HONORS ALGORITHMS

2024-03-01

1

$v_1, \dots, v_n \in \mathbb{R}^n$ basis

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} \alpha_i v_i \;\middle|\; \alpha_i \in \mathbb{Z} \right\}$$

GRAM-SCHMIDT ORTHOGONALIZATION

$v_1^*, \dots, v_n^*$ $\quad v_i^* \perp v_j^*$

$$v_1 = v_1^*$$
$$v_2 = v_2^* + \mu_{21} v_1^*$$
$$\vdots$$
$$v_k = v_k^* + \sum_{i=1}^{k-1} \mu_{ki} v_i^*$$
$$\vdots$$

elementary trf

$v_k \leftarrow v_k - \alpha \cdot v_j$

$j < k, \ \alpha \in \mathbb{Z}$

$v_{i+1} \leftrightarrow v_i$

SmallCoeffs

$\binom{n}{2}$ elem. ops $\Longrightarrow (\forall_{j<k} k j)(|\mu_{kj}| \leq \frac{1}{2})$

for $k = 1$ **to** n

  for $j = k-1$ **downto** 1

    fix μ_{kj}

does not change the v_i^*

---

while $(\exists i)(\|v_{i+1}^*\| < \frac{1}{\sqrt{2}}\|v_i^*\|)$

  swap v_i, v_{i+1}

---

if this terminates

$\rightsquigarrow \|v_1\| \leq 2^{\frac{n-1}{2}} \cdot \min\{\|x\| \mid x \in \mathcal{L}, x \neq 0\}$

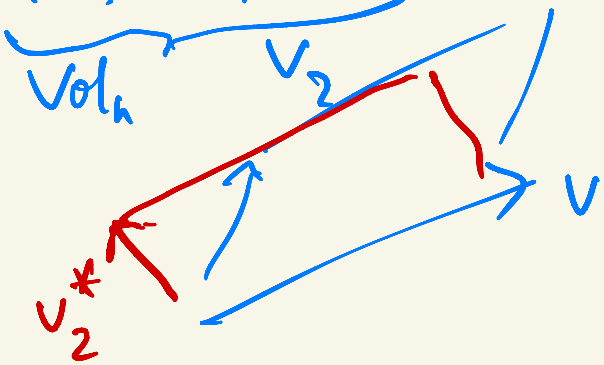
?

SVP

Potential function

$$P = vol(v_1)\cdot vol(v_1\, v_2)\cdot \ldots \cdot vol(v_1 \cdots v_n)$$

$$= \underbrace{\|v_1^*\|}_{vol_1} \cdot \underbrace{\|v_1^*\|\cdot\|v_2^*\|}_{vol_2} \cdot \ldots \cdot \underbrace{\|v_1^*\|\cdots\|v_n^*\|}_{Vol_n}$$



$$= \|v_1^*\|^n \cdot \|v_2^*\|^{n-1}\cdot \ldots \cdot \|v_n^*\|$$

Small Coeffs proc. does not change P

effect of swap $\underbrace{v_i \longleftrightarrow v_{i+1}}$ if $\|v_{i+1}^*\| < \frac{1}{\sqrt{2}}\|v_i^*\|$

P', new value after swap

$$\mathcal{U}_i = span\{v_1 \cdots v_i\} = span\{v_1^* \cdots v_i^*\}$$

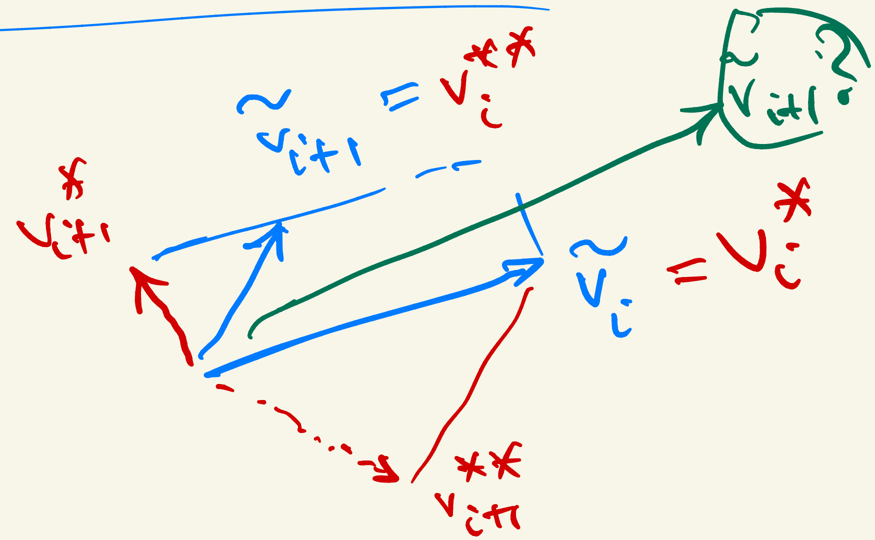
the only $\mathcal{U}_j$ that changes is $\mathcal{U}_i$ v_i^*, v_{i+1}^* change

$$W = \operatorname{span}\{v_i^*, v_{i+1}^*\}$$

$$\operatorname{proj}: \mathbb{R}^n \to W$$

$$\underline{x} = \sum_{j=1}^{n} \delta_j v_j^* \longrightarrow \delta_i v_i^* + \delta_{i+1} v_{i+1}^* \qquad \underline{x} \mapsto \underline{\tilde{x}}$$

$$\tilde{v}_i, \tilde{v}_{i+1}$$



$$\frac{P'}{P} = \frac{\|v_i^{**}\|}{\|v_i^*\|} = \frac{\|\tilde{v}_{i+1}\|}{\|v_i^*\|} < \frac{\sqrt{3}}{2}$$

$$\tilde{v}_{i+1} = v_{i+1}^* + \mu_{i+1,i} v_i^*$$

$$\|\tilde{v}_{i+1}\|^2 = \underbrace{\|v_{i+1}^*\|^2}_{} + \underbrace{\mu^2}_{} \|v_i^*\|^2 < \left(\frac{1}{2} + \frac{1}{4}\right) \underbrace{\|v_i^*\|^2}_{\tilde{v}_i}$$

$$\|v_i^*\| \cdot \|v_{i+1}^*\| = \|v_i^{**}\| \|v_{i+1}^{**}\|$$

5

$\therefore \quad P' \leq \frac{\sqrt{3}}{2} P$

if t rounds: $P_{end} \leq \left(\frac{\sqrt{3}}{2}\right)^t P_{beginning}$

$\therefore \quad \log P_{end} \leq t \cdot \log \frac{\sqrt{3}}{2} + \log P_{beg}$

$\log P_{end} - \log P_{beg} \leq t \cdot \log \frac{\sqrt{3}}{2}$

$\frac{1}{\log \frac{2}{\sqrt{3}}} \log \frac{P_{beg}}{P_{end}} \geq \cancel{t \cdot \underbrace{\log \frac{2}{\sqrt{3}}}}$

$\therefore t \leq O(n \cdot b(\text{input}))$

DO $\quad P^2 \in \mathbb{Z}$

$\therefore \quad \underline{P_{end} \geq 1}$

$\underline{P_{beg} \leq |\text{input}|^n}$ ✓

LLL Lenstra, Lenstra, Lovász

NVP within $2^{\frac{n}{2}}$

1984