Théorème de Cook

Antoine Dequay

21 septembre 2022

Notes

— Prof : .

— Leçon : 913, 915, 916, 928.

— Références :

  — Barbenchon.

Théorème 1 Le problème SAT :
$\begin{cases} \underline{\text{entrée}} : \text{Une formule } \varphi \text{ en logique propositionnelle,} \\ \underline{\text{sortie}} : \text{Oui si } \varphi \text{ est satisfiable, non sinon.} \end{cases}$
est NP-complet.

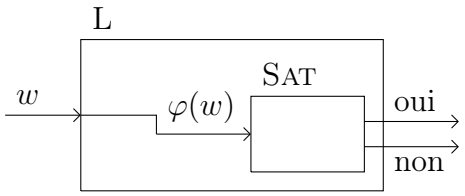
Preuve.

— SAT est dans NP :

La vérification à partir d'une valuation peut se faire en temps polynomial, par exemple par induction sur l'arbre représentant la formule, donc on a bien accès à un certificat polynomial, donc SAT est dans NP.

— SAT est NP-difficile :

Soit L un problème dans NP, on veut faire la réduction :



Soit $M = (Q, \Gamma, q_0, q_f, \delta)$ une machine de Turing non-déterministe qui décide L en temps polynomial. On suppose qu'elle a un unique état q_f et qu'elle boucle sur cet état final.

Soit $P \in \mathbb{R}[X]$ (P est à valeurs entières, on ne peut pas se ramener à $\mathbb{N}[X]$, mais à des combinaisons linéaires des $(\Pi(X-i))/k!$) tel que pour tout $w \in L$, $\#w = n$, M s'arrête en au plus $P(n)$ étapes.

On a donc :

$$w \in L \iff M \text{ s'arrête sur } w \iff M \text{ est dans } q_f \text{ à l'étape } P(n)+1.$$

On peut représenter les exécution de M sur un tableau de configurations de la forme gqd (le pointeur se trouve directement à droite de l'état q) : écrire une seule ligne pour gagner du temps

q_0	w_1	w_2	$\dots$	w_n	#	$\dots$	#
γ_1	q_1	w_2	$\dots$	w_n	#	$\dots$	#
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
γ'_1	$\dots$	γ'_l	q_f	γ'_{l+1}	$\dots$	$\dots$	$\gamma'_{P(n)+1}$

Par définition de P, le nombre de lignes est majoré par P, donc le nombre de colonnes aussi.

Pour pouvoir se ramener à SAT, il ne reste plus qu'à traduire l'ensemble des règles permettant la construction de ce tableau en proposition de la logique propositionnelle, et de vérifier que leur taille est bien polynomiale en n.

On cherche à construire une formule de la forme :

$$\varphi(w) = \underbrace{E}_{existence} \wedge \underbrace{U}_{unicite} \wedge \underbrace{I}_{initialisation} \wedge \underbrace{F}_{etat final} \wedge \underbrace{T}_{transition}.$$

On note $x_{i,j,a}$ les variables propositionnelles, qu'on associe au caractère $a \in A := \Gamma \cup Q$, en position $(i,j) \in [\![0, P(n)]\!]^2$ du tableau. On doit alors avoir :

- $E = \bigwedge_{i,j} \left(\bigvee_{a} x_{i,j,a} \right)$, de taille $O(P(n)^2 \# A)$,
- $U = \bigwedge_{i,j} \left(\bigwedge_{a \neq a'} \neg(x_{i,j,a} \wedge x_{i,j,a'}) \right)$, de taille $O(P(n)^2 \# A^2)$,
- $I = x_{0,0,q_0} \wedge \bigwedge_{j=1}^{n} x_{0,j,w_j} \wedge \bigwedge_{j=n+1}^{P(n)} x_{0,j,\#}$, de taille $O(P(n))$,
- $F = \bigvee_{j=0}^{P(n)} x_{P(n),j,q_f}$, de taille $O(P(n))$,
- T : On examine les différentes situations (les cas aux limites du tableau se traitent de même). A (i,j) fixé, on a les possibilités suivantes :
  -

	$j-1$	j	$j+1$
i	γ_1	γ_2	γ_3
$i+1$	γ_1'	γ_2	γ_3'

    Dans ce cas, on traduit seulement l'égalité du milieu,
  - Si $(q', \gamma_3, \leftarrow) \in \delta(q, \gamma_2)$:

	$j-1$	j	$j+1$
i	γ_1	q	γ_2
$i+1$	q'	γ_1	γ_3

  - Si $(q', \gamma_3, \rightarrow) \in \delta(q, \gamma_2)$:

	$j-1$	j	$j+1$
i	γ_1	q	γ_2
$i+1$	γ_1	γ_3	q'

    Il n'y a pas d'autres cas à considérer (q sur les cotés), car ils sont pris en compte dans ceux ci-dessus !

    Pour traduire ces différentes configurations, il reste à traduire (et on peut le faire polynomialement en n (A, Γ et Q ayant une taille fixée dépendant de L mais pas de n)) :

    - $x_{i,j,\in Q}$,
    - $[x_{i,j} = x_{k,l}]$,

— $\delta^{\leftarrow}(i,j)$, $\delta^{\rightarrow}(i,j)$.

On peut alors écrire (avec des conventions pour les bords...)

$$T = \bigwedge_{i=0}^{P(n)-1} \bigwedge_{j=0}^{P(n)} (((\neg x_{i,j-1,\in Q} \wedge \neg x_{i,j,\in Q} \wedge \neg x_{i,j+1,\in Q}) \rightarrow [x_{i,j} = x_{i+1,j}]) \wedge (x_{i,j,\in Q} \rightarrow (\delta^{\rightarrow}(i,j) \vee \delta^{\leftarrow}(i,j))))$$

La taille des formules est donc en $O(P(n)^2)$ (fois des constantes dépendant de L, mais pas de n).

Il reste à montrer que $\varphi(w)$ est satisfiable si et seulement si $w \in$L.

Pour le sens direct, il suffit de placer dans le tableau en position (i,j) l'unique $a \in A$ tel que $x_{i,j,a}$ soit vrai. Cela montre que w est bien accepté par L.

Pour le sens réciproque, il suffit de définir la valuation associée au tableau de configuration de M acceptant w.

□