Deductive Program Verification: Exercise #3

Yih-Kuen Tsay
Dept. of Information Management, National Taiwan University

FLOLAC 2007: July 2–13, 2007

Note

This assignment is due at the end of the morning lab/tutor hour on July 11, 2007. Please write or type your answers on A4 (or similar size) paper. Late submission will not be accepted. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

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

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

   Program Mux-Sem:

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

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

   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. (100 points)

2. Consider the following program segment that performs the partition procedure of the Quicksort algorithm; the left and right bounds are fixed to be 1 and n for simplicity.

   $L, R := 1, n$; // $n > 0$
   while $L < R$ **do**
   while $X[L] \leq X[1] \wedge L \leq n$ **do** $L := L + 1$ **od**;
   while $X[R] > X[1] \wedge R \geq 1$ **do** $R := R - 1$ **od**;
   if $L < R$ **then** $X[L], X[R] := X[R], X[L]$ **fi**

od;
$M := R$;
$X[1], X[M] := X[M], X[1]$

- Give appropriate pre and post-conditions for the entire program segment.
- Prove its total correctness (according to the given pre and post-conditions); please present your correctness proof as a proof outline, supplying all intermediate assertions.

(0 point)