Calculabilité et complexité

Université de Montpellier

Examen

9 janvier 2017

Durée 3 heures

Aucun document n'est autorisé

Pas de calculatrice, téléphone portable, montre programmable, appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

1. Montrez que $\mathbb{K}$ est énumérable.
2. Montrez que si A et B sont énumérables, alors $A^B = \{x^y,\ x \in A \text{ et } y \in B\}$ l'est aussi.

Exercice 2 archi-classique

Le symbole $\prec$ représente ici la réduction (many-one) entre ensembles d'entiers.
Soit $A = \{x,\ x \text{ diverge sur au moins une entrée}\}$.

1. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
2. Est-ce que $\mathbb{K} \prec A$?
3. Est-ce que $\overline{\mathbb{K}} \prec A$?
4. Est-ce que $A \prec \overline{\mathbb{K}}$?
5. Est-ce que $A \prec \mathbb{K}$?

Exercice 3 toujours facile

1. Montrez qu'il existe une fonction calculable *totale* f telle que $[f(n) \mid \cdot] = [n \mid \cdot] + [n+1 \mid \cdot] + n + 1$
2. Quelles fonctions sont calculées par les points fixes de f ?

Exercice 4 stratégie

Si, dans la suite de votre Master, on vous demande de montrer qu'un problème est NP-complet, comment procèderez-vous ?

Exercice 5 une idée de BPP

Montrez que si SAT est dans BPP, alors $NP \subset BPP$.

Exercice 6 un zeste d'oracle

Montrez qu'il existe un oracle A tel que

$$PSPACE^A \neq EXP^A \ .$$

Exercice 7 un peu de $coNP$

On rappelle qu'un problème A est $coNP$-complet s'il est dans $coNP$, et si pour tout autre problème $B \in coNP$ on a $B \leq_m^p A$. Donnez un exemple de problème $coNP$-complet.

Exercice 8 beaucoup d'effondrements

1. Montrez que si $NP = coNP$, alors

$$\Sigma_2^p = NP \ .$$

2. Montrez que si $NP = coNP$, alors pour tout $n \geq 1$

$$\Sigma_n^p = \Pi_n^p = NP \ .$$

3. Montrez que si le problème SAT est dans $coNP$, alors toutes les classes Σ_n^p et Π_n^p coincident avec NP.

Exercice 9 une goutte de preuves interactives

Montrez que le langage suivant est dans IP

$$NQR = \{(k,p) \mid p \text{ est premier, et il n'existe pas } m \text{ vérifiant } m^2 = k \ mod \ p\} \ .$$