RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

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

Prof. Dr. Ir. J.-P. Katoen
M. Neuhäußer

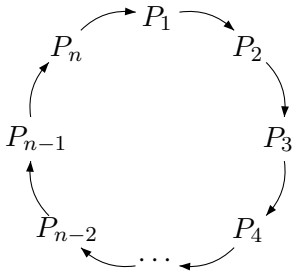
Introduction to Model Checking
Winter term 08/09

– Series 2 –

Hand in on November 7 before the exercise class.

Exercise 1 (2 + 2 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 $id_i = i$.

Exercise 2 (1 + 1 + 2 points)

Consider a system consisting of n processes $P_0, \ldots, P_{n-1}$ and a central moderator M in a fully connected network. Each process P_i (for $0 \leq i < n$) executes the same algorithm and stores a unique identifier $\mathrm{id}_i \in \mathbb{N}$. Further, we assume that n is known a priori.

In order to elect a leader, the system is supposed to determine the process with the highest id and communicate it to every process.

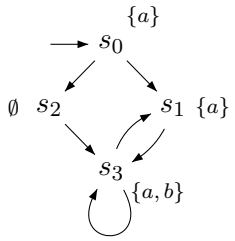
a) Informally describe how to solve the leader election problem in the above setting.

b) Write nanoPromela programs for the algorithm of the process and the moderator. Add comments!

c) Formally derive the program graphs for a process and the moderator.

Exercise 3 (1 points)

Consider the transition system given below. Formally define its traces!



Exercise 4 (3 + 2 points)

A bank uses a non-terminating program that monitors the balance (ab) of all its customers' accounts once per week. The account balances of interest are characterized by the set of atomic propositions

$$AP = \{ab < 0, ab = 0, ab > 100\}\,.$$

a) Express the following informally stated properties as LT-properties:

- an account with positive balance is opened
- the balance is negative only finitely many times
- the balance alternates between debit and credit
- eventually, the account remains with more than 100 € credit
- any debit that occurs is balanced within two weeks
- false and true

b) Determine for each LT-property whether it is a safety property or a liveness property. Justify your answer!