~~TD~~ 08 – Probe Habileté

Cirque

Exercice 1. *Sonné*

Un langage L appartient à la classe P-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).

Exercice 2. *Théorème de hiérarchie non-uniforme*

Il existe différentes façon d'énoncer un théorème de hiérarchie non-uniforme. Nous allons montrer que pour toute fonction $s(n) \leq 2^n/n$, $\mathsf{SIZE}(s(n)) \supsetneq \mathsf{SIZE}(s(n) - \mathcal{O}(n))$.

1. Pourquoi se restreint-on aux fonctions $s(n) \leq 2^n/n$?
2. Soit $f, g : \{0,1\}^n \to \{0,1\}$ telles que f et g diffèrent sur une seule entrée. Montrer que les tailles des circuits minimaux calculant f et g différent d'au plus $\mathcal{O}(n)$.
3. Prouver qu'il existe une fonction booléenne qui est calculable par un circuit de taille $s(n)$ mais pas par un circuit de taille $s(n) - \mathcal{O}(n)$.

Exercice 3. *Réduction des erreurs pour* RP

✎ Énoncer et démontrer un théorème de réduction des erreurs pour RP.

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.

Exercice 4. *Biaise-main*

Une ρ-pièce est une pièce biaisée telle que $\mathbb{P}[\textsc{Face}] = \rho$.

1. Montrer qu'une ρ-pièce peut être simulée par une MTP en temps espéré $\mathcal{O}(1)$ si le i-ème bit de ρ est calculable en temps $\mathsf{poly}(i)$.
2. (Méthode de Von Neumann) Inversement, montrer qu'on peut simuler une 1/2-pièce avec une ρ-pièce en temps espéré $\mathcal{O}(1/\rho(1-\rho))$.
3. Proposer une méthode pour améliorer l'espérance du temps de fonctionnement.
4. Donner un réel ρ tel qu'une MTP utilisant une ρ-pièce peut décider un langage indécidable.
5. Montrer qu'on peut simuler un tirage aléatoire dans $\{1, \dots, N\}$ avec une pièce : pour tout N et $\delta > 0$, il existe un algorithme probabiliste A, polynomial en $\log(N)\log(1/\delta)$, qui renvoie un élément de $\{1, \dots, N, ?\}$ tel que
   1. lorsqu'il ne renvoie pas ?, la sortie de A est uniformément distribuée dans $\{1, \dots, N\}$;
   2. La probabilité que A renvoie ? est au plus δ.