Examen "Introduction à la vérification"

Master 1 Informatique, 2018-2019

Jeudi 2 mai 2019, 14 :30-17 :30

Rédigez les 2 parties sur des copies séparées.

Documents autorisés : notes de cours et TD

Partie 1

Exercice 1 Considérons un ascenseur pour un bâtiment à 2 étages + RdC, pour lequel chaque étage possède une porte d'ascenseur, un voyant indiquant si l'ascenseur a été appelé de l'étage respectif, plus un bouton d'appel.

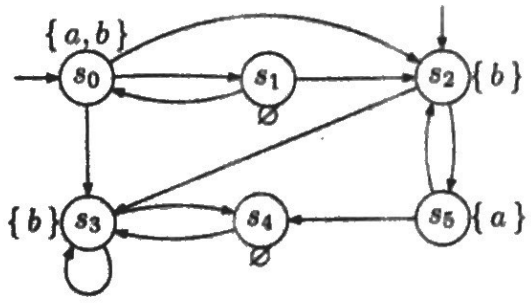
Proposer un nombre minimal de propositions atomiques et des formules CTL permettant de spécifier les propriétés suivantes :

1. L'ascenseur se met en marche seulement lorsqu'il y a eu un appel.
2. A n'importe quel instant, il est possible de ramener l'ascenseur au RdC.
3. Le voyant indique correctement les appels : chaque fois que l'ascenseur est appelé à l'étage i, cette requête reste active jusqu'à ce que l'ascenseur arrive à l'étage i.
4. S'il bouge, l'ascenseur ne s'arrête qu'aux étages où il a été appelé.

Exercice 2 On considère la formule CTL suivante :

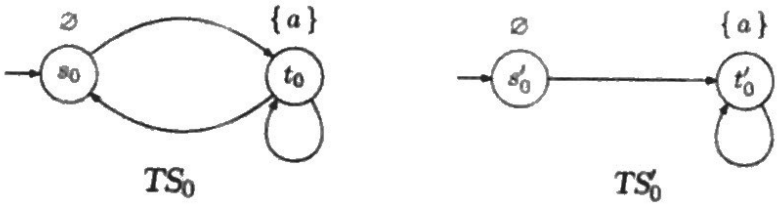
$$\Phi = \mathbf{AX}(\mathbf{A}(\neg a\,\mathbf{U}\,b) \wedge \mathbf{AF}\,\mathbf{EX}(\neg a \wedge \neg b))$$

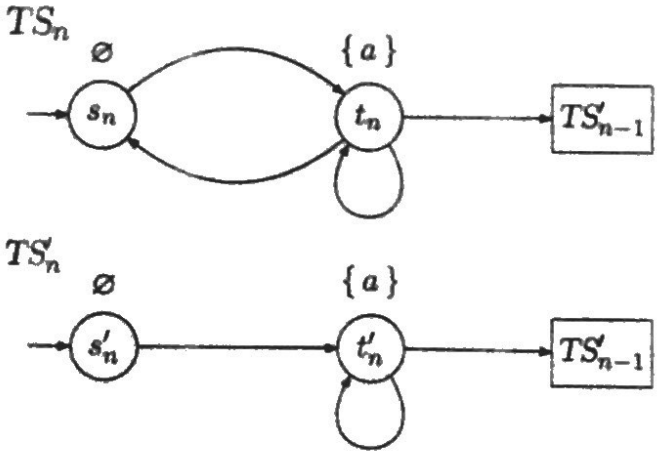
1. Mettez Φ en forme normale existentielle.
2. Calculez $\mathsf{Sat}(\Psi)$ en suivant l'algorithme vu en cours sur le système de transitions suivant.



Exercice 3 Avec cet exercice on peut montrer que la formule LTL $\mathbf{F}\,\mathbf{G}\,a$ n'est pas exprimable en CTL.

On définit les systèmes de transitions TS_n et TS'_n ($n \geq 0$) suivants, par induction (voir figure ce-dessous) :


∅
{a}
s_0
t_0
TS_0
∅
{a}
s'_0
t'_0
TS'_0


TS_n
∅
{a}
s_n
t_n
TS'_{n-1}
TS'_n
∅
{a}
s'_n
t'_n
TS'_{n-1}

1. Déterminez lequel ST parmi TS_n et TS'_n satisfait la formule $\mathbf{F}\,\mathbf{G}\,a$, en justifiant votre réponse.
2. Est-ce que TS_n et TS'_n sont bisimilaires ? Justifiez votre réponse. Si non, indiquez une formule CTL qui les distingue.
3. Supposez que Φ est une formule CTL utilisant seulement les operateurs temporels **EX**, **AX** (en dehors des combinateurs booléens). Montrez par induction que Φ ne peut pas distinguer TS_n et TS'_n si le nombre d'opérateurs de Φ est au plus n.

   Indication : vous allez montrer que $s_n \equiv_n s'_n$, $t_n \equiv_n t'_n$, $s_n \equiv_{n-1} s'_{n-1}$, $t_n \equiv_{n-1} t'_{n-1}$, où $s \equiv_k t$ signifie que les états s, t satisfont les mêmes formules ayant au plus k opérateurs.
4. Supposons qu'on a montré que TS_n et TS'_n satisfont les mêmes formules CTL de longueur au plus n. Déduisez que la formule $\mathbf{F}\,\mathbf{G}\,a$ n'est pas exprimable en CTL.

Exercice 4 Dans cet exercice on cherche un algorithme pour calculer directement $\mathsf{Sat}(\mathbf{AF}\,\phi)$, étant donné $U = \mathsf{Sat}(\phi)$ pour un système de transitions *fini* avec ensemble d'états S.

1. Soit $T \subseteq S$ un ensemble d'états qui satisfait les deux propriétés suivantes :

   (P1) $U \subseteq T$, et

   (P2) Si $s \in S$ est tel que $\mathsf{post}(s) \subseteq T$, alors $s \in T$.

   Montrez que $\mathsf{Sat}(\mathbf{AF}\,\phi) \subseteq T$.

   Indication : vous pouvez procéder par récurrence selon la profondeur minimale d'un arbre qui témoigne que s satisfait $\mathbf{AF}\,\phi$.
2. Déduisez de la question précedente que $\mathsf{Sat}(\mathbf{AF}\,\phi)$ est le plus petit sous-ensemble $T \subseteq S$ qui satisfait les deux propriétés (P1) et (P2).
3. Proposez un algorithme direct qui calcule $\mathsf{Sat}(\mathbf{AF}\,\phi)$ à partir de $U = \mathsf{Sat}(\phi)$. Quelle est la complexité de votre algorithme ?

Examen "Introduction à la vérification", partie 2

Master 1 Informatique, 2018–2019

Jeudi 2 mai 2019 — 14h30–17h30

Exercice 1 Soit φ la formule LTL suivante sur l'alphabet $\Sigma = \{a, b, c\}$:

$$\mathsf{G}(a \Rightarrow \mathsf{X}b) \wedge \mathsf{F}\,\mathsf{G}(a \vee b)$$

1. Donner une expression ω-rationnelle équivalente à φ. On rappelle qu'une telle expression permet d'utiliser, en plus de l'étoile, de la concaténation et de l'union, la répétition infinie : si L est un langage de mots finis, $L^\omega = \{u_0 u_1 u_2 \cdots \mid u_i \in L\}$.
2. Construire un automate de Büchi équivalent à φ.
   Remarque. Il est déconseillé d'utiliser directement l'algorithme vu en cours, il produit trop d'états.
3. Donnez une formule de la logique du premier ordre FO($<$) équivalente à φ.

Exercice 2 On fixe un ensemble AP de propositions atomiques et on note $\Sigma = 2^{\mathrm{AP}}$. L'opérateur *Release* est dual de l'opérateur *Until* :

$$\alpha\,\mathsf{R}\,\beta = \neg(\neg\alpha\,\mathsf{U}\,\neg\beta).$$

1. Montrer que $\alpha\,\mathsf{R}\,\beta = \mathsf{G}\beta \vee (\beta\,\mathsf{U}\,(\alpha \wedge \beta))$.

On définit la classe des E-formules par la syntaxe suivante :

$$\varphi ::= \mathsf{F}\alpha \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathsf{X}\varphi \mid \alpha\,\mathsf{U}\,\varphi \mid \varphi\,\mathsf{R}\,\varphi$$

où α est une formule arbitraire de LTL.

2. Montrer que pour toute E-formule φ, pour tout mot infini $w \in \Sigma^\omega$, pour tous entiers i, j tels que $0 \leqslant i \leqslant j$:

   $$w, j \models \varphi \Longrightarrow w, i \models \varphi$$

   On pourra raisonner par récurrence sur la longueur de la construction de φ par la grammaire.

On définit la classe des A-formules par la syntaxe suivante :

$$\psi = \mathsf{G}\varphi \mid \neg\psi \mid \psi \vee \psi \mid \mathsf{X}\psi \mid \alpha\,\mathsf{U}\,\psi$$

où φ est une E-formule arbitraire et α une formule arbitraire de LTL.

3. Soit ψ une A-formule, $w \in \Sigma^\omega$, et i, j deux entiers. A-t-on l'équivalence suivante ?

   $$w, j \models \varphi \Longleftrightarrow w, i \models \varphi$$

4. Soit ψ une A-formule et α une formule de LTL. Les formules ψ, $\mathsf{X}\psi$ et $\alpha\,\mathsf{U}\,\psi$ sont-elles équivalentes ?

Exercice 3 Pour un automate probabiliste fini $\mathcal{A}$ sur un alphabet A, on note $[\![\mathcal{A}]\!]$ sa sémantique. Autrement dit, pour tout mot $w \in A^*$, la probabilité que w soit accepté par $\mathcal{A}$ est $[\![\mathcal{A}]\!](w)$. Pour $\alpha \in [0, 1]$, on note $L_{>\alpha}(\mathcal{A})$ l'ensemble des mots de A^* acceptés avec probabilité strictement supérieure à α.

1. (Question de cours) Que peut-on dire du problème suivant :

   Donnée Un automate probabiliste $\mathcal{A}$ et un rationnel α de l'intervalle $[0, 1]$.

   Question A-t-on $L_{>\alpha} \neq \emptyset$?

On dit qu'un réel α est un point de coupure isolé s'il existe $\delta > 0$ tel que pour tout mot $w \in A^*$

$$\left| [\![\mathcal{A}]\!](w) - \alpha \right| > \delta.$$

Autrement dit, aucun mot n'a une probabilité d'acceptation dans l'intervalle $[\alpha - \delta, \alpha + \delta]$. On veut montrer que le problème suivant est indécidable :

Donnée Un automate probabiliste $\mathcal{A}$ et un rationnel α de l'intervalle $[0, 1]$.

Question α est-il un point de coupure isolé pour $\mathcal{A}$?

Pour cela, on propose une réduction à partir d'une variante du problème de correspondance de Post, déjà connue indécidable. Étant donné deux mots u, v, on note $u \wedge v$ le plus long suffixe commun à u et v Par exemple, $aba\underline{aac} \wedge abad\underline{aac} = aac$.

Le problème suivant est connu indécidable :

Donnée Deux morphismes $f_i : A^* \to \{0,1\}^*$ $(i = 1, 2)$ tels que $f_i(A) \subseteq 1\{0,1\}^*$.

Question L'ensemble de mots $\{f_1(w) \wedge f_2(w) \mid w \in \Sigma^*\}$ est-il fini ?

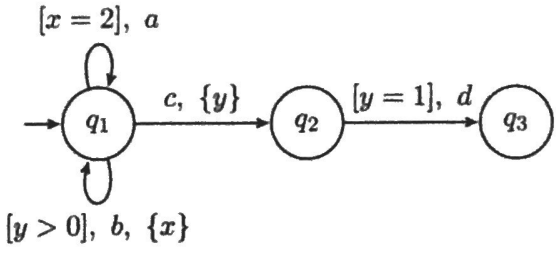
On rappelle la notation du cours pour passer d'un morphisme à une fonction calculée par un automate probabiliste : on définit $\overline{\varepsilon} = 0$ et, pour $w = a_1 \cdots a_n \in \{0,1\}^+$,

$$\overline{w} = \frac{a_n}{2^1} + \frac{a_{n-1}}{2^2} + \cdots + \frac{a_1}{2^n}.$$

Enfin, pour $i = 1, 2$ et $w \in A^*$, on pose $\phi_i(w) = \overline{f_i(w)}$.

2. Montrer l'équivalence $(a) \iff (b)$ des deux points suivants :
   - (a) Il existe $\delta > 0$ tel que, pour tout $w \in A^+$, $|\phi_1(w) - \phi_2(w)| \geqslant \delta$.
   - (b) L'ensemble $\{f_1(w) \wedge f_2(w) \mid w \in \Sigma^*\}$ est fini.
3. En vous inspirant d'une construction du cours, décrire un automate probabiliste $\mathcal{A}$ construit à partir de deux morphismes f_1, f_2 tel que $1/2$ est point de coupure isolé dans $\mathcal{A}$ si et seulement si l'ensemble de mots $\{f_1(w) \wedge f_2(w) \mid w \in \Sigma^*\}$ est fini.
4. Que peut-on conclure de la question précédente ?

Exercice 4 On considère l'automate temporisé suivant :



Les gardes sont indiquées entre crochets [ ], et les resets entre accollades {}.

1. La configuration $(q_3,\ x = 1,\ y = 2)$ est-elle accessible ? Si oui, donner un mot temporisé parvenant à cette configuration, et sinon, justifier. Même question pour la configuration $(q_3,\ x = 3,\ y = 2)$.
2. Calculer les régions de cet automate.
3. Calculer l'automate des régions et vérifier les réponses données à la question 1.