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

佐藤 新

June 26, 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（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

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

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

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

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

と書き換えることができる．更に $\boldsymbol{b}_{\kappa}$ と $\boldsymbol{b}_{\kappa-1}$ の交換後は Lovász 条件は

$$\delta r_{\kappa-2,\kappa-2} \leq s_{\kappa-2}^{(\kappa)}$$

になるので，**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: $[\bar{r}_{\kappa,j}]$, $[\bar{\mu}_{\kappa,j}]$, $[\bar{s}_j]$ $(j \leq \kappa)$，$\{\ldots, \boldsymbol{b}_{\kappa-1}, \boldsymbol{b}'_{\kappa}, \boldsymbol{b}_{\kappa+1}, \ldots\}$
$\bar{\eta} \leftarrow \frac{\eta+1/2}{2} = \frac{2\eta+1}{4}$
do
    for $j = 1$ to $\kappa$ do    /*Cholesky 分解*/
        $\bar{r}_{i,j} \leftarrow \langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle$
        for $k = 1$ to $j - 1$ do $\bar{r}_{i,j} \leftarrow \bar{r}_{i,j} - \bar{r}_{i,k}\bar{\mu}_{j,k}$
        $\bar{\mu}_{i,j} \leftarrow \bar{r}_{i,j}/\bar{r}_{j,j}$
    $s_0 \leftarrow \|\boldsymbol{b}_n\|^2$
    for $k = 1$ to $j - 1$ do $\bar{s}_j \leftarrow \bar{s}_{j-1} - \bar{\mu}_{n,j}\bar{r}_{n,j}$
    $r_{n,n} \leftarrow s_n$
    for $i = \kappa - 1$ downto 1 do
        if $|\bar{\mu}_{k,i}| \geq \bar{\eta}$ then $X_i \leftarrow \lfloor \bar{\mu}_{k,i} \rceil$ else $X_i \leftarrow 0$
        for $j = 1$ to $i - 1$ do $\bar{\mu}_{k,j} \leftarrow \bar{\mu}_{\kappa,j} - X_i\bar{\mu}_{i,j}$
    $\boldsymbol{b}_\kappa \leftarrow \boldsymbol{b}_\kappa - \sum_{i=1}^{\kappa-1} X_i\boldsymbol{b}_i$
while $X \neq \boldsymbol{0}_{\kappa-1}$
```

参考文献 I