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

Sebastian Junges, Lutz Klinkenberg

Model Checking
(Winter Term 2019/2020)

— Exercise Sheet 1 (due October 25th) —

General Remarks

- The exercises are to be solved in groups of *three* students. For sheet one, it is acceptable to form groups of two, but for the remaining sheets, we require you to form groups of three. You may use the moodle forum to search for group members.
- You may hand in your solutions for the exercises just before the exercise class starts at 10:30 or by dropping them into the "Introduction to Model Checking" box at our chair *before 10:20*. Do *not* hand in your solutions via moodle or via e-mail.
- The solution for the first exercise sheet will be presented in the first exercise class on October 25th.
- Unlike previous years, everybody who registered for the exam will be admitted. The exercise sheets are hence not mandatory anymore but highly recommended. The ***marked**** *exercises* are very similar to exam questions.

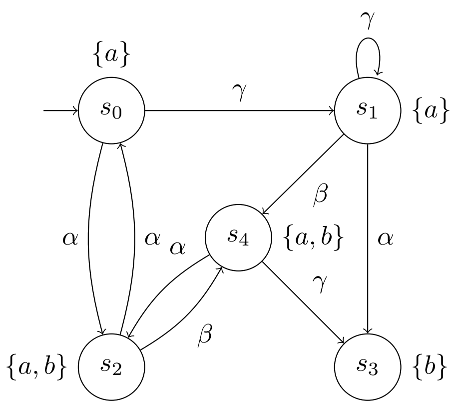
Exercise 1

We call a transition system $\mathrm{TS} = (S, \mathrm{Act}, \rightarrow, I, \mathrm{AP}, L)$

- *action-deterministic* if $|\, I \,| \leq 1$ and $|\, \mathrm{Post}(s, \alpha) \,| \leq 1$ for all $s \in S$ and $\alpha \in \mathrm{Act}$, and
- *AP-deterministic* if $|\, I \,| \leq 1$ and $|\mathrm{Post}(s) \cap \{s' \in S \mid L(s') = A\}\,| \leq 1$ for all $s \in S$ and $A \in 2^{\mathrm{AP}}$,

where $\mathrm{Post}(s, \alpha) = \{s' \in S \mid \exists (s, \alpha, s') \in \rightarrow\}$ and $\mathrm{Post}(s) = \bigcup_{\alpha \in \mathrm{Act}} \mathrm{Post}(s, \alpha)$.

Let the transition system TS_1 be as follows.



(a) Give the formal definition of TS_1.

(b) Specify a finite and an infinite execution of TS_1.

(c) Decide whether TS_1 is (i) *AP*-deterministic, and/or (ii) action-deterministic. Justify your answer.

Exercise 2★

In the lecture we have seen techniques in order to deal with interleavng. A different approach to deal with interleaving is the parallel composition of transition systems via *handshaking*. The handshaking composition of two transition systems is defined as follows:

Let $TS_i = (S_i, \mathrm{Act}_i, \rightarrow_i, I_i, \mathrm{AP}_i, L_i),\ i = 1, 2$ and $H \subseteq \mathrm{Act}_1 \cap \mathrm{Act}_2$.

$$TS_1 \parallel_H TS_2 := (S_1 \times S_2, \mathrm{Act}_1 \cup \mathrm{Act}_2, \rightarrow, I_1 \times I_2, \mathrm{AP}_1 \uplus \mathrm{AP}_2, L)$$

where $L(\langle s_1, s_2\rangle) = L_1(s_1) \cup L_2(s_2)$ and with $\rightarrow$ defined by:

$$\frac{s_1 \xrightarrow{\alpha}_1 s_1'}{\langle s_1, s_2\rangle \xrightarrow{\alpha} \langle s_1', s_2\rangle} \qquad \frac{s_2 \xrightarrow{\alpha}_2 s_2'}{\langle s_1, s_2\rangle \xrightarrow{\alpha} \langle s_1, s_2'\rangle} \qquad \text{interleaving for } \alpha \notin H$$

$$\frac{s_1 \xrightarrow{\alpha}_1 s_1' \quad \wedge \quad s_2 \xrightarrow{\alpha}_2 s_2'}{\langle s_1, s_2\rangle \xrightarrow{\alpha} \langle s_1', s_2'\rangle} \qquad \text{handshaking for } \alpha \in H.$$

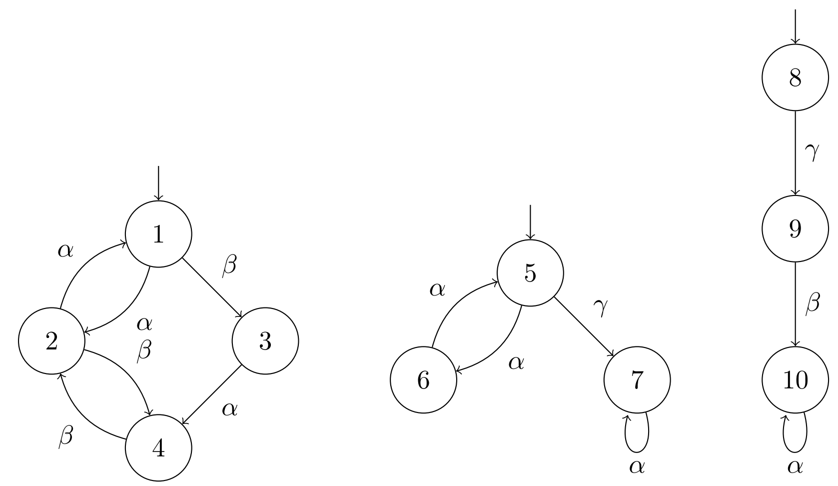
In all following tasks, whenever transition systems are compared via $=$ or $\neq$, this means (in)equality **up to isomorphism**.

(a) Show that the handshaking $\parallel_H$ operator **is not** associative, i.e. that in general

$$(\mathrm{TS}_1 \parallel_H \mathrm{TS}_2) \parallel_{H'} \mathrm{TS}_3 \neq \mathrm{TS}_1 \parallel_H (\mathrm{TS}_2 \parallel_{H'} \mathrm{TS}_3)$$

(b) The handshaking operator $\parallel := \parallel_H$ for $H = \mathrm{Act}_1 \cap \mathrm{Act}_2$, that forces transition systems to synchronize over *all* common actions **is** associative. Consider the following three transition systems:

TS_1 : TS_2 : TS_3 :



Build the composition $(\mathrm{TS}_1 \parallel \mathrm{TS}_2) \parallel \mathrm{TS}_3$.

(c) Show that for arbitrary transition systems $\mathrm{TS}_i = (S_i, \mathrm{Act}_i, \rightarrow_i, S_0^i, \mathrm{AP}_i, L_i)$ for $i \in \{1, 2, 3\}$, it is

$$\underbrace{(\mathrm{TS}_1 \parallel \mathrm{TS}_2) \parallel \mathrm{TS}_3}_{L} = \underbrace{\mathrm{TS}_1 \parallel (\mathrm{TS}_2 \parallel \mathrm{TS}_3)}_{R}.$$

To this end, show that the bijective function $f_\approx \colon ((S_1 \times S_2) \times S_3) \rightarrow (S_1 \times (S_2 \times S_3))$ given by $f_\approx(\langle\langle s_1, s_2\rangle, s_3\rangle) = \langle s_1, \langle s_2, s_3\rangle\rangle$ preserves the transition relation in the sense that for all $\alpha \in \mathrm{Act}_1 \cup \mathrm{Act}_2 \cup \mathrm{Act}_3$ we have

$$\ell \xrightarrow{\alpha}_L \ell' \iff f_\approx(\ell) \xrightarrow{\alpha}_R f_\approx(\ell') \tag{1.1}$$

where $\ell, \ell' \in S_L$, S_L is the state space of transition system L and $\longrightarrow_L$, $\longrightarrow_R$ are the transition relations of L and R, respectively.

Hint: When considering an action α, you need only distinguish the cases

(i) $\alpha \in \text{Act}_1 \setminus (\text{Act}_2 \cup \text{Act}_3)$

(ii) $\alpha \in (\text{Act}_1 \cap \text{Act}_2) \setminus \text{Act}_3$

(iii) $\alpha \in \text{Act}_1 \cap \text{Act}_2 \cap \text{Act}_3$

as all other cases are symmetric. Also, for simplicity, it suffices to show the direction "$\Longrightarrow$" of condition (1.1). However, keep in mind that L and R are not necessarily action-deterministic.

Exercise 3

In the following we show that LT properties are not solely a theoretical concept but have a wide range of practical applications. As proof, we apply the concept of LT properties to movie/TV series quotes.

(a) We assume each following quote informally describes some property. Formulate these properties as LT properties over the given set AP of atomic propositions:

(i) "**Winter is coming.**"
$\text{AP} = \{winter\}$.
$winter$ will eventually by reached.

(ii) "**Everything is awesome.**"
$\text{AP} = \{awesome\}$.
$awesome$ always holds.

(iii) "**I'll be back.**"
$\text{AP} = \{here\}$.
I am currently $here$ but at some point I will not be $here$. However, I will be $here$ again at a later time.

(iv) "**You either die as a hero, or you live long enough to see yourself become the villain.**"
$\text{AP} = \{live, hero\}$.
In the beginning, you $live$ and are a $hero$. You either cease to $live$ and die, still being a $hero$, or you $live$ but become the villain, i.e., you are not a $hero$ anymore.

(v) "**By night one way, by day another**
Thus shall be the norm
Till you receive true love's kiss
then, take love's true form."
$\text{AP} = \{day, form_1, form_2, true\_form, kiss\}$.
You start by having $form_1$ at night, i.e., not day. You alternate between $form_1$ at night and $form_2$ by day. This alternation goes on till at some point you receive true love's $kiss$ and from there on have love's $true\_form$.

(vi) "**A Lannister always pays his debts.**"
$\text{AP} = \{in\_debt\}$.
Whenever a Lannister is in_debt, he will be in_debt as long as he has not payed back his debt. If he has payed back his debt, he is no longer in_debt. A Lannister can be in_debt arbitrarily (but finitely) many times.

(vii) "**Anything is possible [if you just believe].**"
$\text{AP} = \{ap_1, \ldots, ap_n\}$.
We don't consider the second part and just concentrate on the fact, that everything is possible.

(viii) "**It's gonna be legen... wait for it... dary!**"
$\text{AP} = \{legen, wait\_for\_it, dary\}$.
In the beginning it is $legen$, then we have to $wait\_for\_it$ for some time, and then it is $dary$ at some point.

(b) Determine for all LT properties of (a) whether they are

(i) safety properties *and/or*

(ii) liveness properties.

Justify your answers.