Examen terminal - Théorie de la complexité

THX

17 décembre 2020

La précision et la clarté de la rédaction est prise en compte dans l'évaluation. Certaines questions peuvent demander une formalisation très lourde : favorisez alors la pédagogie. Écrivez assez grand. N'hésitez pas à réutiliser des résultats vus en cours ou en TD/DM. Rédigez soigneusement.

1 Graphe acyclique

Question 1. *5 pts* *Étudier la complexité théorique du problème de décision suivant :*

ACYCLIQUE
entrée : un graphe orienté $G = (S, A)$
sortie : oui si le graphe G est acyclique, non sinon.

Donner une démonstration d'appartenance de ce problème à une certaine classe, puis montrer que ce problème est complet pour cette même classe.

2 Factorisation de nombres

On admettra que le problème **PRIMES** suivant est dans P (résultat difficile montré en 2004) :

PRIMES
entrée : un entier n écrit en binaire
sortie : oui, si l'entier n est premier ; non, sinon.

On définit le problème **FACTORISATION** :

FACTORISATION
entrée : deux entiers n, k écrit en binaire avec $n > k > 1$;
sortie : oui, si l'entier n admet un facteur premier p avec $k \leq p < n$; non, sinon.

Question 2. *4.5 pts* *Montrer que* **FACTORISATION** *est dans* $\mathrm{NP} \cap \mathrm{coNP}$.

3 BPP est dans Σ_2^p

On considère une machine de Turing M qui prend en entrée deux mots (x, y), où x est de longueur n, et qui s'exécute en temps n^c. Sans perte de généralité, on suppose que y est un mot sur l'alphabet $\{0, 1\}$ de longueur n^c. On note :

- $\mathcal{A}_x := \{y \in \{0,1\}^{n^c} \mid \text{l'exécution } M(x, y) \text{ est acceptante}\}$;
- $\mathcal{R}_x := \{y \in \{0,1\}^{n^c} \mid \text{l'exécution } M(x, y) \text{ est rejetante}\}$.

Notons $m = n^c$.

Question 3. *0.5 pts* *Donner une équation qui relie $\mathcal{A}_x$ et $\mathcal{R}_x$.*

On dit qu'un problème de décision A est dans la classe BPP (pour *bounded-error probabilistic polynomial time*) s'il existe une machine de Turing comme ci-dessus et un polynôme n^c avec (en reprenant les notations ci-dessus) :

- si $x \in A$, alors $|\mathcal{R}_x| \leq 2^{m-n}$;
- si $x \notin A$, alors $|\mathcal{A}_x| \leq 2^{m-n}$.

On note $\oplus$ l'opération ou exclusif (aussi appelé somme modulo 2) bits à bits. Par exemple $1101 \oplus 0110 = 1011$.

Question 4. *0.5 pts* *Calculer* $10000 \oplus 01101$.

Étant donné deux ensembles W_1 et W_2 de mots de longueur m, on note

$$W_1 \oplus W_2 := \{w_1 \oplus w_2 \mid w_1 \in W_1 \text{ et } w_2 \in W_2\}.$$

On considère un problème de décision A dans BPP. Soit x un mot de longueur n et $m = n^c$. Nous allons montrer l'équivalence suivante, lorsque n est suffisamment grand :

$$x \in A \quad \text{ssi} \quad \text{il existe } (z_1, \ldots, z_m) \in (\{0,1\}^m)^m \text{ tels que } \mathcal{A}_x \oplus \{z_1, \ldots, z_m\} = \{0,1\}^m.$$

Dans l'équivalence, chaque z_i est un mot de longueur m. La question qui suit consiste à montrer le sens $\Rightarrow$ par contraposée.

Question 5. *1 pts* *Montrer que, pour n assez grand, si $x \notin A$, alors il n'existe pas $(z_1, \ldots, z_m) \in (\{0,1\}^m)^m$ tels que $\mathcal{A}_x \oplus \{z_1, \ldots, z_m\} = \{0,1\}^m$.*

Nous allons maintenant montrer le sens $\Rightarrow$. Considérons $x \in A$. On dira que le m-uplet $(z_1, \ldots, z_m)$ est *mauvais* s'il existe $w \in \{0,1\}^m$ avec $\{w\} \oplus \{z_1, \ldots, z_m\} \subseteq \mathcal{R}_x$. Sinon, on dira que $(z_1, \ldots, z_m)$ est *bon*.

Question 6. *2 pts* *Montrer qu'il y a strictement moins de 2^{m^2} mauvais $(z_1, \ldots, z_m)$.*

Question 7. *0.5 pts* *En déduire qu'il existe de bons $(z_1, \ldots, z_m)$.*

Question 8. *1 pts* *Conclure la démonstration du sens $\Rightarrow$.*

Nous sommes maintenant prêt pour démontrer le résultat de l'exercice.

Question 9. *4 pts* *Montrer que A est dans Σ_2^p.*

Question 10. *1 pts* *Montrer que A est aussi dans Π_2^p.*

4 Taille de circuits (bonus)

Question 11. *2 pts* *Montrer qu'il existe une fonction $f : \{0,1\}^n \to \{0,1\}$ qui n'est pas calculable par un circuit avec moins de $\frac{2^n}{10n}$ portes.*

5 Dessin ! (bonus)

Question 12. *0.07 pts* *Donner les relations entre les classes* Logspace, NLogspace, *co*NLogspace, P, NP, coNP, Pspace, NPspace, *co*NPspace, Exptime, NExptime, *co*NExptime, Σ_1^p, Π_1^p, Σ_2^p, Π_2^p, PH, *NC, voire d'autres classes que vous aimez bien.*

Suggestion de présentation : un diagramme d'Euler (des patates) qui représente les inclusions.