Théorème de Cook

Réf : Carton : LFCC / Wolper : Introduction à la calculabilité

Th : SAT est NP-complet

Démo : SAT ∈ NP de manière assez évidente : il suffit d'évaluer la formule.

- Soit $L \in NP$ et M une machine de Turing non-det qui reconnait L. On a $\omega \in L$ ssi $M(\omega) = 1$, ie s'il existe un chemin acceptant de longueur au plus $p(n)$ qui mène à un état accepteur. Pour simplifier, on supposera que tous les chemins acceptant pour ω tq $|\omega| = n$ sont de taille $p(n)$.

- Un calcul acceptant de M sur ω peut être représenté par la suite des configurations de la machine :
  * Un tableau de taille $(p(n) \times p(n))$ donnant pour chaque configuration et chaque case le contenu du ruban dans cette case. Nous représenterons l'élément (t,i) par Ruban$[t,i]$
  * Un vecteur de taille $p(n)$ donnant l'état pour chaque configuration. Nous représenterons l'élément t de ce vecteur par Etat$[t]$
  * Un vecteur de taille $p(n)$ donnant la position de la tête de lecture, nous représenterons l'élément t par Pos$[t]$
  * Un vecteur de taille $p(n)$ donnant le choix effectué par M, où on supposera que M fait le choix entre deux transitions δ_0 et δ_1. Nous noterons l'élément t par Choix$[t]$.

- On choisit un ensemble de variables propositionnelles pour décrire ce tableau :
  * Une proposition $R_{t,i,\alpha}$ pour $\alpha \in \Sigma$
  * ——— $E_{t,q}$ pour $q \in Q$
  * ——— $P_{t,i}$
  * ——— $C_{t,\delta}$ pour $\delta \in \{0,1\}$

- On considère qu'une fonction d'interprétation définit un contenu des tableaux avec la convention $R_{t,j,\alpha} \leftarrow 1$ signifie que le symbole α se trouve dans la case Ruban$[t, j]$. Toutefois, cette convention n'a de sens que s'il existe un seul $\alpha \in \Sigma$ tq $R_{t,j,\alpha} \leftarrow 1, \ldots$

  On créer donc la formule φ_0 qui pose ces contraintes :

  par exemple pour les $R_{t,j,\alpha}$: $\varphi_{0,R} \equiv \bigwedge_{\substack{0 \leq t \leq p(n) \\ 0 \leq i \leq p(n)}} \left[\left(\bigvee_{\alpha \in \Sigma} R_{t,j,\alpha} \right) \wedge \bigwedge_{\alpha \neq \alpha' \in \Sigma} \overbrace{\left(\neg R_{t,j,\alpha} \vee \neg R_{t,j,\alpha'} \right)}^{\neg (R_{t,j,\alpha} \wedge R_{t,j,\alpha'})} \right]$

  La taille de $\varphi_{0,R}$ et $\varphi_{0,P}$ est $O(p(n)^3)$, celle de $\varphi_{0,E}$ et $\varphi_{0,C}$ est $O(p(n)^2)$

  Ainsi φ_0 est de taille $O(p(n)^3)$

- Il faut ensuite vérifier que la configuration initiale est la bonne :

  $\varphi_1 \equiv \left[\bigwedge_{j=0}^{n-1} R_{0,j,w_j} \wedge \bigwedge_{j=n}^{p(n)} R_{0,j,B} \right] \wedge E_{0,q_0} \wedge P_{0,0}$ taille $O(p(n))$

- Il faut maintenant vérifier qu'une ligne est conséquence de la précédente : $\varphi_{2,i}$

  * Si la tête de lecture n'est pas sur une case, elle ne change pas : $\bigwedge_{\substack{0 \leq t \leq p(n) \\ 0 \leq i \leq p(n) \\ \alpha \in \Sigma}} \left[(R_{t,i,\alpha} \wedge \neg P_{t,i}) \Rightarrow R_{t+1,i,\alpha} \right]$

  se réécrit en CNF en $(\neg R_{t,i,\alpha} \vee P_{t,j} \vee R_{t+1,j,\alpha})$

  * Si la tête de lecture est sur la case, on change suivant la transition

  $$\bigwedge_{\substack{0 \leq t \leq p(n) \\ 0 \leq j \leq p(n) \\ q \in Q \\ \alpha \in \Sigma \\ r \in \{0,1\}}} \left[\left(P_{t,j} \wedge R_{t,j,\alpha} \wedge C_{t,r} \wedge E_{t,q} \right) \Rightarrow \left(E_{t+1,q'} \wedge R_{t+1,j,\alpha'} \wedge P_{t+1,j+d} \right) \right]$$

  si $\delta(q, \alpha, r) = (q', \alpha', d)$

- Il ne nous reste plus qu'à vérifier que ~~la configuration finale est acceptante~~ : une configuration acceptante est atteinte durant l'exécution : $\varphi_3 = \bigvee_{\substack{t=0 \\ q \in F}}^{p(n)} \left[E_{t,q} \right]$.

- Finalement, on pose $\varphi_w = \varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$ et on a M accepte w si φ_w est satisfiable. De plus, la longueur de φ_w est $O(p(n)^3)$, donc est polynomiale en n. D'où SAT est NP-dur

$\square$