Master CSI 2 2011-2012

Crypto avancée : feuille de TD 3

– EXERCICE 1. DÉMINEUR.

On considère le jeu du démineur sur un graphe arbitraire G, où certains sommets sont associés à une *mine*, et d'autres sont associés à un nombre entier qui est égal aux nombres de mines voisines.

Soit le problème de décision suivant :

I : Un graphe G, un sous-ensemble de sommets S étiquettés par des entiers positifs.
Q : Est-il possible de placer des mines sur un sous-ensemble de de sommets du complémentaire de S, de tel sorte que chaque entier étiquettant un sommet de S soit égal au nombre de mines voisines ?

Montrer que ce problème est NP-complet. On pourra exhiber une réduction polynomiale à partir de 3-SAT. Suggestion : considérer un graphe biparti Clauses - Variables.

– EXERCICE 2. On considère le problème

double SAT :

I : Une formule booléenne f
Q : Existe-t-il (au moins) *deux* choix de valeurs du n-uple $(x_1, \ldots, x_n)$ des variables qui satisfont la formule ?

Montrer que «double SAT» est NP-complet.

– EXERCICE 3. Montrer que si P=NP, il existe un algorithme qui factorise les entiers en temps polynomial.

– EXERCICE 4. SOLITAIRE.

Ce jeu se joue sur un tableau $k \times n$. Chaque position est dans un de ces trois états :
- vide,
- contient une pierre blanche,
- contient une pierre noire.

Le joueur joue en retirant des pierres. Il a gagné s'il atteint une position où
- chaque colonne ne contient que des pierres d'une même couleur,

– chaque ligne contient au moins une couleur.

On considère le problème de décision associé :

I : Une position sur un tableau $k \times n$
Q : Peut-on gagner ?

Montrer que ce problème est NP-complet. Faire une réduction à 3-SAT.