Examen du cours Complexité (L3)

Les documents (notes, polycopiés, ..) et calculatrices (téléphone, tablette, ..) ne sont pas autorisés.

Date : 15 janv. 2024 à 10h00 / Durée : 2 heures

Exercice 1 : Machines à témoin

On appelle *machine à témoin* une machine de Turing M munie de deux bandes d'entrée (en lecture seule, non modifiables) en plus des bandes de travail habituelles. La première entrée, nommée x, est l'input de la machine comme d'habitude. La deuxième entrée, nommée y, est appelée « témoin » ou « certificat ». On note $M(x, y)$ le calcul de M sur ces deux entrées. Les notions de temps de calcul et d'espace de travail sont inchangées, et M peut être non déterministe. Nous avons vu une caractérisation des langages de NP qui peut s'exprimer avec les machines à témoin :

Thm. 1 (vu en cours). Un langage $L \subseteq A^*$ est dans NP si, et seulement si, il existe un polynôme p et une machine à témoin *déterministe* en temps polynomial M telle que pour tout $x \in A^*$

$$x \in L \Leftrightarrow \exists y : |y| \leq p(|x|) \wedge M(x, y) \text{ accepte.}$$

(*) 1. Rappelez brièvement comment on prouve la direction « si » du Thm. 1, ainsi que la direction « seulement si ».

(*) 2. Que faut-il changer à votre preuve de la question 1 si on renforce le Thm. 1 en exigeant que la 2ème bande d'entrée de la machine à témoin soit à lecture unique (*read-once* en anglais), c.-à-d. que la tête de lecture sur y n'a pas le droit de se déplacer à gauche (de revenir en arrière) ?

(**) 3. Dans une autre direction, que faut-il changer à votre preuve de la question 1 si on renforce le Thm. 1 en exigeant que la machine à témoin soit en espace logarithmique (et toujours déterministe) ?

(***) 4. Quelle classe de langages est obtenue si maintenant on combine les deux restrictions des questions précédents (machine déterministe logspace et témoin *read-once*) ? Justifiez votre réponse.

Problème 2 : Satisfaisabilité et insatisfaisabilité

On considère des formules booléennes $\varphi, \psi, \ldots$ construites comme d'habitude avec les connecteurs logiques $\wedge$, $\vee$, $\neg$, les constantes $\bot$ (faux) et $\top$ (vrai), et des variables booléennes $x_1, x_2, x_3, \ldots$ Ces formules ne sont pas forcément en forme clausale sauf si c'est explicitement précisé. On note $Var(\varphi)$ l'ensemble des variables qui apparaissent dans φ.

On s'intéresse aux problèmes de décision suivants :

SAT : l'ensemble des formules satisfaisables (ou plus exactement le langage des formules satisfaisables dans une notation appropriée) ;

UNSAT : l'ensemble des formules insatisfaisables (*unsatisfiable* en anglais), c.-à-d. des formules φ telles que $v(\varphi) = \bot$ pour toute valuation v des variables ;

SATUNSAT : l'ensemble des couples (φ, ψ) de formules telles que φ est satisfaisable et ψ ne l'est pas ;

SINGLESAT : l'ensemble des couples (φ, ψ) telles qu'une et une seule des deux formules est satisfaisable ;

PAIRSAT : l'ensemble des couples (φ, ψ) de deux formules satisfaisables ;

MINUNSAT : l'ensemble des formules φ en forme clausale $\varphi \equiv C_1 \wedge \cdots \wedge C_m$ telles que φ n'est pas satisfaisable mais le devient dès qu'on retire une clause quelconque (c.-à-d. $\varphi \in$ UNSAT et $\bigwedge_{\substack{1 \leq i \leq m \\ i \neq j}} C_i \in$ SAT pour tout $j = 1, \ldots, m$).

Enfin, pour deux problèmes $L \subseteq A^*$ et $L' \subseteq B^*$ on note $L \leq L'$ quand il existe une réduction de L dans L' (ici, et comme en cours, le mot « réduction » est un raccourci pour « réduction logspace »). Si maintenant $L \leq L' \leq L$ on dit que les deux problèmes sont équivalents.

(*) 5. Donnez une réduction montrant $\mathsf{PAIRSAT} \leq \mathsf{SAT}$.

(*) 6. Donnez une réduction montrant $\mathsf{SATUNSAT} \leq \mathsf{SINGLESAT}$.

(*) 7. Donnez une réduction montrant $\mathsf{SINGLESAT} \leq \mathsf{SATUNSAT}$.

(*) 8. Montrez $\mathsf{MINUNSAT} \leq \mathsf{SINGLESAT}$.

Les questions suivantes cherchent à exhiber une réduction $\mathsf{SATUNSAT} \leq \mathsf{MINUNSAT}$ dans l'autre direction afin de pouvoir conclure $\mathsf{SATUNSAT} \equiv \mathsf{MINUNSAT}$ (ce qu'on fera à la question 13).
Pour ce faire, on considère un ensemble $Z = \{z_1, \ldots, z_n\}$ de n variables booléennes sur lesquelles on définit les clauses suivantes pour tous $i, j = 1, \ldots, n$ tels que $i \neq j$:

$$C_i^Z \equiv z_1 \vee \cdots \vee z_{i-1} \vee \neg z_i \vee z_{i+1} \vee \cdots \vee z_n, \qquad D_{i,j}^Z \equiv \neg z_i \vee \neg z_j.$$

On définit aussi une dernière clause C^Z, ainsi que la formule CNF φ^Z :

$$C^Z \equiv z_1 \vee z_2 \vee \cdots \vee z_n, \qquad \varphi^Z \equiv C^Z \wedge \bigwedge_{i=1}^{n} C_i^Z \wedge \bigwedge_{1 \leq i < j \leq n} D_{i,j}^Z.$$

(**) 9. Montrez que, quelque soit $n \in \mathbb{N}$, φ^Z est dans $\mathsf{MINUNSAT}$. (N'oubliez pas le cas $n = 0$.)

(***) 10. Montrez $\mathsf{UNSAT} \leq \mathsf{MINUNSAT}$. Pour cette réduction $\varphi \mapsto \varphi'$ on pourra supposer que φ est en CNF et, en s'inspirant de ce qui est fait à la question 9, que φ' est obtenue en ajoutant des littéraux à chaque clause de φ ainsi que des clauses supplémentaires qui contraignent les variables nouvelles.

(**) 11. Montrez que $\mathsf{SAT} \leq \mathsf{MINUNSAT}$. Pour ce faire on pourra continuer la construction des deux questions précédentes.

La suite de l'exercice est indépendante des constructions des questions 9 à 11 dont on pourra admettre les conclusions.
On définit $\mathsf{TwoMINUNSAT} \stackrel{\text{def}}{=} \{(S, S') \mid S, S' \in \mathsf{MINUNSAT}\}$.

(**) 12. Donnez une réduction montrant que $\mathsf{TwoMINUNSAT} \leq \mathsf{MINUNSAT}$.

(*) 13. Montrez que $\mathsf{MINUNSAT} \equiv \mathsf{SATUNSAT}$.

On définit DP (pour « différence de langages NP ») via

$$L \in \mathsf{DP} \Leftrightarrow \exists L_1, L_2 \in \mathsf{NP} : L = L_1 \setminus L_2 \,.$$

(**) 14. Montrez qu'il existe des problèmes DP-complets.