ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
Sections d'Informatique et de Systèmes de Communication

Série d'exercices 12 14 Decembre 2007

1. La taille de l'input

Pour chacun des problèmes suivants, donner la taille de l'input en fonction de n :

a) Etant donné un nombre $n \in \mathbb{N}$, trouver sa décomposition en produit de nombres premiers.

b) Etant donné une matrice binaire $n \times n$, calculer l'inverse de cette matrice, s'il existe.

c) Etant donné n entiers non-négatifs plus petits que 1000, trouver le plus grand.

d) Etant donné un graphe G avec des poids entre -100 et 100 (donné par sa matrice d'adjacence) trouver un arbre couvrant minimal.

2.Langages

Un *langage* est un sous-ensemble de $\{0,1\}^*$, i.e. c'est un sous-ensemble de tous les vecteurs de bits. Par exemple, le langage

$$L = \{x \in \{0,1\}^* \mid |x| \geq 1 \wedge x_{|x|} = 1\}. \tag{1}$$

est le langage de tous les mots de bits qui se terminent avec un 1. ($|x|$ dénote la longueur en bits de x).

a) En fait on peut codifier n'importe quel input d'un algorithme sous la forme d'un mot de bits. Résoudre le cas suivant : Donner une méthode pour codifier deux entiers de longueurs (binaires) n et m en un mot binaire, sans utiliser plus que $n + m + O(\log(n))$ bits.

b) A chaque problème de décision correspond un langage : c'est l'ensemble de tous les mots pour lesquels la réponse au problème de décision est TRUE. Inversement, à chaque langage L donné correspond le problème de décision suivant : "Est-ce que $x \in L$?"

A quel problème de décision correspond (1), si l'on interprète le mot comme un nombre binaire ?

3. Complexité

Nous reprenons la définition d'un langage : Un *langage* L est un sous-ensemble de $\{0,1\}^*$. La classe P est l'ensemble des langages pour lesquels il existe un algorithme $\mathcal{S}(x)$ avec comme ensemble d'output $\{\text{TRUE}, \text{FALSE}\}$, et tel que

- $\mathcal{S}(x) = \text{TRUE} \iff x \in L$.
- $\mathcal{S}(x)$ peut être calculé avec un temps de parcours polynomial en $|x|$.

a) Montrer que si $A, B \in P$ alors $A \cap B \in P$

b) Montrer que si $A, B \in P$ alors $A \cup B \in P$

c) Montrer que si $A, B \in P$ alors $(A : B) \in P$, où $A : B$ dénote la *concaténation* des ensembles A et B :

$$A : B = \left\{a : b \mid a \in A, b \in B\right\},$$

et $a : b$ dénote la concaténation des mots a et b (on colle les chiffres de b après ceux de a). Par exemple $(0110) : (111) = (0110111)$.

d) Rappelons la définition d'une *réduction polynomiale*, en termes de langages :

Définition : Soient A et B deux langages. Nous disons que $A \leq_P B$ s'il existe une fonction $f : \{0,1\}^* \to \{0,1\}^*$ telle que :

- $x \in A \iff f(x) \in B$.
- $f(x)$ peut être calculé avec un temps de parcours polynomial en $|x|$.

Montrer que si $A \leq_P B$ alors $\overline{A} \leq_P \overline{B}$.

4. Problème de réduction

Soit P la classe des problèmes décidables en temps polynomial, et soient A et B sont des sousensembles propres non-vides de Σ^* pour un alphabet fini Σ. On suppose que A et B appartiennent à P. Montrer que $A \leq_{\mathsf{P}} B$ et que $B \leq_{\mathsf{P}} A$, i.e., que le langage A est réducible en temps polynomial à B et vice-versa.

5. Réduction polynomiale

Rappelons d'abord qu'une *clique* dans un graphe $G(V, E)$ est un sous-ensemble $S \subseteq V$ tel que $S \times S \subseteq E$, c'est à dire un ensemble de sommets qui sont tous connectés entre eux.

Considérons les problèmes de décision suivants :

Problème : CLIQUE
Input : Un graphe non orienté G, et un entier k.
Output : Vrai si G contient une clique de taille $\geq k$, Faux sinon.

Problème : HALF-CLIQUE
Input : Un graphe non orienté G, ayant n sommets (où n est pair).
Output : Vrai si G contient une clique de taille $\geq n/2$, Faux sinon.

Nous voulons montrer que

$$\text{CLIQUE} \leq_P \text{HALF-CLIQUE}.$$

Ainsi, il s'agit donc de construire une fonction f qui transforme un input (G, k) de CLIQUE en un input G' de HALF-CLIQUE.

a) Soit G un graphe, et soit $f_1(G)$ le graphe obtenu en ajoutant à G un sommet connecté à tous les autres sommets. Montrer que G contient une clique de taille $\geq k$ si et seulement si $f_1(G)$ contient une clique de taille $\geq k+1$.

b) Généraliser la construction ci-dessus. Plus précisément, pour tout $a \in \mathbb{N}$, montrer qu'étant donné un graphe G, on peut construire un graphe $f_a(G)$ tel que G contient une clique de taille $\geq k$ si et seulement si $f_a(G)$ contient une clique de taille $\geq k+a$.

c) Soit m le nombre de sommets dans G. Supposons que $k \leq m/2$. Trouver a en fonction de m et k tel que G contient une clique de taille $\geq k$ si et seulement si $f_a(G)$ contient une clique de taille $\geq n_a/2$, où n_a dénote le nombre de sommets dans $f_a(G)$.

d) Déduire que CLIQUE $\leq_P$ HALF-CLIQUE. (*Indice :* Distinguer les deux cas $k \leq m/2$ et $k > m/2$).