TD14 - Interactive proofs : Arthur et Merlin contre Prouveur et Vérifieur

Exercice 1. *Graph non isomorphism*

1. Rappeler le protocole vu en cours pour la vérification que deux graphes ne sont pas isomorphes. Constater que ce protocole montre que GNI est dans IP, mais pas que GNI est dans AM.

2. Soient G_1 et G_2 deux graphes à n sommets. Quel est le cardinal de l'ensemble

$$\{(H, \pi) : (H \cong G_1) \vee (H \cong G_2), \pi \in aut(H)\}$$

En déduire une caractérisation de l'isomorphisme de G_1 et G_2.

On est donc ramené à un problème d'estimation du cardinal d'un ensemble.

Définition : Fonctions de hashage indépendantes deux à deux.
Soit $H_{n,k}$ un ensemble de fonctions de $\{0,1\}^n$ dans $\{0,1\}^k$. $H_{n,k}$ est appelé un ensemble de fonctions de hashage indépendantes deux à deux si pour tout x, x' dans $\{0,1\}^n$, si x et x' sont différents, alors pour tout y, y' dans $\{0,1\}^k$, $\Pr_{h \in H_{n,k}}[h(x) = y \wedge h(x') = y'] = 2^-2k$

3. Montrer le théorème suivant :

Théorème : Soit $H_{n,n}$ l'ensemble $\{h_{a,b}\}_{a,b \in \{0,1\}^n}$, où pour tous a et b dans $\{0,1\}^n$, la fonction $h_{a,b}$ est définie par $h_{a,b}(x) = ax + b$. Alors $H_{n,n}$ est une collection de fonctions de hashage indépendantes deux à deux.

4. Proposer un protocole AM qui pour un ensemble $S \subseteq \{0,1\}^n$ tel que Arthur sait vérifier (éventuellement avec un certificat de Merlin) l'appartenance à S, et un nombre K compris entre 2^{k-2} et 2^{k-1}, permet de déterminer si $|S| \geq K$ ou si $|S| \leq K/2$ "assez sûrement".

5. Montrer que le protocole précédent accepte avec une probabilité $\geq 3/8$ si $|S| \geq K$, et avec une probabilité $\leq 1/4$ si $|S| \leq K/2$.

6. Conclure : montrer que GNI est dans AM[2].

Exercice 2. *Protocoles particuliers : zero knowledge proofs*
Les protocoles zéro-knowledge vérifient les deux conditions de *completeness* et de *soundness* des protocoles précédents, mais aussi la condition suivante : le vérifieur n'apprend rien d'autre du prouveur que l'appartenance du mot au langage décidé. Formellement, pour un langage L **dans NP**, si M est la machine telle que $x \in L \Leftrightarrow \exists y : M(x, y) = 1$,
Une paire P, V de protocoles probabilistes interactifs est appelée une preuve *zero-knowledge* pour L si les conditions suivantes sont vérifiées :

$$\forall (x, u) : M(x, u) = 1, \ \Pr[\text{out}_V\langle V(x), P(x, u)\rangle = 1] \geq 2/3 \quad (1)$$

$$\forall x \notin L, \forall P^*, \forall u, \ \Pr[\text{out}_V\langle V(x), P^*(x, u)\rangle = 1] \leq 1/3 \quad (2)$$

Ainsi que la condition de zero-knowledge : pour tout vérifieur V^*, il existe un algorithme probabiliste S^* tel que pour tout $x \in L$ et certificat u pour x,

$$\text{out}_{V^*}\langle V^*(x), P(x, u)\rangle \equiv S^*(x)$$

Où $\equiv$ veut dire que ces deux variables aléatoires sont identiquement distribuées. S^* est appelé le simulateur de V^*.

✎ Montrer que le protocole suivant est un protocole *zero-knowledge* pour Graph Isomorphism :

Entrée x : une paire de graphes G_0, G_1 à n sommets (représentés par leur matrice d'adjacence).

Certificat u que connaît le prouveur : $\pi : [n] \to [n]$ tel que $G_1 = \pi(G_0)$,

Premier message du prouveur : le prouveur choisit au hasard une permuation $\pi_1 : [n] \to [n]$ et envoie au vérificateur le graphe $\pi_1(G1)$.

Message du vérifieur : le vérifieur tire une pièce $b \in \{0, 1\}$ et l'envoie au prouveur.

Dernier message du prouveur : Si $b = 1$, le prouveur envoie π_1 au vérificateur. Si $b = 0$, le prouveur envoie $\pi_1 \circ \pi$.

Vérification du prouveur : Soit H le graphe envoyé dans le premier message, et π^* la permutation reçue dans le dernier message, le vérificateur accepte ssi $H = \pi^*(G_b)$.