TD05 – Une classe très polie

Définition (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. $\forall n \geq 0, |a(n)| \leq f(n)$;
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).

Exercice 1.

1. Montrer que $\mathsf{P} \subseteq \mathsf{P/poly}$.

2. Montrer qu'un langage A est dans $\mathsf{P/poly}$ si et seulement s'il admet une famille de circuits booléens de taille polynomiale.

3. Montrer qu'il existe un langage indécidable dans $\mathsf{P/poly}$.

4. Montrer qu'il existe un langage décidable hors de $\mathsf{P/poly}$. *Indication : on pourra faire une diagonalisation sur l'ensemble des circuits de taille* $\leq n^{\log n}$.

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 2. *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 RP $\subseteq$ NP.

6. Montrer que RP $\subset$ 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 probabiliste se trompe).