

1 Classes de complexité

Exercice 1: PP La définition de PP n'est pas immédiatement stable par complémentation. On peut envisager deux "variantes", qui le sont:

1. Qu'obtient-on si on relâche légèrement l'exigence et qu'on se contente d'une probabilité d'erreur *inférieure ou égale* à $1/2$?
2. Même question si on demande que, pour toute instance, la probabilité d'erreur soit strictement inférieure à $1/2$.

Exercice 2: réduction d'erreur bilatérale On cherche à démontrer que, pour $0 < p < p' < 1/2$, on a $BPP(p') \subset BPP(p)$. On suppose donc qu'on a un algorithme A (polynomial) de probabilité d'erreur bornée par p' , et on en cherche un autre (toujours polynomial) de probabilité d'erreur bornée par p .

1. Pour une instance x quelconque, et un entier k , soit N le nombre de mauvaises réponses dans k répétitions indépendantes de A sur x . Montrer que l'espérance de N est majorée par $k \cdot p'$, et son écart-type par $\sqrt{k}/2$.
2. En déduire une valeur de k (en fonction de p et p') qui garantisse que la probabilité que la mauvaise réponse soit majoritaire, est inférieure à p .

Exercice 3: BPP, RP Dans la définition standard de RP, on demande l'existence d'algorithme à *temps polynomial*, avec erreur unilatérale et probabilité d'erreur bornée par $1/2$.

Montrer qu'on obtient la même classe de problèmes si on remplace la contrainte sur le temps par *temps moyen polynomial*.

On pourra faire de même pour BPP.

Exercice 4: Montrer l'identité $ZPP = RP \cap \text{co-RP}$.

2 Simulabilité exacte de lois

Exercice 5: Simulation d'une Bernoulli de paramètre $1/3$

1. Donner un algorithme de simulation exacte d'une variable de Bernoulli de paramètre $1/3$, utilisant en moyenne 2 bits aléatoires. Identifier la loi du nombre de bits aléatoires utilisés.

2. (*Optimalité forte*) Montrer que, pour tout entier k , tout algorithme de simulation exacte d'une Bernoulli de paramètre $1/3$ a probabilité au moins $1/2^k$ d'utiliser au moins k bits aléatoires.
3. *Caractériser* les réels p , $0 < p < 1$, tels qu'il existe un simulateur de variables de Bernoulli de paramètre p utilisant en moyenne strictement moins de 2 bits aléatoires.

Exercice 6: Simulation d'une Bernoulli de paramètre $p = a/b$ Une idée naturelle pour obtenir une Bernoulli de paramètre a/b (avec a et b entiers) est de tirer un entier uniforme entre 0 et $b - 1$, et de retourner 1 si l'entier est entre 0 et $a - 1$, 0 sinon.

1. Proposer un algorithme simple pour tirer un entier uniforme entre 0 et $b - 1$, dans le cas où b est une puissance de 2. Combien cela coûte-t-il de flips?
2. Même question, dans le cas plus général où b n'est pas une puissance de 2.

Exercice 7: Voici un générateur de Bernoulli; déterminer son paramètre:

- $v = 0, u = 1$
- Répéter:
 - $v = 2v + \text{flip}()$
 - $u = 2u$
 - Si $v^2 \geq u$, retourner 0
 - Si $(v + 1)^2 \leq u$, retourner 1

Exercice 8: On considère la loi μ_2 définie comme la loi de la somme de deux variables aléatoires indépendantes, uniformes sur $[0, 1]$.

1. Montrer que, si U_1 et U_2 sont deux variables aléatoires indépendantes, uniformes sur $[0, 1]$, alors $V = U_2 + \mathbf{1}_{U_1 \geq U_2}$ est de loi μ_2
2. Écrire un générateur “par prolongement” de loi μ_2 .
3. Chercher une généralisation au cas de la somme de trois uniformes indépendantes.