

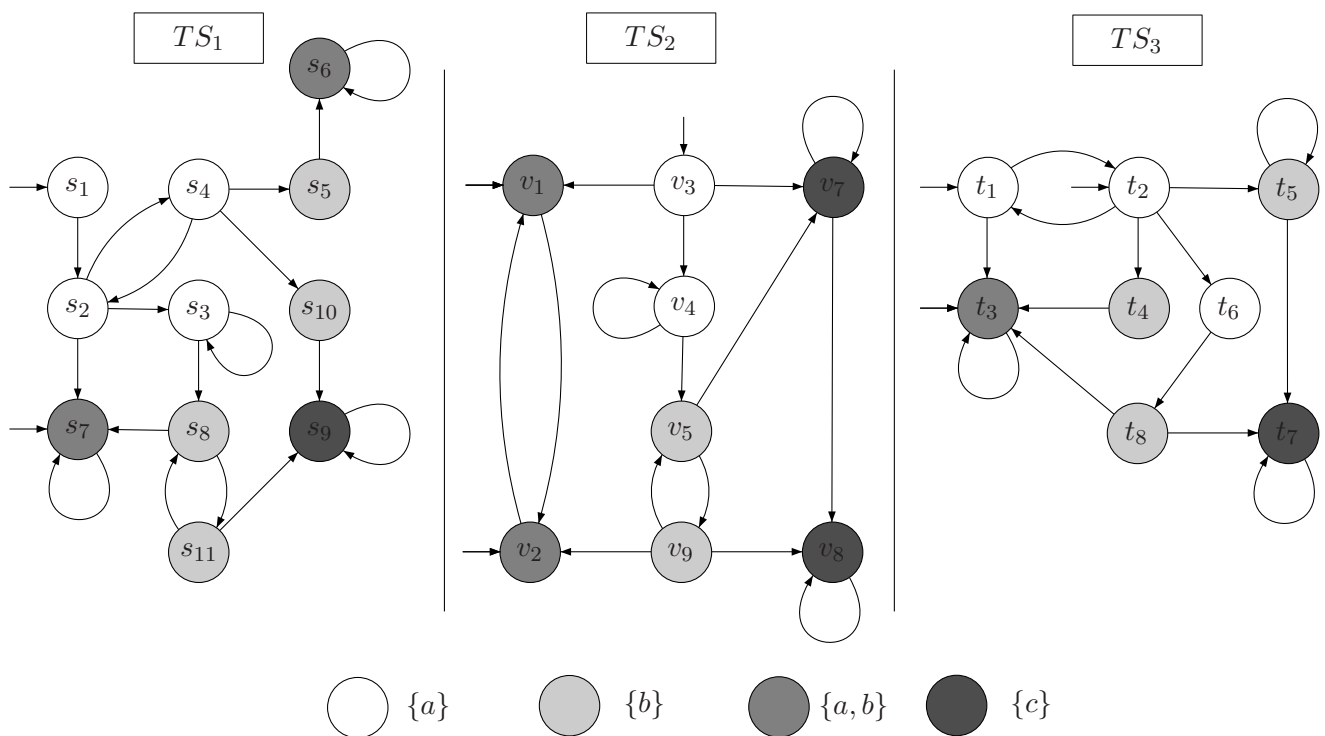
Advanced Model Checking Summer term 2014

– Solution 4 –

Exercise 1

(3 points)

Consider three transitions systems given on the next Figure:



For each $i, j \in \{1 \dots 3\} \times \{1 \dots 3\}$, $i \neq j$, determine whether $TS_i \approx TS_j$ or $TS_i \not\approx TS_j$. Justify your answer.

Solution:

- $TS_1 \approx TS_3$:

– Consider the following binary relation:

$$R = \{(s_1, t_1), (s_1, t_2), (s_2, t_1), (s_2, t_2), (s_4, t_1), (s_4, t_2), (s_3, t_6), (s_5, t_4), (s_6, t_3), (s_7, t_3), (s_8, t_8), (s_{11}, t_8), (s_9, t_7)\}$$

– Notice that R and R^{-1} are stutter-bisimulations for $TS_1 \oplus TS_3$.

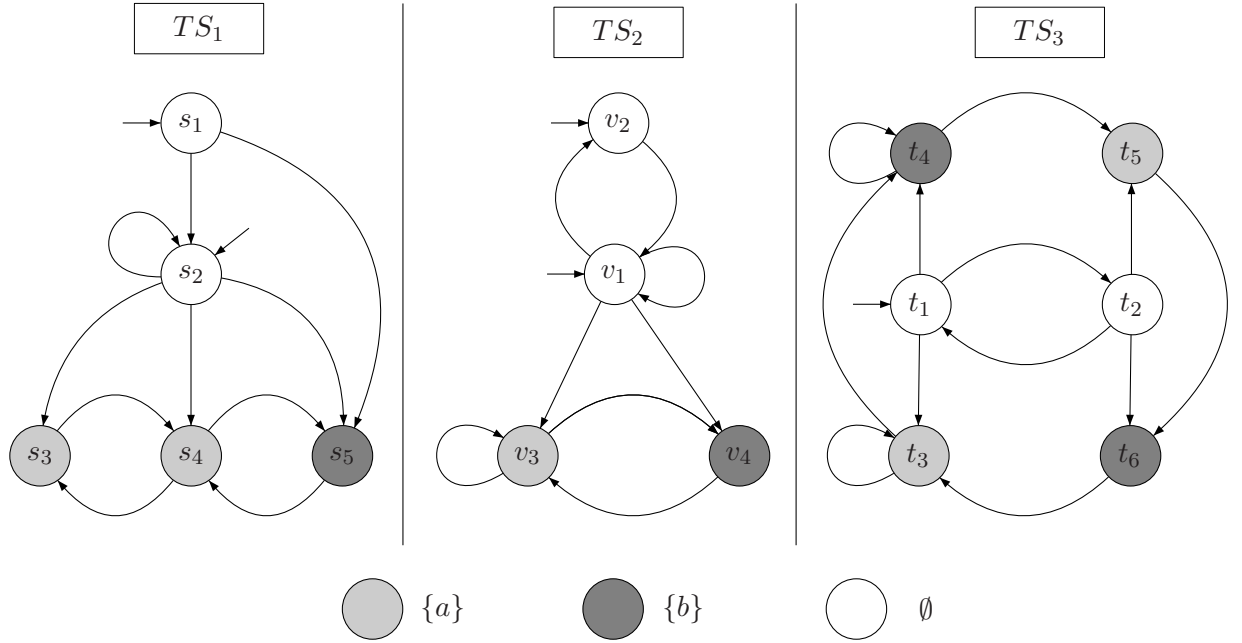
– Also for initial states $I_1 = \{s_1, s_7\}$ of TS_1 and initial states $I_3 = \{t_1, t_2, t_3\}$ of TS_3 we have: $(s_1, t_1) \in R$, $(s_1, t_2) \in R$, $(s_7, t_3) \in R$.

- $TS_1 \not\approx TS_2$: Because of states s_5 and s_{10} in TS_1 that are not stutter bisimilar to any of the states in TS_2 (For TS_3 such states are t_4 and t_5).

Exercise 2

(3 points)

Consider the transition systems TS_1 , TS_2 , TS_3 over $AP = \{a, b\}$ shown in the following figure:



Questions:

- for each $i, j \in \{1 \dots 3\} \times \{1 \dots 3\}$, $i \neq j$, determine whether $TS_i \preceq TS_j$
- for each case $TS_i \not\preceq TS_j$, give a $\forall\text{CTL}_{\setminus \cup}$ -formula that distinguishes TS_i and TS_j .

Solution:

- Try to construct the simulation relation R by the *Definition 7.46* of the Lecture notes:

(1) $TS_1 \preceq TS_2$: The simulation is $R = \{(s_1, v_1), (s_2, v_1), (s_3, v_3), (s_4, v_3), (s_5, v_4)\}$.

(2) $TS_2 \not\preceq TS_3$:

- State v_1 should be simulated by t_1 as an initial state.
- State $v_1 \in \text{Post}(v_1)$ should be simulated by $t_2 \in \text{Post}(t_1)$ as it is the only state from $\text{Post}(t_1)$ such that $L(v_1) = L(t_2)$.
- Then similarly $v_3 \in \text{Post}(v_1)$ should be simulated by $t_5 \in \text{Post}(t_2)$, which is not the case because $v_3 \in \text{Post}(v_3)$ and there is no state in $\text{Post}(t_5)$ labelled with $L(v_3)$.

(3) $TS_1 \not\preceq TS_3$:

- State s_2 should be simulated by t_1 as an initial state.
- State $s_2 \in \text{Post}(s_2)$ should be simulated by $t_2 \in \text{Post}(t_1)$ as it is the only state from $\text{Post}(t_1)$ such that $L(s_2) = L(t_2)$.
- Then similarly $s_3 \in \text{Post}(s_2)$ should be simulated by $t_5 \in \text{Post}(t_2)$, which is not the case because $s_4 \in \text{Post}(s_3)$ and there is no state in $\text{Post}(t_5)$ labelled with $L(s_4)$.

(4) $TS_2 \not\preceq TS_1$:

- State v_1 should be simulated by s_1 or s_2 as an initial state.
- State s_1 does not simulate v_1 because for $v_3 \in \text{Post}(v_1)$ and $\text{Post}(s_1) = \{s_2, s_5\}$ we have $L(v_3) \neq L(s_2)$ and $L(v_3) \neq L(s_5)$.
- For state s_2 to simulate v_1 , state $v_3 \in \text{Post}(v_1)$ should be simulated by s_3 or $s_4 \in \text{Post}(s_2) = \{s_3, s_4, s_5\}$ (as $L(v_3) = L(s_3) = L(s_4) \neq L(s_5)$).

- State v_3 can not be simulated by s_3 as there is no transition to the state labelled with $\{b\}$.
- State s_4 can not simulate v_3 because for $v_3 \in Post(v_3)$ only $s_3 \in Post(s_4)$ could simulate it due to the labelling, but we've seen in the previous point that it is not the case.

(5) $TS_3 \not\preceq TS_1$:

- State t_1 should be simulated by either s_1 or s_2 as an initial state.
- State s_1 does not simulate t_1 because for $t_3 \in Post(t_1)$ and $Post(s_1) = \{s_2, s_5\}$ we have $L(t_3) \neq L(s_2)$ and $L(v_3) \neq L(s_5)$.
- For state s_2 to simulate t_1 , state $t_4 \in Post(t_1)$ should be simulated by $s_5 \in Post(s_2) = \{s_3, s_4, s_5\}$ (as only $L(t_4) = L(s_5)$).
- State t_4 can not be simulated by s_5 as $t_4 \in Post(t_4)$ but there is no transition to the state labelled with $\{b\}$ from s_5 .

(6) $TS_3 \not\preceq TS_2$:

- State t_1 should be simulated by either v_1 or v_2 as an initial state.
- State v_2 does not simulate t_1 because for $t_3 \in Post(t_1)$ and $Post(v_2) = \{v_1\}$ we have $L(t_3) \neq L(v_1)$.
- For state v_1 to simulate t_1 , state $t_4 \in Post(t_1)$ should be simulated by $v_4 \in Post(v_1) = \{v_3, v_4\}$ (as only $L(t_4) = L(v_4)$).
- State t_4 can not be simulated by v_4 as $t_4 \in Post(t_4)$ but there is no transition to the state labelled with $\{b\}$ from v_4 .

(b) Consider the following cases:

- (1) $TS_1 \not\preceq TS_3$ **and** $TS_2 \not\preceq TS_3$: The following formula is valid in TS_3 but not in TS_1 and TS_2 , it is targeted on distinguishing state t_5 from states s_3, s_4, v_3 .

$$\forall \bigcirc (\neg b \vee \forall \bigcirc (\neg a \vee \forall \bigcirc b))$$

- (2) $TS_2 \not\preceq TS_1$: The following formula is valid in TS_1 but not in TS_2 , it is targeted on distinguishing state s_3 from state v_3 .

$$\forall \bigcirc (\neg b \vee \forall \bigcirc \forall \bigcirc (\neg a \vee \forall \bigcirc a))$$

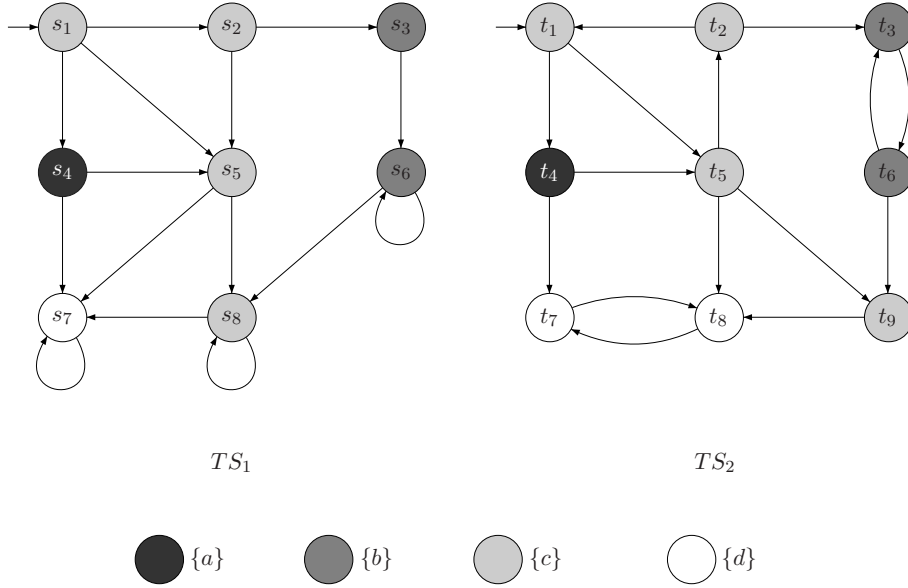
- (3) $TS_3 \not\preceq TS_1$ **and** $TS_3 \not\preceq TS_2$: The following formula is valid in TS_1 and TS_2 but not in TS_3 , it is targeted on distinguishing states s_5, v_4 from state t_4 .

$$\forall \bigcirc (\neg b \vee \forall \bigcirc a)$$

Exercise 3

(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.

Solution:

- (a) No, $TS_1 \not\approx TS_2$. The state space of $TS_1 / \approx$ is $\left\{ \{s_1\}, \{s_2\}, \{s_3, s_6\}, \{s_4\}, \{s_5, s_8\}, \{s_7\} \right\}$. And the state space of $TS_2 / \approx$ is $\left\{ \{t_1, t_2, t_5\}, \{t_4\}, \{t_3, t_6\}, \{t_7, t_8\}, \{t_9\} \right\}$. Let $C_{11} = \{s_1\}$, $C_{12} = \{s_7\}$, $C_{21} = \{t_1, t_2, t_5\}$ and $C_{22} = \{t_7, t_8\}$. C_{11} and C_{21} are initial states in both $TS_1 / \approx$ and $TS_2 / \approx$. In $TS_2 / \approx$, $C_{21} \rightarrow C_{22}$, where $L(C_{21}) = c$ and $L(C_{22}) = d$; but in $TS_1 / \approx$ there is no transition from C_{11} that can mimic this. Thus, $TS_1 \approx (TS_1 / \approx) \not\approx (TS_2 / \approx) \approx TS_2$, so we have $TS_1 \not\approx TS_2$.

- (b) No, $TS_1 \not\approx^{div} TS_2$. Since $\approx^{div}$ implies $\approx$, $TS_1 \not\approx TS_2$ implies $TS_1 \not\approx^{div} TS_2$.

The $CTL \setminus \bigcirc$ formula that can distinguish them is $\Phi = \exists \Diamond (a \wedge \exists \Diamond b)$, where $TS_1 \not\models \Phi$ but $TS_2 \models \Phi$.