TD 11 – Tout ce que je sais, c'est que je ne sais rien

Exercice 1. *Ils se suivent mais se ressemblent-ils ?*

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

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

   En déduire une nouvelle 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 hachage deux à deux indépendantes)**.** Un ensemble $H_{n,k}$ de fonctions de $\{0,1\}^n$ dans $\{0,1\}^k$ est appelé *ensemble de fonctions de hachage deux à deux indépendantes* si pour tout $x \neq x'$ dans $\{0,1\}^n$ et pour tout y, y' dans $\{0,1\}^k$, $\mathbb{P}_{h \in H_{n,k}}[h(x) = y \wedge h(x') = y'] = 2^{-2k}$.

3. Soit $H_{n,n} = \{h_{a,b} : a, b \in \{0,1\}^n\}$, où pour tous a et b dans $\{0,1\}^n$, $h_{a,b}(x) = ax + b$. Montrer que $H_{n,n}$ est un ensemble de fonctions de hachage deux à deux indépendantes.
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 $|S| \leq K/2$ avec bonne probabilité.
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. *Ne rien dire à personne*

Les **protocoles à divulgation nulle** vérifient les deux conditions de complétude et de correction des protocoles interactifs classiques, mais aussi la condition suivante : le vérificateur n'apprend rien d'autre du prouveur que l'appartenance du mot au langage décidé. On se restreint ici au cadre des langages de NP.

Formellement, soit $L \in \mathsf{NP}$. Un protocole interactif (P, V) est appelée une **preuve à divulgation nulle pour** L si les conditions suivantes sont vérifiées :

- si $x \in L$ et u est un certificat pour x, $\mathbb{P}[\text{out}_V\langle P(x,u), V(x)\rangle = 1] \geq 2/3$;
- si $x \notin L$, pour tout prouveur $P^\star$ et tout certificat u, $\mathbb{P}[\text{out}_V\langle P^\star(x,u), V(x)\rangle = 1] \leq 1/3$;
- pour tout vérificateur $V^\star$, il existe un algorithme probabiliste $S^\star$ en temps espéré polynomial tel que pour tout $x \in L$ et certificat u pour x, $\text{out}_{V^\star}\langle P(x,u), V^\star(x)\rangle \equiv S^\star(x)$ (où $\equiv$ veut dire que ces deux variables aléatoires sont identiquement distribuées).

$S^\star$ est appelé le **simulateur** de $V^\star$.

✎ Montrer que le protocole suivant est une preuve à divulgation nulle pour l'isomorphisme de graphes.

- **Entrée** x **:** une paire de graphes (G_0, G_1) à n sommets.
- **Certificat** u **:** une permutation $\pi : [n] \to [n]$ telle que $G_1 = \pi(G_0)$.

1. Le prouveur choisit au hasard une permutation π_1 et envoie au vérificateur $\pi_1(G_1)$.
2. Le vérificateur tire aléatoirement un bit $b \in \{0, 1\}$ et l'envoie au prouveur.
3. Le prouveur envoie $\pi^\star = \pi_1$ au vérificateur si $b = 1$ et $\pi^\star = \pi_1 \circ \pi$ sinon.
4. Le vérificateur accepte si et seulement si $\pi_1(G_1) = \pi^\star(G_b)$.