Model Checking – Exercise sheet 10

Exercise 10.1
Consider the following Kripke structures $\mathcal{K}_1$, $\mathcal{K}_2$, and $\mathcal{K}_3$, over $AP = \{p\}$:

(a) Does $\mathcal{K}_2$ simulate $\mathcal{K}_1$? If yes, give a simulation relation. Otherwise, explain why.
(b) Does $\mathcal{K}_2$ simulate $\mathcal{K}_3$? If yes, give a simulation relation. Otherwise, explain why.
(c) Does $\mathcal{K}_3$ simulate $\mathcal{K}_2$? If yes, give a simulation relation. Otherwise, explain why.
(d) Does $\mathcal{K}_3$ simulate $\mathcal{K}_1$? If yes, give a simulation relation. Otherwise, explain why.

Exercise 10.2
Let $\mathcal{K}_1$, $\mathcal{K}_2$, and $\mathcal{K}_3$ be Kripke structures. Show that if $\mathcal{K}_1$ and $\mathcal{K}_2$ are bisimilar, and $\mathcal{K}_2$ and $\mathcal{K}_3$ are bisimilar, then $\mathcal{K}_1$ and $\mathcal{K}_3$ are also bisimilar.
Exercise 10.3
(Taken from 'Principles of Model Checking')
Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system. A bisimulation for $TS$ is a binary relation $R$ on $S$ such that for all $(s_1, s_2) \in R$:

- $L(s_1) = L(s_2)$.
- If $s'_1 \in \text{Post}(s_1)$, then there exists an $s'_2 \in \text{Post}(s_2)$ with $(s'_1, s'_2) \in R$.
- If $s'_2 \in \text{Post}(s_2)$, then there exists an $s'_1 \in \text{Post}(s_1)$ with $(s'_1, s'_2) \in R$.

States $s_1$ and $s_2$ are bisimulation-equivalent (or bisimilar), denoted $s_1 \sim_{TS} s_2$, if there exists a bisimulation $R$ for $TS$ with $(s_1, s_2) \in R$. The relations $\sim_n \subseteq S \times S$ are inductively defined by:

(a) $s_1 \sim_0 s_2$ iff $L(s_1) = L(s_2)$.

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

Show that for finite $TS$ it holds that $\sim_{TS} = \bigcap_{n \geq 0} \sim_n$, i.e., $s_1 \sim_{TS} s_2$ if and only if $s_1 \sim_n s_2$ for all $n \geq 0$. 
Solution 10.1

(a) Yes. \( H = \{(s_0, t_0), (s_1, t_1), (s_2, t_2), (s_3, t_2), (s_4, t_0)\} \).

(b) No. If there exists a simulation \( H \) from \( K_3 \) to \( K_2 \), then we know that \( (u_0, t_0) \in H \).
Since \( u_0 \rightarrow u_1 \) we have \( (u_1, t_1) \in H \). However, \( u_1 \rightarrow u_4 \) and \( u_4 \) satisfies \( p \), but no successors of \( t_1 \) satisfy \( p \), so \( H \) cannot exist.

(c) Yes. \( H = \{(t_0, u_0), (t_1, u_1), (t_2, u_3)\} \).

(d) Yes. \( H = \{(s_0, u_0), (s_1, u_1), (s_2, u_3), (s_3, u_3), (s_4, u_0)\} \). Alternatively, we can also prove that \( K_1 \) and \( K_2 \) are bisimilar and use the result from (c).

Solution 10.2

Let \( H_{12} \) be a bisimulation between \( K_1 \) and \( K_2 \) and \( H_{23} \) be a bisimulation between \( K_2 \) and \( K_3 \). We define \( H_{13} = \{(s, u) \mid \exists t : (s, t) \in H_{12} \land (t, u) \in H_{23}\} \) and show that \( H_{13} \) is a bisimulation between \( K_1 \) and \( K_3 \).

First, we prove that \( H_{13} \) is a simulation from \( K_1 \) to \( K_3 \). Basically, we need to prove that if \( (s, u) \in H_{13} \) and \( s \rightarrow_1 s' \), then there exists \( u' \) such that \( u \rightarrow_3 u' \) and \( (s', u') \in H_{13} \).
From the definition of \( (s, u) \in H_{13} \), we know that there exists \( t \) such that \( (s, t) \in H_{12} \) and \( (t, u) \in H_{23} \). Since \( (s, t) \in H_{12} \) and \( s \rightarrow_1 s' \), there must exist \( t' \) such that \( t \rightarrow_2 t' \) and \( (s', t') \in H_{12} \). Similarly, since \( (t, u) \in H_{23} \) and \( t \rightarrow_2 t' \), there must exist \( u' \) such that \( u \rightarrow_3 u' \) and \( (t', u') \in H_{23} \). Because \( (s', t') \in H_{12} \) and \( (t', u') \in H_{23} \), by the definition of \( H_{13} \) we have \( (s', u') \in H_{13} \).

Analogously, we can prove that \( \{(u, s) \mid (s, u) \in H_{13}\} \) is a simulation from \( K_3 \) to \( K_1 \).

Solution 10.3

First we’ll show that \( s_1 \sim_{TS} s_2 \implies s_1 \sim_n s_2 \) for all \( n \geq 0 \) using induction on \( n \). Base case is trivial since \( s_1 \sim_{TS} s_2 \implies s_1 \sim_0 s_2 \). For the general case we assume that \( s_1 \sim_{TS} s_2 \implies s_1 \sim_{k-1} s_2 \) and we will show that \( s_1 \sim_{TS} s_2 \implies s_1 \sim_k s_2 \). Now, for a pair of states such that \( s_1 \sim_{TS} s_2 \) there exist an \( R \) such that \( (s_1, s_2) \in R \) and for \( s'_1 \in \text{Post}(s_1) \), there exist \( s'_2 \in \text{Post}(s_2) \) with \( (s'_1, s'_2) \in R \) which implies that \( s'_1 \sim_{TS} s'_2 \). By using the induction assumption, this implies that \( s'_1 \sim_{k-1} s'_2 \). Hence, the second condition in the definition of \( s_1 \sim_k s_2 \) is satisfied. Similarly, we can show that the third condition will also be satisfied.

For the other direction, we define a relation \( R := \{(s_1, s_2) \mid s_1 \sim_n s_2, \forall n \geq 0\} \). We shall now show that this is a bisimulation relation. We first claim that \( s_1 \sim_n s_2 \implies s_1 \sim_k s_2 \) for all \( k \leq n \) (Use induction on \( k \)). Now, since the \( TS \) is finite, there exist \( N \in \mathbb{N} \) such that \( \sim_k = \sim_N \) for all \( k \geq N \) (Why?). Assume \( (s_1, s_2) \in R \) then trivially \( L(s_1) = L(s_2) \) and if \( s'_1 \in \text{Post}(s_1) \) then pick some \( n_0 > N \) and since \( s_1 \sim_{n_0} s_2 \), there exists \( s'_2 \in \text{Post}(s_2) \) with \( s'_1 \sim_{n_0} s'_2 \) which implies that \( s'_1 \sim_n s'_2 \) for all \( n \geq 0 \). This means that \( (s'_1, s'_2) \in R \) and the second condition for \( R \) to be a bisimulation is satisfied. Similarly, \( R \) satisfies the third condition as well.