

TD D: BPP et circuits

DEA d'Algorithmique – Complexité

exo 1: à préparer vers le 12/11/03; le reste en séance

Définition $L \subseteq \{0;1\}^*$ est de la classe P/n^k (autre nom P/Poly s'il existe une relation $R \subset \{0;1\}^* \times \{0;1\}^*$ de la classe P et une "fonction de conseil (*advice*)" $A : \mathbb{N} \rightarrow \{0;1\}^*$, telle que $A(n) \leq n^k$ pour un certain k , telles que

$$x \in L \Leftrightarrow R(x, A(|x|))$$

1. Prouvez que $L \in P/n^k$ si et seulement si sa complexité de circuit est polynomiale.
2. Montrez que si $L \in BPP$, alors il existe un algorithme probabiliste polynomial M avec la probabilité d'erreur sur un x de longueur n inférieure à 2^{-2n} .
3. Déduisez qu'il existe une séquence des choix aléatoires pour laquelle M ne se trompe sur aucun x de longueur n .
4. Déduisez que $BPP \subset P/n^k$