

Classes Probabilistes & Non-Uniformes PC 7.

1 Simulation de lois aléatoires

1. Montrer que l'on peut simuler un tirage aléatoire dans $\{1, 2, \dots, N, ?\}$ avec une pièce : i.e. pour tout N et $\delta > 0$, il existe un algorithme probabiliste A , qui fonctionne en temps polynomiale en $\log N \log(1/\delta)$, qui renvoie un élément de $\{1, 2, \dots, N, ?\}$ tel que
 - lorsqu'il ne renvoie pas $?$, la sortie de A est uniformément distribuée dans $\{1, 2, \dots, N\}$
 - la probabilité que A renvoie $?$ est au plus δ .
2. Soit X une variable aléatoire de fonction de répartition F strictement croissante. Rappel : la fonction F est définie par $F(x) = \Pr(X \leq x)$ strictement croissante. Montrer que $F(X)$ se comporte comme une loi uniforme sur $[0, 1]$.
3. En déduire un moyen de simuler une loi lorsqu'on connaît F^{-1} : par exemple, une loi exponentielle.

2 Problèmes complets pour PP

1. Montrer que PP est close par réduction polynomiale.
2. Le problème de décision MAJ consiste, étant donnée une formule booléenne à décider si elle est satisfaite par plus de la moitié des affectations de variables. Prouver que MAJ \in PP.
3. Le problème de décision #SAT consiste, étant donnée une formule booléenne F , et un entier i , à déterminer si F est satisfaite par plus de i affectations de variables. Montrer que #SAT est PP-difficile.
4. En déduire que MAJ et #SAT sont PP-complets.
5. Existe-t'il des problèmes BPP-complets ?

3 Classe \mathbb{P}

On rappelle que \mathbb{P} correspond aux langages reconnus par une famille de circuits booléens de taille polynomiale.

1. Montrer que \mathbb{P} contient des langages indécidables.

2. Un langage L est dit *creux* lorsqu'il existe un polynôme p tel que, pour tout n , il y a moins de $p(n)$ mots dans L de longueur n .
Montrer que tout langage creux est dans \mathbb{P} .

4 $\mathbb{P} = \mathbb{P}/poly$

Soit \mathcal{C} une classe de problèmes sur l'alphabet fini M . Soit $poly$ la classe des fonctions f de \mathbb{N} dans M^* telle que pour un certain polynôme p , $|f(n)| \leq p(n)$.

La classe $\mathcal{C}/poly$ est la classe des problèmes B tels qu'il existe un problème $A \in \mathcal{C}$ et une fonction $f \in poly$ telle que $x \in B$ si et seulement si $\langle x, f(|x|) \rangle \in A$.

1. Prouver que $\mathbb{P}/poly \subset \mathbb{P}$.
2. Prouver que $\mathbb{P} \subset \mathbb{P}/poly$.
3. En déduire que

$$\mathbb{P} = \mathbb{P}/poly.$$