

勉強会形式ゼミ資料①

P.Q.Nguyen and D. Stehle Floating-Point LLL Revisited[1]

佐藤 新

July 4, 2025

本セミナーで用いられる記号など（基本は[1]に倣った記号）

- 全て $\{b_1, \dots, b_n\}$ を基底としてもつ整数格子
- $B = \max\{\|b\|_i \mid 1 \leq i \leq n\}$
- 浮動小数点数の演算精度は ℓ -bit
- $\diamond(a * b)$ は $a * b$ の浮動小数点演算 ($* \in \{+, -, \times, /\}$)
- $\pi_\ell : \mathbb{R}^n \rightarrow \langle b_1, \dots, b_{\ell-1} \rangle_{\mathbb{R}}^\perp : \langle b_1, \dots, b_{\ell-1} \rangle^\perp$ への直交射影

Gram-Schmidt の計算 (1/5)

今までの GSO 情報の持ち方

Gram-Schmidt の情報は

$$\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j \rangle - \sum_{k=1}^{j-1} \mu_{j,k} \mu_{i,k} \|\mathbf{b}_k^*\|^2}{\|\mathbf{b}_j^*\|^2}, \|\mathbf{b}_i^*\|^2 = \|\mathbf{b}_i\|^2 - \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\mathbf{b}_j^*\|^2$$

という公式で計算可能

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

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

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

という公式で計算可能な形で情報を持つ ($r_{i,i} = \|\mathbf{b}_i^*\|^2, r_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = \mu_{i,j} \|\mathbf{b}_j^*\|^2$)
⇨ 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

Gram-Schmidt の計算 (3/5)

Lovász 条件の書き換え

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

とすると, Lovász 条件 $\delta \|\mathbf{b}_{\kappa-1}^*\|^2 \leq \|\mathbf{b}_{\kappa}^*\|^2 + \mu_{\kappa,\kappa-1}^2 \|\mathbf{b}_{\kappa-1}^*\|^2$ は

$$\begin{aligned} \|\mathbf{b}_{\kappa}^*\|^2 + \mu_{\kappa,\kappa-1}^2 \|\mathbf{b}_{\kappa-1}^*\|^2 &= \|\mathbf{b}_{\kappa}\|^2 - \sum_{j=1}^{\kappa-2} \mu_{\kappa,j}^2 \|\mathbf{b}_j^*\|^2 = \|\mathbf{b}_{\kappa}\|^2 - \sum_{j=1}^{\kappa-2} \mu_{\kappa,j}^2 r_{\kappa,j} \\ &= s_{\kappa-1}^{(\kappa)} \end{aligned}$$

より

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

と書き換えることができる。

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

$$\{c_1, \dots, c_n\} := \{\dots, b_{\kappa-2}, b_\kappa, b_{\kappa-1}, b_{\kappa+1}, \dots\}$$

とすると, 交換後に検証すべき Lovász 条件は

$$(1) \quad \delta \|c_{\kappa-2}^\star\|^2 \leq \|c_{\kappa-1}^\star\|^2 + \nu_{\kappa-1, \kappa-2}^2 \|c_{\kappa-2}^\star\|^2$$

に移る.

Gram-Schmidt の計算 (5/5)

基底の更新後の Lovász 条件 (2/2)

$\|\mathbf{c}_{\kappa-2}^*\|^2 = \|\mathbf{b}_{\kappa-2}^*\|^2$, $\|\mathbf{c}_{\kappa-1}^*\| = \|\pi_{\kappa-1}(\mathbf{b}_{\kappa})\|$, $\nu_{\kappa-1,\kappa-2} = \mu_{\kappa-1,\kappa-2}$ であるので,

$$\begin{aligned}\text{式 (1)} &\iff \delta \|\mathbf{b}_{\kappa-2}^*\|^2 \leq \|\pi_{\kappa-1}(\mathbf{b}_{\kappa})\|^2 + \mu_{\kappa-1,\kappa-2} \|\mathbf{b}_{\kappa-2}^*\|^2 \\ &\iff \delta r_{\kappa-2,\kappa-2} \leq \mu_{\kappa,\kappa-1} \|\mathbf{b}_{\kappa-1}^*\|^2 + \|\mathbf{b}_{\kappa}^*\|^2 + \mu_{\kappa-1,\kappa-2} \|\mathbf{b}_{\kappa-2}^*\|^2 \\ &\iff \delta r_{\kappa-2,\kappa-2} \leq \|\mathbf{b}_{\kappa}\|^2 - \sum_{j=1}^{\kappa-3} \mu_{\kappa,j} r_{\kappa,j} \|\mathbf{b}_j^*\|^2 \\ &\iff \delta r_{\kappa-2,\kappa-2} \leq s_{\kappa-2}^{(\kappa)}\end{aligned}$$

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

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

- ① 基底 $\{b_1, \dots, b_n\}$ の Gram 行列 $G(b_1, \dots, b_n)$ の Cholesky 分解を利用して $[r_{\kappa,j}], [\mu_{\kappa,j}], [s_j^{(\kappa)}]$ を計算

- ② $|\mu_{\kappa,j}| \geq \frac{\eta + \frac{1}{2}}{2}$ のとき

- ▶ $b_{\kappa} \leftarrow b_{\kappa} - [\mu_{\kappa,j}] b_j$ で $|\mu_{\kappa,j}| \leq 1/2$ なるように基底を更新
- ▶ それに合わせて $[r_{\kappa,j}], [\mu_{\kappa,j}], [s_j^{(\kappa)}]$ も更新

※ 条件 $|\mu_{\kappa,j}| \geq \frac{\eta + \frac{1}{2}}{2}$ は $\eta \rightarrow \frac{1}{2} +$ のとき $|\mu_{\kappa,j}| > \frac{1}{2}$

Algorithm size-reduction[3]

Require: $\bar{\eta}$, $\kappa \in \mathbb{Z}$, 基底 $\{b_1, \dots, b_n\}$

Ensure: 簡約された基底 $\{b_1, \dots, b_n\}$

```
1: loop
2:   for  $j = 1$  to  $\kappa - 1$  do
3:      $\bar{r}_{\kappa,j} \leftarrow \diamond(\langle b_{\kappa}, b_j \rangle)$ ; for  $h = 1$  to  $j - 1$  do  $\bar{r}_{\kappa,j} \leftarrow \diamond(\bar{r}_{\kappa,j} - \diamond(\bar{\mu}_{j,h} \times \bar{r}_{\kappa,h}))$  endfor
4:      $\bar{\mu}_{\kappa,j} \leftarrow \diamond(\bar{r}_{\kappa,j} / \bar{r}_{j,j})$ 
5:      $s_1^{(\kappa)} \leftarrow \diamond(\|b_{\kappa}\|^2)$ ; for  $h = 1$  to  $j - 1$  do  $\bar{s}_h^{(\kappa)} \leftarrow \diamond(\bar{s}_{h-1}^{(\kappa)} - \diamond(\bar{\mu}_{\kappa,h-1} \times \bar{r}_{\kappa,h-1}))$  endfor
6:      $\bar{r}_{\kappa,\kappa} \leftarrow \bar{s}_j^{(\kappa)}$ 
7:   if  $\max_{i < \kappa} |\bar{\mu}_{\kappa,i}| > \bar{\eta}$  then
8:     for  $i = \kappa - 1$  downto 1 do
9:        $X \leftarrow \lfloor \bar{\mu}_{\kappa,i} \rfloor$ 
10:       $b_{\kappa} \leftarrow b_{\kappa} - X b_i$ 
11:      for  $j = 1$  to  $i - 1$  do
12:         $\bar{\mu}_{\kappa,j} \leftarrow \diamond(\mu_{\kappa,j} - \diamond(X \times \bar{\mu}_{i,j}))$ 
13:      else
14:        break
```

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

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

L^2 アルゴリズム (2/2)

Algorithm L^2 簡約 [1][2]

Require: パラメタ $\frac{1}{4} < \delta < 1, \frac{1}{2} < \eta < \sqrt{\delta}$, 基底 $\{b_1, \dots, b_n\}$

Ensure: 簡約された基底 $\{b_1, \dots, b_n\}$

- 1: $\bar{\delta} \leftarrow (\delta + 1)/2$
- 2: $\bar{r}_{1,1} \leftarrow \diamond(\|b_1\|^2)$
- 3: $\kappa \leftarrow 2$
- 4: **while** $\kappa \leq n$ **do**
- 5: size-reduce して $[\bar{\mu}_{i,j}], [\bar{r}_{i,j}], [\bar{s}_i^{(\kappa)}]$ を計算 /* Algorithm 1 */
- 6: $\kappa' \leftarrow \kappa$
- 7: **while** $\kappa \geq 2 \wedge \bar{\delta} \bar{r}_{\kappa-1, \kappa-1} \geq \bar{s}_{\kappa-1}^{(\kappa')}$ **do** /* Lovász 条件 */
- 8: $\kappa \leftarrow \kappa - 1$ /* 基底の交換は後回し */
- 9: **for** $i = 1$ to $\kappa - 1$ **do**
- 10: $\bar{\mu}_{\kappa,i} \leftarrow \bar{\mu}_{\kappa',i}; \bar{r}_{\kappa,i} \leftarrow \bar{r}_{\kappa',i}; \bar{r}_{\kappa,\kappa} \leftarrow \bar{s}_{\kappa}^{(\kappa')}$
- 11: $\{b_1, \dots, b_n\} \leftarrow \{\dots, b_{\kappa-1}, b_{\kappa'}, b_{\kappa}, \dots, b_{\kappa'-1}, b_{\kappa'+1}, \dots\}$
- 12: $\kappa \leftarrow \kappa + 1$

L^2 の精度

- $\frac{1}{4} < \delta < 1, \frac{1}{2} < \eta < \sqrt{\delta}$: 簡約パラメタ
- $\rho := \frac{(1+\eta)^2}{\delta-\eta^2}$
- fpa の精度 ℓ は $n\rho^n 2^{-\ell+2} \leq 1$ を満たす
- $M := \max_{j < n} |\mu_{n,j}|$

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

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

b_n が $\{b_1, \dots, b_n\}$ 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

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

L^2 の精度

- $\delta \approx 1, \eta \approx 1/2$ のとき $\rho \approx 3$
- $\ell = 64$ (double) のとき, $2^{-\ell+2} \approx 10^{-19}, 2^{-\ell+4} \approx 10^{-18}, 2^{-\ell+6} \approx 10^{-18}$

$$\begin{aligned} |\bar{r}_{i,j} - r_{i,j}| &\lesssim 10^{-19} \times 3^j n r_{j,j}, & |\bar{\mu}_{i,j} - \mu_{i,j}| &\lesssim 10^{-18} \times 3^j n \\ \left| \bar{s}_j^{(n)} - s_j^{(n)} \right| &\lesssim 10^{-18} \times 3^j n r_{j,j} + 10^{-19} n s_j^{(n)} \end{aligned}$$

DeepL² への展望

- deep-insertion 後の deep-exchange 条件の変化に関する考察
deep-exchange 条件

$$\begin{aligned}\delta \| \mathbf{b}_i^* \|^2 \leq \| \pi_i(\mathbf{b}_\kappa) \|^2 &\iff \delta \| \mathbf{b}_i^* \|^2 \leq \| \mathbf{b}_\kappa \|^2 - \sum_{j=1}^{i-1} \mu_{\kappa,j}^2 \| \mathbf{b}_j^* \|^2 \\ &\iff \delta r_{i,i} \leq s_\kappa^{(i)} \qquad (1 \leq \forall i < \forall \kappa \leq n)\end{aligned}$$

- $[r_{i,j}], [\mu_{i,j}], [s_j^{(i)}]$ のサイズ簡約外での更新

参考文献 I

- [1] Phong Q. Nguyen and Damien Stehlé. Floating-point LLL revisited. In Advances in Cryptology – EUROCRYPT 2005, pages 215–233. Springer Berlin Heidelberg, 2005.
- [2] Phong Q. Nguyen and Damien Stehlé. An LLL algorithm with quadratic complexity. SIAM Journal on Computing, 39(3):874–903, 2009.
- [3] Damien Stehlé. Floating-Point LLL: Theoretical and Practical Aspects, pages 179–213. Springer Berlin Heidelberg, 2010.