勉強会形式ゼミ資料②
L. Ducas, L. N. Pulles and M. Stevens Towards a modern LLL implementation[1]

佐藤 新

July 5, 2025

本セミナーで用いられる記号など

- $\boldsymbol{A} \in M_{n,m}(\mathbb{R})$ に対して，$\|\boldsymbol{A}\|_{\max} := \max_{i,j} |a_{i,j}|$

Seysen 簡約（1/3）

- $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$: 基底
- $\boldsymbol{B} = (\boldsymbol{b}_1^\top, \ldots, \boldsymbol{b}_n^\top)^\top$: 基底行列
- $\boldsymbol{B} = \boldsymbol{R}\boldsymbol{Q}$ ($\boldsymbol{R}$: 下三角行列, $\boldsymbol{Q}$: 直交行列)
- $\boldsymbol{R} = \begin{bmatrix} \boldsymbol{R}_{1,1} & \boldsymbol{O}_{\lfloor n/2 \rfloor, n-\lfloor n/2 \rfloor} \\ \boldsymbol{R}_{2,1} & \boldsymbol{R}_{2,2} \end{bmatrix}$

定義 1 (Seysen 簡約)

$\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ が Seysen 簡約されているとは

$$\boldsymbol{R}_{1,1},\ \boldsymbol{R}_{2,2} \text{が Seysen 簡約されている} \wedge \left\| \boldsymbol{R}_{2,1} \boldsymbol{R}_{1,1}^{-1} \right\|_{\max} \leq \frac{1}{2}$$

Seysen 簡約（2/3）

Seysen 簡約は大まかには次のようなことを $\boldsymbol{B} = \boldsymbol{RQ}$ なる $\boldsymbol{R}$ に対して再帰的に行う．

1. $\boldsymbol{R}$ を $\begin{bmatrix} \boldsymbol{R}_{1,1} & \boldsymbol{O} \\ \boldsymbol{R}_{2,1} & \boldsymbol{R}_{2,2} \end{bmatrix}$ とブロックに分ける
2.

Seysen 簡約（3/3）

Algorithm Seysen 簡約 [1]

Require: 下三角行列 $\boldsymbol{R} \in M_n(\mathbb{R})$ s.t. $\boldsymbol{B} = \boldsymbol{R}\boldsymbol{Q}$

Ensure: $\boldsymbol{U}\boldsymbol{B}$ が簡約基底行列となるような unimodular 行列 $\boldsymbol{U} \in M_n(\mathbb{R})$

if $\boldsymbol{R} \in M_1(\mathbb{R})$ **then**

  return $[1]$

$\begin{bmatrix} \boldsymbol{R}_{1,1} & \boldsymbol{O} \\ \boldsymbol{R}_{2,1} & \boldsymbol{R}_{2,2} \end{bmatrix} \leftarrow \boldsymbol{R}$ /* $\boldsymbol{R}_{1,1} \in M_{\lfloor n \rfloor}(\mathbb{R})$, $\boldsymbol{R}_{2,1} \in M_{n-\lfloor n \rfloor, \lfloor n \rfloor}(\mathbb{R})$, $\boldsymbol{R}_{2,2} \in M_{n-\lfloor n \rfloor, n-\lfloor n \rfloor}(\mathbb{R})$ */

$\boldsymbol{U}_{1,1} \leftarrow \texttt{seysenReduce}(\boldsymbol{R}_{1,1})$

$\boldsymbol{U}_{2,2} \leftarrow \texttt{seysenReduce}(\boldsymbol{R}_{2,2})$

$\boldsymbol{R}_{2,1} \leftarrow \boldsymbol{U}_{2,2}\boldsymbol{R}_{2,1}$

$\boldsymbol{U}_{2,1} \leftarrow \lfloor -\boldsymbol{R}_{2,1}\boldsymbol{R}_{1,1}^{-1} \rceil$

$\boldsymbol{R}_{2,1} \leftarrow \boldsymbol{U}_{2,1}\boldsymbol{R}_{1,1} + \boldsymbol{R}_{2,1}$

return $\begin{bmatrix} \boldsymbol{U}_{1,1} & \boldsymbol{O} \\ \boldsymbol{U}_{2,1}\boldsymbol{U}_{1,1} & \boldsymbol{U}_{2,2} \end{bmatrix}$

参考文献 I

[1] Léo Ducas, Ludo N. Pulles, and Marc Stevens. Towards a modern LLL implementation. Cryptology ePrint Archive, Paper 2025/774, 2025.