

PUNTUACIONES:

	A	B	C	D	total
1	1	.5	1	.5	3
2	1				1
3	.25	.25	.5	1.5	2.5
4	1.5				1.5
5	.25	.25	1.5		2

ACLARACIONES:

- ✓ ☐ quiero que se publique mi calificación.
- ✓ 2⁰ parcial: 3,4,5.
- ✓ Bajo petición, ofrecemos el bucle del apartado 3C por 0.5 puntos.

1 Sea el bucle $\mathcal{R} \doteq * \llbracket x > 0 \rightarrow x := x - 1 \square x > 0 \rightarrow x := x - 2 \rrbracket$, donde x es una variable entera.

A Utilizando la semántica inductiva de los bucles, prueba que $[C \equiv \mathcal{R}.C]$.

SOL Tenemos $\mathcal{R}.C = \exists k : k \geq 0 : H^k.C$. Probaremos por inducción que

$$\forall k : k \geq 0 : [H^k.C \equiv x \leq k]$$

El caso base es trivial ya que $[H^0.C \equiv C \wedge x \leq 0]$. El paso inductivo sería, para $k \geq 0$:

$$\begin{aligned}
 & H^{k+1}.C \\
 = & ! \text{ definición de } H^k, \text{ siendo SI el cuerpo del bucle} \\
 & H^0.C \vee SI.H^k.C \\
 = & ! \text{ Hipótesis de inducción} \\
 & x \leq 0 \vee SI.(x \leq k) \\
 = & ! \text{ semántica de selectiva} \\
 & x \leq 0 \vee x > 0 \wedge x := x - 1.(x \leq k) \wedge x := x - 2.(x \leq k) \\
 = & ! \text{ cálculo} \\
 & x \leq 0 \vee x > 0 \wedge x \leq k + 1 \wedge x \leq k + 2 \\
 = & ! \text{ cálculo} \\
 & x \leq k + 1
 \end{aligned}$$

Finalmente, $ptle, \mathcal{R}.C \equiv \exists k : k \geq 0 : H^k.C \equiv \exists k : k \geq 0 : x \leq k \equiv C_{ierto}$.

B Usando el apartado A, prueba $[C \equiv \mathcal{R}.(x \leq 0)]$.

SOL Ya que para todo bucle tenemos $[\mathcal{R}.X \equiv \mathcal{R}.(¬b \wedge X)]$, basta aplicar A, para obtener $[C \equiv \mathcal{R}.(x \leq 0)]$.

C Utilizando la semántica en términos de puntos fijos prueba $[x = 0 \equiv \mathcal{R}.(x = 0)]$, así como $[x < 0 \equiv \mathcal{R}.(x < 0)]$

SOL En términos de puntos fijos, $\mathcal{R}.X$ es la menor solución de la ecuación (en Y):

$$Y \equiv \neg b \wedge X \vee b \wedge SI.Y$$

En particular:

$$\mathcal{R}.(x = 0) \text{ es la menor solución de: } Y_1 \equiv x = 0 \vee x > 0 \wedge SI.Y_1$$

$$\mathcal{R}.(x < 0) \text{ es la menor solución de: } Y_2 \equiv x < 0 \vee x > 0 \wedge SI.Y_2$$

Para la primera ecuación tenemos que toda solución es más débil que $x = 0$, luego basta probar que $SI.(x = 0)$ es idénticamente falso. En efecto:

$$\begin{aligned}
 & SI.(x = 0) \\
 = & ! \text{ semántica de selectiva} \\
 & x > 0 \wedge x := x - 1.(x = 0) \wedge x := x - 2.(x = 0) \\
 = & ! \text{ cálculo} \\
 & x > 0 \wedge x = 1 \wedge x = 2 \\
 = & ! \text{ cálculo} \\
 & \text{Falso}
 \end{aligned}$$

Para la segunda ecuación razonamos exactamente igual.

D Deduce de los apartados B y C que \mathcal{R} es indeterminista.

SOL En efecto, por los apartados B y C tenemos, *ptle*:

$$\mathcal{R}.(x = 0) \equiv x = 0, \quad \mathcal{R}.(x < 0) \equiv x < 0, \quad \mathcal{R}.(x \leq 0) \equiv \text{Cierta}$$

y en definitiva tenemos:

$$\mathcal{R}.(x = 0) \vee \mathcal{R}.(x < 0) \equiv x \leq 0 \not\equiv \text{Cierta} \equiv \mathcal{R}.(x = 0 \vee x < 0)$$

de donde el transformador \mathcal{R} no es disyuntivo y por tanto es indeterminista.

2 Consideremos el cálculo de Hoare estándar, con las reglas (ref) , $(nada)$, $(;)$, (si_1) , (si_2) y (rep) . Demuestra que si $\vdash_{\mathcal{H}} \{P\}nada\{Q\}$, entonces $[P \Rightarrow Q]$, indicando qué técnica utilizas para ello.

SOL Utilizamos inducción sobre la derivación del triplete $\vdash_{\mathcal{H}} \{P\}nada\{Q\}$. Tal triplete solamente puede obtenerse a partir de dos reglas: (ref) y $(nada)$. El caso base corresponde a la regla $(nada)$, que es trivial, ya que si $\vdash_{\mathcal{H}} \{P\}nada\{Q\}$ ha sido inferido de tal regla, entonces $P \equiv Q$. El paso inductivo corresponde a la regla (ref) , y si el triplete original ha sido inferido de tal regla es que teníamos en el antecedente de la regla:

$$[P \Rightarrow P'] \wedge \vdash_{\mathcal{H}} \{P'\}nada\{Q'\} \wedge [Q' \Rightarrow Q]$$

\Rightarrow ! hipótesis de inducción

$$[P \Rightarrow P'] \wedge [P' \Rightarrow Q'] \wedge [Q' \Rightarrow Q]$$

\Rightarrow ! transitividad de \Rightarrow

$$[P \Rightarrow Q]$$

3 Siendo b una variable entera, se considera la sentencia *incb* con el siguiente transformador de predicados, *ptle*:

$$incb.Z \doteq \forall i : i \geq 0 : b := b + 2i.Z$$

A Prueba alguno de los siguientes tripletes, indicando a la derecha su significado con una pequeña frase:

$$\begin{array}{ll} \{C\}incb\{C\} & \text{significa: } incb \text{ siempre termina} \\ \{b = k\}incb\{b - k \text{ par } \geq 0\} & \text{significa: } incb \text{ incrementa } b \text{ es un valor par no negativo} \end{array}$$

SOL Por definición $[incb.C \equiv C]$, de donde tenemos el primer triplete. Para probar el segundo tenemos:

$$incb.(b - k \text{ par } \geq 0) \equiv \forall i : i \geq 0 : b := b + 2i.(b - k \text{ par } \geq 0) \equiv \forall i : i \geq 0 : b + 2i - k \text{ par } \geq 0 \Leftarrow b = k$$

B Prueba que la sentencia *incb* tiene indeterminismo acotado, y por tanto no es continua.

SOL En efecto. Vemos que $\forall k.k \geq 0.[F \equiv incb.(b \leq k)]$, además de $[C \equiv incb.C]$, y $\forall k.k \geq 0.[F \equiv incb.(b = k)]$

C Utilizando la sentencia *incb* y un bucle, escribe un programa para simular el siguiente juego. Una urna contiene inicialmente 3 bolas rojas y 3 blancas; si el número de bolas de la urna es inferior a dos, termina el juego; si es mayor que uno, se extraen dos bolas, y posteriormente se realizan las siguientes acciones, hasta conseguir que el número de bolas sea menor que dos:

- a.- si son de distinto color, añadimos a la urna un número impar de bolas blancas.
- b.- no se añade nada si son del mismo color.

SOL

$$\begin{array}{l} b, r : \in \mathbb{Z}; b, r := 3, 3; \\ * \llbracket \begin{array}{ll} r > 0 \wedge b > 0 & \rightarrow r := r - 1; b := b - 1; incb \\ r > 1 & \rightarrow r := r - 2 \\ b > 1 & \rightarrow b := b - 2 \end{array} \rrbracket \end{array}$$

[D] Utilizando el teorema de los contadores, prueba que el programa anterior termina sólo débilmente (o sea el juego termina) y al final del juego, la urna contiene exactamente una única bola blanca.

[SOL] Consideremos el predicado $I \doteq b \text{ impar} \wedge b, r \geq 0$. Es fácil ver que es un invariante y que la función $t \doteq (r, b)$ es un contador para el conjunto bien construido $\mathbb{N} \times \mathbb{N}$ con el orden lexicográfico. En efecto: es evidente que I asegura directamente $t \in \mathbb{N} \times \mathbb{N}$. Para ver la invarianza y el decremento de t veamos únicamente el efecto de la primera sentencia del bucle:

$r := r - 1; b := b - 1; incb.((r, b) < t_0 \wedge b \text{ impar} \wedge b \geq 0 \wedge r \geq 0)$
 $= !$ semántica de composición y definición de $incb$
 $r := r - 1. b := b - 1. \forall i : i \geq 0 : b := b + 2i. ((r, b) < t_0 \wedge b \text{ impar} \wedge b \geq 0 \wedge r \geq 0)$
 $= !$ sustitución
 $r := r - 1. b := b - 1. \forall i : i \geq 0 : (r, b + 2i) < t_0 \wedge b + 2i \text{ impar} \wedge b + 2i \geq 0 \wedge r \geq 0$
 $= !$ sustitución
 $r := r - 1. \forall i : i \geq 0 : (r, b - 1 + 2i) < t_0 \wedge b - 1 + 2i \text{ impar} \wedge b - 1 + 2i \geq 0 \wedge r \geq 0$
 $= !$ sustitución
 $\forall i : i \geq 0 : (r - 1, b - 1 + 2i) < t_0 \wedge b - 1 + 2i \text{ impar} \wedge b - 1 + 2i \geq 0 \wedge r - 1 \geq 0$
 $\Leftarrow !$ cálculo, orden lexicográfico
 $(r, b) = t_0 \wedge r > 0 \wedge b > 0 \wedge I(\equiv b \text{ impar} \wedge \dots)$

Por otro lado, tenemos trivialmente: $\{C\}b, r := 3, 3; \{I\}$, y por el teorema de los contadores tendremos también: $\{I\}b, r := 3, 3; \mathcal{R}\{I \wedge \neg OB\}$. Pero

$I \wedge \neg OB$
 \Rightarrow
 $b \text{ impar} \wedge 0 \leq b, r \leq 1 \wedge (r \leq 0 \vee b \leq 0)$
 \equiv
 $b \text{ impar} \wedge 0 \leq b, r \leq 1 \wedge (r = 0 \vee b = 0)$
 \Rightarrow
 $r = 0 \wedge b = 1$

de donde el programa termina con la última bola blanca. Termina solo débilmente ya que no es posible acotar el número de pasos del bucle, ya que una ejecución adecuada de la primera secuencia con guardas exige posteriormente un número de ciclos mayor que cualquier número natural.

4 Sean las definiciones

$$\begin{aligned}
 u &: \in \mathbb{N} \\
 xfact &= \{n, x : \in \mathbb{N} \rightarrow \\
 &\quad \llbracket n = 0 \rightarrow x := 1 \sqcap n > 0 \rightarrow xfact(n - 1, x); x := x * n \rrbracket \}
 \end{aligned}$$

Utilizando la semántica (por nombre) vía puntos fijos de las llamadas a procedimientos, demostrar que se cumple $\forall N : N \in \mathbb{N} : \forall u : u \in \mathbb{N} : [xfact(N, u).(u = N!)]$. (AYUDA.– Inducción sobre N).

[SOL] Sea Z un predicado arbitrario, y sea el predicado $p(N) \doteq \forall u : u \in \mathbb{N} : [xfact(N, u).Z \equiv u := N!.Z]$. Basta probar por inducción sobre N ,

$$\forall N : N \in \mathbb{N} : p(N) \quad (*)$$

donde N varía dentro de los naturales. El caso base corresponde a $N = 0$, y tendremos, para $u : \in \mathbb{N}$:

$xfact(0, u).Z$
 $= !$ semántica por nombre
 $0, u \in \mathbb{N} \wedge \llbracket 0 = 0 \rightarrow u := 1 \sqcap 0 > 0 \rightarrow xfact(0 - 1, u); u := u * 0 \rrbracket .Z$
 $= !$ semántica selectiva
 $0, u \in \mathbb{N} \wedge u := 1.Z$
 $= !$ por la declaración de u , además de $0! = 1$
 $u := 0!.Z$

Veamos ahora el paso inductivo, para $N > 0$:

$xfact(N, u).Z$
 $= !$ semántica por nombre
 $N, u \in \mathbb{N} \wedge \llbracket N = 0 \rightarrow u := 1 \sqcap N > 0 \rightarrow xfact(N - 1, u); u := u * N \rrbracket .Z$
 $= !$ semántica selectiva, $N > 0$, además de $N, u \in \mathbb{N}$
 $xfact(N - 1, u).(u := u * N.Z)$
 $= !$ por hipótesis de inducción
 $u := (N - 1)!.(u := u * N.Z)$
 $= !$ semántica de la asignación y composición
 $u := (N - 1)! * N.Z$
 $= !$ definición de $x!$
 $u := N!.Z$

Ahora aplicamos $(*)$ y tendremos, para $u, N \in \mathbb{N}$:

$xfact(N, u).(u = N!)$
 $= !$ por $(*)$, tomando $Z \doteq (u = N!)$
 $u := N!.(u = N!)$
 $= !$ sustitución
 $N! = N!$
 $= !$
Cierto

5 **A** Dar la definición de triplete en sentido operacional $\vdash_{\mathcal{O}} \{X\}S\{Y\}$ para la semántica natural estándar $\Rightarrow_{\mathcal{N}}$.

SOL

$$\vdash_{\mathcal{O}} \{X\}S\{Y\} \doteq \forall \rho, \rho' : X.\rho \wedge (\rho, S) \Rightarrow_{\mathcal{N}} \rho' : Y.\rho'$$

B Dar la definición de invariante del bucle $\mathcal{R} \doteq * \llbracket b \rightarrow S \rrbracket$, en sentido operacional

SOL Un predicado I es un invariante del bucle \mathcal{R} si verifica: $\vdash_{\mathcal{O}} \{I \wedge b\}S\{I\}$

C Enunciar y demostrar el teorema de invariantes para la semántica operacional estándar.

SOL El enunciado sería: si I es un invariante de \mathcal{R} , entonces se verifica el triplete $\vdash_{\mathcal{O}} \{I\}\mathcal{R}\{I \wedge \neg b\}$.

Para la demostración, teniendo en cuenta la definición de triplete, hemos de probar

$$\forall \rho, \rho' : I.\rho \wedge (\rho, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho' : (I \wedge \neg b).\rho'$$

por inducción sobre la derivación $(\rho, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho'$. Teniendo en cuenta las reglas de la relación $\Rightarrow_{\mathcal{N}}$, tal derivación solamente puede obtenerse vía dos reglas:

$$(R_1) \frac{b.\rho \quad (\rho, S) \Rightarrow_{\mathcal{N}} \tau \quad (\tau, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho'}{(\rho, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho'} \quad (R_2) \frac{\neg b.\rho}{(\rho, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho}$$

Si hubiera sido obtenida por la segunda, tendríamos:

$$I.\rho \wedge \neg b.\rho \wedge \rho \equiv \rho' \Rightarrow (I \wedge \neg b).\rho, \text{ que es lo buscado.}$$

Si hubiera sido obtenida de la primera regla, tendríamos:

$$\begin{aligned}
 & I.\rho \wedge (\rho, S) \Rightarrow_{\mathcal{N}} \tau \wedge b.\rho \wedge (\tau, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho' \\
 & \Rightarrow \quad ! \text{ por ser } I \text{ invariante, } (I.\rho \wedge b.\rho \wedge (\rho, S) \Rightarrow_{\mathcal{N}} \tau) \Rightarrow I.\tau \\
 & I.\tau \wedge (\tau, \mathcal{R}) \Rightarrow_{\mathcal{N}} \rho' \\
 & \Rightarrow \quad ! \text{ hipótesis de inducción} \\
 & (I \wedge \neg b).\rho'
 \end{aligned}$$