Approx-SVP in multiquadratic ideal lattices

Semyon Novoselov

Immanuel Kant Baltic Federal University

Séminaire de Théorie Algorithmique des Nombres
Université de Bordeaux
13.02.2024

Content

I. Introduction
II. Discrete logarithm problem
III. Shortest principal ideal problem
IV. Reduction modulo S-units (overview)

$\left.\begin{array}{l} \text{II} \\ \text{III} \\ \text{IV} \end{array}\right\}$ γ-SVP

I. Introduction

Definitions

Multiquadratic field:

$$K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$$

Class group Cl_K:

- quotient of fractional ideals modulo principal ideals
- $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ is a set of prime ideals that generates Cl_K
- $\mathrm{Cl}_K \simeq \langle \mathfrak{g}_1 \rangle \times \ldots \times \langle \mathfrak{g}_k \rangle$

Discrete logarithm problem (DLP) in Cl_K:

Given an ideal I, find integers $\ell_1, \ldots, \ell_k$ s.t. $[I] = [\mathfrak{g}_1^{\ell_1} \cdot \ldots \cdot \mathfrak{g}_k^{\ell_k}]$.

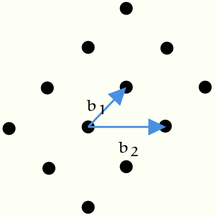
Note: DLP for $I = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$ is simple.

Ideals and lattices

Let $m = 2^n = \deg K$ and $\sigma_1, \ldots, \sigma_m$ are $r_1 + 2r_2$ complex embeddings of K.

Lattice in $\mathbb{R}^m$:

$$\Lambda = \mathbb{Z}b_1 \oplus \ldots \oplus \mathbb{Z}b_r$$



for linear independent vectors $b_1, \ldots, b_r \in \mathbb{R}^m$.

Canonical embedding:

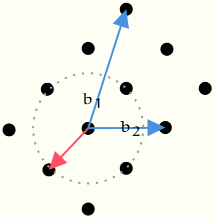
$$\sigma : K \to \mathbb{R}^m, \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_m(\alpha)).$$

An ideal I is a lattice under canonical embedding: $\sigma(I)$.

Shortest vector problem (SVP)

γ**-SVP**: find a vector $v \in \Lambda$ s.t. $v = \gamma \cdot \lambda_1(\Lambda)$.

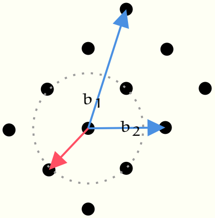
- $\lambda_1(\Lambda)$: Euclidean norm of the shortest vector in Λ.
- γ: approximation factor



Shortest vector problem (SVP)

γ-SVP: find a vector $v \in \Lambda$ s.t. $v = \gamma \cdot \lambda_1(\Lambda)$.

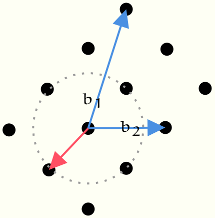
- $\lambda_1(\Lambda)$: Euclidean norm of the shortest vector in Λ.
- γ: approximation factor



Hard problem in general: subexponential γ in subexponential time (BKZ)

Shortest vector problem (SVP)

γ-**SVP**: find a vector $v \in \Lambda$ s.t. $v = \gamma \cdot \lambda_1(\Lambda)$.



- $\lambda_1(\Lambda)$: Euclidean norm of the shortest vector in Λ.
- γ: approximation factor

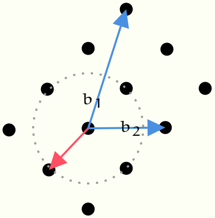
Hard problem in general: subexponential γ in subexponential time (BKZ)

[CDW17]$^+$ cyclotomics: subexponential γ in **polynomial** time

Shortest vector problem (SVP)

γ**-SVP**: find a vector $v \in \Lambda$ s.t. $v = \gamma \cdot \lambda_1(\Lambda)$.

- $\lambda_1(\Lambda)$: Euclidean norm of the shortest vector in Λ.
- γ: approximation factor



Hard problem in general: subexponential γ in subexponential time (BKZ)

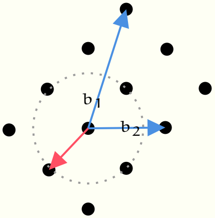
[CDW17]$^+$ cyclotomics: subexponential γ in **polynomial** time

[BBVLV17] multiquadratics: short generators in principal ideals (SPIP) in **quasi-polynomial** time, $\gamma = ?$

Shortest vector problem (SVP)

γ-**SVP**: find a vector $v \in \Lambda$ s.t. $v = \gamma \cdot \lambda_1(\Lambda)$.

- $\lambda_1(\Lambda)$: Euclidean norm of the shortest vector in Λ.
- γ: approximation factor



Hard problem in general: subexponential γ in subexponential time (BKZ)

[CDW17]$^+$ cyclotomics: subexponential γ in **polynomial** time

[BBVLV17] multiquadratics: short generators in principal ideals (SPIP) in **quasi-polynomial** time, $\gamma = ?$

Our goal: finding short vectors in ***non-principal*** ideals of multiquadratic field.

Ideal lattices: bounds for shortest vector

$$\sqrt{m} \cdot N(I)^{1/m} \leq \lambda_1(I) \leq \sqrt{m} \cdot \sqrt{|\Delta_K|}^{1/m} N(I)^{1/m} \left(\frac{2}{\pi}\right)^{r_2/m}$$

Lower bound is a special property of ideal lattices.

$$\Downarrow$$

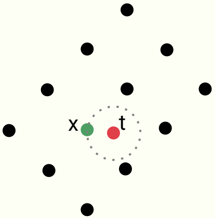
$\lambda_1(I)$ is known up to factor $\mathcal{D}_K = \sqrt{|\Delta_K|}^{1/m}$

- simplifies analysis of γ when $\mathcal{D}_K$ is small
- $\mathcal{D}_K \approx m$ for cyclotomics
- $\mathcal{D}_K \approx \mathrm{quasipoly}(m)$ for multiquadratics (assuming $D = d_1 \cdot \ldots \cdot d_n = \mathrm{quasipoly}(m)$)

Closest vector problem (CVP)

γ-CVP: Given a vector $t \in \mathbb{R}^m$ find $x \in \Lambda$ s.t. $\|x - t\| \leq \gamma \|y - t\|$ for all $y \in \Lambda$.

- hard problem in general
- easy case 1: short basis
- easy case 2: orthogonal basis



γ-SVP in ideal lattices is solved using reduction to easy cases of γ-CVP.

Finding short vectors in non-principal ideals

Approach of [CDW17] and [BLNR22] for cyclotomics (*Sketch*):

1. Compute DLOG for a target ideal
2. Build short basis for the Log-S-unit lattice (Stickelberger ideal + tricks)
3. Reduce result of DLOG computation:
   - using Log-S-unit lattice and its short basis (Babai's alg.)
   - using Log-unit lattice (SPIP)

In this talk we consider first step for multiquadratic fields and determination of γ for $\mathcal{SPIP}$.

Algorithm for solving γ-SVP in multiquadratics

Adaption of [CDW17] and [BLNR21] to multiquadratics:

1. Solve DLOG in Cl_K for a target ideal I:
   find g and $\vec{\alpha}$ s.t. $I = g \prod_i \mathfrak{p}_i^{\alpha_i}$
2. Build a short basis for Log_S-unit lattice Λ
3. Reduce $\vec{\alpha}$ in Λ using the short basis:
   $\vec{\beta} = \mathrm{CVP}(\Lambda, \vec{\alpha})$
   $g = g / \prod_j \gamma_j^{\beta_j}$
4. Reduce g in Log-unit lattice:
   return $\mathrm{SPIP}(g)$

II. Discrete logarithm problem

1. Reducing the problem to subfields
2. Square root of decomposed ideal
3. Algorithm for DLOG
4. Experiments

Reducing the problem to subfields

Multiquadratic fields admit norm relation:

$$I^2 = \frac{I_\sigma \cdot I_\tau}{\sigma(I_{\sigma\tau})} = \frac{N_{K/K_\sigma}(I) \cdot N_{K/K_\tau}(I)}{\sigma(N_{K/K_{\sigma\tau}}(I))}$$

where σ, τ are order 2 automorphisms, and K_σ, K_τ, $K_{\sigma\tau}$ are fixed fields.

$$\Downarrow$$

1. Find DLOGs for I_σ, I_τ, $I_{\sigma\tau}$ in subfields $K_\sigma, K_\tau, K_{\sigma\tau}$
2. Combine this data to obtain DLOG for I^2:

$$I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$$

3. Compute square root of $\alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$ that is equal to I.

Square root of decomposed ideal

Problem:

Given an ideal I and $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$ find α' and $f_1, \ldots, f_d$ s.t.

$I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

Idea: reduce the problem to cyclic subgroups of

$$\mathrm{Cl}_K \simeq \langle \mathfrak{g}_1 \rangle \times \ldots \times \langle \mathfrak{g}_k \rangle \simeq C_{b_1} \times \ldots \times C_{b_k}.$$

- This gives us multiple square roots (up to 2^k).
- Use saturation technique to efficiently select correct square root.

Note: We assume that $\alpha\mathcal{O}_K \neq \prod_{i=1}^{d} \mathfrak{p}_i^{a_i}$, otherwise the problem is trivial.

Saturation technique

FindSquare: Allows us, for a given set $T = \{a_1, \ldots, a_m\} \subset K$ and an element $h \in K$, to find efficiently the set of exponent vectors $\vec{e}$ such that $h \cdot a_1^{e_1} \cdot \ldots \cdot a_m^{e_m}$ is a square.

- described and used for multiquadratics in prior work
- based on quadratic characters computation

Example: Let $I = h\mathcal{O}_K$ and T is a set of generators of $\mathcal{O}_K^\times$. Then

$$\sqrt{I} = \sqrt{h \cdot a_1^{e_1} \cdot \ldots \cdot a_m^{e_m}}\mathcal{O}_K$$

Square roots in cyclic groups

TLDR. Taking square roots is simple since we know the generators.

Consider finding square root of $\mathfrak{g}^e$ in cyclic group $\langle \mathfrak{g} \rangle$ of order b.

CycSqrt:

1. If b is odd then square root is $\mathfrak{g}^{e(\frac{\mathrm{b}+1}{2})}$.
2. Let $\mathrm{b} = 2^{\mathrm{r}} \cdot \mathrm{t}$ where t is odd. Then

$$\sqrt{\mathfrak{g}^e} \in \{\mathfrak{b}, \mathfrak{b} \cdot \mathfrak{g}^{\frac{\mathrm{b}}{2}}\},$$

where $\mathfrak{b} = \mathfrak{g}^{e(\frac{\mathrm{t}+1}{2})} \cdot (\mathfrak{g}^{\mathrm{t}})^{-\frac{\ell}{2}}$ for $\ell = \mathrm{DLOG}_{\mathfrak{g}^{\mathrm{t}}}(\mathfrak{g}^{\mathrm{t} \cdot e})$.
Since $\# \langle \mathfrak{g}^{\mathrm{t}} \rangle = 2^{\mathrm{r}}$ computing the DLOG is simple.

* Carl Pomerance. Elementary thoughts on discrete logarithms. `https://math.dartmouth.edu/~carlp/PDF/dltalk4.pdf`

Applying CycSqrt to our ideal

$$I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} \Rightarrow [I^2] = [\prod_{i=1}^{d} \mathfrak{p}_i^{e_i}] = [\prod_{j=1}^{k} \mathfrak{g}_j^{g_j}]$$

$$\Downarrow \textbf{CycSqrt} \Downarrow$$

$$[I^2] = [\prod_{j=1}^{k} (\mathfrak{a}_j^{x_j} \mathfrak{b}_j)^2], x_j \in \mathbb{F}_2.$$

Then we have

$$I^2 = \frac{\alpha\beta}{\prod_{j=1}^{k} \alpha_j^{x_j}} \prod_{j=1}^{k} (\mathfrak{a}_j^{x_j} \mathfrak{b}_j)^2,$$

where $\mathfrak{a}_j^2 = \langle \alpha_j \rangle$ and $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2 = \langle \beta \rangle$.

Now, we can write the ideal I as

$$I = \sqrt{\frac{\alpha\beta u}{\prod_{j=1}^{k} \alpha_j^{x_j}} \prod_{j=1}^{k} \mathfrak{a}_j^{x_j} \mathfrak{b}_j}$$

for some $u \in \mathcal{O}_K^\times$ and any suitable set of x_j.

Problem: there are 2^k variants of x to enumerate.

Solution: apply the saturation technique (**FindSquare**).

Complete IdealSqrt algorithm

Input: An ideal $I^2 = \alpha \prod_{i=1}^{d} \mathfrak{p}_i^{e_i}$

Output: The ideal $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

1. Compute $\mathfrak{g}$ s.t. $\prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{k} \mathfrak{g}_j^{g_j}$
2. Compute $(\mathfrak{a}_j \mathfrak{b}_j, \mathfrak{b}_j) = \mathrm{CycSqrt}(\mathfrak{g}_j^{g_j})$ for all $j = 1, \dots, k$
3. Compute $\beta \in K$, s.t. $\beta \mathcal{O}_K = \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} / \prod_{j=1}^{k} \mathfrak{b}_j^2$
4. Compute $\alpha_j \in K$, s.t. $\alpha_j \mathcal{O}_K = \mathfrak{a}_j^2$
5. Compute generators $u_1, \dots, u_r$ of $\mathcal{O}_K^\times$
6. $x = \mathrm{FindSquare}(\alpha \cdot \beta, \alpha_1^{-1}, \dots, \alpha_k^{-1}, u_1^{-1}, \dots, u_r^{-1})$
7. Return $\sqrt{\dfrac{\alpha\beta}{\prod_{i=1}^{k} \alpha_i^{x_i} \prod_{i=1}^{r} u_i^{x_{i+k}}}} \prod_{j=1}^{k} \mathfrak{a}_j^{x_j} \mathfrak{b}_j$

Algorithm for DLOG

Input: an ideal I of multiquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Output: the ideal I represented by a pair $(\alpha', f) \in K \times \mathbb{Z}^d$ such that $I = \alpha' \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$.

1. **if** $[K : \mathbb{Q}] = 2$ **then** compute DLOG with Buchmann-Düllmann
2. Select distinct $\sigma, \tau, \sigma\tau \in G_K$ of order 2
3. $I_\sigma = N_{K/K_\sigma}(I)$, $I_\tau = N_{K/K_\tau}(I)$, $I_{\sigma\tau} = N_{K/K_{\sigma\tau}}(I)$
4. $J_\sigma = \mathrm{mqCLDL}(I_\sigma, S_\sigma)$ for $S_\sigma = \{\mathfrak{p} \cap K_\sigma \mid \mathfrak{p} \in S\}$
5. $J_\tau = \mathrm{mqCLDL}(I_\tau, S_\tau)$ for $S_\tau = \{\mathfrak{p} \cap K_\tau \mid \mathfrak{p} \in S\}$
6. $J_{\sigma\tau} = \mathrm{mqCLDL}(I_{\sigma\tau}, S_{\sigma\tau})$ for $S_{\sigma\tau} = \{\mathfrak{p} \cap K_{\sigma\tau} \mid \mathfrak{p} \in S\}$
7. $J = \mathrm{Lift}(J_\sigma) \cdot \mathrm{Lift}(J_\tau) / \mathrm{Lift}(\sigma(J_{\tau\sigma})) = \alpha \cdot \prod_{i=1}^{d} \mathfrak{p}_i^{e_i} = I^2$
8. Return $\mathrm{IdealSqrt}(J)$

Complexity

$$K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$$

- $D = d_1 \cdot \ldots \cdot d_n$ is the largest discriminant of quadratic subfield of K
- $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_d\}$ is a set of all prime ideals generating the ideal class group Cl_K

Main theorem

Let I be an ideal of K and $m = \deg K$. Then computing exponents $f_1, \dots, f_d$ such that $I = \alpha' \prod_i \mathfrak{p}_i^{f_i}$ for some $\alpha' \in K$ takes time

$$e^{\widetilde{\mathcal{O}}(\max(\log m, \sqrt{\log D}))}$$

field operations.

to be compared with: $L_{\Delta_K}(1/2) = e^{\widetilde{\mathcal{O}}(\sqrt{m \log D})}$

Experiments

Table 1: DLOG computation for multiquadratic fields.

$\deg K$	Field	Alg. 5	Sage	Cl_K
16	real	325	0.19	C_4^2
32	real	1607	64	$C_2 \times C_4 \times C_8^4$
64	real	4743	-	$C_2^9 \times C_4^3 \times C_8 \times C_{16}^4 \times C_{48} \times C_{240}$
16	imag.	159	0.41	$C_8 \times C_{48}$
32	imag.	1487	26	$C_2 \times C_4^3 \times C_{24} \times C_{48}^2 \times C_{3360}$
64	imag.	3941	-	$C_2^2 \times C_4^9 \times C_8^3 \times C_{16} \times C_{48} \times C_{96}^2 \times$ $C_2^2 \times \times C_{192}^2 \times C_{6720}^2 \times C_{927360}$

* Timings are given in seconds.

- Implementation is made in SageMath v.10.0
- Computations were done on Intel Core i7-8700 clocked at 3.20GHz and 64 GB of RAM.

III. Shortest principal ideal problem

State of the art

[BBVLV17]: reducing the problem to quadratic subfields for multiquadratics.

- generalized to multicubics, Kummer fields, …
- quasi-polynomial time complexity in m
- analysis of approximation factors is missing

I present the analysis in **this talk**.

Log-unit lattices

Used for reduction of principal ideal generators.

Log-embedding:

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^m \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_m(\alpha)|) \end{aligned}$$

Log-unit lattices

Used for reduction of principal ideal generators.

Log-embedding:

$$\begin{aligned}\mathrm{Log} : K &\to \mathbb{R}^m \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_m(\alpha)|)\end{aligned}$$

Log-unit lattice: $\mathrm{Log}\,\mathcal{O}_K^\times$.

Log-unit lattices

Used for reduction of principal ideal generators.

Log**-embedding:**

$$\begin{aligned}\mathrm{Log} : K &\to \mathbb{R}^m \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_m(\alpha)|)\end{aligned}$$

Log**-unit lattice:** $\mathrm{Log}\,\mathcal{O}_K^\times$.

multiquadratic Log**-unit lattice:** $\mathrm{Log}\,\mathcal{U}_K^\times$.

- $\mathcal{U}_K^\times$: group generated by fundamental units from quadratic subfields of K.

Log-unit lattices

Used for reduction of principal ideal generators.

Log-embedding:

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^m \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_m(\alpha)|) \end{aligned}$$

Log-unit lattice: $\mathrm{Log}\, \mathcal{O}_K^\times$.

multiquadratic Log-unit lattice: $\mathrm{Log}\, \mathcal{U}_K^\times$.

- $\mathcal{U}_K^\times$: group generated by fundamental units from quadratic subfields of K.
- basis is not short $\implies$ can't use methods from cyclotomics

Log-unit lattices

Used for reduction of principal ideal generators.

Log**-embedding:**

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^m \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_m(\alpha)|) \end{aligned}$$

Log**-unit lattice:** $\mathrm{Log}\,\mathcal{O}_K^\times$.

multiquadratic Log**-unit lattice:** $\mathrm{Log}\,\mathcal{U}_K^\times$.

- $\mathcal{U}_K^\times$: group generated by fundamental units from quadratic subfields of K.
- basis is not short $\implies$ can't use methods from cyclotomics
- orthogonal lattice $\implies$ CVP is polynomial time

Log-unit lattices

Used for reduction of principal ideal generators.

Log-embedding:

$$\begin{aligned}\mathrm{Log} : K &\to \mathbb{R}^m \\ \alpha &\mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_m(\alpha)|)\end{aligned}$$

Log-unit lattice: $\mathrm{Log}\,\mathcal{O}_K^\times$.

multiquadratic Log-unit lattice: $\mathrm{Log}\,\mathcal{U}_K^\times$.

- $\mathcal{U}_K^\times$: group generated by fundamental units from quadratic subfields of K.
- basis is not short $\implies$ can't use methods from cyclotomics
- orthogonal lattice $\implies$ CVP is polynomial time
- $(\mathcal{O}_K^\times)^m \subseteq \mathcal{U}_K^\times \implies$ can reduce CVP from $\mathrm{Log}\,\mathcal{O}_K^\times$ to $\mathrm{Log}\,\mathcal{U}_K^\times$

SPIP

Theorem

Let I be a principal ideal and D is quasi-polynomial in m.
If $\exists$ a generator g such that

$$\mathrm{Log}(g) = \sum_{i=1}^{m-1} c_i \,\mathrm{Log}(\varepsilon_i) + c \cdot \vec{1}$$

where $c_i < \frac{1}{2m}$ then g is unique and it can be computed in quasi-polynomial time in m.

Proof

We apply method from §8.4 in [BBVLV'17].

1. find a generator gu of I
2. u^m is multiquadratic unit for any unit u
3. solve CVP for $m\,\mathrm{Log}(gu) \implies u^m$ and so, we know $\pm g^m$
   ($m\,\mathrm{Log}(g)$ has coefficients $< \frac{1}{2} \implies$ rounded to zero)
4. compute g by successive square root computations

Which ideals satisfy conditions of theorem?

Asymptotic bound:

$$\|g\|_2 = \sqrt{m} \cdot e^{\mathcal{O}(D^{1/2+o(1)})} N(I)^{1/m}.$$

For comparison: the **shortest element** of ideal is bounded above as:

$$\lambda_1^{(2)} = \mathcal{O}(\sqrt{m} D^{1/4} N(I)^{1/m}).$$

However, we don't know how the shortest generator differs from the shortest element.

- for cyclotomics: $e^{\mathcal{O}(\sqrt{m})}\lambda_1^{(2)}$ for most of princ. ideals
- **open problem** for multiquadratics in general case.

Size of principal ideal generator (general case)

Theorem

Every principal ideal I of a multiquadratic field K has a generator g such that

$$\|g\| \leq m \cdot e^{D^{1/2+o(1)}} N(I)^{1/m}.$$

Proof (Sketch):

Adaptation of result from [CDPR'16] from cyclotomics. Use covering radius of the lattice $\mathrm{Log}(\mathcal{U}_K)$ and bounds for the lengths of its basis. $\square$

Consequence: we can compute shortest generators of almost all ideals in quasi-polynomial time.

Ideals in crypto

Heuristics from [BBVLV17, §8.1]: for secret generator we have $|c_i| = \left(\frac{1}{\sqrt{m}D^{1/2+o(1)}}\right)$ with probability $\to$ 1 when D is big enough.

Approximation factor: $\gamma = e^{\widetilde{\mathcal{O}}(\sqrt{m})}$.

Proof: for ideal lattices the upper and lower bounds for the shortest vector differs only by the factor $D^{1/4}$.

Complexity: computation in quasi-polynomial time in m when $D = \mathrm{quasipoly}(m)$.

IV. Reduction modulo S-units: overview

Log-S-unit lattices

Used for obtaining short elements of ideals.

Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ is a set of prime ideals

- usually we take S that generates Cl_K

$s \in K$ is a **S-unit** if $s\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_d^{e_d}$ for some $e_1, \ldots, e_d \in \mathbb{Z}$.

S-unit group: $\mathcal{O}_{K,S}^\times$ = all S-units.

Log-S-unit lattice: $\mathrm{Log}_S(\mathcal{O}_{K,S}^\times)$, where

$$\mathrm{Log}_S : s \mapsto (v_{\mathfrak{p}_i})_{i=1,\ldots,d}.$$

Reduction

In adaption of [CDW17] and [BLNR21] to multiquadratics:

1. Solve DLOG in Cl_K for a target ideal I:
   find g and $\vec{\alpha}$ s.t. $I = g \prod_i \mathfrak{p}_i^{\alpha_i}$
2. Build a short basis for Log_S-unit lattice Λ
3. Reduce $\vec{\alpha}$ in Λ using the short basis:
   $\vec{\beta} = \mathrm{CVP}(\Lambda, \vec{\alpha})$
   $g = g / \prod_j \gamma_j^{\beta_j}$
4. Reduce g in Log-unit lattice:
   return $\mathrm{SPIP}(g)$

Short bases: candidates

Stickelberger ideal S_K:

- used in [CDW17] and [BLNR22] for cyclotomics
- short basis of ideal in [BK21]

But S_K is **not full-rank**.

There two approaches to fix this:

- random walk to CL_K^- [CDW17]
  $\Longrightarrow$ h_K^+ steps
  $\Longrightarrow$ bad choice for multiquadratics
- lattice of real relations [BLNR22]

Stickelberger ideal for multiquadratics

[Kučera96]: description of ideal using restriction/correstriction from cyclotomic field

- K is abelian field $\implies$ subfield of a cyclotomic field

[KMNO21]: algorithmization of Kucera's work.

- $K \subset \mathbb{Q}(\zeta_t)$ for $t \approx D \implies$ basis is not short (when adapting [BK21])

Open problem: find short bases from generators of S_K and real class group relations.

Conclusion

Currently, we can solve γ-SVP with $\gamma = e^{\widetilde{\mathcal{O}}(\sqrt{\mathrm{m}})}$ for principal ideals with short generators.

Discrete logarithm problem can be solved in quasi-polynomial time.

Remaining **open problem**: building short bases for Log_S-unit lattice.

Outline

γ-SVP

CL_K[BV'19]

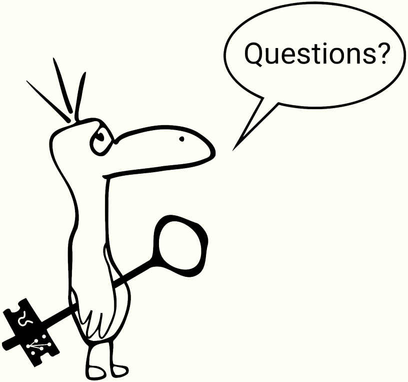
DLOG (this work)

SPIP [BBVLV17]

reduction mod S-units

Stickelberger ideal [KMNO22]

Short bases?



Contact

snovoselov@kantiana.ru

crypto-kantiana.com/semyon.novoselov

References

BD91 Buchmann, J., Düllmann, S. «On the computation of discrete logarithms in class group»

Kučera96 Kučera R. «On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields»

CDPR16 Cramer R., Ducas L., Peikert C., Regev O. «Recovering Short Generators of Principal Ideals in Cyclotomic Rings»

BBVLV17 Bauch, J., Bernstein, D.J., Valence, H.d., Lange, T., van Vredendaal, C. «Short generators without quantum computers: the case of multiquadratics»

CDW17 Cramer R., Ducas L., Wesolowski B. «Short Stickelberger Class Relations and Application to Ideal-SVP»

BK21 Bernard O., Kucera R. «A short basis of the Stickelberger ideal of a cyclotomic field»

KMNO21 Kirshanova E. A., Malygina E. S., Novoselov S. A., Olefirenko D. O. «An algorithm for computing the Stickelberger ideal for multiquadratic number fields»

BLNR22 Bernard, O., Lesavourey, A., Nguyen, T.H., Roux-Langlois, A. «Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP»

BEFHY22 Biasse J.F., Erukulangara, M.R., Fieker C., Hofmann T., Youmans W. «Mildly Short Vectors in Ideals of Cyclotomic Fields Without Quantum Computers»

N23 Novoselov S. A. «On the Discrete Logarithm Problem in the Ideal Class Group of Multiquadratic Fields»