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

Introduction to Model Checking (Summer Term 2018)

— Exercise Sheet 2 (due 7th May) —

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.

Exercise 1 (2 + 5 + 1 Points)

Whenever transition systems are compared via $=$ or $\neq$, this means (in)equality **up to renaming of states** (i.e. isomorphism).

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

$$(\mathrm{TS}_1 \parallel_H TS_2) \parallel_{H'} \mathrm{TS}_3 \neq \mathrm{TS}_1 \parallel_H (\mathrm{TS}_2 \parallel_{H'} \mathrm{TS}_3)$$

(b) The handshaking operator $\|$ that forces transition systems to synchronize over *all* common actions **is** associative. Show that

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

where $\mathrm{TS}_1, \mathrm{TS}_2, \mathrm{TS}_3$ are arbitrary (finite) transition systems. 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

$$l \xrightarrow{\alpha}_L l' \iff f_{\approx}(l) \xrightarrow{\alpha}_R f_{\approx}(l') \tag{2.1}$$

where $l, l' \in S_L$, 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) $\alpha \in \mathrm{Act}_1 \backslash (Act_2 \cup Act_3)$

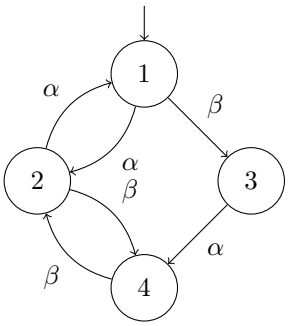
(ii) $\alpha \in (\mathrm{Act}_1 \cap \mathrm{Act}_2) \backslash Act_3$

(iii) $\alpha \in \mathrm{Act}_1 \cap Act_2 \cap Act_3$

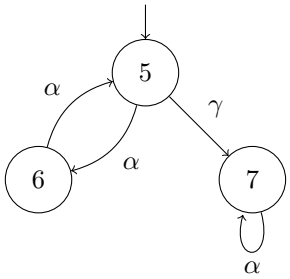
(Act_i is the action set of TS_i) as all other cases are symmetric. Also, for simplicity, it suffices to show the direction "$\Longrightarrow$" of condition (2.1). However, keep in mind that L and R are not necessarily action-deterministic (see exercise sheet 1).

(c) Consider the following three transition systems:

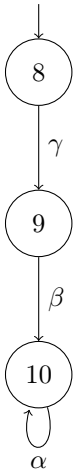
TS_1 :



TS_2 :



TS_3 :



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

Exercise 2 (2 + 5 Points)

(a) In the lecture, channel systems using FIFO (or queue) channels were introduced. We now consider LIFO (or stack) channels. Formally define the SOS rules for the communication such that in the induced transition system the channels have LIFO semantics.

(b) Consider the following decision problem.

Input: A LIFO channel system $[\mathcal{P}_1 \mid \ldots \mid \mathcal{P}_n]$ with program graphs

$$\mathcal{P}_i = (\mathrm{Loc}_i, \mathrm{Act}_i, \mathrm{Effect}_i, \hookrightarrow_i, \mathrm{Loc}_0^i, g_0^i)$$

over $(\mathrm{Var}, \mathrm{Chan})$ and a set $F \subseteq \mathrm{Loc}_1 \times \ldots \mathrm{Loc}_n \times \mathrm{Eval}(\mathrm{Var}) \times \mathrm{Eval}(\mathrm{Chan})$.
Question: Is some state of F reachable in $\mathrm{TS}([\mathcal{P}_1 \mid \ldots \mid \mathcal{P}_n])$?

Prove that this problem is undecidable. For this, reduce the halting problem for (nondeterministic) Turing machines started on an empty tape to the above problem.

Exercise 3★ (1 + 3 + 1 Points)

We consider the problem of the *dining philosophers*. There are n philosophers sitting around a table and one fork is placed in-between any two philosophers sitting next to each other. The philosophers alternate between thinking and eating. Whenever a philosopher wants to eat, she first has to pick up her left and her right fork (in arbitrary order). After having finished eating, she puts both forks back on the table.

(a) Model the dining philosophers as a channel system $\mathcal{C}$.

Hint: Model each fork as a separate channel.

(b) Construct the transition system $\mathrm{TS}(\mathcal{C})$ for the channel system $\mathcal{C}$ defined in (a) for $n = 3$ philosophers. For simplification, you may assume that each philosopher first picks up her left fork and then her right fork. This order is also preserved when placing the forks on the table again. Furthermore, you may assume that each channel initially contains a fixed number of messages. Finally, you can exploit symmetries when constructing the transition system and merge symmetric states. If you do, briefly justify your approach.

(c) Does the transition system of (b) contain a deadlock?