TD 12 – Probablement le dernier

Exercice 1. *Amusons nous avec les définitions...*

1. Montrer que dans la définition de BPP, on peut remplacer la constante $2/3$ par $f(|x|)$ où f est n'importe quelle fonction vérifiant $1/2 + n^{-c} \leq f(n) \leq 1 - 2^{-n^d}$ avec $c, d > 0$.
2. A-t-on les mêmes bornes pour RP ?
3. Montrer que les trois définitions suivantes définissent bien la même classe ZPP :
   1. ZPP est la classe des langages tels qu'il existe une MTP polynomiale qui donne la bonne réponse avec probabilité au moins $1/2$, et répond « je ne sais pas » sinon ;
   2. ZPP est la classe des langages tels qu'il existe une MTP qui donne toujours la bonne réponse et dont l'espérance du temps de calcul est polynomiale ;
   3. $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.
4. Montrer que $\mathsf{RP} \subseteq \mathsf{NP}$.
5. Et $\mathsf{RP} \subseteq \mathsf{P/poly}$?

Exercice 2. *Biaise-main*

Une ρ-pièce est une pièce biaisée telle que $\mathbb{P}[\textsc{Face}] = \rho$.

1. Montrer qu'une ρ-pièce peut être simulée par une MTP en temps espéré $O(1)$ si le i-ème bit de ρ est calculable en temps $\mathsf{poly}(i)$.
2. (Méthode de Von Neumann) Inversement, montrer qu'on peut simuler une $1/2$-pièce avec une ρ-pièce en temps espéré $O(1/\rho(1-\rho))$.
3. Proposer une méthode pour améliorer l'espérance du temps de fonctionnement.
4. Donner un réel ρ tel qu'une MTP utilisant une ρ-pièce peut décider un langage indécidable.
5. Montrer qu'on peut simuler un tirage aléatoire dans $\{1, \dots, N\}$ avec une pièce : pour tout N et $\delta > 0$, il existe un algorithme probabiliste A, polynomial en $\log(N)\log(1/\delta)$, qui renvoie un élément de $\{1, \dots, N, ?\}$ tel que
   1. lorsqu'il ne renvoie pas ?, la sortie de A est uniformément distribuée dans $\{1, \dots, N\}$;
   2. La probabilité que A renvoie ? est au plus δ.

Exercice 3. *Dessins !*

Justifier toutes les inclusions suivantes :