### 勉強会形式ゼミ資料①

## P.Q.Nguyen and D. Stehle Floating-Point LLL Revisited

佐藤 新

June 27, 2025

佐藤 勉強会 June 27, 2025 1/10

#### 本セミナーで用いられる記号など

- 全て  $\{b_1,\ldots,b_n\}$  を基底としてもつ整数格子
- $B = \max\{\|b\|_i \mid 1 \le i \le n\}$
- 浮動小数点数の演算精度は ℓ-bit
- $\bullet$   $\diamond(a*b)$  は a\*b の浮動小数点演算  $(* \in \{+,-, imes,/\})$

佐藤 勉強会 June 27, 2025 2/10

#### Gram-Schmidtの計算(1/5)

今までの GSO 情報の持ち方

Gram-Schmidt の情報は

$$\mu_{i,j} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle - \sum_{k=1}^{j-1} \mu_{j,k} \mu_{i,k} \|\boldsymbol{b}_k^{\star}\|^2}{\left\|\boldsymbol{b}_j^{\star}\right\|^2}, \|\boldsymbol{b}_i^{\star}\|^2 = \|\boldsymbol{b}_i\|^2 - \sum_{j=1}^{i-1} \mu_{i,j}^2 \left\|\boldsymbol{b}_j^{\star}\right\|^2$$

という公式で計算可能

• 内積  $\langle m{b}_i, m{b}_j 
angle$  の計算に浮動小数点数(fpa)が必要 $2^{-\ell} \|m{b}_i\| \|m{b}_j\|$  の潜在的な不確定性がある



佐藤 勉強会 June 27, 2025 3/10

### Gram-Schmidtの計算(2/5)

L<sup>2</sup> での GSO 情報の持ち方

Gram-Schmidt の情報から

$$r_{i,j} = \langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle - \sum_{k=1}^{j-1} \mu_{j,k} r_{i,k}, \ \mu_{i,j} = \frac{r_{i,j}}{r_{j,j}} \quad (i \ge j)$$

という公式で計算可能な形で情報を持つ

- → 精度が改善される
- 内積は Gram 行列から得られる(fpa)である必要なし
- 乗算が2回から1回に

佐藤 勉強会 June 27, 2025 4/10

#### Gram-Schmidtの計算(3/5)

Lovász 条件の書き換え

$$s_j^{(i)} \coloneqq \|\boldsymbol{b}_i\|^2 - \sum_{k=1}^{j-1} \mu_{i,k} r_{i,k} \quad (1 \le j \le i)$$

とすると,Lovász 条件  $\delta \left\| oldsymbol{b}_{\kappa-1}^{\star} \right\|^2 \leq \left\| oldsymbol{b}_{\kappa}^{\star} \right\|^2 + \mu_{\kappa,\kappa-1}^2 \left\| oldsymbol{b}_{\kappa-1}^{\star} \right\|^2$  は

$$\|\boldsymbol{b}_{\kappa}^{\star}\|^{2} + \mu_{\kappa,\kappa-1}^{2} \|\boldsymbol{b}_{\kappa-1}^{\star}\|^{2} = \|\boldsymbol{b}_{\kappa}\|^{2} - \sum_{j=1}^{\kappa-2} \mu_{\kappa,j}^{2} \|\boldsymbol{b}_{j}^{\star}\|^{2} = \|\boldsymbol{b}_{\kappa}\|^{2} - \sum_{j=1}^{\kappa-2} \mu_{\kappa,j} r_{\kappa,j} \|\boldsymbol{b}_{j}^{\star}\|^{2}$$
$$= s_{\kappa-1}^{(\kappa)}$$

より

$$\delta r_{\kappa-1,\kappa-1} \le s_{\kappa-1}^{(\kappa)}$$

と書き換えることができる.

<ロ > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < 回 る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の ○ □ < □ る の

### Gram-Schmidtの計算(4/5)

基底の更新後の Lovász 条件(1/2)

更に $b_{\kappa}$ と $b_{\kappa-1}$ の交換後の基底

$$\{oldsymbol{c}_1,\ldots,oldsymbol{c}_n\}\coloneqq\{\ldots,oldsymbol{b}_{\kappa-2},oldsymbol{b}_{\kappa},oldsymbol{b}_{\kappa-1},oldsymbol{b}_{\kappa+1},\ldots\}$$

とすると、交換後に検証すべき Lovász 条件は

(1) 
$$\delta \|\boldsymbol{c}_{\kappa-2}^{\star}\|^{2} \leq \|\boldsymbol{c}_{\kappa-1}^{\star}\|^{2} + \nu_{\kappa-1,\kappa-2}^{2} \|\boldsymbol{c}_{\kappa-2}^{\star}\|^{2}$$

に移る.

佐藤 June 27, 2025 6/10

### Gram-Schmidtの計算(5/5)

基底の更新後の Lovász 条件 (2/2)

$$egin{aligned} \left\|oldsymbol{c}_{\kappa-2}^{\star}
ight\|^2 &= \left\|oldsymbol{b}_{\kappa-2}^{\star}
ight\|^2, \ \left\|oldsymbol{c}_{\kappa-1}^{\star}
ight\| &= \left\|\pi_{\kappa-1}(oldsymbol{b}_{\kappa})
ight\|^2, \ 
u_{\kappa-1,\kappa-2} &= \mu_{\kappa-1,\kappa-2} \ ag{5.5}$$
 であるので, 式 (1)  $\iff \delta \left\|oldsymbol{b}_{\kappa-2}^{\star} \right\|^2 \leq \left\|\pi_{\kappa-1}(oldsymbol{b}_{\kappa})
ight\|^2 + \mu_{\kappa-1,\kappa-2} \left\|oldsymbol{b}_{\kappa-2}^{\star} \right\|^2 \ \iff \delta r_{\kappa-2,\kappa-2} \leq \mu_{\kappa,\kappa-1} \left\|oldsymbol{b}_{\kappa-1}^{\star} \right\|^2 + \left\|oldsymbol{b}_{\kappa}^{\star} \right\|^2 + \mu_{\kappa-1,\kappa-2} \left\|oldsymbol{b}_{\kappa-2}^{\star} \right\|^2 \ \iff \delta r_{\kappa-2,\kappa-2} \leq \left\|oldsymbol{b}_{\kappa} \right\|^2 - \sum_{i=1}^{\kappa-3} \mu_{\kappa,j} r_{\kappa,j} \left\|oldsymbol{b}_{j}^{\star} \right\|^2 = s_{\kappa-2}^{(\kappa)} \end{aligned}$ 

になるので, $[s_i^{(i)}]$  を持っておくと**追加のコストなく**次の条件に移れる

7/10

#### **Algorithm** $L^2$ 内での size-reduction

```
Require: パラメタ \eta > 1/2, \kappa \in \mathbb{Z}, 基底 \{b_1, \ldots, b_n\}
Ensure: [\bar{r}_{\kappa,i}], [\bar{p}_{\kappa,i}], [\bar{s}_i] (i < \kappa), \{..., b_{\kappa-1}, b'_{\kappa}, b_{\kappa+1}, ...\}
 1: \bar{\eta} \leftarrow \frac{\eta + 1/2}{2} = \frac{2\eta + 1}{4}
 2: do
 3:
              for i=1 to \kappa do /*Cholesky 分解*/
 4:
                     \bar{r}_{i,i} \leftarrow \langle \boldsymbol{b}_i, \boldsymbol{b}_i \rangle
                     for k=1 to j-1 do \bar{r}_{i,j} \leftarrow \diamond(\bar{r}_{i,j} - \diamond(\bar{r}_{i,k}\bar{\mu}_{j,k}))
 5:
 6:
                    \bar{\mu}_{i,j} \leftarrow \diamond(\bar{r}_{i,j}/\bar{r}_{i,j})
            s_0 \leftarrow \|\boldsymbol{b}_n\|^2
 7:
 8:
              for k=1 to j-1 do \bar{s}_i \leftarrow \diamond(\bar{s}_{i-1} - \diamond(\bar{\mu}_{n,i}\bar{r}_{n,i}))
 9:
              r_{n,n} \leftarrow s_n
               for i = \kappa - 1 downto 1 do
10:
11:
                      if |\bar{\mu}_{k,i}| > \bar{\eta} then X_i \leftarrow |\bar{\mu}_{k,i}| else X_i \leftarrow 0
                      for j=1 to i-1 do \bar{\mu}_{k,i} \leftarrow \diamond(\bar{\mu}_{\kappa,i} - \diamond(X_i\bar{\mu}_{i,i}))
12:
              \boldsymbol{b}_{\kappa} \leftarrow \boldsymbol{b}_{\kappa} - \sum_{i=1}^{\kappa-1} X_i \boldsymbol{b}_i
13:
14: while X \neq \mathbf{0}_{\kappa-1}
```

#### Algorithm $L^2$ 簡約

```
Require: パラメタ \eta, \delta, 基底 \{b_1, \ldots, b_n\}
Ensure: 簡約された基底 \{b_1,\ldots,b_n\}
 1: \bar{\delta} \leftarrow (\delta + 1)/2
 2: \bar{r}_{1,1} \leftarrow \|\boldsymbol{b}_1\|^2
 3: \kappa \leftarrow 2
 4: while \kappa < n do
 5:
               size-reduce (Algorithm 1)
 6: \kappa' \leftarrow \kappa
           while \kappa > 2 \wedge \bar{\delta} \bar{r}_{\kappa-1,\kappa-1} > \bar{s}_{\kappa-1} do
 8:
                      \kappa \leftarrow \kappa - 1
 9:
               for i=1 to \kappa-1 do
10:
                       \bar{\mu}_{\kappa,i} \leftarrow \bar{\mu}_{\kappa',i}; \; \bar{r}_{\kappa,i} \leftarrow \bar{r}_{\kappa',i}; \; \bar{r}_{\kappa,\kappa} \leftarrow \bar{s}_{\kappa}
              \{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}\leftarrow \{\ldots,\boldsymbol{b}_{\kappa'-1},\boldsymbol{b}_{\kappa'+1},\ldots,\boldsymbol{b}_{\kappa'},\boldsymbol{b}_{\kappa}\ldots\}
11:
12:
               \kappa \leftarrow \kappa + 1
```

9/10

佐藤 June 27, 2025

# 参考文献 I

10/10