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 1/6

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 2/6

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)
- $egin{array}{ccc} oldsymbol{R} = egin{bmatrix} oldsymbol{R}_{1,1} & oldsymbol{O}_{\lfloor n/2
 floor, n-\lfloor n/2
 floor} \ oldsymbol{R}_{2,1} & oldsymbol{R}_{2,2} \end{bmatrix}$

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 $\wedge \left\| oldsymbol{R}_{2,1} oldsymbol{R}_{1,1}^{-1}
ight\|_{ ext{max}} \leq rac{1}{2}$

◆ロト ◆部 ト ◆ 恵 ト ◆ 恵 ・ 夕 Q ○

July 5, 2025

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.

- **o** Rを $\begin{bmatrix} R_{1,1} & O \ R_{2,1} & R_{2,2} \end{bmatrix}$ とブロックに分ける
- 2

佐藤 勉強会 July 5, 2025 4/6

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} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}(\mathbb{R}) \, ^{\star} / \boldsymbol{R}_{2,2} = M_{n-\lfloor n \rfloor,n-\lfloor n \rfloor}$$

- 4: $U_{1,1} \leftarrow \mathsf{seysenReduce}(R_{1,1})$
- 5: $U_{2,2} \leftarrow \mathsf{seysenReduce}(R_{2,2})$
- 6: $R_{2,1} \leftarrow U_{2,2}R_{2,1}$
- 7: $U_{2,1} \leftarrow \lfloor -R_{2,1}R_{1,1}^{-1} \rceil$
- 8: $R_{2,1} \leftarrow U_{2,1}R_{1,1} + R_{2,1}$
- 9: return $egin{bmatrix} m{U}_{1,1} & m{O} \\ m{U}_{2,1} m{U}_{1,1} & m{U}_{2,2} \end{bmatrix}$

佐藤

|ロト 4回 ト 4 差 ト 4 差 ト | 差 | 夕 Q ()

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.