

Advanced Model Checking Summer term 2014

– Solution 1 –

Exercise 1

(2 + 1 points)

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system. The relations $\sim_n \subseteq S \times S$ are inductively defined by:

- $s_1 \sim_0 s_2$ iff $L(s_1) = L(s_2)$.
- $s_1 \sim_{n+1} s_2$ iff:
 - $L(s_1) = L(s_2)$,
 - for all $s'_1 \in Post(s_1)$ there exists $s'_2 \in Post(s_2)$ with $s'_1 \sim_n s'_2$,
 - for all $s'_2 \in Post(s_2)$ there exists $s'_1 \in Post(s_1)$ with $s'_1 \sim_n s'_2$.

Questions:

- (i) Show that for *finite* TS it holds that $\sim_{TS} = \bigcap_{n \geq 0} \sim_n$, i.e.,

$$s_1 \sim_{TS} s_2 \text{ iff } s_1 \sim_n s_2 \text{ for all } n \geq 0$$

- (ii) Does this also hold for infinite transition systems (provide a proof or a counterexample)?

Solution:

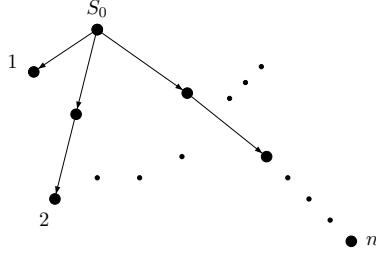
- (i) We have to show that $\sim_{TS} = \bigcap_{n \geq 0} \sim_n$. Let R_n be the relation $\sim_n$ ($n \geq 0$) and R be $\sim_{TS}$. We claim that

$$S \times S \supseteq R_0 \supseteq R_1 \supseteq R_2 \supseteq \dots \supseteq R_i \supseteq R_{i+1} \supseteq \dots$$

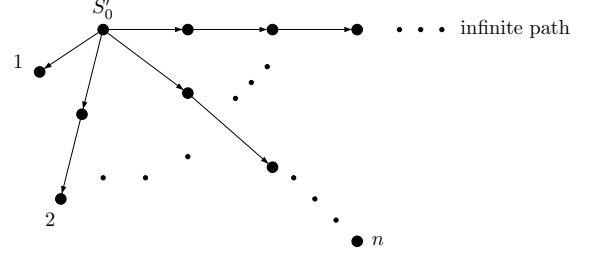
The case $S \times S \supseteq R_0$ is trivial due to the fact that for any two states s_1 and s_2 for which $L(s_1) \neq L(s_2)$ we have $(s_1, s_2) \in S \times S$ and $(s_1, s_2) \notin R_0$. Now, we have to show that $R_i \supseteq R_{i+1}$ for any $i \geq 0$. We consider any two states s_1 and s_2 with two outgoing transitions $s_1 \rightarrow s'_1$ and $s_2 \rightarrow s'_2$, respectively such that $(s_1, s_2) \in R_i$ and $(s'_1, s'_2) \notin R_i$ (note that it doesn't contradict the definition of R_n). By using the definition of R_{i+1} we get that $(s_1, s_2) \notin R_{i+1}$, proving the fact that $R_i \supseteq R_{i+1}$. As the state space S is finite, it is easy to see that there exists a $k \leq |S|$ such that $R_k = R_{k+1} = R_{k+2} = \dots$. Using the relation $R_i \supseteq R_{i+1}$ we can conclude that $\bigcap_{n \geq 0} R_n = R_k$. As $R_k = R_{k+1}$, by the definition of R_{k+1} we get that $R_{k+1} = R$ or $\sim_{TS} = \bigcap_{n \geq 0} \sim_n$.

- (ii) Consider the following two transition systems TS and TS' :

Obviously, S_0 and S'_0 are not bisimilar because of the infinite path in TS' . However, for each $n \geq 0$, there is a path of length n in TS which preserves the bisimilarity of S_0 and S'_0 .



(a) TS : for each n , there is a path of length n in TS .

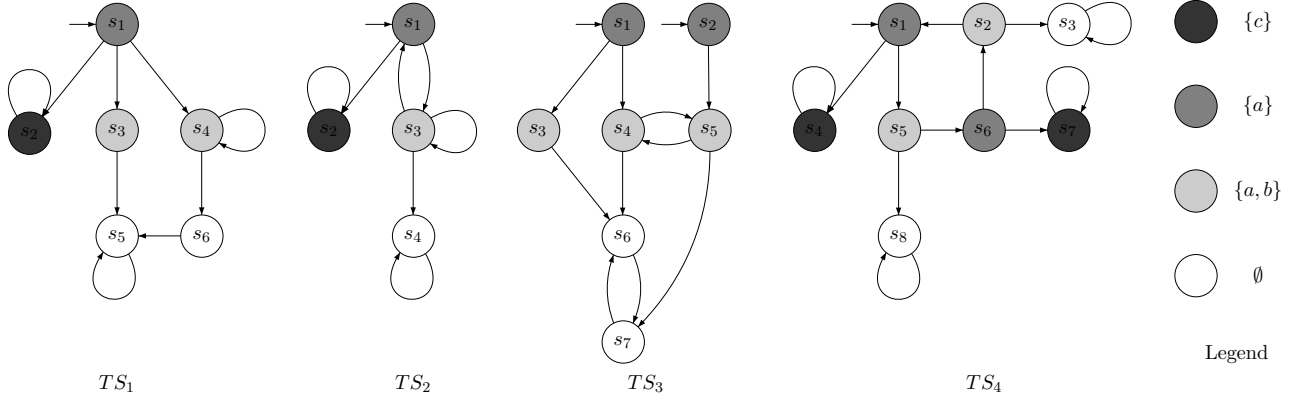


(b) TS' : extension of TS by an infinite path.

Exercise 2

(3 points)

Which of the following transition systems are bisimulation equivalent? Justify your answers by either providing a bisimulation relation or a $CTL_{\setminus U}$ formula that distinguishes the considered transition systems. (Note: a $CTL_{\setminus U}$ formula contains neither an U -operator nor one of its derived operators such as $\Diamond$ and $\Box$)



Solution:

For simplicity, we use $s_{i,j}$ to denote s_i in TS_j , for $j = 1, \dots, 4$.

- $TS_3 \not\sim TS_1, TS_2, TS_4$.

Intuitively, this is because TS_3 does not have a state labeled with $\{c\}$ while TS_1, TS_2 and TS_4 do.

A CTL formula that distinguishes TS_3 from TS_1, TS_2 and TS_4 is the following:

$$\Phi_1 = \exists \bigcirc c$$

Then $TS_3 \not\models_{CTL} \Phi_1$ but $TS_1, TS_2, TS_4 \models_{CTL} \Phi_1$.

- $TS_1 \not\sim TS_2$

A CTL formula that distinguishes TS_1 from TS_2 is the following:

$$\Phi_2 = \exists \bigcirc \exists \bigcirc (a \wedge \neg b)$$

Then $TS_1 \not\models_{CTL} \Phi_2$ but $TS_2 \models_{CTL} \Phi_2$.

Using the definition of bisimulation, one can argue as follows:

Assume $TS_1 \sim TS_2$. Then there exists a bisimulation relation $\mathcal{R} \subseteq S_1 \times S_2$ such that $(s_{1,1}, s_{1,2}) \in \mathcal{R}$. We have $(s_{1,1}, s_{1,2}) \in \mathcal{R}$ implies $(s_{3,1}, s_{3,2}) \in \mathcal{R}$. This cannot be true since we have $s_{1,2} \in \text{Post}(s_{3,2})$ with $L(s_{1,2}) = \{a\}$ but there is no successor state $t \in \text{Post}(s_{3,1})$ such that $L(t) = \{a\}$.

- $TS_1 \not\sim TS_4$

A CTL formula that distinguishes TS_1 from TS_4 is the following:

$$\Phi_3 = \exists \bigcirc \exists \bigcirc (a \wedge \neg b)$$

Then $TS_1 \not\models_{CTL} \Phi_3$ but $TS_4 \models_{CTL} \Phi_3$.

Using the definition of bisimulation, one can argue as follows:

Assume $TS_1 \sim TS_4$. Then there exists a bisimulation relation $\mathcal{R} \subseteq S_1 \times S_4$ such that $(s_{1,1}, s_{1,4}) \in \mathcal{R}$. We have $(s_{1,1}, s_{1,4}) \in \mathcal{R}$ implies $(s_{3,1}, s_{5,4}) \in \mathcal{R}$. This cannot be true since we have $s_{6,4} \in Post(s_{5,4})$ with $L(s_{6,4}) = \{a\}$ but there is no successor state $t \in Post(s_{3,1})$ such that $L(t) = \{a\}$.

- $TS_2 \not\sim TS_4$

A CTL formula that distinguishes TS_2 from TS_4 is the following:

$$\Phi_4 = \exists \bigcirc \exists \bigcirc (a \wedge b)$$

Then $TS_2 \models_{CTL} \Phi_4$ but $TS_4 \not\models_{CTL} \Phi_4$.

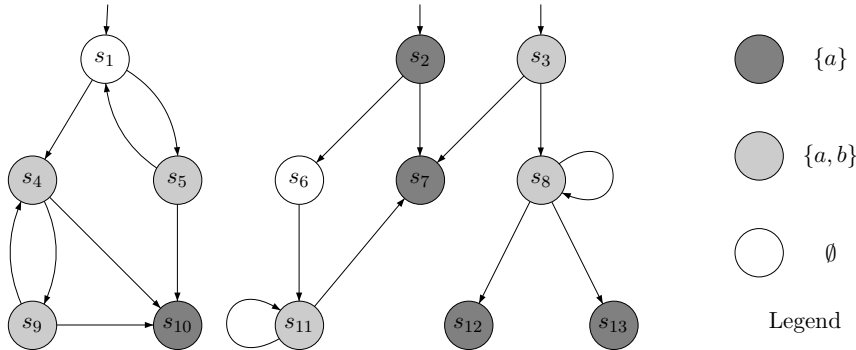
Using the definition of bisimulation, one can argue as follows:

Assume $TS_2 \sim TS_4$. Then there exists a bisimulation relation $\mathcal{R} \subseteq S_2 \times S_4$ such that $(s_{1,2}, s_{1,4}) \in \mathcal{R}$. We have $(s_{1,2}, s_{1,4}) \in \mathcal{R}$ implies $(s_{3,2}, s_{2,4}) \in \mathcal{R}$. This cannot be true since we have $s_{3,2} \in Post(s_{3,2})$ with $L(s_{3,2}) = \{a, b\}$ but there is no successor state $t \in Post(s_{2,4})$ such that $L(t) = \{a, b\}$.

Exercise 3

(2 + 2 points)

Consider the transition system TS over $AP = \{a, b\}$ shown in the figure below:



- Determine the bisimulation equivalence $\sim_{TS}$ and depict the bisimulation quotient system $TS/\sim$.
- Provide CTL master formulae Φ_C for each bisimulation equivalence class $C \in S/\sim$.

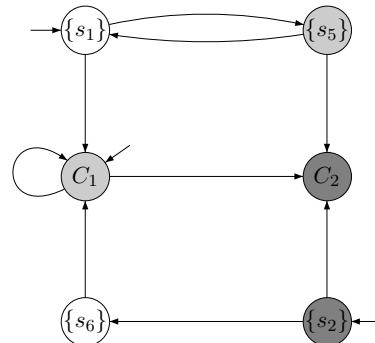
Solution:

- It goes as follows:

The bisimulation equivalence $\sim_{TS}$ is established as:

$$\begin{aligned} & \{(s_4, s_8), (s_4, s_3), (s_4, s_{11}), (s_9, s_8), (s_9, s_3), (s_9, s_{11})\}^* \\ & \cup \{(s_2, s_{10}), (s_7, s_{10}), (s_{10}, s_{12}), (s_{10}, s_{13})\}^* \end{aligned}$$

The quotient induced by $\sim$ is defined as $TS' = (S', Act', \rightarrow', I', AP, L')$, where $S' = \{\{s_1\}, \{s_2\}, \{s_5\}, \{s_6\}, C_1, C_2\}$ and $C_1 = \{s_3, s_4, s_8, s_9, s_{11}\}$, $C_2 = \{s_7, s_{10}, s_{12}, s_{13}\}$. The quotient system is depicted by the right figure.



(b) The master formula for each bisimulation equivalence class is defined as:

$$\begin{array}{ll}
\Phi_{\{s_1\}} = \neg a \wedge \neg b \wedge \exists \bigcirc \exists \bigcirc (\neg a \wedge \neg b) & \Phi_{\{s_2\}} = a \wedge \exists \bigcirc a \\
\Phi_{\{s_6\}} = \neg a \wedge \neg b \wedge \neg \exists \bigcirc \exists \bigcirc (\neg a \wedge \neg b) & \Phi_{\{s_5\}} = a \wedge b \wedge \neg \exists \bigcirc (a \wedge b) \\
\Phi_{C_1} = a \wedge b \wedge \exists \bigcirc (a \wedge b) & \Phi_{C_2} = a \wedge \neg b \wedge \neg \exists \bigcirc a
\end{array}$$