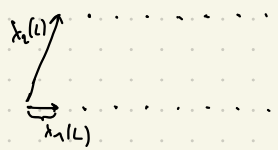
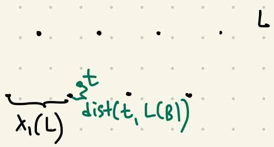
Лекция №8
BDD, uSVP, SVP

I. Определения

– $uSVP_\gamma$ (unique SVP / уникальный SVP): для решётки L, заданной базисом B, такой что $\lambda_2(L) > \gamma \cdot \lambda_1(L)$, найти $v \in L \setminus \{0\}$, $\|v\| = \lambda_1(L)$



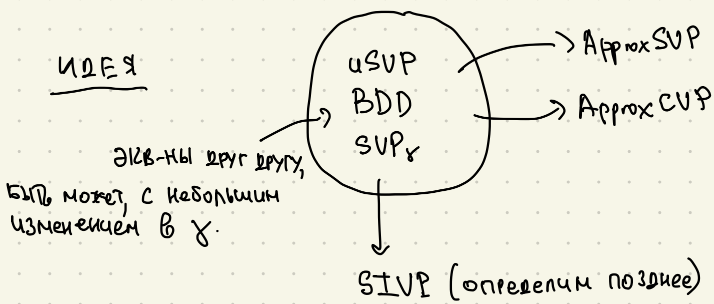
– BDD_γ (bounded distance decoding / декодирование с ограниченным расстоянием): для решётки L, заданной B, и t, т.ч. $dist(L,t) < \frac{1}{\gamma}\lambda_1(L)$, найти $v \in L$ – ближайший к t.



Замечание: $uSVP_\gamma$ сводится к версии поиска SVP ($ApproxSVP_\gamma$)

BDD_γ ——— // ——— CVP ($ApproxCVP_\gamma$).

Идея



II SVP редуцируется к BDD

<u>Теорема 1</u> $\forall \gamma > 2\sqrt{\frac{n}{\lg n}}$, $\exists$ редукция от SVP_γ к $BDD_{\frac{\gamma}{\sqrt{\frac{n}{\lg n}}}}$.

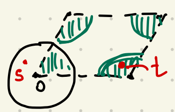
$\triangleleft$ Вход: (B, r) – задача SVP_γ (решить $\lambda_1(L(B)) \le r$, "да", или
$\lambda_1(L(B)) > \gamma \cdot r$, "нет").

повторить процедуру poly(n)-раз
$\begin{cases} 1) \text{ Выбрать } s \xleftarrow{\$} B\left(0, r\cdot\sqrt{\frac{n}{\lg n}}\right) \\ 2) \text{ Вызвать BDD-оракул для } t = s \bmod \mathcal{P}(B) \end{cases}$

Если BDD оракул <u>всегда</u> возвращает $t-s$, то вывод "нет".

Иначе, "да".

<u>Случай 1</u> "нет"

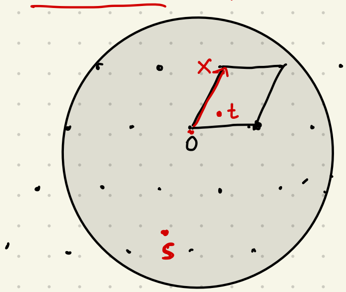


Если $\lambda_1(L) > \gamma\cdot r$ ("нет"), то
$\operatorname{dist}(t, L) = \operatorname{dist}(s, L) \le r\cdot\sqrt{\frac{n}{\lg n}} < \frac{\lambda_1(L)}{\gamma}\cdot\sqrt{\frac{n}{\lg n}}$

$\Rightarrow$ t – валидный вход для $BDD_{\frac{\gamma}{\sqrt{\frac{n}{\lg n}}}}$-оракула.

Кроме того, $\frac{\gamma}{\sqrt{\frac{n}{\lg n}}} < \frac{1}{2} \Rightarrow \exists$ единственное решение $t-s$.

<u>Случай 2</u> "да"



<u>Лемма</u> $\exists x \in \mathbb{R}^n$, т.ч. $\|x\| \le r$, $\exists s \xleftarrow{\$} B\left(0, r\sqrt{\frac{n}{\lg n}}\right)$

Тогда с вероятностью $\delta > \frac{1}{poly(n)}$,

$$\|s - x\| < r\sqrt{\frac{n}{\lg n}}.$$

(док-во самостоятельно, или см
Lyubashevsky, Micciancio'09 "On bounded distance decoding, unique shortest vectors, and the minimum distance problem")

$\lambda_1 \le r$. Положим x, т.ч. $\|x\| = \lambda_1(L)$. Тогда,
по лемме, с в-тью $\frac{1}{poly(n)}$, $\|s-x\| < r\sqrt{\frac{n}{\lg n}} \Rightarrow$

BDD оракул не сможет ответить корректным $t-s$ с в-тью $\geq \frac{1}{2}$ (BDD оракул не отличит s от $s-x$).

После $poly(n)$ запусков, в-ть того, что BDD оракул ответит корректным $t-s$, $< 2^{-\Omega(n)}$. ▶

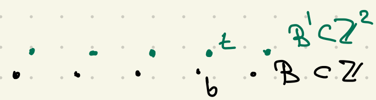
III BDD редуцируется к uSVP.

Теорема 2 $BDD_{2\gamma}$ редуцируется к $uSVP_\gamma$.

◁ Вход: (B, t), т.ч. $dist(t, B) < \frac{\lambda_1(L)}{2\gamma}$

Положим, $b \in L$ - ближайший к t, $dist(b,t) = d$ (положим, d-известно).

$$B' = \begin{bmatrix} B & t \\ 0 & d \end{bmatrix} \in \mathbb{Z}^{(n+1)\times(n+1)}$$



1) Вызываю uSVP на B'.
2) Пусть $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ - выход uSVP $s_1 \in \mathbb{Z}^n$, $s_2 \in \mathbb{Z}$
3) Вернуть $(s_1 + t)$

Корректность B' - решётка uSVP, т.к. $\begin{pmatrix} t-b \\ d \end{pmatrix} \in L(B')$ и

$$\left\| \begin{pmatrix} t-b \\ d \end{pmatrix} \right\| = \sqrt{d^2+d^2} = \sqrt{2}\, d < \frac{\lambda_1(L)\sqrt{2}}{2\gamma} = \frac{\lambda_1(L)}{\sqrt{2}\,\gamma}.$$

Покажем, что другие вектора в L' имеют норму $\geq \frac{\lambda_1(L)}{\sqrt{2}}$ (не параллельны $\begin{pmatrix} t-b \\ d \end{pmatrix}$)

Рассмотрим $\left\| \begin{matrix} c - xt \\ xd \end{matrix} \right\|$, где $c \in L(B)$, $c \neq \alpha \cdot b$ $(\alpha \in \mathbb{Z})$, $x \in \mathbb{Z}$

$$\left\| \begin{matrix} c-xt \\ xd \end{matrix} \right\|^2 = (xd)^2 + \| \underbrace{c - xb}_{\neq 0, \in L,\ \|c-xb\| \geq \lambda_1(L)} + x\overbrace{(b-t)}^{d} \|^2 \geqslant x^2d^2 + (\lambda_1(L) - xd)^2 =$$

т.к. $\left(\|a+b\|^2 \geqslant (\|a\| - \|b\|)^2 \right)$

$$= \underbrace{2x^2d^2 + \lambda_1(L)^2 - 2\lambda_1(L)xd}_{\text{Выражение минимизируется при}} \geqslant 2\frac{\lambda_1(L)^2}{4d^2}d^2 + \lambda_1(L)^2 - 2\lambda_1(L)\frac{\lambda_1(L)}{2d}d$$

$$4xd^2 - 2\lambda_1(L)d = 0$$

$$x = \frac{\lambda_1(L)}{2d}$$

$$= \frac{\lambda_1(L)^2}{2} + \lambda_1(L)^2 - \lambda_1(L^2)$$

$$= \frac{\lambda_1(L)^2}{2}.$$

IV Дуальные решётки

Опр-ие Для решётки L определим $\hat{L}$ - дуальную к L как

$$\hat{L} = \{ \hat{b} \in \operatorname{Span}_{\mathbb{R}} L : \forall b \in L \ \langle b, \hat{b} \rangle \in \mathbb{Z} \}.$$

Примеры 1) $\widehat{\mathbb{Z}^n} = \mathbb{Z}^n$

2) $\widehat{(2 \cdot \mathbb{Z}^n)} = \frac{1}{2}\mathbb{Z}^n$

Св-ва дуальной решётки

1) B - базис L, то $\hat{B} = B\,(B^T \cdot B)^{-1}$ - базис $\hat{L}$

Если B - кв. матрица, то $\hat{B} = B^{-T}$.

$\triangleleft$ $\hat{B} \cdot \mathbb{Z}^n \subseteq \hat{L}$, т.к. $\forall b \in L$ $b = B \cdot x$ $(x \in \mathbb{Z}^n)$ и $\langle Bx, \underset{y \in \mathbb{Z}^n}{\hat{B} y} \rangle =$

$$= x^T \underbrace{B^T \cdot B \cdot (B^T \cdot B)^{-1}}_{Id} \cdot y = x^T \cdot y \in \mathbb{Z}.$$

Обратно, $\forall \hat{b} \in \hat{L}$, $\hat{b} = \hat{B} \cdot y$ для $y \in \mathbb{R}^n$, т.к. $\mathrm{Span}_{\mathbb{R}} \hat{B} = \mathrm{Span}_{\mathbb{R}} B$

По определению дуальной решётки, $B^T \cdot \hat{b} \in \mathbb{Z}^n$ (т.к. B^T содержит в строках вектора L)

$$\Downarrow$$

$$B^T \cdot \hat{B} \cdot y = \underbrace{B^T \cdot B\,(B^T \cdot B)^{-1}}_{Id} \cdot y \in \mathbb{Z} \Rightarrow y \in \mathbb{Z}^n \blacktriangleright$$

2) $\hat{(\hat{L})} = L$ (упр-ие)

3) $\det(\hat{L}) = \dfrac{1}{\det(L)}$

4) $L_1, L_2 \subseteq \mathbb{Z}^n$, то $\widehat{L_1 + L_2} = \hat{L}_1 \cap \hat{L}_2$.

5) $B = QR$, тогда $\hat{B} \cdot J = Q \cdot J\,(J R^{-1} J)$, $J = \begin{bmatrix} & & 1 \\ & \cdots & \\ 1 & & \end{bmatrix}$ – обращает порядок вектор

6) Transferense $\quad 1 \le \lambda_1(L) \cdot \lambda_n(\hat{L}) \le n$

7) $\lambda_1(L) \cdot \lambda_1(\hat{L}) \le n$.