

Advanced Model Checking Summer term 2014

– Solution 3 –

Exercise 1

(2 + 1 points)

Observational equivalence $\approx_{obs}$ is a slight variant of stutter-bisimulation equivalence where state s_2 is allowed to perform a path fragment

$$\underbrace{s_2 u_1 \dots u_m}_{\text{stuttersteps}} \underbrace{v_1 \dots v_k s'_2}_{\text{stuttersteps}}$$

with arbitrary stutter steps at the beginning and at the end and $s'_1 \approx_{obs} s'_2$ to simulate a transition $s_1 \rightarrow s'_1$ of an observational equivalent state s_1 . I.e., it is not required that s_2 and states u_i are observationally equivalent, or that s'_2 and v_i are observationally equivalent. For the special case where $s_1 \rightarrow s'_1$ is a stutter step the path fragment of length 0 (consisting of state $s_2 = s'_2$) can be used to simulate $s_1 \rightarrow s'_1$.

The formal definition of observational equivalence is as follows. Let TS_1 and TS_2 be two transition systems with state-spaces S_1 and S_2 , respectively, and the same set AP of atomic propositions. A binary relation $\mathcal{R} \subseteq S_1 \times S_2$ is called an observational bisimulation for (TS_1, TS_2) iff that the following conditions (A) and (B) are satisfied:

(A) Every initial state of TS_1 is related to an initial state of TS_2 , and vice versa. That is,

$$\forall s_1 \in I_1 \exists s_2 \in I_2. (s_1, s_2) \in \mathcal{R} \quad \text{and} \quad \forall s_2 \in I_2 \exists s_1 \in I_1. (s_1, s_2) \in \mathcal{R}$$

(B) For all $(s_1, s_2) \in \mathcal{R}$, the following conditions (I),(II) and (III) hold:

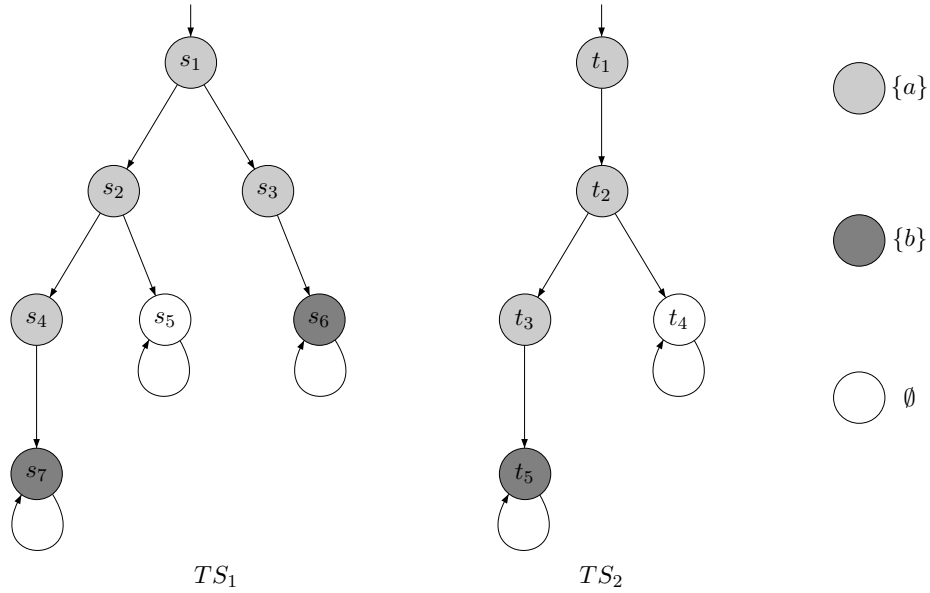
- (I) If $(s_1, s_2) \in \mathcal{R}$ then $L_1(s_1) = L_2(s_2)$.
- (II) If $(s_1, s_2) \in \mathcal{R}$ and $s'_1 \in \text{Post}(s_1)$, then there exists a path fragment $u_0 u_1 \dots u_n$ such that $n \geq 0$ and $u_0 = s_2$, $(s'_1, u_n) \in \mathcal{R}$ and, for some $m \leq n$, $L_2(u_0) = L_2(u_1) = \dots = L_2(u_m)$ and $L_2(u_{m+1}) = L_2(u_{m+2}) = \dots = L_2(u_n)$.
- (III) If $(s_1, s_2) \in \mathcal{R}$ and $s'_2 \in \text{Post}(s_2)$, then there exists a path fragment $u_0 u_1 \dots u_n$ such that $n \geq 0$ and $u_0 = s_1$, $(u_n, s'_2) \in \mathcal{R}$ and, for some $m \leq n$, $L_1(u_0) = L_1(u_1) = \dots = L_1(u_m)$ and $L_1(u_{m+1}) = L_1(u_{m+2}) = \dots = L_1(u_n)$.

TS_1 and TS_2 are called observational equivalent, denoted $TS_1 \approx_{obs} TS_2$, if there exists an observational bisimulation for (TS_1, TS_2) .

Questions:

The goal of this exercise is to show that $\approx_{obs}$ is strictly coarser than stutter-bisimulation equivalence $\approx$.

- (a) Show that $TS_1 \approx TS_2$ implies $TS_1 \approx_{obs} TS_2$.
- (b) Consider the two transition systems TS_1 and TS_2 shown in the following figure. Show that $TS_1 \approx TS_2$ and $TS_1 \not\approx_{obs} TS_2$.



Solution:

- (a) Let us first consider the definition of stutter bisimulation on states and then stutter bisimulation for transition systems:

Definition 1: Transition systems TS_i , $i = 1, 2$ are stutter bisimilar, if there exists a stutter bisimulation $\mathcal{R} \subseteq \mathcal{S}_1 \times \mathcal{S}_2$:

$$\forall s_1 \in I_1 \exists s_2 \in I_2. (s_1, s_2) \in \mathcal{R} \quad \text{and} \quad \forall s_2 \in I_2 \exists s_1 \in I_1. (s_1, s_2) \in \mathcal{R}$$

NOTE 1: The condition regarding the initial states in the definition above is equivalent to the condition (A) from the definition of the observational equivalent transition systems.

Definition 2: For a transition system TS the binary relation $\mathcal{R}$ on $\mathcal{S}$ is a stutter bisimulation if for all $(s_1, s_2) \in \mathcal{R}$:

- (I) $L(s_1) = L(s_2)$
- (II) $s'_1 \in \text{Post}(s_1) \wedge (s_1, s'_1) \notin \mathcal{R}$ then there exists a finite path fragment $s_2 u_1 \dots u_n s'_2$ with $n \geq 0$, such that: $\forall i = 1, \dots, n : (s_1, u_i) \in \mathcal{R} \wedge (s'_1, s'_2) \in \mathcal{R}$
- (III) Symmetrically for $s'_2 \in \text{Post}(s_2)$.

Not let us slightly rephrase the condition (B) from the definition of the observation equivalent transition systems:

- (B) For all $(s_1, s_2) \in \mathcal{R}$, the following conditions (I),(II) and (III) hold:

- (I) $L_1(s_1) = L_2(s_2)$.
- (II) $s'_1 \in \text{Post}(s_1)$, then there exists a path fragment s_2 or $s_2 u_1 \dots u_n s'_2$ such that $n \geq 0$, $(s'_1, s'_2) \in \mathcal{R}$ and, for some $m \leq n$, $L_2(s_2) = L_2(u_1) = \dots = L_2(u_m)$ and $L_2(u_{m+1}) = L_2(u_{m+2}) = \dots = L_2(u_n) = L_2(s'_2)$.
- (III) Symmetrically for $s'_2 \in \text{Post}(s_2)$.

Let us have some observations about the point (II) from above.

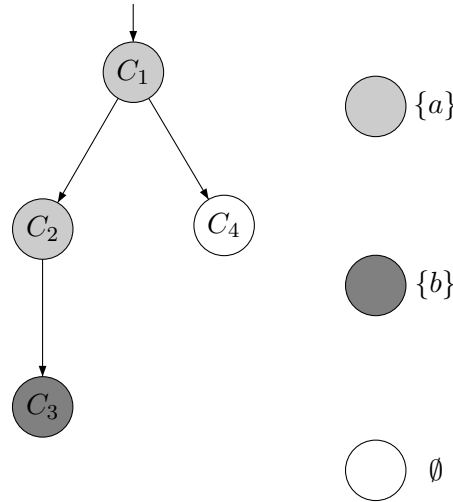
Observation 1: Unlike point (II) in Definition 2 it is not required that $(s_1, s'_1) \notin \mathcal{R}$

Observation 2: Unlike point (II) in Definition 2 it is not required that the path fragment consists of more than one state (in case it is s_2 the situation is trivial ($s_2 = s'_2$) and corresponds to having $(s_1, s'_1) \in \mathcal{R}$).

Observation 3: There is a condition on the path elements labeling: for some $m \leq n$, $L_2(s_2) = L_2(u_1) = \dots = L_2(u_m)$ and $L_2(u_{m+1}) = L_2(u_{m+2}) = \dots = L_2(u_n) = L_2(s'_2)$ instead of having $\forall i = 1, \dots, n : (s_2, u_i) \in \mathcal{R} \wedge (s'_1, s'_2) \in \mathcal{R}$.

At this point to finalize the proof of the fact that $TS_1 \approx TS_2$ implies $TS_1 \approx_{obs} TS_2$ it suffices to show that the point (II) of Definition 2 implies the point (II) of the observation-equivalence definition, which is trivial, since having a stutter bisimulation $\mathcal{R}$:

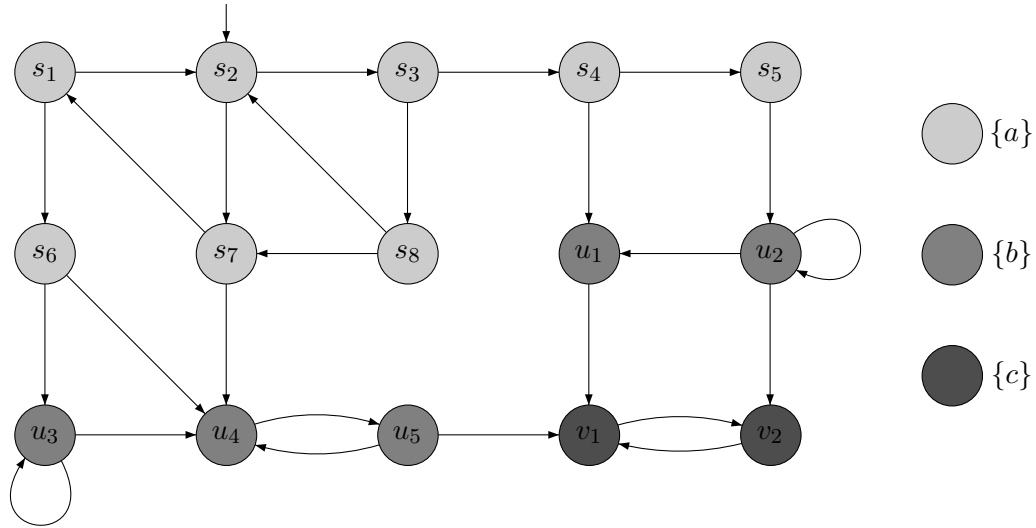
- if $(s_1, s'_1) \in \mathcal{R}$ then the path fragment which should be considered is s_2 ($s_2 = s'_2$) and as $\mathcal{R}$ is an equivalence $(s_2, s_2) \in \mathcal{R}$.
 - if $(s_1, s'_1) \notin \mathcal{R}$ then there exists a finite path fragment $s_2 u_1 \dots u_n s'_2$ with $n \geq 0$, such that: $\forall i = 1, \dots, n : (s_2, u_i) \in \mathcal{R} \wedge (s'_1, s'_2) \in \mathcal{R}$. The latter implies that $L_2(s_2) = L_2(u_1) = \dots = L_2(u_n)$, which means that we just need to take $m = n$ in the definition of observation-equivalence.
- (b) Notice that $TS_1 \approx TS_2$ and thus $TS_1 \approx_{obs} TS_2$. The stutter-bisimulation equivalence relation here is defined by the following equivalence classes: $C_1 = \{s_1, s_2, t_1, t_2\}$, $C_2 = \{s_3, s_4, t_3\}$, $C_3 = \{s_6, s_7, t_5\}$, $C_4 = \{s_5, t_4\}$. The corresponding transition system can be seen on the figure below:



Exercise 2

(1 + 2 points)

Given transition systems TS :

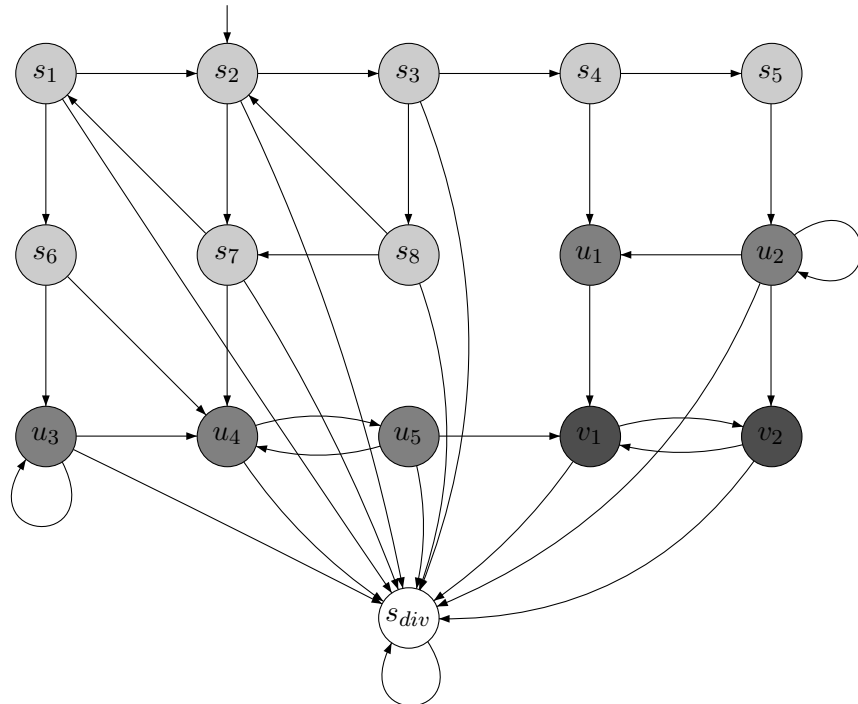


Questions:

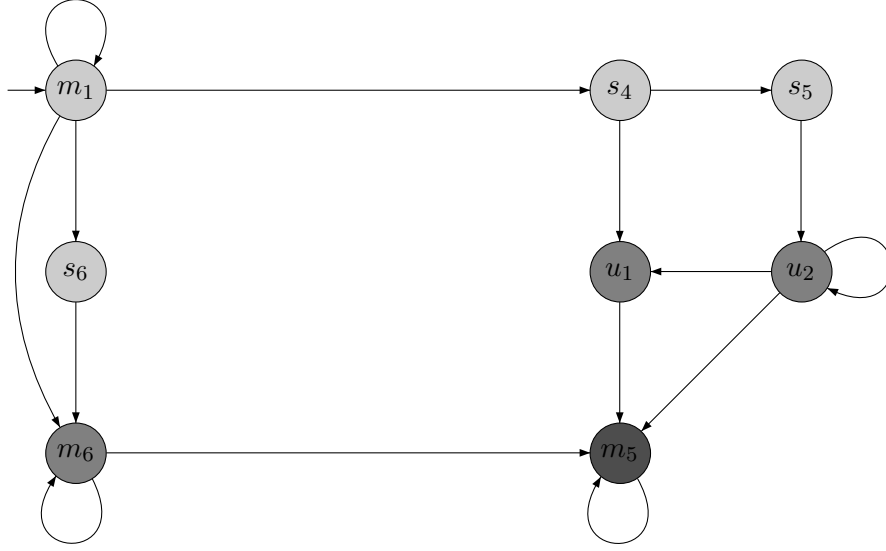
- Depict the divergence-sensitive expansion $\overline{TS}$.
- Determine the divergence-stutter-bisimulation quotient $(\overline{TS})/\approx$, and depict $TS/\approx^{div}$.

Solution:

- The divergence-sensitive expansion $\overline{TS}$:



- $TS/\approx^{div}$:



Exercise 3

(4 points)

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a finite transition system. A stutter simulation for TS is a relation $\mathcal{R}$ on S such that for all $(s_1, s_2) \in \mathcal{R}$:

1. $L(s_1) = L(s_2)$.
2. If $s'_1 \in Post(s_1)$ with $(s_1, s'_1) \notin \mathcal{R}$, then there exists a finite path fragment $s_2 u_1 \dots u_n s'_2$ with $n \geq 0$ and $(s_1, u_i) \in \mathcal{R}$, $i = 1, \dots, n$ and $(s'_1, s'_2) \in \mathcal{R}$.

s_1 is said to be stutter simulated by s_2 , denoted $s_1 \preceq_{st} s_2$, iff there exists a stutter simulation for (s_1, s_2) .

A stutter simulation $\mathcal{R}$ for TS is called divergence-sensitive if for all pairs $(s_1, s_2) \in \mathcal{R}$ and each infinite path fragment $\pi_1 = s_{0,1} s_{1,1} s_{2,1} \dots$ in TS with $s_{0,1} = s_1$ and $(s_{i,1}, s_2) \in \mathcal{R}$ for all $i \geq 0$ there exists a transition $s'_2 \in Post(s_2)$ with $(s_{j,1}, s'_2) \in \mathcal{R}$ for some $j \geq 1$. We write $s_1 \preceq_{st}^{div} s_2$ iff there exists a divergence-sensitive stutter simulation $\mathcal{R}$ for (s_1, s_2) .

Question:

Assume that for all $\forall CTL_{\bigcirc}^*$ formulae Φ and two states s_1 and s_2 in TS we have $s_2 \models \Phi \Rightarrow s_1 \models \Phi$. Show that $s_1 \preceq_{st}^{div} s_2$.

Hint:

Define $\mathcal{R} = \{(s_1, s_2) \in S \times S \mid \forall \Phi \in \forall CTL_{\bigcirc}^*. s_2 \models \Phi \Rightarrow s_1 \models \Phi\}$ and show that $\mathcal{R}$ is a divergence-sensitive stutter simulation relation. This is proven by checking the conditions of the divergence-sensitive stutter simulation.

Solution:

First we define the relation $\mathcal{R} = \{(s_1, s_2) \in S \times S \mid \forall \Phi \in \forall CTL_{\bigcirc}^*. s_2 \models \Phi \Rightarrow s_1 \models \Phi\}$. The task is to show that $\mathcal{R}$ is a divergence-sensitive stutter simulation.

We show that (1) $\mathcal{R}$ is a stutter simulation and (2) $\mathcal{R}$ is divergence-sensitive.

Claim 1. $\mathcal{R}$ is a stutter simulation.

Proof of claim 1. Let $(s_1, s_2) \in \mathcal{R}$. We consider the propositional logical formula

$$\Phi = \bigwedge_{a \in L(s_2)} a \wedge \bigwedge_{a \in AP \setminus L(s_2)} \neg a.$$

Since $s_2 \models \Phi$ and $(s_1, s_2) \in \mathcal{R}$, we obtain $s_1 \models \Phi$. From the structure of the formula Φ we get $L(s_1) = L(s_2)$. This proves the first condition of the stutter simulation relation $\mathcal{R}$.

To establish the second condition of relation $\mathcal{R}$, we define a formula Φ_u for the upward closure of a state u with respect to $\mathcal{R}$, i.e.,

$$Sat(\Phi_u) = u \uparrow = \{t \in S \mid (u, t) \in \mathcal{R}\}.$$

Φ_u is also called the master formula for the state u . We have to show that for all $\forall\text{CTL}_{\bigcirc}^*$ -formulas Φ , if $s_2 \models \Phi \implies s_1 \models \Phi$ then $(s_1, s_2) \in \mathcal{R}$. This also means that $s_1 \models \neg\Phi \implies s_2 \models \neg\Phi$.

Lets consider a state s'_1 such that $s'_1 \in Post(s_1)$, $(s_1, s'_1) \notin \mathcal{R}$ and $s_1 \models \exists(\Phi_{s_1} \mathbf{U} \Phi_{s'_1})$. Then we have that $s_1 \models \neg\forall\neg(\Phi_{s_1} \mathbf{U} \Phi_{s'_1})$. Notice that we can a $\forall\text{CTL}_{\bigcirc}^*$ -formula out of $\forall\neg(\Phi_{s_1} \mathbf{U} \Phi_{s'_1})$ by pushing the negation inside the formula. As $(s_1, s_2) \in \mathcal{R}$ we have that $s_2 \models \neg\forall\neg(\Phi_{s_1} \mathbf{U} \Phi_{s'_1})$ or $s_2 \models \exists(\Phi_{s_1} \mathbf{U} \Phi_{s'_1})$. This means that there exists a path fragment $\pi_2 = s_2 u_1 \dots u_n s'_2$ with $n \geq 0$ such that $s_2 \models \Phi_{s_1}$, $u_i \models \Phi_{s_1}$ for all $i \leq n$ and $s'_2 \models \Phi_{s'_1}$. From the definition of the upward closure of a state we get that $(s_1, u_i) \in \mathcal{R}$ for all $i \leq n$ and $(s'_1, s'_2) \in \mathcal{R}$.

Claim 2. $\mathcal{R}$ is divergence-sensitive stutter simulation.

Proof of claim 2. As before let $(s_1, s_2) \in \mathcal{R}$. We define a formula Φ_u for the downward closure of a state u with respect to $\mathcal{R}$, i.e.,

$$Sat(\Phi_u) = u \downarrow = \{t \in S \mid (t, u) \in \mathcal{R}\}.$$

Consider a path $\pi_1 = s_{0,1} s_{1,1} s_{2,1} \dots$ such that $s_1 = s_{0,1}$ and $\pi_1 \models \Box\Phi_{s_2}$ or $s_1 \models \exists\Box\Phi_{s_2}$. This means $s_1 \models \neg\forall\neg\Box\Phi_{s_2}$ and $s_2 \models \neg\forall\neg\Box\Phi_{s_2}$ or $s_2 \models \exists\Box\Phi_{s_2}$. From the definition of downward closure we get that $(s_{j,1}, s_2) \in \mathcal{R}$ for all $j \geq 0$. As $\mathcal{R}$ is also a stutter-simulation there is a $j \geq 1$ such that $(s_{j,1}, Post(s_2)) \in \mathcal{R}$.