Théorème de Cook-Levin

Benjamin Hellouin

Rey, "Cook-Levin"

Théorème 1 (Théorème de Cook-Levin)**.**

***SAT** est **NP**-complet.*

Idée : Soit L un problème de décision de **NP**. Il existe une machine de Turing non déterministe $M = (\Sigma, B, Q, q_0, F, \Delta)$ qui calcule la réponse de L à toute entrée de taille n en temps $T = P(n)$, où P est un polynôme. Sans perte de généralité, on suppose que M ne possède qu'un ruban de lecture.

L'idée est la suivante : sur une entrée de taille n, la machine passera par un nombre de configurations $\leq P(n)$, chacune occupant un espace $\leq P(n)$). On peut encoder une configuration en un nombre polynômial de variables, et contraindre le "bon fonctionnement" de la machine avec un nombre polynômial de formules de sorte qu'un calcul valable de la machine acceptant l'entrée corresponde à une assignation satisfaisant ces formules, ainsi qu'une dernière formule testant si l'entrée est acceptée.

Soit $w = a_{i_0} a_{i_1} \ldots$ une instance de L, on la transforme en instance de **SAT** de taille polynômiale en $|w|$. L'ensemble Var des variables est :
- $P_{s,t,i}$ représente le fait que la cellule s contient le symbole a_i à l'étape t.
- $Q_{n,t}$ représente le fait que la machine est dans l'état q_n à l'étape t.
- $R_{s,t}$ représente le fait que la tête de lecture est sur la cellule s à l'étape t.

Sous quelles conditions ces variables représentent-elles une configuration valable pour un temps t fixé ? On a les conditions :
- un et un seul état :

$$Etat(t) = \bigvee_{1 \leq n \leq |Q|} Q_{n,t} \wedge \bigvee_{1 \leq n < m \leq |\Sigma|} \overline{Q}_{t,n} \vee \overline{Q}_{t,m}.$$

- un et un seul symbole par case :

$$Symbole(t) = \bigwedge_{-T \leq s \leq T} \left(\bigvee_{1 \leq i \leq |\Sigma|} P_{s,t,i} \wedge \bigvee_{1 \leq i < j \leq |\Sigma|} \overline{P}_{s,t,i} \vee \overline{P}_{s,t,j} \right).$$

- une et une seule position de tête de lecture :

$$Lecture(t) = \bigvee_{-T \leq s \leq T} R_{s,t} \wedge \bigvee_{-T \leq s < r \leq T} \overline{R}_{s,t} \vee \overline{R}_{s,t}$$

Représentons maintenant une étape de calcul. Supposons que $(q_n, a_i, a_j, dir, q_m) \in \Delta$. Pour que les variables représentent un calcul valide, elles doivent vérifier :

$$Trans(t, q_n, a_i, a_j, dir, q_m) = \bigvee_{-T \leq s \leq T} (Q_{n,t} \wedge R_{s,t} \wedge P_{s,t,i}) \Rightarrow (P_{s,t+1,j} \wedge Q_{m,t+1} \wedge R_{s+dir,t+1})$$

$$Calcul(t) = \bigvee_{(q_n,a_i,a_j,dir,q_m) \in \Delta} Trans(t, q_n, a_i, a_j, dir, q_m)$$

de taille totale $O(T|\Delta|)$. On définit maintenant l'état initial (on suppose $a_0 = \text{blanc}$) :

$$Initial = Q_{0,0} \wedge R_{0,0} \wedge \bigwedge_{0 \leq s < |w|} P_{s,0,i_s} \wedge \bigwedge_{\substack{-T \leq s < 0 \\ |w| \leq s \leq T}} P_{s,B,0}$$

Proposition 1. *Une valuation de Var représente des configurations valides jusqu'à $t = t_0$ si $\bigvee_{0 \leq t < t_0} Etat(t) \wedge Symbole(t) \wedge Lecture(t)$ est satisfaite. Elle correspond à un calcul valable si elle satisfait $\bigvee_{0 \leq t < t_0} Calcul(t)$. On note l'ensemble de ces clauses $Valide(t_0)$.*

Proposition 2. *La machine de Turing M accepte l'entrée w si et seulement si il existe une valuation de Var satisfaisant*

$$Initial \wedge \bigvee_{0 \leq t \leq T} Valide(t) \wedge \overline{P}_{s,t,0}$$

Le sens indirect définit trivialement un calcul licite sur l'entrée w qui l'accepte, et donc $w \in L$. Le sens direct s'obtient en assignant les valeurs correspondant au calcul effectué par M pour $t \leq t_0$, et des valeurs arbitraires au-delà.