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 6, 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，$\|\boldsymbol{A}\|_{\max} := \max_{i,j} |a_{i,j}|$
- $\boldsymbol{A} \in M_{n,m}(\mathbb{R})$ に対して，$\boldsymbol{A}_{[r,s]\times[t,u]} := [a_{i,j}]_{r\leq i\leq s, t\leq j\leq u}$

[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

[2] の分割手法

Algorithm Reduce[2]

Require: 格子 L の基底行列 $\boldsymbol{B} \in M_n(\mathbb{Z})$，簡約パラメタ $0 < \eta \leq 1$

Ensure: 簡約された基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

```
n_r ← n 以下最大の specific dimension
computes GSO B ← [||b_i||^*], U ← [μ_{i,j}]
sizeReduce(B)
β̄ ← 2 + ⌈log_2(√n (max_{i≤n} ||b_i||)^n)⌉
for t = 1 to (n/n_r)^2 ⌈log(β̄/η)⌉ do
    for k = 0 to n − n_r do
        B' ← B_[k+1, n_r+k]
        U' ← U_[k+1, n_r+k]
        V ← recReduce(B', U', η, β̄)
        V' ← E_n; B ← V'B
        sizeReduce(B)
```

$n_r \leftarrow n$ 以下最大の specific dimension
computes GSO $B \leftarrow [\|\boldsymbol{b}_i\|^\star], \boldsymbol{U} \leftarrow [\mu_{i,j}]$
$\texttt{sizeReduce}(\boldsymbol{B})$
$\overline{\beta} \leftarrow 2 + \lceil \log_2 (\sqrt{n}(\max_{i \leq n} \|\boldsymbol{b}_i\|)^n) \rceil$
for $t = 1$ to $(n/n_r)^2 \lceil \log(\overline{\beta}/\eta) \rceil$ **do**
  for $k = 0$ to $n - n_r$ **do**
    $B' \leftarrow B_{[k+1, n_r+k]}$
    $\boldsymbol{U}' \leftarrow \boldsymbol{U}_{[k+1, n_r+k]}$
    $\boldsymbol{V} \leftarrow \texttt{recReduce}(B', \boldsymbol{U}', \eta, \overline{\beta})$
    $\boldsymbol{V}' \leftarrow \boldsymbol{E}_n;\ \boldsymbol{B} \leftarrow \boldsymbol{V}'\boldsymbol{B}$
    $\texttt{sizeReduce}(\boldsymbol{B})$

Algorithm L^2 簡約 [**?**]

Require: パラメタ $\frac{1}{4} < \delta < 1, \frac{1}{2} < \eta < \sqrt{\delta}$，基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Ensure: 簡約された基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

if $n = 2$ **then** Schonhage のアルゴリズム **endif**
$\boldsymbol{V} \leftarrow \boldsymbol{E}_n$
for $t = 1$ to$(2n_r/n_{r-1})^2 \lceil \log(8\overline{\beta}/\eta) \rceil$ **do**
  for $k = 2(n_r/n_{r-1})^2$ downto 0 **do**
    $B' \leftarrow B_{[kn_{r-1}/2+1, kn_{r-1}/2+n_{r-1}]}$
    $\boldsymbol{U}' \leftarrow \boldsymbol{U}_{[kn_{r-1}/2+1, kn_{r-1}/2+n_{r-1}]}$
    $\boldsymbol{V}' = \texttt{recReduce}(B', \boldsymbol{U}', \eta, \overline{\beta})$
    $\boldsymbol{V}'' \leftarrow \boldsymbol{E}_{n_r}$
    $\boldsymbol{V} \leftarrow \boldsymbol{V}''\boldsymbol{V} \bmod 2^{\overline{\beta}}$
    $\texttt{sizeReduce}(B, \boldsymbol{U})$

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

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

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 $\boldsymbol{U} \in M_n(\mathbb{R})$

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

2: **return** $[1]$

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

4: $\boldsymbol{U}_{1,1} \leftarrow \texttt{seysenReduce}(\boldsymbol{R}_{1,1})$; $\boldsymbol{U}_{2,2} \leftarrow \texttt{seysenReduce}(\boldsymbol{R}_{2,2})$

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

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

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

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

BLASter LLL

weakly-LLL 簡約

定義 2 (weakly-LLL 簡約基底)

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

$$\|\boldsymbol{b}_k^\star\|^2 \geq (\delta - \mu_{k,k-1}^2)\left\|\boldsymbol{b}_{k-1}^\star\right\|^2$$

なるときをいう．

- Lovász 条件のみを満たす

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 ← 0; U ← E_n
do
    R ← B = RQ なる下三角行列 R (Q : 直交行列)
    i_0 ← ℓ/2 − i_0
    I ← {(i_0 + kℓ + 1, min{n, i_0 + kℓ + ℓ}) | 0 ≤ k < (n − i_0)/ℓ}
    for (i, j) ∈ I do V_i ← LLL(R_[i,j]×[i,j], δ) endfor   /* V_i は LLL 基底を与えるユニモジラ行列 */
    for (i, j) ∈ I do
        B_[i,j]×[1,n] ← V_i B_[i,j]×[1,n]; U_[i,j]×[1,n] ← V_i U_[i,j]×[1,n]
    R ← B = RQ なる下三角行列 R (Q : 直交行列)
    W ← seysenReduce(R); B ← WB; U ← WU
    f ← true   /* B が weakly-LLL 簡約されているか */
    for i = 1ton − 1 do
        if δ r_{i,i}^2 > r_{i,i+1}^2 + r_{i+1,i+1}^2 then f ← 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.