Introduction to specification and verification, exercise 1,

November 10, 2011

1. Design a data structure for transition systems. Describe the structure using diagrams and natural language. Then implement the structure using Java or C.

2. Design an algorithm which finds cycles in transition systems. The input for the algorithm consists of a transition system $P$, an action $a$ and one of its states $s$. The algorithm returns true, if there is a cycle of $a$ transitions starting from $s$.

3. Suppose that the channel in the AB protocol is two-way (so messages can travel in both directions). Moreover, messages may disappear, duplicate and the order of the messages in the channel may change. The channel may contain several messages at the same time. Show, with the help of a scenario, that the AB protocol does not work correctly with this kind of a channel.

Assume next that the channel is as before but the order of the messages does not change in the channel. Is the AB protocol working now properly? If not, give a scenario. If it works, give reasons.

4. In our AB protocol, the timer may timeout too early without waiting for acknowledgements. Modify the description of the AB protocol without channels so that only the lost acknowledgements cause the timer to timeout.

5. Draw the global state graph of your modified AB protocol. Using the global state graph, can you deduce that the modified version is correct?

6. Stenning’s protocol works similarly as the AB protocol, but it tags integers to messages. Thus $d_0$ is sent. When the acknowledgement has come, $d_1$ is sent, then $d_2$ etc. The tag increases by one with every new message and there is no bound for tags.

   a) Give reasons that Stenning’s protocol tolerates more channel mistakes than the AB protocol.

   b) Is it possible to describe or approximate Stenning’s protocol with the help of transition systems? How would you extend the transition system formalism in order to be able to describe the protocols like Stenning’s?