{p}}\right] = \left[\mathfrak{a}^{-1}\right].$$

This finds a $\mathfrak{b}$ such that $[\mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K]$, yet:

- $\mathfrak{b}$ may not be integral (negative exponents, yet easy to solve)
- $N\mathfrak{b} \approx \exp(\|\mathbf{e}\|_1)$ may be huge (unbounded $\mathbf{e}$, want $\|\mathbf{e}\|_1 = \tilde{O}(n^{3/2})$).

Navigating the Class-Group

Cayley-Graph(G, A):

- A node for any element $g \in G$
- An arrow $g \xrightarrow{a} ga$ for any $g \in G$, $a \in A$

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

Rephrased Goal for CPM

Find a **short** path from $[\mathfrak{a}]$ to $[\mathcal{O}_K]$ in Cayley-Graph$(\mathrm{Cl}, \mathfrak{B})$.

- Using a few well chosen ideals in $\mathfrak{B}$, Cayley-Graph$(\mathrm{Cl}, \mathfrak{B})$ is an **expander Graph** [JW15]: very short paths exist.
- Finding such short path generically too costly: $|\mathrm{Cl}| > \exp(n)$

A lattice problem

Cl is **abelian** and **finite**, so $\mathrm{Cl} = \mathbb{Z}^{\mathfrak{B}}/\Lambda$ for some lattice Λ:

$$\Lambda = \left\{ \mathbf{e} \in \mathbb{Z}^{\mathfrak{B}}, \quad s.t. \prod [\mathfrak{p}_{\mathfrak{p}}^{e}] = [\mathcal{O}_K] \right\}$$

i.e. the (full-rank) **lattice of class-relations** in base $\mathfrak{B}$.

Figure: $(\mathbb{Z}/5\mathbb{Z}, +) = \mathbb{Z}^{\{1,2\}}/\Lambda$

Rephrased Goal for CPM: CVP in Λ

Find a **short** path from $t \in \mathbb{Z}^{\mathfrak{B}}$ to any lattice point $v \in \Lambda$.

In general: very hard. But for good Λ, with a good basis, can be easy.

Why should we know anything special about Λ ?

A lattice problem

Cl is **abelian** and **finite**, so $\mathrm{Cl} = \mathbb{Z}^{\mathfrak{B}}/\Lambda$ for some lattice Λ:

$$\Lambda = \left\{ \mathbf{e} \in \mathbb{Z}^{\mathfrak{B}}, \quad s.t. \prod [\mathfrak{p}_{\mathfrak{p}}^{e}] = [\mathcal{O}_K] \right\}$$

i.e. the (full-rank) **lattice of class-relations** in base $\mathfrak{B}$.

Figure: $(\mathbb{Z}/5\mathbb{Z}, +) = \mathbb{Z}^{\{1,2\}}/\Lambda$

Rephrased Goal for CPM: CVP in Λ

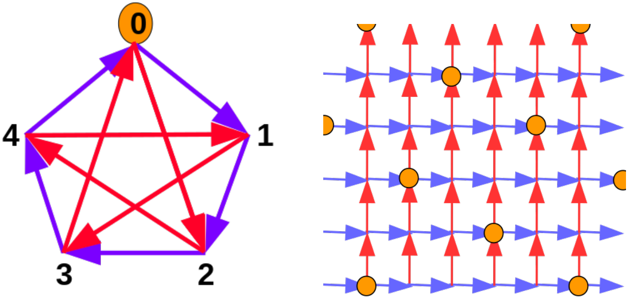
Find a **short** path from $t \in \mathbb{Z}^{\mathfrak{B}}$ to any lattice point $v \in \Lambda$.

In general: very hard. But for good Λ, with a good basis, can be easy.

Why should we know anything special about Λ ?

Example

Figure: Cayley-Graph$(\mathbb{Z}/5\mathbb{Z}, \{1,2\}) \quad \simeq \quad \mathbb{Z}^{\{1,2\}}/\Lambda$



More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^\mathfrak{B}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^\mathfrak{B}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

More than just a lattice

Let G denote the Galois group, it acts on ideals and therefore on classes:

$$[\mathfrak{a}]^\sigma = [\sigma(\mathfrak{a})].$$

Consider the **group-ring** $\mathbb{Z}[G]$ (formal sums on G), extend the G-action:

$$[\mathfrak{a}]^e = \prod_{\sigma \in G} [\sigma(\mathfrak{a})]^{e_\sigma} \qquad \text{where } e = \sum e_\sigma \sigma.$$

- Assume $\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$
- G acts on $\mathfrak{B}$, and so it acts on $\mathbb{Z}^{\mathfrak{B}}$ by permuting coordinates
- the lattice $\Lambda \subset \mathbb{Z}^{\mathfrak{B}}$ is **invariant** by the action of G !

i.e. Λ admits G as a group of **symmetries**

Λ is more than just a lattice: it is a $\mathbb{Z}[G]$-**module**

Stickelberger's Theorem

In fact, we know much more about Λ !

Definition (The Stickelberger ideal)

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

$$\theta = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} \left(\frac{a}{m} \bmod 1 \right) \sigma_a^{-1} \qquad \text{where } G \ni \sigma_a : \omega \mapsto \omega^a.$$

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

Theorem (Stickelberger's theorem)

The Stickelberger ideal annihilates the class group: $\forall e \in S, \mathfrak{a} \subset K$

$$[\mathfrak{a}^e] = [\mathcal{O}_K].$$

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

Geometry of the Stickelberger ideal

Fact

There exists an **explicit** *(efficiently computable)* **short** *basis of S, namely it has ternary coefficients.*

Corollary

Given $t \in \mathbb{Z}[G]$, one can find $x \in S$ suh that $\|x - t\|_1 \leq n^{3/2}$.

Conclusion: back to CPM

Extra technicalities

Convenient simplifications/omissions made so far:

$\mathfrak{B} = \{\mathfrak{p}^\sigma, \sigma \in G\}$ generates the class group.

- can allow a few (say polylog) many different ideals and their conjugates in $\mathfrak{B}$
- Numerical computation says such $\mathfrak{B}$ should exist [Sch98]
- Theorem+Heuristic then say we can find such $\mathfrak{B}$ efficiently

Eliminating minus exponents

- Easy when $h^+ = 1$: $[\mathfrak{a}^{-1}] = [\bar{\mathfrak{a}}]$, doable when $h^+ = \mathrm{poly}(n)$. [a]
- Justified by numerical computations and heuristics

[BPR04, Sch03]

[a] h^+ is the size of the class group of K^+, the max. real subfield of K

The Short Generator Problem

Invocation of $|\text{Quantum}\rangle$ $\mathfrak{Magic}$

Given an ideal $\mathfrak{c}$, one can find a generator h of it using a quantum computer. [EHKS14, Bia14]

The Logarithmic Embedding

The n embeddings $\sigma_i : K \mapsto \mathbb{C}$ for i for $i \in \mathbb{Z}_m^\times$ are given by

$$\sigma_i(\zeta) = \omega^i$$

The logarithmic Embedding is defined as

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^{n/2} \\ x &\mapsto (\log|\sigma_i(x)|)_{i \in \mathbb{Z}_m^\times/\pm 1} \end{aligned}$$

It induces

- a group morphism from $(K \setminus \{0\}, \cdot)$ to $(\mathbb{R}^{n/2}, +)$
- a monoid morphism from $(R \setminus \{0\}, \cdot)$ to $(\mathbb{R}^n/2, +)$

The Unit Group

By Dirichlet Unit Theorem

- the kernel of Log is the cyclic group T of roots of unity of $\mathcal{O}_K$
- $\operatorname{Log} \mathcal{O}_K^\times \subset \mathbb{R}^n$ is an lattice of rank $r + c - 1$
  (where K has r real embeddings and $2c$ complex embeddings)

Reduction modulo $\mathcal{O}_K$: a Close Vector Problem

Elements $g, h \in K$ generate the same ideal if and only if $h = g \cdot u$ for some unit $u \in \mathcal{O}_K^\times$. In particular

$$\operatorname{Log} g \in \operatorname{Log} h + \operatorname{Log} \mathcal{O}_K^\times.$$

and g is the "smallest" generator iff $\operatorname{Log} u \in \operatorname{Log} \mathcal{O}_K^\times$ is a vector "closest" to $\operatorname{Log} h$.

The Unit Group

By Dirichlet Unit Theorem

- the kernel of Log is the cyclic group T of roots of unity of $\mathcal{O}_K$
- $\operatorname{Log} \mathcal{O}_K^\times \subset \mathbb{R}^n$ is an lattice of rank $r + c - 1$
  (where K has r real embeddings and $2c$ complex embeddings)

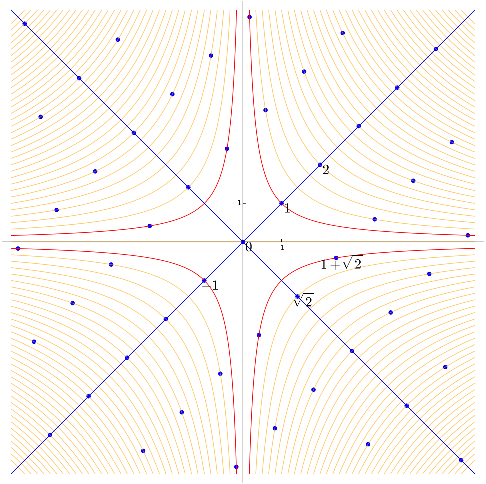
Reduction modulo $\mathcal{O}_K$: a Close Vector Problem

Elements $g, h \in K$ generate the same ideal if and only if $h = g \cdot u$ for some unit $u \in \mathcal{O}_K^\times$. In particular

$$\operatorname{Log} g \in \operatorname{Log} h + \operatorname{Log} \mathcal{O}_K^\times.$$

and g is the “smallest” generator iff $\operatorname{Log} u \in \operatorname{Log} \mathcal{O}_K^\times$ is a vector “closest” to $\operatorname{Log} h$.

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$



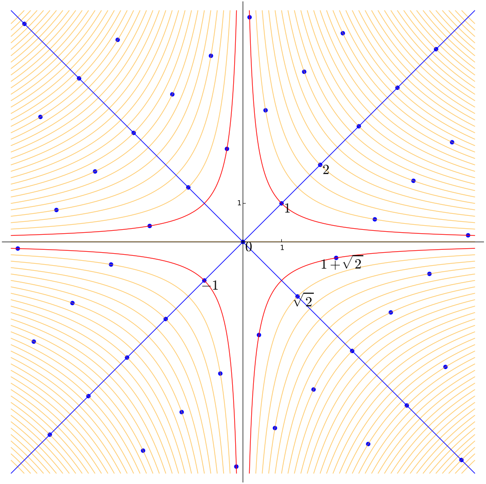
- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication
- Symmetries induced by
  - mult. by -1
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

"Orthogonal" elements

Units (algebraic norm 1)

"Isonorms" curves

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$



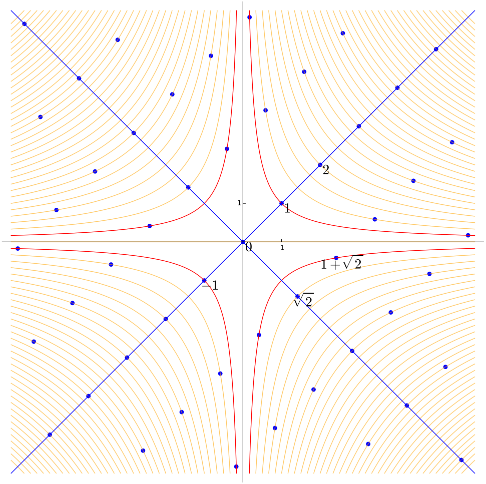
- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication
- Symmetries induced by
  - mult. by -1
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

"Orthogonal" elements

Units (algebraic norm 1)

"Isonorms" curves

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$



- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication

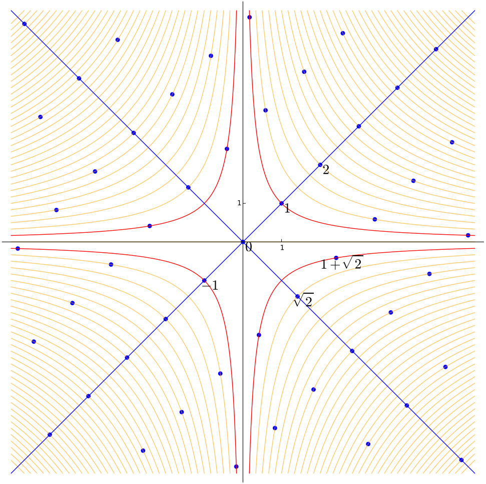
- Symmetries induced by
  - mult. by -1
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

"Orthogonal" elements

Units (algebraic norm 1)

"Isonorms" curves

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

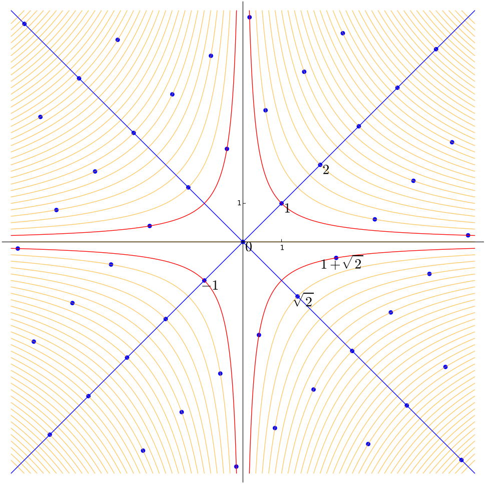


- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication

- Symmetries induced by
  - mult. by -1
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

- "Orthogonal" elements
- Units (algebraic norm 1)
- "Isonorms" curves

Example: Embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

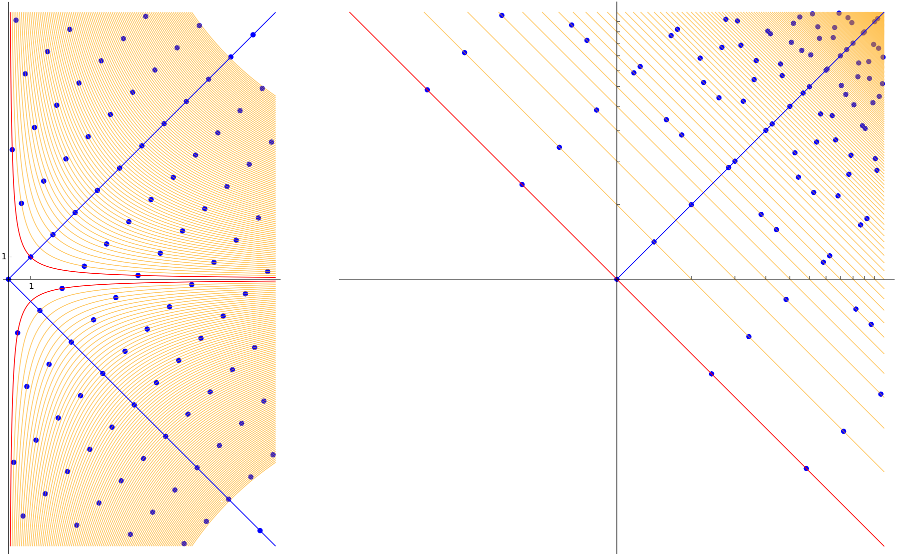


- x-axis: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$
- y-axis: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$
- component-wise multiplication

- Symmetries induced by
  - mult. by -1
  - conjugation $\sqrt{2} \mapsto -\sqrt{2}$

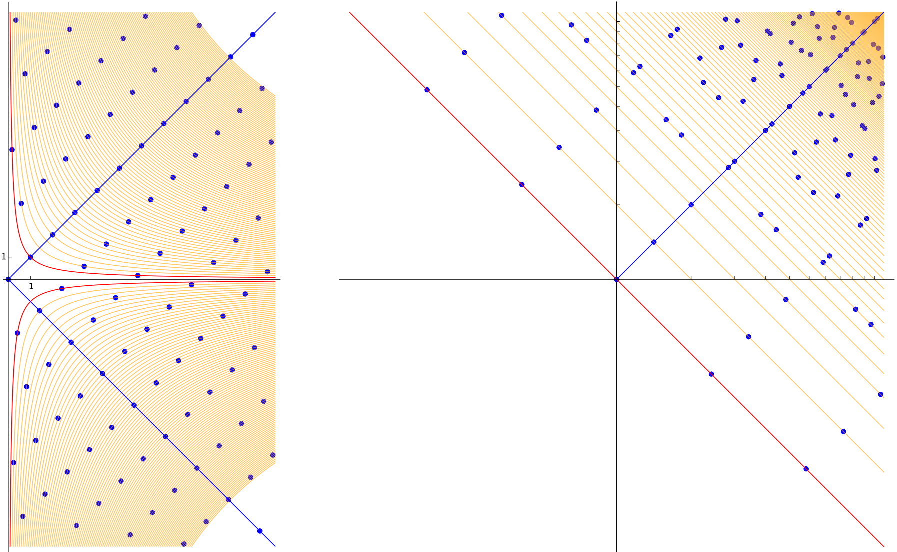
- "Orthogonal" elements
- Units (algebraic norm 1)
- "Isonorms" curves

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



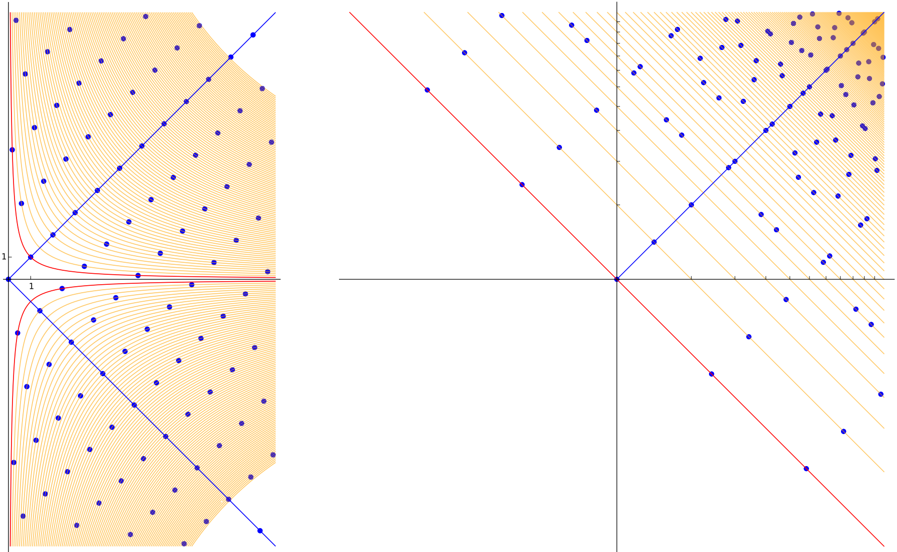
Example: Logarithmic Embedding $\operatorname{Log} \mathbb{Z}[\sqrt{2}]$

$\operatorname{Log} \mathcal{O}_K^\times = (\{\bullet\}, +) \cap \diagdown$ is a lattice of $\mathbb{R}^2$, orthogonal to $(1, 1)$



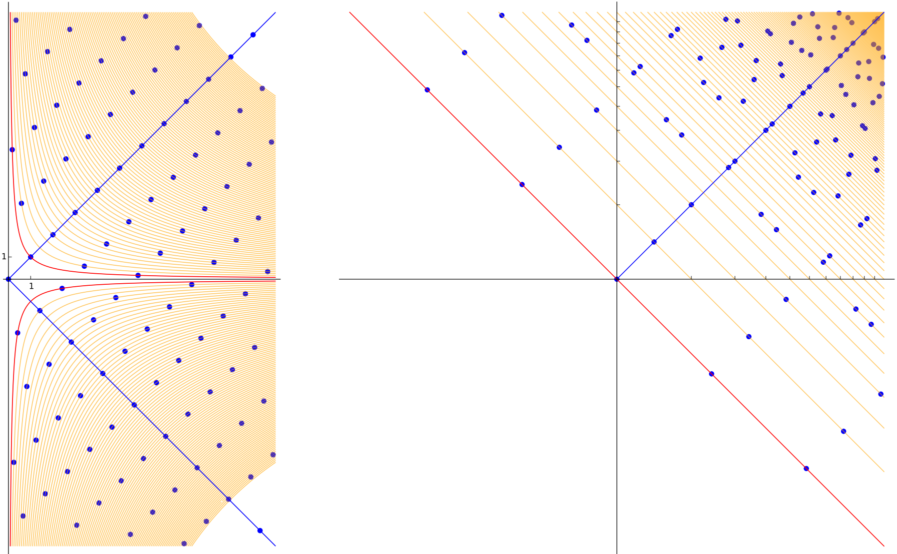
Example: Logarithmic Embedding $\mathrm{Log}\,\mathbb{Z}[\sqrt{2}]$

$\{\bullet\} \cap \diagdown$ are shifted finite copies of $\mathrm{Log}\,\mathcal{O}_K^\times$



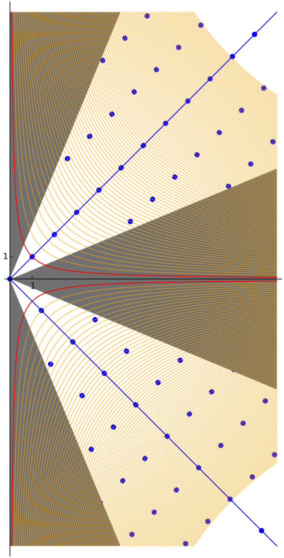
Example: Logarithmic Embedding $\mathrm{Log}\,\mathbb{Z}[\sqrt{2}]$

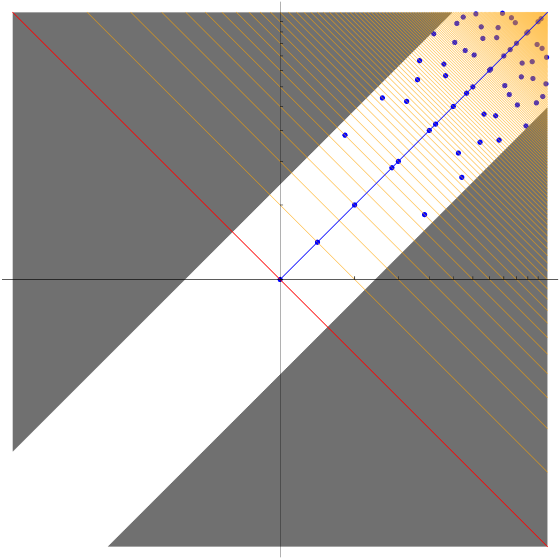
Some $\{\bullet\} \cap$ ╲ may be empty (e.g. no elements of Norm 3 in $\mathbb{Z}[\sqrt{2}]$)



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

The reduction modulo $\mathbb{Z}[\sqrt{2}]^\times$.





Cyclotomic units

Let's assume $m = p^k$ for some prime p.

$$z_j = 1 - \zeta^j \quad \text{and } b_j = z_j / z_1 \text{ for all } j \text{ coprimes with } m.$$

The b_j are units, and the group C generated by

$$\zeta, \quad b_j \quad \text{for } j = 2, \ldots m/2, j \text{ coprime with } m$$

is known as the group of *cyclotomic units*.

Simplification 1 (Weber's Class Number Problem)

We assume[2] that $\mathcal{O}_K^\times = C$. It is conjectured to be true for $m = 2^k$.

Simplification 2 (for this talk)

We study the dual matrix $\mathbf{Z}^\vee$, where $\mathbf{z}_j = \operatorname{Log} z_j$.
It can be proved to close to $\mathbf{B}^\vee$ where $\mathbf{b}_j = \mathbf{z}_j - \mathbf{z}_1$.

[2] One just need the index $[\mathcal{O}_K^\times : C] = h^+(m)$ to be small.

Cyclotomic units

Let's assume $m = p^k$ for some prime p.

$$z_j = 1 - \zeta^j \quad \text{and } b_j = z_j / z_1 \text{ for all } j \text{ coprimes with } m.$$

The b_j are units, and the group C generated by

$$\zeta, \quad b_j \quad \text{for } j = 2, \ldots m/2, j \text{ coprime with } m$$

is known as the group of *cyclotomic units*.

Simplification 1 (Weber's Class Number Problem)

We assume[2] that $\mathcal{O}_K^\times = C$. It is conjectured to be true for $m = 2^k$.

Simplification 2 (for this talk)

We study the dual matrix $\mathbf{Z}^\vee$, where $\mathbf{z}_j = \operatorname{Log} z_j$.
It can be proved to close to $\mathbf{B}^\vee$ where $\mathbf{b}_j = \mathbf{z}_j - \mathbf{z}_1$.

[2]One just need the index $[\mathcal{O}_K^\times : C] = h^+(m)$ to be small.

Cyclotomic units

Let's assume $m = p^k$ for some prime p.

$$z_j = 1 - \zeta^j \quad \text{and } b_j = z_j / z_1 \text{ for all } j \text{ coprimes with } m.$$

The b_j are units, and the group C generated by

$$\zeta, \quad b_j \quad \text{for } j = 2, \ldots m/2, j \text{ coprime with } m$$

is known as the group of *cyclotomic units*.

Simplification 1 (Weber's Class Number Problem)

We assume[2] that $\mathcal{O}_K^\times = C$. It is conjectured to be true for $m = 2^k$.

Simplification 2 (for this talk)

We study the dual matrix $\mathbf{Z}^\vee$, where $\mathbf{z}_j = \operatorname{Log} z_j$.
It can be proved to close to $\mathbf{B}^\vee$ where $\mathbf{b}_j = \mathbf{z}_j - \mathbf{z}_1$.

[2] One just need the index $[\mathcal{O}_K^\times : C] = h^+(m)$ to be small.

How good is this basis

- It is quite easy to prove that $\|\mathbf{z}_i\| \leq O(\sqrt{m})$.
- $\Rightarrow$ One can solve CVP with ℓ_∞ distance $\leq O(\sqrt{n} \log n)$.
- $\Rightarrow$ we can find a generator of length $\|g\| \leq \exp(O(\sqrt{n} \log n)) \cdot (N\mathfrak{c})^{1/n}$.

QED

Recall that the principal ideal $\mathfrak{c} \subset \mathfrak{a}$ verified $N\mathfrak{c} \leq \exp(n^{3/2}) N\mathfrak{a}$. That gives $g \in \mathfrak{a}$:

$$\|g\| \leq \exp(\sqrt{n} \log n) \cdot \mathrm{vol}(\mathfrak{a})^{1/n}.$$

We have solved Ideal-SVP with approximation fact $\exp(O(\sqrt{n} \log n))$

Don't leave !

More fun with $\operatorname{Log} \mathcal{O}_K^\times$...

How well can we solve BDD in this lattice ?

This actually has devastating consequence for 'atypical' crypto schemes (Soliloquy and the first generation of Fully Homomorphic Encryption Scheme)

Round-Off Decoding

We also need the fundamental domain to have an efficient reduction algorithm. The simplest one follows:

$\textsc{RoundOff}(\mathbf{B}, \mathbf{t})$ for $\mathbf{B}$ a basis of Λ

- Return $\mathbf{B} \cdot \lfloor \mathbf{B}^{-1} \cdot \mathbf{t} \rceil$.

Used as a decoding algorithm, its correctness is characterized by the error $\mathbf{e}$ and the *dual basis* $\mathbf{B}^\vee = \mathbf{B}^{-T}$.

Fact

Suppose $\mathbf{t} = \mathbf{v} + \mathbf{e}$ for some $\mathbf{v} \in \Lambda$. If $\langle \mathbf{b}_j^\vee, \mathbf{e} \rangle \in [-\frac{1}{2}, \frac{1}{2})$ for all j, then

$$\textsc{Round}(\mathbf{B}, \mathbf{t}) = \mathbf{v}.$$

Dual of a Circulant Basis

Notice that $\mathbf{Z}_{ij} = \log|\sigma_j(1-\zeta^i)| = \log|1-\omega^{ij}|$:
the matrix $\mathbf{Z}$ is G-circulant for the cyclic group $G = \mathbb{Z}_m^\times / \pm 1$.

Fact

If $\mathbf{M}$ is a non-singular, G-circulant matrix, then

- *its eigenvalues are given by $\lambda_\chi = \sum_{g\in G} \overline{\chi(g)} \cdot \mathbf{M}_{1,g}$ where $\chi \in \widehat{G}$ is a character $G \to \mathbb{C}$*
- *All the vectors of $\mathbf{M}^\vee$ have the same norm $\|\mathbf{m}_i^\vee\|^2 = \sum_{\chi\in\widehat{G}} |\lambda_\chi|^{-2}$*

Note: The characters of G can be extended to even Dirichlet characters mod m: $\chi : \mathbb{Z} \to \mathbb{C}$, by setting $\chi(a) = 0$ if $\gcd(a, m) > 1$.

Dual of a Circulant Basis

Notice that $\mathbf{Z}_{ij} = \log|\sigma_j(1-\zeta^i)| = \log|1-\omega^{ij}|$:
the matrix $\mathbf{Z}$ is G-circulant for the cyclic group $G = \mathbb{Z}_m^\times / \pm 1$.

Fact

If $\mathbf{M}$ *is a non-singular, G-circulant matrix, then*

- *its eigenvalues are given by* $\lambda_\chi = \sum_{g\in G} \overline{\chi(g)} \cdot \mathbf{M}_{1,g}$
  where $\chi \in \widehat{G}$ *is a character* $G \to \mathbb{C}$
- *All the vectors of* $\mathbf{M}^\vee$ *have the same norm* $\|\mathbf{m}_i^\vee\|^2 = \sum_{\chi\in\widehat{G}} |\lambda_\chi|^{-2}$

Note: The characters of G can be extended to even Dirichlet characters mod m: $\chi : \mathbb{Z} \to \mathbb{C}$, by setting $\chi(a) = 0$ if $\gcd(a, m) > 1$.

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log |1 - \omega^a|.$$

We develop using the Taylor series

$$\log |1 - x| = - \sum_{k \geq 1} x^k / k$$

and obtain

$$-\lambda_\chi = \sum_{a \in G} \sum_{k \geq 1} \overline{\chi(a)} \cdot \frac{\omega^{ka}}{k}.$$

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log|1 - \omega^a|.$$

We develop using the Taylor series

$$\log|1 - x| = -\sum_{k \geq 1} x^k / k$$

and obtain

$$-\lambda_\chi = \sum_{a \in G} \sum_{k \geq 1} \overline{\chi(a)} \cdot \frac{\omega^{ka}}{k}.$$

Computing the Eigenvalues

We wish to give a lower bound on $|\lambda_\chi|$ where

$$\lambda_\chi = \sum_{a \in G} \overline{\chi(a)} \cdot \log |1 - \omega^a|.$$

We develop using the Taylor series

$$\log |1 - x| = -\sum_{k \geq 1} x^k / k$$

and obtain

$$-\lambda_\chi = \sum_{a \in G} \sum_{k \geq 1} \overline{\chi(a)} \cdot \frac{\omega^{ka}}{k}.$$

Computing the Eigenvalues (continued)

We were trying to lower bound $|\lambda_\chi|$ where

$$-\lambda_\chi = \sum_{k\geq 1} \frac{1}{k} \cdot \sum_{a \in G} \overline{\chi(a)} \cdot \omega^{ka}.$$

Fact (Separability of Gauss Sums)

If χ is a primitive Dirichlet character $\bmod m$ *then*

$$\sum_{a \in \mathbb{Z}_m^\times} \overline{\chi(a)} \cdot \omega^{ka} = \chi(k) \cdot G(\chi) \quad \text{where } |G(\chi)| = \sqrt{m}.$$

For this talk, let's ignore non-primitive characters. We rewrite

$$|\lambda_\chi| = \sqrt{\frac{m}{2}} \cdot \left| \sum_{k \geq 1} \frac{\chi(k)}{k} \right|.$$

Computing the Eigenvalues (continued)

We were trying to lower bound $|\lambda_\chi|$ where

$$-\lambda_\chi = \sum_{k \geq 1} \frac{1}{k} \cdot \sum_{a \in G} \overline{\chi(a)} \cdot \omega^{ka}.$$

Fact (Separability of Gauss Sums)

If χ is a primitive Dirichlet character $\bmod m$ *then*

$$\sum_{a \in \mathbb{Z}_m^\times} \overline{\chi(a)} \cdot \omega^{ka} = \chi(k) \cdot G(\chi) \quad \text{where } |G(\chi)| = \sqrt{m}.$$

For this talk, let's ignore non-primitive characters. We rewrite

$$|\lambda_\chi| = \sqrt{\frac{m}{2}} \cdot \left| \sum_{k \geq 1} \frac{\chi(k)}{k} \right|.$$

Computing the Eigenvalues (continued)

We were trying to lower bound $|\lambda_\chi|$ where

$$-\lambda_\chi = \sum_{k \geq 1} \frac{1}{k} \cdot \sum_{a \in G} \overline{\chi(a)} \cdot \omega^{ka}.$$

Fact (Separability of Gauss Sums)

If χ is a primitive Dirichlet character $\bmod m$ *then*

$$\sum_{a \in \mathbb{Z}_m^\times} \overline{\chi(a)} \cdot \omega^{ka} = \chi(k) \cdot G(\chi) \quad \textit{where } |G(\chi)| = \sqrt{m}.$$

For this talk, let's ignore non-primitive characters. We rewrite

$$|\lambda_\chi| = \sqrt{\frac{m}{2}} \cdot \left| \sum_{k \geq 1} \frac{\chi(k)}{k} \right|.$$

The Analytic Hammer

We were trying to lower bound $|\lambda_\chi| = \sqrt{\frac{m}{2}} \cdot \left|\sum_{k\geq 1} \frac{\chi(k)}{k}\right|$.
One recognizes a Dirichlet L-series

$$L(s,\chi) = \sum \frac{\chi(k)}{k^s}.$$

Theorem ([Lit24, LLS15])

For any primitive non-quadratic Dirichlet character $\chi \bmod m$ it holds that

$$1/\ell(m) \leq |L(1,\chi)| \leq \ell(m) \qquad \textit{where } \ell(m) = C \ln m$$

for some universal constant $C > 0$.

The Analytic Hammer

We were trying to lower bound $\left|\lambda_\chi\right| = \sqrt{\frac{m}{2}} \cdot \left|\sum_{k\geq 1} \frac{\chi(k)}{k}\right|$.
One recognizes a Dirichlet L-series

$$L(s,\chi) = \sum \frac{\chi(k)}{k^s}.$$

Theorem ([Lit24, LLS15])

For any primitive non-quadratic Dirichlet character χ mod m *it holds that*

$$1/\ell(m) \leq |L(1,\chi)| \leq \ell(m) \qquad \textit{where } \ell(m) = C \ln m$$

for some universal constant $C > 0$.

Conclusion

Theorem

Then, all the vectors of $\mathbf{B}^\vee$ *have the same norm and, this norm is upper bounded as follows*

$$\left\|\mathbf{b}_j^\vee\right\|^2 \leq O\left(m^{-1} \cdot \log^3 m\right).$$

Further work

D., Plancon, Wesolowski 2019

- Analyse the hidden factors behind $\tilde{O}$'s.
- Predict when this algorithm outperform LLL and BKZ

Hanrot, Stehle and Pellet–Mary 2019

- Using some precomputation depending only on the number field K
- Generalize this results to any number field K
- Generalize to a time/approx-factor trade-off

$$T = \exp(\tilde{O}(n^c)), \alpha = \exp(\tilde{O}(n^{(1-c)/2}))$$

References I

Miklós Ajtai.
Generating hard instances of the short basis problem.
In *ICALP*, pages 1–9, 1999.

Jean-François Biasse.
Subexponential time relations in the class group of large degree number fields.
Adv. Math. Commun., 8(4):407–425, 2014.

Joe Buhler, Carl Pomerance, and Leanne Robertson.
Heuristics for class numbers of prime-power real cyclotomic fields.
Fields Inst. Commun, 41:149–157, 2004.

J.-F. Biasse and F. Song.
A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields.
`http://www.lix.polytechnique.fr/Labo/Jean-Francois.Biasse/`, 2015.
In preparation.

Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev.
Recovering short generators of principal ideals in cyclotomic rings.
Eurocrypt 2016, 2016.

References II

Ronald Cramer, Léo Ducas, and Benjamin Wesolowski.
Short stickelberger class relations and application to ideal-svp.
Eurocrypt 2017, 2017.

Léo Ducas.
Advances on quantum cryptanalysis of ideal lattices.
Nieuw Archief voor Wiskunde, 5:184–189, 2017.

Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song.
A quantum algorithm for computing the unit group of an arbitrary degree number field.
In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 293–302. ACM, 2014.

Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte.
NTRUSIGN: Digital signatures using the NTRU lattice.
In *CT-RSA*, pages 122–140, 2003.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.
In *ANTS*, pages 267–288, 1998.

References III

Dimitar Jetchev and Benjamin Wesolowski.
On graphs of isogenies of principally polarizable abelian surfaces and the discrete logarithm problem.
CoRR, abs/1506.00522, 2015.

J. E. Littlewood.
On the zeros of the Riemann zeta-function.
Mathematical Proceedings of the Cambridge Philosophical Society, 22:295–318, September 1924.

Youness Lamzouri, Xiannan Li, and Kannan Soundararajan.
Conditional bounds for the least quadratic non-residue and related problems.
Math. Comp., 84(295):2391–2412, 2015.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
On ideal lattices and learning with errors over rings.
Journal of the ACM, 60(6):43:1–43:35, November 2013.
Preliminary version in Eurocrypt 2010.

Daniele Micciancio.
Generalized compact knapsacks, cyclic lattices, and efficient one-way functions.
Computational Complexity, 16(4):365–411, 2007.
Preliminary version in FOCS 2002.

References IV

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
J. ACM, 56(6):1–40, 2009.
Preliminary version in STOC 2005.

René Schoof.
Minus class groups of the fields of the l-th roots of unity.
Mathematics of Computation of the American Mathematical Society, 67(223):1225–1245, 1998.

René Schoof.
Class numbers of real cyclotomic fields of prime conductor.
Mathematics of computation, 72(242):913–937, 2003.