格子解読アルゴリズムの数理構造 および 解読記録について (王 贇强 / 大阪大)

Contents

□ lattice : $\mathbb{b}_1, \cdots, \mathbb{b}_n \in \mathbb{R}^m$ が $\mathbb{R}$上一次独立で

$$\mathcal{L}(\mathbb{b}_1, \cdots, \mathbb{b}_n) := \mathbb{Z}\mathbb{b}_1 \oplus \cdots \oplus \mathbb{Z}\mathbb{b}_n$$

を格子という.

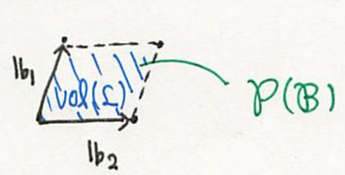
$$\Lambda := \mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathbb{b}_1, \cdots, \mathbb{b}_n).$$

・$n = m$ のとき, フルランクという.

・2つの基底 $\mathcal{B}, \mathcal{B}'$ に対しては,

$$\exists \text{unimodular mat. } U \text{ (s.t.) } U \cdot \mathcal{B} = \mathcal{B}'$$

・格子のボリューム : $\mathrm{vol}(\mathcal{L}) := \sqrt{|\det(\mathcal{B} \cdot {}^t\mathcal{B})|} \underset{\text{if full-rank}}{=} |\det(\mathcal{B})|$



・Fundamental domain : $\mathcal{P}_{\frac{1}{2}}(\mathcal{B}) = \left\{ \sum x_i \mathbb{b}_i \;\middle|\; -\frac{1}{2} \leq x_i < \frac{1}{2} \right\}$ or

$$\mathcal{P}(\mathcal{B}) := \left\{ \sum x_i \mathbb{b}_i \;\middle|\; 0 \leq x_i < 1 \right\}$$

・逐次最小 : $\lambda_i(\mathcal{L}) := \min\limits_{\substack{\mathbb{b}'_1, \cdots, \mathbb{b}'_i \in \mathcal{L} \\ \text{一次独立}}} \max\{\|\mathbb{b}'_1\|, \cdots, \|\mathbb{b}'_i\|\}$

$$\lambda_1(\mathcal{L}) = \min_{\mathbb{v} \in \mathcal{L} - \{0\}} \|\mathbb{v}\|$$

・代表的な格子問題 …… 最短ベクトル問題 (SVP)

・$\mathcal{L}$ の basis $\mathcal{B}$ が与えられたとき、$\|\mathbf{v}\| = \lambda_1(\mathcal{L})$ となる $\mathbf{v} \in \mathcal{L}$ をみつける問題.

・ランダム帰着の下で NP-困難

NP-complete なので……

→ 近似最短ベクトル問題

$\mathcal{L}$ の basis $\mathcal{B}$ と $\gamma \geq 1$ が与えられたとき、$\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$ となるような $\mathbf{v} \in \mathcal{L}$ をみつける.

(γ によって困難さが変わる. $\gamma = 1$ のときは SVP)

これを解くためのアプローチ:

・簡約アルゴリズム : input : "bad" basis
output : "better" basis, whose vectors are shorter & rel. orthogonal to each other

・探索アルゴリズム : input : a basis
output : a non-zero (approximate) shortest vector

(長さを1にはしない, 格子も変わる)

$\mathcal{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ を直交化したものを $\mathcal{B}^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ とする.

Good basis : $\max \|\mathbf{b}_i^*\| \approx \min \|\mathbf{b}_i^*\|$

Bad basis : $\max \|\mathbf{b}_i^*\| \gg \min \|\mathbf{b}_i^*\|$

・直交射影, $\pi_\ell : \mathbb{R}^n \longrightarrow \langle \mathbf{b}_1, \dots, \mathbf{b}_{\ell-1} \rangle_{\mathbb{R}}^{\perp}$ for $1 \leq \ell \leq n$.

$$\langle \mathbf{b}_1, \dots, \mathbf{b}_{\ell-1} \rangle_{\mathbb{R}}^{\perp} = \langle \mathbf{b}_\ell^*, \dots, \mathbf{b}_n^* \rangle$$

このとき, $\mathbf{b}_i = \sum_{j=1}^{i} \mu_{ij} \mathbf{b}_j^*$ なので, $\pi_\ell(\mathbf{b}_i) = \sum \mu_{ij} \mathbf{b}_j^*$ ($i \geq \ell$)

直交化の係数

$\forall \mathbf{x} \in \mathrm{span}_{\mathbb{R}}(\mathcal{L})$ に対して $\pi_\ell(\mathbf{x}) = \sum_{j=\ell}^{n} \frac{\langle \mathbf{x}, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|} \mathbf{b}_j^*$.

$\rightsquigarrow \pi_\ell(\mathcal{B}) = \{\pi_\ell(\mathbf{b}_\ell), \dots, \pi_\ell(\mathbf{b}_n)\}$

・$\mathcal{B}$ の QR分解：R は下三角行列，Q は正規直交基底で

$$\mathcal{B} = RQ$$

ただし，

$$R = \begin{pmatrix} \|b_1^*\| & & & 0 \\ \mu_{11}\|b_1^*\| & \ddots & & \\ \vdots & & \ddots & \\ \mu_{n1}\|b_1^*\| & \cdots & \mu_{n\,n-1}\|b_{n-1}^*\| & \|b_n^*\| \end{pmatrix}$$

□ Gauss - Heuristic

$\mathcal{L}$：n-次元格子

$S \subset \mathbb{R}^m$ が 連続 (convex, symmetric) な部分集合

$\rightsquigarrow$ $\#\{$格子点 $S \cap \mathcal{L}\} \approx \mathrm{vol}(S)/\mathrm{vol}(\mathcal{L})$

$\rightsquigarrow$ $\lambda_1(\mathcal{L}) = GH(\mathcal{L}) := V_n(1)^{-\frac{1}{n}}\,\mathrm{vol}(\mathcal{L})^{\frac{1}{n}} \approx \sqrt{\frac{n}{2\pi e}}\,\mathrm{vol}(\mathcal{L})^{\frac{1}{n}}$

n次元球の体積

$$= \frac{\pi^{\frac{n}{2}}}{\Gamma(1+\frac{n}{2})}$$

□ $HF(\mathcal{B}) := \delta(n)^n = \|b_1\| \cdot \frac{1}{\mathrm{vol}(\mathcal{L})^{\frac{1}{n}}}$

$$\left(\delta(n) = \left(\frac{\|b_1\|}{\mathrm{vol}(\mathcal{L})^{\frac{1}{n}}} \right)^{\frac{1}{n}} \right)$$

(これを root Hermite Factor という)