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

本セミナーで用いられる記号など

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

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

$\rightsquigarrow$ 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

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

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

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

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

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

とすると，交換後に検証すべき Lovász 条件は

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

に移る．

Gram-Schmidt の計算（5/5）

基底の更新後の Lovász 条件（2/2）

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

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

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

Algorithm L^2 内での size-reduction

Require: パラメタ $\eta > 1/2$，$\kappa \in \mathbb{Z}$，基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Ensure: $[\bar{r}_{\kappa,j}]$, $[\bar{\mu}_{\kappa,j}]$, $[\bar{s}_j]$ $(j \le \kappa)$，$\{\ldots, \boldsymbol{b}_{\kappa-1}, \boldsymbol{b}'_\kappa, \boldsymbol{b}_{\kappa+1}, \ldots\}$

$\bar{\eta} \leftarrow \frac{\eta+1/2}{2} = \frac{2\eta+1}{4}$

do

  for $j = 1$ to κ **do** /*Cholesky 分解*/

    $\bar{r}_{i,j} \leftarrow \langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle$

    for $k = 1$ to $j-1$ **do** $\bar{r}_{i,j} \leftarrow \diamond(\bar{r}_{i,j} - \diamond(\bar{r}_{i,k}\bar{\mu}_{j,k}))$

    $\bar{\mu}_{i,j} \leftarrow \diamond(\bar{r}_{i,j}/\bar{r}_{j,j})$

  $s_0 \leftarrow \|\boldsymbol{b}_n\|^2$

  for $k = 1$ to $j-1$ **do** $\bar{s}_j \leftarrow \diamond(\bar{s}_{j-1} - \diamond(\bar{\mu}_{n,j}\bar{r}_{n,j}))$

  $r_{n,n} \leftarrow s_n$

  for $i = \kappa - 1$ downto 1 **do**

    if $|\bar{\mu}_{k,i}| \ge \bar{\eta}$ **then** $X_i \leftarrow \lfloor \bar{\mu}_{k,i} \rceil$ **else** $X_i \leftarrow 0$

    for $j = 1$ to $i-1$ **do** $\bar{\mu}_{k,j} \leftarrow \diamond(\bar{\mu}_{\kappa,j} - \diamond(X_i\bar{\mu}_{i,j}))$

  $\boldsymbol{b}_\kappa \leftarrow \boldsymbol{b}_\kappa - \sum_{i=1}^{\kappa-1} X_i \boldsymbol{b}_i$

while $X \ne \boldsymbol{0}_{\kappa-1}$

Algorithm L^2 簡約

Require: パラメタ η, δ，基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
Ensure: 簡約された基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

$\bar{\delta} \leftarrow (\delta + 1)/2$
$\bar{r}_{1,1} \leftarrow \|\boldsymbol{b}_1\|^2$
$\kappa \leftarrow 2$
while $\kappa \leq n$ **do**
    size-reduce (Algorithm 1)
    $\kappa' \leftarrow \kappa$
    while $\kappa \geq 2 \wedge \bar{\delta}\bar{r}_{\kappa-1,\kappa-1} \geq \bar{s}_{\kappa-1}$ **do**
        $\kappa \leftarrow \kappa - 1$
    for $i = 1$ to $\kappa - 1$ **do**
        $\bar{\mu}_{\kappa,i} \leftarrow \bar{\mu}_{\kappa',i}$; $\bar{r}_{\kappa,i} \leftarrow \bar{r}_{\kappa',i}$; $\bar{r}_{\kappa,\kappa} \leftarrow \bar{s}_{\kappa}$
    $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \leftarrow \{\ldots, \boldsymbol{b}_{\kappa'-1}, \boldsymbol{b}_{\kappa'+1}, \ldots, \boldsymbol{b}_{\kappa'}, \boldsymbol{b}_{\kappa}, \ldots\}$
    $\kappa \leftarrow \kappa + 1$

参考文献 I