

Demostroación de Corrección del Semáforo de Habbermann

Leandro Jorge Fdez. Vega DGIIM

Para probar la corrección de un monitor debemos atender a los siguientes axiomas:

- Inicialización de variables permanentes:

$\{V\}$ inicialización $\{IM\}$

donde V es la verdad total y IM es el invariante del monitor.

- Procedimientos del monitor:

$\{IN \wedge IM\}$ procedimiento: $\{OUT \wedge IM\}$ $\bar{n} = 1 \dots n$
 $n = n + \text{procedimientos}$

donde IN son los parámetros iniciales y OUT la postcondición.

- Operaciones de sincronización con semántica desplazante:

$\{IM \wedge L\}$ $c.wait()$ $\{C \wedge L\}$

$\{ \neg vacio(c) \wedge L \wedge C \}$ $c.signal()$ $\{IM \wedge L\}$

donde L es un invariante local, C una condición de sincronización y c la propietaria de la cola de procesos en espera.

Por tanto, debemos verificar que el IM se mantiene tras el código de inicialización, antes y después de la llamada a un procedimiento, antes de cada $wait()$ y después de cada $signal()$.

Además, se deberán utilizar los axiomas básicos de demostración de corrección.

Monitor Semáforo_Habermann;

var na, np, nv : int
c : cond;

$$IM = \left\{ \begin{array}{l} n_p \leq n_a \\ n_p \leq n_v \\ n_p \geq \min(n_a, n_v) \end{array} \right\}$$

begin

{true}

na := 0

np := 0

nv := 0

{np ≤ na, np ≤ nv, np ≥ min(na, nv)}

end

Procedure V;

begin

{np ≤ na, np ≤ nv, np ≥ min(na, nv)}

nv := nv + 1;

{np ≤ na, np ≤ nv - 1, np ≥ min(na, nv - 1)}

if (na > np)

{np < na, np = nv - 1} (condición sincronización)

then c.signal();

{np ≤ na, np ≤ nv, np ≥ min(na, nv)}

end

procedure P;

begin

{np ≤ na, np ≤ nv, np ≥ min(na, nv)}

na := na + 1;

{np ≤ na - 1, np ≤ nv, np ≥ min(na - 1, nv)}

if (na > nv)

{np ≤ na - 1, np ≤ nv, np ≥ min(na - 1, nv)}

↓

{np ≤ na, np ≤ nv, np ≥ min(na, nv)}

then c.wait();

{np < na, np = nv - 1}

↓ condición sincronización

{np ≤ na - 1, np ≤ nv - 1, np ≥ min(na - 1, nv - 1)}

np := np + 1;

{np ≤ na, np ≤ nv, np ≥ min(na, nv)}

end

Vemos que se verifican todas las condiciones, por lo que queda probada la corrección del monitor.