Master de Mathématiques, Master d'Informatique Fondamentale
Logique et Complexité, TD10
Natacha Portier, jeudi 11 mai 2006

Convention : les langages considérés seront toujours supposés finis.

Exercice 1
(1) Montrer que tout algorithme de décision dans $(\mathbb{R}, +, -, =, 0, 1)$ se simule avec perte de temps seulement polynomiale dans $(\mathbb{R}, +, =, 0, 1)$.
(2) Même question si l'on rajoute l'ordre.
(3) Montrer que $(\mathbb{R}, +, -, \times, ^{-1}, =, 0, 1)$ et $(\mathbb{R}, +, \times, =, 0, 1)$ ont les mêmes problèmes P et les mêmes problèmes $\mathbb{P}$. (On convient que l'inverse de 0 est 0.)
(4) Même question si l'on rajoute l'ordre.

Exercice 2 (1) Soit $\mathfrak{M}$ une structure infinie. Montrer qu'il y a un problème sur $\mathfrak{M}$ qui n'est pas calculable (i.e. il n'existe pas de suite de circuits de décision correspondante).
(2) Soit $\mathfrak{M}$ une structure finie (Par hypothèse $|M| \geq 2$). Montrer qu'il y a un problème booléen sur $\mathfrak{M}$ qui n'est pas $\mathbb{P}$ au sens de $\mathfrak{M}$.
(3) Soit $\mathfrak{M}$ une structure infinie dénombrable. Montrer qu'il y a un problème booléen sur $\mathfrak{M}$ qui n'est pas $\mathbb{P}$ au sens de $\mathfrak{M}$.

Exercice 3 Montrer que dans $(\mathbb{R}, +, -, \ , =, <, 0, 1)$ tout problème booléen est résoluble en temps exponentiel.

Exercice 4 Soit $\mathfrak{M} = (M, +, -, =)$ un groupe abélien divisible sans torsion qui est non trivial. Montrer que les problèmes $\mathbb{P}$ (resp. P) standards sont les mêmes que les problèmes booléens $\mathbb{P}$ (resp. P) au sens de $\mathfrak{M}$.

Exercice 5 Soit $\mathfrak{M}$ une structure dont le langage n'a qu'une fonction unaire, outre l'identité, et pas d'autre fonction. Le sélecteur sera représenté ici par une relation ternaire satisfaite par les uples $(0, 1, 0)$, $(0, 1, 1)$, $(1, 0, 1)$ et $(1, 1, 1)$. Montrer que tout problème booléen P au sens de $\mathfrak{M}$ est $\mathbb{P}$ standard. Donner un exemple où on a égalité.

Exercice 6 Les comptes d'Ofman
(a) Soit $N_1(\bar{x})$ le nombre de 1 dans $\bar{x}$ (écrit en base deux). Montrer que si $\bar{x} < 2^n$ et $n < 2^m$, alors le i-ème chiffre (en partant de la droite) de $N_1(\bar{x})$ (en binaire) s'obtient par un circuit de profondeur inférieure à $A \cdot (m + i)$, pour une constante A. En déduire que $N_1(\bar{x})$ se calcule en temps parallèle logarithmique.

(b) Déterminer une constante A, et une suite C_n de circuits booléens de profondeur A, à $3n$ entrées et $2n+1$ sorties, remplaçant un triple (x, y, z) de nombres de longueur n écrits en binaire par un couple (u, v) tel que $x + y + z = u + v$. (Addition d'Ofman)
(c) En déduire une autre méthode de répondre à la partie (a), consistant à procéder par dichotomie, faire des additions d'Ofman du nombre de 1 des mots partiels considérés, puis une addition des deux chiffres obtenus à la fin.
(d) En déduire aussi l'existence d'un circuit de profondeur proportionnelle à $\log n$, permettant de remplacer n nombres $(x_1, \ldots, x_n)$ de longueur n par deux nombres (u, v) tels que $u + v = x_1 + \cdots + x_n$.
(e) En déduire un algorithme de temps parallèle logarithmique pour la multiplication de deux nombres.
(f) Montrer qu'on peut en outre exiger que la ressource de cet algorithme soit de l'ordre de n^2.

Exercice 7 (1) Montrer que tout problème booléen résoluble en temps parallèle $A \log n$ au sens de $(\mathbb{R}, +, -, =, 0, 1)$ se résout par un algorithme standard de temps parallèle $B (\log n)^2$.
(2) Si on suppose que l'algorithme n'est autorisé qu'à faire un nombre logarithmique de tests, montrer que la simulation standard peut se faire en temps parallèle logarithmique.