## 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

佐藤 勉強会 July 6, 2025 1/10

#### 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, $\|oldsymbol{A}\|_{ ext{max}}\coloneqq \max_{i,j}|a_{i,j}|$
- ullet  $oldsymbol{A}\in M_{n,m}(\mathbb{R})$  に対して、 $oldsymbol{A}_{[r,s] imes[t,u]}\coloneqq [a_{i,j}]_{r\leq i\leq s,t\leq j\leq u}$

# [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

3/10

性藤 勉強会 知识 Manage Manag

# [2]の分割手法

### Algorithm Reduce[2]

11:

```
Require: 格子 L の基底行列 B \in M_n(\mathbb{Z}),簡
     約パラメタ 0 < n < 1
Ensure: 簡約された基底 \{b_1, \ldots, b_n\}
 1: n_r \leftarrow n 以下最大の specific dimension
 2: computes GSO B \leftarrow [\|\boldsymbol{b}_i\|^*], \boldsymbol{U} \leftarrow [\mu_{i,i}]
 3: sizeReduce(B)
4: \overline{\beta} \leftarrow 2 + \lceil \log_2 (\sqrt{n} (\max_{i \leq n} \|\boldsymbol{b}_i\|)^n) \rceil
5: for t=1 to (n/n_r)^2\lceil\log(\overline{\beta}/\eta)\rceil do
       for k=0 to n-n_m do
    B' \leftarrow B_{[k+1,n_r+k]}; \quad U'
    U_{[k+1.n_r+k]\times[k+1,n_r+k]}
8:
             V \leftarrow \text{recReduce}(B', U', \eta, \overline{\beta})
9: V' \leftarrow E_n
      B \leftarrow V'B
10:
```

sizeReduce(B)

#### Algorithm $L^2$ 簡約 [?]

Require:  $\mathcal{N} \supset \mathcal{N} \supset \frac{1}{4} < \delta < 1, \frac{1}{2} < \eta < \sqrt{\delta}$ , 基底  $\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}$ Ensure: 簡約された基底  $\{b_1, \ldots, b_n\}$ 1:  $\overline{\delta} \leftarrow (\delta + 1)/2$ :  $\overline{\eta} \leftarrow \frac{\eta + 1/2}{2}$ 

2: 
$$\overline{r}_{1,1} \leftarrow \diamond(\|\boldsymbol{b}_1\|^2); \ \kappa \leftarrow 2$$

$$z: r_{1,1} \leftarrow \diamond (\|\boldsymbol{o}_1\|); \kappa \leftarrow$$

3: while 
$$\kappa \leq n$$
 do

else

4: sizeReduce
$$(\overline{\eta}, \kappa)$$

5: if 
$$\overline{\delta}\overline{r}_{\kappa-1,\kappa-1}<\overline{r}_{\kappa,\kappa}+\overline{\mu}_{\kappa,\kappa-1}^2\overline{r}_{\kappa-1,\kappa-1}$$
 then

$$\kappa \leftarrow \kappa + 1$$

July 6, 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)
- $lackbox{lack} R = egin{bmatrix} m{R}_{1,1} & m{O}_{\lfloor n/2 
  floor, n-\lfloor n/2 
  floor} \ m{R}_{2,1} & m{R}_{2,2} \end{bmatrix}$

## 定義 1 (Seysen 簡約)

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

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

< □ ト < □ ト < 重 ト < 重 ト ● ■ の < ○

佐藤 勉強会 July 6, 2025 5.

# 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
- 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 6, 2025 6/10

# Seysen 簡約(3/3)

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

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

- 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  $\begin{bmatrix} U_{1,1} & O \\ U_{2,1}U_{1,1} & U_{2,2} \end{bmatrix}$

<ロ > → □ → → □ → → □ → へへの

7/10

佐藤 <u>勉強会</u> July 6, 2025

## **BLASter LLL**

weakly-LLL 簡約

## 定義 2 (weakly-LLL 簡約基底)

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

$$\|\boldsymbol{b}_{k}^{\star}\|^{2} \ge (\delta - \mu_{k,k-1}^{2}) \|\boldsymbol{b}_{k-1}^{\star}\|^{2}$$

なるときをいう.

▶ Lovász 条件のみを満たす



佐藤 勉強会 July 6, 2025 8/10

## **Algorithm** BLASter LLL アルゴリズム [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: 
$$i_0 \leftarrow 0$$
;  $\boldsymbol{U} \leftarrow \boldsymbol{E}_n$ 

- 2: **do**
- 3:  $R \leftarrow B = RQ$  なる下三角行列 R(Q: 直交行列)
- 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:  $\mathsf{for}\ (i,j) \in \mathcal{I}\ \mathsf{do}\ V_i \leftarrow \mathtt{LLL}(R_{[i,j] imes [i,j]}, \delta)\ \mathsf{endfor}\ \ / ^*\ V_i\ \mathsf{td}\ \mathtt{LLL}\ 基底を与えるユニモジラ行列}\ */$
- 7: for  $(i, j) \in \mathcal{I}$  do
- 8:  $B_{[i,j]\times[1,n]} \leftarrow V_i B_{[i,j]\times[1,n]}; \ U_{[i,j]\times[1,n]} \leftarrow V_i U_{[i,j]\times[1,n]}$
- 9:  $R \leftarrow B = RQ$  なる下三角行列 R(Q: 直交行列)
- 10:  $W \leftarrow \mathsf{seysenReduce}(R); \ B \leftarrow WB; \ U \leftarrow WU$
- 11:  $f \leftarrow \text{true}$  /\* B が weakly-LLL 簡約されているか \*/
- 12: **for** i = 1**to**n 1 **do**
- 13: if  $\delta r_{i,i}^2 > r_{i,i+1}^2 + r_{i+1,i+1}^2$  then  $f \leftarrow \text{false}$ ; break endif
- 14: **while** not *f*

◆ロト→団ト→ミト→ミ からぐ

佐藤 勉強会

## 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.

10/10