TD13 - Interactive proofs : Permanent d'une matrice.

Exercice 1. *Retour sur les machines probabilistes*

✎ Montrer que BPL est dans P. *Indication : on pourra compter le nombre de configurations possibles d'une machine dans BPL, et montrer que l'on peut calculer de façon déterministe la probabilité d'arriver dans une configuration acceptante.*

Exercice 2. *Permanent d'une matrice*

Soit $A = (a_{i,j})$ une matrice carrée (à coefficients entiers). On appelle permanent :

$$perm(A) = \Sigma_{\sigma \in S_n} \Pi_{i=1}^{n} a_{i,\sigma(i)}$$

Remarques : le déterminant et le permanent sont les deux seules notions définissables de cette manière à l'aide de morphismes de S_n dans C^* ; le permanent n'est pas multiplicatif.
Dans la suite on notera A_{ij} la matrice obtenue à partir de A en supprimant la i^{e} ligne et la j^{e} colonne.

1. Rappeler la définition du déterminant. Quelle est la complexité du calcul du déterminant ?

Pour le permanent, c'est bien pire. Nous allons montrer que son calcul se fait cependant dans IP.

2. Rappeler la formule de développement selon la première colonne pour le calcul du déterminant. Donner une formule similaire pour le calcul du permanent.

3. En utilisant le développement selon la première colonne, donner un protocole simple de preuve interactive pour le calcul du permanent.

4. Analyse du protocole précédent : le prouveur peut-il berner le vérificateur avec grande probabilité ?

✎ "Arithmetization" : exemple de SAT.

6. Donner une version améliorée de la preuve interactive du calcul du permanent, en utilisant l'arithmétisation.

7. Montrer que lorsque le prouveur donne une réponse incorrecte avec ce protocole, et que le vérificateur ne le rejette pas, alors à l'étape suivante la réponse sera incorrecte aussi, avec probabilité proche de 1.

8. Conclure.

Exercice 3. *Assertions sur IP*

Montrer les assertions suivantes :

1. Montrer que IP est inclus dans PSPACE.
2. Soit IP" la classe obtenue en remplaçant dans la définition de IP la condition (1) par

$$\exists P \forall x \in L \ \Pr[\text{out}_V \langle V, P \rangle(x) = 1] \geq 2/3$$

Montrer que IP"= IP.