T–79.4301 **Spring 2006**

Parallel and Distributed Systems

Tutorial 8 - Wed Apr 12, 2006 11:15 and Fri Apr 21, 2006 14:15

1. Find Kripke models M_a, M_b, M_c and M_d (with $AP = \{p, q\}$) such that

   a) $M_a \models \mathbf{G}\, p$ and $M_a \models \mathbf{G}\,(p \Rightarrow q)$

   b) $M_b \not\models \mathbf{G}\, p$ and $M_b \models \mathbf{G}\,(p \vee \mathbf{Y}\, q)$

   c) $M_c \models \mathbf{G}\,(p \Rightarrow (q\, \mathbf{S}\, \neg p))$ and $M_c \models \mathbf{G}\,(p \Rightarrow \mathbf{Y}\,\mathbf{Y}\, \neg p)$

   d) $M_d \not\models \mathbf{G}\,(p\, \mathbf{S}\, q)$ and $M_d \models \mathbf{G}\,\mathbf{O}\, q$

   (For two formulas ψ_1, ψ_2, a finite word $\pi = x_0 x_1 x_2 \ldots x_n \in (2^{AP})^*$, and an index $0 \leq i \leq n$, $\pi^i \models \psi_1 \Rightarrow \psi_2$ holds iff $\pi^i \models (\neg\psi_1) \vee \psi_2$.)

2. Let $\varphi = \mathbf{G}\,(alarm \;\Rightarrow\; \mathbf{O}\,(crash))$ be a past safety formula over the atomic propositions $AP = \{alarm, crash\}$. Give a deterministic finite state automaton $\overline{\mathcal{S}}$ (over the alphabet 2^{AP}) which accepts the finite words that are counterexamples to the formula φ.

3. Demo exercise: Model the automaton $\overline{\mathcal{S}}$ in Promela by (mis-)using the `never` claim construction to observe the global `bool` variables `alarm` and `crash`, and to execute the Promela statement `assert(false)` when the automaton $\overline{\mathcal{S}}$ would accept the sequence observed so far.