# Сложность CVP

Tuesday 1 March 2022 08:29

Тривиально: $CVP_\gamma$ (принятие решения) сводится к Approx $CVP_\gamma$ (задача поиска)

**Thm 1** Approx $CVP_1$ сводится к $CVP_1$.

◀ $(B\in\mathbb{Z}^{n\times n},\ t\in\mathbb{Q}^n)$ — вход к Approx $CVP_1$. Задача: найти $b\in L(B)$ — ближайший к $t$, используя оракул $CVP_1$.

**Шаг 1** Вызвать оракул $CVP_1$ для $(B,t)$ для аппроксимации $dist(L(B),t)$, используя бинарный поиск по $r$, а именно:

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

$[0,R)$ разбиваю на интервале

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

"да" ↙ ↘ "нет"

$CVP_1(L(B),t,\frac{R}{4})$ $\quad$ $CVP_1(L(B),t,\frac{3R}{4})$

"да" ↙

$CVP_1(L(B),t,\frac{R}{8})$ ...

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

Найдём $x_1 \bmod 2$.

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

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

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

$\Rightarrow CVP_1()$ вернёт "да"

- иначе, $dist(L,t) < dist(L[2b_1,\dots,b_n],t)$, $\forall b$ — ближайшего к $t$ $\Rightarrow$ $CVP_1()$ вернёт "нет"

$\Rightarrow x_1 = 1 \bmod 2$.

Продолжим искать бинарное представление $x_1$: Если $x_1 \equiv 0 \bmod 2$, то повторяем процедуру с $(t'=t, B'=[4b_1, b_2,\dots,b_n])$ (новый целевой)

Если $x_1 \equiv 1 \bmod 2$, — // — $(t'=t-b_1, B'=[4b_1, b_2,\dots,b_n])$

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

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

**Thm 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 $\exists x_i \in\{0,1\}$ : $S=\sum x_i a_i$

"не", иначе.

Решение $CVP_1$ $\Rightarrow$ Решение задачи о рюкзаке

Построим
$$B = \begin{array}{c} \begin{matrix} x_1 & x_2 & \dots & x_n \end{matrix} \\ \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ 2 & & & \\ & 2 & & \\ & & \ddots & \\ & & & 2 \end{bmatrix} \end{array} \in \mathbb{Z}^{(n+1)\times n}, \quad t = \begin{bmatrix} S \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \in \mathbb{Z}^{n+1}$$

Если $\exists x_i\in\{0,1\}$: $\sum x_i a_i = S \Rightarrow dist(\mathcal{L}(B),t) = \|\sum x_i b_i - t\| = \|(0, \underbrace{\overbrace{2x_1-1, 2x_2-1,\dots, 2x_n-1}^{\in\{-1,1\}}}_{n})\| = \sqrt{n}$

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 рюкзака, т.е. $\mathcal{L}(B)$ нет других ближайших к $t$ векторов

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

Т.к. $\mathcal{B}$ содержит "2"-ки на гл. диагонали (в [2 … n+1] -строки от 2 до n+1), то последние $n$-коэфф-тов $\sum x_i b_i - t$ всегда нечётные. Если какой-либо из $2x_i - 1 \notin \{-1, 1\}$, то $\| \sum x_i b_i - t \| > \sqrt{n}$ ↯

$\Rightarrow$ все $x_i \in \{0, 1\}$.

**Замечания**

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