Лекция № 7

Сложность CVP

Тривиально: CVP_γ (принятие решения) сводится к $ApproxCVP_\gamma$ (задача поиска)

Теорема 1 $ApproxCVP_1$ сводится к CVP_1.

◁ ($B \in \mathbb{Z}^{n\times n}$ - базис решётки, $t \in \mathbb{Q}^n$) - вход к $ApproxCVP_1$,

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

Шаг 1. Определение $dist(L(B), t)$

Вызываем оракул CVP_1 на (B, t) для аппроксимации $dist(L(B), t)$, используя бинарный поиск по пар-ру r.

$\exists\, R = \lambda_n(L(B))$ (или $\max\limits_i \|b_i\|$, $b_i \in B$)

Запускаем $CVP_1(L(B), t, r = \frac{R}{2})$

- "да" → $CVP_1(L(B), t, r = \frac{R}{4})$
  - "да" → $CVP(L(B), t, \frac{R}{8})$ → ⋮
  - "нет" → $CVP(L(B), t, \frac{3R}{8})$ → ⋮
- "нет" → $CVP(L(B), t, \frac{3R}{4})$
  - "да" → $CVP(L(B), t, \frac{5R}{4})$ → ⋮
  - "нет" → $CVP(L(B), t, \frac{7R}{8})$ → ⋮

В итоге, имеем $\sim dist(L(B), t)$.

Шаг 2. Поиск ближайшего вектора.

Пусть $b = \sum\limits_{i=1}^{n} x_i b_i$ - ближайший к t в $L(B)$

- Найдём $x_1 \bmod 2$.

Вызовем $CVP_1(L([2b_1, b_2, \dots, b_n]), t, dist(L(B), t))$

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

$$b = \underbrace{\frac{x_1}{2}}_{\in \mathbb{Z}} \cdot 2b_1 + \sum_{i>1} x_i b_i \in L([2b_1, b_2 \dots b_n]) \Rightarrow$$

$\Rightarrow \mathrm{dist}(L(B), t) = \mathrm{dist}(L([2b_1, b_2 \dots b_n]), t) \Rightarrow$

$\Rightarrow CVP_1$ вернёт "ДА".

- Если $x_1 = 1 \mod 2$ для всех ближайших к t векторов, то $\mathrm{dist}(L(B), t) < \mathrm{dist}(L([2b_1, b_2, \dots b_n])) \Rightarrow CVP_1(L[2b_1, b_2 \dots b_n], t)$ вернёт "нет".

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

- Продолжим искать бинарное представление x_1

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

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

- 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: $a_1 \dots a_n,\ S \in \mathbb{Z}$

Выход: "ДА" : Если $\exists\ x_i \in \{0,1\}$: $S = \sum x_i \cdot a_i$

"Нет" : Если $\nexists\ x_i \in \{0,1\}$: $S = \sum x_i a_i$

Имея оракул, решающий CVP_1, мы можем решить задачу о рюкзаке.

Построим

$$B = \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ 2 & 0 & \dots & 0 \\ 0 & 2 & \dots & 0 \\ \vdots & & & \\ 0 & \dots & & 2 \end{bmatrix} \in \mathbb{Z}^{(n+1) \times n}, \quad t = \begin{bmatrix} S \\ 1 \\ \vdots \\ 1 \end{bmatrix} \in \mathbb{Z}^{n+1}$$

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

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

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

—————— // —————— $\to$ "нет", то —//— "нет" ——//——

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

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

Так как B содержит "2"-ки в строках от 2-ой до $(n+1)$-ой, то последние n коэффов $\sum x_i b_i - t$ 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. $\| \sum x_i b_i - t \| \le \sqrt{n}$ должны лежать в $\{0, 1\}$. ▶

Замечания

1. CVP_1 - NP-сложная
2. CVP_γ - NP-сложная $\gamma = n^{\frac{1}{c \cdot \lg \lg n}}$, c - константа [Dinur-Kindler-Safra'99]
3. SVP_1 - NP-сложная (рандомизированная редукция) [Ajtai '98]
4. SVP_γ - NP-сложная для $\gamma = e^{\log(n)^{1-\varepsilon}}$ $(\varepsilon > 0)$ [Haviv-Regev'07]