Correction

Examen de model checking

EPITA ING2 CSI 2009 S4; A. DURET-LUTZ, A. HAMEZ, A. LINARD

Durée : 1 heure 30

Juin 2008

Consignes

- Tous les documents sur papier sont autorisés (livres, notes de cours, polycopiés...).
  Les calculatrices, téléphones, PSP et autres engins électroniques ne le sont pas.
- Répondez sur le sujet dans les cadres, lignes, ou figures prévus à cet effet.
- Il y a 5 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 24.

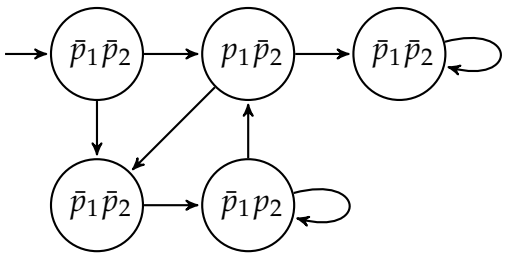


FIG. 1 – Structure de Kripke. Elle sert telle quelle dans l'exercice 1 ; puis vous devrez la modifier dans l'exercice 2

.

1 CTL vs LTL (6 points)

p_1 et p_2 désignent deux propositions atomiques.

Pour chaque formule ci-dessous, indiquez
- S'il s'agit d'une formule LTL ou CTL,
- si elle peut être traduite dans l'autre logique (p.ex. si la formule donnée est une formule CTL, indiquez si elle peut se traduire en LTL) et si oui, donnez la formule équivalente,
- si la structure de Kripke de la figure 1 (avant les modifications de l'exercice 2 vérifie la formule en question.

1. $\mathbf{F}(p_1)$
   ☒ LTL ou □ CTL ?
   □ Pas traduisible ☒ Traduisible : $\mathbf{A}\,\mathbf{F}\,p_1$
   ☒ Vraie ou □ fausse sur la structure de Kripke ?
2. $\mathbf{F}(p_2 \wedge \mathbf{X}\,p_1)$
   ☒ LTL ou □ CTL ?
   ☒ Pas traduisible □ Traduisible :
   □ Vraie ou ☒ fausse sur la structure de Kripke ?

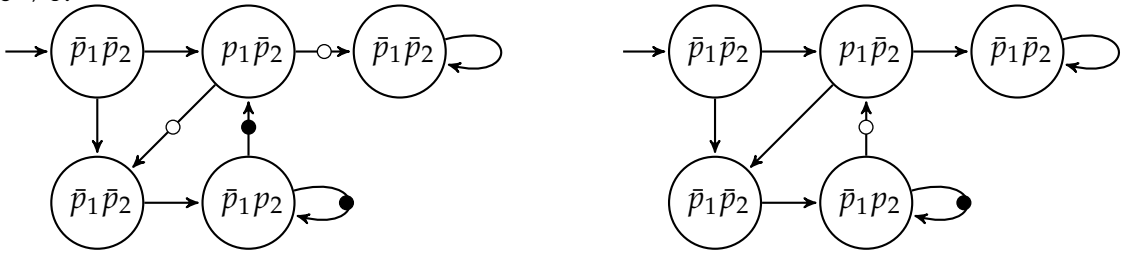
3. $\mathbf{A}\,\mathbf{G}(p_1 \rightarrow \mathbf{E}\,\mathbf{F}\,p_2)$
   ☐ LTL ou ☒ CTL ?
   ☒ Pas traduisible ☐ Traduisible :
   ☒ Vraie ou ☐ fausse sur la structure de Kripke ?
4. $\mathbf{A}\,\mathbf{G}(p_1 \rightarrow \mathbf{A}\,\mathbf{F}\,p_2)$
   ☐ LTL ou ☒ CTL ?
   ☐ Pas traduisible ☒ Traduisible : $\mathbf{G}(p_1 \rightarrow \mathbf{F}\,p_2)$
   ☐ Vraie ou ☒ fausse sur la structure de Kripke ?
5. $\mathbf{E}\,\mathbf{G}(p_1 \rightarrow \mathbf{A}\,\mathbf{F}\,p_2)$
   ☐ LTL ou ☒ CTL ?
   ☒ Pas traduisible ☐ Traduisible :
   ☐ Vraie ou ☒ fausse sur la structure de Kripke ?
6. $\mathbf{E}\,\mathbf{G}(p_1 \rightarrow \mathbf{E}\,\mathbf{F}\,p_2)$
   ☐ LTL ou ☒ CTL ?
   ☒ Pas traduisible ☐ Traduisible :
   ☒ Vraie ou ☐ fausse sur la structure de Kripke ?
7. $\neg(p_1\,\mathbf{U}\,p_2)$
   ☒ LTL ou ☐ CTL ?
   ☐ Pas traduisible ☒ Traduisible : $\neg\,\mathbf{A}(p_1\,\mathbf{U}\,p_2)$
   ☒ Vraie ou ☐ fausse sur la structure de Kripke ?
8. $(\mathbf{G}\,\mathbf{F}\,p_1) \rightarrow (\mathbf{G}\,\mathbf{F}\,p_2)$
   ☒ LTL ou ☐ CTL ?
   ☒ Pas traduisible ☐ Traduisible :
   ☒ Vraie ou ☐ fausse sur la structure de Kripke ?

2 Équité (3 points)

On souhaite modifier la structure de Kripke de la figure 1 de façon à ce que seuls les chemins vérifiant $(\mathbf{G}\,\mathbf{F}\,p_2) \rightarrow (\mathbf{G}\,\mathbf{F}\,p_1)$ soient acceptés.

1. Est-il possible de faire cette modification sans ajouter d'état ni de transition ?
   ☐ Non
   ☐ Oui, sans utiliser de condition d'acceptation
   ☐ Oui, en utilisant des conditions d'acceptation de Büchi
   ☒ Oui, en utilisant des conditions d'acceptation de Streett
2. Dans le cas où cela est possible, effectuez cette modification sur la figure directement. Si vous utilisez des conditions de Büchi ou Streett, vous prendrez soit d'indiquer à côté de la figure l'ensemble des conditions d'acceptation pour l'un et l'ensemble des paires de conditions d'acceptation pour l'autre.

Voici deux solutions parmi d'autres. Il s'agit à chaque fois de conditions d'acceptation de Streett avec ●⇒○.

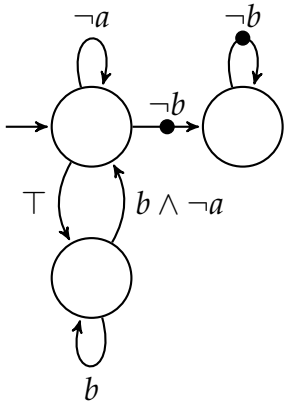


3 Traduction de LTL (5 points)

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

Réponse :

$(a \rightarrow \mathbf{X}\, b)\, \mathbf{U}(\mathbf{G}\, \neg b) = ((\neg a) \vee (\mathbf{X}\, b))\, \mathbf{U}(\neg(\top\, \mathbf{U}\, b))$



L'automate ci-dessus est celui obtenu après construction par tableau. Il est possible de le rendre un peu plus déterministe en remplaçant la transition étiquetée par $\top$ par une transition étiquetée par a, et celle étiquetée par b par une transition étiquetée par ab.

4 Représentation compacte des états (4 points)

1. Quel(s) type(s) de Diagramme de Décision peut (peuvent) être utilisé(s) pour représenter la structure de Kripke de la Figure 1 ?
   ☒ Binary Decision Diagram
   ☒ Multi-valued Decision Diagram
   ☒ Interval Decision Diagram
   ☒ Algebraic Decision Diagram
   ☒ Zero-Suppressed Decision Diagram
   ☒ Data Decision Diagram
2. Combien de variables faut-il pour représenter l'ensemble des états du système ? (une seule réponse possible)
   □ 2
   ☒ 3
   □ 4
   ☒ 5
   □ 6
   □ 7
3. Que représentent ces variables ?

Réponse :

L'ensemble des variables représente l'encodage de l'identifiant de chaque état. Les variables ne correspondent donc pas aux propositions atomiques p_1 et p_2. Il est aussi possible d'avoir une variable par état dont la valeur indique si l'on se trouve dans cet état.
Ainsi, en BDD, il faut 3 variables pour représenter les 5 états du système avec la première solution, et 5 variables pour la seconde. En MDD ou DDD, on peut se contenter d'une seule variable, ou de 5 pour le second cas.

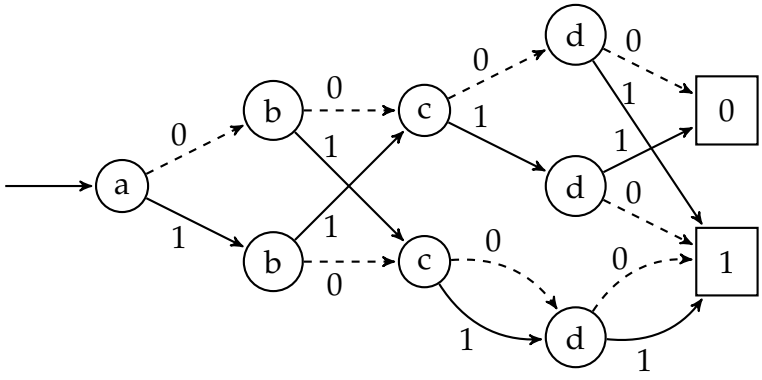


FIG. 2 – Diagramme de décision binaire, utilisé dans l'exercice 5.

5 BDD (3 points)

1. Qu'elle est la formule booléenne représentée par le BDD de la figure 2 ?

Réponse :

$$a\bar{b} \vee \bar{a}b \vee \bar{c}d \vee c\bar{d}$$

2. On peut éviter de représenter certains nœuds (et donc aussi certains arcs) du Diagramme de Décision ci-dessus, en rendant un terminal implicite et en évitant de représenter une variable qu'on peut retrouver à partir du contexte (variable implicite).

   Pour rappel, on définit pour la structure un ensemble de valeurs (*pattern*) telles que, après suppression du terminal implicite, les nœud n'ayant qu'un même successeur pour toutes les valeurs du *pattern* peuvent disparaître.

   Parmi les optimisations présentées ci-dessous, lesquelles permettent d'obtenir un nombre minimal d'arcs pour le BDD de la Figure 2 ?

   □ Suppression du terminal 0 sans variables implicites
   □ Suppression du terminal 1 sans variables implicites
   □ Suppression du terminal 0 et variables implicites pour $\mathbb{B}$
   □ Suppression du terminal 1 et variables implicites pour $\mathbb{B}$
   □ Suppression du terminal 0 et variables implicites pour $\{0\}$
   ☒ Suppression du terminal 1 et variables implicites pour $\{0\}$
   □ Suppression du terminal 0 et variables implicites pour $\{1\}$
   ☒ Suppression du terminal 1 et variables implicites pour $\{1\}$

6 Répartition (3 points)

1. Dans l'algorithme de génération d'un espace d'états que vous avez vu en cours, où introduire l'envoi à une machine distante afin de répartir le calcul ? Reproduisez l'intégralité de l'algorithme.

Réponse :

$SEEN \leftarrow \{initial\_state\}$
$TODO \leftarrow \{initial\_state\}$
while $TODO \neq \emptyset$ do
    pick one s off $TODO$
    for each successor $succ$ of s do
        $n \leftarrow localization(succ)$
        if $n \neq local\_node\_id$ then
            send $succ$ to node n
        else if $succ \notin SEEN$ then
            $SEEN \leftarrow SEEN \cup \{succ\}$
            $TODO \leftarrow TODO \cup \{succ\}$
        end if
    end for
end while

2. Quelles contraintes les états calculés doivent-ils respecter pour une génération répartie ?

Réponse :

Il faut que les états aient la même représentation (endianess, pas de pointeur local) sur tous les nœuds du cluster (ou alors il faut fournir une conversion, pas forcément évidente à écrire). De plus, il faut que le codage d'un état soit connu de tous les nœuds (on ne s'y attendait pas...).