E.T.S.I. Informática. Ordinario de Febrero 2006

Lenguajes de Programación (tercer curso)

APELLIDOS: **SOLUCIONES**

NOMBRE: ______________________

1	2	3	4	5	6	7	8	9	10	11
3.0	2.0	5.0	3.0	1.0	2.0	2.0	2.0	4.0	2.0	4.0

□ si
□ no
} deseo que se publique mi calificación

$\boxed{\mathbf{1}}$ Calcula el predicado $[\![z > x \to z := x \,\square\, z \leq x \to nada]\!] .(z \leq x)$, e **interpreta** el resultado obtenido.

$\boxed{SOL}$ *ptle*, el predicado a evaluar es

$\equiv\because$ semántica de la selectiva binaria

$z > x \wedge z := x.(z \leq x) \vee z \leq x \wedge nada.(z \leq x)$

$\equiv\because$ semántica asignación y $nada$

$z > x \wedge x \leq x \vee z \leq x \wedge z \leq x$

$\equiv\because$ Cálculo de predicados

$Cierto$

Es decir, encontramos $\{Cierto\}[\![z > x \to z := x \,\square\, z \leq x \to nada]\!] \{z \leq x\}$, y la selectiva siempre termina con un valor de z menor o igual al de x, lo que es evidente desde un punto de visa operacional ya que si al principio ocurre lo contrario $z > x$, la selectiva cambiará el valor de z por el valor de x.

$\boxed{\mathbf{2}}$ Interpreta la siguiente propiedad:

$$\{P\}S;T\{Q\} \qquad \Rightarrow \qquad \{P\}S\{Cierto\} \qquad (*)$$

$\boxed{SOL}$ Si para cada estado satisfaciendo el predicado P la composición secuencial $S;T$ termina en un estado verificando Q, entonces, partiendo de un estado satisfaciendo P el programa inicial S termina. Es decir: Los estados que garantizan que $S;T$ termina, también garantizan la terminación del programa S.

$\boxed{\mathbf{3}}$ Prueba la propiedad $(*)$ vía la semántica de Dijkstra.

$\boxed{SOL}$ $\{P\}S\{Cierto\}$

$\equiv\because$ definición de triplete de Dijkstra

$[P \;\Rightarrow\; S.Cierto]$

$\Leftarrow\because$ $[T.Q \;\Rightarrow\; Cierto]$, y por monotonía de S, $[S.(T.Q) \;\Rightarrow\; S.Cierto]$, y por transitividad de $\Rightarrow$,

$[P \;\Rightarrow\; S.(T.Q)]$

$\equiv\because$ semántica de la composición

$[P \;\Rightarrow\; S;T.Q]$

$\equiv\because$ definición de triplete

$\{P\}S;T\{Q\}$

$\boxed{\mathbf{4}}$ Prueba la propiedad $(*)$ para la lógica de Hoare estándar.

$\boxed{SOL}$ Utilizaré como herramienta inducción sobre la derivación del triplete $t \doteq \{P\}S;T\{Q\}$. En la lógica estándar, t solo es posible inferirlo por dos reglas:

1. Por la regla de la composición (caso base), y en el antecedente de la regla aparecerá un triplete de la forma $\{P\}S\{I\}$, y ahora, ya que $[I \;\Rightarrow\; Cierto]$, basta aplicar la regla de refinamiento para obtener $\{P\}S\{Cierto\}$.

2. Por la regla de refinamiento (paso inductivo), y tendremos en el antecedente de la regla:

   $[P \;\Rightarrow\; P'] \wedge \{P'\}S;T\{Q'\} \wedge [Q' \;\Rightarrow\; Q]$

   $\Rightarrow\because$ Ya que el triplete $\{P'\}S;T\{Q'\}$ aparece en el antecedente de la regla, aplicamos Hipótesis de Inducción

$$
\begin{array}{ll}
 & [P \ \Rightarrow \ P'] \wedge \{P'\}S\{Cierto\} \\
\Rightarrow & \because \text{ la regla de refinamiento} \\
 & \{P\}S\{Cierto\}
\end{array}
$$

$\boxed{\mathbf{5}}$ El siguiente programa calcula el mínimo $\mathcal{M}in$ y el máximo $\mathcal{M}ax$ de 4 valores Q_1, Q_2, Q_3, Q_4 pertenecientes a un conjunto $\mathcal{D}$ con una relación de orden total:

$$
\begin{array}{ll}
 & q_1, q_2, q_3, q_4 := Q_1, Q_2, Q_3, Q_4; \\
*[\![& q_1 > q_2 \rightarrow q_1, q_2 := q_2, q_1 \\
\Box & q_1 > q_3 \rightarrow q_1, q_3 := q_3, q_1 \\
\Box & q_4 < q_2 \rightarrow q_2, q_4 := q_4, q_2 \\
\Box & q_4 < q_3 \rightarrow q_3, q_4 := q_4, q_3 \,]\!] \, \{q_1 = \mathcal{M}in \wedge q_4 = \mathcal{M}ax\}
\end{array}
$$

Prueba que la corrección del programa puede obtenerse a través del teorema de los contadores si tomamos un invariante adecuado.

$\boxed{SOL}$ En efecto, basta tomar $I \doteq$ "(q_1, q_2, q_3, q_4) es una permutación de los valores (Q_1, Q_2, Q_3, Q_4)". I es trivialmente cierto antes del bucle, ya que $[Cierto \equiv q_1, q_2, q_3, q_4 := Q_1, Q_2, Q_3, Q_4.I]$. Además, I es un invariante, ya que para cualquier par de índices (i, j) diferentes, se verifica $[I \equiv q_i, q_j := q_j, q_i.I]$. Si el bucle termina, lo hará satisfaciendo $q_1 \leq q_2, q_3 \leq q_4$, de donde concluimos $q_1 = \text{mín}(q_1, q_2, q_3, q_4) \wedge q_4 = \text{máx}(q_1, q_2, q_3, q_4)$. Además, por el teorema de invariantes, terminará satisfaciendo $I \wedge q_1 \leq q_2, q_3 \leq q_4$. Pero también es cierto

$$[I \quad \Rightarrow \quad \text{mín}(q_1, q_2, q_3, q_4) = \text{mín}(Q_1, Q_2, Q_3, Q_4) \wedge \ \text{máx}(q_1, q_2, q_3, q_4) = \text{máx}(Q_1, Q_2, Q_3, Q_4)]$$

y por tanto $[I \wedge q_1 \leq q_2, q_3 \leq q_4 \ \Rightarrow \ q_1 = \mathcal{M}in \wedge q_4 = \mathcal{M}ax]$.

$\boxed{\mathbf{6}}$ Demuestra que $t \doteq \delta_{1,2} + \delta_{1,3} + \delta_{1,4} + \delta_{2,4} + \delta_{3,4}$ es un contador entero, donde $\delta_{i,j} = \begin{cases} 1, & \text{si } q_i > q_j \\ 0, & \text{si } q_i \leq q_j \end{cases}$

$\boxed{SOL}$ Basta probar, para cada guarda y sentencia guardada, $[b_j \ \Rightarrow \ t > 0 \wedge wdec(S_j|t)]$. La implicación $[b_j \ \Rightarrow \ t > 0]$ es consecuencia de ser t suma de ceros o unos, siendo uno de ellos un uno para dicha guarda. Por simetría, la prueba de la segunda implicación bastará hacerla para una guarda. Por ejemplo, veamos la primera: Tendremos, *ptle*

$$
\begin{array}{ll}
 & wdec(q_1, q_2 := q_2, q_1|t) \\
\equiv & \because \text{ Lema 6.43} \\
 & \delta_{2,1} + \delta_{2,3} + \delta_{2,4} + \delta_{1,4} + \delta_{3,4} < \delta_{1,2} + \delta_{1,3} + \delta_{1,4} + \delta_{2,4} + \delta_{3,4} \\
\equiv & \because \text{ Simplificamos términos iguales} \\
 & \delta_{2,1} + \delta_{2,3} + < \delta_{1,2} + \delta_{1,3} \\
\Leftarrow & \because q_1 > q_2 \quad \Rightarrow \quad \delta_{2,3} \leq \delta_{1,3} \wedge \delta_{2,1} = 0 \wedge \delta_{1,2} = 1 \\
 & q_1 > q_2
\end{array}
$$

$\boxed{\mathbf{7}}$ Usa el teorema de los contadores para concluir que el programa calcula $\mathcal{M}in$ y $\mathcal{M}ax$ con un máximo de 5 intercambios, pero en general, no lo puede hacer con un número menor de intercambios, de donde t es el *mejor* contador.

$\boxed{SOL}$ Por el teorema de los contadores el bucle termina. 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. Para $(Q_1, Q_2, Q_3, Q_4) \equiv (4, 2, 3, 1)$, o también si $Q_1 > Q_2 > Q_3 > Q_4$, la siguiente tabla muestra los sucesivos valores de las variables y del contador t para la guarda seleccionada que se indica:

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

8 Generaliza lo anterior para demostrar que es posible calcular el máximo y el mínimo de N valores con un máximo de $2N-3$ intercambios.

SOL Se considera el siguiente programa para N valores y N variables

$$\begin{array}{ll} & q_1, q_2, \ldots, q_N := Q_1, Q_2, \ldots, Q_N; \\ *[\![& q_1 > q_2 \rightarrow q_1, q_2 := q_2, q_1 \\ \ldots & \\ \Box & q_1 > q_{N-1} \rightarrow q_1, q_{N-1} := q_{N-1}, q_1 \\ \Box & q_N < q_2 \rightarrow q_2, q_N := q_N, q_2 \\ \ldots & \\ \Box & q_N < q_{N-1} \rightarrow q_{N-1}, q_N := q_N, q_{N-1}]\!] \{q_1 = \mathcal{M}in \wedge q_N = \mathcal{M}ax\} \end{array}$$

y para éste el contador $t \doteq \delta_{1,2} + \cdots + \delta_{1,N} + \delta_{2,N} + \cdots + \delta_{N-1,N}$. Tendremos evidentemente $[t \leq 2N-3]$. La prueba de que t disminuye al menos en una unidad en cada paso es ahora algo más compleja ya que, por ejemplo:

$$\begin{array}{ll} & wdec(q_1, q_2 := q_2, q_1 | t) \\ \equiv\because & \text{Lema 6.43} \\ & \delta_{2,1} + \delta_{2,3} + \cdots + \delta_{2,N} + \delta_{1,N} + \delta_{3,N} + \cdots + \delta_{N-1,N} < \delta_{1,2} + \delta_{1,3} + \cdots + \delta_{1,N} + \delta_{2,N} + \delta_{3,N} + \cdots + \delta_{N-1,N} \\ \equiv\because & \text{Simplificamos términos iguales} \\ & \delta_{2,1} + \delta_{2,3} + \cdots + \delta_{2,N-1} < \delta_{1,2} + \delta_{1,3} + \cdots + \delta_{1,N-1} \\ \Leftarrow\because & q_1 > q_2 \;\Rightarrow\; \delta_{2,k} \leq \delta_{1,k},\; k = 3, \ldots, N-1 \\ & q_1 > q_2 \end{array}$$

---

9 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.

SOL El *Teorema de los Contadores Generalizados* se enuncia en la forma siguiente: (Véase por ejemplo el Corolario 8.43 de página 176 del texto de la asignatura):

Corolario 8.46 *Sea un bucle* $\mathcal{R} \doteq [\![\;\Box : b_i \; S_i]\!]$ *y sea* t *una aplicación* $t : \xi \rightarrow \mathcal{D}$ *y* $\mathcal{C} \subseteq \mathcal{D}$ *verificando*

(bc) $\mathcal{C}$ *es un conjunto bien construido,*

(f) $\forall i :: [I \wedge b_i \;\Rightarrow\; t \in \mathcal{C}]$,

(id) $\forall i :: [I \wedge b_i \;\Rightarrow\; S_i.I \wedge wdec(S_i, t)]$.

Entonces $[I \;\Rightarrow\; \mathcal{R}.I]$.

Aplicaremos el Corolario anterior tomando:

– $\mathcal{D} \doteq$ el conjunto de permutaciones de los valores (Q_1, Q_2, Q_3, Q_4), con el orden lexicográfico, y $\mathcal{C} = \mathcal{D}$.

– $t \doteq (q_1, q_2, q_3, q_4)$ y $I \doteq t \in \mathcal{C}$.

Trivialmente $\mathcal{C}$ es un conjunto bien construido por ser finito y se satisfacen las dos condiciones (bc) y (f) del Corolario 8.46. La invariabilidad de I es igualmente trivial, y queda probar $[I \wedge b_i \;\Rightarrow\; wdec(S_i, t)]$. Tendremos por ejemplo, *ptle*

$$\begin{array}{ll} & wdec(q_1, q_2 := q_2, q_1 | t) \\ \equiv\because & \text{Lema 6.43, definición de } t\text{, sustitución} \\ & (q_2, q_1, q_3, q_4) < (q_1, q_2, q_3, q_4) \\ \equiv\because & \text{Orden lexicográfico} \\ & q_1 > q_2 \end{array} \qquad \begin{array}{ll} & wdec(q_2, q_4 := q_4, q_2 | t) \\ \equiv\because & \text{Lema 6.43, definición de } t\text{, sustitución} \\ & (q_1, q_4, q_3, q_2) < (q_1, q_2, q_3, q_4) \\ \equiv\because & \text{Orden lexicográfico} \\ & q_4 < q_2 \end{array}$$

siendo las pruebas de las otras dos implicaciones similares. En definitiva, por aplicación del Corolario anterior el bucle termina siempre, ya que antes del bucle se satisface I.

Sea el procedimiento recursivo

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

$\boxed{\textbf{10}}$ Traza una llamada al procedimiento m para los valores iniciales $i = 10, 9, 8, \ldots$. ¿Qué puedes conjeturar sobre el comportamiento de m para estos valores?

$\boxed{SOL}$ Veamos las primeras trazas

i	sentencia a ejecutar	i	sentencia a ejecutar	i	sentencia a ejecutar
10	m	9	m	8	m
10	$i := i + 1; m$	9	$i := i + 1; m$	8	$i := i + 1; m$
11	m	10	m	9	m
11	$i := i - 1$		$\ldots$		$\ldots$
10	$\square$	10	$\square$	10	$\square$

Conjeturamos: "Para los valores $i = 11, 10, 9, 8, \ldots$ la sentencia m se comporta como la sentencia $i := 10$".

$\boxed{\textbf{11}}$ Utilizando la semántica de los procedimientos vía puntos fijos, prueba por inducción sobre k, que para todo predicado Z se satisface:

$$\forall k : k \le 11 : i = k \wedge m.Z \qquad \equiv \qquad i = k \wedge i := 10.Z]$$

$\boxed{SOL}$ El caso base es $k = 11$, y se deduce de la propiedad de *puntualidad* de los predicados como funciones (véase página 15 del texto). Por ejemplo, si Z depende del predicado i, pongamos $Z(i)$, la propiedad de puntualidad se escribe en la forma, $[i_1 = i_2 \;\Rightarrow\; Z(i_1) = Z(i_2)]$. Entonces, *ptle*,

$\qquad i = 11 \wedge m.Z(i) \qquad \equiv \qquad i = 11 \wedge i := 10.Z(i)$

$\equiv \because$ Definición de m, definición de sustitución

$\qquad i = 11 \wedge Z(i-1) \qquad \equiv \qquad i = 11 \wedge Z(10)$

$\equiv \because$ Propiedad de *puntualidad*

$\qquad$ *Cierto*

Veamos ahora el paso inductivo. Supongamos $k < 11$. Entonces

$\qquad i = k \wedge m.Z$

$\equiv \because$ def. de m, $k < 11$

$\qquad i = k \wedge i := i + 1; m.Z$

$\equiv \because$ Sustitución

$\qquad i := i + 1.(i = k + 1 \wedge m.Z)$

$\equiv \because$ $k + 1 \le 11$, Hipótesis de Inducción

$\qquad i := i + 1.(i = k + 1 \wedge i := 10.Z)$

$\equiv \because$ Sustitución

$\qquad i = k \wedge i := i + 1; i := 10.Z$

$\equiv \because$ Lema de sustitución (Lema 4.7(i), página 59).

$\qquad i = k \wedge i := (i := i + 1.10).Z$

$\equiv \because$ i no aparece en la constante 10

$\qquad i = k \wedge i := 10.Z$

Ahora vamos a concluir $\{i = -101\} m \{i = 10\}$

$\qquad \{i = -101\} m \{i = 10\}$

$\equiv \because$ definición de triplete

$\qquad [i = -101 \;\Rightarrow\; m.(i = 10)]$

$\equiv \because$ Regla de oro

$\qquad [i = -101 \equiv i = -101 \wedge m.(i = 10)]$

$\equiv \because$ Propiedad demostrada anteriormente

$\qquad [i = -101 \equiv i = -101 \wedge i := 10.(i = 10)]$

$\equiv \because$ Sustitución, Cálculo de predicados

$\qquad$ *Cierto*