IFT503/711 – Théorie du calcul

Université de Sherbrooke

Devoir 5

Enseignant:	Manuel Lafond
Date de remise:	jeudi 31 mars 2022 avant 10h29 AM
À réaliser:	individuellement ou à deux au 1er cycle individuellement aux cycles supérieurs
Modalités:	à remettre électroniquement via turnin
Pointage:	sur 40 points au 1er cycle (+ 5pts bonus) sur 50 points aux cycles supérieurs

Question 1.

Commencez par quelques petites questions d'échauffement.

(a) Rappelons que $\mathsf{EXPTIME} = \bigcup_{k \in \mathbb{N}} DTIME(2^{n^k})$. Montrez que $\mathsf{PSPACE} \subseteq \mathsf{EXPTIME}$. 2.5 pts

(b) Montrez que le langage MAJSAT du devoir 3 est dans PSPACE. 2.5 pts

(c) Montrez que si $\mathsf{PSPACE} \subseteq \mathsf{P}$, alors $\mathsf{P} = \mathsf{BPP}$. 2.5 pts

(d) On définit $\mathsf{coNPSPACE} = \{L : \overline{L} \in \mathsf{NPSPACE}\}$. Montrez que $\mathsf{coNPSPACE} = \mathsf{NPSPACE}$. 2.5 pts

Question 2.

(a) La taille $|\phi|$ d'une formule booléenne ϕ est le nombre de caractères requis pour la décrire. Chaque variable x_i ou $\overline{x}_i$ compte pour un caractère, ainsi que les symboles $\vee, \wedge, ($ et $)$. Par exemple, la formule $\phi = (x_1 \vee \overline{x}_2) \wedge x_3$ a une taille de $|\phi| = 7$. Deux formules ϕ_1 et ϕ_2 sont *équivalentes* si elles utilisent les mêmes variables $x_1, \ldots, x_n$ et si les deux formules sont satisfaites par exactement le même ensemble d'assignations. Montrez que le langage suivant est dans PSPACE. 6 pts

$$\text{MIN-FORMULA} = \{\phi : \text{ il n'existe pas de formule } \phi' \text{ équivalente à } \phi \text{ telle que } |\phi'| < |\phi|\}$$

(b) Vous devez sortir d'un stationnement chaotique. Chaque voiture est à l'horizontale ou à la verticale et peut avancer ou reculer. Nous sommes à l'horizontale et on veut atteindre une case spécifiée. 6 pts

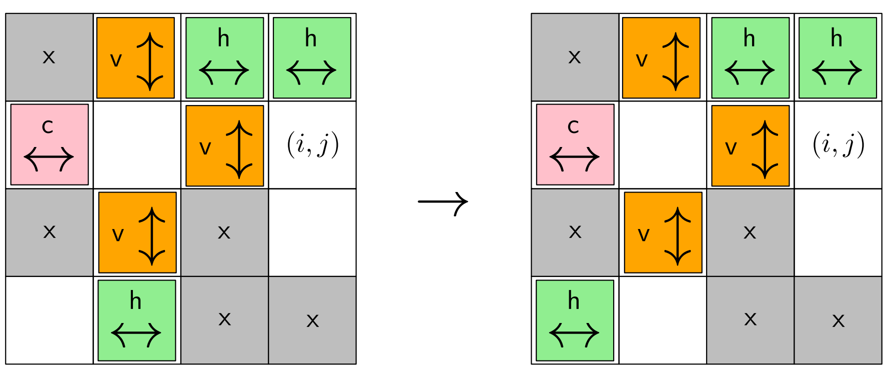

Figure 1 – Un exemple de déplacement légal, ici horizontal. Est-ce que c peut aller à la case (i, j)?

Formellement, on a une matrice M de dimension $n \times n$ dans laquelle chaque cellule contient une valeur parmi $\{\mathsf{c}, \mathsf{h}, \mathsf{v}, \mathsf{x}, \text{␣}\}$. Un déplacement consiste à prendre deux cellules voisines et échanger leur valeur. Plus spécifiquement, un déplacement impliquant deux cellules (i, j) et (i', j') est légal si:

— $M_{i,j} \in \{\mathsf{c}, \mathsf{h}\}$, $M_{i',j'} = \text{␣}$ et $(i', j') \in \{(i, j-1), (i, j+1)\}$; ou

— $M_{i,j} = \mathsf{v}$, $M_{i',j'} = \text{␣}$ et $(i', j') \in \{(i-1, j), (i+1, j)\}$.

On écrit $M \to M'$ s'il existe une séquence de déplacements légaux qui transforme M en M'. Le langage correspondant est:

$$\text{GET-OUT} = \{\langle M, i, j\rangle : \text{il existe } M' \text{ telle que } M \to M' \text{ et } M'_{i,j} = \mathsf{c}\}$$

Montrez que GET-OUT est dans PSPACE.

Note: assurez-vous que votre espace est vraiment polynomial. Je recommande d'utiliser Savitch.

(c) Le problème TQBF présenté en classe supposait une alternance des quantificateurs. En réalité, ce n'est pas exigé. C'est-à-dire, une formule quantifiée peut avoir le même quantificateur plusieurs fois de façon consécutive, par exemple 6 pts

$$\exists x_1 \exists x_2 \forall x_3 \forall x_4 \forall x_5 \exists x_6 \ (x_1 \vee \overline{x}_2) \wedge (x_3 \vee x_4 \vee \overline{x}_5) \wedge (x_6 \vee \overline{x}_6)$$

Soit TQBF-GEN l'ensemble des formules booléennes quantifiées qui n'ont pas nécessairement d'alternance entre les quantificateurs, et TQBF qui a cette alternance. Montrez que TQBF-GEN $\leq_P$ TQBF.

Question 3.

(a) Soit BPPSPACE l'ensemble des langages décidés par une MT probabiliste en espace polynomial (i.e. si $w \in L$, on accepte avec probabilité $\geq 2/3$ et sinon, on accepte avec probabilité $\leq 1/3$). L'argument suivant veut montrer que PSPACE = BPPSPACE, mais est erroné. Dites quelle est l'erreur de la preuve. 6 pts

"Il est clair que PSPACE $\subseteq$ BPPSPACE car une MT en espace $O(n^k)$ est un cas spécial d'une MT probabiliste en espace $O(n^k)$. On peut ensuite argumenter que BPPSPACE $\subseteq$ PSPACE comme suit. Soit $L \in$ BPPSPACE et M une MT probabiliste qui décide L en espace $O(n^k)$. On peut représenter l'exécution de M à l'aide d'une arbre dans lequel les branchements correspondent aux choix aléatoires. De façon déterministe, on peut explorer cet arbre avec une fouille en profondeur et compter le nombre de feuilles k qui acceptent M. On accepte w si et seulement si k est au moins le $2/3$ du nombre de feuilles. Ceci se fait en espace polynomial car M prend un espace polynomial et donc $L \in$ PSPACE."

(b) On définit PP comme l'ensemble des langages L pour lesquels il existe une MT probabiliste M telle que 6 pts
— si $w \in L$, $Pr[M \text{ accepte } w] > 1/2$;
— si $w \notin L$, $Pr[M \text{ accepte } w] \leq 1/2$.
Montrez que NP $\subseteq$ PP.

Suggestion: Prenez SAT. Essayez une assignation aléatoire. Acceptez si A satisfait, et sinon vous acceptez avec une probabilité bien choisie.

Aux cycles supérieurs, choisissez seulement **une des deux questions ci-bas**. Indiquez clairement votre choix. Au 1^{er} cycle, vous pouvez choisir une question et aurez 5 points bonis pour votre réponse.

★ Question 4. (cycles supérieurs)

Considérez le jeu à deux joueurs suivant, que l'on appellera DOUBLE-GEOGRAPHY. On a en entrée un graphe orienté G ainsi que deux sommets distincts v_1 et v_2 de G. Le joueur 1 doit construire un chemin orienté P_1 et le joueur deux un chemin orienté P_2. Initialement, P_1 contient seulement v_1 et P_2 contient seulement v_2. À son tour, le joueur 1 doit prolonger P_1 en ajoutant un sommet à la fin du chemin. Le sommet ajouté doit être un voisin sortant du dernier sommet de P_1 et ne doit pas déjà appartenir à P_1 ni à P_2. De la même façon, le joueur 2 à son tour doit prolonger P_2 avec un sommet qui n'est pas déjà dans P_1 ou P_2. Le premier joueur qui est incapable de prolonger son chemin à son tour a perdu. 10 pts

Le langage DOUBLE-GEOGRAPHY contient les triplets $\langle G, v_1, v_2 \rangle$ tels que le joueur 1 a une stratégie gagnante sur G lorsque v_1 et v_2 sont les points de départ des joueurs 1 et 2, respectivement.

Montrez que DOUBLE-GEOGRAPHY est PSPACE-complet.

★ Question 5. (cycles supérieurs)

Un *prouveur* est une fonction $P : \Sigma^* \to \Sigma^*$. On écrit $M \leftrightarrow P$ pour dénoter une MT *probabiliste* qui peut obtenir des valeurs de $P(w)$ en temps unitaire. C'est-à-dire, $M \leftrightarrow P$ peut écrire un mot w sur un ruban dédié à des requêtes, puis après une unité de temps, w est remplacé par $P(w)$ sur ce ruban. Notez que M peut utiliser un prouveur P' différent, i.e. $M \leftrightarrow P'$ est la même MT, mais les requêtes w seront remplacées par $P'(w)$.

La classe IP (pour *Interactive Polynomial time*) contient les langages qu'on peut décider avec forte probabilité en temps polynomial à l'aide d'un prouveur. Formellement, $L \in \mathsf{IP}$ s'il existe une MT probabiliste M et un prouveur P tels que:

- si $w \in L$, alors $Pr[M \leftrightarrow P \text{ accepte } w] \geq 2/3$;
- si $w \in L$, alors $\forall P'$, $Pr[M \leftrightarrow P' \text{ accepte } w] \leq 1/3$;
- $\forall P'$, $M \leftrightarrow P'$ s'exécute toujours en temps polynomial (incluant le temps des requêtes).

Un résultat important en théorie de la complexité montre que $\mathsf{IP} = \mathsf{PSPACE}$. La preuve n'est pas triviale, mais nous pouvons faire une partie ici.

(a) Montrez que si TQBF $\in \mathsf{IP}$, alors $\mathsf{PSPACE} \subseteq \mathsf{IP}$. 4 pts

(b) Montrez que $\mathsf{IP} \subseteq \mathsf{PSPACE}$. 6 pts
Suggestion: il y a plusieurs façons de faire. De mon côté, j'utiliserais une MT non-déterministe en espace polynomial pour imiter $M \leftrightarrow P$ (justifié par Savitch). On peut simuler tous les choix aléatoires possibles de façon déterministe, mais utiliser le non-déterministe pour simuler le prouveur.