TD06 – Un club très select

Rappels (Karp, Lipton)
Soient Σ un alphabet fini, $\mathcal{C}$ une classe de complexité sur Σ et $f : \mathbb{N} \to \mathbb{N}$ une fonction. On note $\mathcal{C}/f$ l'ensemble des langages A sur Σ vérifiant la propriété suivante : il existe $B \in \mathcal{C}$ et $a : \mathbb{N} \to \Sigma^*$ tels que

1. $\forall n \geq 0$, $|a(n)| = f(n)$;
2. $x \in A \iff (x, a(|x|)) \in B$.

Si $\mathcal{F}$ est un ensemble de fonctions, on note $\mathcal{C}/\mathcal{F}$ la réunion des $\mathcal{C}/f$ pour $f \in \mathcal{F}$. Les ensembles de fonctions courants sont poly (ensemble des fonctions polynomialement bornées) et log (ensemble des fonctions logarithmiquement bornées).

On utilisera aussi :
– lin : l'ensemble des fonctions linéaires de $\mathbb{N}$ dans $\mathbb{N}$;
– quad : l'ensemble des polynômes de degré au plus deux.

Définition
La classe RP est l'ensemble des langages A tels qu'il existe un langage $B \in \mathsf{P}$ et un polynôme p tels que

1. si $x \in A$ alors $|\{y \in \{0,1\}^{p(|x|)} \ : \ (x,y) \notin B\}| \leq (1/2)2^{p(|x|)}$;
2. si $x \notin A$ alors $\{y \in \{0,1\}^{p(|x|)} \ : \ (x,y) \in B\} = \emptyset$.

Exercice 1. *Very* RP

1. Montrer que $\mathsf{P} \subseteq \mathsf{RP}$.

2. Montrer que le seuil $1/2$ dans le point (1) de la définition de RP peut être remplacé par n'importe quelle constante $0 < \alpha < 1$.

3. Montrer qu'on peut réduire exponentiellement la probabilité d'erreur, c'est-à-dire que pour tout polynôme q, il existe $B \in \mathsf{P}$ et un polynôme p tels que

1. si $x \in A$ alors $|\{y \in \{0,1\}^{p(|x|)} \ : \ (x,y) \notin B\}| \leq 2^{-q(|x|)}.2^{p(|x|)}$;
2. si $x \notin A$ alors $\{y \in \{0,1\}^{p(|x|)} \ : \ (x,y) \in B\} = \emptyset$.

4. Un circuit arithmétique est un circuit comprenant des portes $+$ et $\times$ (au lieu de OR, AND et NOT dans les circuits booléens), ayant pour entrée la constante -1 et ne possédant qu'une sortie. Ainsi, un tel circuit calcule un entier relatif.

On définit le problème NonNul comme suit.
– Entrée : un circuit arithmétique C calculant un entier N.
– Problème : décider si $N \neq 0$.
Pourquoi NonNul n'est pas trivialement dans P ? Montrer que NonNul est dans RP. *Indication : on pourra admettre que le nombre $\pi(x)$ de nombres premiers inférieurs à x est $\geq Cx/\ln x$ pour une certaine constante $C > 0$.*

5. Montrer que $\mathsf{RP} \subseteq \mathsf{NP}$.

6. Montrer que $\mathsf{RP} \subset \mathsf{P/poly}$. Pour cela, on réduira la probabilité d'erreur à $2^{-|x|-1}$ grâce à la question 3, puis on majorera le nombre de uns dans le tableau t défini de la manière suivante : pour $x \in \{0,1\}^n$ et $y \in \{0,1\}^{p(n)}$, $t[x,y] = 1$ si et seulement si ($x \in A$ et $(x,y) \notin B$) (i.e. l'algorithme se trompe).

Définition
Un langage $\mathcal{L}$ est dans $\mathsf{P-sel}$ (pour P sélectif) s'il existe $f : \{0;1\}^* \times \{0;1\}^* \to \{0;1\}^*$ calculable en temps polynomial telle que pour tout (x,y) :

$$\begin{cases} f(x,y) \in \{x,y\} \\ \{x,y\} \cap \mathcal{L} \neq \emptyset \Rightarrow f(x,y) \in \mathcal{L} \end{cases}$$

On dit alors que f est une fonction de sélection pour $\mathcal{L}$.

Exercice 2.

1. Montrer que $\mathsf{P} \subseteq \mathsf{P-sel}$.

2. Montrer que si $\mathcal{L} \in \mathsf{P-sel}$ alors son complémentaire l'est aussi.

Exercice 3.

1. Soit r un réel. Soit $\mathcal{L}$ l'ensemble des uples $b_1...b_n$ d'éléments de $\{0;1\}$ tels que n soit un entier et $0, b_1...b_n \leq r$. Montrer que $\mathcal{L}$ est $\mathsf{P-sel}$.

2. Montrer qu'il existe un langage non récursif dans $\mathsf{P-sel}$.

Exercice 4.

Soit $(M_1,p_1),(M_2,p_2),\ldots$ une énumération récursive de tous les couples (M,p) tels que $p(X)$ soit un polynôme (de la forme X^k) et M une machine de Turing qui pour tout entier n et toute entrée de taille n effectue au plus $p(n)$ pas de calcul.
Soit (w_i) la suite définie par :

$$\begin{cases} w_0 &= 2 \\ w_{2n+1} &= 1 + w_{2n} \\ w_{2n+2} &= 2^{2^{2^{w_{2n}}}} \end{cases}$$

Soit $\mathcal{L}$ le langage minimal tel que pour tous i et m :

$$\begin{cases} M_i(w_{2<i,m>}, w_{2<i,m>+1}) = w_{2<i,m>} & \Rightarrow & w_{2<i,m>+1} \in \mathcal{L} \\ M_i(w_{2<i,m>}, w_{2<i,m>+1}) = w_{2<i,m>+1} & \Rightarrow & w_{2<i,m>} \in \mathcal{L} \end{cases}$$

On peut supposer que l'alphabet d'entrée des machines considérées contient 0, 1 et la virgule.

✎ Montrer que $\mathcal{L}$ est récursif sans être dans $\mathsf{P-sel}$.

Exercice 5.
Nous allons montrer que $\mathsf{P-sel} \subseteq \mathsf{P/poly}$.
On appelle *tournoi* tout graphe complet dont on a orienté les arêtes.

1. Montrer le lemme suivant : si $G = (V_G, E_G)$ est un tournoi de taille k, il existe un sous-ensemble H des sommets de cardinal au plus $\lfloor \log_2(k+1) \rfloor$ tel que pour tout $v \in V_G - H$ il existe $g \in H$ tel que $(v,g) \in E_G$.

2. Soit $\mathcal{L}$ dans $\mathsf{P}-\mathsf{sel}$. Montrer qu'il existe une fonction de sélection f pour $\mathcal{L}$ telle que $\forall x,\, y,\, f(x,y) = f(y,x)$.

3. Soit $\mathcal{L}$ dans $\mathsf{P}-\mathsf{sel}$ et soit une fonction de sélection f pour $\mathcal{L}$ telle que pour tout x et y, $f(x,y) = f(y,x)$. Considérons l'ensemble $\mathcal{L}^{=n}$ des mots de $\mathcal{L}$ de longueur n.
Montrer qu'il existe un sous-ensemble H_n de $\mathcal{L}^{=n}$ de cardinal au plus $n+1$ tel que v appartient à $\mathcal{L}^{=n}$ si et seulement s'il existe un mot g de H_n tel que $f(v,g) = v$.

4. Conclure.

5. Montrer que $\mathsf{P}-\mathsf{sel} \subseteq \mathsf{P}/\mathsf{quad}$.

Exercice 6.

1. Montrer le lemme suivant : si G est un tournoi alors il existe un sommet s tel que tout sommet soit accessible à partir de s par un chemin orienté de longueur au plus deux.

2. Montrer que $\mathsf{P}-\mathsf{sel} \subseteq \mathsf{NP}/\mathsf{lin}$.

3. Montrer que $\mathsf{P}-\mathsf{sel} \subseteq \mathsf{NP}/\mathsf{lin} \cap \mathsf{coNP}/\mathsf{lin}$

4. Soit $\mathsf{NP}/(n+1) = \mathsf{NP}/\{f : n \mapsto n+1\}$. Montrer que $\mathsf{P}-\mathsf{sel} \subseteq \mathsf{NP}/(n+1)$.

Soit $\mathsf{NP}/n = \mathsf{NP}/\{f : n \mapsto n\}$. Nous allons montrer que $\mathsf{P}-\mathsf{sel} \not\subseteq \mathsf{NP}/n$.

Exercice 7.
Soit (l_n) la suite définie par $l_0 = 2$ et $l_{i+1} = 2^{2^{2^{l_i}}}$. On pose $E = \{l_i\}_{i\in\mathbb{N}}$.
L'ensemble des mots est muni de l'ordre lexicographique.

Si $\mathcal{L}$ est un langage, on considère les conditions suivantes :

1. Pour tout mot x de $\mathcal{L}$ la longueur de x est dans E.
2. Pour tous x et y de même longueur, $x \leq y$ et $y \in \mathcal{L}$ implique $x \in \mathcal{L}$.
3. $\mathcal{L} \in DTIME[2^{2^n}]$.

1. Montrer que si $\mathcal{L}$ satisfait les conditions (1), (2) et (3) alors $\mathcal{L}$ est $\mathsf{P}-\mathsf{sel}$.
Pour cela on peut considérer la fonction suivante :

$$f(x,y) = \begin{cases} x & \text{si } |y| \notin E \\ y & \text{si } |y| \in E \wedge |x| \notin E \\ \min\{x,y\} & \text{si } |y| \in E \wedge |x| \in E \wedge |x| = |y| \\ \min\{x,y\} & \text{si } |y| \in E \wedge |x| \in E \wedge |x| \neq |y| \wedge \min\{x,y\} \in \mathcal{L} \\ \max\{x,y\} & \text{si } |y| \in E \wedge |x| \in E \wedge |x| \neq |y| \wedge \min\{x,y\} \notin \mathcal{L} \end{cases}$$

Soit $N_1, N_2 \ldots$ une énumération des machines de Turing non déterministes travaillant en temps polynomial.

2. Soit f une fonction telle que $f \in O(2^{2\ell})$. Montrer que l'on peut choisir l'énumération de telle sorte que le temps de calcul de N_i sur les entrées de taille $2l_i$ soit inférieur à $2^{2^{l_i}}/f(l_i)$.

Pour chaque entier l, on définit $\mathcal{L}^{=l}$ comme suit :
– si $l \notin E$ alors $\mathcal{L}^{=l} = \emptyset$.

– si $l \in E$ et s'il existe x de taille l tel que

$$\forall |y| = l, N_i(\langle x, y \rangle) \text{ est rejeté}$$

alors tous les u de taille l tels que $u \leq x$ sont dans $\mathcal{L}$.
– si $l \in E$ mais qu'un tel x n'existe pas, $\mathcal{L}^{=l} = \emptyset$.

3. Montrer que $\mathcal{L} = \bigcup \mathcal{L}^{=l}$ est dans $\mathsf{P} - \mathsf{sel}$.

4. Montrer que $\mathcal{L} \notin \mathsf{NP}/n$.

5. Soit h une fonction récursive quelconque. Montrer que $\mathsf{P} - \mathsf{sel} \nsubseteq DTIME[h(n)]/n$