Hermitian lattices reduction

Thomas Camus

PhD student under the supervision of P. Elbaz-Vincent (IF) and J-G. Dumas (LJK)

January 16, 2015
Hermitian lattices reduction

- Part I: LLL algorithm for hermitian lattices
- Part II: Representations of fractional ideals
The theory of euclidean lattices and its algorithmic approach are well-known, but there are few studies of the algorithmic side for hermitian lattices.

H. Lenstra
A. Lenstra
L. Lovász

The inventors of the LLL algorithm
Part I: LLL algorithm for hermitian lattices

1. Introduction

2. Hermitian lattices over a quadratic euclidean number field

3. LLL-reduction
   - LLL-reduction for hermitian lattices
   - Usefulness for the SVP
   - Computing LLL-reduced basis

4. Probabilistic analysis
   - Average case
   - Experimental results
Let $K = \mathbb{Q}(i\sqrt{d})$ with $d \in \{1, 2, 3, 7, 11\}$ and $\mathbb{Z}_K$ be its maximal order.

**Definition**

A subgroup $\Lambda$ of $\mathbb{C}^m$ is called a $\mathbb{Z}_K$-lattice if there exists $(e_1, \ldots, e_m)$ a $\mathbb{C}$-basis of $\mathbb{C}^m$ such that $\Lambda = \mathbb{Z}_K e_1 \oplus \cdots \oplus \mathbb{Z}_K e_m$.

A $\mathbb{Z}_K$-lattice in $\mathbb{C}^m$ may be described as a $\mathbb{Z}$-lattice in $\mathbb{R}^{2m}$.

**Definition**

The minimal norm of $\Lambda$ is $\lambda_1(\Lambda) = \min_{x \in \Lambda \setminus \{0\}} \|x\|^2$.

**How to compute $\lambda_1(\Lambda)$ and a minimal vector of $\Lambda$?**
LLL-reduction for hermitian lattices

Let $\mathcal{E} = (e_1, \ldots, e_m)$ be a $\mathbb{C}$-basis of $\mathbb{C}^m$. We denote by $e_i^*$ and $\mu_{i,j}$ its Gram-Schmidt orthogonalization.

Let $0 < m_K < \delta < 1$, where $m_K$ is the euclidean minima of $K$:

$$m_K = \sup_{x \in \mathbb{C}} \inf_{y \in \mathbb{Z}_K} |x - y|^2,$$

**Definition**

The basis $\mathcal{E}$ is said $\delta$-LLL-reduced if:

$$\begin{cases} |\mu_{i,j}|^2 \leq m_K & \text{for } 1 \leq j < i \leq m, \\ \|e_i^*\|^2 \geq (\delta - |\mu_{i,i-1}|^2)\|e_{i-1}^*\|^2 & \text{for } 2 \leq i \leq m. \end{cases}$$
Computing a LLL-reduced basis of a $\mathbb{Z}_K$-lattice allow to approximate its minimal norm by giving a quasi-minimal vector.

Theorem

Let $\mathcal{E}$ be a $\delta$-LLL-reduced basis of a $\mathbb{Z}_K$-lattice $\Lambda$ in $\mathbb{C}^m$. Then

$$\|e_1\|^2 \leq \left( \frac{1}{\delta - m_K} \right)^{m-1} \lambda_1(\Lambda).$$
Computing LLL-reduced basis

<table>
<thead>
<tr>
<th>Idea [Napias, Gan/Ling/Mow]</th>
</tr>
</thead>
<tbody>
<tr>
<td>The original LLL algorithm (over ( \mathbb{Z} )) can be generalised for ( \mathbb{Z}_K )-lattices.</td>
</tr>
<tr>
<td>Therefore, one may compute a ( \delta )-LLL-reduced basis of a ( \mathbb{Z}_K )-lattice ( \Lambda ) from one of its basis ( \mathcal{E} = (e_1, \ldots, e_m) ) using</td>
</tr>
</tbody>
</table>
| \[
| \mathcal{O} \left( m^4 \log_\delta \left( \frac{\lambda_1(\Lambda)^{1/2}}{\|\mathcal{E}\|_\infty} \right) \right) |
| operations in \( \mathbb{C} \). |
Probabilistic analysis: average case

The bound $\|e_1\|^2 \leq \left(\frac{1}{\delta - mK}\right)^{m-1} \lambda_1(\Lambda)$ has been proven using $|\mu_{i,i-1}|^2 = m_K$: this is the worst case, which is unrealistic.

**Theorem**

Let $E = (e_1, \ldots, e_m)$ be a basis of a $\mathbb{Z}_K$-lattice $\Lambda$ in $\mathbb{C}^m$, to which the $\delta$-LLL algorithm is applied. Assuming that the coefficients $|\mu_{i,i-1}|^2$ of the GSOP of $E$ are identically distributed random variables of density $p$, we get that:

$$E(\log(\|e_1\|^2)) \leq \log(\lambda_1(\Lambda)) - (m - 1) \int_0^{m_K} \log(\delta - x)p(x)dx.$$ 

The density $p$ has been approximated using experimental data.
(≈ 400 lines). Tested on 500 bases in various dimension (50 to 150).

<table>
<thead>
<tr>
<th>$D$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>7</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_K$</td>
<td>0.5</td>
<td>0.75</td>
<td>0.3333333</td>
<td>0.5714286</td>
<td>0.8181818</td>
</tr>
<tr>
<td>$\int_0^{m_K} \log(\delta - x)p(x)dx$</td>
<td>- 0.0765100</td>
<td>- 0.09183234</td>
<td>- 0.0708416</td>
<td>- 0.0796641</td>
<td>- 0.0927955</td>
</tr>
<tr>
<td>$\frac{1/(\delta - m_K)}{\exp\left(-\int_0^{m_K} \log(\delta - x)p(x)dx\right)}$</td>
<td>1.8904972</td>
<td>3.8010754</td>
<td>1.4186946</td>
<td>2.2061385</td>
<td>6.3860367</td>
</tr>
</tbody>
</table>

$p(x) = \begin{cases} 
\frac{a}{x+b}e^{-x/c} & \text{if } x \in [0, m_K], \\
0 & \text{otherwise}.
\end{cases}$
Distribution and interpolation obtained in \( \mathbb{Q}(i) \) for \( \delta = 0.99 \) (logarithmic scale)

<table>
<thead>
<tr>
<th>proportion</th>
<th>fit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0001</td>
<td></td>
</tr>
<tr>
<td>0.001</td>
<td></td>
</tr>
<tr>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Similar results for other fields.

Thomas Camus
Hermitian lattices reduction
- Part I: LLL algorithm for hermitian lattices
- Part II: Representations of fractional ideals
Let $K$ be a number field of degree $d$ and $\mathbb{Z}_K$ be its ring of integers.

**Definition**

A fractional ideal of $K$ is a $\mathbb{Z}_K$-submodule $\alpha$ of $K$ for which one may find $\zeta \in \mathbb{Z}_K$ such that $\zeta \alpha \subset \mathbb{Z}_K$. In this case, one may find a $\mathbb{Q}$-basis of $K$ which is a $\mathbb{Z}$-basis of $\alpha$.

**How to represent ideals in an algorithmic setting?**

In PARI/GP:

- HNF representation (`idealhnf`) → easy to use.
- Two-element representation (`idealtwoelt`) → memory-friendly.
Part II: representations of a fractional ideal

5 Introduction

6 Matrix representation

7 Two-element representation
   naive algorithm
   Strong reduction, variable success rate
   Weak reduction, bounded failure rate
   Experimental results
Let $\alpha$ be an integral ideal of $K$ and $\omega = (\omega_1, \ldots, \omega_d)$ be an integral basis of $K$. We consider $\mathcal{E} = (e_1, \ldots, e_d)$ a $\mathbb{Z}$-basis of $\alpha$.

Matrix representation of $\alpha$

The ideal $\alpha$ may be represented by the coordinates matrix of $\mathcal{E}$ with respect to $\omega$.

It gives a representation of $\alpha$ as an element of $M_d(\mathbb{Z}) \cap \text{GL}_d(\mathbb{Q})$.

Uniqueness of such a representation is achieved by choosing a specific basis of $\alpha$ (i.e HNF).
Two-element representation: naive algorithm

Let $\mathfrak{a}$ be an integral ideal of $K$.

**Classical result**

Let $x$ be a non-zero element of $\mathfrak{a}$. There exists $y \in \mathfrak{a}$ such that $\mathfrak{a} = (x, y)$. Moreover, an element $y$ chosen uniformly at random in $\mathfrak{a}/(x)$ satisfies $(x, y) = \mathfrak{a}$ with probability:

$$P[(x, y) = \mathfrak{a}] = \prod_{p : \nu_p(x) > \nu_p(\mathfrak{a})} \left(1 - \frac{1}{\mathcal{N}(p)}\right) \geq \prod_{p | \mathfrak{a}} \left(1 - \frac{1}{\mathcal{N}(p)}\right).$$

**Problems:**

- Maximise the shortness of such a representation.
- **Success rate depends on $\mathfrak{a}$**.
Strong reduction, variable success rate

Lets add a size-reduction condition to the naive algorithm:

Algorithm 1

1. Choose $x \in \alpha$ short (w.r.t the $T_2$ norm), using the LLL-algorithm.
2. Find $y \in \alpha$ such that $(x, y) = \alpha$, using naïve algorithm.
3. Size-reduce $y$.

It produces a representation $(x, y) = \alpha$ such that:

$$\max\{\|x\|, \|y\|\} \in O(N(\alpha)^{1/d}).$$

$\rightarrow$ Strong reduction, but no changes on the success rate.

Implemented in GP(2C) ($\approx$ 100 lines in C).
Weak reduction, bounded failure rate

Let's add a size-reduction to the algorithm used in the function `idealtwoelt` of GP:

**Algorithm 2 [Fieker/Sthelé]**

1. Find $b \subset a$ such that $p | b$ implies $N(p) \geq y$, for $y$ a well-chosen constant.
2. Find a small two-element representation of $b$, using the previous algorithm.
3. Recover a two-element representation of $a$ from the one of $b$.

It produces a representation $(x, y) = a$ such that:

$$\max\{\|x\|, \|y\|\} \in O(N(a)^{4/d}).$$

$\rightarrow$ Weaker size-reduction, increase of the overall complexity, but the failure rate is bounded (depending on a "success parameter" $t$):

$$\mathbb{P}[\text{failure}] \leq 0.8^t$$

Implemented in GP(2C) ($\approx 500$ lines in C).
Ratio \( \frac{\text{time algorithm 1}}{\text{time algorithm 2}} \) over all integral ideals of norm \( \leq 5 \cdot 10^4 \) in a field of degree 25:

Despite the bounded failure rate, algorithm 2 tends to be way slower than algorithm 1. It seems that the control of the success rate does not outweigh the complexity explosion.
Heuristic remarks (WiP)

Ratio \( \log \frac{\text{result algorithm 2}}{\text{result algorithm 1}} \) over all integral ideals of norm \( \leq 5 \cdot 10^4 \) in a field of degree 25:

As foreseen, algorithm 1 usually produces shorter representations than algorithm 2.
Heuristic remarks (WiP)

Ratio $\log\frac{\text{theoretical bound}}{\text{result algorithm}}$ over all integral ideals of norm $\leq 5 \cdot 10^4$ in a field of degree 25:

The theoretical bounds on the size of the elements seem to be quite large for both algorithms.
Thanks for listening!

References:

- Napia: *A generalization of the LLL-algorithm over euclidean rings or orders* (Journal de théorie des nombres de Bordeaux, 1996).
- Scheider/Buchmann/Lindner: *Probabilistic analysis of LLL reduced bases* (WEWoRC, 2010).
- Fieker/Stehlé: *Short bases of lattices over number fields* (ANT, 2010).