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，$\|\boldsymbol{A}\|_{\max} := \max_{i,j} |a_{i,j}|$

[1] の貢献

- BLASter の提案
  - 高速かつモダンな LLL の実装
  - [2] の分割手法を利用
  - サイズ簡約を Seysen 簡約に置き換え
  - Cholesky 分解を QR 分解に置き換え

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 $\boldsymbol{B} = \boldsymbol{R}\boldsymbol{Q}$ なる $\boldsymbol{R}$ に対して再帰的に行う．

1. $\boldsymbol{R}$ が 1 次正方なら何もしない
2. $\boldsymbol{R}$ 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
3. $\boldsymbol{R}_{1,1}, \boldsymbol{R}_{2,2}$ をそれぞれ Seysen 簡約

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

Algorithm BLASter LLL アルゴリズム [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 $\boldsymbol{U} \in M_n(\mathbb{R})$

$i_0 \leftarrow 0$; $\boldsymbol{U} \leftarrow \boldsymbol{E}_n$

do

  $\boldsymbol{R} \leftarrow \boldsymbol{B} = \boldsymbol{R}\boldsymbol{Q}$ なる下三角行列 $\boldsymbol{R}$ ($\boldsymbol{Q}$: 直交行列)

  $i_0 \leftarrow \ell/2 - i_0$

  $\mathcal{I} \leftarrow \{(i_0 + k\ell + 1, \min\{n, i_0 + k\ell + \ell\}) \mid 0 \leq k < (n - i_0)/\ell\}$

  for $(i, j) \in \mathcal{I}$ **do** $\boldsymbol{V}_i \leftarrow \mathrm{LLL}(\boldsymbol{R}_{[i,j]\times[i,j]}, \delta)$ **endfor**

  for $(i, j) \in \mathcal{I}$ **do**

    $\boldsymbol{B}_{[i,j]\times[1,n]} \leftarrow \boldsymbol{V}_i \boldsymbol{B}_{[i,j]\times[1,n]}$; $\boldsymbol{U}_{[i,j]\times[1,n]} \leftarrow \boldsymbol{V}_i \boldsymbol{U}_{[i,j]\times[1,n]}$

  $\boldsymbol{R} \leftarrow \boldsymbol{B} = \boldsymbol{R}\boldsymbol{Q}$ なる下三角行列 $\boldsymbol{R}$ ($\boldsymbol{Q}$: 直交行列)

  $\boldsymbol{W} \leftarrow \texttt{seysenReduce}(\boldsymbol{R})$; $\boldsymbol{B} \leftarrow \boldsymbol{W}\boldsymbol{B}$; $\boldsymbol{U} \leftarrow \boldsymbol{W}\boldsymbol{U}$

  $f \leftarrow \texttt{true}$

  for $i = 1$to$n - 1$ **do**

    if $\delta r_{i,i}^2 > r_{i,i+1}^2 + r_{i+1,i+1}^2$ **then** $f \leftarrow \texttt{false}$; **break endif**

while not f

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.

[2] Arnold Neumaier and Damien Stehle. Faster LLL-type reduction of lattice bases. Cryptology ePrint Archive, Paper 2016/852, 2016.