On Approx-SVP in multiquadratic ideal lattices

Semyon Novoselov

Immanuel Kant Baltic Federal University

IndoCrypt 2024

Content

I. Introduction
II. Finding short vectors in non-principal ideal lattices
III. Implementation and experiments

Definitions

Multiquadratic field:

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

Class group $\mathbf{Cl_K}$:

- 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

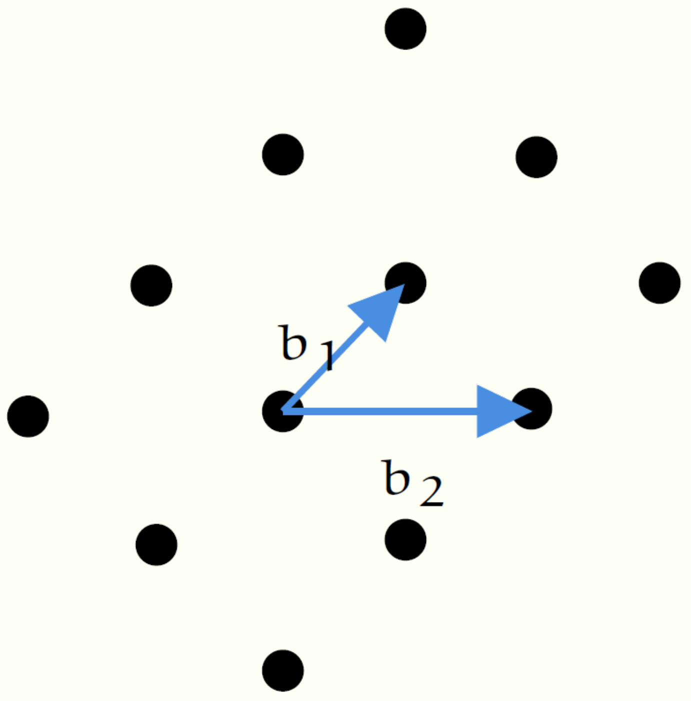
Discrete logarithm problem (DLP) in $\mathbf{Cl_K}$:

Given an ideal I, find $\alpha \in K$ and integers $\ell_1, \ldots, \ell_d$ s.t.

$$\mathrm{I} = \alpha \cdot \mathfrak{p}_1^{\ell_1} \cdot \ldots \cdot \mathfrak{p}_d^{\ell_d}$$

Ideals and lattices

Let $m = 2^n = \deg K$ and $\sigma_1, \ldots, \sigma_m$ be $r_1 + 2\,r_2$ 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:

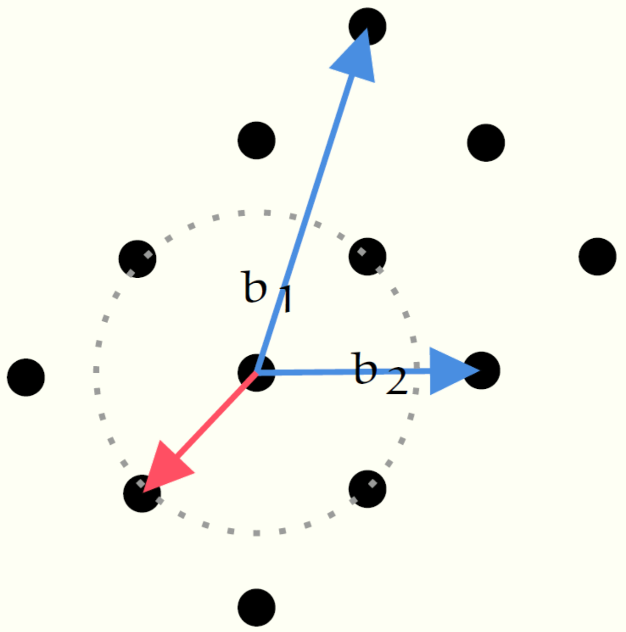
$$\sigma\colon\ \mathrm{K} \to \mathbb{R}^{\mathrm{m}}, \alpha \mapsto (|\sigma_1(\alpha)|, \ldots, |\sigma_{\mathrm{m}}(\alpha)|)$$

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

Shortest vector problem (SVP)

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

- $\lambda_1(\Lambda)$: (Euclidean) norm of the shortest non-zero 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 work: finding "mildly" short elements in non-principal ideals of multiquadratic field in quasi-polynomial time.

Ideal lattices: bounds for shortest vector

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

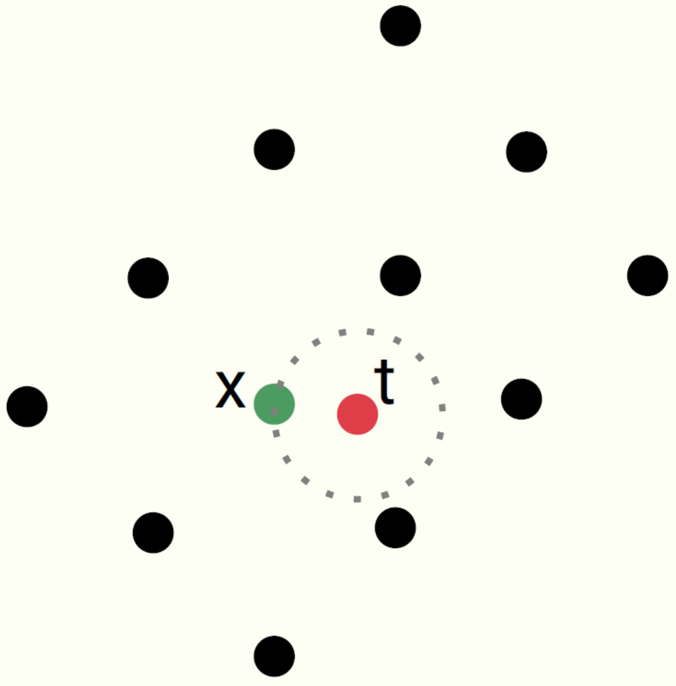
Lower bound is a special property of ideal lattices:

- $\lambda_1(I)$ is known up to factor $D_K = \sqrt{|\Delta_K|}^{\frac{1}{m}}$
- $D_K \approx m$ for cyclotomics
- $D_K \approx \mathrm{quasipoly}(m)$ for multiquadratics (assuming $D = d_1 \cdot \ldots \cdot d_n = \mathrm{quasipoly}(m)$)

Closest vector problem (CVP)

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

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



We solve γ-SVP in ideal lattices using reduction to easy cases of γ-CVP in specially crafted lattices.

Finding short vectors in non-principal ideals

We use approach of [CDW17] and [BLNR22] adapted from cyclotomics:

1. Compute DLOG for a target ideal:

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

   We have $\alpha \in K$, but
   - α is not short
   - $\alpha \in I$ only if all $e_i \geq 0$
2. Reduce element α:
   - Modulo units
   - Modulo S-units with a drift

   } Applying γ-CVP solvers

Reduction modulo units

Assumption 1

Let $K = \mathbb{Q}\left(\sqrt{d_1}, \ldots, \sqrt{d_n}\right)$, $\deg K = m$, and $\log D = \log(d_1 \cdot \ldots \cdot d_n) = (\log m)^{\mathcal{O}(1)}$.

- There is an algorithm ShortGenerator that given a principal ideal $I = \langle h \rangle$ returns an element $g \in I$ such that $\langle h \rangle = \langle g \rangle$ and $\|g\| = e^{\tilde{\mathcal{O}}(\sqrt{m})} N(h)^{\frac{1}{m}}$.
- The algorithm takes quasi-polynomial time in m and $\log N(h)$.
- The element g is a solution of γ-SVP in the lattice $\sigma(I)$ with $\gamma = e^{\tilde{\mathcal{O}}(\sqrt{m})}$.

- We use here a quasi-polynomial algorithm of [BBVLV17].
- For ideals that can be used in crypto, i.e. with short generators, this is theorem.

Reduction modulo S-units

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

- $\beta \in K$ is ***S*-unit** if $\langle \beta \rangle = \prod_{i=1}^{d} \mathfrak{p}_i^{f_i}$

Our goal: find an S-unit β s.t. $||\boldsymbol{e} - \boldsymbol{f}||$ is small and $e_i - f_i \geq 0$.

So, we can replace α with short element $\frac{\alpha}{\beta} \in I$.

This is solving of γ-CVP in Log-S-unit lattice.

Log-S-unit lattice

$$\Lambda_S = \mathrm{Log}_S \mathcal{O}_{K,S}^{\times}$$

- $\mathrm{Log}_S \colon \beta \mapsto (f_1, \ldots, f_d)$
- $\mathcal{O}_{K,S}^{\times}$ is the ring of all S-units

To solve γ-CVP efficiently we have to build a short basis for Λ_S

- γ determined by the size of this basis

This can be done in class group computation with Biasse-van Vredendaal algorithm.

Short basis for Log-S-unit lattice

Assumption 2

Let $K = \mathbb{Q}\left(\sqrt{d_1}, \ldots, \sqrt{d_n}\right)$, $\deg K = m$, $D = d_1 \cdot \ldots \cdot d_n$, and S be a set of prime ideals generating Cl_K.

Then the generators of the lattice $\mathrm{Log}_S \mathcal{O}_{K,S}^{\times}$ obtained by lifting from quadratic subfields of K have length $\mathcal{O}(\sqrt{\mathrm{m} \log \mathrm{D}})$.

- when $\log D = (\log m)^{\mathcal{O}(1)}$ building such a basis take quasi-polynomial time

Class group computations

Table 1. Euclidean lengths for class group relations

Field	m	rank Λ_S	b_2	b_∞	$b_2 \leq \sqrt{m}$	$b_2 \leq 2\sqrt{m}$	$b_2 \leq \sqrt{m \log_2 m}$
imag.	32	128	4	1	✓	✓	✓
imag.	64	512	7	2	✓	✓	✓
imag.	128	1024	12.80	2	x	✓	✓
imag.	256	2944	23.28	2	x	✓	✓
real	32	112	3.16	1	✓	✓	✓
real	64	448	5.29	1	✓	✓	✓
real	128	1344	9.53	2	✓	✓	✓
real	256	1664	15.03	2	✓	✓	✓

- b_2 and b_∞ - lengths of longest vector in the generators with resp. to ℓ_2 and ℓ_∞ norms
- data is given for fields where $d_1, \dots, d_n$ are the first primes s.t. $d_i \equiv 1 \; mod \; 4$

Algorithm for solving γ-SVP in multiquadratics

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

Algorithm 1

1. Solve DLOG in Cl_K for the target ideal I:
   find α and $\mathbf{e}$ s.t. $\langle\alpha\rangle = I \prod_i \mathfrak{p}_i^{e_i}$
2. Build a short basis for the Log-S-unit lattice Λ_S
3. Reduce $\mathbf{e}$ in Λ_S using the found short basis:
   $\mathbf{f} = \mathbf{e} - (\gamma\text{-CVP}(\Lambda_S, \boldsymbol{e} + drift) = \boldsymbol{h} \cdot \mathrm{B}(\Lambda_S))$
   $$\alpha = \alpha \, / \prod_j \beta_j^{h_j}$$
4. Reduce α in the Log-unit lattice:
   return ShortGenerator(α)

- $drift = b_2 \cdot \mathbf{1}$ is added to ensure that $f_i > 0$.

Complexity and approximation factor

Main result

Let $K = \mathbb{Q}\left(\sqrt{d_1}, \dots, \sqrt{d_n}\right)$, $\deg K = m$, and $D = d_1 \cdot \dots \cdot d_n$ be quasi-polynomial in m.

Then

- Algorithm 1 is correct and takes quasi-polynomial time under Assumptions 1,2.
- It returns an element α of norm $\|\alpha\|_2 \leq e^{\tilde{O}(\sqrt{m})} N(I)^{\frac{1}{m}}$.
- The algorithm solves γ-SVP in $\sigma(I)$ with $\gamma = e^{\tilde{O}(\sqrt{m})}$.

- all steps of Algorithm 1 are quasi-polynomial
- bound for length follows from the assumptions

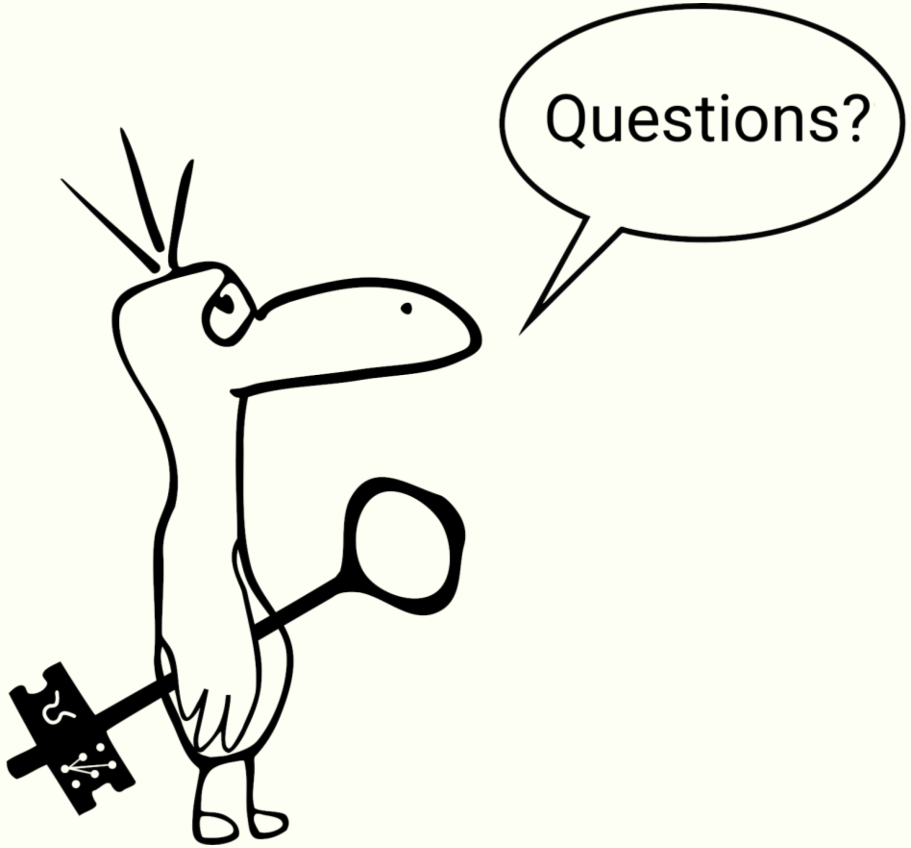
to be compared with: BKZ that takes subexponential time for the same γ

Experiments

Table 2. Approximation factors reached by Algorithm 1

Field	m	$\ln \gamma_{gh}$	$\sqrt{2\, m \log m \log D}$
imag.	8	1.00	13.45
imag.	16	3.09	27.27
imag.	32	11.30	50.55
imag.	64	49.59	89.22
real	8	1.45	15.26
real	16	4.27	30.33
real	32	18.07	55.69
real	64	64.55	97.06

- Implementation is made in SageMath v.10.2
- Computations were done on Intel Xeon Silver 4201R clocked at 2.40GHz on the machine with 629 GB RAM and took less than a week.
- The values of $\ln \gamma_{gh}$ are average for 10 random ideals



Contact

novsem@gmail.com

Source code: https://github.com/novoselov-sa/mqASVP