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 & F. Sher

Introduction to Model Checking
Winter term 2011/2012

– Series 2 –

Hand in on November 2nd before the exercise class.

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 transition systems.

Exercise 2 **(4 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:

- The transitions modelling communication between processes (labeled by $c!v$ and $c?x$) should be guarded.
- Additionally, we do not want to confine ourselves to transferring values. Therefore we extend our definition s.t. we can transfer expressions.

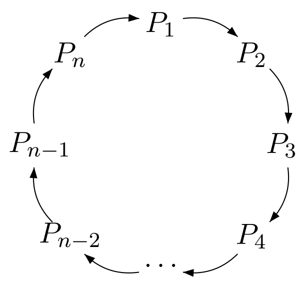
(a) Give a formal definition of the transition system semantics of a channel system $CS = [PG_1|\cdots|PG_n]$ with guarded transitions of the form

$$l \xrightarrow{g:c!v} l' \qquad \text{and} \qquad l \xrightarrow{g:c?x} l'.$$

(b) Now, extend your definition from part (a) in order to transfer expressions (instead of values) by transitions of the form $l \xrightarrow{g:c!ex} l'$. For simplicity, we assume that the type of the expression always corresponds to the domain of the channel.
Hint: To refer to the actual value of an expression ex, you may use the notation $\eta(ex)$.

Exercise 3 **(4 points)**

Consider the following leader election algorithm: For $n \in \mathbb{N}$, n processes $P_1, \ldots, P_n$ are located in a ring topology where each process is connected by an unidirectional channel to its neighbour as outlined on the right.
To distinguish the processes, each process is assigned a unique identifier $id \in \{1, \ldots, n\}$. The aim is to elect the process with the highest identifier as the leader within the ring. Therefore each process executes the following algorithm:




```
send (id);                         initially set to process' id
while (true) do
    receive (m);
    if (m == id) then stop;        process is the leader
    if (m > id) then send (m);     forward identifier
od
```

a) Model the leader election protocol for n processes as a channel system.

b) Give an initial execution fragment of $TS([P_1|P_2|P_3])$ such that at least one process has executed the send-statement within the body of the while-loop.
Assume for $1 \leq i \leq 3$, that process P_i has identifier $id_i = i$.