TD09 - Suite des circuits

Exercice 1. *Théorème de Hoover, Klawe et Pippenger*

Théorème de Hoover, Klawe et Pippenger : À tout circuit booléen C correspond un circuit équivalent C^* de degré sortant deux tel que

$$t(C^*) \leq 3t(C) \text{ et } p(C^*) \leq 2p(C) + \log_2(s(C))$$

.

1. Montrer le résultat pour la taille. Qu'obtient on pour la profondeur ?

2. Donnez un contre-exemple pour une construction de C^* naïve avec uniquement des parapluies.

3. On introduit la notion de pondération dans un arbre binaire renversé. Si toute sortie (toute feuille) est affectée d'un poids, qui est un entier positif, on définit inductivement le poids d'un noeud de l'arbre comme étant le maximum des poids de ses fils, augmenté de un. Montrer que quelle que soit la distribution de poids entiers $a_1, ..., a_n$ dont on affecte les points $p_1, ..., p_n$, il est possible de construire au dessus un arbre renversé dont le poids c de la racine satisfasse $2^c < 2.(2^{a_1} + ... + 2^{a_n})$.

4. Soit C un circuit. On le découpe en niveaux à partir du bas. Soit N_0 l'ensemble des sorties et N_1 l'ensemble des portes qui n'émettent des flèches que vers des sorties. L'ensemble N_2 est constitué des portes qui n'émettent des flèches que vers des portes de N_0 ou N_1. On veut que le circuit soit bien étagé, c'est-à-dire que les portes de N_2 n'émettent des flèches que vers des portes de N_1. Pour cela, on ajoute éventuellement des portes d'identité au niveau N_1 entre une porte de N_2 et une sortie. On construit de même tous les niveaux du circuit. Donner un exemple de cette construction sur un circuit de votre choix.

5. Utiliser les deux questions précédentes pour montrer le résultat sur la profondeur.

Exercice 2.

✎ Montrer que tout circuit acceptant tous les $00..010..00$ et refusant $00...0$ a une profondeur supérieure ou égale à $\log_2 n$. En déduire que l'expression de la fonction $Sup(x_1, ..., x_n)$ nécessite un circuit de profondeur au moins $\log_2 n$ (et donc qu'il n'est pas raisonnable d'exiger des circuits de profondeur moins que logarithmique).

Exercice 3.
Une fonction booléenne $f : \{0,1\}^n \to \{0,1\}$ sera dite monotone croissante si pour tout i, et pour tous $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ on a :

$$f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \geq f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$$

✎ Montrer que les fonctions monotones croissantes sont exactement celles que l'on peut exprimer en n'utilisant que les connecteurs AND, OR, et les constantes 0 et 1.

Exercice 4.
Une expression booléenne est un terme sans constantes 0 ou 1, et où une même variable n'étiquette qu'une seule entrée.

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

Exercice 5.

Soit $N_1(\overline{x})$ le nombre de 1 occurant dans $\overline{x}$ (écrit en base deux).

1. Montrer que si $\overline{x} < 2^n$ et $n < 2^m$, alors le i-ème chiffre (en partant de la droite) de $N_1(\overline{x})$ (en binaire) s'obtient par un circuit de profondeur inférieure à $A \cdot (m + i)$, pour une certaine constante A.

2. 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)

3. En déduire une autre méthode de répondre à la question 1, 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.

4. En déduire aussi l'existence d'un circuit de profondeur proportionnelle à $\log n$, permettant de remplacer n nombres $(x_1, \dots, x_n)$ de longueur n par deux nombres $(u; v)$ tels que $u + v = x_1 + \cdots + x_n$.

5. En déduire un circuit de profondeur n pour la multiplication de deux nombres de taille n.

6. Montrer qu'on peut en outre borner le nombre de portes de ce circuit par $C \cdot n^2$ pour une certaine constante C.

Exercice 6.

✎ Montrer que toute fonction booléenne en n variables peut être représentée par un terme booléen de profondeur (au plus) $n + \log_2 n + 2$ et de taille exponentielle en n. En déduire que pour tout polynôme p il existe pour n assez grand une fonction n-aire non exprimable par un terme de taille $p(n)$. C'est l'effet Shannon. Il montre l'existence de problèmes non-polynomiaux.