Prof. Dr. Ir. J.-P. Katoen
A. Mereacre & H. Yue

Advanced Model Checking
Summer term 2009

– Series 3 –

Hand in on May 11'th before the exercise class.

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

$$\underbrace{s_2 u_1 ... u_m}_{stutter steps} \underbrace{v_1 ... v_k s_2'}_{stutter steps}$$

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,

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

(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 $s_1' \in Post(s_1)$, then there exists a path fragment $u_0 u_1 ... u_n$ such that $n \geq 0$ and $u_0 = s_2$, $(s_1', u_n) \in \mathcal{R}$ and, for some $m \leq n$, $L_2(u_0) = L_2(u_1) = ... = L_2(u_m)$ and $L_2(u_{m+1}) = L_2(u_{m+2}) = ... = L_2(u_n)$.

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

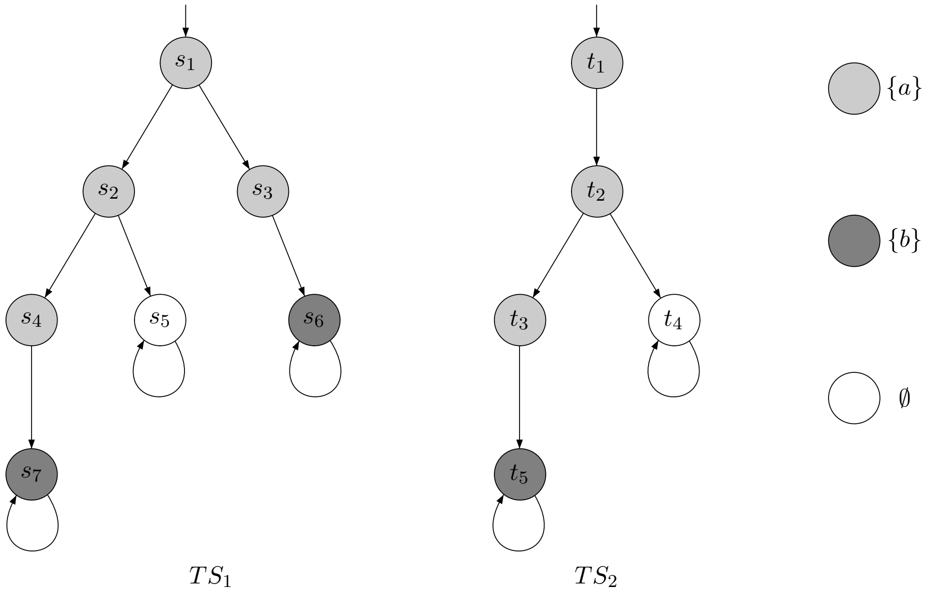
TS_1 and TS_2 are called observational equivalent, denoted $TS_1 \approx_{obs} TS_2$, if there exists an observational bisimulation for (TS_1, TS_2).

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 $TS_1 \approx_{obs} TS_2$.

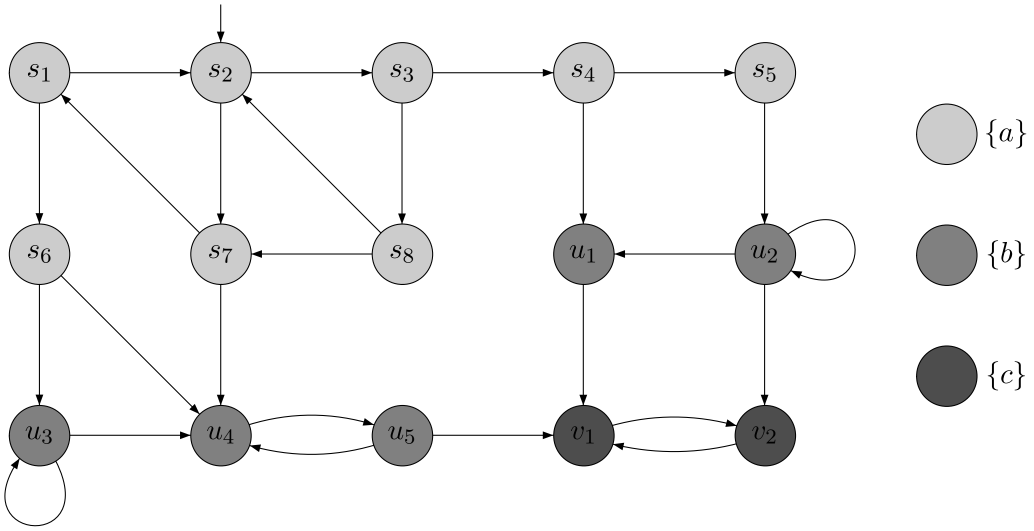
(b) Consider the two transition systems TS_1 and TS_2 shown in the following figure. Show that $TS_1 \not\approx TS_2$ and $TS_1 \approx_{obs} TS_2$.



TS_1 TS_2

Exercise 2 $(1 + 1 + 1$ points)

Given transition systems TS:



Questions:

(a) Depict the divergence-sensitive expansion $\overline{TS}$.

(b) Determine the divergence-stutter-bisimulation quotient $(\overline{TS})/\approx$. Apply the algorithm and give for each iteration the partition of the state space.

(c) Depict $TS/{\approx^{div}}$.

Exercise 3 (4 points)

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a 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 $s_1' \in \mathit{Post}(s_1)$ with $(s_1, s_1') \notin \mathcal{R}$, then there exists a finite path fragment $s_2\, u_1 \ldots u_n\, s_2'$ with $n \geq 0$ and $(s_1, u_i) \in \mathcal{R}$, $i = 1, \ldots, n$ 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 $\pi_1 = s_{0,1}\ s_{1,1}\ s_{2,1} \ldots$ 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 $s_2' \in \mathit{Post}(s_2)$ 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 $\forall\text{CTL}^*_{\setminus \bigcirc}$ 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 $\mathcal{R} = \{(s_1, s_2) \in S \times S \mid \forall \Phi \in \forall\text{CTL}^*_{\setminus \bigcirc}. s_2 \models \Phi \Rightarrow s_1 \models \Phi\}$ 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.