Лекция №8
BDD, uSVP, SVP

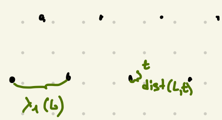
I. Определения

- $uSVP_\gamma$ (unique SVP / уникальный кратчайший вектор):

Для решётки L, заданной базисом B, такой что $\lambda_2(L) > \gamma\, \lambda_1(L)$, найти $v \in L \setminus \{0\}$, $\|v\| = \lambda_1(L)$.

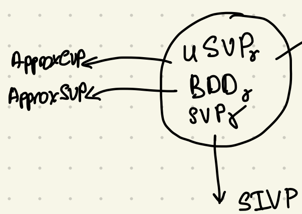
- BDD_γ (bounded distance decoding / декодирование с ограниченным расстоянием):

Для решётки L и t (целевой вектор), 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 ($ApproxSVP_\gamma$, Lec. 6)
BDD_γ сводится к — // — CVP ($ApproxCVP_\gamma$, Lec. 6)

Цель:



эквивалентны друг другу с небольшим изменением γ (быть может, имея оракул, решающий одну из задач, можно решить и две другие задачи)

SIVP (определим позднее)

n — ранг решётки L

II SVP редуцируется к BDD

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

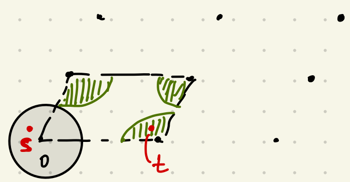
◁ Вход: $(B$ — базис, $r)$ — задача SVP_γ. Решить: $\lambda_1(L(B)) \le r$ "да", или
$\lambda_1(L(B)) > \gamma \cdot r$ "нет"

Повторить процедуру poly(n) раз:

1) Выбрать $s \xleftarrow{\$} \mathcal{B}^n\left(0, r\cdot\sqrt{\frac{n}{\lg n}}\right)$ — шар с центром в 0 и радиусом $r\sqrt{\frac{n}{\lg n}}$)
2) Вызвать BDD-оракул на $L(B)$ и $t = s \bmod \mathcal{P}(B)$

Если BDD оракул на шаге 2) всегда возвращает $t-s$, то вывод "нет". Иначе, "да".

Случай 1 "нет"



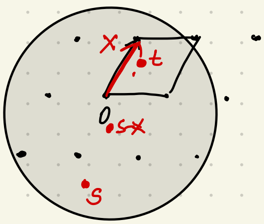
$r < \frac{\lambda_1(L)}{\gamma}$

Если $\lambda_1(L) > \gamma\cdot r$ ("нет"), то
$\mathrm{dist}(t, L) = \mathrm{dist}(s, L) \le r\cdot\sqrt{\frac{n}{\lg n}} <$
$< \frac{\lambda_1(L)}{\gamma}\cdot\sqrt{\frac{n}{\lg n}} \Rightarrow t$ — валидный вход для $BDD_{\frac{\gamma}{\sqrt{\frac{n}{\lg n}}}}$ -оракула

Кроме того, $\sqrt{\frac{n}{\lg n}}/\gamma < \frac{1}{2} \Rightarrow \exists!$

Решение $t-s$.

Случай 2 "да"



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

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 вероятностью $> \frac{1}{poly(n)}$, имеем $\|s - x\| < r\sqrt{\frac{n}{\lg n}} \Rightarrow$ BDD оракул не сможет ответить корректным $t-s$ с в-тью $\ge \frac{1}{2}$, т.к. BDD оракул не отличит s и $s-x$. После poly(n) запусков вероятность того, что BDD оракул ответит корректным $t-s < 2^{-\Omega(n)}$ ▶

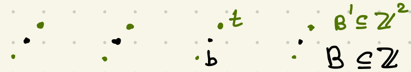
III BDD редуцируется к uSVP

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

◁ Вход: $(B \in \mathbb{Z}^{n\times n}$ – базис L, $t \in \mathbb{Z}^{n})$, т.ч. $dist(t, L(B)) < \frac{\lambda_1(L)}{2\gamma}$

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, где $s_1 \in \mathbb{Z}^n$, $s_2 \in \mathbb{Z}$
3. Вернуть $(s+t)$

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

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

Покажем, что другие вектора (не $\|$-ые $\begin{pmatrix} t-b \\ d \end{pmatrix}$) в L' – решётке, порождённой B', имеют норму $\geq \lambda_1(L)/\sqrt{2}$.

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

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

$$= \underbrace{2x^2d^2 + \lambda_1^2(L) - 2\lambda_1(L)\cdot xd} \geq 2\,\frac{\lambda_1^2(L)}{4d^2}\,d^2 + \lambda_1^2(L) - 2\lambda_1(L)\cdot\frac{\lambda_1(L)}{2d}\cdot d$$

выражение минимизируется при

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

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

$$= \frac{\lambda_1^2}{2} \Rightarrow \left\|\begin{matrix} c-xt \\ xd \end{matrix}\right\| > \frac{\lambda_1(L)}{\sqrt{2}} \Rightarrow$$

$\Rightarrow$ на шаге 1 мы имеем инстанцию задачи $uSVP_{\gamma}$.

▶

IV Дуальные решётки

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

$$\hat{L} = \{ \hat{b} \in Span_{\mathbb{R}} L : \forall b \in L \ \langle b, \hat{b} \rangle \in \mathbb{Z} \}$$

Примеры
1. $\widehat{\mathbb{Z}^n} = \mathbb{Z}^n$
2. $\widehat{2\mathbb{Z}^n} = \frac{1}{2}\mathbb{Z}^n$

Свойства дуальной решётки (док-ва в упражнениях)

1. B – базис L, то $\hat{B} = B \cdot (B^T \cdot B)^{-1}$ – базис $\hat{L}$
   Если B – квадратная, то $\hat{B} = B^{-T}$
2. $\widehat{(\hat{L})} = L$
3. $\det(\hat{L}) = \frac{1}{\det L}$
4. $L_1, L_2 \subseteq \mathbb{Z}^n$, то $\widehat{L_1 + L_2} = \hat{L}_1 \cap \hat{L}_2$
5. $B = Q \cdot R$, то $\hat{B} \cdot J = Q \cdot J \cdot (J \cdot R \cdot J^{-1})$, $J = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}$ – обращает порядок векторов
6. Transference $1 \le \lambda_1(L) \cdot \lambda_n(\hat{L}) \le n$
7. $\lambda_1(L) \cdot \lambda_1(\hat{L}) \le n$.

V uSVP редуцируется к SVP

Теорема 3 $\forall \gamma = poly(n)$ $uSVP_\gamma$ редуцируется к SVP_γ.

Δ $B \in \mathbb{Z}^{n \times n}$ – базис решётки uSVP

Пусть $s \in L(B)$, $\|s\| = \lambda_1(L(B))$. Мы знаем, что все вектора, не $\parallel$-ые s, имеют нормы $\geq \lambda_2 \geq \gamma \cdot \lambda_1$

Идея: построить разреженные решётки, одна из которых содержит s.

$\exists p$ - простое, $p > \gamma$

$$B_0 = [p \cdot b_1, b_2 \dots b_n]$$

$$B_i = [b_1 + i b_2, p \cdot b_2, \dots, b_n]$$

1. Одна из решёток, порождённая B_i ($i \geq 0$) содержит $s = \sum x_i b_i$.

Если $x_1 \equiv 0 \mod p$, то $s \in L(B_0)$.

Иначе, $s \in L(B_i)$, $i = x_2 \cdot x_1^{-1} \mod p$, т.к.

$$s = x_1 (b_1 + x_2 \cdot x_1^{-1} b_2) + \frac{x_2 - (x_2 \cdot x_1^{-1}) \cdot x_1}{p} \cdot p \cdot b_2 + \sum_{i \geq 3} x_i b_i$$

2. Если $s \notin L(B_i)$, то $\lambda_1(L(B_i)) \geq \gamma \cdot \lambda_1(L)$

Если $v \in L(B_i)$, $v \nparallel s$, то $\|v\| \geq \gamma \cdot \lambda_1(L)$

Иначе, если $v \parallel s$, покажем, что $\|v\| \geq p \cdot \|s\| > \gamma \cdot \lambda_1(L)$.

* $B_s = [s | b_2 \dots b_n]$ – базис $L(B)$, где вместо b_1 есть s.

$\det(B_i) = p \cdot \det(B_s)$

Т.к. $v \parallel s$, то $\underset{(k \neq 1)}{v = k \cdot s} \in L(B_i)$.

Покажем, что $\boxed{k = p}$ ($\Rightarrow \|v\| = \|s\| \cdot k = p \cdot \|s\| > \gamma \cdot \lambda_1(L)$)

* $B_{i,s} = [k \cdot s | c_2 \dots c_n]$ – базис $L(B_i)$, где вместо $b_1 + i b_2$ есть ks

$$B_{i,s} = B_s \cdot \begin{bmatrix} k & \\ 0 & \overset{\text{неважно}}{\ast} \\ \vdots & \\ 0 & \end{bmatrix} \Rightarrow \left.\begin{array}{l} \det B_{i,s} = \det B_s (k \cdot \det [\ast]) \\ \det B_{i,s} = \det B_i = p \cdot \det B_s \end{array}\right\} \Rightarrow$$

$$\Rightarrow \det \cancel{B_s} \cdot k \cdot \underbrace{\det [\ast]}_{\in \mathbb{Z}} = p \cdot \det \cancel{B_s} \Rightarrow k | p \Rightarrow \boxed{k = p}$$

Из 1. и 2. следует, что мы можем вызвать SVP_γ на

$(B_i, \overbrace{r = \underset{=\|s\|}{\lambda_1(L(B))}})$. положим, известно.

SVP_γ позволяет детектировать i, т.ч. $s \in L(B_i)$

Повторяем редукцию для $B = B_i$

После $\underline{k}$-ой итерации, имеем $\det(\overbrace{L_k(B)}^{\text{решётка на k-ой итерации}}) = p^k \cdot \det(L(B))$

$\not\exists$ $\widehat{L_k(B)}$. Эта решётка имеет определитель

$$\det \widehat{L_k(B)} = \frac{1}{p^k \cdot \det L(B)}$$

Вызов LLL на $\widehat{L_k(B)}$ вернёт $\hat{b} \in \widehat{L_k(B)}$, т.ч. $\|\hat{b}\| \le 2^n \cdot \frac{1}{(p^k \det L(B))^{1/n}}$

$$|\langle \hat{b}, s \rangle| \le \frac{2^n}{p^{\frac{k}{n}} \cdot (\det B)^{1/n}} \cdot \underbrace{\lambda_1(L)}_{\le \sqrt{n} \cdot (\det L(B))^{1/n}} \le \frac{2^n \cdot \sqrt{n}}{p^{k/n}} < 1 \text{ для } k = \Omega(n \log p)$$

$\Rightarrow |\langle \hat{b}, s \rangle| = 0 \in \mathbb{Z}$

$\Rightarrow \quad s \in L(B) \cap \hat{b}^{\perp} = \widehat{\Pi(\hat{L}, \hat{b}^{\perp})}$ – решётка размерности $n-1$

$\Rightarrow$ Запускаем весь алг-м на $L(B) \cap b^{\perp}$, пока не получим решётку р-ти 1 $\Rightarrow$ знаем s.