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

佐藤 新

June 24, 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

Gram-Schmidt の計算

Gram-Schmidt の情報は

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

という公式で計算可能

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

Gram-Schmidt の計算

Gram-Schmidt の情報から

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

という公式で計算可能な形で情報を持つ

Algorithm L^2 内での size-reduction

Require: 格子 L の基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$
Ensure: δ に関して LLL 簡約された基底

$\bar{\eta} \leftarrow \frac{\eta+1/2}{2} = \frac{2\eta+1}{4}$
do
  for $j = 1$ to κ **do**
    $r_{i,j} \leftarrow \langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle$
    for $k = 1$ to $j-1$ **do** $r_{i,j} \leftarrow r_{i,j} - r_{i,k}\mu_{j,k}$
    $\mu_{i,j} \leftarrow \frac{r_{i,j}}{r_{j,j}}$
  $s_0 \leftarrow \|\boldsymbol{b}_n\|^2$
  for $k = 1$ to $j-1$ **do** $s_j \leftarrow s_{j-1} - \mu_{n,j} r_{n,j}$
  $r_{n,n} \leftarrow s_n$
  for $i = \kappa - 1$ downto 1 **do**
    if $|\bar{\mu}_{k,i}| \geq \bar{\eta}$ **then** $X_i \leftarrow \lfloor \bar{\mu}_{k,i} \rceil$ **else** $X_i \leftarrow 0$
    for $j = 1$ to $i-1$ **do** $\bar{\mu}_{k,j} \leftarrow \bar{\mu}_{\kappa,j} - X_i \bar{\mu}_{i,j}$
while $X \neq \mathbf{0}$

参考文献 I