Corrigé

Examen de model checking

EPITA ING2 CSI/SCIA 2011 S4; A. DURET-LUTZ

Durée : 1 heure 30

Juin 2010

Consignes

- Tous les documents sur papier sont autorisés (livres, notes de cours, polycopiés...).
  Les calculatrices, téléphones, et autres engins électroniques ne le sont pas.
- Répondez sur le sujet dans les cadres prévus à cet effet.
- **Dans les QCM, une absence de réponse sera préférée à une réponse erronée.**
  Vous avez le droit de faire quelques erreurs, mais s'il y a en trop vous aurez des points en moins.
- Il y a 5 pages d'énoncé. Le barème, indicatif, correspond à une note sur 32.

1 LTL (9 points)

Rappel : pour deux formules LTL f_1 et f_2, et une séquence infinie σ (la séquence privée des i premières lettres est notée $\sigma^{i..}$), on a

$$\begin{aligned}
&\sigma \models \mathbf{X} f_1 && \text{ssi } \sigma^{1..} \models f_1\\
&\sigma \models f_1 \mathbf{U} f_2 && \text{ssi } \exists i \geq 0 \text{ tel que } \sigma^{i..} \models f_2 \text{ et } \forall j \in [\![0, i-1]\!],\ \sigma^{j..} \models f_1
\end{aligned}$$

1. **(2 pts)** Justifiez formellement que $(\mathbf{X} f_1)\,\mathbf{U}(\mathbf{X} f_2) \equiv \mathbf{X}(f_1 \mathbf{U} f_2)$

Réponse :

$$\begin{aligned}
\sigma \models (\mathbf{X} f_1)\,\mathbf{U}(\mathbf{X} f_2) &\iff \exists i \geq 0 \text{ tel que } \sigma^{i..} \models \mathbf{X} f_2 \text{ et } \forall j \in [\![0, i-1]\!],\ \sigma^{j..} \models \mathbf{X} f_1\\
&\iff \exists i \geq 0 \text{ tel que } \sigma^{(i+1)..} \models f_2 \text{ et } \forall j \in [\![0, i-1]\!],\ \sigma^{(j+1)..} \models f_1\\
&\iff \sigma^{1..} \models f_1 \mathbf{U} f_2\\
&\iff \sigma \models \mathbf{X}(f_1 \mathbf{U} f_2)
\end{aligned}$$

2. **(2 pts)** Justifiez formellement que pour toute formule LTL φ, on a $\mathbf{G}\,\mathbf{X}\,\varphi \equiv \mathbf{X}\,\mathbf{G}\,\varphi$ et $\mathbf{F}\,\mathbf{X}\,\varphi \equiv \mathbf{X}\,\mathbf{F}\,\varphi$.

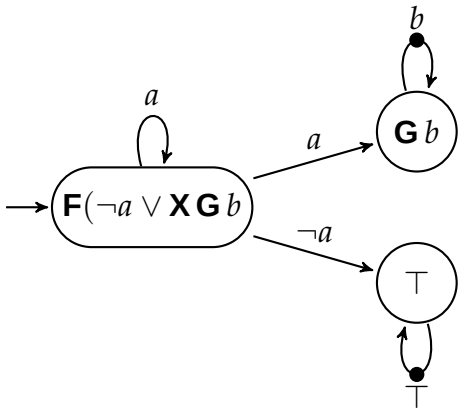
Réponse :

Comme $\mathbf{F}\,\varphi = \top\,\mathbf{U}\,\varphi$ par définition, on a $\mathbf{X}\,\mathbf{F}\,\varphi = \mathbf{X}(\top\,\mathbf{U}\,\varphi) = (\mathbf{X}\top)\,\mathbf{U}(\mathbf{X}\,\varphi) = \top\,\mathbf{U}(\mathbf{X}\,\varphi) = \mathbf{F}\,\varphi$.

D'autre par $\mathbf{G}\,\varphi = \neg(\mathbf{F}\neg\varphi)$. On en déduit que $\mathbf{X}\,\mathbf{G}\,\varphi = \mathbf{X}\neg(\mathbf{F}\neg\varphi) = \neg\mathbf{X}(\mathbf{F}\neg\varphi) = \neg(\mathbf{F}\,\mathbf{X}\neg\varphi) = \neg(\mathbf{F}\neg\mathbf{X}\,\varphi) = \mathbf{G}\,\mathbf{X}\,\varphi$.

3. **(5 pts)** Dessinez un automate de Büchi (étiqueté sur états ou transitions, généralisé ou non) reconnaissant la formule LTL $\mathbf{F}(a \rightarrow \mathbf{G}\,\mathbf{X}\,b)$. On ne vous demande pas de justification, mais on vous conseille de le construire au brouillon avec une approche par tableau.

Réponse :



2 Classes de propriétés (23 points)

Nous avons vu en cours que les propriétés que l'on souhaite vérifier sur des systèmes peuvent être représentées sous formes de formules (LTL, logique monadique, expressions ω-rationnelles...) ou d'automates. Quel que soit le formalisme utilisé pour les représenter, ces propriétés peuvent être interprétées sous forme de langage : le langage associé à une formule LTL ou celui associé à un automate, est l'ensemble des exécutions qui vérifient la propriété. L'objectif de cet exercice est d'étudier deux classes de propriétés, définies en fonction de caractéristiques du langage reconnu.

Soit Σ un alphabet, et soit $\Phi \subseteq \Sigma^+$ un ensemble de séquences finies de taille non nulle. On appellera un tel ensemble Φ une propriété finie.

Soit $\Pi \subseteq \Sigma^\omega$ un ensemble de séquences infinies. On appellera un tel ensemble Π une propriété infinie.

2.1 Les opérations A et E (13 points)

Pour une propriété finie Φ, on note

$$A(\Phi) = \{\sigma \in \Sigma^\omega \mid \forall i > 0,\ \sigma^{0..i} \in \Phi\} \tag{1}$$

$$E(\Phi) = \{\sigma \in \Sigma^\omega \mid \exists i > 0,\ \sigma^{0..i} \in \Phi\} \tag{2}$$

où $\sigma^{0..i}$ désigne la séquence finie des $i+1$ premières lettres de σ.

C'est-à-dire que $A(\Phi)$ est l'ensemble des séquences infinies dont tous les préfixes appartiennent à Φ, tandis que $E(\Phi)$ est l'ensemble des séquences infinies qui ont au moins un préfixe dans Φ.

Par exemple si Φ est la propriété dénotée par l'expression rationnelle $a^+ \cdot b^\star$ définie sur $\Sigma = \{a, b\}$, ce qu'on notera simplement $\Phi = a^+ \cdot b^\star$, alors $A(\Phi) = a^\omega + (a^+ \cdot b^\omega)$.

1. **(1 pt)** Si $\Phi = a^+ \cdot b^\star$, quelle expression ω-rationnelle dénote $E(\Phi)$?

Réponse :

$E(\Phi) = (a^+ \cdot b^\star) \cdot \Sigma^\omega = a^+ \cdot \Sigma^\omega$

2. **(3 pts)** Si Φ est une propriété rationnelle, elle peut-être représentée par un automate fini $\mathcal{A}$. Expliquez comment construire, à partir de $\mathcal{A}$, un automate de Büchi $E(\mathcal{A})$ représentant la propriété $E(\Phi)$. Vous aurez ainsi prouvé que si Φ est rationnel, alors $E(\Phi)$ est ω-rationnel.

Réponse :

À partir de n'importe quel état final de $\mathcal{A}$, doit maintenant accepter n'importe quelle suite, c'est-à-dire $\Sigma^\star$.
On construit donc $E(\mathcal{A})$ en y copiant la structure de $\mathcal{A}$, et en y ajoutant un nouvel état x. On connecte tous les états finaux de $\mathcal{A}$ à x par des transitions étiquetées par Σ. x lui-même possède une boucle étiquetées par Σ, et on impose que les séquences infinie terminent sur x en utilisant une condition d'acceptation qui porte sur x ou sa boucle.

3. **(1 pt)** Si $\Phi = a^+ \cdot b$, quelle expression ω-rationnelle dénote $A(\Phi)$?

Réponse :

$A(\Phi) = a^\omega$

4. **(1 pt)** Justifiez simplement que si l'ensemble des séquences Φ est de cardinalité finie (par exemple $\Phi = (a \cdot b) + (b \cdot a)$ n'accepte que deux séquences) alors $A(\Phi) = \emptyset$.

Réponse :

Si Φ est un ensemble fini (contenant un seul élément), il ne peut donc pas contenir tous les préfixes d'une séquence infinie. L'ensemble des séquences infinies dont les préfixes sont tous dans Φ est donc vide.

5. **(1 pt)** Justifiez que si $\Phi = (a \cdot b)^+$ alors $A(\Phi) = \emptyset$.

Réponse :

La seule séquence infinie qu'on puisse construire sur Φ est $(a \cdot b)^\omega$, mais elle possède aussi une infinité de préfixes de la forme $(a \cdot b)^\star \cdot a$ qui n'appartiennent pas à Φ.

6. **(3 pts)** Pour une propriété finie Φ, on note $\overline{\Phi} = \Sigma^+ \setminus \Phi$. Pour une propriété infinie, on note Π, on note $\overline{\Pi} = \Sigma^\omega \setminus \Pi$. Justifiez que $\overline{A(\Phi)} = E(\overline{\Phi})$ et $\overline{E(\Phi)} = A(\overline{\Phi})$.

Réponse :

$$\begin{aligned}
A(\overline{\Phi}) &= \{\sigma \in \Sigma^\omega \mid \forall i > 0,\, \sigma^{0..i} \in \overline{\Phi}\} \\
&= \{\sigma \in \Sigma^\omega \mid \forall i > 0,\, \sigma^{0..i} \notin \Phi\} \\
&= \{\sigma \in \Sigma^\omega \mid \neg\exists i > 0,\, \sigma^{0..i} \in \Phi\} \\
&= \overline{\{\sigma \in \Sigma^\omega \mid \exists i > 0,\, \sigma^{0..i} \in \Phi\}} \\
&= \overline{E(\Phi)}
\end{aligned}$$

La démonstration est similaire pour $\overline{A(\Phi)} = E(\overline{\Phi})$.

7. **(2 pt)** Sachant que les langages ω-rationnels sont clos par complémentation, démontrez que si Φ est rationnel, alors $A(\Phi)$ est ω-rationnel.

Réponse :

Φ rationnel
$\iff \overline{\Phi}$ rationnel
$\iff E(\overline{\Phi})$ ω-rationnel d'après la question 2
$\iff \overline{E(\overline{\Phi})}$ ω-rationnel d'après l'énoncé
$\iff A(\overline{\Phi})$ ω-rationnel d'après la question précédente

2.2 Sureté et garantie (5 points)

– Π est une propriété de **sûreté** ssi il existe une propriété finie Φ telle que $\Pi = A(\Phi)$.
– Π est une **garantie** ssi il existe une propriété finie Φ telle que $\Pi = E(\Phi)$.

1. **(2.5 pts)** Indiquez le type des propriétés dénotées par les expressions ω-rationnelles suivantes :
   (a) a^ω
   ☒ sûreté ☐ garantie ☐ aucun des deux
   (b) $b \cdot a^\omega$
   ☒ sûreté ☐ garantie ☐ aucun des deux
   (c) $a^\omega + (a^+ \cdot b^\omega)$
   ☒ sûreté ☐ garantie ☐ aucun des deux
   (d) $a \cdot b^\star \cdot \Sigma^\omega$
   ☐ sûreté ☒ garantie ☐ aucun des deux
   (e) $b^+ \cdot a^\omega$
   ☐ sûreté ☐ garantie ☒ aucun des deux
2. **(2.5 pts)** Indiquez le type des propriétés dénotées par les formules LTL suivantes :
   (a) $a \,\mathbf{U}\, b$
   ☐ sûreté ☒ garantie ☐ aucun des deux
   (b) $b \wedge \mathbf{F}(a)$
   ☐ sûreté ☒ garantie ☐ aucun des deux
   (c) $\mathbf{G}(b \wedge a)$
   ☒ sûreté ☐ garantie ☐ aucun des deux
   (d) $\mathbf{X}(\mathbf{X}(a))$
   ☐ sûreté ☒ garantie ☐ aucun des deux
   (e) $a \,\mathbf{U}\, b$
   ☐ sûreté ☒ garantie ☐ aucun des deux

2.3 Automates faibles (5 points)

Un automate de Büchi (non généralisé) avec condition d'acceptation sur les états est **faible** si chaque Composante Fortement Connexe acceptante ne contient que des états acceptants, et si les CFC non acceptantes ne possèdent pas d'états acceptants.

Une définition similaire peut être faite pour les automates de Büchi dont les conditions d'acceptation portent sur les transitions : les transitions de toutes les CFC doivent être acceptantes et seulement celles-ci.

Il se trouve que les propriétés de sûreté et de garantie peuvent être représentées par des automates de Büchi faibles (et même déterministes).

1. **(2 pts)** Justifiez qu'une propriété ω-rationnelle qui est une garantie puisse se représenter par un automate de Büchi faible.

Réponse :

Toutes les garanties sont le la forme $\Phi \cdot \Sigma^\star$.
Un automate pour une telle propriété peut se construire comme on l'a vu précédement en reliant les états finaux d'un automate fini représentant Φ à un nouvel état x possédant un boucle étiquetée par Σ.
Ce seul état étant acceptant (ou sa boucle l'est), on a bien un automate faible.

2. **(3 pts)** Expliquez pourquoi l'*emptiness check* d'un automate de Büchi faible peut se faire avec un simple parcours en profondeur (au lieux des deux parcours imbriqués nécessaires dans le cas général) sans même chercher à trouver les composantes fortement connexes.

Réponse :

Si un cycle est acceptant, tous les états du cycles le sont.
Ainsi si le parcours en profondeur tombe sur un état acceptant qui est sur sa pile de recherche, il peut s'arrêter car il a trouvé un cycle acceptant.
À l'inverse, s'il de retombe jamais sur un état acceptant de sa pile de recherche, il n'existe pas de cycle acceptant dans l'automate.