Maîtrise de Mathématiques
Logique et Complexité (Année 2003-2004)
TD 11

Exercice 1. 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 2. (1) Les entiers x et y étant donnés sous forme binaire, montrer que le problème si x est carré modulo y est NP.
(2) Soit p un nombre premier congru à 3 modulo 4.
(a) Montrer que si $a \in \mathbb{F}_p$ et $b = a^{(p+1)/4}$, alors $b^2 = \pm a$.
(b) Montrer que -1 n'est pas un carré dans $\mathbb{F}_p$. (Indication: en supposant que -1 est un carré, calculer $(-1)^{(p-1)/2}$).
(3) En déduire un algorithme polynomial qui pour p un nombre premier congru à 3 modulo 4 et x un entier, détermine si x est un carré modulo p et calcule alors ses deux racines carrées.

Exercice 3. Une bijection f de $\{0,1\}^*$ qui conserve la taille est *fonctionnelle à sens unique* si elle est calculable en temps polynomial, mais son inverse ne l'est pas. Montrer que l'existence d'une telle fonction implique $P \neq NP$.
(Indication: Considérer $\{(\bar{x}, \bar{y}) : \exists\, \bar{z} \leq \bar{x}\ f(\bar{z}) = \bar{y}\}$, où $\leq$ est l'ordre lexicographique.)

Exercice 4. Montrer que $\langle \mathbb{R}, 0, 1, +, -, = \rangle$ n'a pas de problème booléen $\mathbb{NP}$-complet (ou NP-complet).
(Indication: Soit $\mathfrak{X}$ un problème booléen $\mathbb{NP}$-complet, $\mathfrak{Y}$ le problème de l'indépendance sur $\{0,1\}$ des réels $x_1, \ldots, x_n$, et $f_{\mathfrak{Y}} : \mathbb{R}^* \to \{0,1\}^*$ une fonction $\mathbb{P}$ qui réduit $\mathfrak{Y}$ à $\mathfrak{X}$. Montrer qu'il existent $\bar{a} \in \mathfrak{Y}$ et $\bar{b} \notin \mathfrak{Y}$ avec $f(\bar{a}) = f(\bar{b})$, et obtenir une contradiction.)

Exercice 5. Montrer que le problème de la satisfaisabilité des systèmes d'équations polynomiales de second degré, chacune ayant au plus trois variables, à coefficients complexes, est $\mathbb{NP}$-complet dans $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$.

Exercice 6. Un problème $\mathfrak{X}$ est $\mathbb{P}^+$ au sens d'une structure $\mathfrak{M}$ s'il devient $\mathbb{P}$ quand on rajoute à $\mathfrak{M}$ un nombre fini de fonctions définissables sans quanteurs (c-à-d dont le graphe est donné par une formule sans quanteurs). Montrer que $\mathbb{P} \subseteq \mathbb{P}^+ \subseteq \mathbb{NP}$, et que $\mathbb{NP} = \mathbb{NP}^+$ (avec la définition analogue).

Les problèmes suivant ont été posés aux examens de mai ou septembre 2002.

Problème 1. Soit $\mathfrak{M} = \langle \mathbb{N}, 0, 1, \sigma, \pi, =, < \rangle$ la structure formée des entiers naturels munis de leur ordre, de la fonction-successeur $\sigma(x) = x + 1$, et de la fonction-prédecesseur $\pi(x) = \max\{0, x - 1\}$ (en outre du sélecteur $S(x, y, z)$ qui vaut y si $x = 0$, z si $x = 1$, et x dans les autres cas).

1. On dit que deux k-uples croissants d'entiers $(a_1, \ldots, a_k)$ et $(b_1, \ldots, b_k)$ sont n-*équivalents* si, posant $a_0 = b_0 = 0$, pour chaque $i < k$ soit $a_{i+1} - a_i$ et $b_{i+1} - b_i$ sont égaux, soit tous deux $\geq n$. Montrer que deux uples n-équivalents satisfont les mêmes formules sans quanteurs de longueur au plus n, et que deux uples n^2-équivalents satisfont les mêmes formules existentielles de longueur au plus n.

2. Montrer que si $\exists \bar{y} \varphi(\bar{a}, \bar{y})$ est satisfaite, où φ est une formule sans quanteur de longueur n, on en trouve les témoins parmi les n^2 premiers successeurs ou prédecesseurs des a_i (y inclus $a_0 = 0$). En déduire que $\mathfrak{M}$ satisfait $\mathbb{NP} = \mathbb{NBP}$.

3. Quels sont les problèmes booléens $\mathbb{P}$ et $\mathbb{NP}$ au sens de $\mathfrak{M}$?

4. Montrer que donnée une formule existentielle $\exists \bar{y} \varphi(\bar{y}, \bar{a})$ de longueur n à paramètres $\bar{a}$, on peut construire (en temps polynomial) une formule équivalente $\exists \bar{y}' \varphi'(\bar{y}', \bar{a}')$ avec les $a'_i \leq n^3$. En déduire qu'il y a un problème booléen $\mathbb{NP}$-complet au sens de $\mathfrak{M}$.

Problème 2. Soit $\mathfrak{N}$ la structure $\mathfrak{M}$ du problème 1. où on a supprimé la fonction π.

1. Montrer que π ne se calcule pas par un circuit au sens de $\mathfrak{N}$.

2. Montrer que $\mathfrak{N}$ et $\mathfrak{M}$ ont les mêmes problèmes $\mathbb{P}$ (et donc $\mathbb{NP}$ et $\mathbb{NBP}$).

Problème 3. Soit $\mathfrak{M}$ la structure $\langle \mathbb{R}, 0, 1, +, -, =, \leq, x \mapsto \frac{x}{2} \rangle$. Montrer que $\mathfrak{M}$ a les mêmes problèmes $\mathbb{P}$ et $\mathbb{NP}$ que $\langle \mathbb{R}, 0, 1, +, -, =, \leq \rangle$.

Problème 4. (1) Soit $\mathfrak{M}$ une structure et $\mathfrak{M}^+$ une expansion de $\mathfrak{M}$ par des nouvelles fonctions dont les graphes sont définis dans $\mathfrak{M}$ par des formules sans quanteurs. Montrer que $\mathfrak{M}$ et $\mathfrak{M}^+$ ont les mêmes problèmes $\mathbb{NP}$.

(2) Soit $\mathfrak{M} = \langle \mathbb{R}, 0, 1, \Sigma(x, y, z), = \rangle$ et $\mathfrak{M}^+ = \langle \mathbb{R}, 0, 1, +, -, = \rangle$, où Σ est le graphe de l'addition $x + y = z$. Montrer que les couples $(a, b,)$ des réels vérifiant $a \neq 0$, $a \neq 1$, $b \neq 0$, $b \neq 1$, $a \neq b$, $a \neq 2b$ et $b \neq 2a$ satisfont tous les mêmes formules sans quanteurs et sans paramètres au sens de $\mathfrak{M}$.

Montrer qu'il est impossible d'exprimer la relation $x = 3y$ dans $\mathfrak{M}$ sans quanteurs (attention aux paramètres !).

Montrer que $\mathfrak{M}$ et $\mathfrak{M}^+$ n'ont pas les mêmes problèmes $\mathbb{P}$.