Technische Universität München (I7) **Summer Semester 2018**
J. Esparza / M. Blondin / P. Ashok **05.07.2018**

Model Checking – Sample Solution 11

Exercise 11.1

(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 $\mathcal{K}_3$ to $\mathcal{K}_2$, then we know that $(u_0, t_0) \in H$. Since $u_0 \to u_1$, we have $(u_1, t_1) \in H$. However, $u_1 \to u_4$ 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 $\mathcal{K}_1$ and $\mathcal{K}_2$ are bisimilar and use the result from (c).

Exercise 11.2

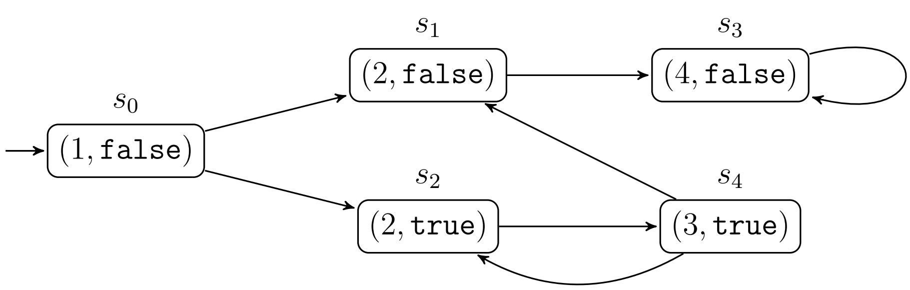
Let H_{12} be a bisimulation between $\mathcal{K}_1$ and $\mathcal{K}_2$ and H_{23} be a bisimulation between $\mathcal{K}_2$ and $\mathcal{K}_3$. We define $H_{13} = \{(s, u) \mid \exists t : (s, t) \in H_{12} \wedge (t, u) \in H_{23}\}$ and show that H_{13} is a bisimulation between $\mathcal{K}_1$ and $\mathcal{K}_3$.

First, we prove that H_{13} is a simulation from $\mathcal{K}_1$ to $\mathcal{K}_3$. Basically, we need to prove that if $(s, u) \in H_{13}$ and $s \to_1 s'$, then there exists u' such that $u \to_3 u'$ 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 $s \to_1 s'$, there must exist t' such that $t \to_2 t'$ and $(s', t') \in H_{12}$. Similarly, since $(t, u) \in H_{23}$ and $t \to_2 t'$, there must exist u' such that $u \to_3 u'$ 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 $(s', u') \in H_{13}$.

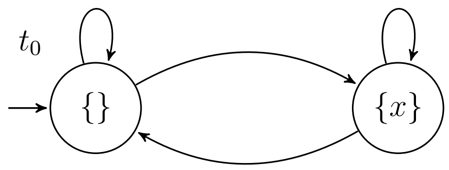
Analogously, we can prove that $\{(u, s) \mid (s, u) \in H_{13}\}$ is a simulation from $\mathcal{K}_3$ to $\mathcal{K}_1$.

Exercise 11.3

(a) Each state of the following Kripke structure $\mathcal{K}$ is a pair of a program location and a valuation of `x`.



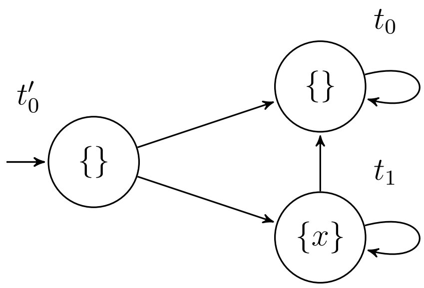
(b) Let $t_0 = [s0] = \{s_0, s_1, s_3\}$ and $t_1 = [s1] = \{s_2, s_4\}$. The abstraction $\mathcal{K}'$ is as follows:



(c) (i) $\mathcal{K}' \models \neg x \; \mathbf{W} \; x$

(ii) $\mathcal{K}' \not\models \mathbf{G}(\neg x \rightarrow \mathbf{X} \neg x)$. A counterexample in $\mathcal{K}'$ is $t_0 t_1 t_1^\omega$, which corresponds to the run $s_0 s_2 (s_4 s_2)^\omega$ in $\mathcal{K}$. So, $\mathcal{K} \not\models \mathbf{G}(\neg x \rightarrow \mathbf{X} \neg x)$.

(iii) $\mathcal{K}' \not\models \mathbf{X}(\neg x \rightarrow \mathbf{G} \neg x)$. A counterexample in $\mathcal{K}'$ is $t_0 t_0 t_1^\omega$. However, there are no corresponding runs in $\mathcal{K}$ because such paths must start with $s_0 s_1$, but no successors of s_1 are in t_1. Since $s_0 \in t_0$ and s_0 has a successor in t_1, we can refine the abstraction to distinguish s_0 from s_1. $t_0' = \{s_0\}$ and $t_0 = \{s_1, s_3\}$, and construct a new Kripke structure $\mathcal{K}''$ as follows.



We have $\mathcal{K}'' \models \mathbf{X}(\neg x \rightarrow \mathbf{G} \neg x)$.