Лекция № 3

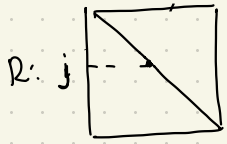
LLL алгоритм

Lenstra - Lenstra- Lovász' 82

I. Редукция по размеру (size reduction)

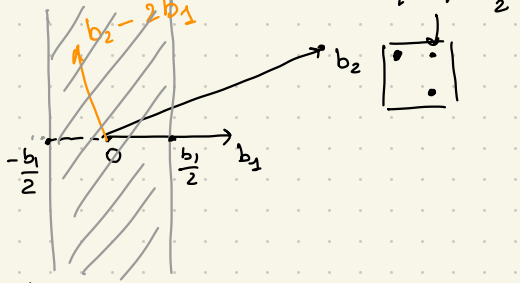
Опр. 1 Базис $B = Q \cdot R$ называется редуцированным по р-ру, если

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



Геометрически

$r_{ji} = \langle b_i, b_j^* \rangle$



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

$\lfloor \cdot \rceil$ - округление

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

$b_i \to b_i^{\text{новый}}$; меняются все $\langle b_i, b_k^* \rangle$, $k < i$

Алгоритм редукции по размеру j-ого вектора. (вход: b_j, R-фактор)

For $i = j-1 \dots 1$

$b_j \leftarrow b_j + \left\lfloor -\frac{r_{ij}}{r_{ii}} \right\rceil b_i$ // изменения в базисе

For $k = 1 \dots i$

$r_{kj} \leftarrow r_{kj} + \left\lfloor -\frac{r_{ij}}{r_{ii}} \right\rceil \cdot r_{ki}$ // изменения в R-факторе

ПРИМЕР: $b_j \leftarrow b_j + \left\lfloor \frac{r_{j-1,j}}{r_{j-1,j-1}} \right\rceil b_{j-1}$ $\Rightarrow$ меняются все $\langle b_j, b_k^* \rangle$, $k \le j-1$

$\parallel$

r_{kj}

Сложность редукции по р-ру: $O(n^2)$ арифм. операций для 1 столбца

Вывод Если мы можем редуцировать r_{ii}-эл-ты на главной диагонали, то мы можем редуцировать и r_{ij}.

Замечание $\Pi r_{ii} = |\det B| = \det L$ не меняется относительно линейных преобразований.

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

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

$\triangleleft$ $S = B \cdot T$, $T \in \mathbb{Z}^{n \times n}$, $\det T \neq 0$, т.к. s_i лин. независимы

$$\begin{bmatrix} | & | & & | \\ s_1 & s_2 & \dots & s_n \\ | & | & & | \end{bmatrix}$$

$\nexists$ H – HNF (эрмитову нормальную форму) для T^t (транспонирование): $T^t = H \cdot U$ (нижне-$\triangle$, унимодулярная)

$\Rightarrow T = (T^t)^t = (H \cdot U)^t = U^t \cdot H^t$

$S = B \cdot T$, $T = U^t \cdot H^t$ $\Rightarrow$ $S = B \cdot U^t \cdot H^t$

$B \cdot U^t$ – какой-то базис L. $B' = B \cdot U$

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

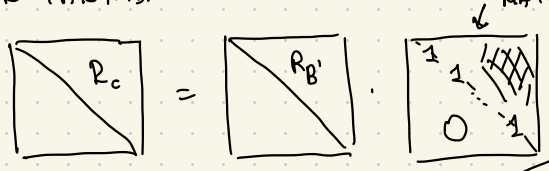
$\Downarrow$ QR-факторизация: $B' = Q_{B'} \cdot R_{B'}$

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

Т.к. QR-факторизация уникальна, то $R_S = R_{B'} \cdot H^t \Rightarrow r_{ii}^{(S)} = r_{ii}^{(B')} \cdot \underbrace{h_{ii}}_{\in \mathbb{Z}^+, \ge 1} \Rightarrow$

$\Rightarrow r_{ii}^{(B')} \le r_{ii}^{(S)} \le \|s_i\|^2$ т.к. $r_{ii} = \|s_i^*\|^2$

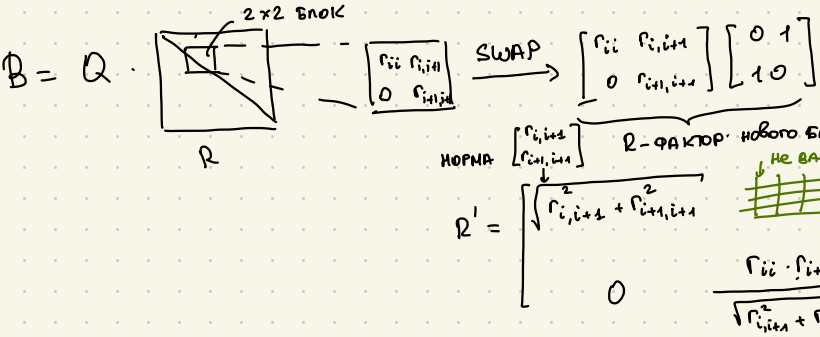
Определим C как редукцию по размеру для B'. Рассмотрим соответствующие R-факторы:



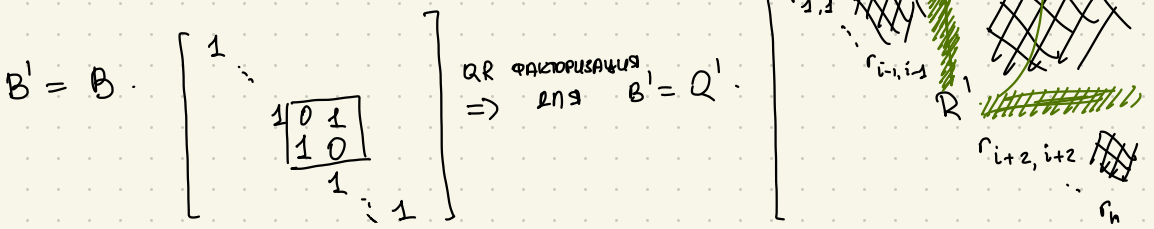
$$\Rightarrow \forall i: \; r_{ii}^{(C)} = r_{ii}^{(B')} \le \|s_i\|^2 \Rightarrow \|c_i\|^2 = \|r_i^{(c)}\|^2 =$$

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

II LLL-алгоритм



Для всего базиса B, SWAP означает:



Если $r_{i,i+1}^2 + r_{i+1,i+1}^2 < r_{ii}^2$, то "SWAP" делает 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. Вычисляем QR-факторизацию B
2. Выполняем редукцию по Р-ру базиса (при этом изменяется R-фактор)
3. Если $\exists\, i$ т.ч. $r_{i,i+1}^2 + r_{i+1,i+1}^2 < \delta^2 \cdot r_{ii}^2$: // условие Lovász

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

Restart

Иначе:

Вернуть $b_1 .. b_n$.

Сложность LLL (число итераций / RESTART'ов)

Смотрим на $P = \prod_{i=1}^{n} \left[\prod_{j=1}^{i} r_{jj} \right]^2$ ← величина меняется только при операции SWAP

$\det R_{[1..i] \times [1..i]}$

$\det \left([b_1 || .. || b_i]^t \cdot [b_1 || .. || b_i] \right)$

Если делаем SWAP для r_{ii} :

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

$$P^{\text{"после"}} \leq \delta^2 P^{\text{"до"}}$$

В начале алгоритма LLL $P = \prod_{i=1}^{n} \det \left([b_1 || .. || b_i]^t \cdot [b_1 || .. || b_i] \right) \leq$

$\leq \{ \det L(b_1 || .. || b_i) \leq \prod \|b_i\| \}$ (Н-во Адамара) $\leq \prod_{i=1}^{n} \prod_{j=1}^{i} \|b_j\|^2 \leq \max_j \|b_j\|^{O(n^2)}$.

В конце алгоритма каждый $\det(\|b_1\| \dots \|b_i\|)$ - целое число ($B \in \mathbb{Z}^{n \times n}$)
≥ 1

$\Rightarrow P^{\text{"в конце LLL"}} \geq 1$

$\Rightarrow$ # итераций : $P^{\text{"в конце LLL"}} \leq (\delta^2)^{\text{# итераций}} \cdot P^{\text{"до"}}$

$\Leftrightarrow$

$\lg P^{\text{"в конце LLL"}} \leq \text{# итераций} \cdot 2\lg\delta + \lg P^{\text{"до"}}$

$2\lg\delta$ # итераций $\geq -\lg P^{\text{"до"}}$ // $\lg\delta < 1$

$$\text{# итераций} \leq O\left(\frac{n^2 \cdot \lg(\max_i \|b_i\|)}{\lg 1/\delta}\right).$$