Master de Mathématiques, Master d'Informatique Fondamentale
Logique et Complexité, TD8
Natacha Portier, jeudi 13 avril 2006

Exercice 1 Montrer que l'addition de 1 à un nombre écrit en binaire de longueur n se représente par un circuit booléen de taille de l'ordre de $An \log n$ et de profondeur de l'ordre de $B \log n$, où A et B sont des constantes à préciser.

Exercice 2,1

Donner un circuit booléen qui calcule la somme de deux entiers $y_n...y_1$ et $x_n...x_1$ écrits en base 2 de taille n et évaluer sa taille et sa profondeur.

Exercice 2,2

On améliore la profondeur du circuit précédent de la manière suivante. On suppose que n est une puissance de 2. On calcule en parallèle la somme de $y_{n/2}...y_1$ et $x_{n/2}...x_1$ ainsi que les sommes $y_n...y_{n/2+1}+x_n...x_{n/2}$ et $y_n...y_{n/2+1}+x_n...x_{n/2}+1$, puis on choisit le résultat en fonction de la retenue. Évaluer la taille et la profondeur du circuit.

Exercice 2,3 Généraliser la construction précédente ("diviser pour régner"), donner la taille et la profondeur du circuit obtenu.

Exercice 3. 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 4

(i) On dit qu'une fonction f de $\{0;1\}^n$ dans $\{0;1\}$ est monotone si chaque fois que $x_1 \leq y_1$ et ... $x_n \leq y_n$, où $\leq$ représente l'ordre naturel sur $\{0;1\}$, alors $f(\bar{x} \leq f(\bar{y})$; on dit qu'elle est positive si elle s'exprime par un circuit booléen sans négation. Montrer qu'il y a identité entre les fonctions positives et les fonctions monotones.

(ii) On appelle dual du circuit booléen C le circuit C^d obtenu en y remplaçant $\wedge$ par $\vee$, $\vee$ par $\wedge$, 0 par 1 et 1 par 0 ; montrer que si C calcule la fonction $f(x_1, \ldots, x_n)$ alors C^d calcule la fonction $\neg f(\neg x_1, \ldots, \neg x_n)$; montrer que tout terme booléen T est équivalent à un terme booléen T^* de taille et de

profondeur inférieures sans porte d'identité et où les portes de négation ne reçoivent leur flèche que d'une entrée étiquetée par une variable.

Exercice 5 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 6 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 7 (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.