Maîtrise de Mathématiques
Logique et Complexité (Année 2003-2004)
TD 9

Exercice 1. Démontrer le théorème de Spira pour $\langle \mathbb{R}, + \rangle$.

Exercice 2.

(1) Soient un ensemble fini $M = \{m_1, \ldots, m_k\}$ et $S : M^{k+1} \to M$ le sélécteur défini par $S(m_i, x_1, \ldots, x_k) = x_i$. Montrer par récurrence sur n, que toute fonction de M^n dans M s'exprime comme terme en S, avec paramètres dans M.

(2) Un langage fonctionnel fini $\mathcal{L}$ est *complet* pour une $\mathcal{L}$-structure $\mathfrak{M}$ si pour tout $n < \omega$ toute fonction de M^n dans M s'exprime comme $\mathcal{L}$-terme. Montrer que l'on peut munir un ensemble M d'un langage fonctionnel fini complet si et seulement si M est fini.

(3) Montrer que le théorème de Spira est vrai pour une structure finie de langage fonctionnel complet.

Exercice 3. Montrer un théorème de Spira basé sur le nombre d'entrées du terme et non pas sur sa taille, d'abord dans le cas des termes booléens, ensuite pour les langages fonctionnels finis complets.

Exercice 4. Dans cet exercice on appelera *langage* tout sous-ensemble de $\{0, 1\}^*$.

(1) On dit que deux mots binaires a et b sont congrus modulo le langage $\mathcal{L}$ si pour tout mot binaire c on a $ac \in \mathcal{L} \Leftrightarrow bc \in \mathcal{L}$.
Montrer que c'est une relation d'équivalence, et que si a est congru à b, alors ac est congru à bc pour tout c.

(2) On dit que $\mathcal{L}$ est régulier (ou rationnel) si cette congruence n'a qu'un nombre fini de classes. Parmi les langage suivants, lesquels sont réguliers ?

(a) Les mots de longueur paire.

(b) Les mots comportant un nombre pair de zéros.

(c) Les mots ayant autant de zéros que de uns.

(d) Les mots formés d'une suite de zéros (éventuellement vide), suivie d'une suite de uns.

(3) Soit $\mathcal{L}$ un langage régulier, et K l'ensemble des classes de sa congruence (qu'on appelle *états*). L'état initial e_0 est le mot vide; la fonction d'acceptation $\alpha : K \to \{0, 1\}$ vaut 1 pour un état de mots qui sont dans $\mathcal{L}$, 0 sinon; la fonction de transition $\theta : K \times \{0, 1\} \to K$ envoie (e, x) sur l'état de ax, où a est un mot quelconque dans l'état e.

Décrire un algorithme, consistant à lire le mot $a = (x_1, \ldots, x_n)$ de gauche à droite, en suivant pas à pas l'état du segment initial de a déjà lu, qui permet de savoir en temps linéaire si $a \in \mathcal{L}$; montrer que cette appartenance équivaut à une condition $t(x_1, \dots, x_n) = 1$, où t est un terme en e_0, θ et α.

(4) Si $K = \{0,1\}^k$, on obtient $\theta : \{0,1\}^{k+1} \to \{0,1\}^k$ et $\alpha : \{0,1\}^k \to \{0,1\}$. Montrer que l'appartenance d'un mot a de longueur n à $\mathcal{L}$ se teste par un circuit booléen de profondeur $A \log n$; évaluer la constante A en fonction de k.

(5) En utilisant les comptes d'Ofman, montrer que l'appartenance à chacun des langages dans (2) se teste en temps parallèle logarithmique.

Exercice 5. Montrer que $\det(X)$, où X est une matrice $n \times n$ sur $\mathbb{R}$ ou $\mathbb{C}$, se calcule par un circuit de taille polynomiale dans le langage comportant addition, soustraction, multiplication et division. (Par convention la division par 0 vaut 0.)

Exercice 6.

(1) 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) Montrer qu'un terme arithmétique avec n entrées calcule un polynôme de degré total au plus n; donner un exemple de circuit de taille $n+1$ calculant un polynôme de degré 2^n ; en déduire qu'il n'y a pas équivalence, au niveau polynomial, entre termes et circuits arithmétiques.

(3) Montrer qu'une expression arithmétique en $\{x_0, \dots, x_n\}$ est équivalente à un terme de la forme $Ax_0 + B$, où A et B sont des expressions en $\{x_1, \dots, x_n\}$, A pouvant en outre pendre la valeur 1 et B la valeur 0. [Attention: $Ax_0 + B$ n'est pas nécessairement une expression, comme A et B peuvent avoir des variables en commun.]

(4) Soit E une expression arithmétique en $\{x_1, \dots, x_n\}$, 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 $\leq K \log t$; montrer qu'il n'existe aucune telle constante pour les circuits arithmétiques.

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

(8) Déduire une autre démonstration du Théorème de Spira pour les circuits booléens, basée sur la distributivité des opérations booléennes.