Principles of Model Checking
Solutions to exercise class 5

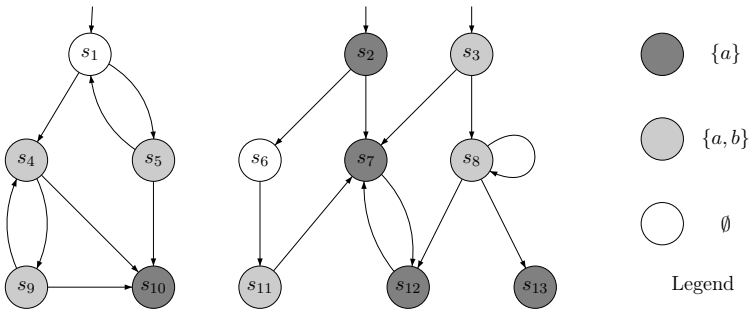
Abstraction

Prof. Dr. Joost-Pieter Katoen, Dr. Taolue Chen,
Dr. Jeroen Ketema, and Ir. Mark Timmer

October, 12, 2012

Problem 1

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



Determine the bisimulation quotient system $TS/\sim$ using the inefficient quotienting algorithm.

Solution:

The inefficient quotienting algorithm is shown in Table 1.

Outer Iteration		
1	$\Pi_{old} = \Pi_{AP} = \Big\{\{s_1, s_6\}, \{s_3, s_4, s_5, s_8, s_9, s_{11}\}, \{s_2, s_7, s_{10}, s_{12}, s_{13}\}\Big\}$	
	Inner iteration	
	1	$C = \{s_1, s_6\}$, $Pre(C) = \{s_2, s_5\}$
		$\Pi = \Big\{\{s_1, s_6\}, \underline{\{s_5\}}, \underline{\{s_3, s_4, s_8, s_9, s_{11}\}}, \underline{\{s_2\}}, \underline{\{s_7, s_{10}, s_{12}, s_{13}\}}\Big\}$
	2	$C = \{s_3, s_4, s_5, s_8, s_9, s_{11}\}$, $Pre(C) = \{s_1, s_3, s_4, s_6, s_8, s_9\}$
		$\Pi = \Big\{\{s_1, s_6\}, \{s_5\}, \underline{\{s_3, s_4, s_8, s_9\}}, \underline{\{s_{11}\}}, \{s_2\}, \{s_7, s_{10}, s_{12}, s_{13}\}\Big\}$
	3	$C = \{s_2, s_7, s_{10}, s_{12}, s_{13}\}$, $Pre(C) = \{s_2, s_3, s_4, s_5, s_7, s_8, s_9, s_{11}, s_{12}\}$
		$\Pi_1 = \Big\{\{s_1, s_6\}, \{s_5\}, \{s_3, s_4, s_8, s_9\}, \{s_{11}\}, \{s_2\}, \underline{\{s_7, s_{12}\}}, \underline{\{s_{10}, s_{13}\}}\Big\}$
2	$\Pi_{old} = \Pi_1 = \Big\{\{s_1, s_6\}, \{s_3, s_4, s_8, s_9\}, \{s_5\}, \{s_{11}\}, \{s_2\}, \{s_7, s_{12}\}, \{s_{10}, s_{13}\}\Big\}$	
	Inner iteration	
	1	$C = \{s_1, s_6\}$, $Pre(C) = \{s_2, s_5\}$
		$\Pi = \Pi_1$, unaffected
	2	$C = \{s_2\}$, $Pre(C) = \emptyset$
		$\Pi = \Pi_1$, unaffected
	3	$C = \{s_3, s_4, s_8, s_9\}$, $Pre(C) = \{s_1, s_3, s_4, s_8, s_9\}$
		$\Pi = \Big\{\underline{\{s_1\}}, \underline{\{s_6\}}, \{s_3, s_4, s_8, s_9\}, \{s_5\}, \{s_{11}\}, \{s_2\}, \{s_7, s_{12}\}, \{s_{10}, s_{13}\}\Big\}$
	4	$C = \{s_5\}$, $Pre(C) = \{s_1\}$
		Π unaffected
	5	$C = \{s_{11}\}$, $Pre(C) = \{s_6\}$
		Π unaffected
	6	$C = \{s_7, s_{12}\}$, $Pre(C) = \{s_2, s_3, s_7, s_8, s_{11}, s_{12}\}$
		$\Pi = \Big\{\{s_1\}, \{s_6\}, \underline{\{s_3, s_8\}}, \underline{\{s_4, s_9\}}, \{s_5\}, \{s_{11}\}, \{s_2\}, \{s_7, s_{12}\}, \{s_{10}, s_{13}\}\Big\}$
	7	$C = \{s_{10}, s_{13}\}$, $Pre(C) = \{s_4, s_5, s_8, s_9\}$
		$\Pi_2 = \Big\{\{s_1\}, \{s_6\}, \underline{\{s_3\}}, \underline{\{s_8\}}, \{s_4, s_9\}, \{s_5\}, \{s_{11}\}, \{s_2\}, \{s_7, s_{12}\}, \{s_{10}, s_{13}\}\Big\}$
3	$\Pi_{old} = \Pi_2 = \Big\{\{s_1\}, \{s_6\}, \{s_3\}, \{s_8\}, \{s_4, s_9\}, \{s_5\}, \{s_{11}\}, \{s_2\}, \{s_7, s_{12}\}, \{s_{10}, s_{13}\}\Big\}$	
	Inner iteration	
	1	$C = \{s_1\}$, $Pre(C) = \{s_5\}$, $\Pi = \Pi_{old}$, unaffected
	2	$C = \{s_6\}$, $Pre(C) = \{s_2\}$, $\Pi = \Pi_{old}$, unaffected
	3	$C = \{s_2\}$, $Pre(C) = \emptyset$, $\Pi = \Pi_{old}$, unaffected
	4	$C = \{s_3\}$, $Pre(C) = \emptyset$, $\Pi = \Pi_{old}$, unaffected
	5	$C = \{s_8\}$, $Pre(C) = \{s_3, s_8\}$, $\Pi = \Pi_{old}$, unaffected
	6	$C = \{s_4, s_9\}$, $Pre(C) = \{s_1, s_4, s_9\}$, $\Pi = \Pi_{old}$, unaffected
	7	$C = \{s_5\}$, $Pre(C) = \{s_1\}$, $\Pi = \Pi_{old}$, unaffected
	8	$C = \{s_{11}\}$, $Pre(C) = \{s_6\}$, $\Pi = \Pi_{old}$, unaffected
	9	$C = \{s_7, s_{12}\}$, $Pre(C) = \{s_2, s_3, s_7, s_8, s_{11}, s_{12}\}$, $\Pi = \Pi_{old}$, unaffected
	10	$C = \{s_{10}, s_{13}\}$, $Pre(C) = \{s_4, s_5, s_8, s_9\}$, $\Pi_3 = \Pi_{old}$, unaffected
	$\Pi_3 = \Pi_{old}$, the algorithm terminates here.	

Table 1: Inefficient bisimulation quotienting algorithm

Problem 2

Let $TS = (S, Act, \to, I, AP, L)$ 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 a $s_2' \in Post(s_2)$ with $s_1' \sim_n s_2'$,
  - for all $s_2' \in Post(s_2)$ there exists a $s_1' \in Post(s_1)$ with $s_1' \sim_n s_2'$.

(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 either a proof or a counterexample)?

Solution:

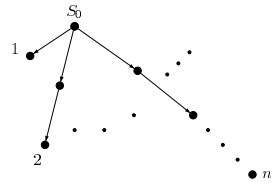
(i) We have to show that $\sim_{TS} = \bigcap_{n \geq 0} \sim_n$. Let R_n be the relation $\sim_n$ ($n \geq 0$) and let R be $\sim_{TS}$. We first claim that

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

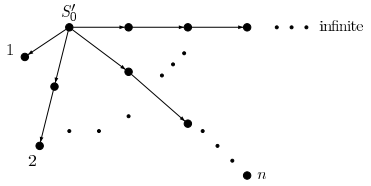
The fact that $S \times S \supseteq R_0$ follows by definition. Also, $R_0 \supseteq R_1$ since the requirements of R_1 contain the requirements of R_0. Now, we show by induction that $R_i \supseteq R_{i+1}$, under the hypothesis that $R_{i-1} \supseteq R_i$. So, let $(s,t) \in R_{i+1}$. We show that also $(s,t) \in R_i$. Since $(s,t) \in R_{i+1}$, by definition $L(s) = L(t)$ and for all $s' \in Post(s)$ there exists a $t' \in Post(t)$ with $s' \sim_i t'$ (and symmetrically). By the induction hypothesis, this implies $s' \sim_{i-1} t'$. Hence, $(s,t) \in R_i$.

As the state space S is finite, it is easy to see that there exists a k such that $R_k = R_{k+1} = R_{k+2} = \cdots$. Hence, using the claim above, we can conclude that $R_k = \bigcap_{n \geq 0} R_n$. As $R_k = R_{k+1}$, we find that $s \sim_k t$ if and only if $s \sim_{k+1} t$. Therefore, by definition of R_{k+1} we get that $R_{k+1} = R$, or, stated differently, that $\sim_{TS} = \bigcap_{n \geq 0} \sim_n$.

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



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

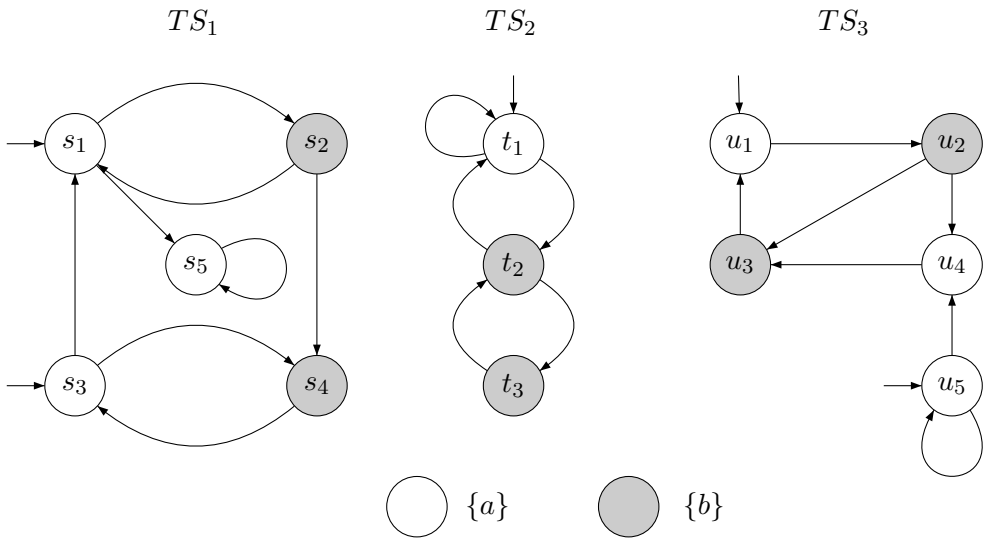


(b) TS': extension of TS by an infinite path.

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 according to $\sim_n$, as its difference from the infinite path in TS' will only be visible after n number of steps (and this is not taken into account by $\sim_n$). Hence, $s_0 \sim_n s'_0$ for every n.

Problem 3

Consider the following transition systems:



For each $i, j \in \{1 \dots 3\}$, $i \neq j$, determine whether $TS_i \trianglelefteq TS_j$ or $TS_i \not\trianglelefteq TS_j$.

Solution:

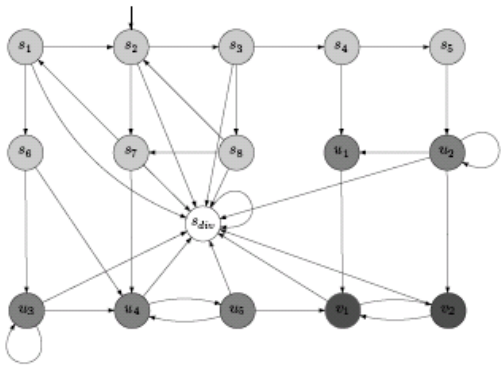
First, note that the traces of TS_1 are all stutter-equivalent to a trace from the set $T_1 = \{(ab)^\omega, (ab)^* a^\omega\}$. The traces of TS_2 are all stutter-equivalent to a trace from the set $T_2 = \{(ab)^\omega, (ab)^* a^\omega, (ab)^+ b^\omega\}$. Finally, the traces of TS_3 are all stutter-equivalent to a trace from the set $T_3 = \{(ab)^\omega, a^\omega\}$.

- $TS_1 \trianglelefteq TS_2$, since $T_1 \subseteq T_2$.
- $TS_2 \not\trianglelefteq TS_1$, since the trace $ab^\omega \in \mathit{Traces}(TS_2)$ cannot be mimicked by a stutter-equivalent trace in TS_1.
- $TS_1 \not\trianglelefteq TS_3$, since $aba^\omega \in \mathit{Traces}(TS_1)$ cannot be mimicked by a stutter-equivalent trace in TS_3.
- $TS_3 \trianglelefteq TS_1$, since both trace types in T_3 can be mimicked by trace types in T_1. After all, note that a^ω is part of $(ab)^* a^\omega$.
- $TS_2 \not\trianglelefteq TS_3$, since $ab^\omega \in \mathit{Traces}(TS_2)$ cannot be mimicked by a stutter-equivalent trace in TS_3.
- $TS_3 \trianglelefteq TS_2$, since $TS_3 \trianglelefteq TS_1$ and $TS_1 \trianglelefteq TS_2$.

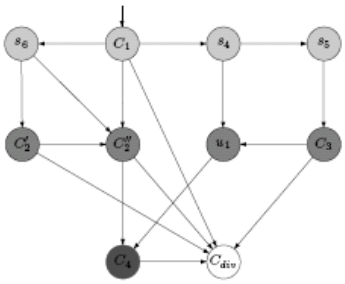
Problem 4

See next pages.

(a) The divergence-sensitive expansion $\overline{TS}$ is as follows:



(b) The first step is to remove stutter cycles (in fact, SCCs) from $\overline{TS}$. This yields the transition system, say $\overline{TS}'$, depicted below where $C_1 = \{ s_1, s_2, s_3, s_7, s_8 \}$, $C_2' = \{ u_3 \}$, $C_2'' = \{ u_4, u_5 \}$, $C_3 = \{ u_2 \}$, $C_4 = \{ v_1, v_2 \}$ and $C_{div} = \{ s_{div} \}$.



We now apply Algorithm 37 to determine $\overline{TS}' / \approx$.

The initial partition is:

$$\Pi_{AP} = \Big\{ \underbrace{\{s_6, C_1, s_4, s_5\}}_{B_1}, \underbrace{\{C_2', C_2'', u_1, C_3\}}_{B_2}, \underbrace{\{C_4\}}_{B_3}, \underbrace{\{C_{div}\}}_{B_4} \Big\}$$

Iteration 1: Choose $C = B_4$. Check whether C is a splitter for B_1 and B_2, respectively. Note that B_3 and B_4 are singleton sets and cannot be split any further. We have $Pre(C) = \{C_1, C_2', C_2'', C_3, C_4\}$.

- Consider B_1. $Bottom(B_1) = \{s_5, s_6\}$. Since $B_1 \neq C$, $B_1 \cap Pre(C) = \{C_1\} \neq \emptyset$ and $Bottom(B_1) \setminus Pre(C) = \{s_5, s_6\} \neq \emptyset$, C is a splitter for B_1. B_1 is splitted by C into two subblocks:
  $B_{11} = B_1 \cap Pre^*_\Pi(C) = \{C_1\}$ and $B_{12} = B_1 \setminus Pre^*_\Pi(C) = \{s_4, s_5, s_6\}$.
- Consider B_2. $Bottom(B_2) = \{C_2'', u_1\}$. Since $B_2 \neq B_4$, $B_2 \cap Pre(C) = \{C_2', C_2'', C_3\} \neq \emptyset$ and $Bottom(B_2) \setminus Pre(C) = \{u_1\} \neq \emptyset$, C is a splitter for B_2. B_2 is splitted by C into two subblocks:
  $B_{21} = B_2 \cap Pre^*_\Pi(C) = \{C_2', C_2'', C_3\}$ and $B_{22} = B_1 \setminus Pre^*_\Pi(C) = \{u_1\}$.

At the end of this iteration, we have:

$$\Pi = \Big\{ \underbrace{\{C_1\}}_{B_{11}}, \underbrace{\{s_6, s_4, s_5\}}_{B_{12}}, \underbrace{\{C_2', C_2'', C_3\}}_{B_{21}}, \underbrace{\{u_1\}}_{B_{22}}, \underbrace{\{C_4\}}_{B_3}, \underbrace{\{C_{div}\}}_{B_4} \Big\}$$

Iteration 2: Choose $C = B_{22}$. Check whether C is a splitter for B_{12} and B_{21}. We have $Pre(C) = \{s_4, C_3\}$.

* Consider B_{12}. We have $Bottom(B_{12}) = \{s_5, s_6\}$. C is a splitter for B_{12}, since $B_{12} \neq C$, $B_{12} \cap Pre(C) = \{s_4\} \neq \varnothing$, and $Bottom(B_{12}) \setminus Pre(C) = \{s_5, s_6\} \neq \varnothing$. B_{12} is split by C into two subblocks:

$$B_{121} = B_{12} \cap Pre^*_\Pi(C) = \{s_4\} \quad \text{and} \quad B_{122} = B_{12} \setminus Pre^*_\Pi(C) = \{s_5, s_6\}.$$

* Consider B_{21}. We have $Bottom(B_{21}) = \{C''_2, C_3\}$. C is a splitter for B_{21}, since $B_{21} \neq C$, $B_{21} \cap Pre(C) = \{C_3\} \neq \varnothing$ and $Bottom(B_{21}) \setminus Pre(C) = \{C''_2\} \neq \varnothing$. B_{21} is split by C into two subblocks:

$$B_{211} = B_{21} \cap Pre^*_\Pi(C) = \{C_3\} \quad \text{and} \quad B_{212} = B_{21} \setminus Pre^*_\Pi(C) = \{C'_2, C''_2\}.$$

At the end of this iteration we have:

$$\Pi = \Big\{ \underbrace{\{C_1\}}_{B_{11}}, \underbrace{\{s_4\}}_{B_{121}}, \underbrace{\{s_6, s_5\}}_{B_{122}}, \underbrace{\{C_3\}}_{B_{211}}, \underbrace{\{C'_2, C''_2\}}_{B_{212}}, \underbrace{\{u_1\}}_{B_{22}}, \underbrace{\{C_4\}}_{B_3}, \underbrace{\{C_{div}\}}_{B_4} \Big\}$$

Iteration 3: Choose $C = B_{211}$, and check whether C is a splitter for B_{122}. We have $Pre(C) = \{s_5\}$.

* Consider B_{122}. We have $Bottom(B_{122}) = \{s_5, s_6\}$. C is a splitter for B_{122}, since $B_{122} \neq C$, $B_{122} \cap Pre(C) = \{s_5\} \neq \varnothing$, and $Bottom(B_{122}) \setminus Pre(C) = \{s_6\} \neq \varnothing$. B_{122} is split by C into two subblocks:

$$B_{1221} = B_{122} \cap Pre^*_\Pi(C) = \{s_5\} \quad \text{and} \quad B_{1222} = B_{122} \setminus Pre^*_\Pi(C) = \{s_6\}.$$

At the end of this iteration, we have:

$$\begin{aligned} \Pi &= \Big\{ \underbrace{\{C_1\}}_{B_{11}}, \underbrace{\{s_4\}}_{B_{121}}, \underbrace{\{s_5\}}_{B_{1221}}, \underbrace{\{s_6\}}_{B_{1222}}, \underbrace{\{C_3\}}_{B_{211}}, \underbrace{\{C'_2, C''_2\}}_{B_{212}}, \underbrace{\{u_1\}}_{B_{22}}, \underbrace{\{C_4\}}_{B_3}, \underbrace{\{C_{div}\}}_{B_4} \Big\} \\ &= \Big\{ \underbrace{\{s_1, s_2, s_3, s_7, s_8\}}_{B'_1}, \underbrace{\{s_4\}}_{B'_2}, \underbrace{\{s_5\}}_{B'_3}, \underbrace{\{s_6\}}_{B'_4}, \underbrace{\{u_2\}}_{B'_6}, \underbrace{\{u_3, u_4, u_5\}}_{B'_7}, \underbrace{\{u_1\}}_{B'_5}, \underbrace{\{v_1, v_2\}}_{B'_8}, \underbrace{\{s_{div}\}}_{B'_9} \Big\} \end{aligned}$$

There are no more splitters for any blocks, thus the algorithm terminates.

(c) $\overline{TS}'/\approx$ and $TS/\approx^{div}$ are shown in the following figures (left and right), respectively.