RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL FÜR INFORMATIK 2
RWTH Aachen · D-52056 Aachen · GERMANY
http://www-i2.informatik.rwth-aachen.de/

Prof. Dr. Ir. J.-P. Katoen
F. Gretz & K. v. d. Pol

Introduction to Model Checking
Winter term 2013/2014

– Series 2 –

Hand in on November 6th before the exercise class or in the box in front of the chair's secretary's office.

Exercise 1 (3 points)

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

$$(\mathrm{T}_1 \|_H T_2) \|_{H'} \mathrm{T}_3 \neq \mathrm{T}_1 \|_H (\mathrm{T}_2 \|_{H'} \mathrm{T}_3)$$

b) Show that the handshaking operator $\|$ that forces transition systems to synchronize over their common actions **is** associative. That is, show that

$$(\mathrm{T}_1 \| \mathrm{T}_2) \| \mathrm{T}_3 \quad = \quad \mathrm{T}_1 \| (\mathrm{T}_2 \| \mathrm{T}_3)$$

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

Hint: One approach to prove the above statement is to show that the transition system on the left hand side is isomorphic to the transition system on the right hand side of the equation. For this observe that the state space of both systems is $S_1 \times S_2 \times S_3$ (even though not necessarily all states are reachable). You can define a mapping that relates those states of the two transition systems that are equal componentwise, i.e. $\langle\langle s_1, s_2\rangle, s_3\rangle \approx \langle s_1, \langle s_2, s_3\rangle\rangle$. From here argue why this mapping is a bijection and why it preserves the transition relation. *When you argue about a transition with some action α you need to make a case distinction:*

1.) $\alpha \in Act_1 \backslash (Act_2 \cup Act_3)$
2.) $\alpha \in (Act_1 \cap Act_2) \backslash Act_3$
3.) $\alpha \in Act_1 \cap Act_2 \cap Act_3$

You may dismiss all other cases because they are symmetric. Also keep in mind that a state can have several successors for one action.

Exercise 2 (3 points)

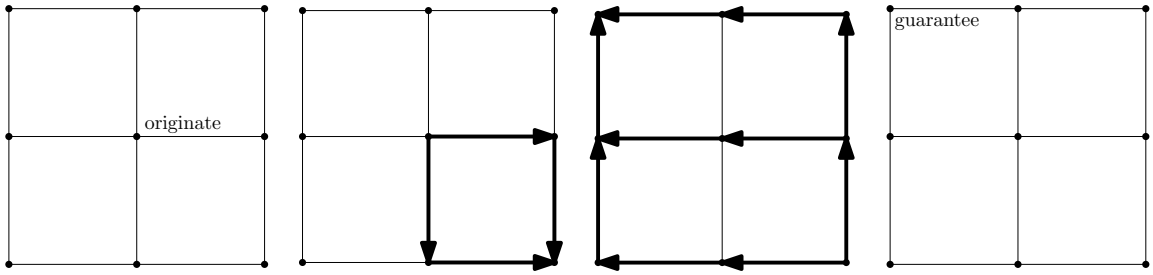
In channel systems, values can be transferred from one process to another process. According to the lecture, the set of transitions of a program graph $PG = (\mathsf{Loc}, \mathsf{Act}, \mathsf{Effect}, \rightarrow, \mathsf{Loc}_0, g_0)$ over $(\mathsf{Var}, \mathsf{Chan})$ is defined as

$$\rightarrow \subseteq \mathsf{Loc} \times (Cond(Var) \times \mathsf{Act}) \times \mathsf{Loc} \quad \cup \quad \mathsf{Loc} \times \mathsf{Comm} \times \mathsf{Loc}$$

where $\mathsf{Comm} = \{c!v, c?x \mid c \in \mathsf{Chan}, v \in \mathsf{dom}(c), x \in \mathsf{Var} \text{ with } \mathsf{dom}(x) \supseteq \mathsf{dom}(c)\}$.
Here we consider two extensions to this definition. Give a formal definition of the transition system semantics of a channel system $CS = [PG_1 | \cdots | PG_n]$ where

a) In asynchronous communication a channel shall always accept a sent value. If the channel is full it will simply drop the oldest element from its FIFO queue.

b) In synchronous message passing a channel may broadcast a value. That is, if several processes are willing to receive a value from a channel they will all receive it (instead of only one of them).



(a) The originator performs the "originate" action.

(b) The message is forwarded down and to the right. The bottom right node starts forwarding after receiving the message from above *or* the left.

(c) The message is forwarded to the left within the rows. The left border only forwards after receiving the message from below *and* the right.

(d) The upper left node performs the "guarantee" action.

Figure 1: The broadcast protocol on a 3×3 grid with the interior node as originator.

Exercise 3 (4 points)

Consider the broadcasting protocol below, on an $n \times m$ grid of processes. Broadcasting protocols are used to deliver a message to every node in a network and provide some guarantee that the message has indeed reached every node.

Assume exactly one process is the originator of the message, to be delivered to every node.

- The originator performs the "originate" action.
- The originator sends its message down and to the right (if these neighbors exist).
- All nodes will, after receiving a message from above or from the left, send it down and to the right (if these neighbors exist).
- The lower right corner of the grid will, upon receiveiving the message, or immediately if it is the originator, send the message up and to the left.
- All nodes on the right border will do the same (if these neighbors exist).
- All nodes on the left border will, after receiving *both* a message from below (if this neighbor exists) and from the right, send the message up (if this neighbor exists).
- All other nodes will, after receiving the message from the right, send it to the left.
- The top left node will, after receiving both a message from below and from the right, perform the "guarantee" action.

The protocol is visualized for a 3×3 grid in Figure 1.

a) Model the broadcasting protocol for an $n \times m$ grid as a channel system.

b) Argue why the message has indeed been delivered to every node in the grid when the "guarantee" action occurs.