Examen, Cours M2 : Méthode de Vérification

15 Décembre 2016

Documents manuscrits autorisés. Durée : 2h.
Les réponses doivent être justifiées. Elles doivent aussi être lisibles et claires.

Exercice 1

On considère la fonction suivante :

$T : Array[0, n-1 : *]$;

Rev $(A : Array[0, n-1 : *])$ =
  $i : Nat$;
  $t : *$;
  for $i = 0..(n-1)$ do $T[i] := A[i]$;
  $i := 0$;
  while $2i < n$ do
    $t := T[i]$;
    $T[i] := T[n-1-i]$;
    $T[n-1-i] := t$;
    $i := i+1$

Cette fonction prend en entrée un A d'éléments de type $*$, dont la taille n est supposée être *paire*. La fonction ci-dessus inverse le tableau A et produit le résultat de cette inversion dans le tableau T. Formellement, la spécification de cette fonction est donnée par le triplet de Hoare suivant :

$$\{\exists K \geq 0.\, n = 2K\}\ \ \mathsf{Rev}(A)\ \ \{\forall j \in Nat.\, (0 \leq j \leq n-1 \Rightarrow T[j] = A[n-j-1])\}$$

Question : Donner l'invariant de la boucle qui permet de prouver la post-condition. Montrer que c'est bien un invariant de la boucle, et qu'il est possible de montrer la post-condition de la fonction à la fin de la boucle. Finir la preuve en montrant que le triplet ci-dessus est valide.

Exercice 2

Donner pour chacune des formules LTL ci-dessous un automate de Büchi qui reconnait l'ensemble des traces qui la satisfont.

1. $(\Diamond\Box p_1) \wedge (\Diamond\Diamond p_1)$

2. $(\Box\Diamond p_1) \vee (\Box\Diamond p_2)$
3. $(\Diamond\Box p_1) \wedge (\Box\Diamond p_2)$
4. $(\Box\Diamond p_1) \Rightarrow (\Box\Diamond p_2)$

NB : Il n'est pas nécessaire d'utiliser l'algorithme de construction des automates vu en cours et/ou en TD. Mais il faut clairement justifier les réponses.

Exercice 3

Soit $Prop = \{p_1, p_2, r_1, r_2\}$ un ensemble de propositions atomiques. On considère le modèle

$M = (Q = \{q_0, q_1, q_2, q_3, q_4\}, \Delta = \{(q_0, q_1), (q_0, q_2), (q_1, q_3), (q_2, q_4), (q_3, q_1), (q_3, q_4), (q_4, q_0)\}, \Pi)$

où $\Pi(q_1) = \{p_1\}, \Pi(q_2) = \{p_2\}, \Pi(q_3) = \{r_1\}, \Pi(q_4) = \{r_2\}, \Pi(q_0) = \emptyset$.

Question 1 : Utiliser l'approche de model-checking de LTL basée sur les automates pour déterminer si $M, q_0 \models_{LTL} ((\Box\Diamond p_1) \Rightarrow (\Box\Diamond r_1))$ est vrai ou faux.

Question 2 : Utiliser l'algorithme de model-checking explicite de CTL pour calculer l'ensemble des états du modèle M défini ci-dessus qui satisfont les formules :

1. $\forall\Diamond(\exists\Box(\neg p_1 \vee \neg r_1))$
2. $\exists\Diamond(\exists\Box(\neg p_1 \vee \neg r_1))$
3. $\neg r_2 \,\mathcal{U}\, \exists\Box(\neg r_2)$

Exercice 4

Soit $Prop = \{a, b, c\}$ et soit les modèles

— $M_1 = (Q_1 = \{q_0, q_1, q_2, q_3, q_4, q_5\}, \Delta_1 = \{(q_0, q_1), (q_1, q_2), (q_1, q_3), (q_0, q_4), (q_4, q_5)\}, \Pi_1)$ où $\Pi(q_0) = \emptyset$, $\Pi(q_1) = \Pi(q_4) = \{a\}$, $\Pi(q_2) = \{c\}$, and $\Pi(q_3) = \Pi(q_5) = \{b\}$.

— $M_2 = (Q_2 = \{s_0, s_1, s_2, s_3\}, \Delta_1 = \{(s_0, s_1), (s_1, s_2), (s_1, s_3)\}, \Pi_1)$ où $\Pi(s_0) = \emptyset$, $\Pi(s_1) = \{a\}$, $\Pi(s_2) = \{c\}$, and $\Pi(s_3) = \{b\}$.

Question : Donner une formule φ de CTL qui distingue les états q_0 et s_0 de chacun des ces modèles, c'est-à-dire, telle que $M_1, q_0 \models_{CTL} \varphi$ alors que $M_2, s_0 \models_{CTL} \neg\varphi$.