TD 07 – Rabool les circuits

Exercice 1. *En cours de route*

Les notations NC^k et NC désignent ici des classes L**-uniformes**.

1. Montrer que $\textsc{Parity} \in \mathsf{NC}^1$.
2. Soit deux matrices booléennes (a_{ij}) et (b_{ij}) de taille $m \times m$. Leur **produit booléen** est la matrice (c_{ij}) définie par $c_{ij} = \bigvee_k (a_{ik} \wedge b_{kj})$. Montrer que le produit booléen est dans FNC^1 (définie comme NC^1 mais avec des circuits à plusieurs sorties).
3. Montrer que $\mathsf{NC}^1 \subseteq \mathsf{L}$, et plus généralement que $\mathsf{NC} \subseteq \mathsf{polyL} = \bigcup_k \mathsf{SPACE}(\log^k n)$.
4. Que peut-on en déduire pour le langage TQBF ?
5. Montrer que $\mathsf{NL} \subseteq \mathsf{NC}^2$.

Exercice 2. *Théorème de Spira*

On dit qu'un circuit est une *formule booléenne* si toute porte (sauf la sortie) émet exactement une flèche. Autrement dit, le graphe sous-jacent est un arbre.

✎ Montrer que pour toute formule F de taille t, il existe une formule équivalente F' de profondeur inférieure à $4 \log t$. Quelle est la taille de F' ? Quelles bornes obtient-on si on transforme une formule en circuit ?

Exercice 3. *En diagonale*

Vous avez vu en cours qu'il existe des langages indécidables dans $\mathsf{P/poly}$.

✎ Montrer qu'il existe des langages décidables qui ne sont pas dans $\mathsf{P/poly}$.
Indication. Diagonalisation sur les circuits de taille $n^{\log n}$.

Exercice 4. *Sonné*

Un langage L appartient à la classe $\mathsf{P\text{-}Sel}$ s'il existe une fonction $f \in \mathsf{FP}$ telle que pour tout $\langle x, y \rangle$, $f(\langle x, y \rangle) \in \{x, y\}$, et $f(\langle x, y \rangle) \in L$ dès que $x \in L$ ou $y \in L$. La fonction f est la *fonction de sélection* de L. Le but de cet exercice est de montrer que $\mathsf{P\text{-}Sel} \subseteq \mathsf{P/poly}$ [Ko, 1983].

1. Montrer qu'on peut supposer f symétrique : pour tout x, y, $f(x, y) = f(y, x)$.
2. On appelle **tournoi** un graphe complet dont on a orienté les arêtes. Montrer que si $G = (V, E)$ est un tournoi à k sommets, alors il existe un sous-ensemble U des sommets, de cardinal au plus $\lfloor \log k + 1 \rfloor$, tel que pour tout $v \in V \setminus U$, il existe $u \in U$ tel que $(v, u) \in E$.
3. On note $L^{=n} = L \cap \{0,1\}^n$. Montrer qu'il existe $A_n \subseteq L^{=n}$, de cardinal au plus $(n+1)$, tel que $x \in L^{=n}$ si et seulement s'il existe $y \in A_n$ tel que $f(x, y) = x$.
4. Conclure.

Note. On peut montrer [1] que $\mathsf{P\text{-}Sel} \subseteq \mathsf{NP/lin} \cap \mathsf{coNP/lin}$, où lin représente l'ensemble des fonctions linéaires de $\mathbb{N}$ dans $\mathbb{N}$. On peut même montrer que $\mathsf{P\text{-}Sel} \subseteq \mathsf{NP}/\{n \mapsto n+1\}$. Par contre, $\mathsf{P\text{-}Sel} \not\subseteq \mathsf{NP}/\{n \mapsto n\}$ (plus dur).

1. C'est un bon entraînement ! On utilise le fait que dans un tournoi, il existe un sommet s d'où on peut atteindre tout autre sommet par un chemin de longueur au plus deux.