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 $\mathsf{RP} = \mathsf{RP}_{f(n)}$.

Solution 1. On montre que pour toute fonction $f\colon \mathbb{N} \to [0,1]$ vérifiant qu'il existe $c, n_0 \in \mathbb{N}$ tels que $f(n) \leq 1 - n^{-c}$ pour tout $n \in \mathbb{N}, n \geq n_0$, l'erreur peut être réduite à $2^{-n^{c'}}$ pour tout $c' \in \mathbb{N}$ en exécutant $n^{c+c'}$ fois la MT pour le langage initial sur des chaînes de bits aléatoires indépendantes et en acceptant si et seulement si au moins l'une de ces exécutions accepte.

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 $X_1, \ldots, X_n$ ($n \in \mathbb{N}$) 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 :

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

Solution 2. On montre que pour toute fonction $f\colon \mathbb{N} \to [0,1]$ vérifiant qu'il existe $c, n_0 \in \mathbb{N}$ tels que $f(n) \leq 1 - n^{-c}$ pour tout $n \in \mathbb{N}, n \geq n_0$, l'erreur peut être réduite à $2^{-n^{c'}}$ pour tout $c' \in \mathbb{N}$ en exécutant $2n^{2c+c'}$ fois la MT pour le langage initial sur des chaînes de bits aléatoires indépendantes et en acceptant si et seulement si au moins la moitié des exécutions accepte.

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

Solution 3. Le fait que $\mathsf{RP} \subseteq \mathsf{NP}$ suit directement de la définition de NP en termes de vérificateur en temps polynomial.

Soit $L \in \mathsf{BPP}$ un langage sur un alphabet Σ. Il existe donc un polynôme p et un langage $K \in \mathsf{P}$ vérifiant, pour tout $w \in \Sigma^*$:

$$w \in L \Rightarrow \mathbb{P}_{r \in \{0,1\}^{p(|w|)}}(\langle w, r\rangle \notin K) \leq \frac{1}{3} \ ;$$
$$w \notin L \Rightarrow \mathbb{P}_{r \in \{0,1\}^{p(|w|)}}(\langle w, r\rangle \in K) \leq \frac{1}{3} \ .$$

Soit $\mathcal{M}$ une MT décidant K en temps polynomial. Pour décider L en espace polynomial, on construit une MT qui pour tout $w \in \Sigma^*$ se comporte selon l'algorithme suivant sur l'entrée w :

$c \leftarrow 0$
pour $r \in \{0,1\}^{p(|w|)}$ **faire**
  si $\mathcal{M}(\langle w, r\rangle)$ accepte **alors**
    $c \leftarrow c + 1$
  fin si
fin pour
si $c \geq 2^{p(|w|)-1}$ **alors**
  accepter
sinon
  rejeter
fin si.

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

Solution 4. Supposons que $\mathrm{SAT} \in \mathsf{BPP}$. Il existe donc un polynôme p et un langage $K \in \mathsf{P}$ vérifiant, pour toute formule booléenne φ à $n \in \mathbb{N}_{>0}$ variables :

$$\langle\varphi\rangle \in \mathrm{SAT} \Rightarrow \mathbb{P}_{r \in \{0,1\}^{p(|\langle\varphi\rangle|)}}(\langle\langle\varphi\rangle, r\rangle \notin K) \leq \frac{1}{2n} \ ;$$
$$\langle\varphi\rangle \notin \mathrm{SAT} \Rightarrow \mathbb{P}_{r \in \{0,1\}^{p(|\langle\varphi\rangle|)}}(\langle\langle\varphi\rangle, r\rangle \in K) \leq \frac{1}{2n} \ .$$

Soit $\mathcal{M}$ une MT décidant K en temps polynomial. Soit également un polynôme q tel que pour tout $l \in \mathbb{N}$, si φ est une formule booléenne avec $n \in \mathbb{N}_{>0}$ variables de longueur d'encodage l, alors $q(l)$ majore la longueur d'encodage de toute formule booléenne obtenue par conjonction de φ et d'un monôme avec au plus n littéraux. On construit une MT $\mathcal{M}'$ qui pour toute formule booléenne φ à $n \in \mathbb{N}_{>0}$ variables et $r \in \{0,1\}^{n \cdot q(|\langle\varphi\rangle|)}$ se comporte selon l'algorithme suivant sur l'entrée $\langle\langle\varphi\rangle, r\rangle$:

$\varphi' \leftarrow \varphi$
pour i de 1 à n **faire**
  si $\mathcal{M}(\langle\langle\varphi' \wedge \neg x_i\rangle, r_{(i-1)\cdot q(|\langle\varphi\rangle|)+1} \cdots r_{(i-1)\cdot q(|\langle\varphi\rangle|)+p(|\langle\varphi' \wedge \neg x_i\rangle|)}\rangle)$ accepte **alors**
    $a_i \leftarrow \bot$
    $\varphi' \leftarrow \varphi' \wedge \neg x_i$
  sinon
    $a_i \leftarrow \top$
    $\varphi' \leftarrow \varphi' \wedge x_i$
  fin si
fin pour
si $(a_1, \ldots, a_n)$ est une affectation satisfaisant φ **alors**
  accepter
sinon
  rejeter
fin si.

La MT $\mathcal{M}'$ décide un langage K' en temps polynomial. Soit maintenant une formule booléenne φ à $n \in \mathbb{N}_{>0}$ variables. Si $\langle\varphi\rangle \notin \mathrm{SAT}$, alors il est évident que

$$\mathbb{P}_{r \in \{0,1\}^{n \cdot q(|\langle\varphi\rangle|)}}(\langle\langle\varphi\rangle, r\rangle \in K') = 0 \ .$$

Si $\langle\varphi\rangle \in \mathrm{SAT}$, alors soit $(b_1, \ldots, b_n) \in \{0,1\}^n$ la plus petite affectation selon l'ordre lexicographique satisfaisant φ. Pour tout $i \in [\![1, n]\!]$, nous allons majorer la probabilité $\mathbb{P}_{r\in\{0,1\}^{n\cdot q(|\langle\varphi\rangle|)}}(a_i \neq b_i \mid \bigwedge_{j=1}^{i-1} a_j = b_j)$ qu'au cours de l'exécution de $\mathcal{M}'$ sur $\langle\langle\varphi\rangle, r\rangle$ avec r tiré uniformément aléatoirement dans $\{0,1\}^{n\cdot q(|\langle\varphi\rangle|)}$, à l'étape i la valeur obtenue pour a_i est différente de b_i, sachant que les valeurs obtenues aux étapes précédentes sont $b_1, \ldots, b_{i-1}$. Si $b_i = \bot$, alors $\langle\varphi' \wedge \neg x_i\rangle \in \mathrm{SAT}$ et donc cette probabilité est majorée par $\frac{1}{2n}$. Si, au contraire, $b_i = \top$, alors $\langle\varphi' \wedge \neg x_i\rangle \notin \mathrm{SAT}$ par minimalité de $(b_1, \ldots, b_n)$ et donc cette probabilité est aussi majorée par $\frac{1}{2n}$. Ainsi donc, on a que

$$\begin{aligned}
\mathbb{P}_{r\in\{0,1\}^{n\cdot q(|\langle\varphi\rangle|)}}(\langle\langle\varphi\rangle, r\rangle \notin K') &\leq \mathbb{P}_{r\in\{0,1\}^{n\cdot q(|\langle\varphi\rangle|)}}(\exists i \in [\![1, n]\!], a_i \neq b_i) \\
&= \sum_{i=1}^{n} \mathbb{P}_{r\in\{0,1\}^{n\cdot q(|\langle\varphi\rangle|)}}\Big(a_i \neq b_i \wedge \bigwedge_{j=1}^{i-1} a_j = b_j\Big) \\
&\leq \sum_{i=1}^{n} \mathbb{P}_{r\in\{0,1\}^{n\cdot q(|\langle\varphi\rangle|)}}\Big(a_i \neq b_i \;\Big|\; \bigwedge_{j=1}^{i-1} a_j = b_j\Big) \\
&= \frac{1}{2} \ .
\end{aligned}$$

Ceci achève de montrer que $\mathrm{SAT} \in \mathsf{RP}$ et on peut ensuite conclure par NP-complétude de SAT et clôture de RP par réduction en temps polynomial.

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

Solution 5. Soit $L \in \mathsf{BPP}$ un langage sur un alphabet Σ. Il existe donc un polynôme p et un langage $K \in \mathsf{P}$ vérifiant, pour tout $w \in \Sigma^*$:

$$\begin{aligned}
w \in L &\Rightarrow \mathbb{P}_{r\in\{0,1\}^{p(|w|)}}(\langle w, r\rangle \notin K) \leq |\Sigma|^{-n-1} \ ; \\
w \notin L &\Rightarrow \mathbb{P}_{r\in\{0,1\}^{p(|w|)}}(\langle w, r\rangle \in K) \leq |\Sigma|^{-n-1} \ .
\end{aligned}$$

Ainsi, pour tout $n \in \mathbb{N}$, on a :

$$\begin{aligned}
&\mathbb{P}_{r\in\{0,1\}^{p(n)}}\big(\exists w \in \Sigma^n, (w \in L \wedge \langle w, r\rangle \notin K) \vee (w \notin L \wedge \langle w, r\rangle \in K)\big) \\
\leq &\sum_{w\in\Sigma^n} \mathbb{P}_{r\in\{0,1\}^{p(n)}}\big((w \in L \wedge \langle w, r\rangle \notin K) \vee (w \notin L \wedge \langle w, r\rangle \in K)\big) \\
\leq &|\Sigma|^{-1} \ .
\end{aligned}$$

Par conséquent, pour tout $n \in \mathbb{N}$, il existe $r_n \in \{0,1\}^{p(n)}$ tel que pour tout $w \in \Sigma^n$, on ait que $w \in L$ si et seulement si $\langle w, r_n\rangle \in K$. On suppose qu'il existe un polynôme q tel que pour tout $n \in \mathbb{N}$, on ait $q(n) = |\langle w, r_n\rangle|$ quel que soit $w \in \Sigma^n$. Vu qu'il existe une suite de circuits booléens $(D_n)_{n\in\mathbb{N}}$ de taille polynomiale décidant K, on peut construire la suite de circuits booléens $(C_n)_{n\in\mathbb{N}}$ tels que pour tout $n \in \mathbb{N}$, on ait que $C_n(w) = D_{q(n)}(\langle w, r_n\rangle)$ pour tout $w \in \Sigma^n$. Cette dernière suite de circuits de taille polynomiale décide L, d'où $L \in \mathsf{P/poly}$.

2 Un problème dans coRP

On rappelle que le *degré d'un monôme* $aX_1^{d_1} \ldots X_n^{d_n}$ 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 $O(1) + c_1 + c_2$ 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.

Solution 6. Considérons le polynôme $(X_1+X_2)\times(X_3+X_4)\times\cdots\times(X_{n-1}+X_n)$: sa taille d'encodage est $O(n\log_2(n))$, mais sa forme développée a 2^n monômes de degré n, soit une taille d'encodage en $\Omega(n\log_2(n)2^n)$.

Soit le langage

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

Exercice 7. Montrer ou admettre le lemme suivant.

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

Solution 7. On montre le résultat par récurrence sur le nombre n de variables.

— Pour $n=0$, le lemme suit directement car $d=0$ et $P=a$ avec $a \in \mathbb{Z}, a \neq 0$.

— Pour $n+1$ avec $n \in \mathbb{N}$, on a qu'il existe $P_0,\dots,P_d \in \mathbb{Z}[X_1,\dots,X_n]$ tels que

$$P = \sum_{i=0}^{d} {X_{n+1}}^{d-i} P_i(X_1,\dots,X_n) .$$

Comme P est non nul, on a que l'un des P_i est non nul, et l'on prend le plus petit tel i. Pour que P s'annule en un certain $(x_1,\dots,x_n,x_{n+1}) \in S^{n+1}$, il faut soit que le polynôme P_i de degré au plus i s'annule en $(x_1,\dots,x_n)$, soit que le polynôme $P(x_1,\dots,x_n,X_{n+1})$ en la variable X_{n+1} non nul de degré $d-i$ s'annule en x_{n+1}.
Par récurrence on a

$$\mathbb{P}\Big(P_i(x_1,\dots,x_n)=0\Big) \leq \frac{i}{|S|}$$

et puisque $P(x_1,\dots,x_n,X_{n+1})$ est un polynôme à une variable de degré $d-i$ et a donc au plus $d-i$ racines, on a

$$\mathbb{P}\Big(P(x_1,\dots,x_n,x_{n+1})=0 \;\Big|\; P_i(x_1,\dots,x_n)\neq 0\Big) \leq \frac{d-i}{|S|} .$$

Par conséquent,

$$\begin{aligned}
&\mathbb{P}\Big(P(x_1,\dots,x_n)=0\Big)\\
\leq&\mathbb{P}\Big(P_i(x_1,\dots,x_n)=0\Big) + \mathbb{P}\Big(P(x_1,\dots,x_n,x_{n+1})=0 \;\Big|\; P_i(x_1,\dots,x_n)\neq 0\Big)\\
\leq&\frac{d}{|S|} .
\end{aligned}$$

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

Solution 8. Étant donné P_1 et P_2 des polynômes à coefficients entiers en forme générale, on procède de la façon suivante. On pose $P = P_1 + (-1)P_2$ et on calcule d le degré maximal de P. On choisit $x_1,\dots,x_n$ uniformément aléatoirement dans $S = [\![1, 2d]\!]$ et on accepte si $P(x_1,\dots,x_n)=0$, autrement on rejette. Puisque P est nul si et seulement si P_1 et P_2 sont égaux, il s'ensuit que si P_1 et P_2 sont égaux, alors on rejette avec probabilité 0 et que si P_1 et P_2 sont différents, alors on accepte avec probabilité au plus $\frac{1}{2}$.

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 $\mathsf{P} \neq \mathsf{NP}$.

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* $\mathsf{NP} \setminus \mathsf{P}$.

Solution 9. L est dans NP en considérant le certificat comme étant $\langle x, y\rangle$ pour $\langle x, f(y)\rangle \in L$.

Si L était dans P, alors étant donné $z \in \{0,1\}^*$ de longueur $n \in \mathbb{N}$, on pourrait chercher par dichotomie sur $\{0,1\}^n$ le plus grand x tel que $\langle x, z\rangle$ est dans le langage L, qui est nécessairement $y \in \{0,1\}^n$ tel que $z = f(y)$. On pourrait alors calculer la fonction inverse de f en temps polynomial, ce qui est supposé impossible.

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

Solution 10. On montre facilement que $\bar{L} \in \mathsf{NP}$, ce qui implique que $L \in \mathsf{coNP}$ et donc que $L \in \mathsf{NP} \cap \mathsf{coNP} \setminus \mathsf{P}$.