CVP & SVP

Monday 8 March 2021 09:56

Трудные задачи на решётках

I. Определения

- **SVP$_\gamma$** ($\gamma \geq 1$) — для решётки $L \leq \mathbb{Z}^n$, заданной базисом B, и $r > 0$ опр
 какой из двух случаев ниже выполняется

 (1) $\lambda_1(L) \leq r$ ("ДА")

 (2) $\lambda_1(L) > \gamma \cdot r$ ("НЕТ")

- **Approx SVP$_\gamma$** — для решётки L, заданной базисом B, найти b

 $0 < \|b\| \leq \gamma \cdot \lambda_1(L)$

SVP$_\gamma$ сводится к Approx SVP$_\gamma$

- **CVP$_\gamma$** — для решётки $L \leq \mathbb{Z}^n$, $t \in \mathbb{Q}^n$ ("целевой" (target) вектор) и $r > 0$, опр
 какой из двух случаев ниже выполняется

 (1) $\mathrm{dist}(t, L) \leq r$ ("ДА"

 (2) $\mathrm{dist}(t, L) > \gamma \cdot r$ ("НЕТ

- **Approx CVP$_\gamma$** — для решётки $L \leq \mathbb{Z}^n$ и $t \in \mathbb{Q}^n$, найти $b \in L$

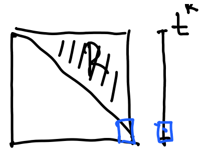
 $\|b - t\| \leq \gamma \cdot \mathrm{dist}(t, L)$

 В случае $t \in L$, вернём $b = t$.

<u>Замечание</u> Мы знаем, что Approx SVP$_\gamma$ $\in P$ для $\gamma \geq e^{\frac{c \cdot n \log\log n}{\log n}}$,
(см. лекцию про BKZ-редукцию)

<u>Thm 1</u> Approx CVP$_\gamma$ $\in P$ для $\gamma = 2^n$

◀ Положим, $B = Q \cdot R$ — LLL-редуцированный базис.
Положим, B — полного ранга ($t \in \mathrm{Span}_{\mathbb{Q}}(B)$)
Пусть $b^* = \sum x_i \vec{b}_i$ — ближайший к t.
Положим $t^R = Q^T \cdot t$, $b^{*R} = Q^T \cdot b$ (рассматриваем b и t относ



Делаем "редукцию по р-ру" для t^R относительно R.

1) находим x_n' т.ч. $t_n^R - x_n' r_{nn} \le \frac{r_{nn}}{2}$

2) — // — x_{n-1}' т.ч. $t_{n-1}^R - x_n' r_{n-1,n} - x_{n-1}' \cdot r_{n-1,n-1} \le \frac{r_{n-1,n-1}}{2}$

$\vdots$

Найдём $x_1' \dots x_n'$, т.ч. i-ая координата $|(t^R -$

Выход: $b' = \sum x_i' \cdot \vec{b_i}$

Случай 1 $\quad \underset{\text{ближайший вектор}}{\|b^*} - t\| \ge \frac{r_{nn}}{2}$

мы нашли b', т.ч. $\|b'-t\|^2 = \|\overset{QR}{B} \cdot x' - Q t^R\|^2 = \| Rx' - t$ — Q не меняет норму

$\le \frac{1}{4} \sum_{i \le n} r_{ii}^2 \underset{LLL}{\le} \frac{1}{4} \sum_i 2^{2(n-i)} r_{nn}^2 \le 2^{2n} \cdot \frac{r_{nn}^2}{4} \Rightarrow$

$(r_{ii} \le \alpha^{n-i} \cdot r_{nn})$

$\Rightarrow \|b'-t\| \le 2^n \cdot \frac{r_{nn}}{2} \le 2^n \cdot \frac{2\|b^*-t\|}{2} \le 2^n \cdot \|b^*-t\|.$

Случай 2 $\quad \|b^*-t\| < \frac{r_{nn}}{2} \Leftrightarrow \|b^{*R} - t^R\| < \frac{r_{nn}}{2} \Rightarrow |x_n \cdot r_{nn} - t_n^R|$

$\Rightarrow x_n' = x_n$ (по опр-ию редукции р-ра);

аналог. рассуждения для x_{n-1}' (рассматриваем $b^* - x_n$

$t - x_n'$

Замечание $\quad$ Процедура, описанная в док-ве Теоремы 1, называ

алгоритмом Бабая.

II CVP vs. SVP

Thm2 SVP_γ сводится к CVP_γ $\forall \gamma \ge 1$. Утверждение верн

◀ для $\gamma = 1$ и версий поиска (Approx).

Цель: построить эффективный алг-м, находящий кратчайший вектор, Оракул, находящий ближайший вектор.

B – базис L ; $B \in \mathbb{Z}^{n \times n}$

$B^{(i)} := [b_1, \dots, b_{i-1}, 2 \cdot b_i, b_{i+1}, \dots, b_n]$

$t^{(i)} := b^{(i)}$

Для $i = 1 \dots n$:

вызвать $CVP(B^{(i)}, t^{(i)})$

$c_i \in L(B^{(i)})$ – результат

Вернуть $(c_i - b_i) = \arg\min_i \|c_i - b_i\|$

Редукция

Покажем, что вывод алг-ма действительно кратчайший вектор в

Пусть $b = \sum x_i b_i \in L$ – кратчайший в L. $\Rightarrow \exists i : x_i$ – нечётно (ин

Запишем $b = b_i + \left[\sum_{j \neq i} x_j \cdot b_j + \underbrace{\left(\frac{x_i - 1}{2}\right)}_{\in \mathbb{Z}} \cdot b_i \cdot 2\right] \in b_i + L(B^{(i)}) \Rightarrow dist($

с другой стороны, по построению $t^{(i)}, B^{(i)}$: $dist(t^{(i)}, B^{(i)}) \geq \lambda_1($

$\Rightarrow \|\underbrace{c_i - b_i}_{\in L}\| = \lambda_1(L) \Rightarrow c_i - b_i$ – решение SVP

Открытые вопросы

1) Редукция в док-ве Т-мы 2 типа "мн

n

?: сделать редукцию 1-1.

2) Обратная редукция от CVP to SVP

III Сложность CVP

Тривиально: CVP_γ сводится к $ApproxCVP_\gamma$ (задача приняти

Т-ма 3 $ApproxCVP_1$ сводится к CVP_1.

◀ ∃ $(B \in \mathbb{Z}^{n \times n}, t \in \mathbb{Q}^n)$ – вход к Approx CVP_1. Задача: найти

используя оракул CVP_1.

<u>Шаг 1</u>. Вызывать оракул CVP_1 для (B, t) для аппроксимац

<u>Шаг 2</u>. Пусть $b = \sum x_i b_i$ – ближайший вектор; найдём x_1 m

Вызовем $CVP_1([2b_1, b_2, .., b_n], t)$

для какого-либо ближайшего b к t

Если $x_1 \equiv 0 \mod 2 \Rightarrow b = \underbrace{\frac{x_1}{2}}_{\in \mathbb{Z}} \cdot 2b_1 + \sum_{i \geq 2} x_i b_i \in [2b_1, b_2, \ldots$

иначе, $dist(b, L) < dist(b, L[2b_1, .. b_n])$ ←

↑ ∀ b-ближайших к t, выполняется $x_1 = 1 \mod 2$.

Продолжим искать бинарное представление x_1; Если $x_1 \equiv 0$

Если $x_1 \equiv 1$

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

<u>Открытые вопросы</u> Улучшить редукцию для $\gamma > 1 + \frac{1}{n}$ (например,

<u>Т-ма 4</u> CVP_1 – NP-полная задача.

◀ Докажем редукцией от задачи о рюкзаке (Subset S

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

Выход: "да", если $\exists x_i \in$

"нет", иначе

Решение CVP_1 $\Rightarrow$ Решение задачи о рюкзаке.

Построим $B = \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ 2 & & & \\ & 2 & & \\ & & \ddots & \\ & & & 2 \end{bmatrix} \in \mathbb{Z}^{(n+1)\times n}$,

Если $\exists x_i \in \{0,1\}$: $\sum x_i a_i = S \Rightarrow dist(\mathcal{L}(B), t) = \sqrt{n}$ =

Если $CVP_1(B,t) \rightarrow$ "да" $\Rightarrow$ выводим "да" для р

— // ——— $\rightarrow$ "нет" $\Rightarrow$ — // — "нет" — //

Покажем, что CVP_1 выводит "да" только для "да" инста

Т $\exists x_1 \dots x_n \in \mathbb{Z}$: $\| \sum x_i b_i - t \| \le \sqrt{n}$. Покажем, что

т.к. B содержит "2"-ки на главной диагонали,

$\sum x_i b_i - t$ всегда нечётные. Если какой-

$\| \sum x_i b_i - t \| > \sqrt{n} \Rightarrow$ все $x_i \in \{0,1\}$. Анало

Замечания

1. CVP_1 - NP-сложная
2. CVP_γ - NP-сложная для $\gamma = n^{\frac{1}{c \lg\lg n}}$, $c \in \Theta(1)$ [

3. SVP_1 - NP-сложная (рандомизированная редукция) [A

4. SVP_γ - NP-сложная для $\gamma = e^{\lg n^{1-\varepsilon}}$ $(\varepsilon > 0)$, [