I. Определения

(shortest vector problem)

• SVP_γ ($\gamma \geq 1$) → для решётки $L \subseteq \mathbb{Z}^n$, заданной базисом B, и $r > 0$ ($\in \mathbb{R}$) определить, какой из двух случаев выполняется:

$$(1)\ \lambda_1(L) \leq r \quad (\text{"да"})$$
$$(2)\ \lambda_1(L) > \gamma \cdot r \quad (\text{"нет"})$$

• Approx SVP_γ — для решётки L, заданной базисом B, найти $b \in L$, т.ч.

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

SVP_γ "сводится" к Approx SVP_γ: A "сводится" к B, если, имея оракул, решающий B, мы можем решить задачу A.

Closest vector problem

• CVP_γ — для решётки $L \subseteq \mathbb{Z}^n$ и $t \in \mathbb{Q}^n$ ("целевой" (target) вектор) и $r > 0$, определить, какой из двух случаев выполняется:

$$(1)\ \mathrm{dist}(t, L) \leq r \quad (\text{"да"})$$
$$(2)\ \mathrm{dist}(t, L) > \gamma \cdot r \quad (\text{"нет"})$$

• Approx CVP_γ — для решётки $L \subseteq \mathbb{Z}^n$, $t \in \mathbb{Q}^n$, найти $b \in L$, т.ч.

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

В случае $t \in L$, то возвращаем $b = t$.

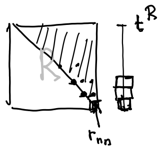
Замечание Мы знаем, что Approx $SVP_\gamma \in P$ (класс Polytime) для $\gamma \geq \exp(n)$ (LLL-редукция)

Thm 1. Approx $CVP_\gamma \in P$ для $\gamma = 2^n$.

◀ Положим $B = QR$ — LLL-редуцированный базис. ($\exists$ B-полного ранга)

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

Положим $t^R = Q^T \cdot t$, $b^{*R} = Q^T \cdot b^*$ (мы $\measuredangle$ b^* и t относительно R)



Делаем "редукцию по размеру" для t^R:

1) находим $x'_n \in \mathbb{Z}$ т.ч. $t^R_n - x'_n \cdot r_{nn} < \frac{r_{nn}}{2}$

2) находим $x'_{n-1} \in \mathbb{Z}$ т.ч. $t^R_{n-1} - x'_n \cdot r_{n-1,n} - x'_{n-1} \cdot r_{n-1,n-1} < \frac{r_{n-1,n-1}}{2}$

$\vdots$

В итоге, получим $x'_1 \dots x'_n$, т.ч. i-ая координата $\left|t^R - \sum x'_i r_i\right| < \frac{r_{ii}}{2}$ $\forall i$

Выход: $b' = \sum x'_j \cdot b_j \in L$

Покажем, что $\|b' - t\| \leq 2^n \|b^* - t\|$

Случай 1 $\|b^* - t\| \geq \frac{r_{nn}}{2}$

Мы нашли b', т.ч. $\|b' - t\|^2 = \|\overset{Q \cdot R}{B} \cdot x' - Q \cdot t^R\|^2 \underset{Q \text{ не меняет нормы}}{=} \|Rx' - t^R\|^2 = \|\sum x'_i r_i - t^R\|^2$

$$\leq \frac{1}{4} \sum_{i=1}^n r_{ii}^2 \underset{LLL}{\leq} \frac{1}{4} \sum 2^{2(n-i)} \cdot r_{nn}^2 \leq 2^{2n} \cdot \frac{r_{nn}^2}{4};$$

$(r_{ii} \leq \alpha^{n-i} \cdot r_{nn},\ \alpha \geq 2)$

$\|b' - t\| \leq 2^n \cdot \frac{r_{nn}}{2} \leq 2^n \cdot \|b^* - t\|$ (случай 1).

Случай 2 $\|b^* - t\| < \frac{r_{nn}}{2} \iff \|b^{*R} - t^R\| < \frac{r_{nn}}{2} \Rightarrow \left|\underline{x_n} \cdot r_{nn} - t^R_n\right| < \frac{r_{nn}}{2} \Rightarrow$

$x_n = x'_n$ ($\Rightarrow$ в р-те редукции по раз-ру для t^R отыщем x_n).

$\leftarrow$ аналогично рассуждаем для x'_{n-1}, рассматривая $(b^* - x_n \cdot b_n)$ — ближайший к $t := t - \underset{x_n}{x'_n} \cdot b_n$) ▶

Замечание Процедура, описанная в док-ве Thm 1., называется алгоритмом Бабая.

II CVP vs. SVP

Thm 2 SVP_γ сводится к CVP_γ $\forall \gamma \geq 1$. Утверждение верно и для Approx-версий задач.

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

Цель: имея оракул для задачи CVP_1, решить задачу SVP_1.

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

редукция

Вернуть $(c_i - b_i)$ т.ч. $\|c_i - b_i\|$ - min. среди $\{\|c_i - b_i\|\}_i$ $\left((c_i - b_i) = \underset{i}{\operatorname{argmin}} \|c_i - b_i\|\right)$

Покажем, что вывод алг-ма действительно кратчайший вектор в L.

Пусть $b = \sum x_i b_i \in L$ - кратчайший в L $\Rightarrow \exists i$, т.ч. x_i - нечётно (иначе, $\left(\frac{b}{2}\right)^{\in L}$ - короче b).

Запишем $b = b_i + \left[\sum_{j \neq i} x_j b_j + \underbrace{\left(\frac{x_i - 1}{2}\right)}_{\in \mathbb{Z}} \cdot 2 b_i\right] \in b_i + L(B^{(i)}) \Rightarrow dist(L(B^{(i)}), \underset{"b_i"}{t^{(i)}}) \leq \|b\| = \lambda_1(L)$

потенциально в $L(B^{(i)}) + b_i$ могут содержаться вектора, короче b.

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

Получаем $dist(L(B^{(i)}), t^{(i)}) = \lambda_1(L) \Rightarrow \|\underbrace{c_i - b_i}_{\in L(B)}\| = \lambda_1(L) \Rightarrow c_i - b_i$ - решение SVP ▶

Открытые вопросы: 1) редукция в док-ве Thm 2. - это редукция типа "много - к - одному"
 (n вызовов CVP → 1 решение SVP)

 Вопрос: редукция 1-1 с сохранением р-ти решёток.

 2) обратная редукция от CVP к SVP с одинаковым пар-ом γ.