HONORS ALGORITHMS | 2024-02-28 | 1

NP-completeness

EXP. TIME HYPOTHESIS: 3SAT cannot be solved in $(2-\varepsilon)^n$

MITIGATION STRATEGY: approximate algorithm

? TAS poly-time approximation scheme

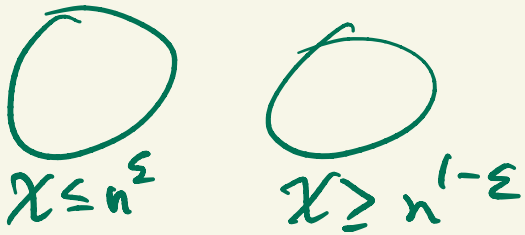
e.g. KNAPSACK

MAX-3SAT $C_1 \dots C_m$ 3-clauses

$\mu :=$ max # simult satisfied 3-clauses

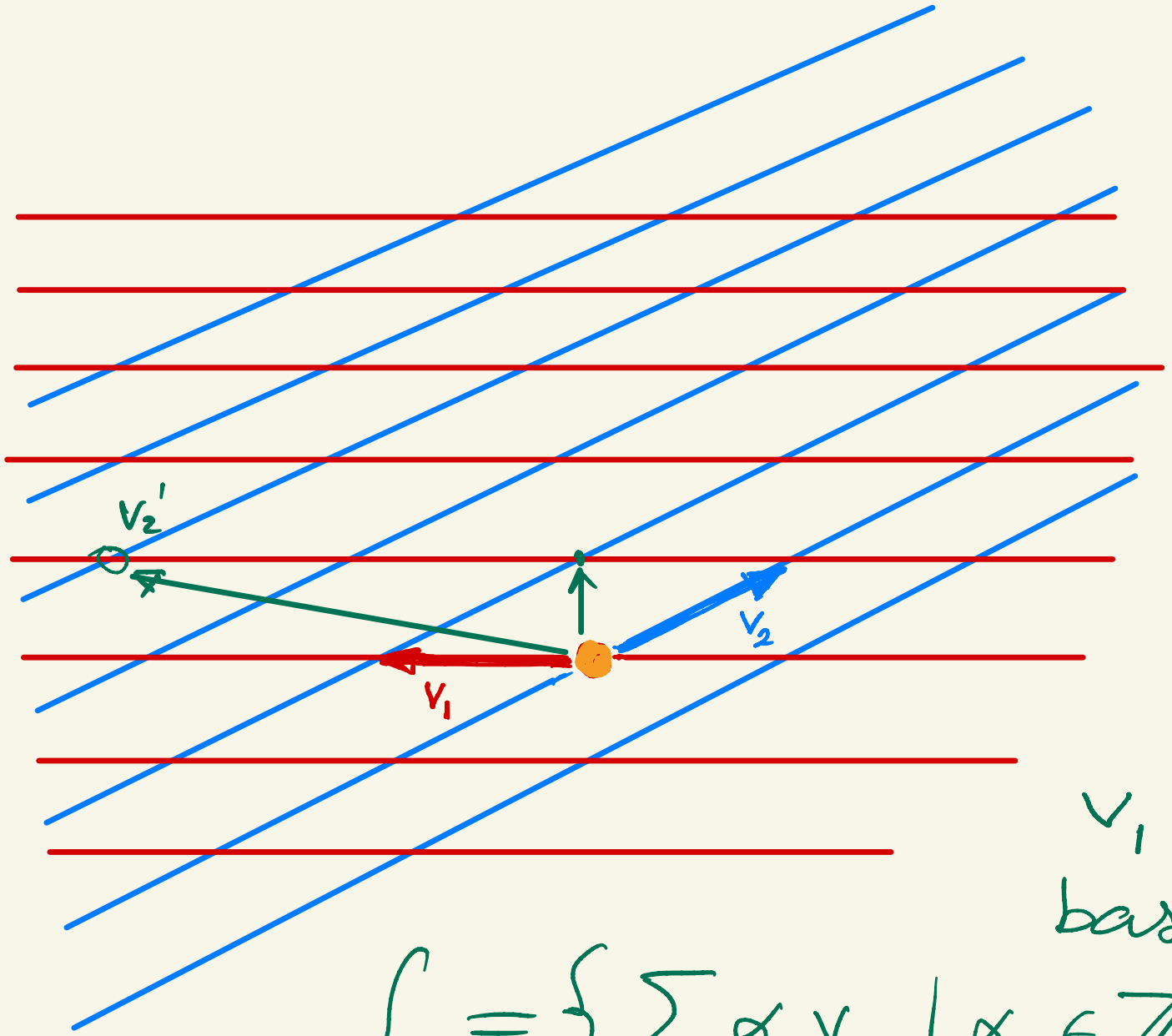
$\mu \geq \frac{7m}{8}$

THM $\left(\frac{7}{8}+\varepsilon\right)\cdot OPT$ is NP-hard



CHROM NUM
CLIQUE } approx within $n^{1-\varepsilon}$ factor is NP-hard

SVP
Shortest vector problem



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

basis

$$\mathcal{L} = \left\{ \sum \alpha_i v_i \mid \alpha_i \in \mathbb{Z} \right\}$$ LATTICE

$v_2' := v_2 - 3v_1$

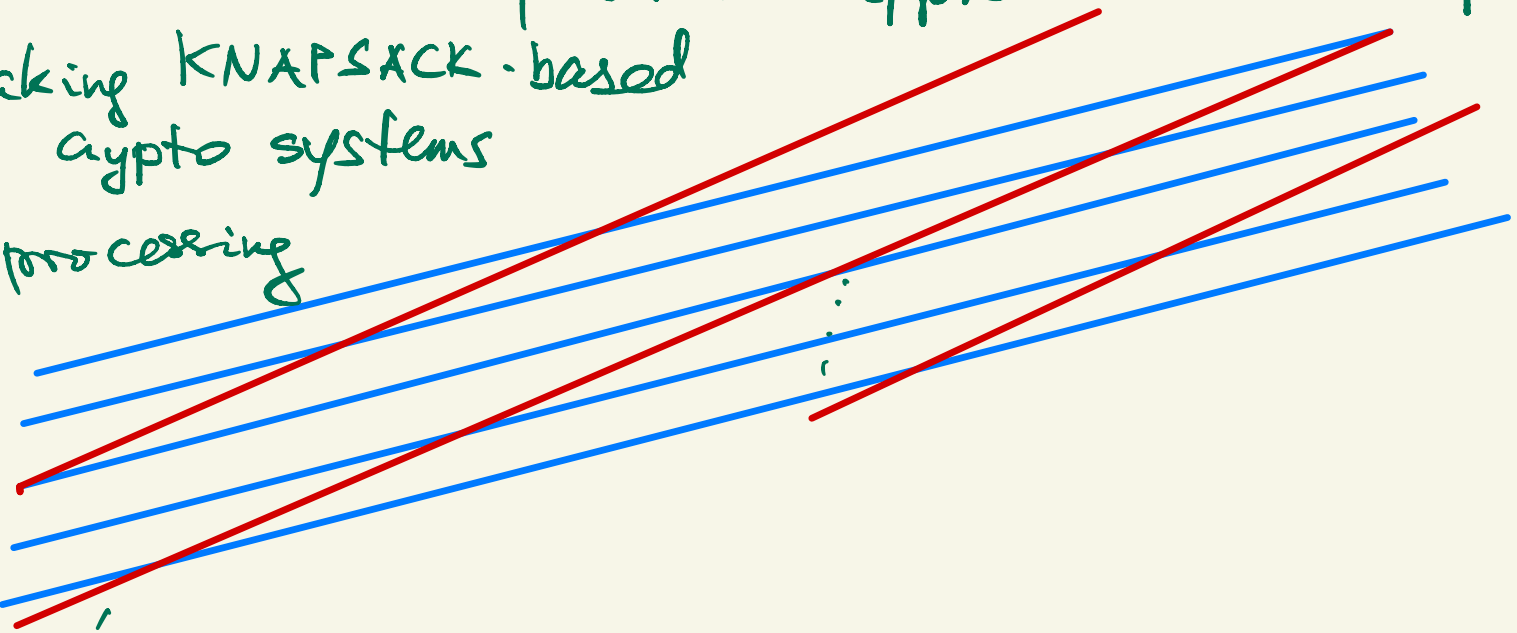
Applications: factoring $f \in \mathbb{Q}[x]$ in poly time

↳ Mertens conj. disproof

↳ diophantine approx $\alpha_1 \ldots \alpha_n \in \mathbb{R}$ $\left|\alpha_i - \frac{p_i}{q}\right| < \varepsilon$

breaking KNAPSACK-based aypto systems

signal processing



$$\varepsilon = \frac{1}{q^{1+\frac{1}{n}}}$$

LÁSZLÓ LOVÁSZ

lattice reduction

finds shortest vector within $2^{\frac{n-1}{2}}$ factor

GRAM-SCHMIDT ORTHOGONALIZATION

$v_1 \dots v_n$ basis of $\mathbb{R}^n$ $\longrightarrow$ [G-S] $\longrightarrow$ $v_1^* \dots v_n^*$

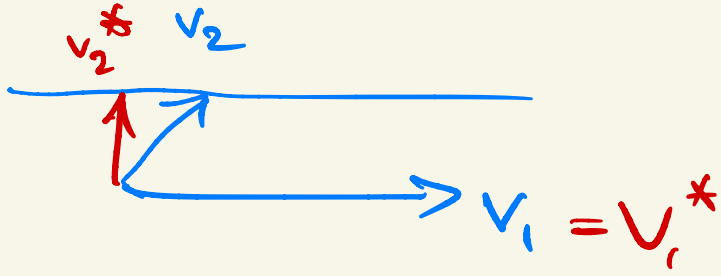
orthogonal $v_i^* \perp v_j^*$ $i \neq j$

$U_0 = \{0\}$ $U_i = \text{span}\{v_1 \dots v_i\} = \text{span}\{v_1^* \dots v_n^*\}$

$v_i - v_i^* \in U_{i-1}$

$$
\begin{aligned}
v_1 &= v_1^* \\
v_2 &= v_2^* - \mu_{21} v_1^* \\
v_3 &= v_3^* - \mu_{32} v_2^* - \mu_{31} v_1^* \\
&\vdots \\
v_k &= v_k^* - \sum_{j=1}^{k-1} \mu_{kj} v_j^* \\
&\vdots
\end{aligned}
$$

$j < k$



If $w \in \mathcal{L}$, $w \neq 0 \Rightarrow \|w\| \geq \min_j \|v_j^*\|$

$\|w\|_2 = \sqrt{\sum w_i^2}$

L achieves:

$\forall i \quad \|v_i^*\| \geq \frac{1}{\sqrt{2}} \|v_{i-1}^*\|$

$\Rightarrow v_1 = v_1^* \in \mathcal{L}, \quad \|v_1\| \leq 2^{\frac{n-1}{2}} \min_{\mathcal{L}}$

Operations

① elementary basis operation $v_j \leftarrow v_j - \alpha \cdot v_l \quad \alpha \in \mathbb{Z}$

② permute basis $v_i \leftrightarrow v_{i+1}$

goal: $\forall\ |\mu_{ij}| \le \frac{1}{2}$

Small Coeffs procedure

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

→ **for** $t = k-1$ **downto** 1

fix μ_{kt}

$a \in \mathbb{Z}$ $\quad |\mu_{kt} - a| \le \frac{1}{2}$

$v_k \leftarrow v_k - a \cdot v_t$

does not affect μ_{lj} with $l < k$

$\binom{n}{2}$ rounds **done**

does not affect the U_i the v_i^*

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

small coeffs

Swap v_{i-1}, v_i

Analysis

if procedure terminates $\Longrightarrow$ achieves goal

$(\forall i)\left(\|v_i^*\| \geq \frac{1}{\sqrt{2}}\|v_{i-1}^*\|\right)$

TERMINATION : potential function

$P = \text{vol}(v_1) \cdot \text{vol}(v_1, v_2) \cdot \ldots \cdot \text{vol}(v_1 \ldots v_n)$

Claim P does not change under small coeffs

goes down by $\leq \frac{1}{\sqrt{2}}$ factor in swap