Maîtrise de Mathématiques
Logique et Complexité, TD10
Jeudi 17 avril 2003
Natacha Portier

Exercice 1

Montrer que dans un groupe abélien divisible sans torsion muni de sa loi de groupe et de l'inverse, les problèmes booléens P sont les P standards et les booléens $\mathbb{P}$ sont les $\mathbb{P}$ standards.

Exercice 2

Montrer que dans un groupe abélien ordonné divisible contenant les réels et muni de sa loi de groupe, de l'inverse et de l'ordre les problèmes booléens P sont les $\mathbb{P}$ standards.

Exercice 3,1

Montrer que tout algorithme de décision dans $(\mathbb{R}; +, -, =)$ se simule avec perte de temps seulement polynomiale dans $(\mathbb{R}; +, =)$; même question avec $(\mathbb{R}; +, -, =, <)$ et $(\mathbb{R}; +, =, <)$.

Exercice 3,2

Montrer que $(\mathbb{R}; +, -, \times, x^{-1}, =)$ et $(\mathbb{R}; +, \times, =)$ ont les mêmes problèmes P et les mêmes problèmes $\mathbb{P}$; même question si on ajoute l'ordre (on convient que l'inverse de 0 est 0, ou bien que tout calcul d'inverse doit être précédé d'un test $x \neq 0$).

Exercice 4

Soit M une structure dont le langage ne comporte que des relations et une seule fonction unaire (sans compter identité et sélecteur) ; montrer que tout problème P au sens de M est $\mathbb{P}$ au sens standard. Donner un exemple d'une telle structure M où les booléens P au sens de M sont exactement les $\mathbb{P}$ standards.

Exercice 5,1

Soit M une structure dont le langage comprend k fonctions d'arité m. Evaluer la taille de l'ensemble des éléments de M expressibles à partir de d paramètres a_1, ..., a_d par un circuit de profondeur p.

Question 5,2

Montrer que quelle que soit la structure ùMù il y a toujours un problème booléen qui n'est pas résoluble au sens de M en temps parallèle $\log(\log n)$.

Exercice 6,1

On fixe un nombre premier p. On rappelle que le corps $\mathbb{F}_p$ a une extension et une seule de dimension d, laquelle a p^d éléments. Montrer qu'il y a au moins p^d/d polynômes irréductibles de degré inférieur à d dans $\mathbb{F}_p[x]$

Question 6,2

On se pose le problème de savoir si un circuit arithmétique sans paramètres définit ou non le paramètre nul . Se ramener au cas où le circuit n'a qu'une seule variable x. Montrer alors que si la taille t du circuit est fixée, il suffit de l'évaluer modulo un polynôme $P_t(x)$ de petit degré. Conclusion ?

Question 6,3

Montrer que pour un corps de caractéristique quelconque, les problèmes booléens qui sont $\mathbb{P}$ sont les $\mathbb{P}$ au sens standard.