Course: Formal Methods
Assignments

Prof: Roberto Sebastiani
TA: Silvia Tomasi

Academic Year 20010-2011

1 Clayton Tunnel Protocol with SPIN

Description Consider a protocol for a railway tunnel having a single one-way track. There are two signalmen A and B at each end of the tunnel. They are equipped with a telegraph for exchange of a small number of predefined messages. There is a signal light (red/green) at the incoming end of the tunnel. In normal functioning, an automatic system guarantee that any train passing a green signal automatically set that signal to red. When a train enters the tunnel the signalman A sends a message to the signalman B saying "train in tunnel". When signalman B gets this message he waits for the train to exit and sends the message "tunnel is free" to the signalman A. When the signalman A gets this message he manually sets the signal to green. A third message can be used by the signalman A in order to ask his colleague: "has the train left the tunnel"?

Notice that this protocol turned out to be incompletely specified and caused a railway accident which took place in Clayton, England (1861). One catch is that the automatic system by which an incoming train sets the signal to red may fail, in which case the signalman A is warned by a bell and the signal remains green till he sets it manually to red.

Exercise Model this protocol in Spin, using different proctypes for the signalmen and the train. Assume 3 trains in the system. Analyze the system for safety faults. If you get a fault, try to fix the protocol and re-validate it using Spin. Briefly describe the corrections made to the protocol.

2 Golo's Dinner Problem in NuSMV

Description Golo wants to eat some eggs that needs to be boiled for exactly 24 minutes. He uses two hourglasses for measuring the passage, respectively, of 7 and 11 minutes

(notice that a hourglass can be inverted to begin timing again). The problem consists of finding a strategy to help Golo cook his dinner.

Exercise Implement in NuSMV language a system that encodes the above problem, and prove with NuSMV that there exists a solution to the problem, by checking the appropriate CTL property and recording the counterexample generated.