Développement : Théorème de Cook

Pierron Théo – Lacoste Cyril

7 octobre 2013

Références : Carton p.189, Wolper p.185

Théorème 1 *Le problème SAT est NP-complet.*

Démonstration.

– SAT est NP : Un algorithme non déterministe polynomial qui résout ce problème est le suivant :
  • On génère de façon non déterministe une valuation.
  • On vérifie que cette valuation satisfait la formule.

– SAT est NP-difficile : On fait une réduction polynomiale de n'importe quel problème NP à SAT. Soit A un problème NP décidé par une machine M non déterministe en temps polynomial.
  On va montrer que pour toute entrée w de M il existe une formule ϕ_w de taille polynomiale en $|w|$ telle que ϕ_w est satisfiable si et seulement si w est acceptée par M. On note $n = |w|$ et on suppose que M décide A en temps n^k pour un certain entier k.
  On suppose que tout calcul acceptant w est de longueur exactement n^k (on peut ajouter quelques états et transitions pour prolonger les calculs). La machine M fonctionnant en temps n^k, elle utilise au plus n^k cellules. Les configurations sont de longueur au plus n^k, on les suppose de longueur exactement n^k quitte à ajouter des symboles #.
  On écrit ces configurations les unes sous les autres pour obtenir un tableau similaire au tableau ci-dessous de symboles de $\Gamma = \Sigma \cup Q$ (Σ étant le langage du ruban de M et Q l'ensemble des états) :

Conf	0	1	2	3	…	n^k
$C_0 =$	q_0	w_1	w_2	w_3	…	#
$C_1 =$	w'_1	q_1	w_2	w_3	…	#
$C_2 =$	w'_1	w'_2	q_2	w_3	…	#
$C_3 =$	…	…	…	…	…	#
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$C_{n^k} =$	…	…	…	…	…	…

  On cherche ϕ_w qui code l'existence d'un tel tableau formé par les configurations successives d'un calcul acceptant w. Pour chaque paire (i, j) avec $0 \leqslant i, j \leqslant n^k$ et pour chaque symbole $a \in \Gamma$, on introduit $x_{i,j,a}$ une variable qui code le fait que la case (i, j) contienne ou non le symbole a.
  Le nombre de ces variables est $|\Gamma|.n^{2k+2}$ qui est polynomial en n. La formule ϕ_w est écrite en utilisant les variables $x_{i,j,a}$. Cette formule se décompose en une conjonction $\phi_0 \wedge \phi_1 \wedge \phi_2 \wedge \phi_3 \wedge \phi_4$ où :
  • ϕ_0 code le fait que chaque cellule contient un unique symbole de Γ :

$$\phi_0 = \bigwedge_{0 \leqslant i,j \leqslant n^k} \left[\left(\bigvee_{a \in \Gamma} x_{i,j,a} \right) \wedge \left(\bigwedge_{a,a' \in \Gamma, a \neq a'} \neg(x_{i,j,a} \wedge x_{i,j,a'}) \right) \right]$$

- ϕ_1 code le fait que la première ligne du tableau est $q_0 w$:

$$\phi_1 = x_{0,0,q_0} \wedge x_{0,1,w_1} \wedge \cdots \wedge x_{0,n,w_n} \wedge x_{0,n+1,\#} \wedge \cdots \wedge x_{0,n^k,\#}$$

- ϕ_2 code le fait qu'il y a un et un seul symbole de Q par ligne :

$$\phi_2 = \bigwedge_{1 \leqslant i \leqslant n^k} \left[\left(\bigvee_{q \in Q, 0 \leqslant j \leqslant n^k} x_{i,j,q} \right) \wedge \left(\bigwedge_{q,q' \in Q, j \neq j'} \neg (x_{i,j,q} \wedge x_{i,j',q'}) \right) \right]$$

- ϕ_3 code le fait qu'au moins une des cases de la dernière ligne contient un état final :

$$\phi_3 = \bigvee_{q \in F, 0 \leqslant j \leqslant n^k} x_{n^k,j,q}$$

- ϕ_4 code le fait que chaque ligne est obtenue en appliquant une transition de M. On remarque que le contenu d'une case (i, j) dépend uniquement des trois cases au-dessus $(i-1, j-1)$, $(i-1, j)$ et $(i-1, j+1)$ et de la transition effectuée par M pour passer de C_{i-1} à C_i.
  Si les trois symboles contenues dans ces trois cases sont dans Σ alors le symbole de (i, j) est identique à celui de $(i-1, j)$.
  Si l'état de C_{i-1} se trouve dans $(i-1, j)$ alors l'état de C_i se trouve dans $(i, j-1)$ ou $(i, j+1)$ suivant que la tête de lecture ait été déplacée vers la gauche ou vers la droite.
  Il est donc possible de vérifier que la ligne i est obtenue à partir de la ligne $i-1$ uniquement en regardant les contenus des fenêtres de taille 2×3, le nombre de contenus possibles ne dépendant que de l'alphabet et des transitions de la machine (et est donc indépendant de n). Le fait que toutes les parties de six cases du tableau correspondent à un des contenus possibles des fenêtres s'exprime par la conjonction pour chaque case d'une disjonction sur les différents contenus. C'est donc une formule de taille polynomiale en n. ■