Cybersecurity Institute
Univ. Grenoble Alpes

LLL over Euclidean imaginary quadratic fields

Titouan Coladon[1], Philippe Elbaz-Vincent[1], Cyril Hugounenq[1], Etienne Marcatel[1,2]

Atelier Pari GP, Grenoble, January 23rd, 2020

financed by
IDEX Université Grenoble Alpes

This work is supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02)

Motivation for Hermitian LLL

Applications:

- Computational Number Theory.
- Cryptography.
- MIMO: Multi Inputs Multi Outputs.

Previous works :

- Napias (1996): motivated by Hermitian lattices.
- Gan, Ling and Mow (2009): motivated by MIMO, only for $\mathbb{Z}[i]$
- Camus (2017): motivated by algorithmic studies of lattices.
- Pellet-Mary, Lee, Stehlé and Wallet (2019): general but using CVP oracle.
- Espitau, Kirchner, Fouque (2019): Not LLL but General and parallelisable.

Classical notations

- Gram-Schmidt Orthogonalization :

$$\begin{cases} b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \cdot b_j^* \\ \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2} \end{cases}$$

- LLL-Reduced for $\delta \in]0.25, 1[$ and $\eta \in [0.5, 1[$:
  - A lattice with basis $(b_1, \ldots, b_n)$ is said to be (δ, η)-LLL reduced if :

$$\begin{cases} |\mu_{i,j}| \leqslant \eta & \text{(size condition)} \\ (\delta - |\mu_{i,j}|^2)\|b_{i-1}^*\|^2 \leqslant \|b_i^*\|^2 & \text{(Lovasz's condition)} \end{cases}$$

Algorithm 1 LLL

Input: A basis $B = (b_1, \ldots, b_n)$ and some reals δ and η.

Output: A (δ, η)-LLL reduced basis.

Compute μ, the GSO B^* and set $\kappa = 1$

while $\kappa \leq n$ **do**

  for $j \in \{1, \ldots, \kappa - 1\}$ **do**

    if $\mu_{\kappa,j} \geq \eta$ **then**

      $b_\kappa \longleftarrow b_\kappa - \lfloor \mu_{\kappa,j} \rceil \cdot b_j$ and update μ accordingly

  if $(\delta - \mu_{\kappa,\kappa-1}^2) \cdot \|b_{\kappa-1}^*\|^2 > \|b_\kappa^*\|^2$ **then**

    Swap $b_{\kappa-1}$ and b_κ and update μ and B^* accordingly

    $\kappa \longleftarrow \kappa - 1$

  else

    $\kappa \longleftarrow \kappa + 1$

return B

We need :

- Euclideanity
- Gram-Schmidt Orthogonalization

Field definition

Let K be an imaginary quadratic field, $\mathcal{O}_K$ its ring of integers.

Hermitian scalar product for $a, b \in \mathbb{C}^n$,

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i \cdot \overline{b_i}$$

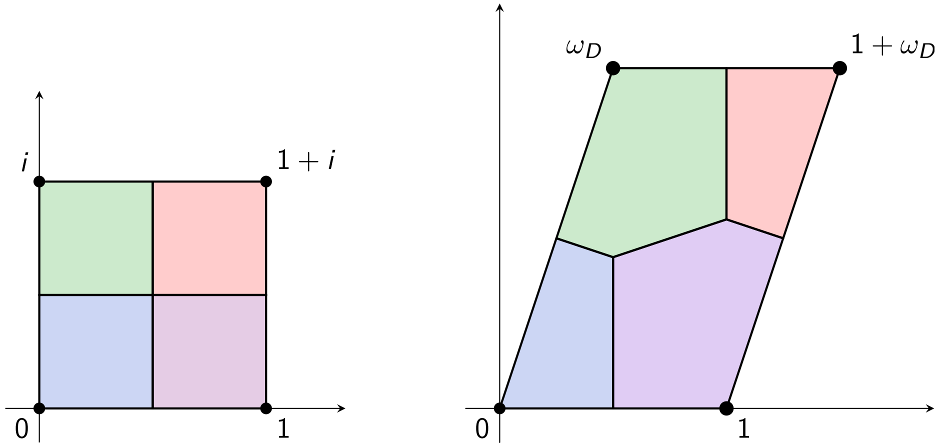
Gram-Schmidt Orthogonalization for a basis $(b_1, \ldots, b_n)$,

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \cdot b_j^* \quad \text{with } \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\| b_i^* \|^2}$$

Admissible fields

We define

$$m_K = \sup_{x \in K} \inf_{y \in \mathcal{O}_K} \mathcal{N}(x - y)$$



Admissible fields

K	$\mathbb{Q}[i]$	$\mathbb{Q}[i\sqrt{2}]$	$\mathbb{Q}[\frac{1+i\sqrt{3}}{2}]$	$\mathbb{Q}[\frac{1+i\sqrt{7}}{2}]$	$\mathbb{Q}[\frac{1+i\sqrt{11}}{2}]$
$\mathcal{O}_K^\times$	$\{\pm 1, \pm i\}$	$\{-1, +1\}$	$e^{\frac{2k\pi}{3}}$	$\{-1, +1\}$	$\{-1, +1\}$
m_K	$1/2$	$3/4$	$1/3$	$4/7$	$9/11$

Algebraic lattices

We refer to Camus PhD. (2017) for the following definitions.

An algebraic lattice of rank n over K is a subgroup Λ of $\mathbb{C}^n$ for which it exists a $\mathbb{C}$-basis $\mathcal{B} = (b_1, \ldots, b_n)$ of $\mathbb{C}^n$ such that:

$$\Lambda = \mathcal{O}_K b_1 \oplus \cdots \oplus \mathcal{O}_K b_n$$

LLL-Reduced for $\delta \in]0.25, 1[$ and $\eta \in [m_K, 1[$:

- $|\mu_{i,j}|^2 \leqslant \eta$
- $\|b_i^*\|^2 \geqslant (\delta - |\mu_{i,j}|^2)\|b_{i-1}^*\|^2$ (Lovasz's condition)

Pari GP script available !

Known fast implementation: fpLLL by N'Guyen and Stehlé (2005-2009)

Exact representation:

- $\mathcal{B} = (b_1, \ldots, b_n)$
- $G = (< b_i, b_j >)_{i,j}$

Floating representation:

- $\mu = (\frac{<b_i, b_j^*>}{\|b_j^*\|^2})_{i,j}$
- $r = (< b_i, b_j^* >)_{i,j}$
- $s^{(i)} = (\|b_i\|^2 - \sum_{k=1}^{j-1} \mu_{i,k} \cdot r_{i,k})_j$

Also : IALatRed, implementation based on interval arithmetics (Espitau and Joux)

INSTITUT FOURIER

Cybersecurity Institute
Univ. Grenoble Alpes

Euclidean	Hermitian
$r_{i,j} = \langle b_i, b_j \rangle - \sum_{k=1}^{j-1} \mu_{j,k} \cdot r_{i,k}$	$r_{i,j} = \langle b_i, b_j \rangle - \sum_{k=1}^{j-1} \overline{\mu_{j,k}} \cdot r_{i,k}$
$s_j^{(i)} = \lVert b_i \rVert^2 - \sum_{k=1}^{j-1} \mu_{i,k} \cdot r_{i,k}$	$s_j^{(i)} = \lVert b_i \rVert^2 - \sum_{k=1}^{j-1} \overline{\mu_{i,k}} \cdot r_{i,k}$
$g_{k,k} = g_{k,k} - 2\lambda \cdot g_{j,k} + \lvert\lambda\rvert^2 \cdot g_{j,j}$	$g_{k,k} = g_{k,k} - 2Re(\overline{\lambda} \cdot g_{j,k}) + \lvert\lambda\rvert^2 \cdot g_{j,j}$

Hermitian fpLLL: features

- For $\mathbb{Z}[i]$:
  - Option -zi
  - LLL, Enumeration, BKZ
- For $\mathbb{Z}[j]$:
  - Option -zj
  - Only LLL for now
- Option -timing
- Hermitian lattice generation : latticegen -zi

Next steps

- Proofs for Hermitian fpLLL (bounds, ...).
- Generalisation to other algebraic lattices:
  - Some (Euclidean) cyclotomic number rings
- Code profiling and optimizations.

Contact `philippe.elbaz-vincent@univ-grenoble-alpes.fr` to beta test.