Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

D. Basin and P. Müller

Formal Methods and Functional Programming

Solutions of Exercise Sheet 14: Modelling and LTL

Sample Promela files that solve Assignments 1, 2, 3, and 5 are posted online.

Assignment 4

First part:

- $T \not\models \varphi_1, \gamma = s_1 s_4 s_5 s_4 s_5 s_4 \ldots$
- $T \models \varphi_2$

  There does not exist a loop in which r does not hold at some point.
- $T \models \varphi_3$

  $\neg r$ holds in s_1 and s_4, but s_1 cannot be a next state, hence only s_4 is of interest. In all states reachable in a single transition from s_4 r holds, hence the formula holds.
- $T \not\models \varphi_4, \gamma = s_1 s_4 s_5 s_5 s_5 \ldots$
- $T \models \varphi_5$

  p holds in s_1 and in all states after s_1 q or r hold.
- $T \not\models \varphi_6, \gamma = s_1 s_4 s_2 s_4 s_2 s_4 s_2 \ldots$
- $T \not\models \varphi_7, \gamma = s_1 s_4 s_2 s_4 s_2 s_4 s_2 \ldots$
- $T \models \varphi_8$

  The only way to satisfy the antecedent is to go into a loop $s_5 s_5 s_5$..., and in this loop the consequent is also satisfied, hence the formula holds. In all traces that do not have an infinite suffix of s_5's, the antecedent is false, and the formula holds trivially. Therefore, the formula holds for all traces.

Second part:

- $\Diamond \Box \neg(p \wedge \neg q \wedge \neg r)$

- $\square(r \to \bigcirc q)$
- $\bigcirc\square(p \to r)$
- $\square((p \wedge q \wedge r) \to ((p \wedge q \wedge r) \,\mathsf{U}\, \neg r))$
- $\Diamond(q \wedge \bigcirc\Diamond q)$
- $\square\Diamond q$
- $(p \wedge \bigcirc\square\neg p) \to (\square\Diamond\neg r)$
- $\square(\neg p \wedge q \wedge \neg r \to \bigcirc\neg(\neg p \wedge q \wedge \neg r))$