Master CSI 2 — 2013-2014

Crypto avancée : feuille de TD 2

– EXERCICE 1. Il s'agit de montrer que le problème suivant

SUBSET SUM

I : des entiers $N_1, \ldots, N_n$ et un entier S
Q : Existe-t-il $(\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$ tel que $\sum_{i=1}^n \varepsilon_i N_i = S$?

est NP-complet. On considère la transformation suivante, d'une instance de 3-SAT vers une instance de SUBSET SUM.

Soit une formule booléenne de la forme

$$f = C_1 \wedge \ldots \wedge C_k$$

sur l'ensemble de variables $x_1, \ldots, x_\ell$. On lui associe $n = 2\ell + 2k$ entiers que l'on représentera par leur écriture décimale. Tout d'abord les 2ℓ entiers

$$Y_1, Z_1, \ldots, Y_\ell, Z_\ell$$

où
- $Y_i = 10^{k+i} + \sum_{j \in I} 10^j$, en convenant que I est l'ensemble des j tels que la variable x_i figure dans la clause j.
- $Z_i = 10^{k+i} + \sum_{j \in J} 10^j$, en convenant que J est l'ensemble des j tels que la variable $\overline{x}_i$ figure dans la clause j.

On complète par les entiers $G_1, H_1, \ldots, G_k, H_k$ où $G_i = H_i = 10^i$. L'entier S est défini par

$$S = \sum_{i=1}^{\ell} 10^{k+i} + 3 \sum_{j=1}^{k} 10^j.$$

a) Écrire la transformation de la formule

$$(x_1 \vee \overline{x}_2 \vee x_3) \wedge (x_1 \vee \overline{x}_2 \vee \overline{x}_3) \wedge (\overline{x}_1 \vee x_2 \vee \overline{x}_3).$$

On pourra représenter $N_1 \ldots N_n$ sous forme d'un tableau.

b) Quel est le rapport entre un choix de valeurs de x_1, x_2, x_3 satisfaisant f et un sous-ensemble de N_i sommant à S ?

c) Montrer que la transformation est une transformation polynômiale.

– Exercice 2. On considère le problème de décision

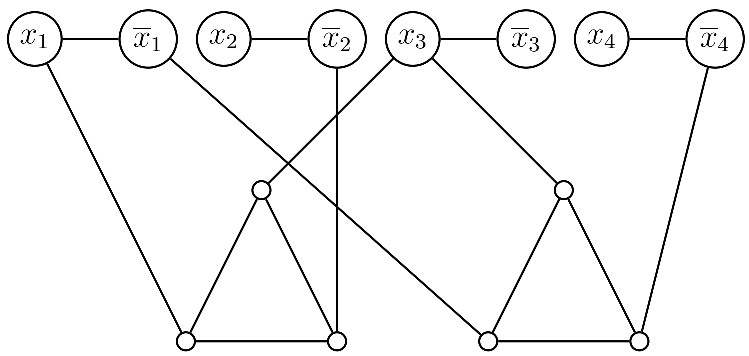
Recouvrement par des sommets :

I : Un graphe G et un entier k
Q : Existe-t-il un sous-ensemble A de k sommets tel que chaque arête du graphe soit incidente à un sommet de A ?

À la formule booléenne suivante

$$F = (x_1 \vee \overline{x}_2 \vee x_3) \wedge (\overline{x}_1 \vee x_3 \vee \overline{x}_4)$$

on associe le graphe



Généraliser pour trouver une transformation polynômiale de 3-SAT vers *recouvrement par de sommets*.

– Exercice 3. 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 4. 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 5. Montrer que si P=NP, il existe un algorithme qui factorise les entiers en temps polynomial.

– Exercice 6. 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.