E.T.S.I. Informática. Parcial, Diciembre 2004

Lenguajes de Programación (tercer curso)

APELLIDOS: **SOLUCIONES**

NOMBRE: _____

PUNTUACIONES:	1	2	3	4	5	6	7	total
	2.5	0.5	1.0	2.0	0.5	0.5	3.0	10.0

□ si
□ no
} deseo que se publique mi calificación

Consideremos la lógica de Hoare $\mathcal{LH}$ para un lenguaje sin bucles con selecciones indeterministas y para las cuales introducimos la siguiente regla:

$$\frac{\{b\}S\{Y\} \qquad \{b'\}S'\{Y\}}{\{b \vee b'\}[\![\, b \to S \,\square\, b' \to S' \,]\!]\{Y\}}$$

1 Prueba que esta lógica $\mathcal{LH}$ es correcta con respecto a la semántica de Dijkstra.

SOL *Probaré:* $\vdash_{\mathcal{H}} \{X\}S\{Y\} \;\Rightarrow\; [X \;\Rightarrow\; S.Y]$. *Y para ello utilizaré como técnica inducción sobre las derivaciones.* Si seguimos el libro de texto (prueba del Teo. 5.14, página 76), vemos que lo único que hay que probar es la validez de las reglas de $\mathcal{LH}$ en la lógica de Dijkstra. Salvo la corrección de la regla de la selectiva indeterminista, las restantes pruebas aparecen em el libro de texto (página 75). Veamos pues la corrección de la regla nueva. Es decir, hay que probar la implicación:

$$[b \;\Rightarrow\; S.Y] \wedge [b' \;\Rightarrow\; S'.Y]$$
$$\Rightarrow$$
$$[b \vee b' \;\Rightarrow\; [\![\, b \to S \,\square\, b' \to S' \,]\!].Y]$$

Desarrollemos pues el consecuente:

$$[b \vee b' \quad \Rightarrow \quad [\![\, b \to S \,\square\, b' \to S' \,]\!].Y]$$
$\equiv\cdot\cdot$ Definición del transformador de la selectiva
$$[b \vee b' \quad \Rightarrow \quad (b \vee b') \wedge (b \;\Rightarrow\; S.Y) \wedge (b' \;\Rightarrow\; S'.Y)]$$
$\equiv\cdot\cdot$ CP: $[A \;\Rightarrow\; B \wedge C \wedge D] \equiv [A \;\Rightarrow\; B] \wedge [A \;\Rightarrow\; C] \wedge [A \;\Rightarrow\; D]$
$$[b \vee b' \;\Rightarrow\; b \vee b'] \wedge [b \vee b' \;\Rightarrow\; (b \;\Rightarrow\; S.Y)] \wedge [b \vee b' \;\Rightarrow\; \wedge (b' \;\Rightarrow\; S'.Y)]$$
$\equiv\cdot\cdot$ CP: $[A \;\Rightarrow\; A] \equiv Cierto$, $[A \;\Rightarrow\; (B \;\Rightarrow\; C) \equiv A \wedge B \;\Rightarrow\; C]$
$$Cierto \wedge [(b \vee b') \wedge b \;\Rightarrow\; S.Y)] \wedge [(b \vee b') \wedge b' \;\Rightarrow\; S'.Y]$$
$\equiv\cdot\cdot$ absorción: $[(b \vee b') \wedge b \equiv b]$
$$[b \;\Rightarrow\; S.Y)] \wedge [b' \;\Rightarrow\; S'.Y)]$$

Obsérvese que hemos obtenido la siguiente identidad para la semántica de Dijkstra:

$$\{b \vee b'\}[\![\, b \to S \,\square\, b' \to S' \,]\!]\{Y\} \equiv \{b\}S\{Y\} \wedge \{b'\}S'\{Y\} \qquad (**)$$

de donde la regla, en el sentido de Dijkstra, es válida así como su inversa.

---

2 Prueba en $\mathcal{LH}$ el triplete $\{C\}[\![\, C \to x := 1 \,\square\, C \to x := 2 \,]\!]\{x = 1 \vee x = 2\}$

SOL Es suficiente construir un árbol de derivación en $\mathcal{LH}$:

$$\dfrac{\dfrac{[C \;\Rightarrow\; 1 = 1 \vee 1 = 2] \qquad \dfrac{}{\{1 = 1 \vee 1 = 2\}x := 1\{x = 1 \vee x = 2\}}\,(asig)}{\{C\}x := 1\{x = 1 \vee x = 2\}}\,(ref) \qquad \dfrac{\ldots}{\{C\}x := 2\{x = 1 \vee x = 2\}}\,(ref)}{\{C\}[\![\, C \to x := 1 \,\square\, C \to x := 2 \,]\!]\{x = 1 \vee x = 2\}}\,(selec)$$

Obsérvese que es necesario usar refinamiento para inferir el triplete $\{C\}x := 1\{x = 1 \vee x = 2\}$.

---

3 ¿Es posible inferir en $\mathcal{LH}$ el triplete $\{C\}[\![\, C \to x := 1 \,\square\, C \to x := 2 \,]\!]\{x = 1\}$?

SOL Probemos que no es inferible en $\mathcal{LH}$ por reducción al absurdo. Si fuera inferible, por la ecuación $(**)$ del apartado 1, se tendría también $[C \;\Rightarrow\; x := 2.(x = 1)]$, pero esto es falso, ya que $[x := 2.(x = 1) \equiv Falso]$.

---

4 Prueba que la precondición más débil para que el cuerpo del bucle $*[\![x > 0 \to x := x-1 \,\square\, x > 2 \to x := x-3]\!]$ se ejecute a lo sumo 1000 veces es $x \leq 1000$, y para ello prueba por inducción en $\mathbb{N}$ la siguiente propiedad:

$$\forall k : k \in \mathbb{N} : [H^k.C \equiv x \leq k] \qquad (*)$$

SOL Procedemos por inducción sobre k. El caso base ($k = 0$) es trivial ya que $H^0.C$ es por definición $Cierto \wedge \neg OB$, y la negación de las guardas es $\neg OB \equiv x \leq 0$. Veamos el paso inductivo; *ptle*:

$H^{k+1}.C$

$\equiv\because$ definición

$\neg OB \vee OB \wedge [\![x > 0 \to x := x-1 \,\square\, x > 2 \to x := x-3]\!].(H^k.C)$

$\equiv\because$ semántica selectiva, $[OB \equiv x > 0]$

$x \leq 0 \vee x > 0 \wedge (x > 0 \;\Rightarrow\; x := x-1.(H^k.C)) \wedge (x > 2 \;\Rightarrow\; x := x-3.(H^k.C))$

$\equiv\because$ Hipótesis de inducción

$x \leq 0 \vee x > 0 \wedge (x > 0 \;\Rightarrow\; x := x-1.(x \leq k)) \wedge (x > 2 \;\Rightarrow\; x := x-3.(x \leq k))$

$\equiv\because$ sustitución y CP: $[A \wedge (A \;\Rightarrow\; B \equiv A \wedge B]$

$x \leq 0 \vee x > 0 \wedge x-1 \leq k \wedge (x \leq 2 \vee x-3 \leq k)$

$\equiv\because$ CP

$x \leq 0 \vee 0 < x \leq k+1 \wedge (x \leq 2 \vee x \leq k+3)$

$\equiv\because$ aritmética, CP

$x \leq 0 \vee 0 < x \leq k+1$

$\equiv\because$ aritmética, CP

$x \leq k+1$

---

5 Justifica operacionalmente la propiedad $(*)$.

SOL El cuerpo del bucle decrementa x es 3 unidades, o en 1. Por tanto, x es un contador que en el peor de los casos (al elegir la primera guarda) se decrementa en una unidad. Luego para cada valor k inicial de x existe una ejecución que realiza k pasos, pero cualquier ejecución no dará más de k pasos ya que el valor inicial de x es una cota del número de pasos. Luego $H^k.C \equiv (x \leq k)$.

---

6 Utilizando $(*)$ prueba que el bucle siempre termina.

SOL Por definición tenemos que $\mathcal{R}.C = \exists k : k \geq 0 : H^k.C =^{\text{por el apartado anterior}} \exists k : k \geq 0 : x \leq k =^{\text{aritmética}} Cierto$, de donde $[\mathcal{R}.C \equiv Cierto]$ y el bucle siempre termina.

---

7 A través del teorema de los contadores y del teorema de invariantes, prueba la corrección del siguiente esquema:

$\{X, Y > 0\}$
$x, y := X, Y;$
$*[\![x > y \to x := x - y$
$\;\square\, x < y \to x, y := y, x]\!]$
$\{x = MCD(X, Y)\}$

(Ayuda:- Busca un contador de la forma $\alpha x + \beta y$).

SOL Para que $t \doteq \alpha x + \beta y$ sea un contador relativo al invariante I tendría que cumplirse:

$$1.[I \wedge b_i \;\Rightarrow\; S_i.I] \qquad 2.[I \wedge b_i \;\Rightarrow\; t > 0] \qquad 3.[I \wedge b_i \;\Rightarrow\; wdec(S_i, t)]$$

Para que se cumpla 2 basta tomar $\alpha, \beta > 0$ y $I \doteq x, y > 0 \wedge \ldots$. Veamos las restricciones que impone la condición 3:

$wdec(x := x - y, t)$

$\equiv\therefore$ Lema 6.43, def. de t, sustitución

$\alpha(x-y)+\beta y < \alpha x+\beta y$

$\equiv\therefore$ Simplificamos

$\alpha y > 0$

$\Leftarrow\therefore$ Aritmética, $I \equiv y > 0 \wedge \ \ldots$

$\alpha > 0 \wedge I$

Luego este caso no impone restricciones adicionales. Veamos el otro:

$wdec(x, y := y, x|t)$

$\equiv\therefore$ Lema 6.43, def. de t, sustitución

$\alpha y + \beta x < \alpha x + \beta y$

$\equiv\therefore$ Simplificamos

$(\alpha - \beta)(x - y) > 0$

$\Leftarrow\therefore$ Aritmética,

$x > y \wedge \alpha > \beta$.

Luego basta tomar $\alpha > \beta > 0$. Por ejemplo $t \doteq 3x + 2y$. Para probar que el bucle termina calculando $x = MCD(X, Y)$ debemos añadir a I otras condiciones. Por ejemplo, basta tomar $I \doteq = x, y > 0 \wedge MCD(X, Y) = MCD(x, y)$, ya que, si I fuera invariante, y si I es cierto antes del bucle, terminará satisfaciendo $I \wedge x = y \Rightarrow MCD(x, x) = MCD(X, Y) \wedge x > 0$, de donde $x = MCD(X, Y)$. Por otro lado es trivial que I se satisface antes del bucle, y que es invariante (véase el libro de texto, páginas 110,111,...