Лекция №7.

Сложность CVP.

<u>Тривиально</u>: CVP_γ (принятия решения) сводится к $\mathrm{Approx}\,CVP_\gamma$ (задача поиска)

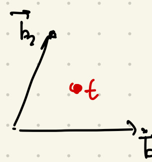
Теорема 1 $\mathrm{Approx}\,CVP_1$ сводится к CVP_1.

$\triangleleft$ $(B \in \mathbb{Z}^{n\times n}, t \in \mathbb{Q}^n)$ – вход к $\mathrm{Approx}\,CVP_1$.

Нужно найти $b \in L(B)$ – ближайший к t, используя оракул CVP_1.

Шаг 1 Вызываем оракул CVP_1 на (B, t) для аппроксимации $\underline{dist(L(B), t)}$, используя бинарный поиск по r.

$\exists R = \lambda_n(L(B))$



dist(t, L(B)) < λ_n

$CVP_1\left(L(B), t, \frac{R}{2}\right)$ $[0, R)$

"да" $\to$ $\left(L(B), t, \frac{R}{4}\right)$; "нет" $\to$ $\left(L(B), t, \frac{3R}{4}\right)$

$\left(L(B), t, \frac{R}{4}\right)$: "да" $\to$ $\left(L(B), t, \frac{R}{8}\right)$; "нет" $\to$ $\left(L(B), t, \frac{3R}{8}\right)$

$\left(L(B), t, \frac{3R}{4}\right)$: "да" $\to$ $\left(L(B), t, \frac{5R}{4}\right)$; нет $\to$ $\left(L(B), t, \frac{7R}{8}\right)$

$\vdots$

Имеем $\sim dist(L(B), t)$.

Шаг 2 Пусть $b = \sum_{i=1}^{n} x_i b_i$ – ближайший к t в $L(B)$.

Найдём $x_1 \bmod 2$

Вызовем $CVP_1\left(L([\underline{2b_1}, b_2, \ldots, b_n]), t, dist(L(B), t)\right)$

- Если $x_1 \equiv 0 \bmod 2$ для какого-либо ближайшего b к t, то

$$b = \underbrace{\frac{x_1}{2}}_{\in \mathbb{Z}} \cdot 2b_1 + \sum_{i>1} x_i b_i \in L([2b_1, \ldots, b_n]) \Rightarrow dist(L(B), t) =$$

$$= dist(L[2b_1 \ldots, b_n], t) \Rightarrow CVP_1 \text{ вернёт "да".}$$

• Если $x_1 \equiv 1 \bmod 2$, $dist(L,t) < dist(L[2b_1.., b_n], t)$ $\forall b$-ближайших к t $\Rightarrow$ $CVP_1(L[2b_1..b_n], t)$ вернёт "нет".

$\Rightarrow$ делаем вывод о $x_1 \bmod 2$.

Продолжим искать бинарное представление x_1:

Если $x_1 \equiv 0 \bmod 2$, то повторяем процедуру для $(t' = t, B' = [4b_1, b_2, .., b_n])$

Если $x_1 \equiv 1 \bmod 2$, то повторяем процедуру для $(t' = t - b_1, B' = [4b_1, b_2, .., b_n])$.

Когда x_1 найден, находим x_2 для $t' = t - x_1 b_1$, $B' = [b_2 \dots b_n]$. ▶

Открытый вопрос: Улучшить редукцию для $\gamma > 1 + \frac{1}{n}$.

Теорема 2 CVP_1 — NP-полная задача.

◁ Докажем редукцией от задачи о рюкзаке (Subset Sum, Knapsack).

Задача о рюкзаке: Вход: $a_1, .. a_n, S \in \mathbb{Z}$

Выход: "да", если $\exists x_i \in \{0,1\};\ S = \sum x_i a_i$

"нет", если $\nexists x_i \dots$,

Решение CVP_1 $\Rightarrow$ решение задачи о рюкзаке.

$$\text{Построим } B = \begin{array}{c} \begin{array}{ccc} x_1 & \quad\quad & x_n \end{array} \\ \begin{bmatrix} a_1 & \dots & a_n \\ 2 & & \\ & \ddots & \\ & & 2 \end{bmatrix} \end{array} \in \mathbb{Z}^{(n+1)\times n} \quad t = \begin{bmatrix} S \\ 1 \\ \vdots \\ 1 \end{bmatrix} \in \mathbb{Z}^{n+1}$$

Если $\exists x_i \in \{0,1\}:\ \sum x_i a_i = S \Rightarrow dist(L(B), t) = \| \sum x_i b_i - t \| =$

$$= \| (0, \underbrace{\overbrace{2x_1 - 1}^{\in\{-1,1\}}, \dots \overbrace{2x_n - 1}^{\in\{\pm 1\}}}_{n}) \| = \sqrt{n}$$

Если $CVP_1(\mathcal{L}(B), t, r = \sqrt{n}) \to$ "да", то выводим "да" для рюкзака

——— " ——— "нет", ——— " ——— "нет" ——— " ———

Покажем, что CVP_1 выводит "да" только для "да" инстанций задачи о рюкзаке, т.е. $\mathcal{L}(B)$ не содержит других ближайших к t векторов.

] $\exists x_1 .. x_n \in \mathbb{Z}: \|\sum x_i b_i - t\| \le \sqrt{n}$. Покажем, что $x_i \in \{0,1\} \Rightarrow x_i$ можно использовать в качестве ответа для задачи о рюкзаке.

Т.к. B содержит "2"-ки в строках от 2-ой до $(n+1)$-ой, то последние n-коэфф-ов $\sum x_i b_i - t$ всегда нечётные. Если какой-либо из $2x_i - 1 \notin \{\pm 1\}$, то $\|\sum x_i b_i - t\| > \sqrt{n}$ $\rightarrow$ все x_i т.ч. $\|\sum x_i b_i - t\| \le \sqrt{n}$ лежат в $\{0,1\}$.

▶

Замечания

1. CVP_1 – NP-сложная
2. CVP_γ – NP-сложная для $\gamma = n^{\frac{1}{c \cdot \lg\lg n}}$, c-конст. [Dinur-Kindler-Safra'98]
3. SVP_1 – NP-сложная (рандоми[illegible] редукция) [Ajtai'98].
4. SVP_γ – NP-сложная для $\gamma = e^{(\lg n)^{1-\varepsilon}}$ $(\varepsilon > 0)$ [Haviv-Regev'07].