勉強会形式ゼミ資料①
P.Q.Nguyen and D. Stehle Floating-Point LLL Revisited[1]

佐藤 新

June 30, 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 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ 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 $(* \in \{+, -, \times, /\})$
- $\pi_\ell : \mathbb{R}^n \to \langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{\ell-1} \rangle_{\mathbb{R}}^{\perp}$: $\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{\ell-1} \rangle^{\perp}$ 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

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

という公式で計算可能

- 内積 $\langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle$ の計算に浮動小数点数（fpa）が必要
  $2^{-\ell}\|\boldsymbol{b}_i\|\|\boldsymbol{b}_j\|$ 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

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

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

$\rightsquigarrow$ 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

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

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

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

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．

Gram-Schmidt の計算（4/5）

基底の更新後の Lovász 条件（1/2）

更に $\boldsymbol{b}_\kappa$ と $\boldsymbol{b}_{\kappa-1}$ の交換後の基底

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

とすると，交換後に検証すべき Lovász 条件は

$$\delta \left\|\boldsymbol{c}^\star_{\kappa-2}\right\|^2 \leq \left\|\boldsymbol{c}^\star_{\kappa-1}\right\|^2 + \nu^2_{\kappa-1,\kappa-2} \left\|\boldsymbol{c}^\star_{\kappa-2}\right\|^2 \tag{1}$$

に移る．

Gram-Schmidt の計算（5/5）

基底の更新後の Lovász 条件（2/2）

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

$$
\begin{aligned}
\text{式 (1)} &\iff \delta\left\|\boldsymbol{b}^{\star}_{\kappa-2}\right\|^2 \leq \left\|\pi_{\kappa-1}(\boldsymbol{b}_{\kappa})\right\|^2 + \mu_{\kappa-1,\kappa-2}\left\|\boldsymbol{b}^{\star}_{\kappa-2}\right\|^2 \\
&\iff \delta r_{\kappa-2,\kappa-2} \leq \mu_{\kappa,\kappa-1}\left\|\boldsymbol{b}^{\star}_{\kappa-1}\right\|^2 + \left\|\boldsymbol{b}^{\star}_{\kappa}\right\|^2 + \mu_{\kappa-1,\kappa-2}\left\|\boldsymbol{b}^{\star}_{\kappa-2}\right\|^2 \\
&\iff \delta r_{\kappa-2,\kappa-2} \leq \left\|\boldsymbol{b}_{\kappa}\right\|^2 - \sum_{j=1}^{\kappa-3} \mu_{\kappa,j} r_{\kappa,j}\left\|\boldsymbol{b}^{\star}_{j}\right\|^2 \\
&\iff \delta r_{\kappa-2,\kappa-2} \leq s^{(\kappa)}_{\kappa-2}
\end{aligned}
$$

になるので，$[s^{(i)}_j]$ 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 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の Gram 行列 $G(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ 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
   - $\boldsymbol{b}_\kappa \leftarrow \boldsymbol{b}_\kappa - \lfloor \mu_{\kappa,j} \rceil \boldsymbol{b}_j$ 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 $\eta \to \frac{1}{2}+$ のとき $|\mu_{\kappa,j}| > \frac{1}{2}$

Algorithm L^2 内での size-reduction[1]

Require: パラメタ $\eta > 1/2$，$\kappa \in \mathbb{Z}$，基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
Ensure: $[\overline{r}_{\kappa,j}]$, $[\overline{\mu}_{\kappa,j}]$, $[\overline{s}_j^{(\kappa)}]$ $(j \leq \kappa)$，簡約された基底 $\{\ldots, \boldsymbol{b}_{\kappa-1}, \boldsymbol{b}'_\kappa, \boldsymbol{b}_{\kappa+1}, \ldots\}$

$\overline{\eta} \leftarrow \frac{\eta+1/2}{2} = \frac{2\eta+1}{4}$
do
  for $j = 1$ to κ **do** /* 部分的な Cholesky 分解で $[r_{\kappa,j}], [\mu_{\kappa,j}], [s_j^{(\kappa)}]$ を更新 */
    $\overline{r}_{\kappa,j} \leftarrow \diamond(\langle \boldsymbol{b}_\kappa, \boldsymbol{b}_j \rangle)$
    for $h = 1$ to $j-1$ **do** $\overline{r}_{\kappa,j} \leftarrow \diamond(\overline{r}_{\kappa,j} - \diamond(\overline{r}_{\kappa,h} \times \overline{\mu}_{j,h}))$
    $\overline{\mu}_{\kappa,j} \leftarrow \diamond(\overline{r}_{\kappa,j} / \overline{r}_{j,j})$
  $s_0^{(\kappa)} \leftarrow \|\boldsymbol{b}_n\|^2$
  for $j = 1$ to n **do** $\overline{s}_j^{(\kappa)} \leftarrow \diamond(\overline{s}_{j-1}^{(\kappa)} - \diamond(\overline{\mu}_{n,j} \times \overline{r}_{n,j}))$ **endfor**; $r_{n,n} \leftarrow s_n^{(\kappa)}$
  for $i = \kappa - 1$ downto 1 **do**
    if $\left|\overline{\mu}_{\kappa,i}\right| \geq \overline{\eta}$ **then** $X_i \leftarrow \left\lfloor \overline{\mu}_{\kappa,i} \right\rceil$ **else** $X_i \leftarrow 0$ /* $|\mu_{\kappa,i}|$ により係数ベクトルを決定 */
    for $j = 1$ to $i-1$ **do** $\overline{\mu}_{\kappa,j} \leftarrow \diamond(\overline{\mu}_{\kappa,j} - \diamond(X_i \times \overline{\mu}_{i,j}))$
  $\boldsymbol{b}_\kappa \leftarrow \boldsymbol{b}_\kappa - \sum_{i=1}^{\kappa-1} X_i \boldsymbol{b}_i$
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 */

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 $\Longrightarrow \delta r_{\kappa-2,\kappa-2} \leq s_{\kappa-2}^{(\kappa)}$ かどうか . . .
   - 真 $\Longrightarrow [\mu_{i,j}], [r_{i,j}], [s_j^\kappa]$ 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]

Require: パラメタ $\frac{1}{4} < \delta < 1, \frac{1}{2} < \eta < \sqrt{\delta}$，基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
Ensure: 簡約された基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

$\overline{\delta} \leftarrow (\delta + 1)/2$
$\overline{r}_{1,1} \leftarrow \diamond(\|\boldsymbol{b}_1\|^2)$
$\kappa \leftarrow 2$
while $\kappa \leq n$ **do**
    size-reduce して $[\overline{\mu}_{i,j}], [\overline{r}_{i,j}], [\overline{s}_i^{(\kappa)}]$ を計算　/* Algorithm 1 */
    $\kappa' \leftarrow \kappa$
    while $\kappa \geq 2 \wedge \overline{\delta}\overline{r}_{\kappa-1,\kappa-1} \geq \overline{s}_{\kappa-1}^{(\kappa')}$ **do**　/* Lovász 条件 */
        $\kappa \leftarrow \kappa - 1$　/* 基底の交換は後回し */
    for $i = 1$ to $\kappa - 1$ **do**
        $\overline{\mu}_{\kappa,i} \leftarrow \overline{\mu}_{\kappa',i}$; $\overline{r}_{\kappa,i} \leftarrow \overline{r}_{\kappa',i}$; $\overline{r}_{\kappa,\kappa} \leftarrow \overline{s}_{\kappa}^{(\kappa')}$
    $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \leftarrow \{\ldots, \boldsymbol{b}_{\kappa-1}, \boldsymbol{b}_{\kappa'}, \boldsymbol{b}_{\kappa}, \ldots, \boldsymbol{b}_{\kappa'-1}, \boldsymbol{b}_{\kappa'+1}, \ldots\}$
    $\kappa \leftarrow \kappa + 1$

L^2 の精度

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

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

(3) $$\forall j < n,\ |\overline{r}_{n,j} - r_{n,j}| \leq n\rho^{j-1}M2^{-\ell+4} r_{j,j} \wedge \left|\overline{\mu}_{n,j} - \mu_{n,j}\right| \leq n\rho^{j-1}M2^{-\ell+6}$$

$\boldsymbol{b}_n$ が $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ 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) $$\left|\overline{s}_j^{(n)} - s_j^{(n)}\right| \leq n\rho^{j-1}2^{-\ell+7} r_{j,j} + n2^{-\ell} s_j^{(n)}$$

L^2 の精度

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

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

DeepL^2 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

$$\delta\|\boldsymbol{b}_i^\star\|^2 \le \|\pi_i(\boldsymbol{b}_\kappa)\|^2 \iff \delta\|\boldsymbol{b}_i^\star\|^2 \le \|\boldsymbol{b}_\kappa\|^2 - \sum_{j=1}^{i-1}\mu_{\kappa,j}^2\|\boldsymbol{b}_j^\star\|^2$$

$$\iff \delta r_{i,i} \le s_\kappa^{(i)} \qquad (1 \le {}^\forall i < {}^\forall \kappa \le n)$$

- $[r_{i,j}], [\mu_{i,j}], [s_j^{(i)}]$ 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 Ronald Cramer, editor, Advances in Cryptology – EUROCRYPT 2005, pages 215–233. Springer Berlin Heidelberg, 2005.