

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 $\{b_1, \dots, b_n\}$ 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 ($* \in \{+, -, \times, /\}$)

Gram-Schmidt の計算

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

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

⇨ 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

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

とすると, Lovász 条件 $\delta \|\mathbf{b}_{\kappa-1}^*\|^2 \leq \|\mathbf{b}_{\kappa}^*\|^2 + \mu_{\kappa,\kappa-1}^2 \|\mathbf{b}_{\kappa-1}^*\|^2$ 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 \mathbf{b}_{κ} と $\mathbf{b}_{\kappa-1}$ 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 $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$

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

```
1:  $\bar{\eta} \leftarrow \frac{\eta+1/2}{2} = \frac{2\eta+1}{4}$ 
2: do
3:   for  $j = 1$  to  $\kappa$  do /*Cholesky 分解*/
4:      $\bar{r}_{i,j} \leftarrow \langle \mathbf{b}_i, \mathbf{b}_j \rangle$ 
5:     for  $k = 1$  to  $j - 1$  do  $\bar{r}_{i,j} \leftarrow \diamond(\bar{r}_{i,j} - \diamond(\bar{r}_{i,k} \bar{\mu}_{j,k}))$ 
6:      $\bar{\mu}_{i,j} \leftarrow \diamond(\bar{r}_{i,j} / \bar{r}_{j,j})$ 
7:      $s_0 \leftarrow \|\mathbf{b}_n\|^2$ 
8:     for  $k = 1$  to  $j - 1$  do  $\bar{s}_j \leftarrow \diamond(\bar{s}_{j-1} - \diamond(\bar{\mu}_{n,j} \bar{r}_{n,j}))$ 
9:      $r_{n,n} \leftarrow s_n$ 
10:    for  $i = \kappa - 1$  downto  $1$  do
11:      if  $|\bar{\mu}_{k,i}| \geq \bar{\eta}$  then  $X_i \leftarrow \lfloor \bar{\mu}_{k,i} \rfloor$  else  $X_i \leftarrow 0$ 
12:      for  $j = 1$  to  $i - 1$  do  $\bar{\mu}_{k,j} \leftarrow \diamond(\bar{\mu}_{\kappa,j} - \diamond(X_i \bar{\mu}_{i,j}))$ 
13:       $\mathbf{b}_{\kappa} \leftarrow \mathbf{b}_{\kappa} - \sum_{i=1}^{\kappa-1} X_i \mathbf{b}_i$ 
14: while  $X \neq \mathbf{0}_{\kappa-1}$ 
```

Algorithm L^2 簡約

Require: パラメタ η, δ , 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: $\bar{r}_{1,1} \leftarrow \|b_1\|^2$
- 3: $\kappa \leftarrow 2$
- 4: **while** $\kappa \leq n$ **do**
- 5: size-reduce (Algorithm 1)
- 6: $\kappa' \leftarrow \kappa$
- 7: **while** $\kappa \geq 2 \wedge \bar{\delta} \bar{r}_{\kappa-1, \kappa-1} \geq \bar{s}_{\kappa-1}$ **do**
- 8: $\kappa \leftarrow \kappa - 1$
- 9: **for** $i = 1$ to $\kappa - 1$ **do**
- 10: $\bar{\mu}_{\kappa, i} \leftarrow \bar{\mu}_{\kappa', i}; \bar{r}_{\kappa, i} \leftarrow \bar{r}_{\kappa', i}; \bar{r}_{\kappa, \kappa} \leftarrow \bar{s}_{\kappa}$
- 11: $\{b_1, \dots, b_n\} \leftarrow \{\dots, b_{\kappa'-1}, b_{\kappa'+1}, \dots, b_{\kappa'}, b_{\kappa}, \dots\}$
- 12: $\kappa \leftarrow \kappa + 1$

参考文献 I