Hermitian lattices reduction

Thomas Camus

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

INSTITUT FOURIER

LABORATOIRE JEAN KUNTZMANN
MATHÉMATIQUES APPLIQUÉES - INFORMATIQUE

UNIVERSITÉ DE GRENOBLE

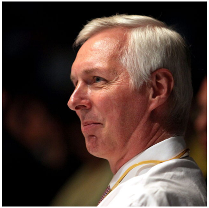
January 16, 2015

- Part I: LLL algorithm for hermitian lattices
- Part II: Representations of fractional ideals

Introduction

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

Hermitian lattices over a quadratic euclidean number field

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 Λ of $\mathbb{C}^m$ is called a $\mathbb{Z}_K$-lattice if there exists $(e_1, \dots, e_m)$ 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 Λ is $\lambda_1(\Lambda) = \min_{x \in \Lambda \setminus \{0\}} \|x\|^2$.

How to compute $\lambda_1(\Lambda)$ and a minimal vector of Λ ?

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 δ-LLL-reduced if:

$$\begin{cases} |\mu_{i,j}|^2 \leqslant m_K & \text{for } 1 \leqslant j < i \leqslant m, \\ \|e_i^*\|^2 \geqslant (\delta - |\mu_{i,i-1}|^2)\|e_{i-1}^*\|^2 & \text{for } 2 \leqslant i \leqslant m. \end{cases}$$

Usefulness for the SVP

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 δ-LLL-reduced basis of a $\mathbb{Z}_K$-lattice Λ in $\mathbb{C}^m$. Then

$$\|e_1\|^2 \leqslant \left(\frac{1}{\delta - m_K}\right)^{m-1} \lambda_1(\Lambda).$$

Computing LLL-reduced basis

Idea [Napias, Gan/Ling/Mow]

The original LLL algorithm (over $\mathbb{Z}$) can be generalised for $\mathbb{Z}_K$-lattices.

Therefore, one may compute a δ-LLL-reduced basis of a $\mathbb{Z}_K$-lattice Λ from one of its basis $\mathcal{E} = (e_1, \ldots, e_m)$ using

$$\mathcal{O}\left(m^4 \log_\delta\left(\frac{\lambda_1(\Lambda)^{1/2}}{\|\mathcal{E}\|_\infty}\right)\right)$$

operations in $\mathbb{C}$.

Probabilistic analysis: average case

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

Theorem

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

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

The density p has been approximated using experimental data.

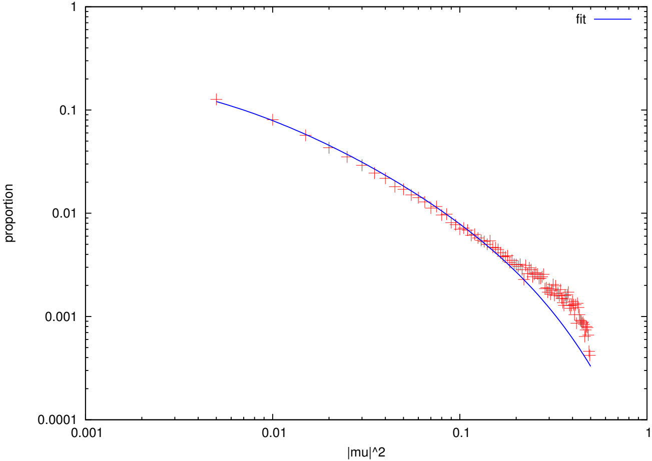
Experimental results

Simple implementation in GP ($\approx$ 400 lines). Tested on 500 bases in various dimension (50 to 150).

D	**1**	**2**	**3**	**7**	**11**
m_K	0.5	0.75	0.3333333	0.5714286	0.8181818
$\int_0^{m_K} \log(\delta - x) p(x) dx$	- 0.0765100	- 0.09183234	- 0.0708416	- 0.0796641	- 0.0927955
$\frac{1/(\delta - m_k)}{\exp\left(-\int_0^{m_K} \log(\delta - x)\tilde{p}(x) dx\right)}$	1.8904972	3.8010754	1.4186946	2.2061385	6.3860367

$$p(x) = \begin{cases} \frac{a}{x+b} e^{-x/c} & \text{if } x \in [0, m_K], \\ 0 & \text{otherwise.} \end{cases}$$

Distribution and interpolation obtained in $\mathbb{Q}(i)$ for $\delta = 0.99$ (logarithmic scale)



Similar results for other fields.

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

How to represent ideals in an algorithmic setting?

In PARI/GP:

- HNF representation (`idealhnf`) $\rightarrow$ easy to use.
- Two-element representation (`idealtwoelt`) $\rightarrow$ memory-friendly.

Part II: representations of a fractional ideal

Matrix representation

Let $\mathfrak{a}$ be an integral ideal of K and $\omega = (\omega_1, \dots, \omega_d)$ be an integral basis of K. We consider $\mathcal{E} = (e_1, \dots, e_d)$ a $\mathbb{Z}$-basis of $\mathfrak{a}$.

Matrix representation of $\mathfrak{a}$

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

It gives a representation of $\mathfrak{a}$ as an element of $\mathrm{M}_d(\mathbb{Z}) \cap \mathrm{GL}_d(\mathbb{Q})$.

Uniqueness of such a representation is achieved by choosing a specific basis of $\mathfrak{a}$ (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:

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

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

It produces a representation $(x, y) = \mathfrak{a}$ such that:

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

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

Implemented in GP(2C) ($\approx$ 100 lines in C).

Weak reduction, bounded failure rate

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

Algorithm 2 [Fieker/Sthelé]

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

It produces a representation $(x, y) = \mathfrak{a}$ such that:

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

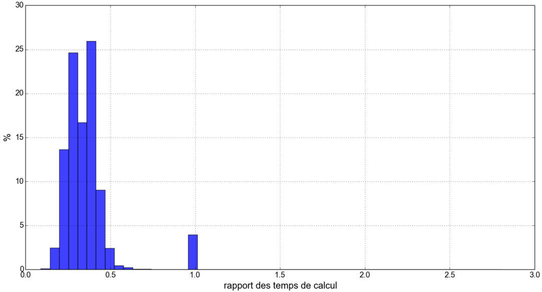
$\rightarrow$ Weaker size-reduction, increase of the overall complexity, but the failure rate is bounded (depending on a "success parameter" t):

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

Implemented in GP(2C) ($\approx$ 500 lines in C).

Heuristic remarks (WiP)

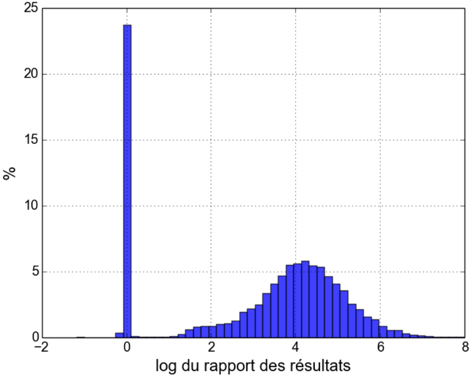
Ratio $\frac{\text{time algorithm 1}}{\text{time algorithm 2}}$ over all integral ideals of norm $\leqslant 5 \cdot 10^4$ in a field of degree 25:



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)

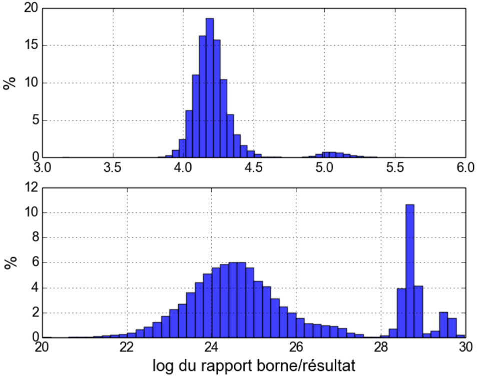
Ratio $\log \frac{\text{result algorithm 2}}{\text{result algorithm 1}}$ over all integral ideals of norm $\leqslant 5 \cdot 10^4$ in a field of degree 25:



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 $\leqslant 5 \cdot 10^4$ 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:

- Napias: *A generalization of the LLL-algorithm over euclidean rings or orders*(Journal de théorie des nombres de Bordeaux, 1996).
- Gan/Ling/Mow: *Complex Lattice Reduction Algorithm for Low-Complexity MIMO Detection* (IEEE, 2009).
- Scheider/Buchmann/Lindner: *Probabilistic analysis of LLL reduced bases* (WEWoRC, 2010).
- Fieker/Stehlé: *Short bases of lattices over number fields* (ANT, 2010).