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

1/11

佐藤 <u>勉強会</u> June 27, 2025

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 $(* \in \{+,-, imes,/\})$

(□▶ ←┛▶ ←差▶ ←差▶ −差 − 釣魚@

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 3/11

Gram-Schmidtの計算(2/5)

 L^2 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

(ロ) (部) (意) (意) (意) の(()

佐藤 勉強会 June 27, 2025 4/11

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) (部) (注) (注) 注 り(0)

勉強会

Gram-Schmidtの計算(4/5)

基底の更新後の Lovász 条件(1/2)

更に b_{κ} 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 <u>勉強会</u> June 27, 2025 6/11

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

4□ > 4回 > 4 = > 4 = > = 900

7/11

L^2 内での size-reduction (1/2)

 L^2 内での size-reduction では,大まかに次のことを行う

- 基底 $\{m{b}_1,\dots,m{b}_n\}$ の Gram 行列 $G(m{b}_1,\dots,m{b}_n)$ の Cholesky 分解を利用して $[r_{\kappa,j}],[\mu_{\kappa,j}],[s_j^{(\kappa)}]$ を計算
- ② $|\mu_{\kappa,j}| \geq rac{\eta + rac{1}{2}}{2}$ のとき
 - ト $m{b}_{\kappa} \leftarrow m{b}_{\kappa} \lfloor \mu_{\kappa,j}
 ceil m{b}_{j}$ で $|\mu_{\kappa,j}| \leq 1/2$ なるように基底を更新
 - ightharpoonup それに合わせて $[r_{\kappa,j}], [\mu_{\kappa,j}], [s_j^{(\kappa)}]$ も更新



佐藤 勉強会 June 27, 2025 8/1

Algorithm L^2 内での size-reduction

```
Require: パラメタ n > 1/2, \kappa \in \mathbb{Z}, 基底 \{b_1, \ldots, b_n\}
Ensure: [\bar{r}_{\kappa,i}], [\bar{\mu}_{\kappa,i}], [\bar{s}_{i}^{(\kappa)}] (j \leq \kappa), 簡約された基底 \{\ldots, b_{\kappa-1}, b'_{\kappa}, b_{\kappa+1}, \ldots\}
 1: \bar{\eta} \leftarrow \frac{\eta + 1/2}{2} = \frac{2\eta + 1}{4}
 2: do
              for j=1 to \kappa do /*部分的な Cholesky 分解で [r_{\kappa,j}], [\mu_{\kappa,j}], [s_i^{(\kappa)}] を更新*/
 3:
 4:
                     \bar{r}_{\kappa,i} \leftarrow \langle \boldsymbol{b}_{\kappa}, \boldsymbol{b}_{i} \rangle
 5:
                     for h=1 to j-1 do \bar{r}_{\kappa,j} \leftarrow \diamond(\bar{r}_{\kappa,j} - \diamond(\bar{r}_{\kappa,h} \times \bar{\mu}_{j,h}))
 6:
                     \bar{\mu}_{\kappa,i} \leftarrow \diamond(\bar{r}_{\kappa,i}/\bar{r}_{i,i})
             s_0^{(\kappa)} \leftarrow \|\boldsymbol{b}_n\|^2
 7:
              for k=1 to j-1 do \bar{s}_i^{(\kappa)} \leftarrow \diamond(\bar{s}_{i-1}^{(\kappa)} - \diamond(\bar{\mu}_{n,i} \times \bar{r}_{n,j})) endfor; r_{n,n} \leftarrow s_n^{(\kappa)}
 8:
 9:
              for i = \kappa - 1 downto 1 do
                      if |\bar{\mu}_{\kappa,i}| \geq \bar{\eta} then X_i \leftarrow |\bar{\mu}_{\kappa,i}| else X_i \leftarrow 0 /*|\mu_{\kappa,i}| により係数ベクトルを決定*/
10:
                       for i = 1 to i - 1 do \bar{\mu}_{\kappa,i} \leftarrow \diamond(\bar{\mu}_{\kappa,i} - \diamond(X_i \times \bar{\mu}_{i,i}))
11:
             \boldsymbol{b}_{\kappa} \leftarrow \boldsymbol{b}_{\kappa} - \sum_{i=1}^{\kappa-1} X_{i} \boldsymbol{b}_{i}
13: while X \neq \mathbf{0}_{\kappa-1}
```

佐藤 勉強会 June 27, 2025 9/11

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
```

佐藤 勉強会 June 27, 2025 10/11

参考文献 I