

Exercises to the lecture “Advanced Model Checking”, winter term 2006

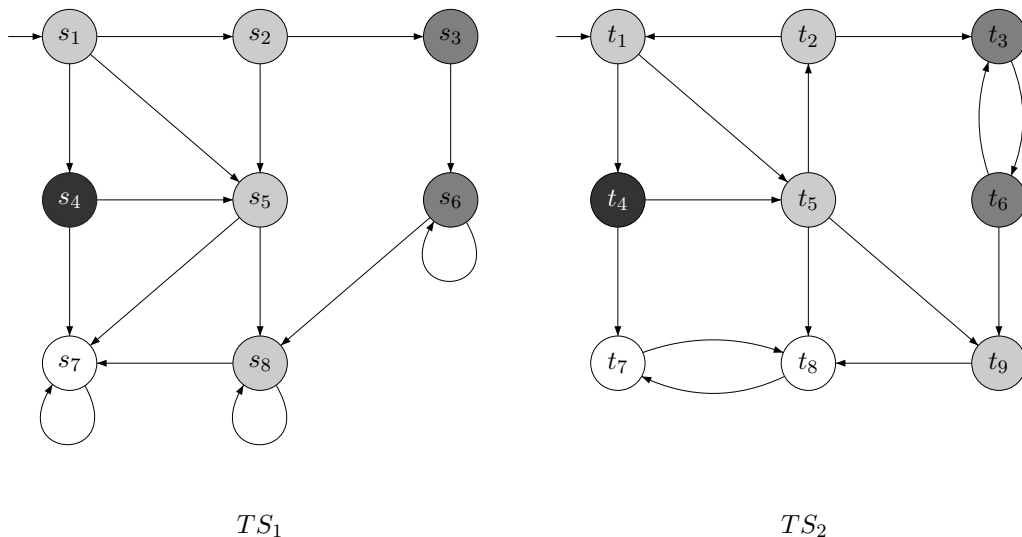
– Assignment 5 –

The solutions are collected on Nov. 24th at the beginning of the exercise class.
Justify your answers!

Exercise 1

(4 points)

Given transition systems TS_1 and TS_2 as follows:



Does it hold that:

(a) $TS_1 \approx TS_2$?

(b) $TS_1 \approx^{div} TS_2$? If not, provide a $CTL \setminus \bigcirc$ formula to distinguish them.

Exercise 2

(4 points)

Let φ be an LTL formula such that $Word(\varphi)$ is stutter insensitive.
Show that φ is equivalent to some $LTL \setminus \bigcirc$ formula ψ .

Exercise 3

(8 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) .

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 $TS_1 \approx_{obs} TS_2$.

