Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen
Christian Hensel, Matthias Volk

# Introduction to Model Checking (Summer Term 2018)

# — Exercise Sheet 10 (due 9th July) —

## General Remarks

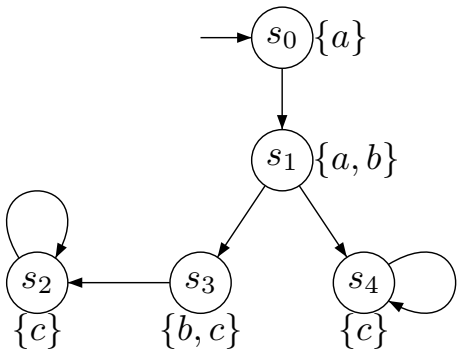
- The exercises are to be solved in groups of *three* students.
- You may hand in your solutions for the exercises just before the exercise class starts at 12:15 or by dropping them into the "Introduction to Model Checking" box at our chair *before 12:00*. Do *not* hand in your solutions via L2P or via 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.

## Exercise 1 (6 Points)

Consider the following CTL-formulae

$$\Phi_1 = \exists\Diamond\forall\Box\, c \quad \text{and} \quad \Phi_2 = \forall(a \,\mathsf{U}\, \forall\Diamond\, c)$$

and the transition system outlined on the right. Decide whether $TS \models \Phi_i$ for $i = 1, 2$ using the CTL model checking algorithm from the lecture. Do not forget to translate to existential normal form and compute the satisfaction sets for subformulae.



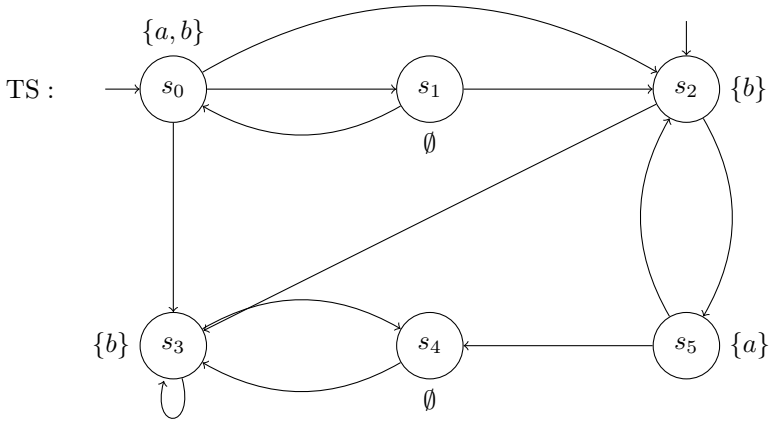

## Exercise 2★ (3+2+3 Points)

Consider the following CTL formula $\Phi$ and the fairness assumption *sfair*:

$$\Phi = \forall\Box\forall\Diamond\, a$$

$$\mathit{sfair} = \Box\Diamond \underbrace{(b \wedge \neg a)}_{\Phi_1} \rightarrow \Box\Diamond \underbrace{\exists\Big(b \,\mathsf{U}\, (a \wedge \neg b)\Big)}_{\Psi_1}$$

and transition system TS over AP $= \{a, b\}$ which is given below.




Here, we abstract from the actions in TS as they are not relevant to the task.

(a) Determine $Sat(\Phi_1)$ and $Sat(\Psi_1)$ (without fairness). Justify your answer.

(b) Determine $Sat_{sfair}(\exists\Box\, true)$. Justify your answer.

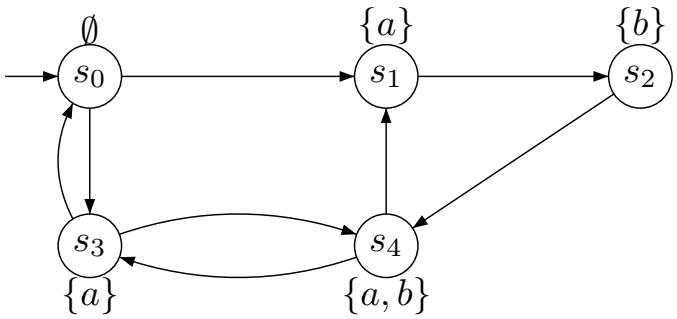
(c) Determine $Sat_{sfair}(\Phi)$. Justify your answer.

## Exercise 3 (6 Points)

Consider the CTL-formula $\Phi = \forall\Box\left(a \rightarrow \forall\Diamond\,(b \wedge \neg a)\right)$ together with the following CTL fairness assumption

$$fair = \Box\Diamond\forall\bigcirc\,(a \wedge \neg b) \rightarrow \Box\Diamond\forall\bigcirc\,(b \wedge \neg a)$$
$$\wedge\,\Diamond\Box\exists\Diamond\, b \rightarrow \Box\Diamond\, b.$$

Check whether $TS \models_{fair} \Phi$ for the transition system TS below.




## Exercise 4 ($5^* + 3^*$ Points)

***This exercise does not count towards the total number of points that you can achieve. Not solving it does not decrease the percentage of points you achieved while solving it may increase it.**

Consider the fragment ECTL of CTL which consists of formulae built according to the following grammar:

$$\Phi ::= a \mid \neg a \mid \Phi \wedge \Phi \mid \exists\varphi$$
$$\varphi ::= \bigcirc\Phi \mid \Box\Phi \mid \Phi\ \mathsf{U}\ \Phi$$

ECTL-formulae are built by atomic propositions, negated atomic propositions, the Boolean connective $\wedge$ and the path quantifier $\exists$ together with the modalities $\bigcirc, \Box$ and $\mathsf{U}$. In particular, negation may only appear in front of atomic propositions.

For two transition systems $TS_1 = (S_1, Act, \rightarrow_1, I_1, AP, L_1)$ and $TS_2 = (S_2, Act, \rightarrow_2, I_2, AP, L_2)$, we define $TS_1 \subseteq TS_2$ iff $S_1 \subseteq S_2$, $\rightarrow_1 \subseteq \rightarrow_2$, $I_1 = I_2$ and $L_1(s) = L_2(s)$ for all $s \in S_1$.

(a) Prove by structural induction on the structure of the formula that for all ECTL-formulae $\Phi$ and all transition systems $TS_1$, $TS_2$ with $TS_1 \subseteq TS_2$, it holds:

$$TS_1 \models \Phi \quad \Longrightarrow \quad TS_2 \models \Phi.$$

*Hint:* You may gain one additional point by showing that the statement does not hold if the definition of $\mathrm{TS}_1 \subseteq \mathrm{TS}_2$ required only $I_1 \subseteq I_2$ instead of $I_1 = I_2$.

(b) Formally prove that there exists a CTL formula $\Phi_1$ for which no equivalent ECTL formula $\Phi_2$ exists.