Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen

Christian Hensel, Matthias Volk

Introduction to Model Checking (Summer Term 2018)

— Solution 11 (due 16th July) —

General Remarks

- The exercises are to be solved in groups of *three* students.
- You may hand in your solutions for the exercises just before the exercise class starts at 12:15 or by dropping them into the "Introduction to Model Checking" box at our chair *before 12:00*. Do *not* hand in your solutions via L2P or via e-mail.
- If a task asks you to justify your answer, an explanation of your reasoning is sufficient. If you are required to prove a statement, you need to give a *formal* proof.
- This is the last exercise sheet. If you have gained at least **90.5 points in total** (40% of 226), you are admitted to the exam. If you have gained at least **59 bonus points** (70% of 84), you get a 0.3 bonus on your grade for the exam.

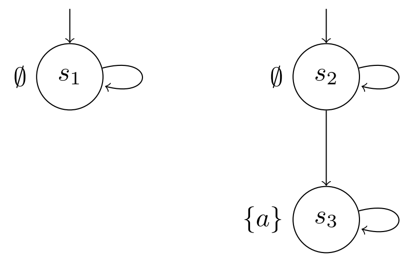
Exercise 1★ (2 + 3 Points)

(a) Give a transition system TS without terminal states that contains two states s_1 and s_2 such that $s_1 \not\equiv_{\mathrm{LTL}} s_2$ and there is *no* LTL formula φ with $s_2 \models \varphi$ and $s_1 \not\models \varphi$.

(b) Let TS_1 and TS_2 be transition systems over AP without terminal states such that $\mathrm{TS}_1 \not\equiv_{\mathrm{CTL}} \mathrm{TS}_2$. Prove or disprove: there exists a CTL formula Φ over AP such that $\mathrm{TS}_1 \models \Phi$ and $\mathrm{TS}_2 \not\models \Phi$.

Solution:

(a) Consider the following states s_1, s_2 in the transition system TS below.



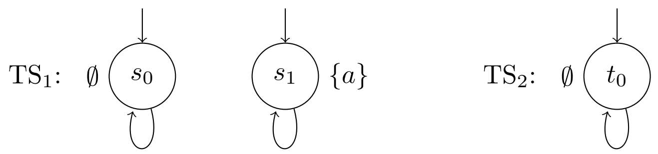
It is $s_1 \not\equiv_{\mathrm{LTL}} s_2$, because for $\psi = \Box\neg a$ we have $s_1 \models \psi$ but $s_2 \not\models \psi$.

We observe that $\mathit{Traces}(s_1) \subseteq \mathit{Traces}(s_2)$ $(*)$. Let φ be an arbitrary LTL formula. Then

$$\begin{aligned} & s_2 \models \varphi \\ \iff & \mathit{Traces}(s_2) \subseteq \mathit{Words}(\varphi) \\ \overset{(*)}{\Longrightarrow} & \mathit{Traces}(s_1) \subseteq \mathit{Words}(\varphi) \\ \Longrightarrow & s_1 \models \varphi \end{aligned}$$

Consequently, there exists no LTL formula φ such that $s_2 \models \varphi$ and $s_1 \not\models \varphi$.

(b) We disprove the claim. Consider the transition systems $\mathrm{TS}_1 = (S_1, \mathrm{Act}_1, \rightarrow_1, S_0^1, \mathrm{AP}, L_1)$ and $\mathrm{TS}_2 = (S_2, \mathrm{Act}_2, \rightarrow_2, S_0^2, \mathrm{AP}, L_2)$ below.



First of all, $\mathrm{TS}_1 \not\equiv_{\mathrm{CTL}} \mathrm{TS}_2$, because $\mathrm{TS}_2 \models \forall\Box\neg a$ and $\mathrm{TS}_1 \not\models \forall\Box\neg a$.
Let Φ be an arbitrary CTL formula. Since $s_0 \sim t_0$, we have $s_0 \models_{\mathrm{CTL}^*} \Phi \iff t_0 \models_{\mathrm{CTL}^*} \Phi$. Then

$$\begin{aligned}
& \mathrm{TS}_1 \models \Phi \\
\iff & \forall s \in S_0^1 \,.\, s \models \Phi \\
\implies & s_0 \models \Phi \\
\overset{s_0 \sim t_0}{\iff} & t_0 \models \Phi \\
\overset{S_0^2 = \{t_0\}}{\iff} & \forall t \in S_0^2 \,.\, t \models \Phi \\
\iff & \mathrm{TS}_2 \models \Phi
\end{aligned}$$

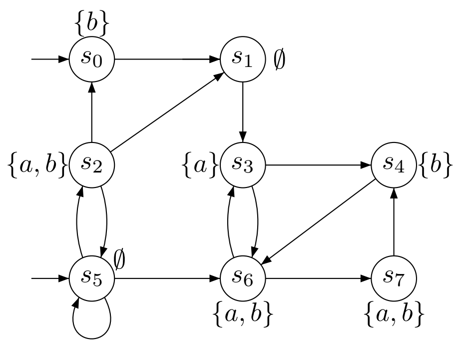
Consequently, there exists no CTL formula Φ such that $\mathrm{TS}_1 \models \Phi$ and $\mathrm{TS}_2 \not\models \Phi$.

Exercise 2 (5 Points)

Consider the CTL*-formula (with derived operators) over $\mathrm{AP} = \{a, b\}$

$$\Phi = \forall\Diamond\Box\exists\bigcirc\left(a \,\mathsf{U}\, \exists\Box b\right)$$

and the transition system TS outlined below:



Apply the CTL* Model Checking algorithm to compute $Sat(\Phi)$ and decide whether $\mathrm{TS} \models \Phi$.
Hint: You may infer the satisfaction sets for LTL formulas directly.

Solution:

We consider the maximal proper state subformulas $Sub(\Phi)$:

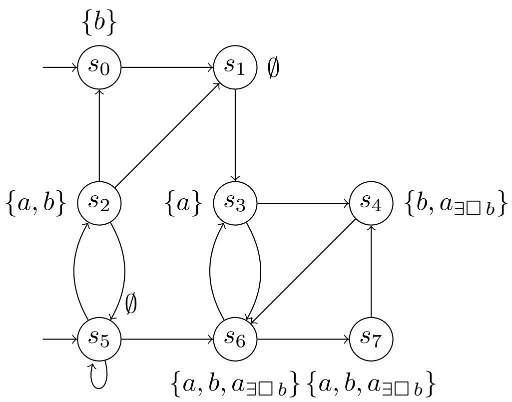
1. $\Psi = a$: $Sat(a) = \{s_2, s_3, s_6, s_7\}$
2. $\Psi = b$: $Sat(b) = \{s_0, s_2, s_4, s_6, s_7\}$
3. $\Psi = \exists\Box b$:
   The following equivalence is used to compute $Sat(\exists\Box b)$:

$$s \models_{\mathrm{CTL}^*} \exists\varphi \quad\iff\quad s \models_{\mathrm{CTL}^*} \neg\forall\neg\varphi \quad\iff\quad s \not\models_{\mathrm{CTL}^*} \forall\neg\varphi \quad\iff\quad s \not\models_{\mathrm{LTL}} \neg\varphi$$

According to the LTL semantics, we have $Sat_{\text{LTL}}(\neg\Box\, b) = Sat_{\text{LTL}}(\Diamond\,\neg b) = \{s_0, s_1, s_2, s_3, s_5\}$. Then, $S \setminus Sat_{\text{LTL}}(\neg\Box\, b) = \{s_4, s_6, s_7\}$ is the satisfaction set $Sat_{\text{CTL}^*}(\exists\Box\, b)$:

$$Sat_{\text{CTL}^*}(\exists\Box\, b) = \{s_4, s_6, s_7\}\,.$$

The labelling is extended by a fresh atomic proposition $a_{\exists\Box\, b}$ according to $Sat_{\text{CTL}^*}(\exists\Box\, b)$. The corresponding subformula $\exists\Box\, b$ of Φ is replaced by $a_{\exists\Box\, b}$.



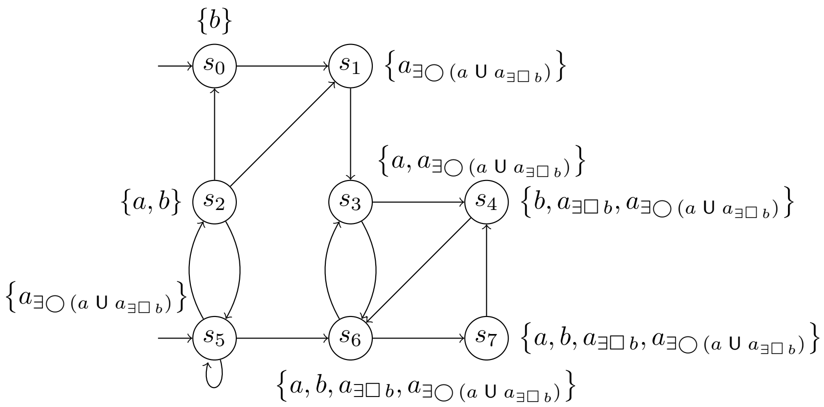
4. $\Psi = \exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})$:
   The above equivalence for existentially quantified path formulas yields:

$$s \models_{\text{CTL}^*} \exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b}) \quad\Longleftrightarrow\quad s \not\models_{\text{LTL}} \neg\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b}).$$

   By the equivalence $\neg\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b}) \equiv \bigcirc\neg(a \,\mathsf{U}\, a_{\exists\Box\, b})$, the satisfaction set of $\neg(a \,\mathsf{U}\, a_{\exists\Box\, b})$ can be inferred:

$$\begin{aligned}
Sat_{\text{LTL}}\big(\neg(a \,\mathsf{U}\, a_{\exists\Box\, b})\big) &= \{s_0, s_1, s_2, s_5\}\\
Sat_{\text{LTL}}\big(\bigcirc\,\neg(a \,\mathsf{U}\, a_{\exists\Box\, b})\big) &= \{s_0, s_2\}\\
Sat_{\text{CTL}^*}\big(\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})\big) &= S \setminus Sat_{\text{LTL}}\big(\bigcirc\,\neg(a \,\mathsf{U}\, a_{\exists\Box\, b})\big)\\
&= S \setminus \{s_0, s_2\}\\
&= \{s_1, s_3, s_4, s_5, s_6, s_7\}
\end{aligned}$$

   The labelling is extended by a new atomic prop. $a_{\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})}$ according to $Sat_{\text{CTL}^*}\big(\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})\big)$. Again, the corresponding subformula Ψ of Φ is replaced by $a_{\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})}$:



5. $\Psi = \forall\Diamond\,\Box\, a_{\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})}$:
   In the case of universal quantification, we can directly apply the LTL–semantics:

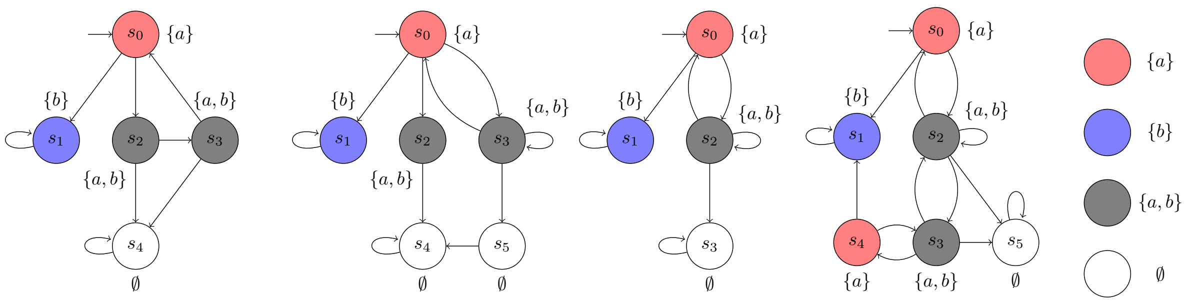
$$Sat_{\text{LTL}}(\Diamond\,\Box\, a_{\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})}) = \{s_0, s_1, s_3, s_4, s_6, s_7\}\,.$$

   Therefore, $Sat(\Phi) = Sat_{\text{CTL}^*}\big(\forall\Diamond\,\Box\, a_{\exists\bigcirc\,(a \,\mathsf{U}\, a_{\exists\Box\, b})}\big) = \{s_0, s_1, s_3, s_4, s_6, s_7\}$.

Because of $s_5 \in S_0$, but $s_5 \notin Sat(\Phi)$, this yields $\text{TS} \not\models_{\text{CTL}^*} \Phi$.

Exercise 3 (2+2 Points)

Consider the following transition systems $\mathrm{TS}_1, \ldots, \mathrm{TS}_4$.



(a) TS_1 (b) TS_2 (c) TS_3 (d) TS_4 (e) legend

(a) Which transition systems are trace equivalent? Justify your answers by either providing the set of traces or a counterexample trace.

(b) Which transition systems are bisimulation equivalent? Justify your answers by either providing a bisimulation relation or a CTL formula that distinguishes the considered transition systems.

Solution:

(a)

- $\mathit{Traces}(\mathrm{TS}_1) \neq \mathit{Traces}(\mathrm{TS}_2), \mathit{Traces}(\mathrm{TS}_3), \mathit{Traces}(\mathrm{TS}_4)$.

  Consider the trace
  $$\pi := \{a\}\,\{a,b\}\,\{a\}\,\{b\}^\omega\,.$$
  It is $\pi \in \mathit{Traces}(\mathrm{TS}_2), \mathit{Traces}(\mathrm{TS}_3), \mathit{Traces}(\mathrm{TS}_4)$ but $\pi \notin \mathit{Traces}(\mathrm{TS}_1)$.

- $\mathit{Traces}(\mathrm{TS}_2) = \mathit{Traces}(\mathrm{TS}_3) = \mathit{Traces}(\mathrm{TS}_4)$.

  The traces are
  $$\mathit{Traces}(\mathrm{TS}_2) := \Big\{ \big(\{a\}\,\{a,b\}^+\big)^*\,\{a\}\,\{b\}^\omega, \big(\{a\}\,\{a,b\}^+\big)^+\emptyset^\omega, \big(\{a\}\,\{a,b\}^+\big)^\omega, \big(\{a\}\,\{a,b\}^+\big)^*\,\{a\}\,\{a,b\}^\omega \Big\}$$

(b)

- $TS_1 \not\sim TS_2, TS_3, TS_4$.

  A distinguishing formula is
  $$\Phi_1 = \exists \bigcirc\, \big(a \wedge b \wedge \exists \bigcirc\, (a \wedge \neg b)\big).$$
  Then $TS_1 \not\models_{CTL} \Phi_1$ but $TS_2, TS_3, TS_4 \models_{CTL} \Phi_1$.

- $TS_2 \not\sim TS_3, TS_4$.

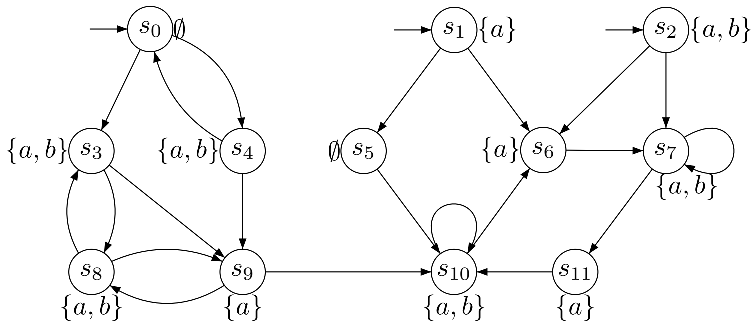
  A distinguishing formula is
  $$\Phi_2 = \exists \bigcirc\, (a \wedge b \wedge \forall \bigcirc\, (\neg a \wedge \neg b)).$$
  Then $TS_2 \models_{CTL} \Phi_2$ but $TS_3, TS_4 \not\models_{CTL} \Phi_2$.

- $TS_3 \sim TS_4$.

  A bisimulation relation $\mathcal{R} \subseteq S_3 \times S_4$ is
  $$\mathcal{R} := \Big\{(s_0,s_0),(s_0,s_4),(s_1,s_1),(s_2,s_2),(s_2,s_3),(s_3,s_5)\Big\}.$$

Exercise 4 (3+3 Points)

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

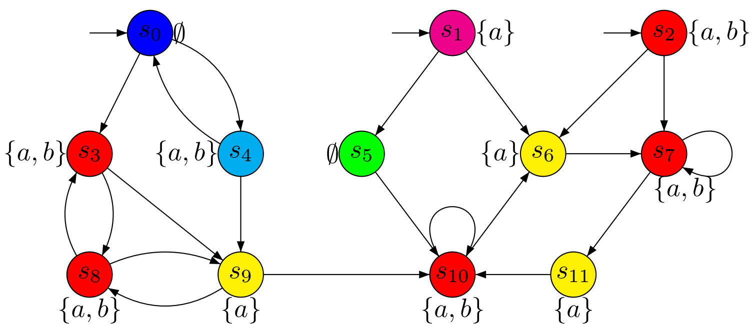


(a) Determine the bisimulation equivalence $\sim_{\text{TS}}$ and depict the bisimulation quotient system TS$/\sim$.

(b) For each bisimulation equivalence class C, provide a CTL formula Φ_C that holds only in the states in C.

Solution:

(a) The bisimulation equivalence classes are depicted in the following (indicated by color):

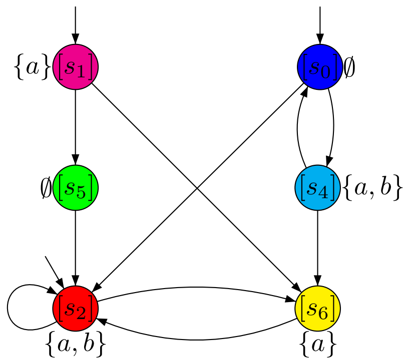


The bisimulation relation $\mathcal{R} \subseteq S \times S$ is given as

$$\begin{aligned}\mathcal{R} := \Big\{&(s_2, s_3), (s_2, s_7), (s_2, s_8), (s_2, s_{10}), (s_3, s_2), (s_3, s_7), (s_3, s_8), (s_3, s_{10}),\\ &(s_7, s_2), (s_7, s_3), (s_7, s_8), (s_7, s_{10}), (s_8, s_2), (s_8, s_3), (s_8, s_7), (s_8, s_{10}),\\ &(s_{10}, s_2), (s_{10}, s_3), (s_{10}, s_7), (s_{10}, s_8),\\ &(s_6, s_9), (s_6, s_{11}), (s_9, s_6), (s_9, s_{11}), (s_{11}, s_6), (s_{11}, s_9)\Big\} \cup \mathcal{I}\end{aligned}$$

where $\mathcal{I} := \{(s, s) \mid s \in S\}$ is the identity relation.

Correspondingly, the bisimulation quotient system TS$/\sim$ can be constructed as follows:



(b) Formulae that characterize the equivalence classes are:

$$\Phi_{[s_0]} = \neg a \wedge \neg b \wedge \exists \bigcirc \exists \bigcirc \neg a \qquad \Phi_{[s_5]} = \neg a \wedge \neg b \wedge (\forall \bigcirc \forall \bigcirc a)$$
$$\Phi_{[s_1]} = a \wedge \neg b \wedge \exists \bigcirc (\neg a \wedge \neg b) \qquad \Phi_{[s_6]} = a \wedge \neg b \wedge \forall \bigcirc (a \wedge b)$$
$$\Phi_{[s_4]} = a \wedge b \wedge \exists \bigcirc (\neg a \wedge \neg b) \qquad \Phi_{[s_2]} = a \wedge b \wedge \forall \bigcirc a$$