TD 13 – Classes de complexité probabilistes et fonctions à sens unique

1 Propriétés des classes de complexité probabilistes

Soit $f\colon \mathbb{N} \to [0,1]$ une fonction.

On définit la classe $\mathsf{RP}_{f(n)}$ comme étant la classe des langages L sur un alphabet Σ quelconque tel qu'il existe un polynôme p et un langage $K \in \mathsf{P}$ vérifiant, pour tout $w \in \Sigma^*$:

$$w \in L \Rightarrow \mathbb{P}_{r\in\{0,1\}^{p(|w|)}}(\langle w, r\rangle \notin K) \leq f(|w|) \ ;$$
$$w \notin L \Rightarrow \mathbb{P}_{r\in\{0,1\}^{p(|w|)}}(\langle w, r\rangle \in K) = 0 \ .$$

De même, on définit la classe $\mathsf{BPP}_{f(n)}$ comme étant la classe des langages L sur un alphabet Σ quelconque tel qu'il existe un polynôme p et un langage $K \in \mathsf{P}$ vérifiant, pour tout $w \in \Sigma^*$:

$$w \in L \Rightarrow \mathbb{P}_{r\in\{0,1\}^{p(|w|)}}(\langle w, r\rangle \notin K) \leq f(|w|) \ ;$$
$$w \notin L \Rightarrow \mathbb{P}_{r\in\{0,1\}^{p(|w|)}}(\langle w, r\rangle \in K) \leq f(|w|) \ .$$

On rappelle que $\mathsf{RP} = \mathsf{RP}_{1/2}$ et $\mathsf{BPP} = \mathsf{BPP}_{1/3}$.

Exercice 1. Montrer que pour toute fonction $f\colon \mathbb{N} \to [0,1]$ vérifiant qu'il existe $c, n_0 \in \mathbb{N}$ tels que $2^{-n^c} \leq f(n) \leq 1 - n^{-c}$ pour tout $n \in \mathbb{N}, n \geq n_0$, on a que $\mathsf{RP} = \mathsf{RP}_{f(n)}$.

Exercice 2. Montrer que pour toute fonction $f\colon \mathbb{N} \to [0,1]$ vérifiant qu'il existe $c, n_0 \in \mathbb{N}$ tels que $2^{-n^c} \leq f(n) \leq \frac{1}{2} - n^{-c}$ pour tout $n \in \mathbb{N}, n \geq n_0$, on a que $\mathsf{BPP} = \mathsf{BPP}_{f(n)}$.

On pourra utiliser le lemme suivant, que l'on pourra admettre.

Lemme 1.1 (Chernoff)**.** *Soit $p \in \left[0, \frac{1}{2}\right[$ et $X_1, \dots, X_n$ ($n \in \mathbb{N}$) des variables aléatoires indépendantes telles que*

$$X_i = \begin{cases} 1 & \text{avec probabilité } p \\ 0 & \text{avec probabilité } 1-p \end{cases}$$

pour tout $i \in [\![1, n]\!]$.

Soit $X = \sum_{i=1}^n X_i$. Alors pour $\epsilon = \frac{1}{2} - p$, on a :

$$\mathbb{P}\Big(X \geq \frac{n}{2}\Big) \leq 2^{-(\epsilon^2/2)n} \ .$$

Exercice 3. Montrer que, d'une part, $\mathsf{RP} \subseteq \mathsf{NP}$ et, d'autre part, $\mathsf{BPP} \subseteq \mathsf{PSPACE}$.

Exercice 4. Montrer que si $\mathsf{NP} \subseteq \mathsf{BPP}$, alors $\mathsf{NP} = \mathsf{RP}$.

Exercice 5. Montrer que $\mathsf{BPP} \subseteq \mathsf{P/poly}$.

2 Un problème dans coRP

On rappelle que le *degré d'un monôme* $aX_1^{d_1} \dots X_n^{d_n}$ est $\sum_{j=1}^n d_j$ et que le *degré d'un polynôme* est le maximum des degrés des monômes le composant. Par exemple $2XXXXY + XYZ - 3Z + 42ZY$ est de degré 5 (car $2XXXXY$ est de degré 5).

Un polynôme peut toujours s'écrire sous la forme de somme de monômes. Un polynôme à coefficients entiers est en *forme générale* quand il est donné comme variable simple (c.-à-d. X_i) ou constante

(c.-à-d. $a \in \mathbb{Z}$), produit ou somme de polynômes à coefficients entiers en forme générale. Par exemple, $\big((X_1 + 2X_2) \times (5X_1 + (-3)X_2) + X_1\big) \times X_1$ est un polynôme à coefficients entiers en forme générale.

On ignore ici volontairement les détails de l'encodage mais on suppose qu'il est non ambigu et que la taille d'un encodage est $\mathrm{O}(\log_2(n))$ pour décrire la n-ième variable, $\mathrm{O}(\log_2(|a| + 1))$ pour décrire une constante $a \in \mathbb{Z}$, et $\mathrm{O}(1) + c_1 + c_2$ pour décrire la somme (ou le produit) de deux polynômes à coefficients entiers de taille d'encodage c_1 et c_2.

Exercice 6. Montrer que la fonction qui transforme un polynôme à coefficients entiers donné en forme générale en un polynôme à coefficients entiers sous forme de somme de monômes ne peut pas être calculée en temps polynomial.

Soit le langage

$$\mathrm{TEP} = \{\langle P_1, P_2\rangle \mid P_1 \text{ et } P_2 \text{ sont deux polynômes à coefficients entiers en forme générale égaux}\}\ .$$

Exercice 7. Montrer ou admettre le lemme suivant.

Lemme 2.1 (Schwartz-Zippel)**.** *Soit $P \in \mathbb{Z}[X_1, \ldots, X_n]$ (avec $n \in \mathbb{N}$) non nul de degré $d \in \mathbb{N}$ et soit S une partie finie de $\mathbb{Z}$. Si $x_1, \ldots, x_n$ sont choisis uniformément aléatoirement dans S, alors $\mathbb{P}\Big(P(x_1, \ldots, x_n) = 0\Big) \leq \frac{d}{|S|}$.*

Exercice 8. En déduire que TEP $\in$ coRP.

3 Fonctions à sens unique

Supposons que :

- on ait une bijection f des entiers sur n bits vers les entiers sur n bits, pour tout $n \in \mathbb{N}$ (c.-à-d., sur une entrée x de n bits, $f(x)$ est un entier sur n bits tel que $f(x) = f(y) \Rightarrow x = y$) ;
- la fonction f se calcule en temps polynomial ;
- la fonction inverse de f ne peut pas se calculer en temps polynomial.

On dit que f est une fonction à sens unique.

Exercice 9. Montrer que si une telle bijection existe, alors P $\neq$ NP.

Indication : Montrer que le langage $L = \{\langle x, f(y)\rangle \mid x, y \in \{0,1\}^*, |x| = |y| \wedge x \leq y\}$ appartient à NP $\setminus$ P.

Exercice 10. Montrer de plus que, si elle existe, alors NP $\cap$ coNP $\neq$ P.