Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen, Tim Quatmann

Alexander Bork, Jip Spel

Exercise Sheet 1

Hints:

- The exercise sheet can be submitted until 20.04.2022 at 16:30 online via RWTHmoodle.
- The exercise sheets have to be solved in groups of 3-4. Submissions with other group sizes might not be corrected. Use the forum in RWTHmoodle to find group-mates.
- Submissions will be graded only for the sake of giving feedback to you. The points are not a precondition for admittance to the exam.
- However, we strongly advice you to solve the exercises and submit your solutions.
- Sample solutions will be presented in the exercise class and published in RWTHmoodle.
- Questions can be asked either during the lecture or exercise class or in the general discussion board on RWTHmoodle.

Exercise 1 (Opening a Bank Account): 10 Points

Together with a friend you are asked to design a system for a bank. One of the things this system should allow, is to let people open a bank account. The minimum balance is 0 Euros, so the bank does not allow for negative balances. Furthermore, for security reasons, the bank wants accounts to hold less than 10.000 Euros. You start with the following method.

Algorithm 1 Opening a bank account

```
if deposit >= 0 and deposit < 10.000 then
    do something with the deposit
else
    throw error
```

Your friend suggests to test this method on the following initial inputs: -1, 0, 500, 9.999, and 10.000. You have to convince him that model checking is the better thing to do. To do so, provide a scenario in which the testing is not sufficient.

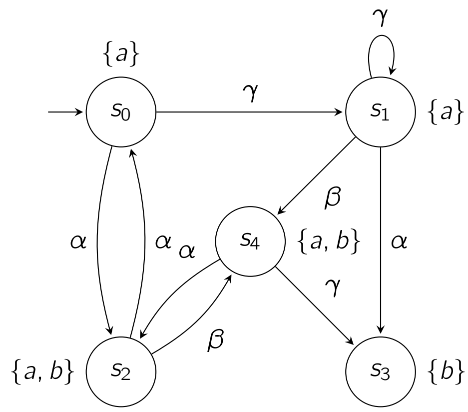
Hint: It is sufficient to describe this scenario in words.

Exercise 2 (Transition Systems): 6+3+6+6+3+6=30 Points

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.

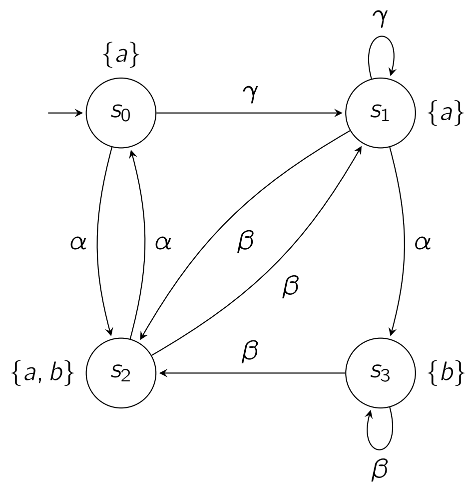


a) Give the formal definition of TS_1.

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.

Let the transition system TS_2 be as follows.



d) Give the formal definition of TS_2.

e) Specify a path π of TS_2, and provide the corresponding *trace*(π).

f) Decide whether TS_2 is (i) *AP*-deterministic, and/or (ii) action-deterministic. Justify your answer.

Exercise 3 (Program Graphs): 8+10+7=25 Points

a) Draw the two program graphs PG_1 and PG_2 for the following programs **1** and **2** over the (shared) integer variables x and y. Use exactly two locations for PG_1 and exactly two locations for PG_2.

1:

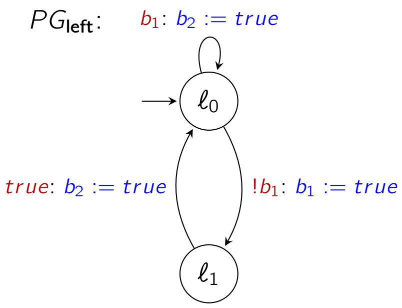
```
while (true) do
    if (y > 0) then
        y := y - 1
    x := x − y
```

2:

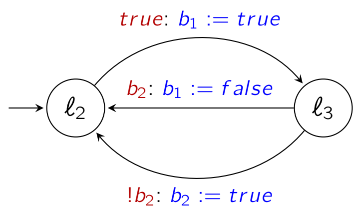
```
while (true) do
    x := x − 1
    if (x < 0) then
        x := 1 − x
    else
        x := x − 1
```

b) Draw the interleaving $PG_{\text{Left}} \,|||\, PG_{\text{right}}$ for the following two program graphs.

PG_{left}:



PG_{right}:



c) Draw the reachable part of the transition system $TS(PG_{\text{Left}} \,|||\, PG_{\text{right}})$ of the program graph from **c)**. *Assume the initial condition* $b1 \wedge b2$.

Exercise 4 (Handshaking): 10+5+20=35 Points

In the lecture we have seen techniques in order to deal with interleaving. 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 $H \subseteq \mathrm{Act}_1 \cap \mathrm{Act}_2$.

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

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

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

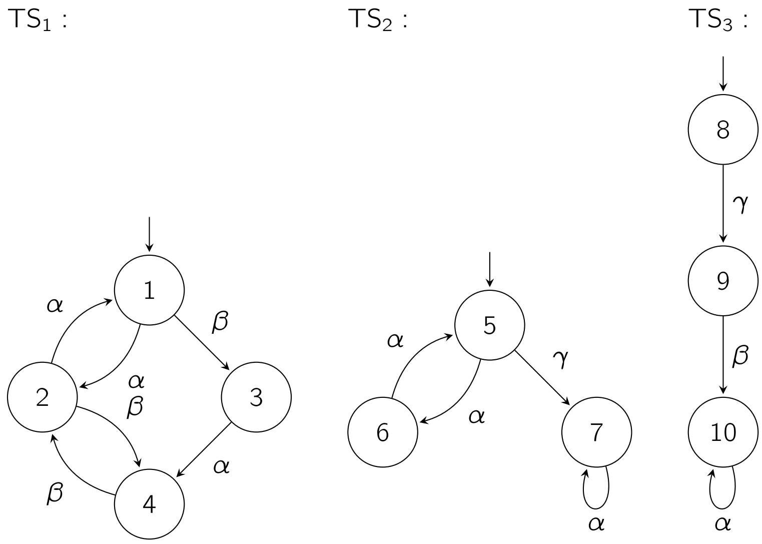
$$\frac{s_1 \xrightarrow{\alpha}_1 s_1' \quad \wedge \quad s_2 \xrightarrow{\alpha}_2 s_2'}{\langle s_1, s_2\rangle \xrightarrow{\alpha} \langle s_1', s_2'\rangle} \qquad \text{handshaking for } \alpha \in H.$$

We also define the handshaking operator $\| := \|_H$ for $H = \mathrm{Act}_1 \cap \mathrm{Act}_2$, that forces transition systems to synchronize over *all* common actions.
In all following tasks, whenever transition systems are compared via $=$ or $\neq$, this means (in)equality **up to isomorphism**.

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

$$(\mathrm{TS}_1 \,\|_H\, \mathrm{TS}_2) \,\|_{H'}\, \mathrm{TS}_3 \neq \mathrm{TS}_1 \,\|_H\, (\mathrm{TS}_2 \,\|_{H'}\, \mathrm{TS}_3)$$

b) Consider the following three transition systems:



Build the composition $(\mathsf{TS}_1 \parallel \mathsf{TS}_2) \parallel \mathsf{TS}_3$. Show intermediate steps. You can use that the $\parallel$ operator is associative which will be shown in exercise **c)**.

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

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

To this end, show that the bijective function $f_{\approx} \colon ((S_1 \times S_2) \times S_3) \to (S_1 \times (S_2 \times S_3))$ 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 $\alpha \in \mathsf{Act}_1 \cup \mathsf{Act}_2 \cup \mathsf{Act}_3$ we have

$$\ell \xrightarrow{\alpha}_L \ell' \iff f_{\approx}(\ell) \xrightarrow{\alpha}_R f_{\approx}(\ell') \tag{1}$$

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 only need to distinguish the cases

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

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

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

as all other cases are symmetric. Also, for simplicity, it suffices to show the direction "$\Longrightarrow$" of condition (1). However, keep in mind that L and R are not necessarily action-deterministic.