

Th de Cook

[Auton p 203] [Wolper p 185] et Sylvain Perifel, Complexité algorithmique ?

- Le problème SAT : Entrée = Une formule du calcul propositionnel φ
 Q^c : φ est-elle satisfiable ?

- Th : SAT est NP complet

démo $\rightarrow$ SAT $\in$ NP. En effet, $\exists$ 1 vérificateur en temps polynomial pour SAT

Étant donnée φ (dont la taille = nb de symboles pour écrire φ) et 1 valuation, v , il suffit pour savoir si v satisfait φ de construire puis évaluer l'arbre correspondant à φ des feuilles à la racine. Le vérificateur est donc linéaire.

$\rightarrow$ Reste à voir SAT est NP-difficile. On voit 1 pb de NP se réduit à SAT polynomial

Soit $L \in$ NP : ce langage est donc décidé par une MT $M = (Q, \Sigma, \Gamma, E, q_0, F, \#)$ non det en temps polynomial (car $\exists P \in \mathbb{R}[x], \forall w \in L$ de taille n , temps d'exécution de M sur $w \in P(n)$)

$\rightarrow$ justifie l'introduction de M' pour avoir 1 tableau auxiliaire car on ne sait pas quand arrive la dernière étape du calcul sur $w \in L$

Construisons la machine $M' = (Q, \Sigma, \Gamma, E, q_0, F, \#)$ qui coïncide avec M

jusqu'à son arrêt puis qui entre dans un état d'attente S si le mot

en entrée est accepté et dans un autre état d'attente sinon puis boucle dans ces états

(= une fois qu'on est accepté, on boucle dans l'état d'acceptation ; une fois qu'on est refusé

on boucle dans l'état de refus). De cette façon le calcul de M' sur w dure autant qu'on veut

Soit $w \in L$ et $n = |w|$. on a $w \in L \stackrel{(*)}{\Leftrightarrow} M$ accepte $w \Rightarrow M'$ est dans l'état S
"
 $w_1 \dots w_n$ $\uparrow$
à l'étape $P(n)+1$ puisque la durée d'1

calcul de M dure au plus $P(n)$

Construisons 1 formule φ_w , polynomiale en $|w|$, et tq φ_w satisfiable

$\Leftrightarrow M'$ est dans l'état S à l'étape $P(n)+1$

On représente une exécution valide de M' par un tableau dont chaque ligne est la représentation ggd ($g \in G, g, d \in \Gamma^*$) du subam. Comme on ne s'intéresse qu'aux exécutions en au plus $P(m)+1$ étape (et que $\text{cpté spatiale} \leq \text{cpté temporelle}$) on peut se regarder que les $P(m)+1$ cases du subam $\rightarrow$ on obtient donc 1 tableau $(P(m)+1) \times (P(m)+1)$ (numéroté à partir de 0)

On exprime alors φ_w comme 1 conjonction de contraintes sur ce tableau à l'aide des variables propositionnelles $p_{i,j,a}$ où $i,j \in [0, P(m)]$ et $a \in \Gamma \cup Q$ et qui symbolise

"la case (i,j) contient le symbole a " ET des raccourcis suivants :

$$(p_{i,j} = p_{k,l}) \equiv \bigvee_{a \in \Gamma \cup Q} (p_{i,j,a} \wedge p_{k,l,a}) ; \quad ((i,j) \in C_j) \equiv (p_{i,j} \in \Gamma \vee p_{i,j-1} \in \Gamma \vee p_{i,j+1} \in \Gamma) \text{ avec } p_{i,j} \in \Gamma \equiv \bigvee_{a \in \Gamma} p_{i,j,a}$$

et $((i,j) \notin C_j) \equiv \neg((i,j) \in C_j)$

$$\delta^{\leftarrow}(i,j) = \bigvee_{\substack{q_1, q_2 \in \Gamma \\ q \in Q}} (p_{i,j-1,q_1} \wedge p_{i,j,q} \wedge p_{i,j+1,q_2} \wedge p_{i+1,j-1,q} \wedge p_{i+1,j,q_1} \wedge p_{i+1,j+1,q_2}) \cdot \text{de m\u00eame } \delta^{\rightarrow}(i,j)$$

$\delta(q, \gamma_2) = (q', \gamma_3, \leftarrow)$

Alors : $C = \bigwedge_{i,j} \left(\bigvee_{a \in \Gamma \cup Q} p_{i,j,a} \right)$ = coh\u00e9rence = chaque case du tableau contient 1 et 1 seul symbole ; de taille $|\Gamma \cup Q| (P(m)+1)^2$

$$I = p_{0,0,q_0} \wedge \left(\bigwedge_{j=1}^m p_{0,j,w_j} \right) \wedge \left(\bigwedge_{j=m+1}^{P(m)} p_{0,j,\#} \right) = \text{initialisation} = \text{la config initiale est } q_0 w ; \text{ de taille } P(m)+1$$

$$S = \bigvee_j p_{P(m)+1,j,S} = \text{\u00e9tat stationnaire} = \text{\u00e0 la derni\u00e8re \u00e9tape on est ds } S ; \text{ taille } P(m)+1$$

$$\text{et } T = \bigwedge_{i=0}^{P(m)-1} \left(\bigwedge_{j=0}^{P(m)} \underbrace{((i,j) \notin C_j) \wedge (p_{i+1,j} = p_{i,j})}_{\text{on m' est pas ds la case cubique et on ne change rien}} \vee \underbrace{((i,j) \in C_j \wedge (\delta^{\rightarrow}(i,j) \vee \delta^{\leftarrow}(i,j)))}_{\text{on est ds la case cubique et y a 1 transition correcte}} \right)$$

o\u00f9 C_j est l'unique fen\u00eatre de 6 cases telle que

i	$*$	$q = \text{start}$	$*$
$i+1$	$*$	$*$	$*$

Cette fen\u00eatre existe toujours m\u00eame si y a des pbs d'indices qd l'\u00e9tat est tout devant.

on ne tient pas compte des pbs d'initialisation par manque de temps

T est de taille polynomiale en m car $\leq (P(m)+1)^2 \times (\text{cste} + \text{cste})$ car $|\Gamma|, |Q|$ et $|S|$ cotes

En prenant $\varphi_w = C \wedge I \wedge S \wedge T$, on a bien construit 1 formule de taille

polynomiale en $n = |w|$ qui est satisfiable $\Leftrightarrow M'$ stationnaire en $S \Leftrightarrow w \in L$

Donc SAT est NP-difficile