

$$k\text{-CNF} \dots \psi = C_1 \wedge C_2 \wedge \dots \wedge C_m$$

$$\text{klauzule } C_i = x_{i,1} \vee \neg x_{i,2} \vee \dots \vee \neg x_{i,k}$$

každá klauzule obsahuje $\leq k$ literálů.

$k\text{-SAT} = \{\langle \psi \rangle; \psi \text{ je booleanská formule v } k\text{-CNF, která je splnitelná}\}$

Algoritmy pro $k\text{-SAT}$: $n \dots$ počet proměnných
 $m \dots$ počet klauzulí

- $2^n \cdot m^{O(1)} \dots$ triviální algoritmus
- $1.33^n \cdot m^{O(1)} \dots$ algoritmus pro 3-SAT
- $2^{(1-\frac{O(1)}{k})n} \cdot m^{O(1)} \dots$ algoritmus pro $k\text{-SAT}$

Otázka: \exists alg. pro $k\text{-SAT}$ pracující v čase $2^{o(n)}$?

Domněnky:

Exponential Time Hypothesis (ETH)

- $\exists \delta > 0 + \bar{e}$. žádný algoritmus pro 3-SAT nepracuje v čase lepší než $2^{(1-\delta)n}$

Strong Exponential Time Hypothesis (SETH)

- $\forall \varepsilon > 0 \exists k \geq 1 \text{ t.ž. } k\text{-SAT}$ nemá algoritmus pracující v čase $2^{(1-\varepsilon)n}$.

Fakt: $\text{SETH} \Rightarrow \text{ETH}$. (Důležitá netriviálnost)

Problém ortogonálních vektorů (OVP)

Dána množina vektorů $S \subseteq \{0,1\}^d$, $|S|=n$,

existuje $x, y \in S$ t.ž. $\langle x, y \rangle = 0$

$$\hookrightarrow \sum_{i=1}^d x_i \cdot y_i$$

Poznámka: OVP lze řešit v čase $O(n^2 \cdot \text{poly}(d))$.

Q: Lze OVP řešit v čase $O(n^{2-\varepsilon} \text{poly}(d))$ pro nějaké $\varepsilon > 0$?

Vol: Pokud platí SETH, pak OVP nelze řešit v čase $O(n^{2-\varepsilon} \text{poly}(d))$ pro žádné $\varepsilon > 0$.

Dle: $k\text{-SAT}$ zredukujeme na OVP tak, že $O(n^{2-\varepsilon} \text{poly}(d))$ alg pro OVP dá $2^{(1-\frac{\varepsilon}{k})n}$ alg pro $k\text{-SAT}$.

k -CNF $\psi = C_1 \wedge C_2 \wedge \dots \wedge C_m$

$d = m + 2$

pro jednoduchost
 n je sudé

pro každé ohodnocení proměnných $x_1, \dots, x_{\frac{n}{2}}$
 $a \in \{0, 1\}^{n/2}$

vytvořím vektor

$u_a = 1 \ 0 \ \underbrace{0/1 \ 0/1 \ \dots \ 0/1}_m$

$\hookrightarrow i$ -tý bit je 0 pokud
proměnná $x_1 \dots x_{\frac{n}{2}}$ při
ohodnocení a splňuje
klauzuli C_i
jinak je bit 1.

podobně $\forall b \in \{0, 1\}^{n/2}$ ohodnocení $x_{\frac{n}{2}+1} \dots x_n$

vytvořím vektor

$v_b = 0 \ 1 \ \underbrace{0/1 \ 0/1 \ \dots \ 0/1}_m$

$\hookrightarrow i$ -tý bit je 0 pokud
ohodnocení b pro $x_{\frac{n}{2}+1} \dots x_n$
splňuje C_i

$\Rightarrow (u_a, v_b) = 0 \iff a, b$ tvoří splňující

ohodnotit ψ .

$$\rightarrow S = \{u_a : a \in \{0,1\}^{n/2}\} \cup \{v_b : b \in \{0,1\}^{n/2}\}$$

$$|S| = 2^{n/2+1} = N$$

algoritmus $k \geq 1$ v \bar{c} case $O(N^{2-\epsilon} \text{poly}(n))$

pro DVP instance S , \bar{c} case k -SAT

$$\text{v } \bar{c} \text{ case } O\left(\left(2^{n/2}\right)^{2-\epsilon} \text{poly}(n)\right) =$$

$$= O\left(2^{n(1-\frac{\epsilon}{2})} \text{poly}(n)\right).$$

□