Apellidos: _____

E.T.S.I. Informática. Ordinario de Febrero 2009

Lenguajes de Programación (tercer curso)

Nombre: _____

Días de asistencia a clase en el parcial 3º: _ de 10

Puntos:	1	2	3	4	5	6	total
	1.5	1.5	1.5	1.5	1.5	1.5	10.0

Parciales { 1º: 1, 2 ; 2º: 3, 4 ; 3º: 5, 6 } Parciales | o | o | o |

---

1 Sea S un programa sano verificando $[S.(a \wedge b) \equiv Cierto]$; demuestra que entonces $[S.\neg b \equiv Falso]$. ¿Qué interpretación tiene?

La interpretación es ...

---

2 Escribe un programa S indeterminista satisfaciendo $[S.(x = 1) \equiv Cierto]$ $[S.(y = 1) \equiv Falso]$. Prueba que es indeterminista.

3 Sea el bucle $\mathcal{R} \doteq *[\![b \to nada \,\square\, b \to aborta]\!]$. Utilizando la semántica en términos de puntos fijos, demuestra $[\mathcal{R}.X \equiv \neg b \wedge X]$ (prueba y usa $[SI.\neg b = Falso]$).

¿Qué interpretación tiene?

¿Cambia la situación si sustituimos la sentencia *nada* por otra sentencia arbitraria?

---

4 Enuncia el Teorema de los Contadores Generalizados

Justifica la siguiente frase: "si t es un contador generalizado para un conjunto finito bien construido $\mathcal{C}$, entonces el número de pasos del bucle está acotado por el cardinal de $\mathcal{C}$.

E.T.S.I. Informática. Ordinario de Febrero 2009
Lenguajes de Programación (tercer curso)

APELLIDOS: _____

NOMBRE: _____

5 Sea el procedimiento recursivo

$$m = [\![\quad i > 10 \to i := i - 2 \\ \quad\quad i \leq 10 \to i := i + 3; m \,]\!]$$

Traza una llamada al procedimiento m para los valores iniciales de $i = 13, 12, 11, 10, 9, 8, \ldots$ ¿Qué puedes conjeturar sobre el comportamiento de m para estos valores?

SOL La siguiente tabla ilustra el resultado de la traza

valor inicial de i	13	12	11	10	9	8	7	6	5	...
valor final de i	11	10	9	11	10	9	11	10	9	...

La tabla anterior se va completando según valores decreciente; por ejemplo, para $i = 10$,

valor de i	sentencia a ejecutar13	comentario
10	m	sem. puntos fijos y semántica selectiva
10	$i := i + 3; m$	sem. asignación
13	m	sem. puntos fijos y semántica selectiva
13	$i := i - 2$	sem. asignación
11	$\square$	

de donde se conjetura $\forall k : k \leq 13 : \quad [\ i = k \wedge m.Z \quad \equiv \quad i = k \wedge \boxed{i := 9 + (k+1) \bmod 3}.Z\ ]$.
Probaremos lo anterior por inducción sobre $k \leq 13$.

CASOS BASE: $11 \leq k \leq 13$:

$\quad i = k \wedge m.Z$
$= \because 11 \leq k \leq 13$, sem. puntos fijos y semántica selectiva
$\quad i = k \wedge i := i - 2.Z$
$= \because$ def. sustitución, regla de Liebniz
$\quad i = k \wedge i := k - 2.Z$
$= \because$ def. sustitución, regla de Liebniz, $11 \leq k \leq 13 \ \Rightarrow\ 9 + (k+1) \bmod 3 = k - 2$
$\quad i = k \wedge i := 9 + (k+1) \bmod 3$

PASO INDUCTIVO: $k \leq 10$:

$\quad i = k \wedge m.Z$
$= \because k \leq 10$, sem. puntos fijos y semántica selectiva
$\quad i = k \wedge i := i + 3.m.Z$
$= \because$ def. sustitución
$\quad i := i + 3.(i = k + 3 \wedge m.Z)$
$= \because$ H.I. para $k + 3$, $k + 3 \leq 13$
$\quad i := i + 3.(i = k + 3 \wedge i := 9 + ((k+3) + 1) \bmod 3)$
$= \because$ def.sustitución, lema de sustitución
$\quad i = k \wedge i := 9 + (k + 3 + 1) \bmod 3)$
$= \because (k + 3 + 1) \bmod 3 = (k + 1) \bmod 3$, Leibniz
$\quad i = k \wedge i := 9 + (k+1) \bmod 3)$

OBSERVACIÓN: También se podría haber probado la fórmula

$$\forall k : k \leq 13 : \quad [\ i = k \wedge m.Z \quad \equiv \quad i = k \wedge i := 9 + (i+1) \bmod 3.Z\ ]$$

también por inducción; en ese caso el paso inductivo sería:

PASO INDUCTIVO: $k \leq 10$:

$\quad i = k \wedge m.Z$
$= \because k \leq 10$, sem. puntos fijos y semántica selectiva
$\quad i = k \wedge i := i + 3.m.Z$
$= \because$ def. sustitución

$i := i + 3.(i = k + 3 \wedge m.Z)$
$= \because$ H.I. $k + 3 \leq 13$
$i := i + 3.(i = k + 3 \wedge i := 9 + (i + 1) \bmod 3)$
$= \because$ def. sustitución
$i = k \wedge i := i + 3.i := 9 + (i + 1) \bmod 3$
$= \because$ Lema de sustitución
$i = k \wedge i := 9 + (i + 3 + 1) \bmod 3$
$= \because (i + 3 + 1) \bmod 3 = (i + 1) \bmod 3$, Leibniz
$i = k \wedge i := 9 + (i + 1) \bmod 3$

ESTUDIO DE PROCEDIMIENTOS GENÉRICOS DE LA FORMA:

$$m' = [\![\quad i > \alpha \to S \\ \qquad i \leq \alpha \to i := i + \beta; m']\!]$$

donde $\beta(> 0)$ y α son enteros, y en la sentencia S no aparece m'.

En primer lugar veamos que podemos simplificar el estudio si sustituimos S por la sentencia *nada*. Más concretamente, veamos que m' tiene la misma semántica que $m; S$ donde m está dado por

$$m = [\![\quad i > \alpha \to nada \\ \qquad i \leq \alpha \to i := i + \beta; m]\!]$$

En efecto: Sabemos que $m.Z$ es el menor punto fijo de la ecuación en Y:

$$[Y \equiv i > \alpha \wedge Z \vee i \leq \alpha \wedge i := i + \beta.Y] \qquad (1)$$

Además, $m'.Z$ es el menor punto fijo de la ecuación en Y':

$$[Y' \equiv i > \alpha \wedge S.Z \vee i \leq \alpha \wedge i := i + \beta.Y'] \qquad (2)$$

De la misma forma que $m.Z$ satisface (1), tenemos que $m.(S.Z)$ satisface la equivalencia:

$$[m.(S.Z) \equiv i > \alpha \wedge (S.Z) \vee i \leq \alpha \wedge i := i + \beta.m.S.Z]$$

de donde, $m.S.Z$ es solución de (2), de donde obtenemos $[m'.Z \ \Rightarrow \ m.S.Z]$. La implicación recíproca se prueba en forma parecida: $m'.Z$ es solución de la ecuación

$$[Y \equiv i > \alpha \wedge S.Z \vee i \leq \alpha \wedge i := i + \beta.Y] \qquad (1')$$

cuya menor solución es $m.(S.Z)$, de donde $[m.S.Z \ \Rightarrow \ m'.Z]$. En definitiva $[m'.Z \equiv m.S.Z]$, y podemos reducir el estudio de m' al de m.

Ahora consideremos la traza del procedimiento m para valores descendentes de i:

valor inicial de i	$\alpha+\beta$	$\alpha+\beta-1$	$\ldots$	$\alpha+1$	α	$\alpha-1$	$\ldots$	$\alpha-\beta+1$	$\alpha-\beta$	$\alpha-\beta-1$	$\ldots$
valor final de i	$\alpha+\beta$	$\alpha+\beta-1$	$\ldots$	$\alpha+1$	$\alpha+\beta$	$\alpha+\beta-1$	$\ldots$	$\alpha+1$	$\alpha+\beta$	$\alpha+\beta-1$	$\ldots$

Oservamos el ciclo de valores finales $\alpha+\beta, \alpha+\beta-1, \ldots, \alpha+1$, de donde podemos conjeturar que el comportamiento de m es el mismo que el de la sentencia $i := \alpha + 1 + (i - \alpha - 1) \bmod \beta$ para valores $i \leq \alpha + \beta$. Es decir:

$$\forall k : k \leq \alpha + \beta : \qquad [\ i = k \wedge m.Z \qquad \equiv \qquad i = k \wedge i := \alpha + 1 + (i - \alpha - 1) \bmod \beta]$$

La demostración es similar a la prueba anterior, o sea, por inducción sobre $k \leq \alpha + \beta$.
CASOS BASE: $\alpha + 1 \leq k \leq \alpha + \beta$:

$i = k \wedge m.Z$
$= \because \alpha + 1 \leq k \leq \alpha + \beta$, sem. puntos fijos y semántica selectiva
$i = k \wedge nada.Z$
$= \because$ def. sustitución, regla de Liebniz
$i = k \wedge i := i.Z$

$= \because$ def. sustitución, regla de Liebniz, $\alpha+1 \leq i \leq \alpha+\beta \;\Rightarrow\; 0 \leq i-\alpha-1 \leq \beta-1 \;\Rightarrow\; \alpha+1+(i-\alpha-1) \bmod \beta = i$
$i = k \wedge i := \alpha + 1 + (i - \alpha - 1) \bmod \beta$

PASO INDUCTIVO: $k \leq \alpha$:

$i = k \wedge m.Z$
$= \because$ $k \leq \alpha$, sem. puntos fijos y semántica selectiva
$i = k \wedge i := i + \beta.m.Z$
$= \because$ def. sustitución
$i := i + \beta.(i = k + \beta \wedge m.Z)$
$= \because$ H.I. para $k + \beta \leq \alpha + \beta$
$i := i + \beta.(i = k + \beta \wedge i := \alpha + 1 + (i - \alpha - 1) \bmod \beta)$
$= \because$ def.sustitución, lema de sustitución
$i = \beta \wedge i := i := \alpha + 1 + (i + \beta - \alpha - 1) \bmod \beta$
$= \because$ $(i + \beta - \alpha - 1) \bmod \beta = (i + \alpha - 1) \bmod \beta$, Leibniz
$i = k \wedge i := \alpha + 1 + (i - \alpha - 1) \bmod \beta$

Por ejemplo, el procedimiento definido en la forma:

$$m = [\![\quad i > 20 \to nada \\ \quad\quad i \leq 20 \to i := i + 6; m \,]\!]$$

tiene el comportamiento $\forall k : k \leq 26 : [\ i = k \wedge m.Z \equiv i = k \wedge i := 21 + (i - 21) \bmod 6]$ o lo que es lo mismo: $\forall k : k \leq 26 : [\ i = k \wedge m.Z \equiv i = k \wedge i := 21 + (i - 3) \bmod 6]$

y por tanto, el procedimiento

$$m' = [\![\quad i > 20 \to i := i + 6 \\ \quad\quad i \leq 20 \to i := i + 6; m' \,]\!]$$

tiene el siguiente comportamiento $\forall k : k \leq 26 : [\ i = k \wedge m.Z \equiv i = k \wedge i := 27 + (i - 3) \bmod 6]$

Los procedimientos definidos en la forma:

$$m' = [\![\quad i < \alpha \to S \\ \quad\quad i \geq \alpha \to i := i - \beta; m' \,]\!]$$

donde $\beta > 0$ se estudian en la misma forma si en la sentencia S no aparece m'.

---

6 Consideremos la lógica de Hoare estándar para un lenguaje sin bucles; es decir, con las reglas (ref), $(:=)$, $(;)$, (si) indeterminista. Interpreta y prueba la equivalencia:

$$\vdash_{\mathcal{H}} \{P\}S;T\{Q\} \qquad \Longleftrightarrow \qquad \exists Y :: \qquad \vdash_{\mathcal{H}} \{P\}S\{Y\} \wedge \vdash_{\mathcal{H}} \{Y\}P\{Q\}$$

Ejercicio complementario (puede sustituir al ejercicio 5)

Siendo A,B naturales positivos, sea el procedimiento para calcular el $mcm(A,B)$ (el mínimo común múltiplo de A y B)

$$f = \{x, y :\in \mathbb{N} \to [\![\quad \begin{array}{l} x < y \to f(x + A, y) \\ x > y \to f(x, y + B) \\ x = y \to m := x \,]\!] \, \} \end{array}$$

Probad: $[f(A,B).(m = mcm(A,B)]$

AYUDA. Probad por inducción sobre $(p,q) \in \mathbb{N}^+ \times \mathbb{N}^+$,

$$\forall p, q : p, q \in \mathbb{N}^+ : p, q \leq mcm(A,B) \wedge p \in A^\bullet \wedge q \in B^\bullet \;\Rightarrow\; [f(p,q).(m = mcm(A,B)]$$

utilizando las siguientes propiedades del mcm

(1) $a, b \leq mcm(a,b)$
(2) $mcm(a,b) = mcm(b,a)$
(3) $\alpha a < \beta b \leq mcm(a,b) \;\Rightarrow\; (\alpha + 1)a \leq mcm(a,b)$
(4) $\alpha a = \beta b \leq mcm(a,b) \;\Rightarrow\; \alpha a = mcm(a,b)$

NOTA. $A^\bullet$ denota los múltiplos postivos de A.