Systèmes de transitions - Modélisation TLA+

Durée 1h45 - Documents autorisés

20 mai 2014

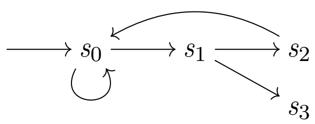
1 Questions de cours ($2,5$ points)

Soit un module TLA+ avec deux variables x et y, et soit défini l'opérateur `diviseurs(a)` qui renvoie l'ensemble des diviseurs d'un nombre. Par exemple $\texttt{diviseurs}(12) = \{1, 2, 3, 4, 6, 12\}$. Répondre aux questions suivantes en respectant la syntaxe TLA+.

1. Donner une propriété temporelle établissant que x ne peut prendre que des valeurs entières strictement positives.
   $\Box(x \in \mathit{Nat} \setminus \{0\})$
2. Donner un prédicat d'état établissant si x et y ont au moins un diviseur commun différent de 1.
   $\mathit{diviseurs}(x) \cap \mathit{diviseurs}(y) \setminus \{1\} \neq \emptyset$
   $\mathit{cardinality}(\mathit{diviseurs}(x) \cap \mathit{diviseurs}(y)) > 1$
   $\exists i \in \mathit{Nat} : i \neq 1 \land i \in \mathit{diviseurs}(x) \land i \in \mathit{diviseurs}(y)$
3. Donner une action qui change x en 3, à condition que x soit un diviseur de y.
   $x \in \mathit{diviseur}(y) \land x' = 3(\land \text{UNCHANGED } y)$
4. Donner une action non déterministe qui change x en un diviseur pair de y.
   $x' \in \{a \in \mathit{diviseurs}(y) : a\%2 = 0\}(\land \text{UNCHANGED } y)$
   $x' \in \mathit{diviseurs}(y) \land x'\%2 = 0(\land \text{UNCHANGED } y)$
5. Donner une propriété temporelle établissant que si x est nul, alors y prendra la valeur 6.
   $(x = 0) \leadsto (y = 6)$
   $\Box((x = 0) \Rightarrow \Diamond(y = 6))$
   $(x = 0) \Rightarrow \Diamond(y = 6)$ *(c'est ambigu si ça doit être toujours vrai ou seulement dans l'état initial)*
   $\Diamond((x = 0) \Rightarrow \Diamond(y = 6))$ *(voire un jour...)*
   $(x = 0) \Rightarrow (y' = 6)$ *n'a guère de sens s'il y a du bégaiement possible*

2 Exercice ($4,5$ points)

Soit le système de transition suivant :



Les propriétés suivantes, exprimées en logique LTL ou CTL, sont-elles vérifiées (donner une justification informelle), selon les équités sur les transitions spécifiées ?

	aucune	$WF(s_0 \to s_1)$	$WF(s_0 \to s_1)$ $SF(s_1 \to s_3)$	explication
$\Diamond s_1$				
$\Box\Diamond(s_2 \vee s_3)$				
$\Diamond s_3$				
$\exists\Box s_0$				
$\exists\Diamond s_3$				
$\forall\Box\exists\Diamond s_3$				

	aucune	$WF(s_0 \to s_1)$	$WF(s_0 \to s_1)$ $SF(s_1 \to s_3)$	*explication*
$\Diamond s_1$	*n*	*o*	*o*	*équité élimine* ${s_0}^\omega$
$\Box\Diamond(s_2 \vee s_3)$	*n*	*o*	*o*	*idem*
$\Diamond s_3$	*n*	*n*	*o*	*équité élimine* $(s_0 \to s_1 \to s_2)^\omega$
$\exists\Box s_0$	*o*	*n*	*n*	*équité*
$\exists\Diamond s_3$	*o*	*o*	*o*	s_3 *accessible depuis état initial*
$\forall\Box\exists\Diamond s_3$	*o*	*o*	*o*	s_3 *toujours accessible*

3 Problème : Épidémie (13 points)

On souhaite modéliser en TLA un problème de propagation d'épidémie. On suppose un nombre d'individus fixe, qui peuvent être sains, contagieux ou morts. Une personne contagieuse contamine à chaque tour au plus une personne (vivante) de son entourage, cet entourage étant supposé fixe. Une personne contagieuse peut également mourir ou redevenir saine à tout instant. Toute personne morte reste contagieuse. La propagation est garantie en interdisant à toute personne contagieuse de guérir tant que tous ses voisins sont sains. Enfin, on suppose qu'à l'instant initial, un individu unique quelconque est contaminé, les autres étant sains. Un squelette de module TLA `Epidemie.tla` modélisant ce phénomène est donné en 3.5.

3.1 Transitions

Définir les prédicats de transitions suivants, en respectant attentivement les règles énoncées ci-dessus :

1. `contaminer(i,j)` : contamination par l'individu contagieux i d'un voisin j vivant.
   $$\begin{aligned} &contaminer(i,j) \triangleq \\ &\quad \land \langle i,j \rangle \in Voisinage \\ &\quad \land etat[i] = Contagieux \lor etat[i] = Mort \\ &\quad \land etat[j] = Sain \\ &\quad \land etat' = [etat\ EXCEPT\ ![j] = Contagieux] \end{aligned}$$
2. `mourir(i)` : mort de l'individu contagieux i.
   $$\begin{aligned} &mourir(i) \triangleq \\ &\quad \land etat[i] = Contagieux \\ &\quad \land etat' = [etat\ EXCEPT\ ![i] = Mort] \end{aligned}$$
3. `guerir(i)` : guérison de l'individu contagieux i.
   $$\begin{aligned} &mourir(i) \triangleq \\ &\quad \land etat[i] = Contagieux \\ &\quad \land \exists j \in Individus : \langle i,j \rangle \in voisinage \land etat[j] \neq Sain \\ &\quad \land etat' = [etat\ EXCEPT\ ![i] = Sain] \end{aligned}$$
4. `Next` : toutes les transitions possibles du problème modélisé.
   $$\begin{aligned} &Next \triangleq \\ &\quad \exists\ i \in Individus : \\ &\quad\quad \lor \exists\ j \in Individus : Contaminer(i,j) \\ &\quad\quad \lor Mourir(i) \\ &\quad\quad \lor Guerir(i) \end{aligned}$$

3.2 Équité

Définir les contraintes d'équité minimales suivantes sur les transitions qui illustrent au mieux les phénomènes de contagion suivants :

5. Un individu sain continûment en présence d'un individu contagieux ne peut échapper à la contagion.
   $\forall i,j \in Individus : WF_{vars}(Contaminer(i,j))$
6. Tout individu finit par mourir ou par rester définitivement sain.
   $\forall i \in Individus : SF_{vars}(Mourir(i))$

3.3 Spécification

Définir les propriétés suivantes (qui ne sont pas nécessairement vérifiées par le modèle) :

7. `MortStable` : la mort est un état stable.
   $\forall i \in Individus : \Box(etat[i] = Mort \Rightarrow \Box(etat[i] = Mort))$

8. `MortContagieuse` : tout individu mort finit par faire mourir un de ses voisins.
   $\forall i \in Individus : etat[i] = Mort \leadsto \exists j \in Individus : \langle i, j \rangle \in Voisinage \land etat[j] = Mort$
   Mais $\forall i \in Individus : \exists j \in Individus : \langle i, j \rangle \in Voisinage \land etat[i] = Mort \leadsto etat[j] = Mort$ *est faux : ça serait toujours le même voisin qui meurt.*
   Noter qu'on ne peut pas exprimer que i est la cause de la mort de j.
9. `Propagation` : tout individu contagieux finit par en contaminer un autre, à moins qu'il ne meure.
   Formulation ambiguë (un voisin, ou un site quelconque ?) :
   $\forall i \in Individus : etat[i] = Contagieux \leadsto etat[i] = Mort \lor \exists j \in Individus \setminus \{i\} : etat[j] \neq Sain$
   $\forall i \in Individus : etat[i] = Contagieux \leadsto etat[i] = Mort \lor \exists j \in Individus : \langle i, j \rangle \in Voisinage \land etat[j] \neq Sain$
10. `ImpossibleTousSains` : il est impossible que tout le monde soit sain en même temps.
   $\Box(\exists i \in Individus : etat[i] \neq Sain)$
   $\Box(Cardinality(\{i \in Individus : etat[i] \neq Sain\}) \geq 1)$
11. `FinalementTousMorts` : tous les individus finiront par mourir.
   Formulation ambiguë :
   Chaque individu : $\forall i \in Individus : \Diamond(etat[i] = Mort)$
   L'ensemble des individus : $\Diamond(\forall i \in Individus : etat[i] = Mort)$
   (2 $\Rightarrow$ 1 mais pas l'inverse)
12. `BrebisGaleuse` : il existe un individu infiniment souvent contagieux ou mort.
   $\exists i \in Individus : \Box\Diamond(etat[i] \neq Sain)$

3.4 Analyse du problème

Répondre informellement aux questions suivantes, éventuellement en illustrant la réponse par des (contre-)exemples. On suppose que le graphe de voisinage est connexe et qu'il y a au moins deux individus :

13. Expliquer pourquoi la propriété `MortContagieuse` est vraie.
   (a) *MortStable $\Rightarrow$ i reste mort*
   (b) *Soit un voisin j sain. j finit par être contaminé (WF sur contaminer)*
   (c) *j peut guérir, mais cas précédent $\Rightarrow$ j est infiniment souvent contaminé*
   (d) *SF sur mourir $\Rightarrow$ j meurt*
14. Expliquer pourquoi la propriété `Propagation` est vraie.
   Un individu contagieux peut soit mourir ($\Rightarrow$ OK), soit redevenir sain. Et s'il redevient sain, c'est qu'un de ses voisins est contaminé (contagieux ou mort) $\Rightarrow$ OK.
15. La propriété `BrebisGaleuse` est-elle alors vérifiée ?
   Oui, car le nombre d'individu est fini.
16. La propriété `FinalementTousMorts` est-elle alors vérifiée ?
   Oui : SF sur mourir (c'est un peu court...)

3.5 Module fourni : `Epidemie.tla`

MODULE *Epidemie*

EXTENDS *Naturals*, *FiniteSets*

CONSTANTS

N, nombre d'individus

Voisinage relation de voisinage entre individus

$Individus \triangleq 0 \,..\, N-1$

Il y a au moins 2 individus

ASSUME $N > 1$

Le *Voisinage* est une relation entre individus

ASSUME $Voisinage \in \text{SUBSET}\ (Individus \times Individus)$

Aucun individu n'est voisin de lui-même

ASSUME $\forall\, i \in Individus : \langle i, i \rangle \notin Voisinage$

Le graphe de *Voisinage* est connexe

$Stable(S) \triangleq \forall\, paire \in Voisinage : paire[1] \in S \Rightarrow paire[2] \in S$

ASSUME $\forall\, S \in \text{SUBSET}\ Individus \setminus \{\} : Stable(S) \Rightarrow Cardinality(S) = N$

VARIABLES

etat état d'un individu

$Sain \triangleq$ "sain"

$Contagieux \triangleq$ "contagieux"

$Mort \triangleq$ "mort"

$Etat \triangleq \{Sain, Contagieux, Mort\}$

$TypeInvariant \triangleq$

$\quad \Box(etat \in [Individus \rightarrow Etat])$

$Init \triangleq$

$\quad$ LET $malade \triangleq$ CHOOSE $i \in Individus$: TRUE IN le *malade* initial

$\quad \land\, etat = [i \in Individus \mapsto$ IF $i = malade$ THEN $Contagieux$ ELSE $Sain]$

$Contaminer(i, j) \triangleq$ L'individu i tente de contaminer l'individu j, s'ils sont voisins

$\quad \land\, \langle i, j \rangle \in Voisinage$

À *COMPLÉTER*

$Mourir(i) \triangleq$ L'individu i meurt

À *COMPLÉTER*

$Guerir(i) \triangleq$ L'individu i repasse à l'état *Sain*

À *COMPLÉTER*

$Next \triangleq$

À *COMPLÉTER*

$Spec \triangleq$

$\quad \land\, Init$

$\quad \land\, \Box[Next]_{etat}$

À *COMPLÉTER*