TD Notations n°1

Circuits booléens linéaires

Ce TD est tiré d'une épreuve orale d'informatique fondamental de l'ENS Ulm en MP option informatique, en 2022.

Soit $\mathscr{X}_n = \{x_1, \ldots, x_n\}$ un ensemble énuméré de variables. Un *circuit booléen* sur $\mathscr{X}_n$ est un graphe orienté acyclique (V, E), où les sommets de degré entrant 0, les *entrées* du circuit, sont étiquetées par des variables de $\mathscr{X}_n$ et les autres nœuds, les *portes internes* du circuit, sont étiquetées par des fonctions $\{0,1\}^r \to \{0,1\}$ avec r le degré entrant du nœud. Dans la suite, pour une porte p du circuit, on note e_p la fonction qui l'étiquète. On ne considère que des fonctions parmi $\land$, $\lor$, $\neg$, respectivement ET, OU, NON logique des booléens en entrée. Une *sortie* du circuit est un nœud de degré sortant 0.

Une *assignation booléenne* de $\mathscr{X}_n$ est une fonction $g : \mathscr{X}_n \to \{0,1\}$. Pour une porte p du circuit, on définit son évaluation g_p comme suit :
- pour une entrée du circuit $p = x_i$, pour un certain i, on définit $g_p = g(x_i)$;
- pour un nœud interne p, on définit $g_p = e_p\left(g_{p_1}, \ldots, g_{p_r}\right)$, où $p_1, \ldots, p_r$ sont les antécédents de p dans le circuit.

Une fonction $f : \{0,1\}^n \to \{0,1\}^k$ est *calculée* par un circuit si, pour toute évaluation g, nous avons

$$f(g(x_1), \ldots, g(x_n)) = \left(g_{o_1}, \ldots, g_{o_k}\right)$$

avec $o_1, \ldots, o_k$ une séquence de portes de sortie du circuit. Un ensemble de mots $E \subseteq \{0,1\}^n$ est *calculé* par un circuit si sa fonction caractéristique (c'est-à-dire, la fonction $\mathbf{1}_E$ telle que $\mathbf{1}_E(u) = 1$ si, et seulement si, $u \in E$) est calculée par le circuit.

Dans la suite, on appellera *câbles* les arêtes du graphe.

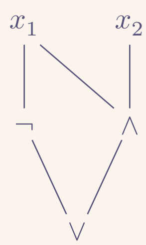

Fig. 1. Un circuit calculant l'ensemble $\{00, 01, 11\}$

Q1. Montrer que toute fonction $f : \{0,1\}^n \to \{0,1\}$ est calculable par un circuit booléen. Indiquer le nombre de portes nécessaires et le nombres de câbles nécessaires. Quelle relation y a-t'il entre ces deux nombres ?

Q2. La *profondeur* du circuit est le plus long chemin d'une entrée à la sortie. Soit $k \in \mathbb{N}$. On note T_k^n l'ensemble des mots de $\{0,1\}^n$ qui ont au plus k positions à 1.

(1) Proposer un circuit avec un nombre de câbles linéaires en n,[1] qui calcule l'ensemble T_k^n. Quelle est sa profondeur en fonction de n ?

(2) Proposer un circuit de profondeur constante qui calcule l'ensemble T_k^n. Quelle est sa taille (câbles et portes) en fonction de n ?

Q3. On va construire un circuit de profondeur constante avec un nombre de câbles linéaires en n qui calcule T_k^n. Pour ce faire, on passe par une fonction intermédiaire qu'on nomme

$$\text{PREFIX-}\vee_n : \{0,1\}^n \to \{0,1\}^n$$

telle que $\text{PREFIX-}\vee_n(x_1, \ldots, x_n)_i = \bigvee_{j \leq i} x_j$.

Montrez que, si un circuit de profondeur constante avec un nombre de câbles linéaires en n pour $\text{PREFIX-}\vee_n$ existe, alors il en existe également pour T_k^n.

Q4. Construire un circuit de profondeur constante avec un nombre de câbles linéaires en n pour $\text{PREFIX-}\vee_n$.

Indication. On pourra regrouper les entrées par paquets de taille $\sqrt{n}$ afin d'identifier à gros trait où peut être le premier 1 dans le mot et appliquer de manière parcimonieuse un circuit naïf des ensembles de portes de taille $\sqrt{n}$.

Q5. Soit $\text{BIN}_n : \{0,1\}^n \to [\![0, 2^n]\!]$ la fonction qui associe un nombre à son écriture en binaire. On considère maintenant la fonction $\text{ADDITION}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{n+1}$ qui réalise l'addition d'entiers représentés en binaire. Formellement, pour deux entiers $i, j < 2^n$, on a :

$$\text{ADDITION}_n(\text{BIN}_n(i), \text{BIN}_n(j)) = \text{BIN}_{n+1}(i+j).$$

(1) Montrer que la fonction ADDITION_n est calculable par un circuit ayant un nombre de câbles linéaires en n.
(2) Montrer que la fonction ADDITION_n est calculable par un circuit ayant un nombre de câbles polynômial en n et de profondeur constante.

Q6. Montrer en appliquant une méthode similaire à Q4, que si on sait implémenter ADDITION_n à profondeur constante avec un circuit utilisant $n \leq f(n) \leq n^2$ câbles, alors il est possible de construire un circuit avec un nombre de câbles en $\mathcal{O}(\sqrt{n} \cdot f(\sqrt{n}))$.

En déduire que, pour tout $\varepsilon > 0$, il existe un circuit calculant ADDITION_n utilisant un nombre de câbles en $\mathcal{O}(n^{1+\varepsilon})$.

Théorème 1. Pour tout entier d, il existe une fonction $f_d : \mathbb{N} \to \mathbb{N}$ croissante et non bornée telle que tout n-super concentrateur de profondeur d a un nombre d'arêtes au moins égal à $\Omega(n \cdot f_d(n))$.

Q7. Soit $G = (V, E)$ un graphe acyclique avec n sources $s_1, \ldots, s_n$ (nœuds de degré entrant 0), et n sorties $o_1, \ldots, o_n$ (nœuds de degré sortant 0). On dit que G est un n-*super concentrateur* si pour un entier $k < n$, et pour toute séquence $i_1 < j_1 < i_2 < \cdots < i_k < j_k$, il existe des k-chemins disjoints qui relient i_1 à j_1, i_2 à j_2, *etc.* On admettra le théorème difficile ci-dessus (Théorème 1).

En déduire qu'il n'existe pas de circuit de profondeur constante et avec un nombre de câbles linéaire en n qui calcule ADDITION_n.

Indication. On pourra éventuellement s'aider du *théorème de Menger* : étant donné deux ensembles de sommets I et J, le nombre maximal de chemins disjoints reliant I et J est égale à la taille de la plus petite coupe entre I et J.

[1]mais pas forcément linéaire en k, qui est vue comme une constante fixée