Partiel de Complexité algébrique - 7 novembre 2008

Exercice 1. *Oracles*

Soient A, C_1 et C_2 trois classes de complexité.

1. Est-ce que $C_1 = C_2 \Rightarrow A^{C_1} = A^{C_2}$? Justifiez votre réponse.

2. Est-ce que $C_1 = C_2 \Rightarrow C_1^A = C_2^A$? (Une preuve exacte n'est pas demandée)

Exercice 2. *Espace, Temps*

On considère des machines de Turing avec un ruban d'entrée en lecture seule, plus un ou plusieurs rubans de travail. Une fonction $f : \mathbb{N} \to \mathbb{N}$ est dite constructible en temps (respectivement en espace) s'il existe k et une machine à k rubans de travail qui, sur toute entrée de taille n, s'arrête en temps exactement $f(n)$ (resp. utilise exactement un espace $f(n)$ sur ses rubans de travail).

Pour la constructibilité en espace, on ne compte pas la lecture d'une case blanche en fin de mot si on n'écrit rien dessus.

1. Montrer que la fonction $f(n) = \lfloor \log_2 n \rfloor + 1$ est constructible en *espace*.

2. Montrer que la fonction $f(n) = \lfloor \sqrt{n} \rfloor + 1$ est constructible en *espace*.

3. Montrer que si les fonctions f et g sont constructibles en *temps*, alors il en est de même de leur composition $f \circ g$.

4. Quelles sont les fonctions f constructibles en *temps* telles qu'il existe un entier m vérifiant $f(m) < m$?

Exercice 3. *Réductions*

Soient A et B deux langages. On dit que A se réduit à B par réduction Turing, et on note $A \leq_T B$, s'il existe une machine de Turing à oracle M fonctionnant en temps polyomial telle que A soit le langage reconnu par la machine M munie de l'oracle B (en symboles, $A \in \mathbf{P}^B$).

1. On suppose que A se réduit à B par réduction polynomiale en temps (la réduction habituelle). Montrer que A se réduit à B par réduction Turing.

2. La réciproque est-elle vraie (Warning : cette question étant dure, ne vous sentez pas obligés de donner une preuve...) ?

Exercice 4. *Formules*

✎ Soit f une fonction de $\{0,1\}^l$ dans $\{0,1\}$. Montrer que f peut s'écrire comme une formule sous forme normale conjonctive de taille $l.2^l$.

Exercice 5. *Hiérarchie*

On rappelle l'existence d'une machine universelle U capable de simuler une machine M sur une entrée x de taille n en temps $O(n \log n)$. Pour toute fonction $f : \mathbb{N} \to \mathbb{N}$, la classe $\mathbf{DTIME}(f(n))$ est l'ensemble des langages décidés par une machine de Turing déterministe fonctionnant en temps au plus $c.f(n)$ pour une certaine constante c.

✎ Montrer que pour toute paire de fonctions f et g constructibles en temps vérifiant : $f(n) \log f(n) = o(g(n))$, on a

$$\mathbf{DTIME}(f(n)) \subsetneq \mathbf{DTIME}(g(n))$$

Exercice 6. *Machines de Turing*

Une fonction $f : \{0,1\}^* \to \{0,1\}^*$ est *implicitement calculable en espace logarithmique* si f est bornée polynomialement (il existe c t.q. $|f(x)| \leq |x|^c$ pour tout $x \in \{0,1\}^*$), et les langages $L_f = \{< x, i > | f(x)_i = 1\}$ et $L'_f = \{< x, i > | i \leq |f(x)|\}$ sont dans **L** (calculables en espace logarithmique).

Une fonction $f : \{0,1\}^* \to \{0,1\}^*$ est dite calculable *write once* en espace logarithmique si elle peut être calculée en espace logarithmique par une machine de Turing M dont le ruban de sortie est *write once*, c'est à dire qu'en chaque étape de calcul M peut soit laisser la tête de lecture de ce ruban sur la même case, soit écrire un symbole et la décaler d'une case sur la droite. Le ruban de sortie n'est pas compté dans l'espace de travail de M .

✎ Montrer que f est calculable write-once en espace logarithmique si et seulement si elle est implicitement calculable en espace logarithmique.

Exercice 7. *Bonus, si il vous reste du temps*

On rapelle que TQBF est l'ensemble des formules booléennes quantifiées (aucune variable n'est libre) qui sont vraies.

1. Montrer que pour toute formule quantifiée ϕ de taille m et de nombre de variables n, on peut vérifier si ϕ est dans TQBF en espace $O(n.m)$.

2. Peut-on faire mieux, par exemple en espace $O(n + m)$?

Exercice 8. *Bonus, si il vous reste de la place dans la marge*

✎ Prouvez que $P = NP$ ou que $P \neq NP$