Редукция базиса решетки

Monday 25 January 2021 22:34

Смысл: нахождение "хорошего" представления (базиса) решётки.

I. HNF (Hermite Normal Form)
Эрмитова Нормальная Форма

$\forall B \in \mathbb{Z}^{n\times k}$, $\exists U \in GL_k(\mathbb{Z})$, т.ч. $B \cdot U = \begin{bmatrix} 0\ 0\ \dots\ 0 \\ \times\ \times\ \dots\ \times \\ 0\ \times\ \dots\ \times \\ \vdots \\ 0\ 0\ \dots\ \times \end{bmatrix}$, и коэфф. в строке с эл-том $\times$ на главной диагонали лежат в интервале $[0, \times)$

Полученная матрица уникальна для B и носит название HNF формы B.

Находится HNF аналог. "Гауссову преобр-ию" (Gaussian elimination), где деление заменено на НОД

Приложение: B_1, B_2 - базисы $L_1, L_2 \subseteq \mathbb{Z}^n$, HNF позволяет вычислить базис $L_1 + L_2 = B_1\mathbb{Z}^n + B_2\mathbb{Z}^n$, а именно $HNF(B_1 \| B_2)$.

Сложность вычисления HNF: $\tilde{O}\left(\max(n,k)^{\omega+1} \cdot \lg \max \|b_i\|\right)$ - битовая сложность.

II QR - факторизация

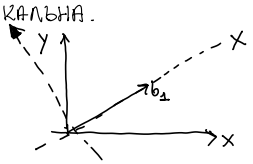
$Q^T \cdot Q = Q \cdot Q^T = Id$

Опр. 1 $\forall B \in \mathbb{R}^{n\times n}$, $\det B \neq 0$. $\exists$ Q - ортогональная и R - Δ-ая матрицы, т.ч.

$B = QR$ $\quad$ $\boxed{B} = \boxed{Q} \cdot \boxed{R}$, $r_{ii} > 0$ $\forall i$.

Такая декомпозиция уникальна.

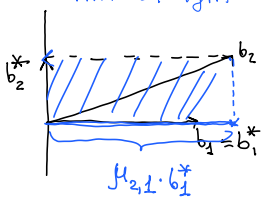
Смысл Q:



QR - факторизация связана с ортогонализацией Грам-Шмидта

$b_1^* = b_1$

$b_i^* = b_i - \sum_{j<i} \mu_{i,j} b_j^*$, $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$, $\mu_{ii} = 1$



$B = Q \cdot R = Q \cdot \underbrace{diag(r_{ii})}_{B^*} \cdot \underbrace{diag(r_{ii})^{-1} \cdot R}_{(\mu_{ij})_{i,j}}$

$\begin{bmatrix} r_{11} & & & \\ & r_{22} & & \\ & & \ddots & \\ & & & r_{nn} \end{bmatrix}$

Замечание: QR и Г-Ш несут одну и ту же инф-цию о решётке

1) Q, R не обязаны быть рациональными, B^*, μ - рациональны для $B \in \mathbb{Z}^{n\times n}$ и их битовая длина числ./знаменат. эл-тов B^*, μ полином. от $\lg(b_{ij})$.

Сложность: $O(n^3)$ арифмет. операций ↗ точно Г-Ш
↘ прибл. QR

Лемма 1. $\forall x$: $\|Bx\| = \|Rx\|$, $B = QR$.

$\triangleleft$ $\|Bx\| = \|\underbrace{QRx}_{y}\| = \|Qy\| = \sqrt{\langle Qy, Qy\rangle} = \sqrt{\langle y^T Q^T, Q \cdot y\rangle} = \sqrt{y^T \underbrace{Q^T \cdot Q}_{I} \cdot y} = \sqrt{y^T \cdot y} = \|y\| = \|Rx\|$ $\triangleright$.

Лемма 2 $L = L(B)$, $B = QR$. $\lambda_1(L) \geq \min_i (r_{ii})$.

$\triangleleft$ $b = B \cdot x$, $x \in \mathbb{Z}^n$, $b = \lambda_1(L)$

Лемма 1 $\Rightarrow$ $\|b\| = \|QRx\| = \|Rx\| = \|(\dots, \underbrace{r_{n-1,n-1} \cdot x_{n-1} + r_{n-1,n} \cdot x_n}_{\neq 0}, \underbrace{r_{nn} \cdot x_n}_{\neq 0})\|$

$\begin{bmatrix} 0 & \dots & r_{n-1,n-1} & r_{n-1,n} \\ & & & r_{nn} \end{bmatrix}$

- $x_n \neq 0$, тогда $\|(\dots, \dots, r_{nn} \cdot x_n)\| \geq r_{nn}$
- $x_n = 0$, $x_{n-1} \neq 0$, тогда $\|(\dots r_{n-1,n-1} \cdot x_{n-1}, 0)\| \geq r_{n-1,n-1}$
- $x_{n-1} = x_n = 0$, тогда $\|(\dots r_{n-2,n-2} \cdot x_{n-2}, 0, 0)\| \geq r_{n-2,n-2}$, x_{n-2}

Рассматриваем max i, т.ч. $x_i \neq 0$. $\triangleright$.