Applicazioni

1. CVP-γ Closest vector
2. fattorizzazione $f(x) \in \mathbb{Z}[x]$
3. Attacchi a RSA

---

1. CVP-γ. Dato un reticolo $\mathcal{L}(B) \subset \mathbb{Z}^m$ di rango n e $t \in \mathbb{R}^m$ trovare $x \in \mathcal{L}(B)$ t.c. $\forall y \in \mathcal{L}(B)$ $\|x-t\| < \gamma \|y-t\|$

Algoritmo Babai $\gamma = 2\left(\frac{2}{\sqrt{3}}\right)^n$, $\delta = \left(\frac{1}{4} + \frac{3}{4}^{n/n-1}\right)$

Noi proviamo $\gamma = 2^{n/2}$ $\delta = \frac{3}{4}$

<u>IDEA</u> $\mathcal{L} \to$ calcoliamo B LLL-ridotta

procediamo "aggiungendo" t e considerando (B, t). Da $t^* = t - \sum \mu_j b_j^*$ $\mu_j = \frac{(t, b_j^*)}{\|b_j^*\|}$

"costruiamo $x \in \mathcal{L}(B)$ tale che

$x = t - x = t - \sum [\mu_j] b_j$ e proviamo

che x ha le prop. richieste

Algoritmo

Input: $\mathcal{B}$ base di un reticolo $\mathcal{L} \subset \mathbb{R}^n$ di rango n
$t \in \mathbb{Z}^n$

output: $x \in \mathcal{L}$ t.c. $\|x - t\| \leq 2^{\frac{n}{2}} d(t, \mathcal{L})$

1. Calcola B la base LLL ridotta, $\delta = \frac{3}{4}$
2. $b := t$
3. for j $n..1$ repeat

$$b := b - c_j b_j \quad \text{con} \quad c_j = \left\lceil \frac{(b, b_j^*)}{\|b_j\|^2} \right\rfloor$$

4. output $t - b$.

1 <u>oss.</u> Come prima se scriviamo la matrice rispetto a $\frac{b_1^*}{\|b_1^*\|}, \dots, \frac{b_n^*}{\|b_n^*\|}, \underbrace{a_{n+1}, \dots a_m}_{\text{completo base ortonormale}}$ si ha

$$\left(\begin{array}{ccccc} \|b_1^*\| & * & * & * & \cdots \\ & \|b_2^*\| & * & * & \cdots \\ & & \ddots & & \\ & & & & \|b_n^*\| \\ \hline & & 0 & & \end{array}\right) \qquad \begin{pmatrix} t_1 \\ \vdots \\ \vdots \\ t_m \end{pmatrix}$$

Con le operazioni che facciamo cerchiamo una combinazione lineare delle colonne in modo che $\forall i$ la coordinata i-esima sia $\leq t_i \pm \frac{1}{2}\|b_i^*\|$.

Vediamo che l'algoritmo è corretto.

Sia $t \in \mathbb{Z}^m$ e x l'output dell'alg.

e $y \in \mathcal{L}(B)$ il vettore più vicino a t

$d(t, \mathcal{L}(B)) = y$.

Vogliamo vedere che

$$\|x-t\| \le 2^{n/2} \|t-y\|$$

Oss. - Se $t \in (b_1, \dots, b_n)$ $\|x-t\|^2 \le \frac{1}{4} \sum_1^n \|b_i^2\|$

Inoltre

$$\|x-t\| \le \frac{1}{2} \cdot 2^{n/2} \|b_n^*\|$$

Infatti * Lovacz $\forall i$ $\|b_i^*\| \le 2^{\frac{n-i}{2}} \|b_n^*\|$

e quindi

$$\|x-t\|^2 \le \frac{1}{4} \sum_1^n \|b_i^*\|^2 \le \frac{1}{4} \sum 2^{n-i} \|b_n^*\|^2$$

$$\le \frac{1}{4} 2^n \|b_n^*\|^2$$

In particolare se $d(t,\mathcal{L}) \geq \frac{1}{2}\|b_n^*\|$, $t \in (b_1,..,b_n)$

l'algoritmo è corretto perché

$$\frac{\|x-t\|}{d(t,\mathcal{L})} \leq \frac{\frac{1}{2}\, 2^{n/2}\,\|b_n^*\|}{\frac{1}{2}\|b_n^*\|} = 2^{n/2}$$

Vediamo gli altri casi, $t \notin (b_1,..,b_n)$, $\|t-y\| < \frac{1}{2}\|b_n^*\|$

→ Sia $s = \pi(t)$ la proiezione di t su $(b_1,..,b_n)$

Proviamo per induzione su n che

$$\|x-s\| \leq 2^{n/2}\|y-s\|$$

(a) $\|y-s\| < \frac{\|b_n^*\|}{2}$ allora c è la scelta migliore

e

$y \in c y_n + y'$ $\quad y' \in \mathcal{L}(b_1,..,b_{n-1})$

ed è il punto più vicino a $s' = s - cb_n$

per le ipotesi induttive

$$\|x-s\| = \|x'-s'\| \leq 2^{\frac{n-1}{2}}\|y'-s'\| =$$

$$= 2^{\frac{n-1}{2}}\|y-s\| \leq 2^{n/2}\|y-s\|$$

Se $\|y-s\| > \frac{\|b_n^*\|}{2}$ applichiamo l'osservazione a $s \in \mathcal{L}(b_1, \dots, b_{n-1})$ e x

$$\|x-s\| \leq \frac{1}{2} 2^{n/2} \|b_n^*\| \leq 2^{n/2} \|y-s\| \, .$$

Da questo segue che

$$\begin{aligned} \|x-t\|^2 &= \|s-t\|^2 + \|x-s\|^2 \leq \\ &\leq \|s-t\|^2 + 2^{n} \|y-s\| \\ &\leq 2^n (\|s-t\|^2 + \|y-s\|^2) \\ &= 2^n \|y-t\| \end{aligned}$$

$\boxtimes$