LLL алгоритм

Monday 1 February 2021 22:58

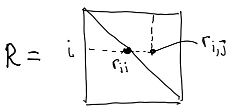
(Lenstra – Lenstra – Lovász '82)

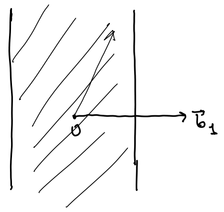
I "Редукция размера" (size-reduction)

Опр. 1 Базис $B = QR$ называется редуцированным по р-ру, если

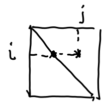
$$|r_{ij}| < \frac{r_{ii}}{2} \quad \forall i<j$$

Геометрически:





$\lceil \cdot \rfloor$, $\lfloor \cdot \rceil$ – округление



$r_{ij} - \lceil \frac{r_{ij}}{r_{ii}} \rfloor \cdot r_{ii}$ $\qquad r_{ij}^{новое} = r_{ij} + \lfloor -\frac{r_{ij}}{r_{ii}} \rceil \cdot r_{ii} \Rightarrow r_{ij}^{новое} \le \frac{|r_{ii}|}{2}$;

Замечание: для того, чтобы редуцировать строку, идём снизу вверх, т.к. редукция r_{ij} "портит" $r_{i'j}$ $\forall i'<i$.

Алгоритм редукции размера:

для j-ого столбца:

For $i = j-1$ to 1:

 $b_j \leftarrow b_j + \lceil -\frac{r_{ij}}{r_{ii}} \rfloor \cdot b_i$ // для текущего базиса

 For $k=1$ to i:

  $r_{kj} \leftarrow r_{kj} + \lceil -\frac{r_{ij}}{r_{ii}} \rfloor \cdot r_{ki}$ // изменение в R-факторе

$O(n^3)$ арифм. операций для 1 столбца

Если мы можем редуцировать r_{ii}, то мы можем редуцировать r_{ij} ⇒ сделать R малым.

Замечание: $\prod r_{ii} = |\det B| = \det L$ – не меняется относ. лин. преобр-ий ⇒ редукция р-ра делает r_{ii} сбалансированными.

Лемма 1 Пусть $B \subseteq \mathbb{R}^{n\times n}$ – базис L. Пусть $s_1, \dots, s_n \in L$ – лин. независ. и короткие. Тогда мы можем найти C – короткий базис L, т.ч.

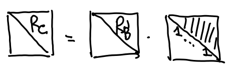
$$\|C_i\| \le \max_{j\le i} \|s_j\| \cdot \sqrt{i} \quad \forall i.$$

◄ $\exists T \in \mathbb{Z}^{n\times n}$: $S = B\cdot T$ ($\det T \ne 0$, т.к. s_i лин. незав.); HNF для T^t ⇒ $T^t = \underset{\text{нижне-}\Delta}{H} \cdot \underset{\text{унимод.}}{U}$; $T = (T^t)^t = (H\cdot U)^t = U^t \cdot H^t$ $\Big\}$ $S = \underbrace{B\cdot U^t}_{\text{базис } L} \cdot \overbrace{H^t}^{\text{верхне-}\Delta}$, $B' = B\cdot U^t$

S ⇓ QR-факт-ия: $Q_S R_S = Q_{B'} R_{B'} \cdot \underbrace{H^t}_{\text{верхне-}\Delta}$; ($B'$ ⇓ QR-фактор)

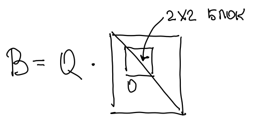
т.к. QR-фак-ия уникальна $R_S = R_{B'} \cdot H^t \Rightarrow r_{ii}^{(S)} = r_{ii}^{(B')} \cdot \underbrace{h_{ii}}_{\in \mathbb{Z},\, \ge 1} \Rightarrow r_{ii}^{(B')} \le r_{ii}^{(S)} \le \|S_i\|$

Определим C как редукцию р-ра для B';



$\Rightarrow \forall i \;\; r_{ii}^{(C)} = r_{ii}^{(B)} \le \|S_i\| \Rightarrow \|C_i\|^2 = \|r_i^{(C)}\|^2 = \sum_{k\le i} r_{ki}^2 \le \sum_{k<i} r_{ki}^2 + r_{ii}^2 \le$
$\le \sum_{k<i} \frac{1}{4} r_{kk}^2 + r_{ii}^2 \le i \cdot \max_{k\le i} r_{kk}^2$. ►

II LLL алгоритм



$\begin{bmatrix} r_{ii} & r_{i,i+1} \\ 0 & r_{i+1,i+1} \end{bmatrix} \xrightarrow{\text{SWAP}} \underbrace{\begin{bmatrix} r_{ii} & r_{i,i+1} \\ 0 & r_{i+1,i+1} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}$

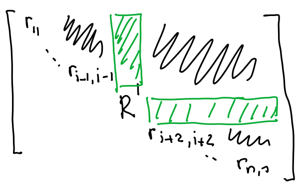
⇓ QR факторизация даст R' фактор

длина $\begin{bmatrix} r_{i,i+1} \\ r_{i+1,i+1} \end{bmatrix}$

$$R' = \begin{bmatrix} (r_{i,i+1}^2 + r_{i+1,i+1}^2)^{1/2} & \text{не важно} \\ 0 & \dfrac{r_{ii}\cdot r_{i+1,i+1}}{(r_{i,i+1}^2 + r_{i+1,i+1}^2)^{1/2}} \end{bmatrix}$$

В целом для базиса B

$$B' = B \cdot \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix} \xRightarrow{\text{QR-факторизация } B'} Q' \cdot$$



"SWAP" имеет след. эффект на R-фактор:

$$r_{ii} \to (r_{i,i+1}^2 + r_{i+1,i+1}^2)^{1/2}$$

$$r_{i+1,i+1} \to \frac{r_{ii} \cdot r_{i+1,i+1}}{(r_{i,i+1}^2 + r_{i+1,i+1}^2)^{1/2}}$$

Если $\underline{r_{i,i+1}^2 + r_{i+1,i+1}^2} < r_{ii}^2$, то "SWAP" сделает убывание r_{jj}-ых менее быстрым;

Алгоритм LLL (спар-ром $\delta < 1$, $\delta > \frac{1}{2}$)

Вход: $B \in \mathbb{Z}^{n \times n}$

1. Вычислить QR-факт-ия
2. Редукция р-ра R-фактора
3. Если $\exists i$, т.ч. $\left(r_{i,i+1}^2 + r_{i+1,i+1}^2\right)^{1/2} < \delta \cdot r_{ii}$

   $b_i \leftrightarrow b_{i+1}$ // SWAP (b_i, b_{i+1})

   Restart

   иначе

   Вернуть $b_1 \dots b_n$.

Сложность

задана числом итераций (Restart'ов);

Смотрим на $$P = \prod_{i=1}^{n} \Big[\underbrace{\prod_{j=1}^{i} r_{jj}}_{\det R_{[1..i]\times[1..i]}} \Big]^2$$ ← вел-на меняется только при операции SWAP

$$\underbrace{\qquad\qquad}_{\det\left([b_1\|..\|b_i]^T \cdot [b_1\|..\|b_i]\right)}$$

Если делаем SWAP для r_{ii}:

- $\forall i' < i$ $\left(\prod_{j=1}^{i'} r_{jj}\right)^2$ не изменится
- $\forall i' > i$ $\left(\prod_{j=1}^{i'} r_{jj}\right)$ не изменится (т.к. $L(b_1 .. b_{i'})$ не изменится, а значит, не изменится её опр-ль $\left(\prod_{j=1}^{i'} r_{jj}^2\right)$)
- только $\left(\prod_{j \le i} r_{jj}\right)^2$ изменится, в этом пр-ии изменится только r_{ii}^2 при операции SWAP, а именно, $P^{\text{"после"}} \le \delta^2 \cdot P^{\text{"до"}}$

в начале $P = \prod_{i=1}^{n} \underbrace{(\det L[b_1\|..\|b_i])^2}_{\le \prod_{j=1}^{i} \|b_j\|^2} \underset{\text{н-во Адамара}}{\le} \prod_{i=1}^{n} \prod_{j=1}^{i} \|b_j\|^2 \le \left(\max_j \|b_j\|\right)^{O(n^2)}$

в конце алг-ма: каждый $\det(L[b_1..b_i])$ – целое число $\ge 1 \Rightarrow P^{\text{"после"}} \ge 1$.

#итераций: $P^{\text{"после"}} \le (\delta^2)^{\#\text{итераций}} \cdot P^{\text{"до"}}$

$$1 \le (\delta^2)^{\#\text{итераций}} \cdot \left(\max_j \|b_j\|\right)^{O(n^2)}$$

$$\Leftrightarrow$$

$$\#\text{итераций} \le O\left(\frac{n^2 \lg\left(\max_j \|b_j\|\right)}{\lg(1/\delta)}\right)$$

Качество базиса

Если SWAP не выполняется, то $\underline{r_{i,i+1}^2} + r_{i+1,i+1}^2 \ge \delta^2 \cdot r_{ii}^2$ $\xRightarrow{\text{редукция р-ра}}$

$$\frac{1}{4} r_{ii}^2 + r_{i+1,i+1}^2 \ge \delta^2 r_{ii}^2 \Rightarrow$$

$$r_{i+1,i+1} \ge \sqrt{\delta^2 - \tfrac{1}{4}}\, r_{i,i}$$

То есть "локально" r_{ii} убывают максимум на фактор $\sqrt{\delta^2 - \frac{1}{4}}$

Теорема

Если $\mathcal{B}$ – LLL-редуцированный базис, то

1. $\boxed{\|b_1\| \le \alpha^{\frac{n-1}{2}} \cdot (\det L)^{1/n},}$ где $\alpha = \left(\frac{1}{\delta^2 - 1/4}\right)^{1/2} > 1$
2. $\|b_1\| \le \alpha^{n-1} \cdot \lambda_1(L)$
3. $r_{ii} \le \alpha^{n-1} \cdot r_{nn}$, $\forall i$

LLL возвращает экспоненц. аппроксимацию к кратчайшему вектору

◀ 3. Т.к. $r_{ii} \le \alpha \cdot r_{i+1,i+1}$ $\forall i \Rightarrow$ св-во 3.

2. для $i = 1 \Rightarrow$ св-во 2. $\Big(\underset{r_{11}}{\|b_1\|} \le \alpha^{n-1} \cdot r_{nn}$

$\underline{\lambda_1(L)} \ge \min\limits_i r_{ii} \ge \min\limits_i \alpha^{-i+1} \cdot r_{11} = r_{11} \cdot \alpha^{-n+1} = \underline{\|b_1\| \cdot \alpha^{-n+1}} \Big)$

1. $\underline{\det L} = \prod\limits_{i=1}^{n} r_{ii} \ge \prod\limits_{i=1}^{n} \left(\alpha^{-i+1} r_{11}\right) = \underline{\|b_1\|^n \cdot \alpha^{-\frac{n(n-1)}{2}}}$

$\|b_1\| \le \alpha^{\frac{n-1}{2}} \cdot (\det L)^{\frac{1}{n}}$ ▶