Сложность SIS

Tuesday 20 April 2021 08:57

SIS: $\overset{x}{\longrightarrow}\ {}_m\underset{}{\overset{n}{\boxed{A}}} = 0 \bmod q$; $A \leftarrow U(\mathbb{Z}_q^{m\times n})$

$0 < \|x\| \le \beta$

Цель: редукция от $SIVP_\gamma$ "в худшем" к $SIS_{q,m,\beta}$ "в среднем"

(short indep. vectors problem)

$SIVP_\gamma$ — по заданному базису B решётки L, найти $s_1 \dots s_n \in L$ лин. незав-ые векторов, т.ч. $\max_i \|s_i\| \le \gamma\cdot\lambda_n(L)$.

Теорема [Ajtai'96; GPV'08] $\forall$ полином. вероятностный алг-м, решающий $SIS_{q(n),m(n),\beta(n)}$ с непренебрежимо малой в-ю, может быть использован для решения задачи $SIVP_{\gamma(n)}$ в решётке р-ти n с в-тью $1-2^{-\Omega(n)}$ для $\gamma \ge q \ge 8\cdot n\cdot\beta\sqrt{m}$.

◀ Промежуточная задача (переформулировка SIVP), $IncIVP(\underset{\text{базис}}{B}, \underset{\text{мн-во лин. незав. векторов}}{S}, \overset{\text{гиперплоскость}}{H})$ (Incremental) : найти $v \in L\setminus H$ т.ч. $\|v\| \le \max_i \|s_i\|/2$; где $\max_i \|s_i\| \ge \gamma\cdot\lambda_n(L(B))$.

Редукция от IncIVP к SIS.

Вход: B, $S \subset L$, H; O^{SIS} - оракул для SIS

Выход: v - решение IncIVP

1. Из B и S, построить базис C решётки L, такой что $\max_i r_{ii} \le \|S\|$ (для $C = QR$) (LLL алг-м), $\|S\| = \max_i \|s_i\|$

2. Для $i = 1 \dots m$

   Выбрать $y_i \leftarrow D_{L,\sigma,0}$, где $\sigma = \sqrt{n}\cdot\|S\|$ (используем Klein)

3. Вызвать O^{SIS} на $A = (B^{-1}\cdot Y)^T \bmod q$, где $Y = [y_1\ y_2 \dots y_m]$

   $\Downarrow$ i-ая строка матрицы A - вектор-координат для y_i относ. базиса B, взятый $\bmod q$.

   Пусть O^{SIS} вернёт $x \in \mathbb{Z}^m$; $x^T A = 0 \bmod q$

4. Вернуть $v = Y\cdot x/q = \frac{1}{q}\sum x_i y_i$.

Замечания
1. $x \in \mathbb{Z}^m$ из шага 3. - обнуляет координаты y_i относ. базиса $B \bmod q$ => $Y\cdot x$ - короткий вектор решётки с координатами относ. базиса B, кратные q.
2. Редукция работает за время $poly(n)$;
3. Если в-ть успеха редукции $\ge \frac{1}{poly(n)}$, увеличиваем в-ть до $1-2^{-\Omega(n)}$, повторяя $poly(n)$ раз.

Утверждение 1 Распределение матрицы A на шаге 3. обладает статист. разностью с $U(\mathbb{Z}_q^{m\times n})$ в $2^{-\Omega(n)}$.

◀ Докажем для строки $a_1 = (B^{-1}\cdot y_1)^T \bmod q$. Для $a_2 \dots a_n$ - аналог., т.к. y_i выбираются независимо.

$$\varphi: \begin{array}{l} L \to \mathbb{Z}_q^n \\ y \mapsto B^{-1}y \bmod q \end{array}$$ - сюръективный гомоморфизм

=> $\exists$ биекция м/д $\mathbb{Z}_q^n$ и $\underbrace{L/\ker\varphi} = L/qL$ =>

=> $B^{-1}y \bmod q$ распр-н равномерно в $\mathbb{Z}_q^n$ $\Leftrightarrow$ $y \bmod qL$ распр-н равном. в L/qL.

Для $\sigma \ge \eta_{2^{-n}}(qL)$ справедливо $\Delta(D_{L,\sigma} \bmod qL,\ U(L/qL)) \le 2^{-\Omega(n)}$.

◀ для $b \in L/qL$: $\Pr(b \leftarrow D_{L/qL,\sigma}) = \Pr[y \in b+qL] = \sum_{y\in b+qL}\frac{\rho_\sigma(y)}{\rho_\sigma(L)} = \frac{\rho_\sigma(b+qL)}{\rho_\sigma(L)}$ ← незав-ие. от b при $\sigma \ge \eta_{2^{-n}}(qL)$ ▶

=> оракул O^{SIS} получает на вход A с "корректным" распр-ем.

▶

Из Утв.1 => O^{SIS} выдаст $x \in \mathbb{Z}_q^m$ т.ч. $x^T A = 0$ и $0 < \|x\| \le \beta$.

Утверждение 2 При условии корректной работы O^{SIS},

1) $v \in L$,
2) $\|v\| \le \frac{1}{q}\cdot\beta\cdot n\sqrt{m}\cdot\|S\| \le \|S\|/2$,
3) $\Pr[v \notin H] = \Omega(1)$.

◀ 1. $v = \frac{1}{q}\cdot Y x = \frac{1}{q}\cdot B\cdot \underbrace{B^{-1} Y x}_{= x^T(B^{-1}Y)^T \equiv 0 \bmod q} = B\cdot\underbrace{\frac{1}{q}\cdot B^{-1} Y x}_{\in\mathbb{Z}} = B\cdot\mathbb{Z} \in L$.

2. $\|v\| = \frac{1}{q}\|Y\cdot X\| \le \frac{1}{q}\underbrace{\|X\|_1}_{\sum |x_i|} \cdot \underbrace{\max_i \|y_i\|}_{\le \sigma\cdot\sqrt{n}} \le \frac{1}{q}\cdot\sqrt{m}\cdot\beta\cdot\sigma\sqrt{n} = \frac{\beta}{q}\cdot n\sqrt{m}\cdot\|S\|.$

$\sigma\sqrt{n} = \sqrt{n}\cdot\|S\|$

$\le \sigma\cdot\sqrt{n}$ (Гауссов хвост)

$\|X\|_1 < \sqrt{m}\cdot\|X\|_2$

3. O^{SIS} знает только $a_i = B^{-1}\cdot y_i \bmod q \Leftrightarrow y_i \bmod qL$ (см. биекцию из Утв. 1).

При условии a_i, y_i распределены в соотв-ии $D_{qL+c_i,\sigma}$, где $c_i \in L$, т.к. $B^{-1}\cdot c_i = a_i \bmod q$.

Покажем, что y_i не может содержаться в $\mathcal{H}$.

Утверждение 2.1. L - решётка; $\mathcal{H}$ - гиперплоскость, $\frac{\sigma}{\sqrt{2}} \geqslant \eta_{2^{-n}}(L)$, то

$$\Pr_{b \leftarrow D_{L,\sigma}}[b \notin \mathcal{H}] \geqslant \Omega(1).$$

◁ Пусть $\mathcal{H}$ - гиперплоскость, ортогональная $(1, 0, 0 \dots, 0)$.

Если $b \leftarrow D_{L,\sigma}$, $b = (b_1 \dots b_n)$

$$e^{\frac{-\pi b_1^2}{\sigma^2} + \frac{-\pi b_1^2}{\sigma^2}} = e^{\frac{-\pi b_1^2}{(\sigma^2/2)}}$$

$$\rho_\sigma(\vec{b}) = \rho_\sigma(b_1)\,\rho_\sigma(b_2)\cdot\ldots\cdot\rho_\sigma(b_n)$$

$$\Pr_{b\leftarrow D_{L,\sigma}}[b \in \mathcal{H}] = \Pr[b_1 = 0] \underset{\text{нер-во Маркова}}{\le} \mathbb{E}[\rho_\sigma(b_1)] = \sum_{b\in L}\rho_\sigma(b_1)\cdot\frac{\rho_\sigma(\vec{b})}{\rho_\sigma(L)} = \sum_{b\in L}\rho_{\sigma/\sqrt{2}}\cdot\frac{\rho_\sigma(b_2)\dots\rho_\sigma(b_n)}{\rho_\sigma(L)}$$

$$\overset{PSF}{=} \frac{1}{\rho_\sigma(L)}\cdot\det(\hat{L})\cdot\frac{\sigma^n}{\sqrt{2}}\sum_{\hat{b}\in\hat{L}}\rho_{\frac{\sqrt{2}}{\sigma}}(\hat{b}_1)\dots\rho_{\frac{1}{\sigma}}(\hat{b}_n) \le \frac{\det(\hat{L})\cdot\sigma^n}{\rho_\sigma(L)\sqrt{2}}\underbrace{\sum_{\hat{b}\in\hat{L}}\rho_{\frac{\sqrt{2}}{\sigma}}(\hat{b})}_{\le(1+2^{-n})} \le \frac{\det(\hat{L})\cdot\sigma^n}{\rho_\sigma(L)\sqrt{2}}\cdot(1+2^{-n})$$

сглаж. пар-р

$\frac{\det(\hat{L})\cdot\sigma^n}{\rho_\sigma(L)} \in [1-2^{-n}, 1+2^{-n}]$

т.к. $\rho_{\frac{1}{\sigma}}(\hat{b}_i) \le \rho_{\frac{\sqrt{2}}{\sigma}}(\hat{b}_i)$

$e^{-\pi\hat{b}_i^2\cdot\sigma^2} \le e^{-\pi\frac{\sigma^2}{2}\cdot\hat{b}_i^2}$

$$\le [1 + 2^{-\Omega(n)}]\cdot\frac{1}{\sqrt{2}}.$$

$$\Rightarrow \Pr[b \in \mathcal{H}] \le \frac{1+2^{-\Omega(n)}}{\sqrt{2}} \Rightarrow \Pr[b \notin \mathcal{H}] \geqslant 1 - \frac{1+2^{-\Omega(n)}}{\sqrt{2}} = \Omega(1).$$

▶