#### 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

佐藤 勉強会 July 5, 2025 1/8

本セミナーで用いられる記号など

ullet  $oldsymbol{A}\in M_{n,m}(\mathbb{R})$  に対して, $\|oldsymbol{A}\|_{ ext{max}}\coloneqq \max_{i,j}|a_{i,j}|$ 

佐藤 勉強会 July 5, 2025 2/8

# [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

3/8

佐藤 勉強会 **July 5, 2025** 

# Seysen 簡約(1/3)

- $\{b_1, \ldots, b_n\}$ : 基底
- $\boldsymbol{B} = (\boldsymbol{b}_1^\top, \dots, \boldsymbol{b}_n^\top)^\top$ : 基底行列
- B = RQ(R: 下三角行列, Q: 直交行列)
- $egin{aligned} oldsymbol{\circ} & oldsymbol{R} = egin{bmatrix} oldsymbol{R}_{1,1} & oldsymbol{O}_{\lfloor n/2 
  floor, n \lfloor n/2 
  floor} \ oldsymbol{R}_{2,1} & oldsymbol{R}_{2,2} \end{bmatrix} \end{aligned}$

#### 定義 1 (Seysen 簡約)

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

$$oldsymbol{R}_{1,1}, \; oldsymbol{R}_{2,2}$$
が Seysen 簡約されている  $\wedge \left\| oldsymbol{R}_{2,1} oldsymbol{R}_{1,1}^{-1} 
ight\|_{ ext{max}} \leq rac{1}{2}$ 

◆□▶◆□▶◆壹▶◆壹▶ 壹 かへで

佐藤

### Seysen 簡約(2/3)

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

- lacktriangle  $m{R}$  が 1 次正方なら何もしない
- $m{2}$   $m{R}$ を $egin{bmatrix} m{R}_{1,1} & m{O} \ m{R}_{2,1} & m{R}_{2,2} \end{bmatrix}$ とブロックに分ける
- ③  $R_{1,1}, R_{2,2}$  をそれぞれ Seysen 簡約



佐藤 勉強会 July 5, 2025 5/8

## Seysen 簡約(3/3)

#### Algorithm Seysen 簡約 [1]

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

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

- 1: if  $\mathbf{R} \in M_1(\mathbb{R})$  then
- 2: **return** [1]

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

- 4:  $ar{m{U}}_{1,1} \leftarrow m{ ext{seysenReduce}}(m{R}_{1,1}); \ m{U}_{2,2} \leftarrow m{ ext{seysenReduce}}(m{R}_{2,2})$
- 5:  $R_{2,1} \leftarrow U_{2,2}R_{2,1}$
- 6:  $U_{2,1} \leftarrow \lfloor -R_{2,1}R_{1,1}^{-1} 
  brace$
- 7:  $R_{2,1} \leftarrow U_{2,1}R_{1,1} + R_{2,1}$
- 8: return  $\begin{bmatrix} U_{1,1} & O \\ U_{2,1}U_{1,1} & U_{2,2} \end{bmatrix}$



佐藤 勉強会 July 5, 2025 6/8

#### **Algorithm** BLASter LLL アルゴリズム [1]

```
Require: 下三角行列 R \in M_n(\mathbb{R}) s.t. B = RQ
Ensure: UB が簡約基底行列となるような unimodular 行列 U \in M_n(\mathbb{R})
 1: i_0 \leftarrow 0; \boldsymbol{U} \leftarrow \boldsymbol{E}_n
 2: do
          R \leftarrow B = RQ なる下三角行列 R(Q: 直交行列)
 3:
 4:
         i_0 \leftarrow \ell/2 - i_0
 5:
         \mathcal{I} \leftarrow \{(i_0 + k\ell + 1, \min\{n, i_0 + k\ell + \ell\}) \mid 0 \le k < (n - i_0)/\ell\}
 6:
         for (i, j) \in \mathcal{I} do V_i \leftarrow \text{LLL}(R_{[i, j] \times [i, j]}, \delta) endfor
 7:
         for (i, j) \in \mathcal{I} do
 8:
              B_{[i,j]\times[1,n]} \leftarrow V_i B_{[i,j]\times[1,n]}; \ U_{[i,j]\times[1,n]} \leftarrow V_i U_{[i,j]\times[1,n]}
          R \leftarrow B = RQ なる下三角行列 R(Q: 直交行列)
9:
          m{W} \leftarrow 	exttt{seysenReduce}(m{R}); \ m{B} \leftarrow m{W} m{B}; \ m{U} \leftarrow m{W} m{U}
10:
       f \leftarrow \mathsf{true}
11:
         for i = 1ton - 1 do
12:
               if \delta r_{i,i}^2 > r_{i,i+1}^2 + r_{i+1,i+1}^2 then f \leftarrow \text{false}; break endif
13:
14: while not f
```

July 5, 2025

#### 参考文献

- [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.

8/8