Correction

Examen de model checking

EPITA ING2 CSI/SCIA 2010 S4; A. DURET-LUTZ, A. HAMEZ, A. LINARD

Durée : 1 heure 30

Juillet 2009

Consignes

– Tous les documents sur papier sont autorisés (livres, notes de cours, polycopiés...), ainsi que les salières.
  Les calculatrices, téléphones, PSP 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 6 pages. Rappelez votre nom en haut de chaque feuille au cas où elles se mélangeraient.
– Le barème est indicatif et correspond à une note sur 31, plus 1 point bonus.

1 Stutter-Invariance (13 points)

Dans toute cette section, on considère des séquences d'exécution étiquetées par les propositions a et b, c'est-à-dire des ω-mots sur $2^{\{a,b\}}$.

Intuitivement, une propriété *stutter-invariant* est une propriété insensible au bégaiement des exécutions.

Par exemple la formule LTL $a \,\mathbf{U}\, b$ est un propriété *stutter-invariant* car dans n'importe quelle séquence d'exécution qui la vérifie (par exemple $a\bar{b} \cdot a\bar{b} \cdot \bar{a}b \cdot ab \cdot ab \cdot ab \cdots$) on peut répéter n'importe quels états et obtenir une séquence (comme $a\bar{b} \cdot a\bar{b} \cdot a\bar{b} \cdot \bar{a}b \cdot \bar{a}b \cdot ab \cdot ab \cdot ab \cdots$) qui vérifiera elle aussi la propriété.

À l'inverse, la formule LTL $a \wedge \mathbf{X}\, b$ n'est pas *stutter-invariant*. En effet elle est vérifiée par $a\bar{b} \cdot \bar{a}b \cdot ab \cdots$ mais pas par $a\bar{b} \cdot a\bar{b} \cdot \bar{a}b \cdot ab \cdots$

Plus formellement, étant donné un ω-mot $w = w_0 \cdot w_1 \cdot w_2 \cdots$ et une fonction $f : \mathbb{N} \mapsto \mathbb{N}^+$ notons

$$w[f] = w_0^{f(0)} \cdot w_1^{f(1)} \cdot w_2^{f(2)} \cdots$$

avec la convention que w_i^n désigne la concaténation de n copies de w_i.

Un langage L est dit *stutter-invariant* si pour tout mot w et toute fonction $f : \mathbb{N} \mapsto \mathbb{N}^+$, on a

$$w \in L \iff w[f] \in L$$

Une formule LTL est dite *stutter-invariant* si le langage des mots qu'elle reconnaît est *stutter-invariant*.

Enfin **un mot** w est *stutter-free* si pour tout $i \geq 0$, $w_i \neq w_{i+1}$, ou bien $w_i = w_j$ pour tout $j > i$.

1. **(1,5 points)**Les mots suivants sont-ils *stutter free* ?
   – $ab \cdot \bar{a}b \cdot \bar{a}\bar{b} \cdot \bar{a}\bar{b} \cdot \bar{a}\bar{b} \cdot \bar{a}\bar{b} \cdots$
     ☒ oui ☐ non
   – $ab \cdot a\bar{b} \cdot a\bar{b} \cdot ab \cdot ab \cdots$
     ☐ oui ☒ non

– $ab \cdot ab \cdot ab \cdot ab \cdots$
☒ oui ☐ non

2. **(4 points)** Les formules LTL suivantes sont elles *stutter-invariant* ?
– a
☒ oui ☐ non
– $\mathbf{G}\, a$
☒ oui ☐ non
– $\mathbf{X}\,\mathbf{G}\, a$
☐ oui ☒ non
– $\mathbf{F}(a \vee \mathbf{G}\, b)$
☒ oui ☐ non
– $\mathbf{G}(a \rightarrow \mathbf{F}\, b)$
☒ oui ☐ non
– $\mathbf{G}\,\mathbf{F}(a \rightarrow \mathbf{G}\,\mathbf{F}\, b)$
☒ oui ☐ non
– $\mathbf{G}(a \rightarrow \mathbf{X}\, b)$
☐ oui ☒ non
– $\mathbf{F}\,\mathbf{X}\, b$
☐ oui ☒ non

3. **(4,5 points)** Le langage

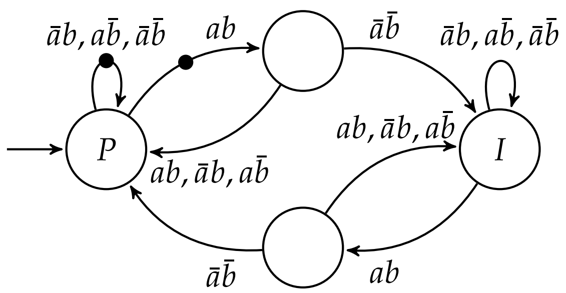
$$L = \{w \in (2^{\{a,b\}})^\omega \mid \text{la sous-séquence } ab \cdot \bar{a}\bar{b} \text{ apparaît un nombre pair de fois dans } w\}$$

est-il :
– rationnel ?
☐ oui ☒ non
– ω-rationnel ?
☒ oui ☐ non
– stutter-invariant ?
☒ oui ☐ non
– reconnaissable par une formule LTL ?
☐ oui ☒ non
Si oui, laquelle ?

Réponse :

– reconnaissable par un automate de Büchi (généralisé ou non) ?
☒ oui ☐ non
Si oui, lequel ?

Réponse :



avec $\mathcal{F} = \{\bullet\}$

Dans l'état P, l'automate a lu un nombre pair de sous-séquences $ab \cdot \bar{a}\bar{b}$, et il peut y passer infiniment (les transitions sortantes de cet état sont donc acceptantes, on aurait pu convenir de marquer les transitions entrantes à la place, ou même en plus). Dans l'état I il n'a lu qu'un nombre impair de sous-séquences, et ne doit donc y passer qu'un nombre fini de fois.

4. **(3 points)** Pour un langage L, notons $SF(L) = \{w \in L \mid w \text{ est } \textit{stutter-free}\}$ l'ensemble des mots *stutter-free* de L.
   – Soient L et L' deux langages *stutter-invariant*. Est-il correct de dire que $L = L'$ si et seulement si ces deux langages possèdent les même mots *stutter-free* ? Justifiez votre réponse.

Réponse :

Oui.
Si $L = L'$ il est évident que $SF(L) = SF(L')$.
À l'inverse supposons par l'absurde que $SF(L) = SF(L')$ mais qu'il existe un mot w de L qui n'est pas dans L'.
Il est facile de trouver un mot *stutter-free* v et une fonction f telle que $v[f] = w$: il suffit de supprimer (et compter) toutes les répétitions finies de w. Par définition d'un langage *stutter-invariant*, on a $v[f] \in L \iff v \in L$, donc v est un mot *stutter-free* de L. Autrement dit $v \in SF(L)$. Comme on a supposé que $SF(L) = SF(L')$ on en déduit que $v \in L'$ et donc $v[f] \in L'$. Cela contredit l'hypothèse que $w = v[f] \notin L'$. Conclusion : si $SF(L) = SF(L')$ alors $L = L'$.

   – Soient L et L' deux langages quelconques. Est-il correct de dire que $L = L'$ si et seulement si ces deux langages possèdent les même mots *stutter-free* ? Justifiez votre réponse.

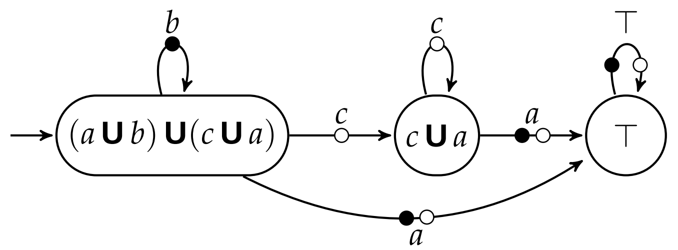
Réponse :

Bien sûr que non. Par exemple $L = \{bba^\omega\}$, $L' = \{bbba^\omega\}$ sont deux langages différents ne possèdent qu'un seul mot qui bégaye initialement. On a pourtant $SF(L) = SF(L') = \emptyset$.

2 Traduction de LTL (8 points)

1. **(6 points)** Dessinez un automate de Büchi (étiqueté sur états ou transitions, généralisé au non) reconnaissant la formule LTL $(a \,\mathbf{U}\, b) \,\mathbf{U}\, (c \,\mathbf{U}\, a)$. On ne vous demande pas de justification, mais on vous conseille de le construire au brouillon avec une approche par tableau.

Réponse :

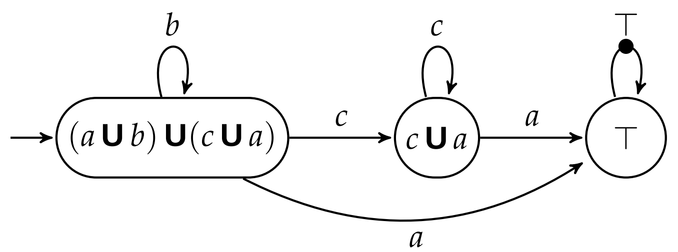


avec $\mathcal{F} = \{\bullet, \circ\}$

2. **(2 points)** L'automate construit ci-dessus possède normalement plusieurs conditions d'acceptation. Sont-elles toutes utiles ? Est-il possible de se limiter à une seule condition d'acceptation sans rajouter d'états ? (Dans l'affirmative, dessinez le nouvel automate.)

Réponse :

Seul l'état $\top$ peut-être visité infiniment souvent. Il suffit de ne garder qu'une condition d'acceptation pour l'indiquer.



avec $\mathcal{F} = \{\bullet\}$

3 Simplification de formules LTL (5 points)

Considérons une formule LTL du type $\alpha \wedge \beta$ où α et β sont deux sous-formules LTL.

Si l'on sait montrer que $\alpha \implies \beta$ alors la formule $\alpha \wedge \beta$ peut être réécrite simplement α.

Par exemple la formule $(\mathbf{G}\, a) \wedge (\mathbf{X}\, a)$ peut-être simplifiée en $\mathbf{G}\, a$, car on a $(\mathbf{G}\, a) \implies (\mathbf{X}\, a)$.

– **(2 points)** Supposez que l'on vous demande d'écrire un algorithme de simplification de formules LTL implémentant ce type de réécritures. Étant donné deux sous-formules α et β, comment feriez-vous pour tester si $\alpha \implies \beta$? (Indice : pensez à ce que cela signifie au niveau des langages, et comment cela peut-être testé avec des automates.)

Réponse :

$\alpha \implies \beta$ ssi $\mathscr{L}(A_\alpha \otimes A_{\neg\beta}) = \emptyset$. On peut donc traduire α et $\neg\beta$ sous forme d'automates de Büchi, et vérifier que leur produit est vide.

– **(1 point)** Supposez que vous ayez prouvé que $\alpha \implies \beta$. Comment simplifieriez-vous la formule LTL $\alpha\, \mathbf{U}\, \beta$?

Réponse :

Si $\alpha \implies \beta$ alors $\alpha\, \mathbf{U}\, \beta \equiv \beta$.

– **(2 points)** Quelle condition sur α et β faut-il pour avoir le droit de simplifier $\alpha\, \mathbf{U}\, \beta$ en $\mathbf{F}\, \beta$?

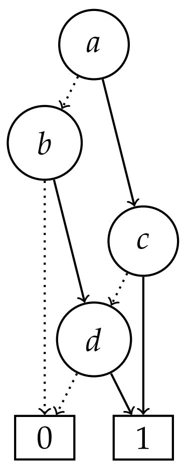
Réponse :

Si $(\neg\beta) \implies \alpha$ alors $\alpha\, \mathbf{U}\, \beta \equiv \mathbf{F}\, \beta$.

4 BDD (5 points)

Dessinez un BDD (réduit et ordonné) représentant la formule $(a \vee b) \wedge (c \vee d) \wedge (a \vee d)$. Pour ordonner les variables, vous choisirez l'ordre alphabétique.

Réponse :



5 Un peu de sel dans ce partiel (1 point bonus)

Question bonus pour ceux qui ne sont pas venus en cours, ou qui sont ici par hasard.

Lors d'un pique-nique sur la plage de l'Aquaboulevard, Damien a renversé le contenu d'une salière sur le sable. Décrivez un procédé permettant de séparer le sel du sable. Les réponses utilisant les outils théoriques du cours seront préférées à celles utilisant des notions de physique-chimie vues en 5^{e}.

Réponse :

Les pique-niques sont interdits à l'Aquaboulevard.