Complexité structurelle – TD 11
Protocoles interactifs et Arthur-Merlin

Exercice 1
Montrer que dans un protocole Arthur-Merlin, on peut remplacer sans perte de généralité le seuil d'acceptation 3/4 par toute constante $c \in]1/2, 1[$.

On note $IP_k(log, log)$ l'ensemble des langages L reconnus par un protocole interactif à k tours lors duquel le vérificateur utilise $r(n) = O(\log n)$ bits aléatoires, et dans lequel chaque question et chaque réponse est de taille $q(n) = O(\log n)$. On suppose en outre que les prouveurs sont déterministes (sans perte de généralité comme on l'a vu au précédent TD).
Exercice 2 Le but de cet exercice est de montrer que pour tout $k \geq 2$, on a

$$IP_k(log, log) \subseteq AM_{O(k)}.$$

1. Soit V le vérificateur d'un protocole $IP_k(log, log)$. Soit α la suite de taille $r(n)$ des bits aléatoires utilisés par V. Montrer que la connaissance de α ainsi que des réponses $z_1, \ldots, z_k$ du prouveur suffit à simuler en temps polynomial l'exécution de V.
   Pour un prouveur P, on note $h_{x,\alpha,P}$ le mot $y_1 z_1 \ldots y_k z_k$ constitué des questions y_i et des réponses z_i successives de V et P pour l'exécution de V selon les choix aléatoires α et sur l'entrée x. On dit que $h_{x,\alpha,P}$ est acceptant si la suite de ces choix aléatoires, questions et réponses fait que V accepte x.
2. Pour un prouveur P et un mot s, on note $A(s, x, P)$ l'ensemble des mots α de taille $r(n)$ tels que $h_{x,\alpha,P}$ soit acceptant et s soit un préfixe de $h_{x,\alpha,P}$. Selon le prouveur P, que dire de $|A(\epsilon, x, P)|$?
3. Montrer que si $|s| = 2iq(n)$ avec $0 \leq i \leq k-1$, alors pour tout P,
$$|A(s, x, P)| = \sum_{|y|=q(n)} |A(sy, x, P)| = \sum_{|y|=q(n)} \left(\max_{|z|=q(n)} |A(syz, x, P)| \right).$$
4. En utilisant l'égalité précédente, proposer un protocole Arthur-Merlin pour un langage $L \in IP_k(log, log)$, dans lequel Merlin essaye de convaincre Arthur que si le protocole $IP_k(log, log)$ pour L tourne sur l'entrée x, alors $|A(\epsilon, x, P)| > \mu 2^{r(n)}$, où μ est le seuil d'acceptation du protocole (c'est-à-dire qu'il essaye de convaincre Arthur que le protocole interactif accepte x). On pourra simuler le protocole interactif étape par étape et utiliser le fait que $q(n)$ et $r(n)$ sont logarithmiques.
5. Montrer que le protocole fonctionne correctement pour les entrées $x \in L$.
6. Montrer que le protocole fonctionne correctement pour les entrées $x \notin L$. On pourra étudier les probabilités qu'Arthur accepte en partant de l'étape i et en connaissant le début de l'exécution.
7. Conclure.

On note AM la classe des langages reconnus par un protocole Arthur-Merlin sans borne sur le nombre de tours (c'est-à-dire que le nombre de tours est polynomial).
Exercice 3
En utilisant judicieusement le même protocole que dans l'exercice précédent, montrer l'égalité

$$IP = AM.$$