Complexité - Nicolas Ollinger

Alexandre Masson

15 Janvier 2013

Table des matières

1 non-déterminisme

$P = \cup_{k>0} DTIME(n^k)$ la classe des problèmes qu'on peut résoudre en temps polynomial.
$NP = \cup_{k>0} NTIME(n^k)$ la classe des problèmes vérifiables en temps polynomial

Rétrospective DFA : automate déterminisme , NFA non déterminisme.
ex : $(a+b)^*baba$ mot finissant par baba. Tout NFA non déterminisme, se code en DFA, mais au prix d'une complexité plus importante en nombre d'état.

Définition une MTND (MT non déterministe), est une MT avec comme table de transition :

$$T \subseteq (Qx\Gamma^k)^{input} x (Qx\Gamma^k x\{<-, v, ->\})^{output}$$

on redéfinie la relation de transition :

$c \vdash c'$ si T contient une transition applicable sur c qui produit c'

Une exécution d'une MTND partant d'une entrée u est une suite de transition valides de la configuration initiale associée à u à une configuration d'arrêt.

$$c_0 \vdash c_1 \vdash ... \vdash c_n$$

Une MTND M accepte un mot $u \in \Sigma^*$ s'il existe une exécution acceptée pour u.

	MT	MTND
Rejet	l'exécution doit s'arrêter sur q_{non}	toutes les exécutions doivent s'arrêter sur q_{non}
Acceptation	l'exécution s'arrête sur q_{oui}	un seul état à oui renvoie oui

remarque A un ralentissement linéaire près, on peut supposer que les choix non déterministes sont au plus binaires : pour tout configuration c :
- ou bien c n'as pas d'image (arrêt)
- ou bien $c \vdash c'$ unique.
- ou bien $c \vdash c' \& c \vdash c''$

exemple le 3-color, entrée : un graphe G=(V,E), sortie : G est il 3-colorable 3Color est reconnu par une MTND dont les exécutions s'arrêtent en temps polynomial en la taille de l'instance.
la machine fonctionne en deux temps.
- Choix non déterministe d'une couleur par sommet (O(|v|)
- Vérification déterministe que le coloriage choisit est valide : si oui accepte, sinon rejette.

Définition NTIME(f(n)) est la classe des langages reconnus par une MTND dont toutes les exécutions sont de longueur $\leq$ f(n) sur les entrées de taille n.

proposition Si $f(n) \leq g(n)$ alors $NTIME(f(n)) \subseteq NTIME(g(n))$
$DTIME(f(n)) \subseteq NTIME(f(n))$
$NTIME(f(n)) \subseteq DTIME(2^{O(f(n))})$
Idée : Il suffit de simuler les choix de la MTND par du backtracking

def $NP = \cup_{k>0} NTIME(n^k)$
$NEXP = \cup_{k>0} NTIME(2^{n^k})$
Question : Est ce que P NP, **rq :** $P \subseteq NP$
prop NP ets clos par union et intersection.
def $co\Im = \{!L | L \in \Im\}$ ou $\Im$ et une classe de langages.

Un problème B est un **certificateur** pour un problème A si $\forall x \in \Sigma^*, x \in A <=> \exists y \in \Sigma^* < x, y > \in B$ on dit que y est un certificat pour x.

thm Np la classe des langages qui possèdent un certificateur dans P avec certificats de longueur polynomiale en la longueur de l'instance.
ex 3Color $\in$ NP , cf exemple antérieur. certificateur pour 3COLOR.
sur l'entrée <G,C> avec colorisation des sommets vérifier que les arêtes ont des couleurs distinctes à chaque extrémité. Ce certificat est dans P(car il ne fais que parcourir les arêtes pour vérifier une propriété). la taille du certificat est polynomiale.

Démonstration

i (dans ce sens, on connait A de P , et B le certificateur, on essaie de construire un chemin qui accepte x dnas la machine M, ce chemin s'appelle y , si l'on suis le chemin y pour arrive en qoui ave x en entrée, alros y est certificat et le certif existe , donc B est certificateur.)
Soit A un langage qui possède un certificateur B $\in$ P avec certificat de longueur $\leq$ p(n) sur les instances de longueur n ou p est polynomiale en n.
montrons que A ets dans NP en construisant une MTND M qui reconnait A comme suit :

- choisir grace au non déterminisme un mot y de longueur $\leq$ p(|x|)
- exécuter une MT qui reconnait B sur l'entrée <x,y>
- accepter si (2) accepte

M s'exécute bien en temps polynomial en |x| et M accepte x ssi $\exists y : |y| \leq p(n)$ et <x,y> $\in$ B, si x$\in$ A.

ii (dans ce sens, on sais que le Y sera un certificat, puisqu'on chosiit un chemin acceptant de x dans l'exécution de M, donc si B repond ok , vu que le Y ets ok , cela veux dir que B est bon)
Soit $A \in NP$ On va construire un certificat $B \in P$ pour A avec certificats polynomiaux.
Soit M un MTND qui reconnais A.
On utilise les exécutions acceptantes de M comme certificats et B se content de

vérifier l'exécution. Sur l'entrée <x,y>B vérifie que Y est une exécution acceptable pour M sur l'entrée x. B est bien un certificateur dans P avec certificat polynomiaux pour A.
Np est la classe des problèmes vérifiables en temps polynomial.

3Color : E : graphe G, S : est il 3Colorable, certif : coloration, Verif : pas d'arete monochrome.

Hamilton : E/S idem : certif : une permutation des sommets, i.e le cycle, verif : les aretes existent bien.

CLIQUE(sous graphe complet du graphe) Entrée : un graphe et un entier k : certif : la clique, verfi : les aretes existe =elles

tata