勉強会形式ゼミ資料①

P.Q.Nguyen and D. Stehle Floating-Point LLL Revisited[?]

佐藤 新

June 30, 2025

佐藤

勉強会 June 30, 2025 1/13

本セミナーで用いられる記号など([?] に倣った記号)

- 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
- ullet $\diamond(a*b)$ は a*b の浮動小数点演算 $(*\in\{+,-, imes,/\})$

◆□▶ ◆御▶ ◆巻▶ ◆巻▶ - 巻 - 夕へ@

佐藤 勉強会 June 30, 2025 2 / 13

Gram-Schmidt の計算(1/5)

今までの GSO 情報の持ち方

Gram-Schmidt の情報は

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

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

< ロ ト ∢団 ト ∢ 豆 ト ∢ 豆 ト 、 豆 ・ 夕 Q (^)

3 / 13

Gram-Schmidt の計算(2/5)

L² 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

◆ロト ◆個 ト ◆ 差 ト ◆ 差 ・ 釣 へ ○

4 / 13

佐藤 勉強会 勉強会 June 30, 2025

Gram-Schmidt の計算(3/5)

Lovász 条件の書き換え

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

とすると,Lovász 条件 $\delta ig\|oldsymbol{b}_{\kappa-1}^\starig\|^2 \leq ig\|oldsymbol{b}_\kappa^\starig\|^2 + \mu_{\kappa,\kappa-1}^2ig\|oldsymbol{b}_{\kappa-1}^\starig\|^2$ 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 > < 巨 > < 巨 > 三 の < @

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

に移る.

6/13

Gram-Schmidt の計算(5/5)

基底の更新後の Lovász 条件 (2/2)

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

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 ロ ト 4 個 ト 4 差 ト 4 差 ト - 差 - 夕 Q @

7 / 13

L^2 内での size-reduction (1/2)

L² 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
 - ▶ $m{b}_{\kappa} \leftarrow m{b}_{\kappa} \lfloor \mu_{\kappa,j}
 ceil m{b}_{j}$ 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
 - st 条件 $|\mu_{\kappa,j}| \geq rac{\eta+rac{1}{2}}{2}$ は $\eta o rac{1}{2}$ + のとき $|\mu_{\kappa,j}| > rac{1}{2}$

<ロト < 個 ト < 直 ト < 直 ト へ 直 ト へ 直 ・ の Q ()

8 / 13

佐藤 勉強会 June 30, 2025

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: [\overline{r}_{\kappa,j}], [\overline{\mu}_{\kappa,j}], [\overline{s}_i^{(\kappa)}] (j \leq \kappa), 簡約された基底 \{\ldots, b_{\kappa-1}, b'_{\kappa}, b_{\kappa+1}, \ldots\}
 1: \overline{\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:
                       \overline{r}_{\kappa,i} \leftarrow \diamond(\langle \boldsymbol{b}_{\kappa}, \boldsymbol{b}_{i} \rangle)
 4:
 5:
                       for h=1 to j-1 do \overline{r}_{\kappa,j} \leftarrow \diamond(\overline{r}_{\kappa,j} - \diamond(\overline{r}_{\kappa,h} \times \overline{\mu}_{j,h}))
 6:
                       \overline{\mu}_{\kappa,i} \leftarrow \diamond(\overline{r}_{\kappa,i}/\overline{r}_{i,i})
             s_0^{(\kappa)} \leftarrow \|\boldsymbol{b}_n\|^2
 7:
              for j=1 to n do \overline{s}_i^{(\kappa)} \leftarrow \diamond (\overline{s}_{i-1}^{(\kappa)} - \diamond (\overline{\mu}_{n,j} \times \overline{r}_{n,j})) endfor; r_{n,n} \leftarrow s_n^{(\kappa)}
 8:
 9.
               for i = \kappa - 1 downto 1 do
                       if |\overline{\mu}_{\kappa,i}| \geq \overline{\eta} then X_i \leftarrow |\overline{\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 j=1 to i-1 do \overline{\mu}_{\kappa,i} \leftarrow \diamond (\overline{\mu}_{\kappa,i} - \diamond (X_i \times \overline{\mu}_{i,i}))
11:
              \boldsymbol{b}_{\kappa} \leftarrow \boldsymbol{b}_{\kappa} - \sum_{i=1}^{\kappa-1} X_{i} \boldsymbol{b}_{i}
12:
13: while (X_1,\ldots,X_{\kappa-1})\neq \mathbf{0}_{\kappa-1} /* すべての \mu_{\kappa,j} が size-reduce されたら終了 */
```

 佐藤
 勉強会
 June 30, 2025
 9 / 13

L^2 アルゴリズム (1/2)

L^2 アルゴリズムでは,大まかに次のようなことを行う

- 💵 基底を size-reduce(Algorithm 1) するとともに, $[r_{i,j}], [\mu_{i,j}], [s_i^{\kappa}]$ を計算
- ② $\delta r_{\kappa-1,\kappa-1} \leq s_{\kappa-1}^{(\kappa)}$ かどうか(Lovász 条件)
 - 偽 $\Longrightarrow \delta r_{\kappa-2,\kappa-2} \leq s_{\kappa-2}^{(\kappa)}$ かどうか . . .
 - 真 $\Longrightarrow [\mu_{i,j}], [r_{i,j}], [s_i^{\kappa}]$ を更新し,基底の交換

佐藤 勉強会 June 30, 2025 10 / 13

L^2 アルゴリズム (2/2)

Algorithm L^2 簡約

```
Require: パラメタ \frac{1}{4} < \delta < 1, \frac{1}{2} < \eta < \sqrt{\delta},基底 \{b_1, \ldots, b_n\}
Ensure: 簡約された基底 \{b_1, \ldots, b_n\}
 1: \overline{\delta} \leftarrow (\delta + 1)/2
 2: \overline{r}_1 \leftarrow \diamond(\|\boldsymbol{b}_1\|^2)
 3: \kappa \leftarrow 2
 4: while \kappa < n do
               size-reduce して [\overline{\mu}_{i,j}], [\overline{r}_{i,j}], [\overline{s}_{i}^{(\kappa)}] を計算 /* Algorithm 1 */
 5:
 6:
            \kappa' \leftarrow \kappa
            while \kappa > 2 \wedge \overline{\delta} \overline{r}_{\kappa-1} \kappa-1 > \overline{s}_{\kappa-1}^{(\kappa')} do /* Lovász 条件 */
 7:
                        \kappa \leftarrow \kappa - 1 /* 基底の交換は後回し */
 8:
 9:
               for i=1 to \kappa-1 do
                        \overline{\mu}_{\kappa,i} \leftarrow \overline{\mu}_{\kappa',i}; \ \overline{r}_{\kappa,i} \leftarrow \overline{r}_{\kappa',i}; \ \overline{r}_{\kappa,\kappa} \leftarrow \overline{s}_{\kappa}^{(\kappa')}
10:
               \{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}\leftarrow \{\ldots,\boldsymbol{b}_{\kappa-1},\boldsymbol{b}_{\kappa'},\boldsymbol{b}_{\kappa},\ldots,\boldsymbol{b}_{\kappa'-1},\boldsymbol{b}_{\kappa'+1},\ldots\}
11:
12:
                \kappa \leftarrow \kappa + 1
```

ullet $rac{1}{4}<\delta<1,rac{1}{2}<\eta<\sqrt{\delta}$:簡約パラメタ

$$\rho := \frac{(1+\eta)^2}{\delta - \eta^2}$$

 \bullet $\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\}$: n 次元格子 L の基底

• fpa の精度 ℓ は $n\rho^n 2^{-\ell+2} \le 1$ を満たす

• $M := \max_{j < n} |\mu_{n,j}|$

[?]

(2)
$$\forall j \leq \forall i < n, |\overline{r}_{i,j} - r_{i,j}| \leq n\rho^{j-1}2^{-\ell+4}r_{j,j} \wedge |\overline{\mu}_{i,j} - \mu_{i,j}| \leq n\rho^{j-1}2^{-\ell+6}$$

(3)
$$\forall j < n, \ |\overline{r}_{n,j} - r_{n,j}| \le n\rho^{j-1} M 2^{-\ell+4} r_{j,j} \wedge |\overline{\mu}_{n,j} - \mu_{n,j}| \le n\rho^{j-1} M 2^{-\ell+6}$$

 b_n が $\{b_1,\ldots,b_n\}$ に対して簡約パラメタ η に関してサイズ簡約されているとき

(4)
$$\left| \overline{s}_j^{(n)} - s_j^{(n)} \right| \le n \rho^{j-1} 2^{-\ell+7} r_{j,j} + n 2^{-\ell} s_j^{(n)}$$

◆□▶ ◆圖▶ ◆差▶ ◆差▶ 差 めぬ()

June 30, 2025

· 佐藤

参考文献 I