Master de Mathématiques, Master d'Informatique Fondamentale
Logique et Complexité, Examen
Documents et téléphones interdits
jeudi 1er juin 2006

Exercice 1
Décrire un circuit qui décide si la formule $\varphi(x, y, z)$ suivante est satisfaite dans le corps des réels. Ce circuit peut avoir un nombre quelconque de portes d'addition, de soustraction et de multiplication mais ne doit avoir au maximum 3 tests, qui peuvent être étiquetés par $=$ ou $\leq$.

$$\varphi(x, y, z) = \forall u \exists v \quad uv(x + uv) + z + yv = 0$$

Exercice 2
Décrire une suite de circuits C_n qui additionne deux entiers de taille n en base deux en temps parallèle logarithmique. Evaluer la taille et la profondeur des circuits. On donnera une majoration des constantes, qui pourra être grossière mais qui sera justifiée.

Exercice 3
Montrer que tout algorithme de décision dans $(\mathbb{R}, +, -, \times, {}^{-1}, =, <, 0, 1)$ se simule avec perte de temps seulement polynomiale dans $(\mathbb{R}, +, \times, =, <, 0, 1)$.

Exercice 4
Considérant un circuit arithmétique C de taille t et de profondeur p, montrer par induction sur p qu'on peut trouver un circuit C' de profondeur $2p$ et taille $4t$, avec deux fois plus de sorties, la moitié d'entre elles calculants les polynômes qui arrivent aux sorties de C, les autres leurs dérivées respectives par rapport à une variable x fixée.

Exercice 5
Montrer que dans toute structure $\mathfrak{M}$ le problème de la satisfaction des énoncés existentiels à paramètres dans $\mathfrak{M}$ est NP-complet et $\mathbb{NP}$-complet.

Exercice 6

(1) Un circuit arithmétique est un circuit dont les portes de calcul sont étiquetées par les fonctions $+$ ou $\times$, qui sont d'arité 2 (pas de test). Montrer que deux circuits arithmétiques sans paramètres qui sont équivalents pour $(\mathbb{R}, 0, 1, +, \cdot)$ sont aussi équivalents dans tout anneau commutatif unitaire.

(2) Un terme arithmétique est un circuit dont toutes les portes sont de valence au plus un, et qui n'a qu'une seule sortie. Quel est le degré maximal d'un

polynôme calculé par un terme arithmétique avec n entrées ? Démontrez le. Même question pour un circuit arithmétique.

(3) Une expression arithmétique est un terme arithmétique tel que les entrées sont étiquetées par des variables, et ces variables sont toutes distinctes. Montrer qu'une expression arithmétique en $\{x_0, \ldots, x_n\}$ est équivalente à un terme de la forme $Ax_0 + B$, où A et B sont des expressions en $\{x_1, \ldots, x_n\}$, A pouvant en outre pendre la valeur 1 et B la valeur 0.

(4) Soit E une expression arithmétique en $\{x_1, \ldots, x_n\}$, et F une sous-expression de E de profondeur minimum contenant strictement plus de $n/2$ variables. Soit G l'expression obtenue à partir de E en y remplaçant F par une seule porte d'entrée, affectée d'une nouvelle variable u. Evaluer le nombre de variables de G, et des deux sous-expressions immédiates de F (si F n'est pas une entrée).

(5) Montrer que toute expression arithmétique en n variables est équivalente à un terme arithmétique de profondeur majorée par $3 \log n$.

(6) Déterminer une constante K telle que tout terme arithmétique de taille t soit équivalent à un terme arithmétique de profondeur $\leq K \log t$. Existe t-il une telle constante pour les circuits arithmétiques ?

(7) Adapter les question précédentes quand on ajoute au langage les fonctions unaires identité $I(x)$ et opposé $-x$.

(8) Un terme booléen est un circuit dont les portes de calcul sont étiquetées par les fonctions binaire $\vee$, $\wedge$, ou par les fonctions unaire identité et $\neg$, dont toutes les portes sont de valence au plus un, et qui n'a qu'une seule sortie.

Utiliser ce qui précède pour montrer qu'il existe K', que l'on précisera, tel que tout terme booléen de taille t soit équivalent à un terme de profondeur au plus $K' \log t$.