TD11 - Problèmes P-complets, P-SEL

Exercice 1. *P-complétude*

Le problème de la valeur d'un circuit est le suivant : étant donné un circuit C à n entrées et un mot $a \in \{0,1\}^n$, est-ce que $C(a) = 1$?

✎ Montrer que Circuit Value est P-complet

Problèmes avec fonction de sélection polynomiale

Définition : un problème X est dans $P-sel$ (pour P sélectif) s'il existe une fonction de $\{0;1\}^* \times \{0;1\}^*$ dans $\{0;1\}^*$ calculable en temps polynomial telle que pour tout $(x,y) \in \{0;1\}^* \times \{0;1\}^*$ on ait $f(x,y) \in \{x,y\}$ et $\{x,y\} \cap X \neq \emptyset \Rightarrow f(x,y) \in X$. On dit alors que f est une fonction de sélection pour X.

Exercice 2.

✎ Montrer que $P \subseteq P - sel$.

Exercice 3.

1. Soit r un réel. Soit X l'ensemble des uples $b_1...b_n$ d'éléments de $\{0;1\}$ tels que n soit un entier et $0, b_1...b_n \leq r$. Montrer que X est $P - sel$.

2. Montrer qu'il existe un problème $P - sel$ mais non récursif.

Exercice 4.

Soit $(M_1, p_1), (M_2, p_2), \dots$ une énumération récursive de tous les couples (M, p) tels que $p(X)$ soit un polynôme (de la forme X^k) et M une machine de Turing qui pour tout entier n et toute entrée de taille n effectue au plus $p(n)$ pas de calcul. Soit (w_i) une suite d'entiers définie par : $w_0 = 2$ et pour tout n entier naturel $w_{2n+1} = 1 + w_{2n}$ et $w_{2n+2} = 2^{2^{2^{w_{2n}}}}$. Définissons le langage L de la manière suivante. Pour tous les entiers i et m, si $M_i(w_{2<i,m>}, w_{2<i,m>+1}) = w_{2<i,m>}$ alors $w_{2<i,m>+1} \in L$, si $M_i(w_{2<i,m>}, w_{2<i,m>+1}) = w_{2<i,m>+1}$ alors $w_{2<i,m>} \in L$, et L ne contient rien d'autre. Remarque : $< i, m >$ est le code habituel du couple (i, m) (dont on pourra préciser les bonnes propriétés). On peut supposer que l'alphabet d'entrée des machines considérées contient 0, 1 et la virgule.

1. Montrer que L est récursif sans être dans $P - sel$.

Exercice 5.

1. Montrer que si X est $P - sel$ alors son complémentaire l'est aussi.

Exercice 6.

Nous allons montrer que $P - sel \subseteq P/poly$.

On donne les définitions suivantes : Soit $\mathcal{C}$ une classe de complexité et $\mathcal{F}$ un ensemble de fonctions de $\mathbf{N}$ dans $\mathbf{N}$. La classe $\mathcal{C}/\mathcal{F}$ est l'ensemble des problèmes X tels qu'il existe un problème Y dans $\mathcal{C}$, une fonction f dans $\mathcal{F}$, une suite (a_n) de uples de booléens telle que pour tout entier n le uple a_n (appelé conseil pour les mots de longueur n) soit de longueur au plus $f(n)$, et vérifiant : pour tout n-uple x de booléens, $x \in X$ si et seulement si $(a_n, x) \in Y$. Soit lin l'ensemble des fonctions linéaires de $\mathbf{N}$ dans $\mathbf{N}$, $quad$ l'ensemble des polynômes de degré au plus deux de $\mathbf{N}$ dans $\mathbf{N}$ et $poly$ l'ensemble des polynômes de $\mathbf{N}$ dans $\mathbf{N}$.

1. Définition : Un tournoi est un graphe complet fini dont on oriente les arêtes (de manière quelconque). Imaginez par exemple un ensemble de n joueurs et tous les matches où deux joueurs s'affrontent. Les sommets du tournoi sont alors les joueurs et chaque arête pointe vers le gagnant du match (on n'admet pas de match nul).

Lemme : Si G est un tournoi dont l'ensemble des sommets est $V_G = \{1; 2; \ldots; k\}$ et l'ensemble des arêtes est E_G alors il existe un sous-ensemble H des sommets de cardinal au plus $\lfloor \log(k+1) \rfloor$ tel que pour tout $v \in V_G - H$ il existe $g \in H$ tel que $(v, g) \in E_G$. (le log est en base 2)

Prouver le lemme, par exemple par récurrence.

2. Soit X dans $P - sel$. Montrer qu'il existe une fonction de sélection f pour X telle que pour tout x et y, $f(x, y) = f(y, x)$.

Soit X dans $P - sel$ et soit une fonction de sélection f pour X telle que pour tout x et y, $f(x, y) = f(y, x)$. Considérons l'ensemble $X^{=n}$ des mots de X de longueur n.

3. Montrer qu'il existe un sous-ensemble H_n de $X^{=n}$ de cardinal au plus $n + 1$ tel que pour tout mot v de longueur n, v appartient à $X^{=n}$ si et seulement s'il existe un mot g de H_n tel que $f(v, g) = v$.

4. Conclure.

5. Montrer que $P - sel \subseteq P/quad$.

Exercice 7.

Nous allons montrer que $P - sel \subseteq NP/lin$.

1. Lemme : Si G est un tournoi alors il existe un sommet s tel que tout sommet soit accessible à partir de s par un chemin orienté de longueur au plus deux.

Montrer ce lemme (par exemple par récurrence).

2. Montrer que $P - sel \subseteq NP/lin$. Si X est dans $P - sel$ et f est une fonction de sélection bien choisie pour X, on pourra considérer pour tout entier n le tournoi dont l'ensemble des sommets est $X^{=n}$ et les arêtes les (x, y) tels que $f(x, y) = y$.

3. Montrer que $P - sel \subseteq NP/lin \cap coNP/lin$

4. Montrer que $P - sel \subseteq NP/n + 1$ ($NP/n + 1 = NP/\{f : n \mapsto n + 1\}$).

Exercice 8.

Nous allons montrer que $P - sel \not\subseteq NP/n$ ($NP/n = NP/\{f : n \mapsto n\}$).

Soit $l_0 = 2$ et pour tout entier i strictement positif $l_i = 2^{2^{2^{l_{i-1}}}}$. Soit E l'ensemble des l_i. L'ensemble des mots booléens est muni de l'ordre lexicographique et on utilisera les notations habituelles $\leq$, $\min$, ... Si X est un ensemble de mots booléens considérons les conditions suivantes :
(1) Pour tout mot x de X la longueur de x est dans E.
(2) Pour tous x et y de même longueur, $x \leq y$ et $y \in X$ implique $x \in X$.
(3) $X \in DTIME[2^{2^n}]$

1. Montrer que si X satisfait les conditions (1), (2) et (3) alors X est $P - sel$. Pour cela on peut considérer la fonction suivante :

$$f(x,y) = \begin{cases} x & si|y| \notin E \\ y & si|y| \in E \wedge |x| \notin E \\ \min\{x,y\} & si|y| \in E \wedge |x| \in E \wedge |x| = |y| \\ \min\{x,y\} & si|y| \in E \wedge |x| \in E \wedge |x| \neq |y| \wedge \min\{x,y\} \in X \\ \max\{x,y\} & si|y| \in E \wedge |x| \in E \wedge |x| \neq |y| \wedge \min\{x,y\} \notin X \end{cases}$$

2. Soit $N_1, N_2 \dots$ une énumération (que l'on choisira bien) des machines de Turing non déterministes travaillant en temps polynomial, et soit $N'_1, N'_2 \dots$ l'énumération telle que pour tout k on ait $N'_{<i,k>} = N_i$. On définit le problème X de la manière suivante. Pour chaque entier l voici la définition de $X^{=l}$. Si $l \notin E$ alors $X^{=l} = \emptyset$. Sinon on effectue le calcul suivant, et si celui-ci nécessite plus de 2^{2^l} pas de calcul alors on arrête le calcul et on pose $X^{=l} = \emptyset$. Soient i et k tels que l soit le $< i,k >$-ème élément de E. Pour chaque mot y de longueur l calculer le mot $plusadroite(y)$ de la manière suivante. Pour chaque mot x de longueur l calculer $N'_{<i,k>}(< x,y >)$. Si aucun de ces calculs n'accepte alors $plusadroite(y) = 1^{l-1}$. Sinon $plusadroite(y)$ est le plus grand x de longueur l tel que $N'_{<i,k>}(< x,y >)$ accepte. Soit $J_l = (\{0;1\}^l \cup \{1^{l-1}\}) - \{plusadroite(y) | y \in \{0;1\}^l\}$, $j_l = \min(J_l)$ et $X^{=l} = \{x / |x| = l \wedge x \leq j_l\}$.

Montrer que J_l n'est pas vide ($l \in E$). Montrer que X ainsi défini est $P - sel$.

3. Supposons que X soit NP/n grâce à la machine N_I et à la suite de mots (a_j). Montrer qu'il existe $L \in E$ tel que le calcul de $X^{=L}$ (cf ce qui précède) nécessite moins de 2^{2^L} pas de calcul et donc se termine sans être interrompu. Montrer qu'alors aucun mot a_L ne convient. Conclure

4. Soit h une fonction récursive quelconque. Montrer que $P - sel \not\subseteq DTIME[h(n)]/n$