Лекция №3

LLL редукция

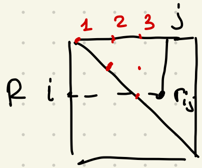
Lenstra – Lenstra – Lovász '82

I. "Редукция размера" (size-reduction)

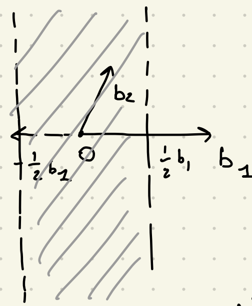
$$|\det B| = |\overset{\pm 1}{\det Q}|\det R = \prod r_{ii}$$

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

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



Геометрически



$$r_{ij} - \left\lfloor \frac{r_{ij}}{r_{ii}} \right\rceil \cdot r_{ii}$$

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

$$r_{ij}^{\text{новое}} = r_{ij} + \left\lfloor -\frac{r_{ij}}{r_{ii}} \right\rceil \cdot r_{ii} \Rightarrow \left|r_{ij}^{\text{новое}}\right| < \frac{r_{ii}}{2}$$

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

Алгоритм редукции размера

Для j-ого вектора

```
For i = j-1 to 1:
    b_j <- b_j + ⌈-r_ij / r_ii⌋ b_i      // изменения в базисе
    For k = 1 to i:                      // изменение в R-факторе
        r_kj <- r_kj + ⌈r_ij / r_ii⌋ r_ki
```

$O(n^2)$ арифм. операций для 1 столбца

Вывод: Если мы можем редуцировать r_{ii}, то мы можем редуцировать и r_{ij} $\Rightarrow$ сделать R-фактор малым.

Замечание $\prod r_{ii} = |\det B| = \det L$ не меняется относит. линейных преобразований. $\Rightarrow$ редукция р-ра делает r_{ii}-е сбалансированными.

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

$$\underbrace{\|c_i\|}_{i\text{-ый базисный вектор}} \leq \max_{j \leq i} \|s_j\| \sqrt{i} \quad \forall i.$$

$\triangleleft$ $\underset{\left[\begin{smallmatrix} | & | & & | \\ s_1 & s_2 & \ldots & s_n \\ | & | & & | \end{smallmatrix}\right]}{S} = B \cdot \underset{}{T}$, $T \in \mathbb{Z}^{n\times n}$, $\det T \neq 0$, т.к. s_i - лин. независ.

HNF для T^t (трансп.): $T^t = \underset{\text{нижне-}\Delta}{H} \cdot \underset{\text{унимод}}{U}$. $\Rightarrow T = (T^t)^t = (H\cdot U)^t = U^t \cdot H^t$

$$\left.\begin{array}{l} S = B\cdot T \\ T = U^t \cdot H^t \end{array}\right\} \Rightarrow S = \underbrace{B\cdot U^t}_{\text{какой-то базис } L,\ B' := B\cdot U^t} \cdot H^t$$

QR-факторизация: $\Downarrow$ $S = Q_S \cdot R_S$

QR-факторизация $\Downarrow$ $B' = Q_{B'} R_{B'}$

$$\Downarrow$$

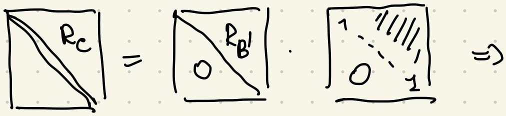
$$Q_S \cdot R_S = Q_{B'} \cdot \underbrace{R_{B'} \cdot H^t}_{\text{верхне-}\Delta}$$

Т.к. QR-факторизация уникальна $\Rightarrow R_S = R_{B'} \cdot H^t \Rightarrow$

$\Rightarrow r_{ii}^{(S)} = r_{ii}^{(B')} \cdot \underbrace{h_{ii}}_{\in \mathbb{Z}^+,\ \geq 1} \Rightarrow r_{ii}^{(B')} \leq r_{ii}^{(S)} \leq \|s_i\|$, т.к. $r_{ii} = \|s_i^*\|$.

Определим C как редукцию р-ра для B'.

Рассмотрим соотв. R-фактор.



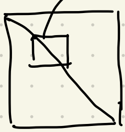
i-ый столбец в $R^{(c)}$

$$\Rightarrow \forall i \quad r_{ii}^{(c)} = r_{ii}^{(B')} \le \|s_i\| \Rightarrow \|c_i\|^2 = \|r_i^{(c)}\|^2 = \sum_{k\le i} r_{ki}^2 \le$$

$$\le \sum_{i<k} r_{ki}^2 + r_{ii}^2 \le \sum_{k<i} \frac{1}{4} r_{ii}^2 + r_{ii}^2 \le i \cdot \max_{k\le i} r_{kk}^{(c)2} \quad \blacktriangleright$$

II LLL-алгоритм

2x2 блок

$B = Q \cdot$ 

R

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

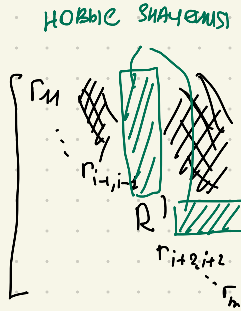
длина $\begin{bmatrix} r_{i,i+1} \\ r_{i+1,i+1} \end{bmatrix}$

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

НЕ ВАЖНО

В целом для базиса B

$$B' = B \cdot \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{bmatrix}$$

QR факторизация $\Longrightarrow$ для $B' = Q'$ 

«SWAP» имеет след. эффект на R-фактор:

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

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

Если $(r_{i,i+1}^2 + r_{i+1,i+2}^2)^{1/2} < r_{ii}^2$, то "SWAP" сделает убывание r_{jj}'-ых менее быстрым.

Алгоритм LLL (с пар-ом $\delta < 1$, $\delta > 1/2$)

Вход: $B \in \mathbb{Z}^{n\times n}$

1. Вычислить QR-факторизацию
2. Редукция по р-ру на R-факторе
3. Если $\exists i$; т.ч. $(r_{i,i+1}^2 + r_{i+1,i+2}^2)^{1/2} < \delta \cdot r_{ii}$:

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

   Restart

   Иначе:

   Вернуть $b_1 .. b_n$.

Сложность задана числом итераций (Restart'ов)

Смотрим на $P = \prod_{i=1}^{n} \Big[\underbrace{\underbrace{\prod_{j=1}^{i} r_{jj}}_{\det R_{[1..i]\times[1..i]}}}_{\det([b_1 \| .. \| b_i]^t \cdot [b_1 \| .. b_i])} \Big]^2$ ← вел-на меняется только при операции SWAP

Если делаем SWAP для r_{ii}:

- $\forall i' < i$ $\left(\prod_{j=1}^{i'} r_{jj}\right)^2$ не изменится
- $\forall i' > i$ $\left(\prod_{j=1}^{i'} r_{jj}\right)^2$ не изменится
- только $\left(\prod_{j=1}^{i} r_{jj}\right)^2$ изменится. В этом пр-ии изменится только r_{ii}^2 при операции SWAP.

А именно, $\underline{P}^{\text{"после"}} \le \delta^2 \, P^{\text{"до"}}$

<u>В начале алг-ма</u> $\underline{P} = \prod_{i=1}^{n} \underbrace{\det\left([b_1 .. b_i]^t \cdot [b_1 .. b_i]\right)^2}_{..} \le$

$\left\{ \det L(b_1 .. b_i) \le \prod \|b_i\| \right\}$ — н-во Адамара

$$\le \prod_{i=1}^{n} \prod_{j=1}^{i} \|b_j\|^2 \le \left(\max_j \|b_j\|\right)^{O(n^2)}$$

<u>В конце алг-ма</u> каждый $\det([b_1 .. b_i)$ – целое число $(B \in \mathbb{Z}^{m \times n})$ ≥ 1.

$$\Rightarrow P^{\text{"после"}} \geq 1$$

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

$\Leftrightarrow$

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