Ecole Normal Supérieure de Lyon
MIM1
Modèles de calcul, Examen (3H)

Mardi 15 Mai 2001

I -

Soient deux langages A et B sur les alphabets respectifs Σ et Γ. On dit qu'ils sont p-isomorphes, et on le dénote $A \sim_p B$, s'il existe une application bijective $f : \Sigma^\star \longmapsto \Gamma^\star$ telle que :

- f et f^{-1} sont calculables en temps polynomial,
- $u \in A$ si et seulement si $f(u) \in B$

On considère le problème EI suivant :

- entrée : un graphe fini $G = (V, E)$ et un entier k, $k \geq 0$,
- question : G a-t-il un ensemble indépendant de taille k, c'est-à-dire existe-t-il une partie V' de V de taille k telle que quels que soient les sommets u, v dans V', $\{u, v\} \notin E$?

1. Prouver que EI est NP-complet.
2. Prouver que $CLIQUE$ et EI sont p-isomorphes.

II -

Précisons quelques définitions et notations.

- Une application $f : \Sigma^\star \longmapsto \Gamma^\star$ est dite longueur-croissante, ou *lc*, lorsque pour tout x, $x \in \Sigma^\star$, $|f(x)| > |x|$.
- Une application injective $f : \Sigma^\star \longmapsto \Gamma^\star$ est dite polynomialement inversible, ou *inv*, s'il existe un algorithme en temps polynomial qui, pour tout y, $y \in \Gamma^\star$, répond NON si $y \notin f(\Sigma^\star)$ ou trouve x, $x \in \Gamma^\star$, tel que $y = f(x)$.
- On dénotera $A \leq_{inv,lc} B$ le fait qu'il existe une application injective $f : \Sigma^\star \longmapsto \Gamma^\star$ polynomialement inversible et longueur croissante telle que $u \in A$ si et seulement si $f(u) \in B$.

On suppose que A et B sont deux langages tels que $A \leq_{inv,lc} B$ via f et $B \leq_{inv,lc} A$ via g.

On considère les langages $R_1 = \{(g \circ f)^k(x)/k \geq 0 \text{ et } x \in \Sigma^\star - g(\Gamma^\star)\}$ et $R_2 = \{(g \circ (f \circ g)^h)(y)/h \geq 0 \text{ et } y \in \Gamma^\star - f(\Sigma^\star)\}$.

1. (a) Prouver que $R_1 \cap R_2 = \emptyset$,
   (b) Prouver que $R_1 \cup R_2 = \Sigma^\star$,
   (c) Prouver que A et B sont p-isomorphes.

2. Montrer que SAT et 3-SAT sont p-isomorphes.

III -

Un langage $A \subseteq \Sigma^\star$ est dit rembourrable s'il existe une fonction r de $\Sigma^\star \times \Sigma^\star$ dans $\Sigma^\star$, calculable en temps polynomial et polynomialement inversible, telle que $r(x, y) \in A$ si et seulement si $x \in A$. Une telle fonction, dite de remplissage, est dite longueur-croissante si pour tous x et y, elle satisfait $|r(x, y)| > |x| + |y|$.

1. Prouver qu'un langage $A \subseteq \Sigma^\star$ est rembourrable si et seulement s'il existe des fonctions r de $\Sigma^\star \times \Sigma^\star$ dans $\Sigma^\star$ et q de $\Sigma^\star$ dans lui-même, calculables en temps polynomial, telles que :

   - $r(x, y) \in A$ si et seulement si $x \in A$, et
   - $(q \circ r)(x, y) = y$.

2. Soient deux alphabets Σ et Γ. Existe-t-il une fonction d'encodage longueur-croissante de $\Sigma^\star$ dans $\Gamma^\star$?

3. On suppose que $A \subseteq \Sigma^\star$ est polynomialement réductible à $B \subseteq \Gamma^\star$ (avec les notations usuelles $A \leq B$) et que B est rembourrable grâce à une fonction de remplissage longueur-croissante. Prouver alors que $A \leq_{inv,lc} B$.

4. En déduire que si A et B sont deux langages rembourrables via des fonctions de remplissage longueur-croissantes et s'ils sont polynomialement équivalents ($A \leq B$ et $B \leq A$), alors $A \sim_p B$.

Remarque : De très nombreux langages NP-complets classiques sont ainsi prouvés p-isomorphes, mais qu'ils le soient tous est (encore) une conjecture, dite de "l'isomorphisme de Berman- Hartmanis".