Langages formels, calculabilité et complexité
TD12

19 décembre 2014

Exercice 1 Si P=NP ... (*base*)

Montrer que si P = NP, alors tout langage de NP sauf les langages triviaux $\emptyset$ et A^* est NP-complet. Pourquoi doit-on exclure ces langages triviaux ?

Exercice 2 Factorisation (*base*)

On considère les deux problèmes suivants :

- FINDFACTOR : Étant donné un entier positif N en binaire, trouver un facteur non-trivial de N s'il en existe un.
- HASFACTOR ? : Étant donnés deux entiers positifs N et M en binaire, décider si N a un facteur non-trivial inférieur à M.

1. Montrer que si HASFACTOR ? est résoluble en temps polynomial, alors aussi FINDFACTOR.
2. Montrer que si FINDFACTOR est résoluble en temps polynomial, alors aussi HASFACTOR ?.

Exercice 3 L'étoile et la classe P (*base*)

Soit L un langage qui est décidable en temps polynomial. Montrer que le langage L^* est décidable en temps polynomial.

Exercice 4 Théorème de hiérarchie (*base*)

Une fonction $f : \mathbb{N} \to \mathbb{N}$ est dite *constructible en temps* s'il existe une machine de Turing qui calcule pour une entrée 1^n le mot $1^{f(n)}$ en temps $O(f(n))$.

1. Soit f croissante non-bornée et constructible en temps. Montrer que $\text{TIME}(f(\lfloor n/2 \rfloor)) \subsetneq \text{TIME}(f(n)^3)$ en considérant le langage des couples (M, x) tel que la machine M accepte l'entrée x en temps $f(|x|)$.

Soient $\text{P} = \bigcup_{k \in \mathbb{N}} \text{TIME}(n^k)$ et $\text{EXPTIME} = \bigcup_{k \in \mathbb{N}} \text{TIME}(2^{n^k})$

2. Conclure que $\text{P} \subsetneq \text{EXPTIME}$.

Exercice 5 Fonctions à sens unique (*avancé*)

Supposons que :

- on a une bijection f des entiers sur n bits vers les entiers sur n bits, pour tout n (i.e., sur une entrée x de n bits, $f(x)$ est un entier sur n bits tel que $f(x) \neq f(y)$ quand $x \neq y$).
- la fonction f se calcule en temps polynomial.
- la fonction inverse de f ne peut pas se calculer en temps polynomial. (On dit que c'est une fonction à sens unique.)

1. Montrer que si une telle bijection existe, alors $\text{P} \neq \text{NP}$. (Idée : Montrer que le langage $L = \{(x, f(y)) : x < y\}$ appartient à $\text{NP} \setminus \text{P}$.)
2. Montrer de plus, que si elle existe, alors $\text{NP} \cap \text{coNP} \neq \text{P}$.