Maîtrise de Mathématiques
Logique et Complexité (Anne 2003-2004)
TD 8

Exercice 1. Montrer que dans toute expression booléenne $C(x_0, \ldots, x_n)$ il y a $i < j$ tel que $C(\ldots, x_i, \ldots, x_j, \ldots) = C(\ldots, x_j, \ldots, x_i, \ldots)$, ou bien tel que $C(\ldots, x_i, \ldots, x_j, \ldots) = C(\ldots, \neg x_j, \ldots, \neg x_i, \ldots)$. En déduire que le sélecteur ne se calcule pas par une expression booléenne.

Exercice 2. Montrer que si C est un circuit (non booléen) d'arité n (≥ 2), alors $t(C) \leq s(C)[n^{p(C)+1} - 1]/(n-1)$.

Exercice 3. Les comptes d'Ofman
(a) Soit $N_1(\bar{x})$ le nombre de 1 occurant dans $\bar{x}$ (écrit en base deux). Montrer que si $\bar{x} < 2^n$ et $n < 2^m$, alors le i-me 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 4. (a) Montrer que la méthode utilisée dans la preuve du théorème de Spira transforme un terme de taille t en un circuit de profondeur $4 \log t$ et de taille au plus $A \cdot t^{1+\log 3}$, ou bien en un terme de profondeur $4 \cdot \log t$ et de taille $B \cdot t^3$; on majorera les constantes A et B par des sommes de séries convergentes.
(b) En fait, ces estimations sont trop élevées : appliquer la méthode aux formules de taille inférieure à 2^m ; écrire, et résoudre, les équations de récurrence vérifiées par les tailles ; transformer une formule de taille t en un circuit de taille $C \cdot t^2$, ou une formule de taille $D \cdot t^{1+\log 3}$ et de profondeur $4 \cdot (\log t + 1)$; évaluer les constantes C et D.
(c) Estimer le temps, et aussi le temps parallèle, nécessaires pour effectuer ces transformations.