

Advanced Model Checking Summer term 2014

– Series 6 –

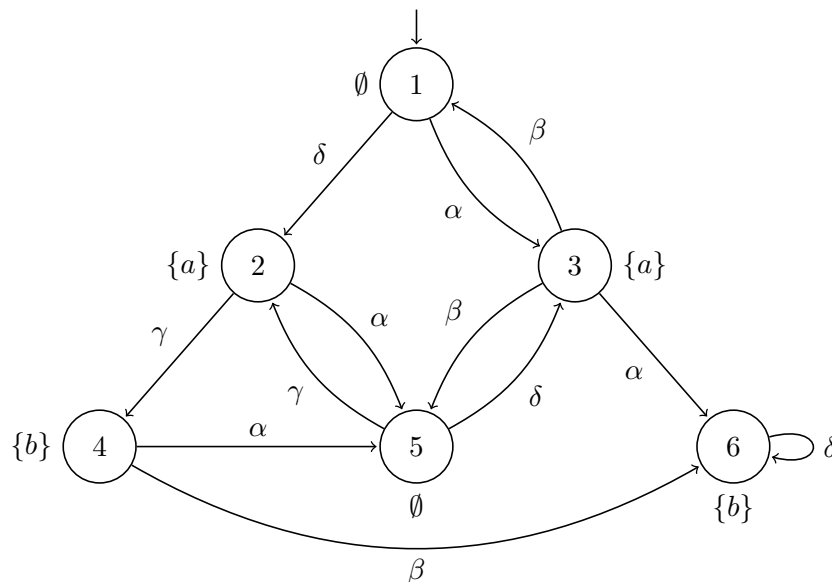
Hand in on 28 May before the exercise class.

Note: From now on, if you have questions regarding the lecture or the exercises, please contact me (dehnert@cs.rwth...)

Exercise 1

(3 points)

Consider the following transition system TS. Compute the simulation preorder $\preceq_{\text{TS}}$ using (the first version of) the HHK algorithm presented in the lecture (slide 199). Whenever there are multiple states k such that $\text{Sim}_{\text{old}}(k) \neq \text{Sim}(k)$, then pick the **largest** such k .



Solution:

Initialization:

- $\text{Sim}_{\text{old}}(i) = S$ for all $i \in S$
- $\text{Sim}(1) = \text{Sim}(5) = \{1, 5\}$
- $\text{Sim}(2) = \text{Sim}(3) = \{2, 3\}$
- $\text{Sim}(4) = \text{Sim}(6) = \{4, 6\}$

Loop:

- Pick $s'_1 = 6$:
 - $\text{Remove}(6) = S \setminus \text{Pre}(\text{Sim}(6)) = S \setminus \{2, 3, 4, 6\} = \{1, 5\}$
 - $\text{Sim}(4) = \text{Sim}(4) \setminus \text{Remove}(6) = \{4, 6\}$

- $\text{Sim}(6) = \text{Sim}(6) \setminus \text{Remove}(6) = \{4, 6\}$
- $\text{Sim}(3) = \text{Sim}(3) \setminus \text{Remove}(6) = \{2, 3\}$
- $\text{Sim}_{\text{old}}(6) = \text{Sim}(6) = \{4, 6\}$
- Pick $s'_1 = 5$:
 - $\text{Remove}(5) = S \setminus \text{Pre}(\text{Sim}(5)) = S \setminus \{2, 3, 4\} = \{1, 5, 6\}$
 - $\text{Sim}(2) = \text{Sim}(2) \setminus \text{Remove}(5) = \{2, 3\}$
 - $\text{Sim}(3) = \text{Sim}(3) \setminus \text{Remove}(5) = \{2, 3\}$
 - $\text{Sim}(4) = \text{Sim}(4) \setminus \text{Remove}(5) = \{4\}$
 - $\text{Sim}_{\text{old}}(5) = \text{Sim}(5) = \{1, 5\}$
- Pick $s'_1 = 4$:
 - $\text{Remove}(s_4) = S \setminus \text{Pre}(\text{Sim}(4)) = S \setminus \{2\} = \{1, 3, 4, 5, 6\}$
 - $\text{Sim}(2) = \text{Sim}(2) \setminus \text{Remove}(4) = \{2\}$
 - $\text{Sim}_{\text{old}}(4) = \text{Sim}(4) = \{4\}$
- Pick $s'_1 = 3$:
 - $\text{Remove}(3) = S \setminus \text{Pre}(\text{Sim}(3)) = S \setminus \{1, 5\} = \{2, 3, 4, 6\}$
 - $\text{Sim}(1) = \text{Sim}(1) \setminus \text{Remove}(3) = \{1, 5\}$
 - $\text{Sim}(5) = \text{Sim}(5) \setminus \text{Remove}(3) = \{1, 5\}$
 - $\text{Sim}_{\text{old}}(3) = \text{Sim}(3) = \{2, 3\}$
- Pick $s'_1 = 2$:
 - $\text{Remove}(2) = S \setminus \text{Pre}(\text{Sim}(2)) = S \setminus \{1, 5\} = \{2, 3, 4, 6\}$
 - $\text{Sim}(1) = \text{Sim}(1) \setminus \text{Remove}(2) = \{1, 5\}$
 - $\text{Sim}(5) = \text{Sim}(5) \setminus \text{Remove}(2) = \{1, 5\}$
 - $\text{Sim}_{\text{old}}(2) = \text{Sim}(2) = \{2\}$
- Pick $s'_1 = 1$:
 - $\text{Remove}(1) = S \setminus \text{Pre}(\text{Sim}(1)) = S \setminus \{2, 3, 4\} = \{1, 5, 6\}$
 - $\text{Sim}(3) = \text{Sim}(3) \setminus \text{Remove}(1) = \{2, 3\}$
 - $\text{Sim}_{\text{old}}(1) = \text{Sim}(1) = \{1, 5\}$

Done. The resulting simulator sets are:

- $\text{Sim}(1) = \text{Sim}(5) = \{1, 5\}$
- $\text{Sim}(2) = \{2\}$
- $\text{Sim}(3) = \{2, 3\}$
- $\text{Sim}(4) = \{4\}$
- $\text{Sim}(6) = \{4, 6\}$

Exercise 2

(7 points)

For a transition system $TS = (S, Act, \longrightarrow, I, AP, L)$ without terminal states, a stutter simulation for TS is a binary relation $\mathcal{R} \subseteq S \times S$ such that for all $(s_1, s_2) \in \mathcal{R}$:

- (i) $L(s_1) = L(s_2)$.
- (ii) If $s'_1 \in Post(s_1)$ with $(s'_1, s_2) \notin \mathcal{R}$, then there exists a finite path fragment $s_2 u_1 \dots u_n s'_2$ with $n \geq 0$, $(s_1, u_i) \in \mathcal{R}$ for $1 \leq i \leq n$ and $(s'_1, s'_2) \in \mathcal{R}$.

Let $s_1 \preceq_{TS}^{st} s_2$ if there exists a stutter simulation $\mathcal{R}$ for TS such that $(s_1, s_2) \in \mathcal{R}$.

- (a) Show that $\preceq_{TS}^{st}$ is a preorder.
- (b) Which logical fragment A of CTL^* characterizes¹ the kernel² of $\preceq_{TS}^{st}$? Justify your answer.
- (c) Suppose for all $\Phi \in A$, we have $s_2 \models \Phi$ if and only if $s_1 \models \Phi$. Show that $L(s_1) = L(s_2)$.

Solution:

- a) To show this, we need to prove that $\preceq_{TS}^{st}$ is reflexive and transitive. Reflexivity follows directly from the definition, so we only need to establish the transitivity. For this, suppose we have (i) $s_1 \preceq_{TS}^{st} s_2$ and (ii) $s_2 \preceq_{TS}^{st} s_3$. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be stutter simulations such that $(s_1, s_2) \in \mathcal{R}_1$ and $(s_2, s_3) \in \mathcal{R}_2$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2 \text{ such that } (s_1, s_2) \in \mathcal{R}_1 \text{ and } (s_2, s_3) \in \mathcal{R}_2\}.$$

We have to prove that $\mathcal{R}$ is indeed a stutter simulation, so we need to check both conditions for $\mathcal{R}$.

Therefore, let $(s_1, s_3) \in \mathcal{R}$ and s_2 be a state such that $(s_1, s_2) \in \mathcal{R}_1$ and $(s_2, s_3) \in \mathcal{R}_2$.

Condition (i): Since $(s_1, s_2) \in \mathcal{R}_1$ and $(s_2, s_3) \in \mathcal{R}_2$ we have $L(s_1) = L(s_2) = L(s_3)$.

Condition (ii): Let $s'_1 \in Post(s_1)$ with $(s'_1, s_3) \notin \mathcal{R}$. Furthermore, let $\pi \downarrow$ denote the last state of a non-empty state sequence π .

- Then, we have $(s'_1, s_2) \notin \mathcal{R}_1$ (because otherwise, it would follow from $(s_2, s_3) \in \mathcal{R}_2$ and the definition of $\mathcal{R}$ that $(s'_1, s_3) \in \mathcal{R}$, which is a contradiction).
- Since $(s'_1, s_2) \notin \mathcal{R}_1$ and $(s_1, s_2) \in \mathcal{R}_1$, there exists a finite path fragment $u_0 u_1 \dots u_{n-1} u_n$ with $n > 0$, $u_0 = s_2$, $(s_1, u_i) \in \mathcal{R}_1$ for all $1 \leq i < n$ and $(s'_1, u_n) \in \mathcal{R}_1$.
- Define $\pi: \{0, \dots, n\} \rightarrow S^*$ by

$$\pi(i) = \begin{cases} s_3 & \text{if } i = 0 \\ v_0^i & \text{if } (u_i, \pi(i-1)\downarrow) \in \mathcal{R}_2, v_0^i = \pi(i-1)\downarrow \text{ and } i > 0 \\ \pi_{sim}^i & \text{if } (u_i, \pi(i-1)\downarrow) \notin \mathcal{R}_2 \text{ and } i > 0 \end{cases}$$

where $\pi_{sim}^i = v_0^i \dots v_{m_i}^i$, $m_i > 0$, $v_0^i = \pi(i-1)\downarrow$, $(u_{i-1}, v_j^i) \in \mathcal{R}_2$ for all $1 \leq i < n$, $1 \leq j < m_i$ and $(u_i, v_{m_i}^i) \in \mathcal{R}_2$. This path fragment exists, because $u_i \in Post(u_{i-1})$ and $(u_i, \pi(i-1)\downarrow) \notin \mathcal{R}_2$. Furthermore, define $m_i := 1$ in case $\pi(i) = v_0^i = \pi(i-1)\downarrow$.

- Obviously $\pi(i)\downarrow$ is the first state of $\pi(i+1)$ for $0 \leq i < n$. Let $s_1 \dots s_n \circ s_n t_1 \dots t_m = s_1 \dots s_n t_1 \dots t_m$.

Then $\pi(0) \circ \dots \circ \pi(n)$ is an execution fragment in TS starting in s_3 . Since $(s_1, u_i) \in \mathcal{R}_1$ for all $1 \leq i < n$ and $(u_{i-1}, v_j^i) \in \mathcal{R}_2$ for all $1 \leq i < n$ and $1 \leq j < m_i$, we have $(s_1, v_j^i) \in \mathcal{R}$ for all $1 \leq i < n$ and $1 \leq j < m_i$. Finally, $(u_n, \pi(n)\downarrow) \in \mathcal{R}_2$ and therefore $(s'_1, \pi(n)\downarrow) \in \mathcal{R}$.

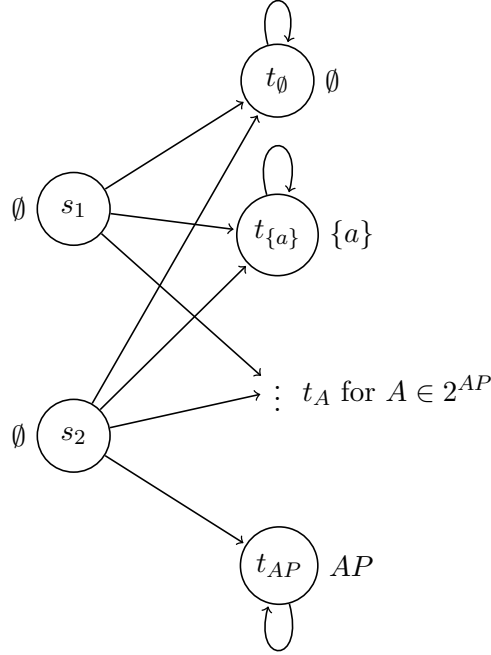
- This means that condition (ii) is satisfied.

¹That is, two states are equivalent if and only if they satisfy the same formulae of the logic.

²The kernel of a binary relation $\mathcal{R}$ is defined as the intersection $\mathcal{R} \cap \mathcal{R}^{-1}$.

b) Let $\simeq_{\text{TS}}^{\text{st}}$ denote the kernel of $\preceq_{\text{TS}}^{\text{st}}$.

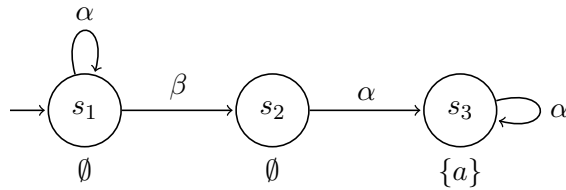
First of all, if infinite transition systems are considered, there is no such fragment. Consider the following transition system with an infinite set of atomic propositions.



Obviously, $s_1 \not\simeq_{\text{TS}}^{\text{st}} s_2$, but s_1 and s_2 cannot be distinguished by any CTL* formula, because every formula can only mention finitely many atomic propositions and $s_1 \simeq_{\text{TS}}^{\text{st}} s_2$ if the set of atomic propositions is restricted to any finite subset. Let us therefore now consider finite transition systems (without terminal states) only.

$\simeq_{\text{TS}}^{\text{st}}$ is at least as coarse as $\simeq_{\text{TS}}$, so there is no hope to preserve any properties that are not preserved by regular simulation. Hence, we can focus our attention to the existential (and later universal) fragment of CTL.

Just like for stuttering bisimulation, it is clear that $\simeq_{\text{TS}}^{\text{st}}$ cannot preserve formulae involving the $\bigcirc$ operator. Consider, for example the transition TS:



Then, $s_1 \simeq_{\text{TS}}^{\text{st}} s_2$, but $s_1 \models \exists \bigcirc \neg a$ whereas $s_2 \not\models \exists \bigcirc \neg a$. Similarly, since there is no divergence sensitivity built into the stutter simulation, we cannot preserve formulae involving the release operator. To see this, consider once again the transition system TS. Although $s_1 \models \exists(\text{false } R \neg a)$, we have $s_2 \not\models \exists(\text{false } R \neg a)$.

This leads to the conjecture that the sought logical fragment is $\exists\text{CTL}_{\setminus\{\bigcirc, R\}}$.

From the example transition system, it's clear that in the universal fragment the U operator cannot be preserved, since $s_2 \models \forall(\text{true } U a)$ but $s_1 \not\models \forall(\text{true } U a)$. Consequently, an alternative characterization is $\forall\text{CTL}_{\setminus\{\bigcirc, U\}}$.

c) Take $A = \forall\text{CTL}_{\setminus\{\bigcirc, U\}}$ and assume for all $\Phi \in A$, we have $s_2 \models \Phi$ if and only if $s_1 \models \Phi$.

If $a \in L(s_1)$, then $s_1 \models a$. From the assumption we get $s_2 \models a$ and therefore $a \in L(s_2)$. Likewise, if $a \notin L(s_1)$, then $s_1 \models \neg a$. By the assumption, we have $s_2 \models \neg a$ and therefore $a \notin L(s_2)$. It follows that $L(s_1) = L(s_2)$.