M1, 2005–2006

Complexité structurelle – TD 10
Protocoles interactifs

Exercice 1
Montrer que l'on peut supposer sans perte de généralité que dans un protocole interactif les réponses du prouveur sont de taille 1 (de simples bits).

Exercice 2
Montrer que l'on peut supposer sans perte de généralité que dans un protocole interactif le prouveur est déterministe (par opposition à probabiliste). En d'autres termes, il s'agit de transformer un protocole avec un prouveur probabiliste qui convainc le vérificateur avec probabilité $\geq 3/4$ en un protocole avec un prouveur déterministe qui convainc le vérificateur avec probabilité $\geq 3/4$.

Exercice 3
1. Proposer une définition naturelle de protocoles à plusieurs prouveurs qui ne peuvent pas communiquer entre eux (MIP).
2. Proposer une définition naturelle de protocoles avec un seul prouveur, mais qui se comporte comme un oracle. On appelera un tel protocole *probabiliste à oracle*.
3. Méditer sur la différence entre les deux définitions.
4. Montrer qu'un protocole MIP à $k \geq 2$ prouveurs peut être simulé par un protocole probabiliste à oracle.
5. Proposer un protocole MIP à deux prouveurs pour simuler un protocole probabiliste à oracle.
6. Montrer que ce protocole est correct. On rappelle l'inégalité de Tchebychev :
$$\Pr(|X - E(X)| \geq \delta) \leq \frac{\mathrm{Var}(X)}{\delta^2}.$$
7. En déduire qu'un langage est dans MIP si et seulement s'il est reconnu par un protocole probabiliste à oracle.
8. Combien de prouveurs sont nécessaires pour capturer toute la puissance de MIP ?