Deductive Program Verification: Solutions to Exercise #3

Yu-Fang Chen
Dept. of Information Management, National Taiwan University

FLOLAC 2007: July 2–13, 2007

Note

We assume the binding powers of the various operators decrease in this order: $(\cdot)^n$ (exponentiation), $\{+, -\}$, $\neg$, $\{=, \geq, \leq\}$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\equiv$.

Solution

1. Consider the following program skeleton of mutual exclusion by a semaphore.

   Program Mux-Sem:

$$s : \text{natural } \textbf{initially } s = 1$$

$$\left[\begin{array}{l} l_0 : \textbf{loop forever do} \\ \left[\begin{array}{ll} l_1 : & \text{request}(s); \\ l_2 : & \text{release}(s); \end{array}\right] \end{array}\right] \parallel \left[\begin{array}{l} m_0 : \textbf{loop forever do} \\ \left[\begin{array}{ll} m_1 : & \text{request}(s); \\ m_2 : & \text{release}(s); \end{array}\right] \end{array}\right]$$

   where

   - $\text{request}(s) \triangleq \textbf{await } s > 0 \textbf{ then } s := s - 1 \textbf{ end}$
   - $\text{release}(s) \triangleq s := s + 1$

   Please re-describe the program as a fair transition system (FTS) and specify its safety and response properties in LTL.

   Solution.

   - $V \triangleq \{s : natural, \pi_0 : \{l_0, l_1, l_2\}, \pi_1 : \{m_0, m_1, m_2\}\}$
   - $\Theta \triangleq \pi_0 = l_0 \wedge \pi_1 = m_0 \wedge s = 1$
   - $\mathcal{T} \triangleq \{\tau_I, \tau_{l_0}, \tau_{l_1}, \tau_{l_2}, \tau_{m_0}, \tau_{m_1}, \tau_{m_2}\}$, whose transition relations are
     $\rho_I : \pi_0' = \pi_0 \wedge \pi_1' = \pi_1 \wedge s' = s$
     $\rho_{l_0} : \pi_0 = l_0 \wedge \pi_0' = l_1 \wedge s' = s \wedge \pi_1' = \pi_1$
     $\rho_{l_1} : \pi_0 = l_1 \wedge s > 0 \wedge \pi_0' = l_2 \wedge s' = s - 1 \wedge \pi_1' = \pi_1$
     $\rho_{l_2} : \pi_0 = l_2 \wedge s' = s + 1 \wedge \pi_1' = \pi_1$
     $\rho_{m_0} : \pi_1 = m_0 \wedge \pi_1' = m_1 \wedge s' = s \wedge \pi_0' = \pi_0$
     $\rho_{m_1} : \pi_1 = m_1 \wedge s > 0 \wedge \pi_1' = m_2 \wedge s' = s - 1 \wedge \pi_0' = \pi_0$

$\rho_{m_2} : \pi_1 = m_2 \wedge s' = s + 1 \wedge \pi_0' = \pi_0$

- $\mathcal{J} = \{\tau_{l_0}, \tau_{l_2}, \tau_{m_0}, \tau_{m_2}\}$
- $\mathcal{C} = \{\tau_{l_1}, \tau_{m_1}\}$

The safety property satisfied by this model:
$\Box(\neg(\pi_0 = l_2 \wedge \pi_1 = m_2))$
The response property satisfied by this model:
$\Box(\pi_0 = l_1 \rightarrow \Diamond(\pi_0 = l_2)) \wedge \Box(\pi_1 = m_1 \rightarrow \Diamond(\pi_1 = m_2))$ $\Box$