

2G1516 Formal Methods – HT05

Modelling Software Systems

Advice Starred exercises are slightly more advanced than unstarred ones. Do the latter first, then try the starred ones.

Exercise* 1 (Slide 11)¹ Consider the transition system specification described in Slide 9. For the generated state space prove that it has the *diamond property*, i.e. that whenever $q \rightarrow q_1$ and $q \rightarrow q_2$ with $q_1 \neq q_2$ then there is a q_3 such that $q_1 \rightarrow q_3$ and $q_2 \rightarrow q_3$. Why is this called the diamond property? \square

Exercise* 2 (Slide 12) For the generated state space associated to the transition system specification in Ex. 1, give a mathematical proof that the state

$$\langle a = 2, b = 3, c = 4, d = 2, e = 1 \rangle$$

is not reachable from any initial state. \square

Exercise 3 The following program purports to solve mutual exclusion. Let $req_i, cs_i, i \in \{0, 1\}$, be variables over the domain of truthvalues $\{0, 1\}$ all with initial value 0. Let $P_i, i \in \{0, 1\}$, be the program:

$P_i : \text{while } 1 = 1 \text{ do } req_i := 1; req_{i \oplus 1} \neq 1 \rightarrow cs_i := 1; (cs_i, req_i) := (0, 0) \text{ od}$

where \oplus is addition modulo 2. Represent the system $P_0 \parallel P_1$ as a transition system specification. Show that the generated state space has a deadlocked state. \square

Exercise 4 Consider the PROMELA implementation of the Alternating-Bit Protocol that is available from the *Source Code* section of the course web-page:

1. Give a transition system specification for the case when there is no message loss (i.e. when variable LOSS is 1).
2. Write the generated state space corresponding to the transition system specification.

\square

¹Slide numbers correspond to slides for lecture 1, *Modelling Software Systems*, available from the course web-page.

Exercise 5 (Peled's exercise 4.12.1) Describe a scheduling algorithm that will guarantee that the scheduled executions will satisfy weak process fairness. Explain why your algorithm will not generate all the executions satisfying the weak process fairness assumption. \square