Master CSI 2 — 2011-2012

Crypto avancée : feuille de TD 2

– EXERCICE 1.

a) Montrer que la formule booléenne $x \vee y$ est réalisée (vaut 1) si et seulement si la formule

$$(x \vee y \vee z) \wedge ((x \vee y \vee \overline{z}))$$

l'est. On dira que les deux formules sont équivalentes.

b) Montrer que la formule $x_1 \vee x_2 \vee x_3 \vee x_4$ est équivalente à la formule

$$(x_1 \vee x_2 \vee y) \wedge (x_3 \vee x_4 \vee \overline{y}).$$

c) Exhiber une transformation polynomiale f de SAT vers 3-SAT.

– EXERCICE 2. Une *fonction booléenne* est une fonction $f : \{0,1\}^n \to \{0,1\}$. Elle peut être représentée par une table, par exemple :

x_1	x_2	x_3	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Un *circuit* de calcul est un graphe orienté, dont les sommets sont étiquetés par un des termes $0, 1, \vee, \wedge, \neg, \mathbf{x}_1, \ldots, x_n$, «sortie». De plus,
- Les sommets étiquetés $0, 1, x_i$ ont 0 comme degré rentrant.
- Les sommets étiquetés $\neg$ ont 1 comme degré rentrant.
- Les sommet étiquetés $\vee, \wedge$ ont 2 comme degré rentrant.
- Il y a un unique sommet étiqueté «sortie», il a 1 comme degré rentrant, et 0 comme degré sortant.

a) Écrire un circuit qui calcule la fonction f donnée par la table ci-dessus.

b) Donner une procédure qui construit, à partir d'une table définissant une fonction booléenne f, un circuit calculant f. Que peut-on dire de la taille du circuit ?

– EXERCICE 3. 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 4. On considère le problème de décision

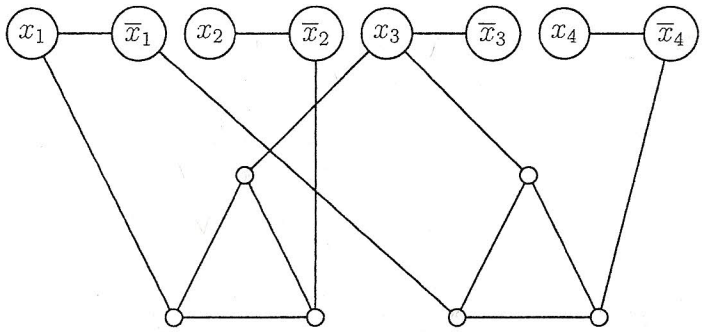
Recouvrement par des sommets :

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.*