Лекция № 6
CVP. SVP

I. Определения

Shortest Vector Problem (SVP) / Задача короткого вектора

- SVP_γ $(\gamma \geq 1)$ для решётки $\mathcal{L} \subset \mathbb{Z}^n$, заданной базисом B, и $r > 0$ определить, какой из двух случаев выполняется:

  (1) $\lambda_1(L) \leq r$ ("да")

  (2) $\lambda_1(L) > \gamma \cdot r$ ("нет")

- $ApproxSVP_\gamma$: для решётки L, найти $b \neq 0 \in L$, т.ч.

$$\|b\| \leq \gamma \cdot \lambda_1(L)$$

SVP_γ "сводится" к $ApproxSVP_\gamma$.

Задача A "сводится" к задаче B, если, имея оракул, решающий B, мы можем решить A.

Closest Vector Problem (CVP) / Задача ближайшего вектора

- CVP_γ для решётки $L \subseteq \mathbb{Z}^n$ и "целевой" вектор $t \in \mathbb{R}^n$ и $r > 0$
  (target)
  определить, какой из двух случаев выполняется:

$dist(t, L) = \min\limits_{v \in L} \|v - t\|$

  (1) $dist(t, L) \leq r$ ("да")

  (2) $dist(t, L) > \gamma \cdot r$ ("нет")

- $ApproxCVP_\gamma$ для решётки $L \subseteq \mathbb{Z}^n$ и $t \in \mathbb{R}^n$, найти $b \in L$, т.ч.

$$\|b - t\| \leq \gamma \cdot dist(t, L).$$

В случае $t \in L$, возвращаем $b = t$.

ЗАМЕЧАНИЕ $\mathrm{ApproxSVP}_\gamma \in \mathbb{P}$ ← класс polytime для $\gamma = 2^n$ (LLL редукция базиса)

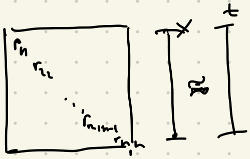
Теорема 1 $\mathrm{ApproxCVP}_\gamma \in \mathbb{P}$ для $\gamma = 2^n$

Δ Положим $B = QR$ − LLL редуцированный базис.

Пусть $b^* = \sum_{i=1}^{n} x_i b_i$ − ближайший к t вектор из L

$]$ t − данный целевой вектор, положим $t^R = Q^T \cdot t$, $b^{*R} = Q^T \cdot b$ (мы $*$ t, b^* относительно R-фактора)

Делаем "редукцию по размеру" (см. лек. 3) для $t^R = (t_1^R .. t_n^R)$



1) находим $x_n' \in \mathbb{Z}$ т.ч. $t_n^R - x_n' r_{nn} < \frac{r_{nn}}{2}$

2) находим $x_{n-1}' \in \mathbb{Z}$ т.ч. $t_{n-1}^R - x_n' r_{n-1,n} - x_{n-1}' r_{n-1,n-1} \le \frac{r_{n-1,n-1}}{2}$

3) —"— $x_{n-2}' \in \mathbb{Z}$ т.ч. $t_{n-2}^R - x_n' r_{n-2,n} - x_{n-1}' r_{n-2,n-1} - x_{n-2}' r_{n-2,n-2} \le \frac{r_{n-2,n-2}}{2}$

$\vdots$

В итоге получим $x_n' .. x_1' \in \mathbb{Z}$, т.ч.:

$$\Big|\underbrace{\big(t^R - \sum x_i' r_{ii}\big)[i]}_{i\text{-ая координата вектора}}\Big| < \frac{r_{ii}}{2} \quad \forall i$$

Выход: $b' = \sum_{i=1}^{n} x_i' \cdot b_i \in L$.

Покажем, что $\|b' - t\| \le 2^n \cdot \|b^* - t\|$

Случай 1 $\|b^* - t\| \ge \frac{r_{nn}}{2}$.

Мы нашли b', т.ч. $\|b' - t\|^2 = \|\overset{Q\cdot R}{B} \cdot x' - \underbrace{Q \cdot t^R}_{\overbrace{Q\cdot Q^T}^{Id}\cdot t}\|^2 \underset{Q \text{ не меняет } \|\cdot\|}{=} \|Rx' - t^R\|^2$

$$= \|\sum_{i=1}^{n} x_i' \cdot \underbrace{r_i}_{i\text{-ый столбец } R} - t^R\|^2 \le \frac{1}{4}\sum_{i=1}^{n} r_{ii}^2 \underset{\substack{\text{LLL гарантия на } B \\ (r_{ii} \le d^{n-i} \cdot r_{nn},\ d \ge 2)}}{\le} \frac{1}{4}\sum_i 2^{2(n-i)} \cdot r_{nn}^2$$

$$\le 2^{2n} \cdot \frac{r_{nn}^2}{4} \Rightarrow \|b' - t\| \le 2^n \cdot \frac{r_{nn}}{2} \underset{\text{случай 1}}{\le} 2^n \cdot \|b^* - t\|$$

Случай 2 $\|b^* - t\| < \frac{r_{nn}}{2} \overset{\text{выносим } Q}{\iff} \|b^{*R} - t^R\| < \frac{r_{nn}}{2} \Rightarrow |x_n r_{nn} - t_n^R| < \frac{r_{nn}}{2}$

$\Rightarrow x_n' = x_n$ в ходе алг-ма редукции по р-ру на 1м шаге.

Аналогично рассуждаем для x'_{n-1}, рассматривая $b^* - x_n b_n$ — ближайший к $\underset{x''_n}{t} = t - x'_n \cdot b_n$)

Замечание. Процедура, описанная в док-ве Теоремы 1, называется алгоритмом Бабая (L. Babai).

II CVP vs SVP

Теорема 2. SVP_γ сводится к CVP_γ $\forall \gamma \geq 1$.

Утверждение т-мы 2. верно и для approx-версий задач.

Док-во (для $\gamma = 1$ и approx-версии = версии поиска)

Цель: имея оракул для задачи CVP_1, решить SVP_1.

$B \in \mathbb{Z}^{n \times n}$ — базис L

$B^{(i)} := [b_1, \ldots b_{i-1}, 2b_i, b_{i+1}, \ldots b_n]$

$t^{(i)} := b_i$

для $i = 1..n$

вызвать $CVP_1(B^{(i)}, t^{(i)})$

получаем $c_i \in B^{(i)}$ - результат

вернуть $c_i - b_i$ т.ч. $\|c_i - b_i\| = \min\limits_j \|c_j - b_j\|$

} редукция

Покажем, что вывод алг-ма действительно кратчайший в L.

$\exists\, b = \sum\limits_{i=1}^n x_i b_i \in L$ — кратчайший в $L \Rightarrow \exists i$, т.ч. x_i — нечётно

(иначе $\frac{b}{2} = \sum\limits_{i=1}^n \underbrace{\left(\frac{x_i}{2}\right)}_{\in \mathbb{Z}} b_i \in L$, $\|\frac{b}{2}\| < \|b\|$).

Запишем $b = -b_i + \sum\limits_{j \neq i} x_j b_j + \underbrace{\left(\frac{x_i + 1}{2}\right)}_{\in \mathbb{Z}} \cdot 2b_i \in -b_i + L(B^{(i)})$

$\Rightarrow \operatorname{dist}(L(B^{(i)}), \underset{b^{(i)}}{t^{(i)}}) \leq \|b\| = \lambda_1(L)$

потенциально в $L(B^{(i)}) - b_i$ могут содержаться вектора, короче b.

С другой стороны, по построению $t^{(i)}, B^{(i)}$ $\operatorname{dist}(L(B^{(i)}), t^{(i)}) \geq \lambda_1(L)$.

Получаем $\operatorname{dist}(L(B^{(i)}), t^{(i)}) = \lambda_1(L) \Rightarrow \|\underbrace{c_i - b_i}_{\in L}\| = \lambda_1(L)$. ▶

Открытые вопросы

1. Редукция в теореме 2 – это редукция типа "$\underset{\text{n вызовов CVP}}{\text{много}}$-к-$\underset{\text{1 решение SVP}}{\text{одному}}$"

Вопрос: редукция 1-к-1 (с сохранением размерности решётки).

2. Обратная редукция: от CVP к SVP с одинаковым пар-ом γ.