TD 09 – Eh bé, pépé !

Exercice 1. *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 $\mathcal{O}(1)$ 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 $\mathcal{O}(1/\rho(1-\rho))$.
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 la probabilité que A renvoie ? est au plus δ, et les autres éléments sont équiprobables.

Exercice 2. *Probablement Jivaro*

Un langage B **se réduit en temps polynomial probabiliste** à un langage C, noté $B \leq_r C$, s'il existe une MTP M tel que pour tout $x \in \{0,1\}^\star$, $\mathbb{P}[C(M(x)) = B(x)] \geq 2/3$. Pour une classe de complexité $\mathcal{C}$, on définit $\mathsf{BP} \cdot \mathcal{C} = \{L \subset \{0,1\}^\star : \exists C \in \mathcal{C}, L \leq_r C\}$.

1. La réduction probabiliste est-elle transitive ?
2. Montrer que si $B \leq_r C$ et $C \in \mathsf{BPP}$, alors $B \in \mathsf{BPP}$.
3. Montrer que $\mathsf{BP} \cdot \mathsf{P} = \mathsf{BPP}$.

Un **circuit non déterministe** est un circuit C à deux entrées x et y qui accepte un mot x s'il existe y tel que $C(x, y) = 1$.

4. Définir $\mathsf{NP/poly}$ et montrer que $\mathsf{BP} \cdot \mathsf{NP} \subseteq \mathsf{NP/poly}$.

Exercice 3. *Sat alors !*

Soit PP la classe des langages L décidés par une MTP M telle que $\mathbb{P}[M(x) = L(x)] > 1/2$. On considère les variantes suivantes du langage Sat :

$$\textsc{MajSat} = \{\phi : \phi \text{ est satisfaite par } > 1/2 \text{ de ses assignations}\}$$
$$\#\textsc{Sat} = \{(\phi, k) : \phi \text{ est satisfaite par } > k \text{ assignations}\}$$

1. Comparer BPP et PP.
2. Montrer que $\textsc{MajSat} \in \mathsf{PP}$.
3. Montrer que $\#\textsc{Sat} \leq_p \textsc{MajSat}$.
4. Montrer que $\#\textsc{Sat}$ et $\textsc{MajSat}$ sont PP-complets.

Exercice 4. *Inclusions probabilistes*

Justifier les inclusions suivantes, et retenir ce dessin :