E.T.S.I. Informática. 9 de Febrero de 2007

Lenguajes de Programación (tercer curso)

APELLIDOS: **SOLUCIONES**

NOMBRE: _____

1	2	3	4	5	N

□ si
□ no
} deseo que se publique mi calificación

[Todo: 2,3,4,5; 1º parcial: 1, 2º parc.: 2
3º parc.: 3, 4º parc.: 5,6]

---

1 Interpreta la siguiente propiedad $(*)$ y demuéstrala vía la semántica de Dijkstra:

$$\{P\}S\{Q\} \wedge [Q \equiv Falso] \qquad \Rightarrow \qquad [P \equiv Falso] \qquad (*)$$

SOL Si se satisface el triplete $\{P\}S\{Q\}$ y existiera algún estado ι satisfaciendo P, entonces, partiendo de este estado ι, S termina siempre en un estado satisfaciendo el predicado Q, que es incompatible con la condición $[Q \equiv Falso]$.

Veamos ahora la demostración en la lógica de Dijkstra:

$\{P\}S\{Q\} \wedge [Q \equiv Falso]$

$\equiv \because$ definición de triplete en la lógica de Dijkstra

$[P \ \Rightarrow \ S.Q] \wedge [Q \equiv Falso]$

$\Rightarrow \because$ sustitutividad y CP

$[P \ \Rightarrow \ S.Falso]$

$\equiv \because$ por LME tenemos $[Falso \equiv S.Falso]$, y por sustitutividad

$[P \ \Rightarrow \ Falso]$

$\equiv \because$ CP

$[P \equiv Falso]$

---

2 Sea $\mathcal{D}$ un conjunto con una relación de orden total $<$. Queremos probar que es posible calcular el segundo mayor ($\mathcal{SM}$) de 4 valores Q_1, Q_2, Q_3, Q_4 del conjunto $\mathcal{D}$ realizando un máximo de 5 intercambios vía el programa:

$$\begin{array}{rl} & q_1, q_2, q_3, q_4 := Q_1, Q_2, Q_3, Q_4; \\ *[\!] & q_1 > q_3 \rightarrow q_1, q_3 := q_3, q_1 \\ \Box & q_2 > q_3 \rightarrow q_2, q_3 := q_3, q_2 \\ \Box & q_3 > q_4 \rightarrow q_3, q_4 := q_4, q_3 \ ]\!] \{q_3 = \mathcal{SM}\} \end{array}$$

A Prueba en primer lugar que la función $t \doteq \delta_{1,3} + \delta_{2,3} + \delta_{1,4} + \delta_{2,4} + \delta_{3,4}$ es un contador entero, siendo $\delta_{i,j} = \begin{cases} 1, & \text{si } q_i > q_j \\ 0, & \text{si } q_i \leq q_j \end{cases}$

SOL Dado un bucle con n guardas $*[\!] \ \Box_{k=1..n} b_k \rightarrow S_k \ ]\!]$, un contador entero relativo a un invariante I es una función $t : \mathcal{E} \rightarrow \mathbb{Z}$ satisfaciendo las condiciones, $\forall k : k = 1..n$, y *ptle*:

1. $I \wedge b_k \ \Rightarrow \ S_k.I$
2. $I \wedge b_k \ \Rightarrow \ t > 0$
3. $I \wedge b_k \ \Rightarrow \ wdec(S_k, t)$

Para el caso $t \doteq \delta_{1,3} + \delta_{2,3} + \delta_{1,4} + \delta_{2,4} + \delta_{3,4}$, ya que $\delta_{i,j} \geq 0$, se verifica $t \geq 0$, y si alguna guarda $q_i > q_j$ es cierta, para esa guarda tenemos $\delta_{i,j} = 1$, de donde se satisface la condición (2).

Si tomamos como candidato a invariante el predicado $I \doteq (q_1, q_2, q_3, q_4) \in \mathcal{P}erm(Q_1, Q_2, Q_3, Q_4)$ ($\doteq$ el conjunto de tuplas permutaciones de (Q_1, Q_2, Q_3, Q_4)), entonces (las demás implicaciones se prueban de igual forma), *ptle*:

$I \wedge q_1 > q_3 \ \Rightarrow \ q_1, q_3 := q_3, q_1.I$

$\equiv \because$ definición de I

$(q_1, q_2, q_3, q_4) \in \mathcal{P}erm(Q_1, Q_2, Q_3, Q_4) \wedge q_1 > q_3 \ \Rightarrow \ (q_3, q_2, q_1, q_4) \in \mathcal{P}erm(Q_1, Q_2, Q_3, Q_4)$

$\equiv \because$ definición de permutación

Cierto

La condición (3) es la más delicada. Por simetría basta probar los casos:

$$(a) \qquad [q_1 > q_3 \;\Rightarrow\; wdec(q_1, q_3 := q_3, q_1, t)] \qquad\qquad (b) \qquad [q_3 > q_4 \;\Rightarrow\; wdec(q_3, q_4 := q_4, q_3, t)]$$

Ambos se hacen igual; veamos por ejemplo el primero, *ptle*:

$wdec(q_1, q_3 := q_3, q_1, t) \wedge q_1 > q_3$

$\equiv \because$ Lema 6.43 del libro de Texto

$\delta_{3,1} + \delta_{2,1} + \delta_{3,4} + \delta_{2,4} + \delta_{1,4} < \delta_{1,3} + \delta_{2,3} + \delta_{1,4} + \delta_{2,4} + \delta_{3,4} \wedge q_1 > q_3$

$\equiv \because$ def. de $\delta_{i,j}$, y cancelación de términos iguales

$0 + \delta_{2,1} < 1 + \delta_{2,3} \wedge q_1 > q_3$

$\equiv \because$ si def. $\delta_{2,3} = 1$ la desigualdad queda $0 + \delta_{2,1} < 2$ y es trivial; si $\delta_{2,3} = 0$, entonces $q_2 \leq q_3$, y al ser $q_3 < q_1$, tendremos $q_2 \leq q_1$ de donde también $\delta_{2,1} = 0$, y la desigualdad queda $0 + 0 < 1 + 0$.

B Usa el *Teorema de los Contadores enteros* (TCE) para concluir que el programa calcula $\mathcal{SM}$ con un máximo de 5 intercambios, pero, en general, no lo puede hacer con un número menor de intercambios; concluye de esto que t es el *mejor* contador. (AYUDA.- (1) Prueba que cierto predicado I es un invariante, y aplica el TCE para probar que el programa termina. (2) Da una cota del número de intercambios a partir del mayor valor del contador. (3) Toma por ejemplo $\mathcal{D} \doteq \mathbb{N}$, y prueba que para el conjunto de valores $(Q_1, Q_2, Q_3, Q_4) = (3, 4, 2, 1)$, existe una ejecución del bucle que realiza exactamente 5 intercambios).

SOL Sigamos la ayuda.

(1) El predicado I del apartado anterior es un invariante. I es trivialmente cierto antes del bucle, ya que $[Cierto \equiv q_1, q_2, q_3, q_4 := Q_1, Q_2, Q_3, Q_4.I]$. Por tanto, aplicando el TCE tendremos para nuestro programa, $\{Cierto\} q_1, ... := ... \quad ; *[\![q_1 > q_3 ...]\!] \{q_1, q_2 \leq q_3 \leq q_4 \wedge I\}$, y el último predicado asegura $q_3 = \mathcal{SM}$.

(2) Por ser t suma de un máximo de 5 unos, tendremos $[t \leq 5]$, de donde el número de pasos del bucle (es decir, el número de intercambios), que sabemos que está acotado por el valor inicial del contador t, es a lo sumo 5. Para probar que es el "mejor" contador basta encontrar ejecuciones del bucle con 5 intercambios. Por ejemplo, la siguiente tabla muestra los sucesivos valores de las variables, y de t para la guarda seleccionada que se indica:

guarda seleccionada	q_1	q_2	q_3	q_4	t
3^a	3	4	2	1	5
1^a	3	4	1	2	4
2^a	1	4	3	2	3
3^a	1	3	4	2	2
2^a	1	3	2	4	1
	1	2	3	4	0

---

3 Interpreta la siguiente propiedad $(*)$ y prueba que es cierta dentro de la lógica de Hoare estándar.

$$\{P\}S\{Q\} \wedge [Q \equiv Falso] \qquad \Rightarrow \qquad [P \equiv Falso] \qquad (*)$$

SOL Si se satisface el triplete $\{P\}S\{Q\}$ y existiera algún estado ι satisfaciendo P, entonces, partiendo de este estado ι, S termina siempre en un estado satisfaciendo el predicado Q, que es incompatible con la condición $[Q \equiv Falso]$.

SOL *Ahora probaremos* $(*)$ *por inducción sobre* **las derivaciones del triplete {P} S {Q }** que satisfacen $[Q \equiv Falso]$. Los casos base son sencillos:

1. Si la última regla aplicada es $(aborta)\frac{}{\{Falso\}aborta\{Q\}}$, ya tenemos directamente que P es sintácticamente igual a $Falso$.
2. Si la última regla aplicada es $(nada)\frac{}{\{Q\}nada\{Q\}}$, tenemos directamente que P es sintácticamente igual a Q, y por tanto también $[P \equiv Falso]$.
3. Si la última regla aplicada es la asignación $\frac{}{\{x:=E.Q\}x:=E\{Q\}}$, entonces, P es sintácticamente igual a $x := E.Q$, y aplicamos la siguiente propiedad:

$$[Q \equiv Falso] \qquad \Rightarrow \qquad [x := E.Q \equiv Falso]$$

que a su vez es consecuencia de esta otra:

$$[Q \equiv Q'] \qquad \Rightarrow \qquad [(x := E.Q) \equiv (x := E.Q')]$$

que es consecuencia de la regla de Leibnitz (página 11 del libro de texto).

Veamos los pasos inductivos. Supongamos en lo que sigue que $[Q \equiv Falso]$.

1. Si el triple $\{P\}S;T\{Q\}$ es consecuencia de la regla de la composición con antecedente:
   $\{P\}S\{X\} \wedge \{X\}T\{Q\}$, además de $[Q \equiv Falso]$
   $\Rightarrow\because$ Hipótesis de inducción aplicada al segundo triplete
   $\{P\}S\{X\} \wedge [X \equiv Falso]$
   $\Rightarrow\because$ HI aplicada al primer triplete
   $[P \equiv Falso]$.

2. Si el triple $\{P\}if\ b\ then\ S\ else\ T\{Q\}$ es consecuencia de la regla de la composición con antecedente:
   $\{P \wedge b\}S\{Q\} \wedge \{P \wedge \neg b\}T\{Q\}$, además de $[Q \equiv Falso]$
   $\Rightarrow\because$ Hipótesis de inducción dos veces
   $[P \wedge b \equiv Falso] \wedge [P \wedge \neg b \equiv Falso]$
   $\Rightarrow\because$ CP (tercio excluido)
   $[P \equiv Falso]$

---

4 Demuestra que la tupla $t \doteq (q_1, q_2, q_3, q_4)$ es un contador generalizado, y usa el Teorema de los Contadores Generalizados para probar que el bucle termina siempre.

SOL El *Teorema de los Contadores Generalizados* (TCG) se enuncia en la forma siguiente: véase el Corolario 8.46, página 176 del libro de texto, así como el Ejemplo 8.47 7(página 177). Tomamos $\mathcal{D} = \mathcal{C} = \mathcal{P}er(Q_1, Q_2, Q_3, Q_4)$, que al ser finito es bien construido para el orden lexicográfico. Tomamos el invariante descrito en el apartado 2.A; tomamos ahora $t \doteq (q_2, q_1, q_3, q_4)$; todas las condiciones del TCG son triviales, salvo las implicaciones:
$(a) \quad [q_1 > q_3 \ \Rightarrow\ wdec(q_1, q_3 := q_3, q_1, t)]$ $(b) \quad [q_2 > q_3 \ \Rightarrow\ wdec(q_2, q_3 := q_3, q_2, t)]$
$(c) \quad [q_3 > q_4 \ \Rightarrow\ wdec(q_3, q_4 := q_4, q_3, t)]$
Las dos primeras son simétricas. Las otras dos se prueban de forma similar; veamos la tercera:
$wdec(q_3, q_4 := q_4, q_3, t) \wedge q_3 > q_4$
$\equiv\because$ Lema 6.43 del libro de Texto
$(q_2, q_1, q_4, q_3) < (q_2, q_1, q_3, q_4) \wedge q_3 > q_4$
$\equiv\because$ orden lexicográfico
$Cierto$

5 Sea el procedimiento recursivo

$$m = [\![\quad i > 10 \to i := i - 1 \\ \quad\ \ i \leq 10 \to i := i + 2; m \,]\!]$$

A Traza una llamada al procedimiento m para los valores iniciales de $i = 12, 11, 10, 9, 8, 7, \ldots$. ¿Qué puedes conjeturar sobre el comportamiento de m para estos valores?

SOL Trazando la ejecución de m (véase, el Ejemplo 9.10, páginas 191-194 del Texto de la asignatura) se conjetura el siguiente comportamiento:

$$\{i \text{ par}, i \leq 12\}m\{i = 11\}, \qquad \{i \text{ impar}, i \leq 11\}m\{i = 10\}$$

B Utilizando la semántica de los procedimientos vía puntos fijos, prueba, por inducción sobre k, que para todo predicado Z se satisface:

$$\forall k : k \leq 6 : \qquad [\ i = 2k \wedge m.Z \qquad \equiv \qquad i = 2k \wedge i := 11.Z\ ]$$

$\boxed{SOL}$

Caso base: $k = 6$. tenemos, *ptle*

$i = 12 \wedge m.Z$

$\equiv\because$ semántica puntos fijos, semántica selectiva $(i > 10)$

$i = 12 \wedge i := i - 1.Z$

$\equiv\because$ Leibniz: $[i = p \wedge i := E(i).Z \quad \equiv \quad i = p \wedge i := E(p).Z]$

$i = 12 \wedge i := 12 - 1.Z$

Paso inductivo: $k < 6$.

$i = 2k \wedge m.Z$

$\equiv\because$ semántica puntos fijos, semántica selectiva $(i = 2k \leq 10)$

$i = 2k \wedge i := i + 2.m.Z$

$\equiv\because$ sustitución

$i := i + 2.(i = 2k + 2 \wedge m.Z)$

$\equiv\because$ Hipótesis de inducción $(2k + 2 \leq 12)$

$i := i + 2.(i = 2k + 2 \wedge i := 11.Z)$

$\equiv\because$ sustitución y lema de sustitución

$i = 2k \wedge i := 11.Z$

$\boxed{SOL}$ **y concluye el triplete** $\{i = -100\}m\{i = 11\}$

$\{i = -100\}m\{i = 11\}$

$\equiv\because$ definición de triplete

$[i = -100 \quad \Rightarrow \quad m.(i = 11)]$

$\equiv\because$ regla de oro

$[i = -100 \wedge m.(i = 11) \equiv i = -100]$

$\equiv\because$ propiedad del apartado B anterior para $k = -50$

$[i = -100 \wedge i := 11.(i = 11) \equiv i = -100]$

$\equiv\because$ sustitución

$[i = -100 \wedge 11 = 11 \equiv i = -100]$

$\equiv\because$ Cálculo de predicados

Cierto

C Si cambiamos la sentencia $i := i + 2$ por la sentencia $i := i + 5$, ¿qué comportamiento se espera de m?

$\boxed{SOL}$ El comportamiento se resume en la forma siguiente:

$\{i = p \leq 12\}m\{i = 10 + (p - 1) \text{ módulo } 5\}$

Completa el triplete $\{i = -97\}m\{i = \dots\}$

$\boxed{SOL}$ $\{i = -97\}m\{i = 10 + -98 \text{ módulo } 5\}$, es decir: $\{i = -97\}m\{i = 10 + 2\}$