Transformadores de Predicados y Semántica de Programas

A la memoria de mi padre,
Manuel Ruiz Hoyos,
sencillo matemático y gran Profesor.

A mi nieto recién nacido,
Manuel Ruiz Sánchez,
con el deseo de que complete la
cuarta generación de matemáticos.

Blas C. Ruiz Jiménez

Blas Carlos Ruiz Jiménez

Profesor Titular de Universidad
Departamento de Lenguajes y Ciencias de la Computación

E.T.S.I. Informática. Universidad de Málaga

Transformadores de Predicados

y Semántica de Programas

(Corrección de la 2ª Ed. – Setiembre de 2003)

Málaga, Octubre de 2010

IMPRIME: *IMAGRAF–Impresores.*
C/Nabuco, Nave 14-D. 29006–Málaga. Tel.: 2328597

I.S.B.N.: **84-607-5971-7**
Depósito Legal: MA-1203-2003

Composición realizada por el autor en $\LaTeX 2\epsilon$.

Índice general

Índice de figuras

Capítulo 12

Soluciones a los Ejercicios

3.5 [44] Supongamos $S = S'$ entonces, $\forall \iota, \sigma : \iota, \sigma \in \mathcal{E}$:

$$\begin{array}{ll} & \{P^\iota\}S\{P^\sigma\} \\ = & \quad \because \text{definición de triplete} \\ & [P^\iota \;\Rightarrow\; S.P^\sigma] \\ = & \quad \because S = S' \\ & [P^\iota \;\Rightarrow\; S'.P^\sigma] \\ = & \quad \because \text{definición de triplete} \\ & \{P^\iota\}S'\{P^\sigma\} \end{array}$$

La interpretación es fácil: ya que el predicado P^ι solamente es verificado por el estado ι, partiendo de tal estado, si vía S el estado final es σ, entonces, vía S' también el estado final debe ser σ.

3.10 [46] Calculemos según la definición de triplete y suponiendo que S es sana

$$\begin{array}{ll} & \{Falso\}S\{X\} \\ = & \quad \because \text{definición de triplete} \\ & [Falso \;\Rightarrow\; S.X] \\ = & \quad \because \text{CP} \\ & Cierto \end{array}$$

$$\begin{array}{ll} & \{P\}S\{Falso\} \\ = & \quad \because \text{definición de triplete} \\ & [P \;\Rightarrow\; S.F] \\ = & \quad \because S \text{ es estricta} \\ & [P \;\Rightarrow\; F] \\ = & \quad \because \text{CP} \\ & [\neg P] \end{array}$$

Por tanto, el segundo triplete solo es cierto cuando $[P \equiv Falso]$, y la interpretación es muy simple: si S termina debe hacerlo en algún estado (es la interpretación de la *Ley del Milagro Excluido*.

3.18 [49] Sea S sano y disyuntivo. Probaremos la propiedad de unicidad de los estados finales por reducción al absurdo. Sea un estado inicial ι para el cual S termina en al menos dos estados distintos. Consideremos el conjunto Σ de estados finales para ι. Entonces tendremos:

$$\begin{array}{ll} & Cierto \\ = & \quad \because \Sigma \text{ es el conjunto de los posibles estados finales para } \iota \\ & (S.(\bigvee_{\sigma\in\Sigma} P^\sigma)_\iota \\ = & \quad \because S \text{ es disyuntivo} \\ & \bigvee_{\sigma\in\Sigma}(S.P^\sigma)_\iota \\ = & \quad \because (S.P^\sigma)_\iota \text{ es falso: no garantizo que } S \text{ termine en } \sigma \text{ partiendo de } \iota \\ & Falso \end{array}$$

3.19 [49] Si S no es disyuntivo, existen predicados A y B, y un estado ι tales que

$$(S.A)_\iota \vee (S.B)_\iota \not\equiv (S.(A \vee B))_\iota.$$

Por ello, los posibles valores de tales predicados son

$(S.A)_\iota$	$(S.B)_\iota$	$(S.(A \vee B))_\iota$
C	F	F
F	C	F
C	C	F
F	F	C

Por ser S es monótono ($[S.A \vee S.B \;\Rightarrow\; S.(A \vee B)]$), solo es posible que se den los valores de la última línea de la tabla anterior; es decir:

$$(S.A)_\iota \equiv Falso \qquad (S.B)_\iota \equiv Falso \qquad (S.(A \vee B))_\iota \equiv Cierto$$

Por esto último, partiendo de ι, S termina; pero no podemos asegurar que el estado final sea único; si lo fuera, éste verificaría $A \vee B$, pero esto no es posible, ya que $(S.A)_\iota \equiv (S.B)_\iota \equiv Falso$.

3.23 [50] (Véase también la Nota 4.1) Si tomamos

$$S \;\doteq\; [\![\, b \to aborta \,\square\, C \to nada \,]\!]$$

entonces $S^*.(\neg b) \equiv C$, y $\hat{S}.(\neg b) \equiv \neg b$, y son distinguibles.

3.24 [50] Tenemos que $[U.F \equiv b]$, y por tanto U no es estricta; si fuera $[U.F \equiv F]$, entonces debería tenerse $[b \equiv F]$, de donde $U = S$, y sería una sentencia sana.

4.6 [59] ¡No! ya que la variable t queda alterada, y tenemos, por ejemplo

$$\begin{array}{lcl} \{t = 1 \wedge x = 2 \wedge y = 3\} & t := x; x := y; y := t & \{t = 2\} \\ \{t = 1 \wedge x = 2 \wedge y = 3\} & x, y := y, x & \{t = 1\} \end{array}$$

de donde las sentencias son distinguibles.

4.10 [61] Supongamos que E dependa únicamente de a y b (cualquier otra dependencia no afecta al siguiente razonamiento). Entonces, *ptle*, debería tenerse

$$\begin{array}{ll} & a := a + 1; b := E(a, b).a = b \\ = & \quad \because \text{semántica asignación dos veces} \\ & E(a + 1, b) = a + 1 \\ = & \\ & Cierto \end{array}$$

luego $[E(a + 1, b) = a + 1]$, y por ello E no depende de b y tomamos $E(a) \equiv a$. Obsérvese que el razonamiento sirve si eliminamos la sentencia $a := a + 1$.

4.12 [61] AYUDA.- Sea un predicado $E(x, y, z)$ arbitrario que dependa únicamente de las variables x, y y z (esta suposición es suficiente ya que si E dependiera de otras variables, en la propiedad de $inter(x, y)$ podríamos tomar cada una de tales variables). Estudiad – por inducción – tripletes de la forma

$$\{E(a, b, c)\}inter(x, y)\{E(b, a, c)\}$$

4.13 [61] Sea X un predicado arbitrario; entonces, *ptle*

$$
\begin{aligned}
& (S;T)^*.X \\
= & \quad \because \text{Definición 3.20} \\
& \neg(S;T).(\neg X) \\
= & \quad \because \text{semántica composición} \\
& \neg S.(T.(\neg X)) \\
= & \quad \because \text{doble negación} \\
& \neg S.(\neg\neg T.(\neg X)) \\
= & \quad \because \text{Definición 3.20} \\
& \neg S.(\neg T^*.X) \\
= & \quad \because \text{Definición 3.20} \\
& S^*.(T^*.X) \\
= & \quad \because \text{semántica composición} \\
& S^*;T^*.X
\end{aligned}
$$

4.15 [61] Si S es sana, la función $X \longmapsto (b \Rightarrow S.X)$ es conjuntiva en X, pero no es estricta en general, ya que $[(b \Rightarrow S.F) \equiv \neg b]$.

4.16 [61] No existe tal expresión, ya que si $E \equiv E(a,b)$ depende de a y b, tenemos

$$
\begin{aligned}
& b := N.a := E.(N > \text{máx}(a,b)) \\
= \; & b := N.(N > \text{máx}(E(a,b),b)) \\
= \; & N > \text{máx}(E(a,N),N) \\
= \; & Falso
\end{aligned}
$$

4.17 [61] Probaremos que si S es sana, la sentencia $T \doteq \langle\langle b \to S\rangle\rangle$, en general, NO se puede implementar en el lenguaje de Dijkstra ya que T es estricta, pero no es necesariamente conjuntiva. Para probarlo sea $T \doteq \langle\langle x = 2 \to x := x - 1\rangle\rangle$, $A \doteq x > 1$; entonces

$$
\begin{aligned}
& T.A \wedge T.\neg A \\
= & \quad \because \text{definición, cálculo, } S \text{ conjuntiva, LME} \\
& b \wedge \neg A \wedge S.A \vee b \wedge A \wedge S.\neg A \\
= & \quad \because \text{en nuestro caso particular} \\
& x = 2 \wedge (x \leq 1 \wedge x > 2 \vee x > 1 \wedge x \leq 2) \\
= & \quad \because \text{CP} \\
& x = 2
\end{aligned}
$$

En general, T no es conjuntiva si S determinista con $[S.C \equiv C]$ (hágase como ejercicio, aplicando el Teorema 3.21(iii): $[S.\neg A \equiv \neg S.A]$).

4.19 [63] $\mathcal{S}.X \overset{\text{semántica}}{\equiv} y := 1.x := 1.X \wedge y := 0.x := 1.X$, de donde , *ptle*,

$$\mathcal{S}.(y = 1) \equiv Falso \qquad \mathcal{S}.(y = 0) \equiv Falso \qquad \mathcal{S}.(y = 1 \vee y = 0) \equiv Cierto$$

y por tanto

$$\mathcal{S}.(y = 1 \vee y = 0) \not\equiv \mathcal{S}.y = 1 \vee \mathcal{S}.y = 0$$

Además, $[\mathcal{S}.(x = 1) \equiv Cierto]$, de donde $\{C\}\mathcal{S}\{x = 1\}$.

4.22 [65]

$SI.m > a$

$$
\begin{array}{ll}
= & \because \text{semántica selectiva} \\
& OB \wedge (a > b \Rightarrow m := a.m > a) \wedge (a < b \Rightarrow m := b.m > a) \wedge \\
& (a = b \Rightarrow nada.m > a) \\
= & \because \text{semántica asignación y nada} \\
& C \wedge (a > b \Rightarrow a > a) \wedge (a < b \Rightarrow b > a) \wedge (a = b \Rightarrow m > a) \\
= & \because \text{CP} \\
& C \wedge a \leq b \wedge C \wedge (a \neq b \vee m > a) \\
= & \because \text{CP} \\
& a < b \vee a \leq b \wedge m > a \\
\Leftarrow & \\
& a < b
\end{array}
$$

4.23 [65] Tenemos que $OB \equiv x \neq 0 \wedge x \neq 1$. Además

$$
\begin{array}{ll}
& SI.x \neq 0 \\
= & \because \text{semántica selectiva} \\
& x \neq 0 \wedge x \neq 1 \\
\wedge & x < 0 \Rightarrow x := -x.x \neq 0 \\
\wedge & x > 1 \Rightarrow x := x - 1.x \neq 0 \\
\wedge & x > 2 \Rightarrow x := x \div 2.x \neq 0 \\
= & \because \text{semántica asignación} \\
& x \neq 0 \wedge x \neq 1 \wedge (x \geq 0 \vee -x \neq 0) \wedge (x \leq 1 \vee x \neq 1) \\
\wedge & (x \leq 2 \vee x \div 2 \neq 0) \\
= & \because \text{CP} \\
& x \neq 0 \wedge x \neq 1
\end{array}
$$

y por tanto $[OB \equiv SI.x \neq 0]$. La interpretación es que para asegurar la terminación de la selectiva con $x \neq 0$ basta con que alguna guarda sea cierta.

4.28 [68] Véase Ejercicio 5.23.

4.29 [68] Los apartados (B) y (C) son triviales. AYUDA.– para el apartado (A): estudiad la siguiente sentencia

$$
\begin{array}{lllllll}
[\![& a & \rightarrow & [\![& \neg a & \rightarrow & x := 1 \\
& & & \Box & a & \rightarrow & x := 2]\!] \\
\Box & \neg a & \rightarrow & [\![& a & \rightarrow & x := 1 \\
& & & \Box & \neg a & \rightarrow & x := 2]\!] \quad]\!]
\end{array}
$$

Para el apartado (D) consideremos la sentencia $SI \doteq [\![b \rightarrow U \Box b \rightarrow U]\!]$, donde $U.Z \doteq (b \Rightarrow S.Z)$, y S sana. Entonces, SI es conjuntiva; además, U no es estricta, pero $SI.Z \equiv b \wedge S.Z$ es estricta.

4.33 [70] Utilizando la interpretación de la selectiva, podemos escribir, *ptle*

$$SI.X \doteq (\neg OB \Rightarrow S'.X) \wedge (\forall i : 1 \leq i \leq n : b_i \Rightarrow S_i.X)$$

4.36 [70] En efecto; si tomamos $[\![b \rightarrow S]\!]$, su transformador es T; además, es determinista si lo es S.

4.37 [70] Véase el Ejemplo 3.13:47.

4.38 [70] Por la semántica de la selectiva: $[SI.M \equiv x := 1.M \wedge x, y := 1, 0.M]$. Por tanto, $[SI.(x = 1) \equiv Cierto]$, lo que prueba el triplete $\{C\}SI\{x = 1\}$. Para probar que es indeterminista, tomamos los predicados $A \doteq y = 0, B \doteq y \neq 0$; entonces, tenemos, *ptle*

$$SI.A \equiv (x = 1), \qquad SI.B \equiv Falso, \qquad SI.(A \vee B) \equiv Cierto.$$

Por tanto, $SI.(A \vee B) \not\equiv SI.A \vee SI.B$, y SI resulta ser indeterminista.

4.39 [70] (A).— $[b \Rightarrow \neg S.C]$; un ejemplo es $[\![\neg b \rightarrow x := 1]\!]$.

(B).— $[X \Rightarrow S.\neg X]$; no existen ejemplos con S sano. Véase Ejemplo 3.13:47.

(C).— $[S.C \Rightarrow S.Y]$; un ejemplo es $S \doteq [\![x > 0 \rightarrow x := 0]\!]$ e $Y \doteq (x = 0)$.

(D).— $\neg[b \Rightarrow S.C]$; un ejemplo es $b \doteq x > 0$ y $S \doteq [\![x > 6 \rightarrow x := 1]\!]$.

4.40 [70] (A).— Véase el concepto de programa útil en página 48.

(B).— Hay que probar que para todo predicado X se verifica, *ptle*

$$\begin{array}{ll}
 & [\, [\![x > 1 \rightarrow nada \,\square\, x > 1 \rightarrow aborta]\!] .X \equiv aborta.X \,] \\
= & \quad \because \text{semántica selección, y definición de } aborta \\
 & [\, x > 1 \wedge nada.X \wedge aborta.X \equiv F \,] \\
= & \\
 & [F \equiv F]
\end{array}$$

(C).— Supongamos x una variable entera; entonces, *ptle*

$$\begin{array}{ll}
 & [\![x > 0 \rightarrow x := 2 \,\square\, x > 1 \rightarrow x := 3]\!] .(x = 2) \\
= & \quad \because \text{semántica selección} \\
 & x > 0 \wedge (x > 0 \Rightarrow x := 2.x = 2) \wedge (x > 1 \rightarrow x := 3.x = 2) \\
= & \quad \because \text{CP} \\
 & x > 0 \wedge 2 = 2 \wedge (x > 1 \rightarrow 3 = 2) \\
= & \quad \because \text{CP} \\
 & x > 0 \wedge x \leq 1 \\
= & \quad \because x \text{ es entera} \\
 & x = 1
\end{array}$$

Luego los estados para los que la sentencia termina verificando $x = 2$ vienen determinados por $x = 1$, si $x \in \mathbb{Z}$.

(D).— No necesariamente; por ejemplo si $[b \equiv Cierto]$ entonces

$$\begin{array}{ll}
 & [\![C \rightarrow \mathcal{S} \,\square\, \neg C \rightarrow \mathcal{S}']\!] .X \\
= & \quad \because \text{semántica selección} \\
 & C \wedge (C \Rightarrow \mathcal{S}.X) \wedge (F \Rightarrow \mathcal{S}'.X) \\
= & \quad \because \text{CP} \\
 & \mathcal{S}.X
\end{array}$$

Luego $[\![C \rightarrow \mathcal{S} \,\square\, \neg C \rightarrow \mathcal{S}']\!] = \mathcal{S}$, que es indeterminista si lo es $\mathcal{S}$.

5.8 [74] Por la regla de refinamiento, bastará probar, por inducción sobre la estructura de la sentencia,

$$\forall S : S \in \mathcal{P}rog : \vdash_{\mathcal{H}} \{Cierto\} S \{Cierto\}$$

— CASOS BASES :

(:=) sigue de $[x := a.C \equiv C]$.
$nada$ es trivial.

— PI 1 : COMPOSICIÓN

$$\begin{array}{ll} & \{C\}S;T\{C\} \\ \Leftarrow & \quad \because (;) \\ & \{C\}S\{C\}, \{C\}T\{C\} \\ \Leftarrow & \\ & HI \end{array}$$

— PI 2 : SELECTIVA

$$\begin{array}{ll} & \{C\}[\![\, b \to S \,\Box\, \neg b \to T \,]\!]\,\{C\} \\ \Leftarrow & \quad \because \text{regla selectiva} \\ & \{C \wedge b\}S\{C\} \wedge \{C \wedge \neg b\}T\{C\} \\ \Leftarrow & \quad \because \text{regla de refinamiento} \\ & \{C\}S\{C\} \wedge \{C\}T\{C\} \\ \Leftarrow & \\ & HI \end{array}$$

— PI 3 : BUCLE

$$\begin{array}{ll} & \{C\} * [\![\, b \to S \,]\!]\,\{C\} \\ \Leftarrow & \quad \because \text{regla de refinamiento} \\ & \{C\} * [\![\, b \to S \,]\!]\,\{b\} \\ \Leftarrow & \quad \because \text{regla del bucle} \\ & \{C \wedge b\}S\{b\} \\ \Leftarrow & \quad \because \text{regla de refinamiento} \\ & HI \end{array}$$

5.9 [74] El primero siempre es inferible (véase el Ejemplo 5.6). El segundo no necesariamente; por ejemplo, $\{x > 0\}x := 1\{Falso\}$ no se puede inferir en $\mathcal{LH}$; además, se puede demostrar:

$$\vdash_{\mathcal{H}} \{P\}S\{Falso\} \Longleftrightarrow [P \equiv Falso]$$

(hágase como ejercicio).

5.11 [74] Véase el Ejercicio 5.27.

5.23 [84] (A).— Por la semántica informal que nos dicen, deducimos la regla

$$\frac{\{P\}S\{X\} \qquad \{P\}T\{X\}}{\{P\}S \odot T\{X\}}$$

(B).— Según la semántica informal de $S \odot T$, *ptle*

$$\begin{array}{ll} & S \odot T.X \\ = & \\ & [\![\, C \to S \,\Box\, C \to T \,]\!]\,.X \\ = & \quad \because \text{semántica condicional} \\ & (C \Rightarrow S.X) \wedge (C \Rightarrow T.X) \\ = & \quad \because \text{CP} \\ & S.X \wedge T.X \end{array}$$

(C).— Por (B), $nada \odot nada \equiv nada$, que es determinista; además $U \doteq (f := Cierto) \odot (f := Falso)$ es indeterminista, ya que $[U.(f = C) \equiv F]$, $[U.(f = F) \equiv F]$ y $[U.C \equiv C]$, de donde U no es disyuntiva. Otro ejemplo de determinismo (indeterminismo) es $S \odot S$, si S es determinista (indeterminista).

5.24 [85] (A).— Consideremos las reglas de la Figura 5.0 eliminado las reglas de la selectiva y sustituyéndolas por la regla

$$\frac{\{b \wedge X\}S\{Y\} \qquad \{b' \wedge X\}S'\{Y\} \qquad [X \Rightarrow b \vee b']}{\{X\}[\![\, b \to S \,\Box\, b' \to S' \,]\!]\,\{Y\}}\ (si)$$

NOTA 12.0 *Si en la regla de la selectiva suprimimos el predicado* $[X \Rightarrow b \vee b']$*, entonces, como después veremos, el sistema no es correcto para la semántica de Dijkstra; por otro lado, si reemplazamos la regla de la selectiva por dos reglas, del estilo de*

$$\frac{\{b \wedge X\}S\{Y\}}{\{X\}[\![b \rightarrow S \,\Box\, b' \rightarrow S']\!]\{Y\}}$$

entonces el sistema no capturaría correctamente el indeterminismo, ya que podríamos derivar $\vdash_{\mathcal{H}} \{x = 1\}[\![x > 0 \rightarrow x := x + 1 \,\Box\, x > 0 \rightarrow x := x - 1]\!] \{x = 2\}$.

$\underline{(B)}$.— Por la regla de refinamiento, basta demostrar, $\forall S :: \vdash_{\mathcal{H}} \{C\}S\{C\}$, y esto último se prueba por inducción estructural sobre la sentencia. Todos los casos son iguales que los del Ejercicio 5.8, salvo el correspondiente a la selectiva:

$$\begin{array}{ll} & \vdash_{\mathcal{H}} \{C\}[\![b \rightarrow S \,\Box\, b' \rightarrow S']\!] \{C\} \\ \Leftarrow & \qquad \because \text{(si)} \\ & \{b\}S\{C\} \wedge \{b'\}S'\{C\} \wedge [C \Rightarrow b \vee b'] \\ \Leftarrow & \qquad \because \text{HI} \\ & [b \vee b'] \end{array}$$

Por tanto, tales tripletes serán válidos si consideramos solamente selectivas para las cuales siempre una guarda es cierta. En este caso, se puede suprimir el término $[X \Rightarrow b \vee b']$ en la regla (si).

$\underline{(C)}$.— El sistema del apartado (A) es completo si los tripletes derivables en la semántica de Dijkstra también son derivables en tal sistema; o sea :

$$\forall X, S, Y :: [X \Rightarrow S.Y] \Rightarrow \vdash_{\mathcal{H}} \{X\}S\{Y\}$$

$\underline{(D)}$.— Basta demostrar $\forall S, Y :: \vdash_{\mathcal{H}} \{S.Y\}S\{Y\}$, ya que entonces, tendremos

$$\begin{array}{ll} & [X \Rightarrow S.Y] \\ \Rightarrow & \qquad \because \text{regla de refinamiento, } \vdash_{\mathcal{H}} \{S.Y\}S\{Y\} \\ & \vdash_{\mathcal{H}} \{X\}S\{Y\} \end{array}$$

Demostraremos $\forall S, Y :: \vdash_{\mathcal{H}} \{S.Y\}S\{Y\}$ por inducción estructural sobre la sentencia. La prueba es igual que la prueba del Teorema 5.15:78, salvo el paso correspondiente a la selectiva:

$$\begin{array}{ll} & \vdash_{\mathcal{H}} \{SI.Y\}SI\{Y\} \\ \Leftarrow & \qquad \because \text{regla } (si) \\ & \vdash_{\mathcal{H}} \{b \wedge SI.Y\}S\{Y\} \wedge \vdash_{\mathcal{H}} \{b' \wedge SI.Y\}T\{Y\} \wedge [SI.Y \Rightarrow b \vee b'] \\ \Leftarrow & \qquad \because \text{regla de refinamiento, } SI.Y \equiv (b \vee b') \wedge (b \Rightarrow S.Y) \wedge (b' \Rightarrow T.Y) \\ & [b \wedge SI.Y \Rightarrow S.Y] \wedge \vdash_{\mathcal{H}} \{S.Y\}S\{Y\} \\ \wedge & [b' \wedge SI.Y \Rightarrow T.Y] \wedge \vdash_{\mathcal{H}} \{T.Y\}T\{Y\} \\ = & \qquad \because \text{por HI: los dos tripletes son derivables; } [b \wedge SI.Y \equiv b \wedge S.Y \wedge \ldots] \\ & Cierto \end{array}$$

$\underline{(E)}$.— El sistema del apartado (A) es correcto significa que los tripletes derivables en tal sistema son válidos en la semántica de Dijkstra; o sea :

$$\forall X, S, Y :: \vdash_{\mathcal{H}} \{X\}S\{Y\} \Rightarrow [X \Rightarrow S.Y]$$

(F).— Hay que demostrar, por inducción sobre la derivación,

$$\forall S, X, Y :: \vdash_{\mathcal{H}} \{P\}S\{Q\} \Rightarrow [P \Rightarrow S.Q]$$

La prueba es igual que la del Teorema 5.14, salvo el caso correspondiente a la selectiva,

$$\begin{array}{ll}
& \vdash_{\mathcal{H}} \{b \wedge X\}U\{Y\} \wedge \vdash_{\mathcal{H}} \{b' \wedge X\}V\{Y\} \wedge [X \Rightarrow b \vee b'] \\
\Rightarrow & \quad \because \text{HI} \\
& [b \wedge X \Rightarrow U.Y] \wedge [b' \wedge X \Rightarrow V.Y] \wedge [X \Rightarrow b \vee b'] \\
\Rightarrow & \quad \because \text{conjuntividad de } [\,], \text{cálculo} \\
& [X \Rightarrow (b \Rightarrow U.Y) \wedge (b' \Rightarrow V.Y) \wedge (b \vee b')] \\
= & \quad \because \text{semántica selectiva} \\
& [X \Rightarrow [\![\, b \rightarrow U \,\Box\, b' \rightarrow V \,]\!].Y]
\end{array}$$

5.25 [85] (A).—

$$\begin{array}{ll}
& \{P\}[\![\, b \rightarrow S \,\Box\, b \rightarrow T \,]\!]\{Q\} \\
= & \quad \because \text{def. de triplete} \\
& [P \Rightarrow [\![\, b \rightarrow S \,\Box\, b \rightarrow T \,]\!].Q] \\
= & \quad \because \text{semántica selección} \\
& [P \Rightarrow b \wedge (b \Rightarrow S.Q) \wedge (b \Rightarrow T.Q)] \\
= & \quad \because A \wedge (A \Rightarrow B) \equiv A \wedge B \\
& [P \Rightarrow b \wedge S.Q \wedge T.Q] \\
= & \quad \because (A \Rightarrow B \wedge C) \equiv (A \Rightarrow B) \wedge (A \Rightarrow C), \text{ conjuntividad de } [\,] \\
& [P \Rightarrow b] \wedge [P \Rightarrow S.Q] \wedge [P \Rightarrow T.Q] \\
= & \quad \because \text{def. de triplete} \\
& [P \Rightarrow b] \wedge \{P\}S\{Q\} \wedge \{P\}T\{Q\}
\end{array}$$

Obsérvese que al final se obtiene una equivalencia:

$$\{P\}[\![\, b \rightarrow S \,\Box\, b \rightarrow T \,]\!]\{Q\} \qquad \equiv \qquad [P \Rightarrow b] \wedge \{P\}S\{Q\} \wedge \{P\}T\{Q\}$$

(B).— $W.Q \overset{\text{semántica}}{\equiv} x > 0 \wedge x := 2.Q \wedge x := 4.Q$, de donde $\{P\}W\{Q\} = [P \Rightarrow x > 0 \wedge x := 2.Q \wedge x := 4.Q]$; luego

$$\begin{array}{lllll}
\{x > 1\}W\{x = 2\} & \equiv & [x > 1 \Rightarrow F] & \equiv & [x \leq 1] \;\equiv\; Falso \\
\{x > 1\}W\{x = 2 \vee x = 4\} & \equiv & [x > 1 \Rightarrow x > 0] & \equiv & Cierto
\end{array}$$

De la misma forma tenemos que el triplete $\{x > 1\}W\{x = 4\}$ es falso, y por tanto W es indeterminista.

(C).— Puesto que en (A) derivamos una igualdad, se puede aplicar la regla para calcular los tripletes anteriores; en general, tenemos

$$\begin{array}{ll}
& \{P\}[\![\, b \rightarrow S \,\Box\, b \rightarrow T \,]\!]\{Q\} \\
= & \\
& [P \Rightarrow b] \wedge \{P\}S\{Q\} \wedge \{P\}T\{Q\}
\end{array}$$

y en particular

$$\{x > 1\}[\![\, x > 0 \rightarrow x := 2 \,\Box\, x > 0 \rightarrow x := 4 \,]\!]\{x = 2\}$$

$=$
$[x > 1 \ \Rightarrow \ x > 0] \wedge \{x > 1\}x := 2\{x = 2\} \wedge \{x > 1\}x := 4\{x = 2\}$
$=$
$C \wedge [x \leq 1] \wedge F$
$=$
$Falso$

de donde el primer triplete es $Falso$; para el segundo

$\{x > 1\}[\![x > 0 \rightarrow x := 2 \,\square\, x > 0 \rightarrow x := 4]\!]\{x = 2 \vee x = 4\}$
$=$
$[x > 1 \ \Rightarrow \ x > 0]$
$\wedge$
$\{x > 1\}x := 2\{x = 2 \vee x = 4\} \wedge \{x > 1\}x := 4\{x = 2 \vee x = 4\}$
$=$
$C \wedge C \wedge C$

5.26 [85]
$\{P \wedge b\}S_1\{Q\} \wedge \{P \wedge c\}S_2\{Q\} \wedge [P \wedge \neg c \ \Rightarrow \ Q]$
$=$ $\quad\because$ def. de triplete
$[P \wedge b \ \Rightarrow \ S_1.Q] \wedge [P \wedge c \ \Rightarrow \ S_2.Q] \wedge [P \wedge \neg c \ \Rightarrow \ Q]$
$\Rightarrow$ $\quad\because$ transitividad de $\Rightarrow$
$[P \wedge b \ \Rightarrow \ S_1.Q] \wedge [P \wedge \neg b \wedge c \ \Rightarrow \ S_2.Q] \wedge [P \wedge \neg b \neg c \ \Rightarrow \ Q]$
$=$ $\quad\because$ conjuntividad de [ ], regla de intercambio
$[P \ \Rightarrow \ (b \ \Rightarrow \ S_1.Q) \wedge (\neg b \ \Rightarrow \ (c \ \Rightarrow \ S_2.Q \wedge \neg c \ \Rightarrow \ Q))]$
$=$ $\quad\because$ semántica de la selectiva
$[P \ \Rightarrow \ [\![b \rightarrow S_1 \,\square\, \neg b \rightarrow [\![c \rightarrow S_2 \,\square\, \neg c \rightarrow nada]\!]]\!].Q]$
$=$
$[P \ \Rightarrow \ if\ b\ then\ S_1\ else\ if\ c\ then\ S_2.Q]$
$=$ $\quad\because$ definición de triplete
$\{P\}if\ b\ then\ S_1\ else\ if\ c\ then\ S_2\{Q\}$

5.27 [85] La definición de equivalencia aparece en Definición 5.10:74:

$$U =_{\mathcal{H}} V \ \doteq \ \forall P, Q : P, Q \in \mathcal{P} : \vdash_{\mathcal{H}} \{P\}U\{Q\} \iff \vdash_{\mathcal{H}} \{P\}V\{Q\}$$

Tendremos que demostrar, $\forall P, Q, S$

$$\vdash_{\mathcal{H}} \{P\}S; nada\{Q\} \iff \vdash_{\mathcal{H}} \{P\}S\{Q\}$$

La implicación $(\Leftarrow)$ es trivial y es consecuencia de las reglas $(nada)$ y $(;)$:

$$\dfrac{\dfrac{\text{hipótesis}}{\{P\}S\{Q\}} \qquad \dfrac{}{\{Q\}nada\{Q\}}\,(nada)}{\{P\}S; nada\{Q\}}\,(;)$$

La otra implicación $\vdash_{\mathcal{H}} \{P\}S; nada\{Q\} \ \Rightarrow \vdash_{\mathcal{H}} \{P\}S\{Q\}$ la probaremos por inducción sobre la derivación del triplete $\{P\}S; nada\{Q\}$ (véase el esquema en la prueba del Teorema 5.14:76). Solamente es posible tal derivación por la aplicación de dos reglas: composición y refinamiento. Si $\{P\}S; nada\{Q\}$ ha sido obtenido a través de la regla de refinamiento, entonces existen dos predicados X e Y tales que

$[P \ \Rightarrow \ Y] \wedge \{Y\}S; nada\{X\} \wedge [X \ \Rightarrow \ Q]$
$\Rightarrow$ $\quad\because$ HI
$[P \ \Rightarrow \ Y] \wedge \{Y\}S\{X\} \wedge [X \ \Rightarrow \ Q]$
$\Rightarrow$ $\quad\because$ regla de refinamiento

$\{P\}S\{Q\}$

Si fue obtenido por la regla de la composición, entonces, para cierto X

$\{P\}S\{X\} \wedge \{X\}nada\{Q\}$
$\Rightarrow$ $\because$ por la regla de $nada$
$\{P\}S\{X\}, [X \Rightarrow Q]$
$\Rightarrow$ $\because$ por refinamiento
$\{P\}S\{Q\}$

5.29 [86] 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 $P \equiv Q$ (sintácticamente). El paso inductivo corresponde a la regla (ref); si el triplete original ha sido inferido de tal regla es que teníamos en el antecedente de la regla:

$[P \Rightarrow P'] \wedge \vdash_{\mathcal{H}} \{P'\}nada\{Q'\} \wedge [Q' \Rightarrow Q]$
$\Rightarrow$ $\because$ HI
$[P \Rightarrow P'] \wedge [P' \Rightarrow Q'] \wedge [Q' \Rightarrow Q]$
$\Rightarrow$ $\because$ transitividad de $\Rightarrow$
$[P \Rightarrow Q]$

5.30 [86] (A).— Véanse Ejemplo 5.6, §5.14 y §3.2.

(B).— Sea $\mathcal{S} \doteq [\![C \to y := 1 \,\Box\, C \to y := 0]\!] \,; x := 1$. Entonces $\mathcal{S}$ es indeterminista y $\{C\}\mathcal{S}\{x = 1\}$ (véase la solución del Ejercicio 4.19:257).

(C).—

$\{P\}[\![b \to S \,\Box\, b \to T \,\Box\, b \to nada]\!] \{R\}$
$=$ $\because$ def. triplete y semántica selección
$[P \Rightarrow b \wedge (b \Rightarrow S.R) \wedge (b \Rightarrow T.R) \wedge (b \Rightarrow nada.R)]$
$=$ $\because$ CP
$[P \Rightarrow b \wedge S.R \wedge T.Rnada.R]$
$=$ $\because$ semántica $nada$, $[\,]$ es conjuntivo
$[P \Rightarrow b] \wedge [P \Rightarrow S.R] \wedge [P \Rightarrow T.R] \wedge [P \Rightarrow R]$
$\Leftarrow$ $\because$ cálculo: monotonía de S y T
$[P \Rightarrow b] \wedge [P \Rightarrow R] \wedge [Q \Rightarrow R] \wedge [P \Rightarrow S.Q] \wedge [P \Rightarrow T.Q]$
$=$ $\because$ definición de triplete
$[P \Rightarrow b] \wedge [P \Rightarrow R] \wedge [Q \Rightarrow R] \wedge \{P\}S\{Q\} \wedge \{P\}T\{Q\}$

5.31 [86]
$[P \Rightarrow b \wedge c] \wedge \{P\}S\{Q\} \wedge \{P\}T\{Q\}$
$=$ $\because$ definición de triplete, conjuntividad de $[\,]$
$[(P \Rightarrow b \wedge c) \wedge (P \Rightarrow S.Q) \wedge (P \Rightarrow T.Q)]$
$=$ $\because (P \Rightarrow b \wedge c) \Rightarrow ((P \Rightarrow b) \wedge (P \Rightarrow b \vee c))$
$[P \Rightarrow ((b \vee c) \wedge (b \Rightarrow S.Q) \wedge (c \Rightarrow T.Q)]$
$=$ $\because$ semántica selectiva
$[P \Rightarrow [\![b \to S \,\Box\, c \to T]\!] .Q]$
$=$ $\because$ definición de triplete
$\{P\}[\![b \to S \,\Box\, c \to T]\!] \{Q\}$

5.32 [86]

$$
\begin{array}{ll}
 & \{X\}S; [\![\, b \rightarrow A \,\square\, \neg b \rightarrow B \,]\!]\,\{Y\} \\
= & \quad \because \text{definición de triplete} \\
 & [X \;\Rightarrow\; S; [\![\, b \rightarrow A \,\square\, \neg b \rightarrow B \,]\!].Y] \\
= & \quad \because \text{semántica de la composición y selectiva} \\
 & [X \;\Rightarrow\; S.((b \;\Rightarrow\; A.Y) \wedge (\neg b \;\Rightarrow\; B.Y))] \\
\Leftarrow & \quad \because \text{conjuntividad de } [\,],\ S \text{ monótona, } [A.Y \;\Rightarrow\; (b \;\Rightarrow\; A.Y)] \\
 & [X \;\Rightarrow\; S.A.Y] \wedge [X \;\Rightarrow\; S.B.Y] \\
= & \quad \because \text{definición de triplete} \\
 & \{X\}S; A\{Y\} \wedge \{X\}S; B\{Y\}
\end{array}
$$

5.34 [86] Véase el Teorema 4.24 y Ejemplo 4.25

5.35 [86] Véase Ejemplo 5.6, Ejercicio 5.8 y Ejercicio 5.9.

5.36 [86] (Véase también el Ejercicio 4.25:66). Siendo $SI \doteq [\![\, b \rightarrow S \,\square\, b' \rightarrow S' \,]\!]$, razonemos por inducción sobre la derivación $\vdash_{\mathcal{H}} \{P\}SI\{Q\}$. Tal derivación solamente puede obtenerse vía dos reglas: (1) por la regla (si), y el resultado es trivial; o bien (2) por la regla de refinamiento, a partir de

$$
\begin{array}{ll}
 & [P \;\Rightarrow\; P'] \wedge \{P'\}SI\{Q'\} \wedge [Q' \;\Rightarrow\; Q] \\
\Rightarrow & \quad \because \text{HI} \\
 & [P \;\Rightarrow\; P'] \wedge [P' \;\Rightarrow\; b \vee b'] \wedge [Q' \;\Rightarrow\; Q] \\
\Rightarrow & \quad \because \text{conjuntividad de } [\,], \text{ transitividad de } \Rightarrow \\
 & [P \;\Rightarrow\; b \vee b']
\end{array}
$$

6.4 [90] Si $[S.\neg b \equiv Falso]$, entonces, por monotonía, $[S.(\neg b \wedge X) \equiv Falso]$. Y de aquí es fácil probar por inducción que

$$\forall k : k \geq 0 : [H^k.(X) \equiv \neg b \wedge X]$$

El caso base es trivial. Y el paso inductivo sería

$$
\begin{array}{ll}
 & H^{k+1}.X \\
= & \quad \because \text{definición} \\
 & \neg b \wedge X \vee S.H^k.X \\
= & \quad \because \text{HI} \\
 & \neg b \wedge X \vee S.(\neg b \wedge X) \\
= & \quad \because [S.(\neg b \wedge X) \equiv Falso], \text{ CP} \\
 & \neg b \wedge X
\end{array}
$$

6.5 [90] Inducción sobre S.

– CASOS BASE. Hay que demostrar, $\forall X$, y *ptle*

$$
\begin{array}{lcl}
Q \wedge nada.X & \equiv & Q \wedge nada.(Q \wedge X) \\
Q \wedge aborta.X & \equiv & Q \wedge aborta.(Q \wedge X) \\
Q \wedge z := E.X & \equiv & Q \wedge z := E.(Q \wedge X)
\end{array}
$$

Para $z := E$ aplicamos que z no aparece en Q. El resto es trivial.

– PASOS INDUCTIVOS.

– *Composición*. Sean dos sentencias arbitrarias S y T, y un predicado arbitrario X; entonces, *ptle*

$$
\begin{array}{ll}
& Q \wedge S;T.X \\
= & \quad \because \text{semántica composición} \\
& Q \wedge S.(T.X) \\
= & \quad \because \text{HI para } S \\
& Q \wedge S.(Q \wedge T.X) \\
= & \quad \because \text{HI para } T \\
& Q \wedge S.(Q \wedge T.(Q \wedge X)) \\
= & \quad \because \text{HI para } S \\
& Q \wedge S.(T.(Q \wedge X)) \\
= & \quad \because \text{semántica composición} \\
& Q \wedge S;T.(Q \wedge X)
\end{array}
$$

– *Selectiva*.

$$
\begin{array}{ll}
& Q \wedge [\![\, \Box \, b_i \to S_i \,]\!] .(Q \wedge X) \\
= & \quad \because \text{semántica} \\
& Q \wedge OB \wedge \forall i :: b_i \ \Rightarrow \ S_i.(Q \wedge X) \\
= & \quad \because \text{HI} \\
& Q \wedge OB \wedge \forall i :: b_i \ \Rightarrow \ Q \wedge S_i.X \\
= & \quad \because \text{CP: } [Q \wedge (A \ \Rightarrow \ B) \equiv Q \wedge (A \ \Rightarrow \ Q \wedge B)] \\
& Q \wedge OB \wedge \forall i :: b_i \ \Rightarrow \ S_i.X \\
= & \quad \because \text{semántica} \\
& Q \wedge [\![\, \Box \, b_i \to S_i \,]\!] .X
\end{array}
$$

– *Bucle*. Sea el bucle $*[\![\, b \to S \,]\!]$. Entonces, es fácil probar (en forma similar a las anteriores), y por inducción sobre n, que

$$\forall n : n \geq 0 : Q \wedge H^k.(Q \wedge X) \equiv Q \wedge H^k.X$$

y de aquí el resultado.

<u>6.7</u> [91] (Véase también el Ejercicio 8.40) Si x es entera, entonces, *ptle*

$$
\begin{array}{lcl}
H^0.C & \doteq & x \leq 0 \wedge x \leq 1 \wedge C \quad \equiv \quad x \leq 0 \\
H^1.C & \doteq & H^0.C \vee SI.H^0.C
\end{array}
$$

y $H^1.C$ es la precondición más débil para que el bucle se ejecute a lo sumo una vez, pero

$$
\begin{array}{ll}
& SI.H^0.C \\
= & \quad \because \text{semántica selectiva} \\
& OB \wedge (x > 0 \ \Rightarrow \ x := x - 1.x \leq 0) \wedge (x > 1 \ \Rightarrow \ x := x - 2.x \leq 0) \\
= & \\
& x > 0 \wedge (x > 0 \ \Rightarrow \ x \leq 1) \wedge (x > 1 \ \Rightarrow \ x \leq 2) \\
= & \quad \because \text{CP} \\
& x > 0 \wedge x \leq 1 \wedge (x > 1 \ \Rightarrow \ \ldots) \\
= & \quad \because x \text{ es entera}
\end{array}
$$

$$x = 1$$

luego $[H^1.C \equiv x \leq 1]$, siempre que x sea una variable entera. Obsérvese que el resultado es el mismo si sustituimos la sentencia $x := x - 2$ por una sentencia arbitraria.

6.9 [92] (Véase el Ejercicio 8.50:179). Probaremos $[\mathcal{R}.C]$. Tenemos $[H^0.C \equiv \neg b]$. Además, utilizando la semántica de la selectiva es fácil probar:

$$SI.Z \equiv b \wedge x, b := x+1, x < 1.Z \wedge b := Falso.Z \tag{0}$$

Y de aquí obtenemos, por un cálculo simple, *ptle*

$$\begin{array}{lcccl} H^1.C & \doteq & H^0.C \vee SI.(H^1.C) & \equiv & \neg b \vee b \wedge x \geq 1 \\ H^2.C & \doteq & H^0.C \vee SI.(H^2.C) & \equiv & \neg b \vee b \wedge x \geq 0 \end{array}$$

Y podemos conjeturar:

$$\forall k : k \geq 1 : [H^k.C \equiv \neg b \vee b \wedge x \geq 2 - k] \tag{$*$}$$

Probaremos $(*)$ por inducción. El caso base ($k = 1$) ya está demostrado, y el paso inductivo es

$$\begin{array}{ll} & H^{k+1}.C \\ = & \quad \because \text{definición} \\ & H^0.C \vee SI.(H^k.C) \\ = & \quad \because \text{HI, (0)} \\ & \neg b \vee b \wedge x, b := x+1, x < 1.(\neg b \vee b \wedge x \geq 2-k) \\ \wedge & b := Falso.(\neg b \vee \ldots) \\ = & \quad \because \text{CP} \\ & \neg b \vee b \wedge (x \geq 1 \vee x < 1 \wedge x + 1 \geq 2 - k) \wedge C \\ = & \quad \because \text{CP} \\ & \neg b \vee b \wedge x \geq 2 - (k+1) \end{array}$$

Por tanto, según $(*)$ y según la definición inductiva de la semántica de los bucles (Definición 6.2), *ptle*

$$\begin{array}{ll} & \mathcal{R}.C \\ = & \quad \because \text{semántica inductiva, y } (*) \\ & \neg b \vee \exists k : k \geq 1 : \neg b \vee b \wedge x \geq 2 - k \\ = & \quad \because \text{idempotencia, conmutatividad de } \vee \\ & \neg b \vee b \wedge (x \geq 1 \vee x \geq 0 \vee x \geq -1 \vee \ldots) \\ = & \quad \because x \in \mathbb{Z} \\ & \neg b \vee b \wedge C \\ = & \quad \because \text{tercio excluido} \\ & Cierto \end{array}$$

6.16 [96] Seguiremos un razonamiento similar al de la prueba del Teorema 6.14 (véase también el Ejercicio 8.71). Bastará demostrar, para todo predicado X,

$$\begin{array}{ll} & [P \wedge \mathcal{R}.X \equiv P \wedge \mathcal{R}'.X] \\ = & \quad \because \text{semántica inductiva de los bucles} \\ & [P \wedge (\exists k : k \geq 0 : H^k.X) \equiv P \wedge (\exists k : k \geq 0 : {H'}^k.X)] \\ \Leftarrow & \quad \because \text{CP} \end{array}$$

$$
\begin{array}{ll}
 & \forall k : k \geq 0 : [P \wedge H^k.X \equiv P \wedge H'^k.X] \\
= & \qquad \because \text{inducción estructural} \\
 & [P \wedge H^0.X \equiv P \wedge H'^0.X] \qquad (1) \\
\wedge & \forall k \geq 0 : [P \wedge H^k.X \equiv P \wedge H'^k.X] \\
 & \qquad\qquad \Rightarrow \; [P \wedge H^{k+1}.X \equiv P \wedge H'^{k+1}.X] \qquad (2)
\end{array}
$$

(1) es trivial. Es fácil probar que si S' tiene el mismo comportamiento que S en el entorno P, y P es invariante de $\mathcal{R}$, entonces P también es invariante de $\mathcal{R}'$. En efecto,

$$
\begin{array}{ll}
 & [P \wedge b \;\Rightarrow\; S.P] \\
= & \qquad \because \text{CP} \\
 & [P \wedge b \;\Rightarrow\; P \wedge S.P] \\
= & \qquad \because (0) \\
 & [P \wedge b \;\Rightarrow\; P \wedge S'.P] \\
= & \qquad \because \text{CP} \\
 & [P \wedge b \;\Rightarrow\; S'.P] \\
= & P \text{ es invariante del bucle } \mathcal{R}' \;\doteq\; * [\![\, b \rightarrow S' \,]\!]
\end{array}
$$

La prueba del paso inductivo (2) sería

$$
\begin{array}{ll}
 & [P \wedge H^{k+1}.X \equiv P \wedge H'^{k+1}.X] \\
= & \qquad \because \text{definición} \\
 & [P \wedge (H^0.X \vee b \wedge S.H^k.X) \equiv P \wedge (H'^0.X \vee b \wedge S'.H'^k.X)] \\
\Leftarrow & \\
 & [P \wedge b \wedge S.H^k.X \equiv P \wedge b \wedge S'.H'^k.X] \\
= & \qquad \because P \text{ invariante, } S \text{ y } S' \text{ conjuntivas} \\
 & [P \wedge b \wedge S.(P \wedge H^k.X) \equiv P \wedge b \wedge S'.(P \wedge H'^k.X)] \\
= & \qquad \because \text{HI, regla de Leibniz} \\
 & [P \wedge b \wedge S.(P \wedge H^k.X) \equiv P \wedge b \wedge S'.(P \wedge H^k.X)] \\
= & \qquad \because S \text{ y } S' \text{ tienen el mismo comportamiento en el entorno de } P \\
 & Cierto
\end{array}
$$

OBSERVACIÓN.– En el Teorema 6.14 se prueba que los bucles tienen el mismo comportamiento si $\forall X :: [b \wedge S.X \equiv b \wedge T.X]$, pero en el presente ejercicio se prueba que tienen el mismo comportamiento en presencia del invariante P; el lector deberá observar la diferencia importante entre los dos conceptos. $\boxed{\text{OBS}}$

6.20 [97] Véase Ejercicio 6.21.

6.21 [97] Sea $J^k.X$ la precondición más débil para que el cuerpo del bucle se ejecute exactamente k veces terminando verificando X; entonces, con esta definición (pongamos $J^k.X == J^k$):

$$J^0 \;\doteq\; \neg b \wedge X \qquad\qquad J^n \;\doteq\; b \wedge S.J^{n-1}$$

Si S es una sentencia arbitraria se cumple:

$$(\exists k : k \geq 0 : J^k.X) \;\Rightarrow\; *[\![\, b \rightarrow S \,]\!].X \qquad (1)$$

Para probarlo basta probar $[\; \exists k : 0 \leq k \leq n : J^k \;\Rightarrow\; H^n \;]$, donde los H^n son los correspondientes a la Definición 6.2, y $H^k.X == H^k$. Lo probamos por inducción. El caso base es trivial, siendo el paso inductivo, *ptle*

H^{n+1}
$=$ $\because$ definición
$H^0 \vee b \wedge S.H^n$
$=$ $\because$ HI, monotonía de S
$J^0 \vee b \wedge S.(\exists k : 0 \leq k \leq n : J^k)$
$\Leftarrow$ $\because$ monotonía de S, distributividad
$J^0 \vee b \wedge (\exists k : 0 \leq k \leq n : S.J^k)$
$=$ $\because$ definición
$J^0 \vee \exists k : 0 \leq k \leq n : J^{k+1}$
$=$ $\because$ CP
$\exists k : 0 \leq k \leq n+1 : J^k$

La implicación recíproca de (1) es posible probarla si S es determinista. En efecto, basta probar, por inducción

$$\forall n : n \geq 0 : [H^n \ \Rightarrow \ \exists k : k \geq 0 : J^k]$$

El caso base es trivial, siendo el paso inductivo, *ptle*,
$[H^n \ \Rightarrow \ \exists k : k \geq 0 : J^k]$
$\Rightarrow$ $\because$ monotonía de S
$[S.H^n \ \Rightarrow \ S.(\exists k : k \geq 0 : J^k)]$
$\Rightarrow$ $\because$ determinismo de S
$[S.H^n \ \Rightarrow \ \exists k : k \geq 0 : S.J^k]$
$\Rightarrow$ $\because$ CP
$[H^0 \vee b \wedge S.H^n \ \Rightarrow \ J^0 \vee \exists k : k \geq 0 : b \wedge S.J^k]$
$=$ $\because$ definición y CP
$[H^{n+1} \ \Rightarrow \ \exists k : k \geq 0 : J^k]$

6.30 [100] Respondemos al apartado (C) en forma general. Queremos estudiar la conmutatividad

$$(x := E; S) \ = \ (S; x := E)$$

Si S es la asignación $y := F$ podemos aplicar el Lema 4.7(ii):59. Si S modifica alguna variable libre en E puede haber problemas: por ejemplo

$$\begin{array}{lcl} x := y; y := y+1.(x = a \wedge y = b) & \equiv & a = b-1 \wedge y = b-1 \\ y := y+1; x := y.(x = a \wedge y = b) & \equiv & y = a-1 \wedge y = b-1 \end{array}$$

y los transformadores son distintos. Añadimos pues la condición:

S no modifica ninguna variable de la expresión E.

Y razonamos por inducción sobre la sentencia S. Los casos base $nada$ y $aborta$ son triviales. Para la asignación, si x puede aparecer en E, y S es la sentencia $y := F$ necesariamente debe darse $x \neq y$, y en ese caso E no puede depender de y, ni F de x, y siendo $M(x, y)$ un predicado arbitrario tendremos

$x := E; y := F.M(x, y)$
$=$
$x := E.M(x, F(y))$
$=$
$M(E(x), F(y))$
$=$
$y := F; x := E.M$

Los pasos inductivos son fáciles

$$
\begin{array}{ll}
& x := E; (S_1; S_2) \\
= & \quad \because \text{asociatividad} \\
& (x := E; S_1); S_2 \\
= & \quad \because \text{HI} \\
& (S_1; x := E); S_2 \\
= & \quad \because \text{asociatividad} \\
& S_1; (x := E; S_2) \\
= & \quad \because \text{HI} \\
& S_1; (S_2; x := E) \\
= & \quad \because \text{asociatividad} \\
& (S_1; S_2); x := E
\end{array}
$$

Para la selectiva, por el Teorema 4.24, basta razonar para dos guardas,

$$
\begin{array}{ll}
& x := E; [\![\, b \rightarrow S \,\Box\, b' \rightarrow S' \,]\!] \\
= & \quad \because \text{en las guardas no aparece } x \\
& [\![\, b \rightarrow x := E; S \,\Box\, b' \rightarrow x := E; S' \,]\!] \\
= & \quad \because \text{HI} \\
& [\![\, b \rightarrow S; x := E \,\Box\, b' \rightarrow S'; x := E \,]\!] \\
= & \quad \because \text{distributividad de } selec(b, b') \text{ (véase Ejercicio 6.28}(D)) \\
& [\![\, b \rightarrow S \,\Box\, b' \rightarrow S' \,]\!] \,; x := E
\end{array}
$$

Para los bucles necesitamos la propiedad

$$\forall k : k \geq 0 : [(x := E; H^k) = (H^k; x := E)] \tag{$*$}$$

ya que a partir de la anterior tendremos:

$$
\begin{array}{ll}
& x := E; *[\![\, b \rightarrow S \,]\!] \,.\, Z \\
= & \quad \because \text{semántica del bucle} \\
& x := E.(\exists k : k \geq 0 : H^k.Z) \\
= & \quad \because \text{definición de sustitución} \\
& \exists k : k \geq 0 : x := E.H^k.Z \\
= & \quad \because (*) \\
& \exists k : k \geq 0 : H^k.(x := E.Z) \\
= & \quad \because \text{semántica del bucle} \\
& *[\![\, b \rightarrow S \,]\!].(x := E.Z) \\
= & \quad \because \text{semántica de la composición} \\
& *[\![\, b \rightarrow S \,]\!] \,; x := E \,.\, Z
\end{array}
$$

Finalmente, probaremos $(*)$ por inducción sobre k:

— CASO BASE ($k = 0$):

$$
\begin{array}{ll}
& x := E; H^0.Z \\
= & \quad \because \text{semántica de la composición, y definición de } H^0 \\
& x := E.(\neg b \wedge Z) \\
= & \quad \because x \text{ no aparece en } b \\
& \neg b \wedge x := E.Z \\
= & \quad \because \text{definición de } H^0 \text{ y semántica de la composición} \\
& H^0; x := E.Z
\end{array}
$$

— PASO INDUCTIVO:

$$x := E; H^{n+1} . Z$$

$= \quad \because$ semántica de la composición, y definición de H^{n+1}

$$x := E.(H^0.Z \vee b \wedge S.H^n.Z)$$

$= \quad \because$ caso base; x no aparece en b

$$H^0.(x := E.Z) \vee b \wedge x := E.S.H^n.Z)$$

$= \quad \because S$ no modifica variables de E

$$H^0.(x := E.Z) \vee b \wedge S.(x := E.H^n.Z)$$

$= \quad \because$ HI

$$H^0.(x := E.Z) \vee b \wedge S.(H^n.(x := E.Z))$$

$= \quad \because$ semántica de la composición, y definición de H^{n+1}

$$H^{n+1}; x := E . Z$$

6.31 [101] (A).— $Z_1 \equiv (x = a \vee x = b) \wedge x \geq a, b, \quad Z_2 \equiv (x = a \vee x = b) \wedge x \leq a, b.$

(B).— Calculemos, *ptle*

$\mathcal{S}.Z$

$= \quad \because$ semántica

$(a \geq b \;\Rightarrow\; x, y := a, b.Z) \wedge (a \leq b \;\Rightarrow\; x, y := b, a.Z)$

$= \quad \because$ CP

$(a \geq b \;\Rightarrow\; a = \text{máx}(a, b) \wedge b = \text{mín}(a, b))$
$\wedge$
$(a \leq b \;\Rightarrow\; b = \text{máx}(a, b) \wedge a = \text{mín}(a, b))$

$= \quad \because a = \text{máx}(a, b) \equiv a \geq b, \ldots$

$Cierto$

Calculemos $\mathcal{S}'.Z$, o sea, $x, y := a, b.(H^0.Z \vee H^1.Z \vee \ldots)$. Veremos que el segundo término de la disyunción vale $Cierto$, y al ser la sucesión creciente, $[\mathcal{R}.C \equiv Cierto]$. Por definición, $[x, y := a, b.H^0.Z \equiv b \leq a]$, de donde, *ptle*

$x, y := a, b.H^1.Z$

$= \quad \because$ definición de $H^1.Z$

$b \leq a \vee x, y := a, b.(y > x \wedge x, y := y, x.H^0.Z)$

$= \quad \because$ semántica, $x, y := a, b; x, y := y, x = x, y := b, a$

$b \leq a \vee b > a \wedge x, y := b, a.H^0.Z$

$= \quad \because$ definición de sustitución

$b \leq a \vee b > a \wedge a \leq b$

$= \quad \because$ CP

$Cierto$

(C).— Los tripletes $\{Cierto\}\mathcal{S}\{Z\}$ y $\{Cierto\}\mathcal{S}'\{Z\}$ son consecuencia inmediata de la definición de triplete y del apartado anterior.

6.33 [103]

$$
\begin{array}{ll}
 & I \wedge J \text{ invariante de } *[\![\, b \rightarrow S \,]\!] \\
= & \quad \because \text{definición} \\
 & [I \wedge J \wedge b \;\Rightarrow\; S.(I \wedge J)] \\
= & \quad \because S \text{ conjuntiva y cálculo} \\
 & [I \wedge J \wedge b \;\Rightarrow\; S.I] \\
\wedge & [I \wedge J \wedge b \;\Rightarrow\; S.J] \\
\Leftarrow & \quad \because [I \wedge J \;\Rightarrow\; I], \ldots \\
 & [I \wedge b \;\Rightarrow\; S.I] \\
\wedge & [J \wedge b \;\Rightarrow\; S.J] \\
= & \quad \because I \text{ invariante, } J \text{ invariante} \\
 & \mathit{Cierto}
\end{array}
$$

$$
\begin{array}{ll}
 & I \vee J \text{ invariante de } *[\![\, b \rightarrow S \,]\!] \\
= & \quad \because \text{definición} \\
 & [(I \vee J) \wedge b \;\Rightarrow\; S.(I \vee J)] \\
= & \quad \because \text{CP} \\
 & [I \wedge b \;\Rightarrow\; S.(I \vee J)] \\
\wedge & [J \wedge b \;\Rightarrow\; S.(I \vee J)] \\
\Leftarrow & \quad \because \text{monotonía de } S \\
 & [I \wedge b \;\Rightarrow\; S.I] \\
\wedge & [J \wedge b \;\Rightarrow\; S.J] \\
= & \quad \because I, J \text{ invariantes} \\
 & \mathit{Cierto}
\end{array}
$$

6.34 [103] Por el Ejercicio 6.35, bastará probar que I es invariante del bucle:

$$*[\![\, b \wedge f \rightarrow S \,\square\, b \wedge \neg f \rightarrow T \,]\!]$$

sii se verifica

$$[I \wedge b \wedge f \;\Rightarrow\; S.I] \wedge [I \wedge b \wedge \neg f \;\Rightarrow\; T.I]$$

lo cual es trivial.

6.35 [103] Tenemos que

$$
\begin{array}{ll}
 & *[\![\, b \wedge f \rightarrow S \,\square\, b \wedge \neg f \rightarrow T \,]\!] \\
= & \quad \because \text{Teorema 6.10} \\
 & *[\![\, b \rightarrow [\![\, b \wedge f \rightarrow S \,\square\, b \wedge \neg f \rightarrow T \,]\!] \,]\!] \\
= & \quad \because \text{Teorema 6.14} \\
 & *[\![\, b \rightarrow [\![\, f \rightarrow S \,\square\, \neg f \rightarrow T \,]\!] \,]\!]
\end{array}
$$

Y quedará probar que los dos cuerpos tienen el mismo comportamiento en el entorno de la guarda b para poder aplicar el Teorema 6.14; es decir, habría que probar, *ptle*, y para todo X,

$$b \wedge [\![\, f \rightarrow S \,\square\, \neg f \rightarrow T \,]\!].X \;\equiv\; b \wedge [\![\, b \wedge f \rightarrow S \,\square\, b \wedge \neg f \rightarrow T \,]\!].X$$

lo cual es muy fácil y sigue directamente de la semántica de la selectiva.

6.41 [106] Podemos debilitar la tesis del teorema en la forma siguiente

$$
\begin{array}{ll}
 & [I \;\Rightarrow\; \mathcal{R}.C] \\
= & \quad \because k \text{ entero, de donde } [t \leq 0 \vee t = 0 \vee t = 1 \vee \ \ldots], \text{ definición de } \mathcal{R}.C \\
 & [I \wedge (t \leq 0 \vee t = 0 \vee t = 1 \vee \ \ldots) \;\Rightarrow\; (H^0.C \vee H^1.C \vee \ \ldots)] \\
\Leftarrow & \quad \because \text{CP} \\
 & [I \wedge t \leq 0 \;\Rightarrow\; H^0.C] \wedge \forall k : k \geq 0 : [I \wedge t = k \;\Rightarrow\; H^k.C]
\end{array}
$$

La prueba del primer término es fácil:

$$
\begin{array}{ll}
 & [I \wedge t \leq 0 \;\Rightarrow\; H^0.C] \\
= & \quad \because H^0.C \equiv \neg b \\
 & [I \wedge t \leq 0 \;\Rightarrow\; \neg b] \\
= & \quad \because \text{regla de intercambio dos veces} \\
 & [I \wedge b \;\Rightarrow\; t > 0] \\
= & \\
 & (b)
\end{array}
$$

La implicación $[I \wedge t = k \;\Rightarrow\; H^k.C]$ se interpreta en la forma siguiente: si $t = k$, entonces el cuerpo del bucle se ejecuta a lo sumo k veces. La prueba por inducción del último predicado sería:

CASO BASE ($k = 0$):

$[I \wedge t = 0 \;\Rightarrow\; H^0.C]$
$=$ $\quad\because H^0.C \equiv \neg b$
$[I \wedge t = 0 \;\Rightarrow\; \neg b]$
$=$ $\quad\because$ regla de intercambio
$[I \wedge b \;\Rightarrow\; t \neq 0]$
$\Leftarrow$ $\quad\because$ CP
(b)

PASO INDUCTIVO:

$[I \wedge t = k+1 \;\Rightarrow\; H^{k+1}.C]$
$=$ $\quad\because$ definición
$[I \wedge t = k+1 \;\Rightarrow\; \neg b \vee b \wedge S.H^k.C]$
$=$ $\quad\because$ regla de intercambio
$[I \wedge b \wedge t = k+1 \;\Rightarrow\; S.H^k.C]$
$\Leftarrow$ $\quad\because \;\Downarrow (c)$, transitividad
$[I \wedge b \wedge S.(t < k+1) \;\Rightarrow\; S.H^k.C]$
$\Leftarrow$ $\quad\because \Downarrow (a)$, transitividad
$[S.I \wedge S.(t < k+1) \;\Rightarrow\; S.H^k.C]$
$\Leftarrow$ $\quad\because S$ es conjuntiva y monótona
$[I \wedge t < k+1 \;\Rightarrow\; H^k.C]$

Probemos la última implicación de la derecha razonando como sigue

$I \wedge t < k+1$
$=$ $\quad\because k$ y t son enteros
$I \wedge (t \leq 0 \vee t = 1 \vee \;\ldots\; \vee t = k)$
$\Rightarrow$ $\quad\because$ por lo anterior, y por hipótesis de inducción
$H^0.C \vee H^1.C \vee \;\ldots\; \vee H^k.C$
$=$ $\quad\because$ la sucesión de transformadores H^k es creciente — Teorema 6.15(ii)
$H^k.C$

6.45 [108] Tenemos, *ptle*

$wdec([\![\, x > 1 \rightarrow x := x - 1 \,\square\, x > 0 \rightarrow x := x + 2 \,]\!], 3x)$
$=$ $\quad\because$ Lema 6.43(iii)
$(x > 1 \vee x > 0)$
$\wedge\; x > 1 \;\Rightarrow\; wdec(x := x - 1, 3x)$
$\wedge\; x > 0 \;\Rightarrow\; wdec(x := x + 2, 3x)$
$=$ $\quad\because$ Lema 6.43(i)
$x > 0 \wedge (x > 1 \;\Rightarrow\; (x := x - 1{,}3x) < 3x)$
$\wedge\; (x > 0 \;\Rightarrow\; (x := x + 2{,}3x) < 3x)$
$=$ $\quad\because$ definición asignación
$x > 0 \wedge (x > 1 \;\Rightarrow\; 3(x-1) < 3x) \wedge (x > 0 \;\Rightarrow\; 3(x+2) < 3x)$
$=$ $\quad\because$ CP
$x > 0 \wedge (x > 1 \;\Rightarrow\; Cierto) \wedge (x > 0 \;\Rightarrow\; Falso)$
$=$ $\quad\because$ CP
$x > 0 \wedge C \wedge x \leq 0$
$=$ $\quad\because$ CP
$Falso$

Interpretación: es posible elegir la segunda guarda, en presencia de la primera, y entonces $3x$ no disminuye.

6.50 [110] Probaremos, para $t_0 \in \mathbb{Z}$, el triplete

$\{A \wedge t = t_0\}S; T\{t < t_0\}$
$\Leftarrow$ $\quad\because$ semántica composición

$$
\begin{array}{ll}
& \{A \wedge t = t_0\}S\{B \wedge t < t_0\}T\{t < t_0\} \\
= & \qquad \because \text{conjuntividad} \\
& \{A \wedge t = t_0\}S\{B\} \wedge \{A \wedge t = t_0\}S\{t < t_0\} \wedge \{B \wedge t < t_0\}T\{t < t_0\} \\
\Leftarrow & \qquad \because \text{propiedades } (a) \text{ y } (b) \text{ (que se citan) y regla refinamiento} \\
& \{B \wedge t < t_0\}T\{t < t_0\} \\
\Leftarrow & \qquad \because \text{regla refinamiento} \\
& (c)
\end{array}
$$

6.52 [113] Para $t \doteq |x - y|$, despreciamos el intercambio $x, y := y, x$, ya que no altera t. Para las otras sentencias:

$$
\begin{array}{ll}
& x := x - y.t < t \\
= & \qquad \because \text{Lema 6.43, semántica asignación} \\
& |x - y - y| < |x - y| \\
\Leftarrow & \\
& x > 2y \wedge y > 0
\end{array}
$$

Pero observamos (recordemos $I \Rightarrow x, y > 0$)

$$
\begin{array}{ll}
& I \wedge x \neq y \wedge (x := x + y.t) < t \\
= & \qquad \because \text{semántica asignación} \\
& I \wedge x \neq y \wedge |x| < |x - y| \\
= & \\
& I \wedge x > y \wedge |x| < |x - y| \ \ \vee \ \ I \wedge x < y \wedge |x| < |x - y| \\
= & \qquad \because \text{el primer término es } Falso \text{ por ser } I \Rightarrow y > 0 \\
& I \wedge 2x < y
\end{array}
$$

Obsérvese además que $I \wedge (x > 2y \vee 2x < y) \Rightarrow t > 0 \wedge x \neq y$. Luego un fragmento del bucle es

$$
\begin{array}{lll}
*[\![& x > 2y & \to x := x - y \\
\Box & 2x < y & \to x := x + y \qquad \text{— o también } y := y - x \\
\Box & \ldots]\!] &
\end{array}
$$

El estudio del resto de funciones contadoras se deja al lector.

6.65 [124] Para deducir la sentencia S estudiemos la poscondición, ya su precondición debe ser el invariante. Es decir: $\{I\}S; x, y := y, x \bmod y\{I\}$. Por consiguiente debe tenerse, *ptle*:

$$
\begin{array}{ll}
& x, y := y, x \text{ mod } y.I \\
= & \qquad \because \text{semántica asignación} \\
& MCD(X,Y) = \text{ mcd}(y, x \text{ mod } y) \wedge y = pX + qY \wedge x \text{ mod } y = rX + sY \\
\wedge & \\
& y \geq x \bmod y \geq 0
\end{array}
$$

Pero tenemos:

$$
\begin{array}{ll}
& y = pX + qY \wedge x \text{ mod } y = rX + sY \\
\Rightarrow & \qquad \because x = \lfloor x/y \rfloor \, y + x \text{ mod } y \\
& y = pX + qY \wedge x = \lfloor x/y \rfloor \, (pX + qY) + rX + sY \\
= & \\
& y = pX + qY \wedge x = (r + \lfloor x/y \rfloor p)X + (s + \lfloor x/y \rfloor q)Y
\end{array}
$$

por tanto, debe verificarse:

$$
\begin{array}{l}
\{x = pX + Qy \wedge y = rX + sY\} \\
S; \\
\{y = pX + qY \wedge x = (r + \lfloor x/y \rfloor\, p)X + (s + \lfloor x/y \rfloor\, q)Y\}
\end{array}
$$

y S puede ser la sentencia

$$p, q, r, s := r, s, p - \lfloor x/y \rfloor\, r, q - \lfloor x/y \rfloor\, s$$

Además, por el Teorema 6.63, el bucle da a lo sumo $\lfloor 2 \log(M+1) \rfloor$ pasos.

6.66 [125] El predicado

$$I \doteq MCD(x, y) = MCD(X, Y) \wedge x, y > 0 \wedge xu + yv = 2XY$$

es un invariante para los tres bucles y queda probar que terminan; se verifica

$$
\begin{array}{l}
\{I\} \\
*[\![\, x > y \rightarrow x, v := x - y, u + v \,]\!]\,; \\
\{I \wedge x \leq y\} \\
*[\![\, x < y \rightarrow y, u := y - x, u + v \,]\!] \\
\{I \wedge x \geq y\}
\end{array}
$$

Los bucles internos terminan trivialmente, ya que la función $t_1 \doteq x$ así como la función $t_2 \doteq y$ son contadores. Vamos a probar que el bucle externo termina. Para ello hay que encontrar un contador; veamos que el valor $t \doteq x + y$ se decrementa en cada paso. Basta demostrar que los predicados I_1 y I_2 que figuran en el siguiente esquema son invariantes, y aplicar el Teorema de Invariantes:

$$
\begin{array}{ll}
 & \{P\}(\doteq x, y \geq 0 \wedge x + y = k \wedge x \neq y) \\
\Rightarrow & \\
 & \{x + y \leq k \wedge x, y > 0 \wedge (x = y \Rightarrow x + y \neq k)\}(\doteq I_1)\} \\
 & *[\![\, x > y \rightarrow x := x - y \,]\!] \\
 & \{I_1 \wedge x \leq y\} \\
\Rightarrow & \quad \because x \geq y \wedge x \leq y \Rightarrow (x = y \Rightarrow x + y \neq k) \\
 & \{x + y \leq k \wedge (x \geq y \Rightarrow x + y \neq k) \wedge x, y > 0\}(\doteq I_2) \\
 & *[\![\, x < y \rightarrow y := y - x \,]\!] \\
 & \{I_2 \wedge x \geq y\} \\
\Rightarrow & \\
 & \{x + y < k\}
\end{array}
$$

Para probar la invariabilidad de I_2, tenemos

$$
\begin{array}{ll}
 & y := y - x . I_2 \\
= & \\
 & y \leq k \wedge (x \geq y - x \Rightarrow y \neq k) \wedge x > 0 \wedge y - x > 0 \\
\Leftarrow & \quad \because y = k \wedge x + y \leq k \Rightarrow x \leq 0 \\
 & x + y \leq k \wedge (x \geq y \Rightarrow x + y \neq k) \wedge x, y > 0 \wedge y > x \\
= & \\
 & I_2 \wedge y > x
\end{array}
$$

Para probar la invariabilidad de I_1 razonamos en la forma siguiente

$$
\begin{array}{ll}
 & x := x - y . I_1 \\
= & \\
 & x \leq k \wedge x > y \wedge y > 0 \wedge (x - y = y \Rightarrow x \neq k) \\
\Leftarrow & \quad \because x = k \wedge x + y \leq k \Rightarrow y \leq 0 \\
 & I \wedge x > y
\end{array}
$$

6.67 [125] Vamos a probar por inducción sobre $k(\geq 0)$ que, *ptle*:

$$H^k.C \equiv \exists p, q : 0 \leq q \leq k : n = 2^q(2p+1)$$

– CASO BASE: $(k = 0)$ trivial.

– PASO INDUCTIVO. Supongamos $k \geq 1$; entonces, *ptle*:

$$\begin{array}{ll}
 & H^{k+1}.C \\
= & \quad \because \text{definición} \\
 & H^0.C \vee [\![\, n\ par \rightarrow n := n/2 \,]\!] .H^k.C \\
= & \quad \because \text{semántica} \\
 & H^0.C \vee n\ par \wedge n := n/2.H^k.C \\
= & \quad \because \text{HI} \\
 & H^0.C \vee n\ par \wedge n := n/2.(\exists p, q : 0 \leq q \leq k : n = 2^q(2p+1)) \\
= & \quad \because \text{semántica} \\
 & H^0.C \vee n\ par \wedge \exists p, q : 0 \leq q \leq k : n/2 = 2^q(2p+1) \\
= & \quad \because \text{absorción, } n\ par \ \Rightarrow \ (n/2) * 2 = n \\
 & H^0.C \vee \exists p, q : 0 \leq q \leq k : n = 2^{q+1}(2p+1) \\
= & \quad \because \text{cambio cuantificador } q \text{ por } q-1, \text{ ya que } k \geq 1 \\
 & H^0.C \vee \exists p, q : 1 \leq q \leq k+1 : n = 2^q(2p+1) \\
= & \quad \because \text{CP} \\
 & \exists p, q : 0 \leq q \leq k+1 : n = 2^q(2p+1)
\end{array}$$

6.69 [125] Pongamos un ejemplo:

$$\begin{array}{ccccc}
0 & & 1 & & 2 \\
\boxed{3} & \xrightarrow{\ \ 5\ \ } & \boxed{2} & \xrightarrow{\ \ 1\ \ } & \boxed{5} \\
 & & & & \\
2 \uparrow & & & & 3 \downarrow \\
 & & & & \\
\boxed{4} & \xrightarrow{\ \ 6\ \ } & \boxed{3} & \xrightarrow{\ \ 1\ \ } & \boxed{1} \\
5 & & 4 & & 3
\end{array}$$

donde el número en el recuadro indica el número d_i de litros disponible en la gasolinera e_i y el número en la flecha el gasto g_i en el recorrido; el otro número indica el índice de la estación. Sea:

$$D.i.j = \sum_{i \leq k < j} d_k - g_k$$

entendiéndose en el sumatorio las desigualdades $\leq$ y $<$ en sentido horario (módulo n); por ejemplo:

$$D.0.2 = 5 - 6 = -1 \qquad\qquad D.5.1 = 5 - 7 = -2$$

Para poder ir de la gasolinera e_i a la gasolinera e_j debe ocurrir $D.i.k \geq 0$, para todos los valores k del tramo $i \leq k \leq j$ (módulo n), ya que no podemos quedarnos sin gasolina en un tramo intermedio; o sea, debe ocurrir

$$\forall k : i \leq k \leq j : D.i.k \geq 0$$

Por consiguiente si definimos el predicado

$$S.x \doteq \forall i : x \leq i < x + 5 : D.x.i \geq 0$$

una estación e_x que sea solución del problema debe satisfacer el predicado anterior, y recíprocamente; por otro lado tenemos:

$$D.x.i. = D.0.i - D.0.x$$

y por tanto:

$$S.x \equiv \forall i : x \leq i < x + 5 : D.0.i \geq D.0.x$$

y todo consiste en encontrar un mínimo de la función $D.0.i$; por ejemplo, para el caso de la figura anterior tenemos:

i	0	1	2	3	4	5
$D.0.i$	0	-2	-1	1	1	-2

y las soluciones son las estaciones e_1 y e_5.

6.71 [125] Probaremos que el predicado I definido en la forma

$$I \doteq z + uy = xy \wedge x, y > 0 \wedge u \geq 0$$

es un invariante, ya que $I \wedge u = 0 \ \Rightarrow\ z = xy$, y además:

$$\begin{array}{ll} & z, u := 0, x.I \\ = & \quad \because \text{semántica} \\ & 0 + xy = xy \wedge x, y > 0 \\ = & \\ & x, y > 0 \end{array} \qquad \begin{array}{ll} & z, u := z + y, u - 1.I \\ = & \quad \because \text{semántica asignación} \\ & z + y + (u-1)y = xy \\ \wedge & \\ & x, y > 0 \wedge u - 1 \geq 0 \\ \Leftarrow & \\ & I \wedge u \neq 0 \end{array}$$

Para aplicar el Teorema de los Contadores basta probar que $t \doteq u$ es un contador, lo que es trivial ya que

$$[wdec(u := u - 1, t) \equiv C] \qquad\qquad [u \neq 0 \wedge I \ \Rightarrow\ (u =)t > 0]$$

6.72 [125] Basta probar que el predicado I definido en la forma

$$I \doteq b = \binom{n}{x} \wedge x + y = n + 1 \wedge y \geq 1 \wedge 0 \leq k \leq x \leq n$$

es un invariante, ya que $I \wedge x = k \ \Rightarrow\ b = \binom{n}{k}$. Veamos que I es cierto antes del comienzo del bucle:

$$\begin{array}{ll} & x, y, b := n, 1, 1, I \\ = & \quad \because \text{semántica} \end{array}$$

$$\begin{array}{ll} & 1 = \binom{n}{n} \wedge n+1 = n+1 \wedge y \geq 1 \wedge 0 \leq k \leq n \leq n \\ = & \\ & n \geq k \geq 0 \end{array}$$

La invariabilidad se prueba en la forma

$$\begin{array}{ll} & b := b * x \div y;\ x, y := x-1, y+1.I \\ = & \quad \because \text{semántica asignación} \\ & b := b * x \div y.b = \binom{n}{x-1} \wedge x - 1 + y + 1 = n+1 \\ \wedge & y+1 \geq 1 \wedge 0 \leq k \leq x-1 \leq n \\ = & \quad \because \text{semántica asignación} \\ & bx \div y = \binom{n}{x-1} \wedge x + y = n+1 \wedge y \geq 0 \wedge 0 \leq k \leq x-1 \leq n \\ \Leftarrow & \quad \because x\binom{n}{x} = (n-x+1)\binom{n}{x-1}, \text{ para } 0 \leq k \leq x \leq n \\ & I \wedge x \neq k \end{array}$$

Para aplicar el Teorema de los Contadores probamos que $t \doteq x$ es un contador, lo que es trivial ya que

$$[wdec(S,t) \equiv C] \qquad\qquad [x \neq k \wedge I \ \Rightarrow\ (x =)t > 0]$$

6.73 [125] Tenemos $\{b\}\mathcal{R}\{C\} \equiv [b \ \Rightarrow\ \mathcal{R}.C] \equiv [\neg b]$. Entonces, b debe ser F *ptle*, y en ese caso el bucle $\mathcal{R}$ equivale a $nada$. Interpretación: si queremos asegurar que termina el bucle con cuerpo $nada$, hay que asegurar *no entrar* en el bucle; es decir, hay que asegurar que b sea falso.

6.74 [126] Por ejemplo $\mathcal{S} \doteq [\![\neg b \rightarrow nada \,\square\, \neg b \rightarrow b := Falso]\!]$, ya que, *ptle*

$$\begin{array}{ll} & \mathcal{S}.X \\ = & \\ & [\![\neg b \rightarrow nada \,\square\, \neg b \rightarrow b := Falso]\!].X \\ = & \\ & \neg b \wedge (\neg b \ \Rightarrow\ nada.X) \wedge (\neg b \ \Rightarrow\ b := falso.X) \\ = & \\ & \neg b \wedge nada.X \wedge b := Falso.X \end{array}$$

En definitiva

$$[\ \mathcal{S}.X \ \equiv\ \neg b \wedge X \wedge b := Falso.X\ ] \qquad (*)$$

A partir de $(*)$ es fácil comprobar que

$$[S.(b=F) \equiv F] \qquad [S.(b=C) \equiv F] \qquad [S.(b=F \vee b=C) \equiv \neg b]$$

de donde S es indeterminista. Además, $[b \wedge \mathcal{S}.X = F]$.

Para el bucle $*[\![b \rightarrow \mathcal{S}]\!]$ todos los predicados H^k asociados verifican

$$\forall k : k \geq 0 : [b \wedge H^k.C \equiv F]$$

como se prueba fácilmente por inducción; el caso base es trivial, y el paso inductivo es, *ptle*

$$\begin{array}{ll} & b \wedge H^{k+1}.C \\ = & \quad \because \text{definición} \\ & b \wedge (H^0.C \vee b \wedge \mathcal{S}.H^k.C) \end{array}$$

$=\quad \because$ CP
$b \wedge \mathcal{S}.H^k.C$
$=\quad \because (*)$
$b \wedge (\neg b \wedge H^k.C \wedge b := Falso.(H^k.C))$
$=\quad \because$ cálculo
$Falso$

También se puede tomar $\mathcal{S} \doteq [\![\neg b \rightarrow T \,\square\, \neg b \rightarrow T']\!]$ siendo T indeterminista con $[T.C]$ y tal que no altere la variable b; es decir, que el predicado b sea invariante para T.

6.75 [126] (A).— Veremos tres soluciones: una basándonos en la Ayuda 1, otra solución más ingeniosa y sencilla, y una tercera solución basada en la Ayuda 2.

PRIMERA SOLUCIÓN.– Es trivial que $I \doteq |x| < K$ es un invariante, donde $K \doteq |x_0| + 1$, ya que $\{x = x_0\}\{I\}$, $[x := -x.I \equiv I]$ y

$$\begin{array}{ll} & x := x - 1.I \\ = & \\ & |x-1| < K \\ \Leftarrow & \\ & x > 1 \wedge x < K \end{array} \qquad \begin{array}{ll} & x := x \div 2.I \\ = & \\ & |x \div 2| < K \\ \Leftarrow & \\ & x > 2 \wedge I \end{array}$$

Además,

$$I \wedge \neg OB = I \wedge x \geq 0 \wedge x \leq 1 \overset{x\in\mathbb{Z}}{\Rightarrow} x = 0 \vee x = 1.$$

Luego, según el teorema de invariantes, ya que $[\neg OB \equiv x = 0 \vee x = 1]$, basta probar que el bucle termina; para ello probaremos que la siguiente función es un contador:

$$t(x) \doteq \begin{cases} K & \text{si} \quad x < 0 \\ x & \text{si} \quad x \geq 0 \end{cases}$$

Tenemos

$I \wedge x < 0 \wedge wdec(x := -x, t)$
$=\quad \because$ Lema 6.43
$I \wedge x < 0 \wedge t(-x) < t(x)$
$=\quad \because$ def. de t, con $-x > 0$
$I \wedge x < 0 \wedge x < K$
$=$
$I \wedge x < 0$

$I \wedge x > 1 \wedge wdec(x := x-1, t)$
$=\quad \because$ Lema 6.43
$I \wedge x > 1 \wedge t(x-1) < t(x)$
$=\quad \because$ def. de t, con $x - 1 > 0$
$I \wedge x > 0 \wedge x - 1 < x$
$=$
$I \wedge x > 1$

$I \wedge x > 2 \wedge wdec(x := x \div 2, t)$
$=\quad \because$ Lema 6.43
$I \wedge x > 2 \wedge t(x \div 2) < t(x)$
$=\quad \because$ definición de t, además de $x > 2 \;\Rightarrow\; x \div 2 > 0$
$I \wedge x > 2 \wedge x \div 2 < x$
$=$
$I \wedge x > 2$

y por la regla de oro (3 veces) obtenemos $[I \wedge b_i \;\Rightarrow\; wdec(S_i, t)]$. Queda probar $[I \wedge b_i \;\Rightarrow\; t > 0]$, lo cual es trivial.

SEGUNDA SOLUCIÓN.– Otra forma de resolver el problema consiste en considerar como invariante el predicado constante *Cierto* y el contador

$$t(x) = \begin{cases} |x| + 1 & \text{si} \quad x < 0 \\ x & \text{si} \quad x \geq 0 \end{cases}$$

Entonces, *ptle*,

$$
\begin{array}{ll}
 & x < 0 \wedge wdec(x := -x, t) \\
= & \\
 & x < 0 \wedge t(-x) < t(x) \\
= & \\
 & x < 0 \wedge (-x) < |x| + 1 \\
= & \\
 & x < 0
\end{array}
$$

y ahora aplicamos la regla de oro para obtener $[I \wedge x < 0 \Rightarrow wdec(x := -x, t)]$. El resto de implicaciones se estudien igual que antes.

TERCERA SOLUCIÓN.– Sigamos la AYUDA 2. Demostremos los dos tripletes que nos piden. Para probar el segundo se prueba que $I \doteq x \geq 0$ es un invariante (lo que es trivial). Además, es fácil probar (pruébese como ejercicio)

$$SI.X =_{x \geq 0} [\![\, x > 1 \rightarrow x := x - 1 \,\square\, x > 2 \rightarrow x := x \div 2 \,]\!]$$

donde la relación $S =_p S'$ se define en la forma siguiente:

$$S =_p S' \doteq \forall X :: [p \wedge S.X \equiv p \wedge S'.X]$$

y se lee: S y S' tienen el mismo comportamiento el entorno del predicado p. (para un estudio de la relación $S =_p S'$ véase el Ejercicio 8.71, pág. 182). Entonces, aplicando el Teorema 6.14 podemos eliminar la secuencia guardada $x < 0 \rightarrow x := -x$, y hemos de estudiar el siguiente bucle equivalente

$$
\begin{array}{lllll}
\mathcal{R} \doteq & *[\![& x > 1 & \rightarrow & x := x - 1 \\
 & \square & x > 2 & \rightarrow & x := x \div 2 \,]\!]
\end{array}
$$

para el cual $t \doteq x$ es trivialmente un contador. Veamos el primer triplete. Tenemos, *ptle*

$$
\begin{array}{ll}
 & x < 0 \wedge \mathcal{R}.(x = 0 \vee x = 1) \\
= & \quad \because \text{por Teorema 8.3, } [OB \wedge \mathcal{R}.Z \equiv OB \wedge SI; \mathcal{R}.Z] \\
 & x < 0 \wedge SI; \mathcal{R}.(x = 0 \vee x = 1) \\
= & \quad \because SI =_{x<0} x := -x \\
 & x < 0 \wedge x := -x.\mathcal{R}.(x = 0 \vee x = 1) \\
= & \quad \because \text{semántica asignación} \\
 & x := -x.(x > 0 \wedge \mathcal{R}.(x = 0 \vee x = 1)) \\
= & \quad \because \text{por el segundo triplete y la regla de Leibniz} \\
 & x := -x.(x > 0) \\
= & \quad \because \text{semántica asignación} \\
 & x < 0
\end{array}
$$

Luego, hemos probado $[x < 0 \equiv x < 0 \wedge \mathcal{R}.(x = 0 \vee x = 1)]$; de aquí, para obtener el primer triplete aplicamos la regla de oro y la definición de triplete.

$\underline{(B)}$.— Para probar que la sentencia es determinista, probaremos los tripletes

$$\{x \neq 0\}\mathcal{R}\{x = 1\} \qquad \{x = 0\}\mathcal{R}\{x = 0\}$$

El segundo triplete es trivial ya que para $x = 0$ todas las guardas son falsas. Obsérvese que el predicado $x \geq 1$ es invariante del bucle, y por el apartado

(A) el bucle termina, por tanto tenemos $[x > 0 \Rightarrow \mathcal{R}.(x = 1)]$; es decir, hemos demostrado el triplete

$$\{x > 0\}\mathcal{R}\{x = 1\} \tag{1}$$

Pero esto no es suficiente para probar el primer triplete. Razonando igual que en el apartado anterior tenemos, *ptle*

$x < 0 \wedge \mathcal{R}.(x = 1)$
$=$ $\quad\because$ por Teorema 8.3, $[OB \wedge \mathcal{R}.Z \equiv OB \wedge SI; \mathcal{R}.Z]$
$x < 0 \wedge SI; \mathcal{R}.(x = 1)$
$=$ $\quad\because$ igual que antes
$x < 0 \wedge x := -x.\mathcal{R}.(x = 1)$
$=$ $\quad\because$ semántica asignación
$x := -x.(x > 0 \wedge \mathcal{R}.(x = 1))$
$=$ $\quad\because$ por el triplete (1)
$x := -x.(x > 0)$
$=$ $\quad\because$ semántica asignación
$x < 0$

y esto último probaría el triplete $\{x < 0\}\mathcal{R}\{x = 1\}$ que junto a (1) establece una prueba de $\{x \neq 0\}\mathcal{R}\{x = 1\}$.

6.78 [126] Veamos primero (B). Supongamos,

$$\forall k : k \geq 0 : [\, H^k.C \equiv \neg f \vee N - k \leq x \leq N - 1 \,] \tag{0}$$

De aquí obtenemos, *ptle*, $\mathcal{R}.C$
$=$ $\quad\because$ semántica inductiva de los bucles
$\exists k : k \geq 0 : H^k.C$
$=$
$\exists k : k \geq 0 : \neg f \vee N - k \leq x \leq N - 1$
$=$
$\neg f \vee x < N$

Es decir, $[\mathcal{R}.C \equiv \neg f \vee x < N]$, y por tanto, *ptle*, $\mathcal{S}.C$
$=$ $\quad\because$ definición
$x := 0; f := Cierto; \mathcal{R}.C$
$=$ $\quad\because$ por lo anterior
$x := 0.f := Cierto.(x < N \vee \neg f)$
$=$ $\quad\because$ semántica asignación
$N > 0$

Probemos (0) por inducción sobre k,

— Caso Base. Trivial ya que $[H^0.C \equiv \neg f]$.

— Paso Inductivo:

$H^{k+1}.C$
$=$ $\quad\because$ definición
$H^0.C \vee SI.H^k.C$
$=$ $\quad\because$ semántica selectiva
$\neg f \vee f \wedge f := Falso.H^k.C$
$\wedge$

$$
\begin{array}{ll}
& x := x+1; [\![\, x = N \rightarrow f := Falso \,\Box\, x \neq N \rightarrow nada \,]\!] .H^k.C \\
= & \quad \because \text{HI} \\
& \neg f \vee f \wedge x := x+1; [\![\, x = N \rightarrow f := Falso \,\Box\, x \neq N \rightarrow nada \,]\!] .H^k.C \\
= & \quad \because \text{semántica selectiva} \\
& \neg f \vee f \wedge x := x+1.(x = N \wedge f := Falso.H^k.C \vee x \neq N \wedge H^k.C) \\
= & \quad \because \text{HI} \\
& \neg f \vee f \wedge x := x+1.(x = N \vee x \neq N \wedge (\neg f \vee N-k \leq x \leq N-1)) \\
= & \quad \because \text{semántica asignación, absorción, consenso dos veces} \\
& \neg f \vee x+1 = N \vee N-k \leq x+1 \leq N-1 \\
= & \quad \because \text{CP} \\
& \neg f \vee N-(k+1) \leq x \leq N-1
\end{array}
$$

El bucle puede terminar con $x = 0 \wedge f = Falso$ (el lector puede encontrar fácilmente una posible ejecución del programa). Queda claro que el predicado $0 \leq x < N$ no es invariante ¿y el predicado $0 \leq x \leq N$? (hágase como ejercicio). Veamos que el siguiente predicado más restrictivo es un invariante:

$$I \doteq 0 \leq x \leq N \wedge (x = N \Rightarrow \neg f) \wedge N > 0$$

Tenemos que

$$
\begin{array}{ll}
& x := 0; f := Cierto.I \\
= & 0 \leq 0 \leq N \wedge (0 = N \Rightarrow Falso) \wedge N > 0 \\
= & N > 0
\end{array}
$$

Por otro lado,

$$I \wedge f \equiv 0 \leq x < N \wedge f \tag{1}$$

De esto último concluimos, por un lado

$$
\begin{array}{ll}
& f := Falso.I \\
= & 0 \leq x \leq N \wedge N > 0 \\
\Leftarrow & \quad \because (1) \\
& I \wedge f
\end{array}
$$

y por otro lado

$$
\begin{array}{ll}
& x := x+1.[\![\, x = N \rightarrow f := Falso \,\Box\, x \neq N \rightarrow nada \,]\!] .I \\
= & \quad \because \text{semántica selectiva} \\
& x := x+1.((x = N \Rightarrow 0 \leq x \leq N \wedge N > 0) \wedge (x \neq N \Rightarrow I)) \\
= & \quad \because \text{cálculo, } N > 0 \\
& x := x+1.(x \neq N \Rightarrow I) \\
= & \quad \because \text{CP} \\
& x := x+1.(0 \leq x \leq N) \\
= & \quad \because \text{semántica asignación} \\
& 0 \leq x+1 \leq N \\
\Leftarrow & \quad \because (1) \\
& I \wedge f
\end{array}
$$

Por tanto, I es un invariante. Además, *ptle*, $I \wedge \neg f$

$=$ $\quad \because (a \Rightarrow \neg f) \wedge \neg f \equiv \neg f$

$0 \leq x \leq N \wedge \neg f \wedge N > 0$

$\Rightarrow$

$0 \leq x \leq N$

En definitiva, si el bucle termina, lo hace verificando $0 \leq x \leq N$, y hemos demostrado la corrección parcial de

$$\{N > 0\}\mathcal{S}\{0 \leq x \leq N\}$$

Podemos probar la terminación directamente a través del contador

$$t \doteq \begin{cases} N+1-x, & \text{si } f \\ 0, & \text{si } \neg f \end{cases}$$

Probaremos las siguientes implicaciones, *ptle*

(2) $[I \wedge f \Rightarrow t > 0]$,
(3) $[I \wedge f \Rightarrow wdec(f := Falso, t)]$,
(4) $[I \wedge f \Rightarrow wdec(x := x+1; SI \mid t)]$.

$I \wedge f \wedge t > 0$

$=$ $\quad \because (1)$, definición de t

$0 \leq x \leq N \wedge f \wedge N+1-x > 0$

$=$ $\quad \because (1)$

$I \wedge f$

lo que prueba (2).

$f \wedge wdec(f := Falso, t)$

$=$ $\quad \because$ Lema 6.43

$f \wedge f := Falso.t(f) < t(f)$

$=$ $\quad \because$ semántica asignación

$t \wedge t(Falso) < t(f)$

$=$ $\quad \because$ definición de t

$f \wedge 0 < N+1-x$

$\Leftarrow$ $\quad \because (2)$

$I \wedge f$

lo que prueba (3).

Finalmente, veamos (4). Por el Ejercicio 6.50, basta demostrar, *ptle*

(5_1) $I \wedge f \Rightarrow wdec(x := x+1, t)$
(5_2) $\{I \wedge f\}x := x+1\{0 \leq x-1 < N \wedge f\}$
(5_3) $0 \leq x-1 < N \wedge f \wedge t < t_0 \Rightarrow SI.(t < t_0)$

Tenemos, *ptle*,

$I \wedge f \wedge wdec(x := x+1, t)$

$=$ $\quad \because$ Lema 6.43

$I \wedge f \wedge (x := x+1.t) < t$

$=$ $\quad \because$ definición de t

$I \wedge f \wedge N+1-(x+1) < N+1-x$

$=$

$I \wedge f$

y ahora basta aplicar la regla de oro para obtener (5_1). Veamos (5_2):

$x := x+1.(0 \leq x-1 < N \wedge f)$

$=$

$0 \leq x < N \wedge f$

$=$ $\quad \because (1)$

$I \wedge f$

Y finalmente, veamos (5_3). Por el teorema fundamental de la sentencia selectiva, basta probarlo para las dos guardas:

$$\begin{array}{lcl} 0 \leq x-1 < N \wedge f \wedge t < t_0 \wedge x = N & \Rightarrow & f := Falso.(t < t_0) \\ 0 \leq x-1 < N \wedge f \wedge t < t_0 \wedge x \neq N & \Rightarrow & nada.(t < t_0) \end{array}$$

La segunda es trivial, y la primera es muy fácil:

$$\begin{array}{ll} & f := Falso.(t < t_0) \\ = & \\ & 0 < t_0 \\ \Leftarrow & \\ & 0 \leq t < t_0 \\ \Leftarrow & \qquad \because \text{ya que } f \wedge 0. \leq x-1 < N \;\Rightarrow\; t = N - x + 1 (> 0) \\ & 0 \leq x-1 < N \wedge f \wedge t < t_0 \end{array}$$

La distribución de probabilidades es $P[x = k] = 2^{-k}$, ya que

$$P[x = 0] = \frac{1}{2} \qquad\qquad P[x = k] = \frac{1}{2}P[x = k-1], \text{ para } k > 0$$

Para una distribución binomial, $P[x = k] \doteq \begin{pmatrix} N \\ k \end{pmatrix} p^k(1-p)^{N-k}$, puede servir el programa

$$i := 1; *[\![\, i \leq n \rightarrow [\![\, C \rightarrow x := x + 1 \,\Box\, C \rightarrow nada \,]\!] \,]\!]$$

Para obtener con una distribución uniforme de números de N cifras, podemos utilizar el programa:

$$\begin{array}{lcllll} i := 0; x := 0 & & & & & \\ *[\![\, i \leq N & \rightarrow & [\![& C & \rightarrow & x := x + 10^i \\ & & \Box & C & \rightarrow & x := x + 2 * 10^i \\ & & & & \ldots & \\ & & \Box & C & \rightarrow & x := x + 9 * 10^i \,]\!] \;;\; i := i + 1 \,]\!] \end{array}$$

Otro ejemplo es:

$$\begin{array}{l} \{N > 1\} \\ a, c := 1, 1; \\ *[\![\, c < N \rightarrow a, c := a + 1, c + 1 \\ \;\Box\, c < N \rightarrow c := N \,]\!] \\ \{1 \leq a \leq N\} \end{array}$$

con distribución de probabilidades:

$$P[a = k] = \begin{cases} 2^{-k}, & \text{si } 1 \leq k < N \\ 2^{N-1}, & \text{si } K = N \end{cases}$$

y, finalmente, otro con idénticas probabilidades es:

$$\begin{array}{lll} a, b := Cierto, Cierto; & & \\ *[\![\, a \rightarrow & N := N - 1; & \\ & [\![\quad N = 1 & \rightarrow a := Falso \\ & \;\Box \quad N \neq 1 & \rightarrow nada \,]\!] \\ \;\Box\, b \rightarrow & a, b := Falso, Falso \,]\!] & \end{array}$$

7.5 [132] Sea la poscondición:

$$R \doteq k = \textit{número de llanos de } b[0..n-1]$$

Sustituyendo la constante n por una variable obtenemos el candidato a invariante:

$$I \doteq 0 \leq i \leq n \wedge k = \text{ número de llanos de } b[0..i-1]$$

Podemos observar que, por ser b una tabla ordenada, al igual que vimos en el Ejemplo 7.4,

$$I \equiv 0 \leq i \leq n \wedge k = (Nj : 1 \leq j < p \leq n : b[j-1] \neq b[j]) + 1$$

y tenemos el esquema:

$$\begin{array}{l} \{n > 0\} i, k := 1, 0; \{I\} \\ *[\![\, i < n \rightarrow \textit{incrementar } i \textit{ con invariabilidad de } I \,]\!] \\ \{R\} \end{array}$$

Además:

$$\begin{array}{ll} & i := i + 1.I \\ = & \\ & 0 \leq i + 1 \leq n \wedge k = \text{número de llanos de } b[0..i] \\ \Leftarrow & \\ & i < n \wedge I \wedge b[i-1] = b[i] \end{array}$$

y es fácil demostrar que I es invariante para el bucle:

$$\begin{array}{llll} *[\![\, i < n \rightarrow & [\![& b[i-1] = b[i] & \rightarrow \quad i := i + 1 \\ & \square & b[i-1] \neq b[i] & \rightarrow \quad i, k := i + 1, k + 1 \,]\!] \quad]\!] \end{array}$$

7.7 [133] Se observa que en el bucle interno dd es un múltiplo de d; sea el nuevo invariante para el bucle interno:

$$J \doteq d \mid (a - r) \wedge 0 \leq r < d \wedge d \mid dd \wedge dd \geq 0$$

Puesto que el anterior I era invariante, lo es el nuevo para el bucle externo y el propio $t \doteq r$ sigue siendo un contador. Hay que probar que J es invariante del bucle interno; es decir, la corrección de:

$$\begin{array}{llll} *[\![& r \geq d \rightarrow & \{I\} & \\ & & dd := d; & \\ & & \{J\} & \\ & & *[\![\, r \geq dd \rightarrow & r := r - dd; \\ & & & dd := dd + dd \,]\!] \\ & & \{J\} \{ \Rightarrow \} \{I\} & \\ ]\!] & & & \end{array}$$

El primer triplete es trivial; para la invariabilidad del segundo tenemos:

$$\begin{array}{ll} & r := r - dd; dd := dd + dd.J \\ = & \quad \because \text{semántica} \\ & r := r - dd.(d \mid (a - r) \wedge 0 \leq r < d \wedge d \mid 2dd \wedge 2dd \geq 0) \\ = & \quad \because \text{semántica} \end{array}$$

$$
\begin{array}{ll}
 & d \mid (a-r-dd) \wedge 0 \le r - dd < d \wedge d \mid 2dd \wedge 2dd \ge 0 \\
\Leftarrow & \qquad \because x \mid u \wedge x \mid v \;\Rightarrow\; x \mid u - v \\
 & d \mid (a-r) \wedge d \mid dd \wedge 0 \le r - dd < d \wedge dd \ge 0 \\
\Leftarrow & \\
 & d \mid (a-r) \wedge d \mid dd \wedge dd \le r \wedge r < d + dd \wedge dd \ge 0 \\
\Leftarrow & \\
 & dd \le r \wedge d \mid (a-r) \wedge d \mid dd \wedge 0 \le r < d \wedge dd \ge 0 \\
\Leftarrow & \\
 & dd \le r \wedge J
\end{array}
$$

La función $t \doteq r$ es un contador del bucle interno, por lo que éste termina; para probar que también es contador del externo, sea S el cuerpo del bucle interno, y $\mathcal{R} \doteq *[\![\, r \ge dd \to S \,]\!]$ el bucle interno; vamos a demostrar el triplete

$$\{r = k \wedge dd \ge 0\}\mathcal{R}\{r < k\}$$

Tenemos, *ptle*

$$
\begin{array}{ll}
 & r = k \wedge dd \ge 0 \wedge \mathcal{R}.(r < k) \\
= & \qquad \because \text{por Teorema 8.3, } [b \wedge \mathcal{R}.X = b \wedge S; \mathcal{R}.X] \text{, tomando } b == r \ge dd \\
 & r = k \wedge dd \ge 0 \wedge r := r - dd; dd := dd + dd.\mathcal{R}.(r < k) \\
= & \qquad \because \text{semántica asignación} \\
 & r = k \wedge r := r - dd; dd := dd + dd. \\
 & \qquad (r = k - dd \wedge r < k \wedge dd \ge 0 \wedge \mathcal{R}.(r < k)) \\
= & \qquad \because \mathcal{R} \text{ termina, } r < k \wedge dd \ge 0 \text{ es invariante de } \mathcal{R} \text{, y regla de oro} \\
 & r = k \wedge r := r - dd; dd := dd + dd.(r = k - dd \wedge r < k \wedge dd \ge 0) \\
= & \qquad \because \text{semántica asignación} \\
 & r = k \wedge dd \ge 0
\end{array}
$$

Es decir, hemos demostrado

$$[r = k \wedge dd \ge 0 \wedge \mathcal{R}.(r < k) \equiv r = k \wedge dd \ge 0]$$

y por la regla de oro, $[r = k \wedge dd \ge 0 \;\Rightarrow\; \mathcal{R}.(r < k)]$, y en consecuencia $[dd \ge 0 \;\Rightarrow\; wdec(\mathcal{R}, t)]$.

7.10 [134] Podemos dar un esquema en la forma:

$$
\begin{array}{l}
i := 0; \{I\} \\
*[\![\, i < m \to [\![\, x \ne b[i] \to \boxed{?} \,\square\, \ldots \,]\!] \\
]\!] \\
\{I \wedge \neg b\}\{\Rightarrow\}\{R\}
\end{array}
$$

donde el invariante es parecido al anterior. Sin embargo la verificación (y el diseño) son más engorrosas. En este caso veremos que un pequeño truco permite resolver el problema de forma más elegante; sea la tabla $c[0..m]$:

$$c[i] = \begin{cases} b[i] & \text{si} \quad 0 \le i < m \\ x & \text{si} \quad i = m \end{cases}$$

Entonces se tiene el siguiente programa *correcto*:

$$
\begin{array}{l}
\{P'\}(\doteq m > 0 \wedge x \in c[0..m]) \\
i := 0; \\
\{I\} \\
*[\![\, x \ne c[i] \to i := i + 1 \,]\!] \\
\{R'\}(\doteq 0 \le i < m + 1 \wedge x \notin c[0..i-1] \wedge x = c[i])
\end{array}
$$

y trivialmente $[R' \Rightarrow R]$.

Otra forma, sin utilizar una tabla auxiliar, parte de los predicados

$$\begin{array}{lcl} I & \doteq & b(1) \leq x \leq b[j] \wedge 1 \leq j < n \\ \neg b & \doteq & b[j-1] \leq x \vee j = 2 \end{array}$$

y el programa (cuya corrección se deja como ejercicio)

$$\begin{array}{l} \{P'\} \\ j := n; \\ *[\![\, b[j-1] > x \wedge j \neq 2 \rightarrow j := j-1 \,]\!] \, \{R\} \end{array}$$

7.15 [139] Supongamos $n \geq 0$ un predicado universal (incluido en todos); sea:

$$P \doteq a^2 \leq n < (a+c)^2 \wedge (\exists i : i \geq 0 : c = 2^i)$$

Vamos a probar la corrección de:

$$\begin{array}{l} \{n \geq 0\} \\ a, c := 0, 1; \\ \{I_1\}(\doteq a = 0 \wedge 0 \leq n \wedge \exists i : i \geq 0 : c = 2^i) \\ *[\![\, c^2 \leq n \rightarrow c := 2 * c \,]\!] \\ \{a = 0, 0 \leq n \wedge (\exists i : i \geq 0 : c = 2^i) \wedge n < c^2\} \\ \{P(a,c)\}(\doteq a^2 \leq n < (a+c)^2 \wedge (\exists i : i \geq 0 : c = 2^i \,) \,) \\ \quad *[\![\, c \neq 1 \rightarrow \quad \{P(a,c) \wedge c \geq 2\} \\ \qquad\qquad\qquad\quad c := c/2; \\ \qquad\qquad\qquad\quad \{P(a, 2c) \wedge c \geq 1\} \\ \qquad\qquad\qquad\quad [\![\quad (a+c)^2 \leq n \quad \rightarrow \quad a := a + c \\ \qquad\qquad\qquad\quad \ \ \square \quad (a+c)^2 > n \quad \rightarrow \quad nada \,]\!] \\ \qquad\qquad\qquad\quad \{P(a,c)\} \qquad\qquad\qquad\qquad - (2) \\ \quad]\!] \\ \{P \wedge c = 1 \Rightarrow a^2 \leq n < (a+1)^2\} \end{array}$$

Es fácil ver que el predicado I_1 es un invariante del primer bucle:

$$\begin{array}{ll} & c := 2 * c.I_1 \\ = & \\ & c := 2 * c.(a = 0 \wedge 0 \leq n \wedge (\exists i : i \geq 0 : c = 2^i)) \\ = & \quad \because \text{semántica} \\ & a = 0 \wedge 0 \leq n \wedge (\exists i : i \geq 0 : 2c = 2^i) \\ \Leftarrow & \\ & a = 0 \wedge 0 \leq n \wedge (\exists i : i \geq 0 : c = 2^i) \\ = & \\ & I_1 \end{array}$$

Un contador de este bucle es $t \doteq n - c^2$. En efecto, *ptle*

$$\begin{array}{ll} & c := 2c.(n - c^2) < n - c^2 \\ = & \\ & n - 4c^2 < n - c^2 \\ \Leftarrow & \\ & c > 0 \\ \Leftarrow & \\ & I_1 \end{array}$$

y por tanto $[I_1 \Rightarrow wdec(c := 2c, t]$. Además $[I_1 \wedge b \Rightarrow t > 0]$. Queda probar la invariabilidad de P en el punto (2); pero tenemos:

$$
\begin{array}{l}
\quad a := a + c.P \\
= \\
\quad (a+c)^2 \leq n < (a+2c)^2 \wedge (\exists i : i \geq 0 : c = 2^i) \\
\Leftarrow \\
\quad (a+c)^2 \leq n \wedge P(a,2c) \wedge c \geq 1
\end{array}
$$

además, *ptle*, $nada.P \equiv P \;\Leftarrow\; P(a,2c) \wedge c \geq 1$; luego

$$
\begin{array}{l}
\quad [\![\, (a+c)^2 \leq n \rightarrow a := a + c \,\square\, (a+c)^2 > n \rightarrow nada \,]\!] .P \\
\Leftarrow \\
\quad P(a,2c) \wedge c \geq 1
\end{array}
$$

7.30 [156] Q puede escribirse en la forma:

$$Q \equiv \forall i : 1 \leq i \leq \lfloor n/2 \rfloor : a[i] = A_{n-i+1} \wedge a[n-i+1] = A_i$$

Podemos derivar un invariante sustituyendo la constante $\lfloor n/2 \rfloor$ por una variable h, pero tenemos que añadir condiciones para la parte central; por ejemplo tomamos:

$$I \;\doteq\; I_1(h) \wedge I_2(h) \wedge 0 \leq h \leq \lfloor n/2 \rfloor$$

donde

$$
\begin{array}{lcl}
I_1 & \doteq & \forall i : 1 \leq i \leq h : a[i] = A_{n-i+1} \wedge a[n-i+1] = A_i \\
I_2 & \doteq & \forall i : h < i \leq \lfloor n/2 \rfloor : a[i] = A_i \wedge a[n-i+1] = A_{n-i+1}
\end{array}
$$

de donde el programa:

$$
\begin{array}{l}
h := 0; \{I\} \\
*[\![\, h \neq \lfloor n/2 \rfloor \rightarrow h := h+1; inter(a[h], a[n-h+1]) \,]\!]
\end{array}
$$

donde $inter(a[h], a[n-h+1]) \;\doteq\; a[h], a[n-h+1] := a[n-h+1], a[h]$. Entonces $P \;\Rightarrow\; I_1(0) \wedge I_2(0)$. Además

$$
\begin{array}{l}
\quad h := h+1.inter(a[h], a[n-h+1]).(I_1(h) \wedge I_2(h) \wedge 0 \leq h \leq \lfloor n/2 \rfloor) \\
= \\
\quad h := h+1.inter(a[h], a[n-h+1]). \\
\quad I_1(h-1) \wedge I_2(h) \wedge a[h] = A_{n-h+1} \wedge a[n-h+1] = A_h \wedge 0 \leq h \leq \lfloor n/2 \rfloor \\
= \qquad \because \text{semántica de } inter \\
\quad h := h+1. \\
\quad I_1(h-1) \wedge I_2(h) \wedge a[n-h+1] = A_{n-h+1} \wedge a[h] = A_h \wedge 0 \leq h \leq \lfloor n/2 \rfloor \\
= \qquad \because \text{semántica asignación} \\
\quad I_1(h) \wedge I_2(h+1) \wedge a[n-h+1] = A_{n-h+1} \wedge a[h] = A_h \wedge \\
\quad 0 \leq h+1 \leq \lfloor n/2 \rfloor \\
= \qquad \because \text{definición de } I_2(h) \\
\quad I_1(h) \wedge I_2(h) \wedge 0 \leq h < \lfloor n/2 \rfloor
\end{array}
$$

7.34 [156] Para la poscondición $\{m = Msa(n)\}$, donde

$$Msa(n) \;\doteq\; \text{máx}\{j - i \,|\, 0 \leq i < j \leq n \wedge as(i,j)\}$$

cambiamos la constante n por una variable k para obtener un invariante:

$$I \;\doteq\; 0 < k \leq n \wedge m = Msa(k)$$

y el esquema:

$$
\begin{array}{l}
k, m := 1, 1; \{I\} \\
*[\![\, k < n \rightarrow \textit{incrementar } k \textit{ con invariabilidad de } I \\
\{I \wedge k \geq n\} \; \{\Rightarrow\} \; \{m = Msa(k)\}
\end{array}
$$

Si consideramos el contador $t \doteq n - k$, la sentencia $k := k + 1$ decrementa el contador y hay que estudiar:

$$\begin{array}{l} Msa(k+1) \\ = \\ \text{máx}\{M_j \mid 0 < j \leq k+1\} \\ = \\ \text{máx}(\text{máx}\{M_j \mid 0 < j \leq k\}, M_{k+1}) \\ = \\ \text{máx}(Msa(k), M_{k+1}) \end{array}$$

Pero por otro lado se verifica:

$$M_{k+1} = \begin{cases} M_k + 1 & \text{si} \quad a[k-1] \leq a[k] \\ 1 & \text{si} \quad a[k-1] > a[k] \end{cases}$$

de donde, si introducimos una nueva variable p para memorizar el valor de M_k, y consideramos el nuevo invariante:

$$I \doteq 0 < k \leq n \wedge m = Msa(k) \wedge p = M_k$$

obtenemos el siguiente programa correcto:

$$\begin{array}{ll} k, m, p := 1, 1, 1; & \\ \{I\} & \\ *[\![\, k < n \rightarrow & [\![\, a[k-1] \leq a[k] \rightarrow p := p + 1 \\ & \;\square\, a[k-1] > a[k] \rightarrow p := 1 \quad]\!] \\ & m := \text{máx}(m, p); \\ & k := k + 1 \;\;]\!] \end{array}$$

7.35 [156] Sea la poscondición

$$R \quad \doteq \quad a[0..n-1] \text{ es un array ordenado con los } n \text{ primeros números de Hamming,}$$

de la cual podemos derivar el invariante:

$$P \quad \doteq \quad a[0..i-1] \text{ contiene los } i \text{ primeros números de Hamming } \wedge 0 \leq i \leq n$$

de donde el esquema:

$$\begin{array}{ll} i, a[0] := 1, 1; & \\ \{I\} & \\ *[\![\, i < n \rightarrow & \textit{calcular sig } (\equiv i\text{–ésimo número de Hamming}); \\ & i, a[i] := i + 1, sig \;\;]\!] \end{array}$$

El problema es calcular sig. Este será un producto de la forma $2x$ o $3x$ o $5x$, con $x \in b[0..i-1]$ y entre todos ellos el menor que es mayor que $b[i-1]$. Si consideramos tres variables $x2, x3, x5$ tales que se cumpla

$$\begin{array}{ll} P1 \doteq & x2 \text{ es el menor valor} > a[i-1] \text{ de la forma } 2 * x, x \in a[0..i-1] \wedge \\ & x3 \text{ es el menor valor} > a[i-1] \text{ de la forma } 3 * x, x \in a[0..i-1] \wedge \\ & x5 \text{ es el menor valor} > a[i-1] \text{ de la forma } 5 * x, x \in a[0..i-1] \end{array}$$

queda claro que el siguiente número de Hamming es

$$sig = \text{mín}(x2, x3, x5)$$

Tomando como nuevo invariante $I \doteq P \wedge P1$, obtenemos el nuevo esquema

$$\begin{array}{l} i, a[0], x2, x3, x5 := 1, 1, 2, 3, 5\{I\} \\ \ast[\![\, i < n \rightarrow \quad i, a[i] := i+1, \text{mín}(x2, x3, x5); \\ \qquad\qquad\qquad \textit{restablecer el invariante } I \,]\!] \end{array}$$

Podemos asociar a las variables $x2, x3$ y $x5$ tres índices $j2, j3$ y $j5$ de forma que, para $i \geq 1$:

$$\begin{array}{rl} P1 \equiv & j2 = \text{mín}\{0 \leq j \leq i-1 \mid a[i-1] < 2 * a[j]\} \wedge x2 = 2 * a[j2] \wedge \\ & j3 = \text{mín}\{0 \leq j \leq i-1 \mid a[i-1] < 3 * a[j]\} \wedge x3 = 3 * a[j3] \wedge \\ & j5 = \text{mín}\{0 \leq j \leq i-1 \mid a[i-1] < 5 * a[j]\} \wedge x5 = 5 * a[j5] \end{array}$$

y obtenemos el esquema:

$$\begin{array}{l} i, a[0], x2, x3, x5, j2, j3, j5 := 1, 1, 2, 3, 5, 0, 0, 0 : \{I\} \\ \ast[\![\, i < n \rightarrow \\ \qquad i, a[i] := i+1, \text{mín}(x2, x3, x5); \\ \qquad \ast[\![\, x2 \leq a[i-1] \rightarrow j2 := j2+1; x2 := 2 * a[j2] \,]\!]\,; \\ \qquad \ast[\![\, x3 \leq a[i-1] \rightarrow j3 := j3+1; x3 := 3 * a[j3] \,]\!]\,; \\ \qquad \ast[\![\, x5 \leq a[i-1] \rightarrow j5 := j5+1; x5 := 5 * a[j5] \,]\!] \\ ]\!] \end{array}$$

7.36 [157] Introducimos los siguientes predicados

$$\begin{array}{l} u, v := x, 1; \\ \{P\} \ (\equiv u = x \wedge v = 1) \\ \ast[\![\, u \leq 100 \vee v \neq 1 \rightarrow \quad [\![\quad u > 100 \ \rightarrow \ u, v := u - 10, v - 1 \\ \qquad\qquad\qquad\qquad\qquad\quad \Box \quad u \leq 100 \ \rightarrow \ u, v := u + 11, v + 1 \,]\!] \\ \ ]\!]\,; \\ \{R\} \ (\equiv u = x \wedge x > 100 \vee u = 101 \wedge x \leq 100) \\ z := u - 10 \\ \{z = x - 10 \wedge x > 100 \vee z = 91 \wedge x \leq 100\} \end{array}$$

Basta probar la corrección para el bucle $\mathcal{R}$. Se observa que tal bucle es determinista; por tanto es suficiente probar, *ptle*

$$P \wedge x > 100 \ \Rightarrow \ \mathcal{R}.(u = x \wedge x > 100) \tag{a}$$

$$P \wedge x \leq 100 \ \Rightarrow \ \mathcal{R}.(u = 101 \wedge x \leq 100) \tag{b}$$

(a) es trivial ya que

$$P \wedge x > 100 \ \Rightarrow \ \neg b \wedge P \ \Rightarrow \ \neg(u \leq 100 \vee v \neq 1) \ \Rightarrow \ \mathcal{R}.(\neg b \wedge P).$$

Para probar (b) observamos las sentencias del cuerpo del bucle:

$$u, v := u - 10, v - 1 \qquad\qquad u, v := u + 11, v + 1$$

de donde se desprende que los sucesivos valores de u y v son de la forma:

$$u = x + 11k - 10q \qquad v = 1 + k - q \qquad \text{con } k, q \geq 0.$$

Si consideramos el candidato a invariante:

$$\begin{array}{lcl} I & \doteq & x \leq 100 \wedge np = 2(101 - x) - k - q \geq 0 \wedge \\ & & u = x + 11k - 10q \wedge v = 1 + k - q \wedge k, q \geq 0 \end{array}$$

se observa que

$$\begin{array}{ll} & I \wedge u > 100 \wedge v = 1 \\ \Rightarrow & \\ & k = q \wedge u = x + k \wedge np = 2(101 - u) \geq 0 \\ \Rightarrow & \quad \because np \geq 0 \\ & 101 \geq u \end{array}$$

de donde:

$$I \wedge u > 100 \wedge v = 1 \;\Rightarrow\; u = 101$$

Por tanto, salvo la invariabilidad de I y la terminación hemos probado:

$$\begin{array}{l} \{x \leq 100\} \\ u, v, k, q, np := x, 1, 0, 0, 2(101 - x); \\ \{I\} \\ \;*[\![\, u \leq 100 \vee v \neq 1 \rightarrow \quad np := np - 1; \\ \qquad\qquad\qquad\qquad\qquad [\![\quad u > 100 \rightarrow u, v, q := u - 10, v - 1, q + 1 \\ \qquad\qquad\qquad\qquad\qquad \Box \quad u \leq 100 \rightarrow u, v, k := u + 11, v + 1, k + 1 \,]\!] \\ \;]\!] \\ \{I \wedge u > 100 \wedge v = 1\}\{u = 101\} \end{array}$$

La invariabilidad de I es muy fácil, y para probar que el bucle termina basta tomar como contador np.

7.37 [157] Se considera el invariante resultado de introducir dos variables

$$I \;\doteq\; P \wedge s = \sum_{0 \leq i < j} f(i) \wedge t = (s < 1000) \wedge j \leq n$$

de forma que el programa es

$$\begin{array}{l} \{P\} \\ Init; *[\![\, j < n \wedge t \rightarrow S \,]\!] \\ \{t = \sum_{0 \leq i < n} f(i) < 1000\} \end{array}$$

(A) Probaremos

$$\begin{array}{lll} & I \wedge \neg(j < n \wedge t) \;\Rightarrow\; t = \sum_{0 \leq i < n} f(i) < 1000 & \\ = & & \\ & I \wedge j \geq n \;\Rightarrow\; t = \sum_{0 \leq i < n} f(i) < 1000 & (1) \\ \wedge & & \\ & I \wedge \neg t \;\Rightarrow\; t = \sum_{0 \leq i < n} f(i) < 1000 & (2) \end{array}$$

$$\begin{array}{ll} & I \wedge j \geq n \\ \Rightarrow & \quad \because I \;\Rightarrow\; j \leq n \end{array}$$

$$
\begin{array}{l}
\quad I \land j = n \\
\Rightarrow \\
\quad t = \sum_{0 \le i < n} f(i) < 1000
\end{array}
$$

lo que prueba (1). Para probar (2), tenemos

$$
\begin{array}{l}
\quad I \land \neg t \\
\Rightarrow \\
\quad I \land s \ge 1000 \land \neg t \\
\Rightarrow \qquad \because \text{todos los } f(i) \text{ son positivos} \\
\quad \sum_{0 \le i < n} f(i) \ge 1000 \land \neg t \\
\Rightarrow \\
\quad t = \sum_{0 \le i < n} f(i) < 1000
\end{array}
$$

(B) La inicialización puede ser $Init \doteq t, j, s := Cierto, 0, 0$ ya que, *ptle*

$$Init.I \ \equiv\ P \land 0 = 0 \land Cierto = (0 < 1000) \land 0 \le n \ \Leftarrow\ P$$

(C) Por otro lado, la sentencia $j := j + 1$ destruye el invariante, que puede establecerse alterando convenientemente las variables s y t:

$$
\begin{array}{l}
\quad s := s + f(j); t, j := s < 1000, j + 1.I \\
= \\
\quad s := s + f(j).(P \land s = \sum_{0 \le i < j} f(i) + f(j) \land j + 1 \le n) \\
= \\
\quad P \land s + f(j) = \sum_{0 \le i < j} f(i) + f(j) \land j + 1 \le n \\
\Leftarrow \\
\quad I \land j < n
\end{array}
$$

7.40 [157] Consideremos la poscondición $R \doteq x2 = a_{1000}$. No puede derivarse un invariante si no introducimos algunas variables adicionales para recordar los valores anteriores, por lo que se considera la poscondición

$$R \doteq x0 = a_{998} \land x1 = a_{999} \land x2 = a_{1000}$$

y cambiamos 1000 por $k + 2$, de donde el candidato a invariante

$$I \doteq x0 = a_k \land x1 = a_{k+1} \land x2 = a_{k+2} \land 0 \le k \le 998$$

que es trivialmente cierto después de las asignaciones

$$k := 0; x0, x1, x2 := 1, 1, 1; \{I\}$$

de donde el esquema

$$
\begin{array}{l}
k := 0; x0, x1, x2 := 1, 1, 1; \{I\} \\
*[\![\, k \ne 998 \to \mathcal{S} \,]\!]
\end{array}
$$

El contador $t \doteq 1000 - k$ se decrementa para la sentencia $k := k + 1$, aunque esta sentencia no conserva el invariante; sí lo conserva la sentencia

$$k, x0, x1, x2 := k + 1, x1, x2, x1 * x2 + x3$$

ya que tenemos

$$\begin{array}{ll} & k, x0, x1, x2 := k+1, x1, x2, x1 * x2 + x3.I \\ = & \\ & x1 = a_{k+1} \wedge x2 = a_{k+2} \wedge x1 * x2 + x0 = a_{k+3} \wedge 0 \leq k+1 \leq 998 \\ \Leftarrow & \\ & I \wedge k \neq 998. \end{array}$$

7.42 [158] Sea $M3$ el conjunto de múltiplos de 3. Escribamos la precondición en la forma

$$P \equiv a[0..n-1] \subseteq \mathbb{Z} \wedge a\!\uparrow \;\; \wedge a(n-1) \in M3 \wedge n > 0.$$

y la poscondición en la forma

$$R \equiv a(x) \in M3 \wedge a[0..x-1] \cap M3 = \emptyset \wedge 0 \leq x < n \wedge P,$$

de donde

$$R \;\Rightarrow\; a(x) \text{ es el menor múltiplo de 3 de } a[0..n-1].$$

R puede debilitarse eliminando el predicado $a(x) \in M3$ para obtener el candidato a invariante

$$I \doteq a[0..x-1] \cap M3 = \emptyset \wedge 0 \leq x < n \wedge P$$

de donde el programa

$$\begin{array}{l} \{P\} \\ x := 0; \{I\} \\ *[\![\, a(x) \notin M \rightarrow x := x+1 \,]\!] \\ \{I \wedge a(x) \in M3 \equiv R\} \end{array}$$

En efecto:

$$\begin{array}{ll} & x := 0.I \\ = & \\ & a[0..-1] \cap M3 = \emptyset \wedge 0 \leq 0 < n \wedge P \\ \Leftarrow & \qquad \because a[0..-1] = \emptyset \\ & P \end{array}$$

La invariabilidad es consecuencia de

$$\begin{array}{ll} & x := x+1.I \\ = & \\ & a[0..x] \cap M3 = \emptyset \wedge 0 \leq x+1 < n \wedge P \\ \Leftarrow & \qquad \because (A \cup A') \cap M = \emptyset \;\Leftarrow\; A \cap M = \emptyset \wedge A' \cap M = \emptyset \\ & a[0..x-1] \cap M3 = \emptyset \wedge a(x) \notin M3 \wedge x+1 < n \wedge P \\ \Leftarrow & \\ & a(x) \notin M3 \wedge I \wedge x+1 < n \\ \Leftarrow & \qquad \because a(n-1) \in M3 \;\Leftarrow\; P \\ & a(x) \notin M3 \wedge I \end{array}$$

Finalmente, $t \doteq n - x$ es un contador, ya que, además de decrementarse

$$a(x) \notin M3 \wedge I \;\Rightarrow\; x+1 < n \;\Rightarrow\; t > 0.$$

7.43 [158] Consideramos la precondición

$$P \doteq a, b, c \uparrow \text{ estrictamente}, m, n, s \geq 0$$

universal; la poscondición se escribe $R \doteq u = \operatorname{card} A(n, m, s)$, donde

$$A(p, q, r) \doteq \{(i, j, k) \mid 0 \leq i < p, 0 \leq j < q, 0 \leq k < r, a[i] = b[j] = c[k]\}$$

y $\operatorname{card} X$ indica el cardinal del conjunto X. Al igual que en el Ejemplo 7.20, o en el Ejemplo 7.21, al tratarse de un problema de conteo, añadimos a la variable que cuenta parte del problema para derivar el invariante:

$$\begin{array}{rcl} I \doteq u + \boxed{\operatorname{card} A(p, q, r)} & = & \operatorname{card} A(n, m, s) \\ & \wedge & 0 \leq p \leq m \wedge 0 \leq q \leq n \wedge 0 \leq r \leq s \end{array}$$

de donde el esquema:

$$\begin{array}{l} u, p, q, r := 0, n, m, p; \{I\} \\ *[\![\, p \neq 0 \wedge q \neq 0 \wedge r \neq 0 \rightarrow \mathcal{S} \,]\!] \\ \{I \wedge (p = 0 \vee q = 0 \vee r = 0)\} \ \{ \Rightarrow \} \ \{A(p, q, r) = \emptyset\} \ \{ \Rightarrow \} \ \{R\} \end{array}$$

Las sentencias más simples que *estrechan* el conjunto A son

$$p := p - 1 \qquad q := q - 1 \qquad r := r - 1$$

Por simetría, basta estudiar cualquiera de ellas:

$$\begin{array}{ll} & p := p - 1.I \\ = & \\ & u + \operatorname{card} A(p - 1, q, r) = \operatorname{card} A(n, m, s) \\ \wedge & 0 \leq p - 1 \leq m \wedge 0 \leq q \leq n \wedge 0 \leq r \leq s \\ \Leftarrow & \\ & I \wedge p \neq 0 \wedge A(p - 1, q, r) = A(p, q, r) \\ \Leftarrow & \because \left\{ \begin{array}{ll} & A(p, q, r) \\ = & \\ & A(p - 1, q, r) \cup \\ & \{(p, j, k) \mid 0 \leq j < q, 0 \leq k < r, a[p] = b[j] = c[k]\} \\ & \\ & a[p] > b[q] \wedge b \uparrow \\ \Rightarrow & \\ & \{(p, j, k) \mid 0 \leq j < q, 0 \leq k < r, a[p] = b[j] = c[k]\} = \emptyset \end{array} \right. \\ & I \wedge p \neq 0 \wedge a[p] > b[q] \end{array}$$

de donde la guarda:

$$[\![\, a[p] > b[q] \rightarrow p := p - 1 \,\square\, \ldots \,]\!]$$

El estudio de las restantes guardas ($a[p] = a[q], \ldots$) se deja como ejercicio.

7.44 [158] Véase el Ejemplo 6.51.

7.45 [158] R puede debilitarse (eliminando el predicado $a(x) \in \mathcal{P}$) para obtener un candidato a invariante en la forma

$$I \doteq a[0..x - 1] \cap \mathcal{P} = \emptyset \wedge 0 \leq x < n \wedge P$$

de donde el esquema

$$\begin{array}{l} \{P\}x := 0; \{I\} \\ *[\![\, impar\ a(x) \rightarrow x := x+1 \,]\!] \\ \{I \wedge par\ a(x)\}\{R\} \end{array}$$

En efecto:

$$\begin{array}{ll} & x := 0.I \\ = & \\ & a[0..-1] \cap \mathcal{P} = \emptyset \wedge 0 \leq 0 < n \wedge P \\ \Leftarrow & \quad \because a[0..-1] = \emptyset \\ & P \end{array}$$

La invariabilidad es consecuencia de

$$\begin{array}{ll} & x := x+1.I \\ = & \\ & a[0..x] \cap \mathcal{P} = \emptyset \wedge 0 \leq x+1 < n \wedge P \\ \Leftarrow & \quad \because (A \cup A') \cap B = \emptyset \equiv A \cap B = \emptyset \wedge A' \cap B = \emptyset \\ & a[0..x-1] \cap \mathcal{P} = \emptyset \wedge a(x) \notin \mathcal{P} \wedge x+1 < n \wedge P \\ \Leftarrow & \\ & a(x) \notin \mathcal{P} \wedge I \wedge x+1 < n \\ \Leftarrow & \quad \because a(n-1) \in \mathcal{P} \ \Leftarrow\ P, \text{ de donde } x < n \\ & a(x) \notin \mathcal{P} \wedge I \end{array}$$

Finalmente, $t \doteq n - x$ es un contador, ya que, además de disminuir,

$$a(x) \notin \mathcal{P} \wedge I \ \Rightarrow\ x+1 < n \ \Rightarrow\ t > 0.$$

7.46 [158] La especificación del problema se puede escribir $\{P\}\mathcal{S}\{R\}$ siendo

$$\begin{array}{lcl} P & \doteq & n \geq 1 \wedge \exists x, y : x, y \in a[0..n-1] : x \neq y \\ R & \doteq & x \in a[0..n-1] \wedge x \neq \text{mín}\, a[0..n-1] \end{array}$$

Para resolver el problema basta encontrar dos elementos distintos de la tabla y después calcular su máximo:

$$\begin{array}{l} \{P\} \\ T; \\ \{R'\}(\ \doteq\ iguales\ a[0..j-1] \wedge j \leq n \wedge a[0] \neq a[j]) \\ [\![\, a[0] > a[j] \rightarrow x := a[0] \,\Box\, a[0] < a[j] \rightarrow x := a[j] \,]\!] \\ \{x \in a[0..n-1] \wedge x \neq \text{mín}\, a[0..n-1]\} \end{array}$$

donde el predicado *iguales* se define

$$iguales\ a[0..j-1] \ \doteq\ \forall k : 0 \leq k \leq j-1 : a[k] = a[0].$$

Veamos como encontrar el programa T. Debilitemos la poscondición

$$iguales\ a[0..j-1] \wedge j \leq n \wedge a[0] \neq a[j]$$

para obtener el candidato a invariante de cierto bucle

$$I \ \doteq\ iguales\ a[0..j-1] \wedge j \leq n \wedge P$$

(añadimos P por problemas de terminación); de donde el esquema para el programa T

$$\{P\}j := 1;$$
$$*[\![\, a[0] = a[j] \to \mathcal{S}\,]\!]$$

1. El invariante es cierto al principio

$$j := 1.I \equiv iguales\ a[0.,0] \wedge 0 \leq n \wedge P \equiv P$$

2. Conjeturamos el contador $t \doteq n - j$, ya que

$$I \wedge a[0] = a[j] \ \Rightarrow\ iguales\ a[0..j] \ \Rightarrow\ j < n \ \Rightarrow\ t > 0$$

3. La sentencia más simple que decrementa t es $\mathcal{S} \doteq j := j + 1$, pero

$$\begin{array}{ll} & j := j + 1.I \\ = & \\ & iguales\ a[0..j] \wedge j + 1 \leq n \wedge P \\ \Leftarrow & \qquad \because iguales\ a[0..j] \wedge P \ \Rightarrow\ j + 1 \leq n, \text{ regla de oro, def. de } iguales \\ & iguales\ a[0..j-1] \wedge a[0] = a[j] \end{array}$$

Luego I es invariante para la sentencia $j := j + 1$, y de aquí la corrección.

7.47 [158] Sea el predicado

$$Q \doteq n \geq 2 \wedge x = \text{mín}\, a[0..n-1] \wedge y = \text{mín}(a[0..n-1] - \{x\})$$

del cual se deduce que y *es el segundo menor elemento de la tabla*. Podemos obtener un invariante sustituyendo la constante n por una variable

$$I \doteq 2 \leq i \leq n \wedge x = \text{mín}\, a[0..i-1] \wedge y = \text{mín}(a[0..i-1] - \{x\})$$

de donde tendremos el esquema

$$\begin{array}{l} \{n \geq 2\} \\ i, x, y := 2, \text{mín}\, a[0.,1], \text{máx}\, a[0.,1]; \\ *[\![\, i < n \to \textit{decrementar } n - i \textit{ con invariabilidad de } I\,]\!] \\ \{I \wedge i \geq n\} \{\ \Rightarrow\ \} \{I \wedge i = n\} \{\ \Rightarrow\ \} \{Q\} \end{array}$$

Como es usual, para derivar el cuerpo del bucle estudiamos la invariabilidad de I bajo la sentencia $i := i + 1$

$$\begin{array}{ll} & i := i + 1.I \\ = & \\ & 2 \leq i + 1 \leq n \wedge x = \text{mín}\, a[0..i] \wedge y = \text{mín}(a[0..i] - \{x\}) \\ \Leftarrow & \qquad \because y \leq a[i] \wedge y = \text{mín}(a[0..i-1] - \{x\}) \ \Rightarrow\ y = \text{mín}(a[0..i] - \{x\}) \\ & x = \text{mín}\, a[0..i-1] \wedge y \leq a[i] \wedge y = \text{mín}(a[0..i-1] - \{x\}) \\ \Leftarrow & \\ & x \leq y \leq a[i] \wedge x = \text{mín}\, a[0..i-1] \\ \Leftarrow & \\ & x = \text{mín}\, a[0..i] \wedge I \wedge i < n \wedge y \leq a[i] \end{array}$$

Si por el contrario se da $y > a[i]$, es evidente que habrá que actualizar las variables x e y, dependiendo del valor de $x > a[i]$, por lo que conjeturamos que el cuerpo del bucle es

$$\begin{array}{lll} [\![& y \leq a[i] & \to i := i + 1 \\ \Box & x \leq a[i] < y & \to y, i := a[i], i + 1 \\ \Box & a[i] < x \wedge a[i] < y & \to x, y, i := a[i], x, i + 1\,]\!] \end{array}$$

Solo queda demostrar que conserva la invariabilidad. Estudiemos, por ejemplo, la segunda sentencia

$$
\begin{array}{ll}
 & y, i := a[i], i+1.I \\
= & \quad \because \text{semántica} \\
 & 2 \leq i+1 \leq n \wedge x = \text{mín}\, a[0..i] \wedge a[i] = \text{mín}(a[0..i] - \{x\}) \\
\Leftarrow & \\
 & i < n \wedge I \wedge x \leq a[i] < y
\end{array}
$$

<u>7.48</u> [158] La poscondición se escribe $R \doteq q \equiv (\exists i : 0 \leq i < n : a[i] = 6)$. Cambiando n por la variable j obtenemos el candidato a invariante

$$I \doteq q \equiv (\exists i : 0 \leq i < j : a[i] = 6) \quad \wedge \quad 0 \leq j \leq n$$

de donde el esquema

$$
\begin{array}{l}
j, q := 0, Falso; \\
*[\![\, j < n \rightarrow \textit{decrementar } t(\doteq n - j) \textit{ con invariabilidad de } I \,]\!]
\end{array}
$$

Si estudiamos la sentencia más simple que decrementa el contador, tenemos

$$
\begin{array}{ll}
 & j := j+1.I \\
= & \\
 & q \equiv (\exists i : 0 \leq i < j+1 : a[i] = 6) \quad \wedge \quad 0 \leq j+1 \leq n \\
= & \\
 & q \equiv ((\exists i : 0 \leq i < j : a[i] = 6) \vee a[j] = 6) \quad \wedge \quad 0 \leq j+1 \leq n
\end{array}
$$

y vemos que es necesario también alterar el valor de q

$$
\begin{array}{ll}
 & q, j := (a[j] = 6), j+1.I \\
= & \\
 & (a[j] = 6) \equiv ((\exists i : 0 \leq i < j : a[i] = 6) \vee a[j] = 6) \quad \wedge \quad 0 \leq j+1 \leq n \\
\Leftarrow & \\
 & I \wedge j < n \wedge \neg q
\end{array}
$$

de donde la invariabilidad de I y, por el teorema de invariantes, la corrección parcial del programa

$$
\begin{array}{l}
j, q := 0, falso; \\
*[\![\, j < n \wedge \neg q \rightarrow q, j := (a[j] = 6), j+1.I \,]\!]
\end{array}
$$

Para probar que termina asegurando la poscondición hemos de probar

$$[I \wedge (j \geq n \vee q) \ \Rightarrow \ R]$$

$$
\begin{array}{ll}
 & I \wedge (j \geq n \vee q) \\
= & \\
 & (q \equiv \exists i : 0 \leq i < j : a[i] = 6) \wedge 0 \leq j \leq n \wedge j \geq n) \vee I \wedge q \\
\Rightarrow & \quad \because \exists i : 0 \leq i < j : a[i] = 6 \ \Rightarrow \ \exists i : 0 \leq i < n : a[i] = 6, \text{ de donde } I \wedge q \ \Rightarrow \ R \\
 & (q \equiv \exists i : 0 \leq i < n : a[i] = 6) \vee R \\
\Rightarrow & \\
 & R
\end{array}
$$

<u>7.49</u> [158] Según la técnica apuntada, debemos considerar el candidato a invariante:

$$I \doteq k + \boxed{Card\, B(p, q)} = Card\, B(0, n) \wedge 0 \leq p \leq q \leq n$$

Además, tenemos

$$
\begin{array}{ll}
 & p, q, k := 0, n, 0.I \\
= & \quad \because \text{semántica} \\
 & 0 + Card\,B(0,n) = Card\,B(0,n) \wedge 0 \le 0 \le n \le n \\
= & \quad \because \text{cálculo} \\
 & 0 \le n
\end{array}
$$

Por otro lado tenemos $p = q \;\Rightarrow\; Card\,B(p,q) = 0$, de donde el esquema:

$$
\begin{array}{l}
\{n > 0\}p, q, k := 0, n, 0; \{I\} \\
*[\![\, p \neq q \rightarrow \textit{decrementar } t \doteq q - p \textit{ con invariabilidad de } I \,]\!] \\
\{I \wedge p = q\} \;\Rightarrow\; \{R\}
\end{array}
$$

Si tomamos la sentencia $p := p + 1$, observamos que

$$
\begin{array}{ll}
 & p := p + 1.I \\
= & \\
 & k + Card\,B(p+1,q) = Card\,B(0,n) \wedge 0 \le p+1 \le q \le n \\
\Leftarrow & \quad \because \text{si } A[p] \neq 6 \text{ entonces } B(p+1,q) \equiv B(p,q) \\
 & I \wedge p \neq q \wedge A[p] \neq 6
\end{array}
$$

y el cuerpo del bucle puede ser:

$$
\begin{array}{lll}
[\![& & A[p] \neq 6 \rightarrow p := p + 1 \\
 & \square & A[p] = 6 \rightarrow k, p := k + 1, p + 1 \,]\!]
\end{array}
$$

Es evidente que t es un contador (cualquiera de la dos sentencias lo decrementa, y además $I \wedge b \;\Rightarrow\; t > 0$) de donde el bucle termina, y por el teorema de invariantes obtenemos la corrección total del esquema. Pero, podemos aprovechar que la tabla es no decreciente y refinar el cuerpo del bucle en la forma siguiente:

$$
\begin{array}{lll}
[\![& & A[p] > 6 \rightarrow p := q \\
 & \square & A[p] < 6 \rightarrow p := p + 1 \\
 & \square & A[p] = 6 \rightarrow k, p := k + 1, p + 1 \,]\!]
\end{array}
$$

La corrección se deduce de cosas elementales, como que $I \wedge A[p] > 6 \;\Rightarrow\; Card\,B(p,q) = 0, \ldots$ Además, $t \doteq q - p$ sigue siendo un contador, ya que para la primera sentencia tendremos:

$$
wdec(p := q, t) \overset{\text{definición}}{\equiv} p := q.(q-p) < q - p \;\equiv\; p < q \;\Leftarrow\; I \wedge p \neq q
$$

7.50 [158] Véase Ejemplo 7.21.

7.51 [158] La poscondición puede escribirse también en la forma

$$
P \;\doteq\; q = \neg(\forall i : 0 \le i < n : a.0 = a.i)
$$

de la cual se deriva un invariante cambiando la constante n por una variable j

$$
I \;\doteq\; j \le n \wedge q = \neg(\forall i : 0 \le i < j : a.0 = a.i)
$$

de donde el esquema $j, q := 0, Falso; *[\![\, j < n \rightarrow S \,]\!]$. Para el contador $t \;\doteq\; n - j$, tenemos

$$
\begin{array}{ll}
 & j := j + 1.I \\
= & \\
 & j + 1 \le n \wedge q = \neg(\forall i : 0 \le i < j + 1 : a.0 = a.i)
\end{array}
$$

$$
\begin{array}{ll}
= & \because \text{cálculo} \\
& j+1 \leq n \wedge q = \neg(\forall i : 0 \leq i < j : a.0 = a.i) \vee a.0 \neq a.j
\end{array}
$$

de donde el cuerpo del bucle debe alterar también el valor de q, y tendremos

$$
\begin{array}{ll}
& j, q := j+1, a.0 \neq a.j.I \\
= & \\
& j+1 \leq n \wedge (a.0 \neq a.j) = \neg(\forall i : 0 \leq i < j : a.0 = a.i) \vee a.0 \neq a.j \\
\Rightarrow & \\
& I \wedge j < n \wedge \neg q
\end{array}
$$

y por tanto el bucle

$$*[\![\, j < n \wedge \neg q \rightarrow j, q := j+1, a.0 \neq a.j \,]\!]$$

que es más eficiente y termina verificando la poscondición ya que

$$
\begin{array}{ll}
& [I \wedge \neg(j < n \wedge \neg q) \ \Rightarrow \ P] \\
= & \because \text{cálculo} \\
& [I \wedge j \geq n \ \Rightarrow \ P] \wedge [I \wedge q \ \Rightarrow \ P]
\end{array}
$$

La primera implicación sigue de $[I \wedge j \geq n \ \Rightarrow \ j = n]$, y la segunda es consecuencia de

$$\neg(\forall i : 0 \leq i < j : a.0 = a.i) \ \Rightarrow \ \neg(\forall i : 0 \leq i < n : a.0 = a.i)$$

7.52 [158] Pongamos

$$P \ \doteq \ a[0..n-1] \subseteq \mathbb{Z} \wedge a\uparrow \ \wedge a(0) \in \mathcal{P} \wedge n > 0$$

(siendo $\mathcal{P}$ el subconjunto de los enteros pares) y la poscondición en la forma

$$R \ \doteq \ P \wedge a(i) \in \mathcal{P} \wedge a[i+1..n-1] \cap \mathcal{P} = \emptyset \wedge 0 \leq i \leq n-1.$$

Basta debilitar la poscondición eliminado el predicado $a(i) \in \mathcal{P}$, para obtener el candidato a invariante $I \ \doteq \ P \wedge a[i+1..n-1] \cap \mathcal{P} = \emptyset \wedge 0 \leq i \leq n-1$. Obviamente tenemos

$$
\begin{array}{ll}
& i := n-1.I \\
= & \\
& P \wedge a[n..n-1] \cap \mathcal{P} = \emptyset \wedge 0 \leq n-1 \leq n-1 \\
\Leftarrow & \because a[n..n-1] = \emptyset \\
& P
\end{array}
$$

de donde el esquema:

$$
\begin{array}{l}
i := n-1; \{I\} \\
*[\![\, \mathit{impar}\ a(i) \rightarrow i := i-1 \,]\!] \\
\{I \wedge \mathit{par}\ a(i)\} \ \{\Rightarrow\} \ \{R\}
\end{array}
$$

y solo queda probar la invariabilidad y la terminación. Tenemos, *ptle*

$$
\begin{array}{ll}
& i := i-1.I \\
= & \\
& P \wedge a[i..n-1] \cap \mathcal{P} = \emptyset \wedge 0 \leq i-1 \leq n-1 \\
\Leftarrow & \because P \wedge \mathit{impar}\ a(i) \ \Rightarrow \ i > 0 \\
& P \wedge \mathit{impar}\ a(i) \wedge a[i-1..n-1] \cap \mathcal{P} = \emptyset \wedge 0 \leq i \leq n-1 \\
\Leftarrow &
\end{array}
$$

$I \wedge impar\ a(i)$

Para probar la terminación basta probar que $t \doteq i$ es un contador:

$$
\begin{array}{ll}
 & I \wedge impar\ a(i) \Rightarrow (i := i-1).i < i \ \wedge \ i > 0 \\
= & \qquad \because P \wedge impar\ a(i) \Rightarrow i > 0 \\
 & Cierto
\end{array}
$$

8.14 [166] (Véase también la solución del Ejercicio 6.4.) Si $[S.\neg b \equiv Falso]$, entonces, por monotonía, $[S.(\neg b \wedge X) \equiv Falso]$. Y de aquí es fácil probar que $\neg b \wedge X$ es solución de la ecuación:

$$Y : [\, Y \equiv \neg b \wedge X \vee b \wedge \ \wedge S.Y \,]$$

Y ahora aplicamos lo dicho en la Nota 8.12 para obtener $\mathcal{R}.X \equiv \neg b \wedge X$. La interpretación es que ya que S no cambia nunca la guarda, para que el bucle termine, no debe empezar.

8.15 [166] Calculemos la semántica del bucle $\mathcal{R}.C$ vía puntos fijos. El predicado $\neg b$ es un punto fijo de la función $Y \longmapsto \neg b \vee b \wedge nada.Y$. Ahora aplicamos lo obtenido en la Nota 8.12 para deducir $[\mathcal{R}.C \equiv \neg b]$. Además,

$$\{b\}\mathcal{R}\{C\} \doteq [b \Rightarrow \mathcal{R}.C] \equiv [\neg b]$$

Por tanto, *ptle*, b debe ser Falso.

8.20 [168] En primer lugar es fácil probar que entonces P es invariante de S' (véase la solución del Ejercicio 6.16 en la página 267). Entonces,

$$
\begin{array}{ll}
 & [P \wedge \mathcal{R}.X \Rightarrow \mathcal{R}'.X] \\
= & \qquad \because \text{regla de intercambio} \\
 & [\mathcal{R}.X \Rightarrow \neg P \vee \mathcal{R}'.X] \\
\Leftarrow & \qquad \because \text{TK – Teorema 8.10}(ii) \text{ – con } f.Y \doteq \neg b \wedge X \vee b \wedge S.Y \\
 & [f.(\neg P \vee \mathcal{R}'.X) \Rightarrow \neg P \vee \mathcal{R}'.X] \\
= & \qquad \because \text{definición de } f \\
 & [\neg b \wedge X \vee b \wedge S.(\neg P \vee \mathcal{R}'.X) \Rightarrow \neg P \vee \mathcal{R}'.X] \\
= & \qquad \because \text{regla de intercambio} \\
 & [\neg b \wedge P \wedge X \vee b \wedge P \wedge S.(\neg P \vee \mathcal{R}'.X) \Rightarrow \mathcal{R}'.X] \\
= & \qquad \because P \wedge S.Q \equiv P \wedge S'.Q \\
 & [\neg b \wedge P \wedge X \vee b \wedge P \wedge S'.(\neg P \vee \mathcal{R}'.X) \Rightarrow \mathcal{R}'.X] \\
= & \qquad \because \text{por } [b \wedge P \Rightarrow S'.P] \text{ y regla de oro: } [b \wedge P \wedge S'.P \equiv b \wedge P] \\
 & [\neg b \wedge P \wedge X \vee b \wedge P \wedge S'.P \wedge S'.(\neg P \vee \mathcal{R}'.X) \Rightarrow \mathcal{R}'.X] \\
= & \qquad \because \text{conjuntividad} \\
 & [\neg b \wedge P \wedge X \vee b \wedge P \wedge S'.(P \wedge \mathcal{R}'.X) \Rightarrow \mathcal{R}'.X] \\
= & \qquad \because [b \wedge P \wedge S'.P \equiv b \wedge P] \text{, conjuntividad y distributividad} \\
 & [P \wedge (\neg b \wedge X \vee b \wedge S'.\mathcal{R}'.X) \Rightarrow \mathcal{R}'.X] \\
= & \qquad \because \mathcal{R}'.X \text{ es un punto fijo} \\
 & [P \wedge \mathcal{R}'.X \Rightarrow \mathcal{R}'.X] \\
= & \\
 & Cierto
\end{array}
$$

La otra implicación se prueba en forma similar.

8.24 [170] Sean los bucles $\mathcal{R} \doteq *[\![b \to nada]\!]$ y $\mathcal{R}' \doteq *[\![b \to aborta]\!]$. Calculemos la semántica de cada bucle y veamos que coinciden. Es fácil probar:

$\neg b \wedge X$ es solución de:	$\neg b \wedge X$ es solución de:
$[Y \equiv \neg b \wedge X \vee b \wedge nada.Y]$	$[Y \equiv \neg b \wedge X \vee b \wedge aborta.Y]$

Entonces, por la Nota 8.12:165, $[\mathcal{R}.X \equiv \neg b \wedge X]$, junto a $[\mathcal{R}'.X \equiv \neg b \wedge X]$, y por tanto son iguales.

8.25 [170] Como vimos en el Ejemplo 8.13, $[\mathcal{R}.X \equiv \neg b \wedge X]$, de donde

$$\begin{array}{ll} & \mathcal{S}.X \\ = & \quad \because \mathcal{S} \doteq b := Cierto; \mathcal{R} \\ & b := Cierto.\mathcal{R}.X \\ = & \\ & b := Cierto.(\neg b \wedge X) \\ = & \\ & Falso \end{array}$$

luego $[\mathcal{S}.X = Falso]$, de lo cual concluimos $\mathcal{S} = aborta$.

8.26 [170] Véase también el Ejercicio 6.28.

8.27 [170] Razonemos igual que en el Ejemplo 8.13, pero para el bucle:

$$\mathcal{R} \doteq *[\![q \to nada \,\square\, q \to q := \neg q]\!]$$

Probemos que $\neg q \wedge X$ es solución de la ecuación

$$Y : [\, Y \equiv \neg q \wedge X \vee q \wedge S.Y \,] \qquad (**)$$

de donde obtendríamos $\mathcal{R}.X \equiv \neg q \wedge X$, lo que probaría (A). En efecto,

$$\begin{array}{ll} & \neg q \wedge X \vee q \wedge [\![q \to nada \,\square\, q \to \dots]\!].(\neg q \wedge X) \\ = & \quad \because \text{semántica selección} \\ & \neg q \wedge X \vee q \wedge (q \Rightarrow nada.(\neg q \wedge X)) \wedge \dots \\ = & \quad \because \text{CP, semántica} \\ & \neg q \wedge X \vee q \wedge (\neg q \wedge X) \wedge \dots \\ = & \quad \because \text{CP} \\ & \neg b \wedge X \end{array}$$

(B) es consecuencia de $\forall n : n \geq 0 : [H^n.X \equiv \neg q \wedge X]$, que se prueba fácilmente por inducción sobre n. (C) sigue de $[\![\neg q \to nada]\!].X \equiv \neg q \wedge X$.

8.29 [170] Sea $\mathcal{R} \doteq *[\![b \to S]\!]$. Probemos $[\mathcal{R}.C \Rightarrow \mathcal{R}.\neg b]$ utilizando la semántica inductiva:

$$\begin{array}{ll} & [\mathcal{R}.X \Rightarrow \mathcal{R}.\neg b] \\ = & \quad \because \text{semántica inductiva de los bucles (Definición 6.2)} \\ & [\exists k : k \geq 0 : H^n.X \Rightarrow \exists k : k \geq 0 : H^n.\neg b] \\ \Leftarrow & \quad \because \text{CP} \\ & \forall n : n \geq 0 : [H^n.X \Rightarrow H^n.\neg b] \end{array}$$

y vemos esto último por inducción; para $n = 0$ es trivial; el paso inductivo es:

$$\begin{array}{ll} & [H^{n+1}.X \Rightarrow H^{n+1}.\neg b] \\ = & \quad \because \text{definición} \end{array}$$

$[\neg b \wedge X \vee b \wedge S.H^n.X \;\Rightarrow\; \neg b \vee b \wedge S.H^n.\neg b]$
$\Leftarrow \qquad \because$ cálculo
$[S.H^n.X \;\Rightarrow\; S.H^n.\neg b]$
$= \qquad \because S$ monótona
$[H^n.X \;\Rightarrow\; H^n.\neg b]$
$= \qquad \because$ HI
$Cierto$

Para probar $[\mathcal{R}.C \;\Rightarrow\; \mathcal{R}.\neg b]$ vía la semántica según puntos fijos basta probar que $\mathcal{R}.\neg b$ satisface la ecuación característica de $\mathcal{R}.C$:

$$Y : [Y \equiv \neg b \vee b \wedge S.Y]$$

lo cual es trivial por ser $\mathcal{R}.\neg b \equiv \mu Y : \neg b \wedge \neg b \vee b \wedge S.Y$.

8.30 [171] Hay que probar $[A \;\Rightarrow\; \mathcal{R}.C] \;\Rightarrow\; [S.A \;\Rightarrow\; \mathcal{R}.C]$. En efecto, *ptle*

$\mathcal{R}.C$
$= \qquad \because$ definición semántica como menor p.f.
$\neg b \vee b \wedge S.\mathcal{R}.C$
$\Leftarrow \qquad \because [A \;\Rightarrow\; \mathcal{R}.C]$, monotonía de S, transitividad de $\Rightarrow$
$\neg b \vee b \wedge S.A$
$\Leftarrow \qquad \because$ Ley de intercambio o también Nota 1.13:19
$S.A$

La interpretación operacional es simple: para cada estado inicial ι que satisfaga $S.A$, por la ley del tercio excluido, pueden darse,
— o bien ι satisface $\neg b$, y entonces el bucle termina partiendo de ι,
— o bien ι satisface b; en ese caso debemos ejecutar S, que sabemos que termina en cierto estado σ satisfaciendo A (ya que el estado inicial satisface $S.A$); entonces, ya que por hipótesis $[A \;\Rightarrow\; \mathcal{R}.C]$, tendremos que σ también satisface $\mathcal{R}.C$, y el bucle termina a partir de ι.

8.31 [171] Véase la Sección 8.2 (pág. 164).

8.32 [171] Véase también el Ejercicio 8.37.

$\{b\}S\{\neg b\}$
$= \qquad \because$ definición de triplete de Dijkstra
$[b \;\Rightarrow\; S.\neg b]$
$\Rightarrow \qquad \because [\mathcal{R}.C = \neg b \vee b \wedge S.\mathcal{R}.C]$, luego $[\neg b \;\Rightarrow\; \mathcal{R}.C]$, y por monotonía de S
$[b \;\Rightarrow\; S.\mathcal{R}.C]$
$= \qquad \because$ regla de oro
$[b \wedge S.\mathcal{R}.C = b]$
$\Rightarrow \qquad \because [\mathcal{R}.C = \neg b \vee b \wedge S.\mathcal{R}.C]$
$[\mathcal{R}.C = \neg b \vee b]$
$= \qquad \because$ tercio excluido
$[\mathcal{R}.C = Cierto]$

8.33 [171] Calculemos la semántica del bucle $\mathcal{R}.C$ vía puntos fijos. El predicado $x \leq 1$ es un punto fijo de la función g dada por

$$g.Y \;\doteq\; x \leq 1 \vee [\![\, x > 1 \rightarrow x := x + 1 \,\square\, x > 2 \rightarrow x := x - 4 \,]\!].Y$$

ya que

$$
\begin{array}{ll}
 & [\![\, x > 1 \rightarrow x := x+1 \,\Box\, x > 2 \rightarrow x := x-4 \,]\!].(x \leq 1) \\
= & \qquad \because \text{semántica selectiva y cálculo} \\
 & x > 1 \wedge x := x+1.(x \leq 1) \wedge \ \ldots \\
= & \qquad \because \text{semántica asignación y cálculo} \\
 & Falso
\end{array}
$$

Luego, por la Nota 8.12:165, $\mathcal{R}.C \equiv (\mu Y : g.Y) \equiv (x \leq 1)$, y la sentencia $\mathcal{S}$ no afecta a la semántica de $\mathcal{R}$. La interpretación es que, vía indeterminismo, partiendo de un estado verificando $x > 1$ es posible siempre elegir la primera guarda y el bucle no terminaría.

8.34 [171] (A).— Cada solución de la ecuación característica de $\mathcal{R}.X$:

$$Y : [Y \equiv \neg b \wedge X \vee b \wedge S.Y]$$

es solución de la ecuación correspondiente a $\mathcal{R}.(\neg b \wedge X)$:

$$Y : [Y \equiv \neg b \wedge (\neg b \wedge X) \vee b \wedge S.Y]$$

luego los menores puntos fijos coinciden.

(B).— Siendo SI la sentencia $[\![\, b \rightarrow A \,\Box\, \neg b \rightarrow B \,]\!]$,tenemos, *ptle*

$$
\begin{array}{ll}
 & \mathcal{R}.SI.X \\
= & \qquad \because \text{por } (A) \\
 & \mathcal{R}.(\neg b \wedge SI.X) \\
= & \qquad \because \text{semántica selección} \\
 & \mathcal{R}.(\neg b \wedge B.X) \\
= & \qquad \because \text{por } (A) \\
 & \mathcal{R}.(B.X) \\
= & \\
 & \mathcal{R}; B.X
\end{array}
$$

8.35 [171] (A).— A partir de la igualdad (véase Teorema 6.10)

$$\mathcal{R} = *[\![\, p \vee q \rightarrow SI \,]\!]$$

donde $SI \equiv [\![\, p \rightarrow S \,\Box\, q \rightarrow T \,]\!]$, podemos demostrar:

(1) SI es determinista (véase Teorema 4.27).

(2) El bucle $\mathcal{R} \doteq *[\![\, b \rightarrow SI \,]\!]$ es determinista si lo es SI (Lema 8.16(iv)).

(B).— Sabemos, *ptle*

$$\mathcal{R}.C \doteq \exists k : k \geq 0 : H^k, \text{ donde } H^0 \doteq \neg OB, H^{k+1} \doteq H^0 \vee SI.H^k$$

pero, ya que, *ptle*, $\neg OB \equiv Falso$, tenemos, también *ptle*

$$
\begin{array}{lll}
H^0 & \equiv & F \\
H^1 & \equiv & H^0 \vee SI.H^0 \overset{SI \text{ es sana}}{\equiv} F
\end{array}
$$

y en general $[H^k \equiv F]$ (por inducción), y de aquí, $[\mathcal{R}.C \equiv F]$. Entonces, por monotonía, $\forall X :: [\mathcal{R}.X \equiv F]$, es decir, $\mathcal{R} = aborta$.

Otra forma, vía PF, consiste en probar que F es solución de la ecuación característica de $\mathcal{R}.X$:

$$Y : [Y \equiv \neg C \wedge X \vee C \wedge S.Y]$$

lo cual es trivial por ser S estricta (véase también la Nota 8.12:165).

(C).— $\{C\}\mathcal{R}\{C\} \equiv [C \;\Rightarrow\; \mathcal{R}.C] \equiv [C \;\Rightarrow\; F] \equiv Falso$. Interpretación: un bucle que tiene siempre una guarda cierta no puede terminar.

8.36 [171] Véase Ejercicio 8.72.

8.37 [171] (A).— Tenemos, *ptle*,

$$\begin{array}{ll}
 & \mathcal{R}.C \\
= & \quad \because [\mathcal{R}.C \equiv \mathcal{R}.(\neg b)] \\
 & \mathcal{R}.(\neg b) \\
= & \quad \because \text{semántica en términos de puntos fijos} \\
 & \neg b \vee b \wedge S.\mathcal{R}.(\neg b) \\
= & \quad \because \text{semántica en términos de puntos fijos} \\
 & \neg b \vee b \wedge S.(\neg b \vee b \wedge S.\mathcal{R}.(\neg b)) \\
\Leftarrow & \quad \because \text{monotonía de } S \\
 & \neg b \vee b \wedge S.\neg b \\
= & \quad \because \text{por la hipótesis } \{b\}S\{\neg b\} \equiv [b \;\Rightarrow\; S.\neg b] \text{, y regla de oro} \\
 & \neg b \vee b \\
= & \quad \because \text{tercio excluido} \\
 & Cierto
\end{array}$$

Otra demostración parte de $\mathcal{R} = [\![\, \neg b \;\rightarrow\; nada \,\Box\, b \;\rightarrow\; S;\mathcal{R} \,]\!]$. Entonces, transformamos la secuencia con guardas,

$$\begin{array}{ll}
 & b \rightarrow S;\mathcal{R} \\
= & \quad \because \text{utilizamos la hipótesis } \{b\}S\{\neg b\} \\
 & b \rightarrow \{b\}S\{\neg b\};\mathcal{R} \\
= & \quad \because \text{semántica en términos de puntos fijos: } [\neg b \wedge \mathcal{R}.X \equiv \neg b \wedge nada.X] \\
 & b \rightarrow \{b\}S\{\neg b\};nada \\
= & \quad \because nada \text{ es neutro} \\
 & b \rightarrow S
\end{array}$$

de donde $\mathcal{R} = [\![\, \neg b \rightarrow nada \,\Box\, b \rightarrow S \,]\!]$. Pero, *ptle*

$$\begin{array}{ll}
 & b \wedge S.C \\
= & \quad \because \text{hipótesis } b \;\Rightarrow\; S.\neg b \text{ y regla de oro} \\
 & b \wedge S.\neg b \wedge S.C \\
= & \quad \because \text{conjuntividad} \\
 & b \wedge S.\neg b \\
= & \\
 & b
\end{array}$$

y de aquí, $\mathcal{R}.C \equiv \neg b \wedge C \vee b \wedge SC \equiv \neg b \vee b \equiv C$.

(B).— Si se verifica $\{b\}S\{\neg b\}$, por la equivalencia $\mathcal{R}.X \equiv [\![\, \neg b \rightarrow nada \,\Box\, b \rightarrow S;\mathcal{R} \,]\!]$ el cuerpo del bucle se ejecuta a lo sumo una vez, ya que, si entra en el bucle, cambia la guarda. Luego $\{b\}S\{\neg b\}$ asegura la terminación del bucle.

(C).— Por ejemplo, el bucle $\mathcal{R} \doteq *[\![x > 0 \rightarrow x := x - 1]\!]$ obviamente termina siempre, de donde $[\mathcal{R}.C]$. Pero el cuerpo no necesariamente cambia la guarda para todos los estados.

8.39 [172] (A).— La justificación es que *para asegurar que el bucle termina debemos partir de z=0*. En efecto: (1) si $z > 0$, no termina, trivialmente; (2) si $z < 0$, p.e., $z = -1$, puede ejecutar indefinidamente la segunda guarda, y no termina; (3) si $z = 0$ termina trivialmente al ser las dos guardas falsas.

(B).— Se verifica, *ptle*, $\mathcal{S}.Q \equiv z \neq 0 \wedge z := z + 1.Q \wedge z := z + 2.Q$, de donde obtenemos $\mathcal{S}.(z = a) \equiv Falso$. La justificación es que $\mathcal{S}$ es indeterminista, y no podemos asegurar un valor final prefijado.

(C).— Por lo anterior, $[\mathcal{S}.(z = 2 \vee z = 3) \equiv (z = 1)$. Luego $\mathcal{S}.(z = 2 \vee z = 3) \not\equiv \mathcal{S}.(z = 2) \vee \mathcal{S}.(z = 3)$, y por tanto $\mathcal{S}$ no es disyuntivo; i.e., es indeterminista.

(D).— $\mathcal{R}.C$ es la menor solución de la ecuación

$$Y : [Y \equiv z = 0 \vee z \neq 0 \wedge S.Y].$$

(E).— Por el apartado (B), $z = 0$ es solución de la ecuación del apartado (D). Además, toda solución de esta ecuación es de la forma $z = 0 \vee \ldots$, de donde $z = 0$ es la menor. Luego $[\mathcal{R}.C \equiv (z = 0)]$.

(F).— En primer lugar tenemos que $[\mathcal{R}.C \equiv \mathcal{R}.(\neg b \wedge C) \equiv \mathcal{R}.(z = 0)]$, y por el apartado (E) tendremos $[\mathcal{R}.(z = 0) \equiv (z = 0)]$. Además, por definición de triplete tenemos:

$$[z = k \Rightarrow \mathcal{R}.(z = 0)] \equiv [z = k \Rightarrow z = 0] \equiv k = 0.$$

8.40 [172] Sea el bucle $\mathcal{R} \doteq *[\![x > 0 \rightarrow x := x - 1 \,\square\, x > 0 \rightarrow x := x - 2]\!]$, donde x es una variable entera.

(A).— Tenemos $\mathcal{R}.C \equiv \exists k : k \geq 0 : H^k.C$. Probaremos por inducción que

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

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

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

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

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

$\underline{(C)}$.— En términos de puntos fijos, $\mathcal{R}.X$ es la menor solución de la ecuación:

$$Y : [Y \equiv \neg b \wedge X \vee b \wedge SI.Y]$$

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

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

Para la segunda ecuación razonamos exactamente igual ($[SI.(x < 0) \equiv F]$).

$\underline{(D)}$.— En efecto, por los apartados (B) y (C) tenemos, *ptle*:
$\mathcal{R}.(x = 0) \equiv (x = 0),\ \ \mathcal{R}.(x < 0) \equiv (x < 0),\ \ \mathcal{R}.(x \leq 0) \equiv Cierto$
y en definitiva tenemos:
$\mathcal{R}.(x = 0) \vee \mathcal{R}.(x < 0) \equiv x \leq 0 \not\equiv Cierto \equiv \mathcal{R}.(x = 0 \vee x < 0)$
de donde el transformador $\mathcal{R}$ no es disyuntivo y por tanto es indeterminista.

<u>8.41</u> [172] $\underline{(A)}$.— Basta que el espacio de estados tenga dos valores distintos. Por ejemplo, para el espacio de estados correspondiente a la declaración $x :\in \{0, 1\}$, tenemos, *ptle*, $desastre.(x = k) \equiv [x = k]$, que será falso ya que $[x = k] \equiv Falso$; sin embargo, $desastre.(x \in \{0, 1\}) \equiv Cierto$, de donde, $desastre$ es indeterminista.

$\underline{(B)}$.— Para que tenga indeterminismo no acotado el espacio debe ser infinito, ya que en ese caso la sentencia es no continua (véase Ejemplo 8.2).

$\underline{(C)}$.— Sea $\mathcal{R}$ el bucle $*[\![\, x > 3 \rightarrow desastre \,]\!]$. Hay que probar:

$$[\, x := 8.\mathcal{R}.C \ \equiv\ Falso \,]$$

La semántica de $\mathcal{R}.C$ es el menor punto fijo de la ecuación:

$$Y : [Y \equiv x \leq 3 \vee x > 3 \wedge desastre.Y]$$

que admite como punto fijo $x \leq 3$, ya que $desastre.(x \leq 3) \equiv Falso$, *ptle*. Ahora aplicamos la Nota 8.12:165, y el menor PF es $x \leq 3$. En ese caso, tenemos

$$\begin{array}{ll} & x := 8.\mathcal{R}.C \\ = & \\ & x := 8.(x \leq 3) \\ = & \quad \because \text{semántica asignación} \\ & Falso \end{array}$$

$\underline{(D)}$.— La solución es muy parecida a la del Ejemplo 8.48, y el bucle siempre termina, pero débilmente. Es decir, $[\mathcal{R}.C \equiv Cierto]$.

$\underline{(E)}$.— Cambiemos la sentencia $Azar_y$ por la sentencia $desastre$. Entonces la semántica de $\mathcal{R}.C$ es el menor punto fijo de la ecuación:

$$Y : [Y \equiv \neg b \vee b \wedge (x > 1 \;\Rightarrow\; x := x - 1.desastre.Y) \wedge (y > 1 \;\Rightarrow\; y := y - 1.Y)]$$

donde $b \equiv x > 1 \vee y > 1$. Tal ecuación admite como solución $\neg b$, ya que $x := x - 1.desastre.\neg b \equiv Falso$, y ahora aplicamos la Nota 8.12 para obtener $[\mathcal{R}.C \equiv x \leq 1 \wedge y \leq 1]$. Es decir, el cambio es drástico: para asegurar la terminación deben fallar las guardas al principio. La razón es que la sentencia $desastre$ *puede alterar* la variable x usada para construir el contador (x, y).

$\underline{8.50}$ [179] Véase también el Ejercicio 6.9:92.

$\underline{(A)}$.— Para el bucle $\mathcal{R} \doteq *[\![\, b \rightarrow x, b := x - 1, x > 1 \,\square\, b \rightarrow b := Falso \,]\!]$ calculemos sucesivamente (pongamos $H^n.C == H^n$ para simplificar), $H^0, H^1, \ldots,$ y encontramos, *ptle*

$$\begin{array}{lcl} H^0 & \equiv & \neg b \\ H^1 & \equiv & \neg b \vee b \wedge x \leq 1 \\ H^2 & \equiv & \neg b \vee b \wedge x \leq 2 \end{array}$$

Podemos conjeturar el valor de H^k, y a continuación probar por inducción,

$$\forall k : k \geq 1 : [\, H^k \equiv \neg b \vee b \wedge x \leq k \,] \qquad (*)$$

de donde obtendríamos

$$\begin{array}{ll} & \exists k : k \geq 0 : H^k \\ = & \quad \because (*) \\ & \exists k : k \geq 0 : \neg b \vee b \wedge x \leq k \\ = & \quad \because \text{CP} \\ & \neg b \vee b \wedge \exists k : k \geq 0 : x \leq k \\ = & \quad \because x \text{ tendrá un valor acotado} \\ & \neg b \vee b \wedge C \\ = & \quad \because \text{CP} \\ & Cierto \end{array}$$

y de aquí, *ptle*, $\mathcal{R}.C \equiv (\exists k : k \geq 0 : H^k) \equiv C$.

$\underline{(B)}$.— El programa es continuo, y por aplicación del Teorema 8.49, el indeterminismo debe ser acotado.

$\underline{(C)}$.— Es obvio que el predicado $J \doteq x \leq 100$ es un invariante. Lo que no parece del todo obvio es que el predicado $0 \leq x$ sea otro invariante; si intentamos probarlo encontramos un problema, ya que debemos buscar un invariante donde intervenga b para dar una cota inferior de x en función de b.

Observamos que si partimos de un valor $x > 0$, es imposible llegar al estado $(C, 0)$, donde la primera componente del par indica el valor de b y la segunda el valor de x. En efecto. Si llegamos al estado $(C, 0)$ ejecutando el cuerpo S, es porque hemos ejecutado la primera sentencia, y el estado inicial debería ser $(F, 1)$, que es imposible ya que falla la guarda. Luego el estado $(C, 0)$ es inaccesible. Por otro lado, el estado $(F, 0)$ si puede alcanzarse. Por ejemplo a partir del estado $(C, 1)$. Luego conjeturamos el invariante,

$$I \doteq b \wedge x > 0 \vee \neg b \wedge x \geq 0$$

$$\begin{array}{ll}
 & b := F.I \\
= & \quad \because \text{sustitución, CP} \\
 & x \geq 0 \\
\Leftarrow & \\
 & I \wedge b
\end{array}$$

$$\begin{array}{ll}
 & x, b := x-1, x > 1.I \\
= & \quad \because \text{sustitución} \\
 & x > 1 \wedge x - 1 > 0 \vee x \leq 1 \wedge x - 1 \geq 0 \\
= & \quad \because \text{CP} \\
 & x \geq 1 \\
\Leftarrow & \\
 & I \wedge b
\end{array}$$

Por consiguiente, tenemos dos invariantes, I y J, de donde – véase Ejercicio 6.33 – el predicado $I \wedge J$ es invariante. Si el programa termina fuertemente, lo hace con $\neg b$, de donde tendremos $I \wedge J \wedge \neg b \;\Rightarrow\; 0 \leq x \leq 100$; luego el indeterminismo es acotado, si el programa termina.

Para probar la terminación buscaremos un contador. El propio x no sirve ya que la ejecución de la segunda sentencia guardada no lo altera, pero ésta cambia el valor de b. Entonces es fácil probar que la función

$$t(x, b) \doteq \begin{cases} x, & \text{si } b \\ 0, & \text{si } \neg b \end{cases}$$

es un contador asociado al invariante I. En efecto,
— por un lado, $I \wedge b (\equiv b \wedge x > 0) \;\Rightarrow\; t > 0$ (trivial)
— por otro lado, hemos de estudiar

$$\begin{array}{ll}
 & wdec(x, b := x-1, x > 1 \mid t) \\
= & \quad \because \text{Lema } 6.43(i') \\
 & (x, b := x-1, x > 1 \,.\, t(x, b)) < t(x, b) \\
= & \quad \because \text{sustitución y definición de } t \\
 & t(x-1, x > 1) < t(x, b)
\end{array}$$

Pero tenemos la siguiente tabla de valores según la definición de t,

$I \wedge b$	$t(x, b)$	$t(x-1, x > 1)$
$b \wedge x > 0$	x	$x - 1$

de la cual se desprende claramente $[\, I \wedge b \;\Rightarrow\; wdec(x, b := x-1, x > 1 \mid t) \,]$. La prueba de la implicación $[\, I \wedge b \;\Rightarrow\; wdec(b := Falso \mid t) \,]$ es fácil:

$$\begin{array}{ll}
 & [\, I \wedge b \;\Rightarrow\; wdec(b := Falso \mid t) \,] \\
= & \quad \because \text{Lema } 6.43(i) \\
 & [\, I \wedge b \;\Rightarrow\; (b := Falso.t(x, b)) \;<\; t(x, b) \,] \\
= & \quad \because \text{sustitución} \\
 & [\, I \wedge b \;\Rightarrow\; t(x, Falso) \;<\; t(x, b) \,] \\
= & \quad \because \text{definición de } t,\ (I \wedge b \;\Rightarrow\; Q) \equiv (I \wedge b \;\Rightarrow\; b \wedge Q) \\
 & [\, I \wedge b \;\Rightarrow\; 0 < x \,] \\
= & \quad \because [I \wedge b \equiv b \wedge 0 < x] \\
 & Cierto
\end{array}$$

Además, por existir un contador entero, el indeterminismo es acotado.

8.52 [179] Si consideramos cinco variables (a, b, c, d, e), y la inicialización

$$a, b, c, d, e := A, B, C, D, E$$

sería suficiente encontrar la poscondición $a \leq b \leq c, d, e \ \wedge \ I$ siendo

$$I \ \doteq \ (a, b, c, d, e) \textit{ es una permutación de } (A, B, C, D, E)$$

Si el siguiente programa termina

$$\begin{array}{ll} & a, b, c, d, e := A, B, C, D, E; \\ *[\![& a > b \rightarrow a, b := b, a \\ \Box & b > c \rightarrow b, c := c, b \\ \Box & b > d \rightarrow b, d := d, b \\ \Box & b > e \rightarrow b, e := e, b]\!] \end{array}$$

terminará calculando en la variable b el segundo menor valor. Por el teorema de los contadores, la invariabilidad y la terminación quedará probada si probamos que la función $t : \mathcal{E} \rightarrow \mathbb{Z}^5$ definida en la forma $t \ \doteq \ (a, b, c, d, e)$ es un $\mathbb{Z}^5$ contador para el conjunto $\mathcal{C}$ bien construido (por ser finito),

$$\mathcal{C} \ \doteq \ \{(x, y, z, u, w) \mid (x, y, z, u, w) \textit{ es una permutación de } (A, B, C, D, E)\}$$

con la relación de orden lexicográfica. Para ello, hay que probar, *ptle*

$$\begin{array}{ll} (a) & I \wedge OB \ \Rightarrow \ t \in \mathcal{C} \\ (b) & I \wedge a > b \ \Rightarrow \ a, b := b, a.I \\ & I \wedge b > c \ \Rightarrow \ b, c := c, b.I \\ & \ldots \\ (c) & I \wedge a > b \ \Rightarrow \ (a, b := b, a.t) < t \\ & I \wedge b > c \ \Rightarrow \ (b, c := c, b.t) < t \\ & \ldots \end{array}$$

Las implicaciones de (b) son evidentes, mientras que las de (c) se prueban todas de la misma forma; por ejemplo

$$\begin{array}{ll} & (b, c := c, b.t) < t \\ = & \quad \because \text{definición de } t \\ & (a, c, b, d, e) < (a, b, c, d, e) \\ \Leftarrow & \quad \because \text{orden lexicográfico} \\ & b > c \end{array}$$

8.53 [179] Consideremos cinco variables (a, b, c, d, e); según el Teorema de Invariantes, para probar la corrección del programa

$$\begin{array}{ll} & a, b, c, d, e := A, B, C, D, E\{I\} \\ *[\![& a > c \rightarrow a, c := c, a \\ \Box & b > c \rightarrow b, c := c, b \\ \Box & c > d \rightarrow c, d := d, c \\ \Box & c > e \rightarrow c, e := e, c]\!] \\ & \{I \wedge a, b \leq c \leq d, e \ \Rightarrow \ c \textit{ es la mediana}\} \end{array}$$

basta considerar el invariante

$$I \ \doteq \ (a, b, c, d, e) \textit{ es una permutación de } (A, B, C, D, E)$$

y, según el teorema de los contadores, bastará probar que la función $t : \mathcal{E} \to \mathbb{Z}^5$, definida en la forma $t \doteq (a, b, c, d, e)$, es un $\mathbb{Z}^5$ contador para el conjunto $\mathcal{C}$ bien construido (por ser finito)

$$\mathcal{C} = \{(x, y, z, u, w) \mid (x, y, z, u, w) \textit{ es una permutación de } (A, B, C, D, E)\}$$

con la relación de orden lexicográfica. Para ello, hay que probar

$$\begin{array}{ll} (a) & I \wedge OB \;\Rightarrow\; t \in \mathcal{C} \qquad \text{— trivial} \\ (b) & I \wedge a > c \;\Rightarrow\; a, c := c, a.I, \\ & I \wedge b > c \;\Rightarrow\; b, c := c, b.I, \\ & \ldots \\ (c) & I \wedge a > c \;\Rightarrow\; a, c := c, a.t < t \\ & I \wedge b > c \;\Rightarrow\; b, c := c, b.t < t \\ & \ldots \end{array}$$

Las implicaciones de (b) son evidentes, mientras que las de (c) se prueban todas de la misma forma; por ejemplo

$$\begin{array}{ll} & (b, c := c, b.t) < t \\ = & \qquad \because \text{definición de } t \\ & (a, c, b, d, e) < (a, b, c, d, e) \\ \Leftarrow & \qquad \because \text{orden lexicográfico} \\ & b > c \end{array}$$

Si las constantes son enteras, busquemos un contador entero de la forma

$$t \doteq \alpha a + \beta b + \gamma c + \delta c + \epsilon e.$$

En efecto, *ptle*

$$\begin{array}{ll} & wdec(a, c := c, a \mid t) \\ = & \qquad \because \text{Lema 6.43} \\ & (a, c := c, a.t) < t \\ = & \\ & \alpha c + \beta b + \gamma a + \delta c + \epsilon e < \alpha a + \beta b + \gamma c + \delta c + \epsilon e \\ = & \qquad \because \text{CP} \\ & 0 < (\alpha - \gamma)(a - c) \end{array}$$

y de la misma forma, *ptle*,

$$\begin{array}{rcl} wdec(b, c := c, b \mid t) & \equiv & 0 < (\beta - \gamma)(b - c), \\ wdec(c, d := d, c \mid t) & \equiv & 0 < (\gamma - \delta)(b - c), \\ wdec(c, e := e, c \mid t) & \equiv & 0 < (\gamma - \epsilon)(b - c). \end{array}$$

Por tanto, a la vista de las guardas, para que t sea un contador debería tenerse

$$\alpha < \gamma \qquad \beta < \gamma \qquad \gamma < \delta \qquad \gamma < \epsilon.$$

Por ejemplo, podemos tomar: $t \doteq a + b + 2c + 3d + 3e$.

8.54 [179] Considerando seis variables, bastará probar la corrección del programa

$$
\begin{array}{l}
a, b, c, d, e, f := A, B, C, D, E, F; \\
\{I\}\{\ \doteq\ (a, b, c, d, e, f) \textit{ es una permutación de } (A, B, C, D, E, F)\} \\
\ *[\![\quad a > c \rightarrow a, c := c, a \\
\quad \Box \quad b > c \rightarrow b, c := c, b \\
\quad \Box \quad c > d \rightarrow d, c := c, d \\
\quad \Box \quad c > e \rightarrow e, c := c, e \\
\quad \Box \quad c > f \rightarrow f, c := c, f\,]\!] \\
\{a, b \leq c \leq d, e, f \wedge I\}\ \{\Rightarrow\}\ \{\ c \text{ es el tercer menor elemento}\}
\end{array}
$$

La invariabilidad de I es trivial, y solo hemos de probar la terminación. Para ello se considera el subconjunto $\mathcal{C}$ de permutaciones de los valores iniciales, que resulta ser un conjunto finito de $\mathcal{D}^6$ con la relación de orden lexicográfica, y por tanto es un conjunto bien construido; ahora basta probar las condiciones del teorema de los contadores generalizados. Tomaremos $t : \mathcal{E} \rightarrow \mathcal{D}^6$, definida en la forma $t\ \doteq\ (a, b, c, d, e, f)$; probaremos

$$
\begin{array}{ll}
(a) & \forall i : 1 \leq i \leq 6 : [I \wedge b_i\ \Rightarrow\ t \in C] \text{ —trivial} \\
(b) & \forall i : 1 \leq i \leq 6 : [I \wedge b_i\ \Rightarrow\ wdec(S_i, t)].
\end{array}
$$

Probemos la condición (b) para un valor particular de i; por ejemplo, para la primera secuencia guardada

$$
\begin{array}{ll}
 & (a, c := c, a.t) < t \\
= & \\
 & (c, b, a, d, e, f) < (a, b, c, d, e, f) \\
= & \qquad \because \text{orden lexicográfico} \\
 & c < a
\end{array}
$$

8.55 [179] La negación de las guardas es $\neg OB \equiv y \leq 2 \wedge x \leq 1$, y tenemos que buscar un invariante verificando

$$
I \wedge OB \equiv I \wedge y \leq 2 \wedge x \leq 1\ \Rightarrow\ y = 1 \wedge x = 0
$$

Observando que las sentencias del bucle no alteran la paridad de las variables, podemos conjeturar como invariante el predicado

$$
I\ \doteq\ par\ x \wedge impar\ y \wedge x, y \geq 0
$$

que verifica

(A).– I se satisface delante del bucle:

$$
\begin{array}{ll}
 & x, y := 1000, 2001.I \\
= & \\
 & par\ 1000 \wedge impar\ 2001 \wedge 1000, 2001 \geq 0 \\
= & \\
 & Cierto
\end{array}
$$

(B).– I es invariante:

$$
\begin{array}{llll}
(B_1) & I \wedge y > 2 & \Rightarrow & y := y - 2.I \\
(B_2) & I \wedge x > 1 \wedge y \leq 2 & \Rightarrow & x, y := x - 2, x + 1.I
\end{array}
$$

En efecto

$$\begin{array}{ll} & y := y - 2.I \\ = & \\ & par\ x \wedge impar\ (y-2) \wedge x, y-2 \geq 0 \\ = & \\ & par\ x \wedge impar\ y \wedge x \geq 0, y \geq 2 \\ \Leftarrow & \\ & I \wedge y > 2 \end{array}
\qquad
\begin{array}{ll} & x, y := x-2, x+1.I \\ = & \\ & par\ (x-2) \wedge impar\ (x+1) \\ \wedge & x-2, y+1 \geq 0 \\ = & \\ & par\ x \wedge x \geq 2 \wedge y \geq 0 \\ \Leftarrow & \\ & I \wedge x > 1 \end{array}$$

Si el programa termina, por el teorema de invariantes lo hace con $I \wedge \neg OB$, y de aquí $x = 0 \wedge y = 1$. Para probar que termina podemos buscar un contador entero o también un contador sobre $\mathbb{Z}^2$. Un contador entero es $t \doteq x^2 + y$ ya que tenemos, *ptle*

$$\begin{array}{llcll} (C_1) & I \wedge OB & \Rightarrow & t > 0 & \text{— trivial} \\ (C_2) & I \wedge y > 2 & \Rightarrow & wdec(y := y-2, t) & \\ & I \wedge x > 1 \wedge y \leq 2 & \Rightarrow & wdec(x, y := x-2, x+1 \mid t) & \end{array}$$

En efecto

$$\begin{array}{ll} & wdec(y := y-2, t) \\ = & \quad \because \text{Lema 6.43} \\ & (y := y-2.t) < t \\ = & \\ & x^2 + y - 2 < x^2 + y \\ = & \\ & -2 < 0 \\ = & \\ & Cierto \end{array}
\qquad
\begin{array}{ll} & wdec(x, y := x-2, x+1 \mid t) \\ = & \quad \because \text{Lema 6.43} \\ & (x, y := x-2, x+1.t) < t \\ = & \\ & (x-2)^2 + x + 1 < x^2 + y \\ = & \\ & -3x + 5 < y \\ \Leftarrow & \\ & I \wedge x > 1 \end{array}$$

Veamos que la función $t : \mathcal{E} \to \mathbb{Z}^2$, dada por $t(x, y) \doteq (x, y)$, es un contador generalizado sobre el conjunto bien construido $\mathcal{C} = \mathbb{N}^2$, si consideramos la relación de orden lexicográfica

$$(x, y) < (x', y') \doteq x < x' \vee x = x' \wedge y < y'.$$

Para ello probaremos, *ptle*:

$$\begin{array}{llcll} (CE_1) & I \wedge OB & \Rightarrow & t \in \mathcal{C} & \text{— trivial} \\ (CE_2) & I \wedge y > 2 & \Rightarrow & (y := y-2.t) < t & \\ & I \wedge x > 1 \wedge y \leq 2 & \Rightarrow & (x, y := x-2, x+1.t) < t & \end{array}$$

En efecto

$$\begin{array}{ll} & y := y-2.t < t \\ = & \\ & (x, y-2) < (x, y) \\ = & \quad \because \text{orden lexicográfico} \\ & Cierto \end{array}
\qquad
\begin{array}{ll} & x, y := x-2, x+1.t < t \\ = & \\ & (x-2, x+1) < (x, y) \\ = & \quad \because \text{orden lexicográfico} \\ & Cierto \end{array}$$

Cambiemos ahora la segunda sentencia guardada en la forma

$$x > 1 \wedge y \leq 2 \to x := x-2; y : -Impar$$

donde la sentencia $y : -Impar$ asigna un impar positivo arbitrario a la variable y en forma indeterminista no acotada. Tal sentencia tiene por transformador de predicados, *ptle*:

$$y : -Impar.Z \doteq \forall k : k \geq 0 : y := 2k+1.Z \tag{$*$}$$

Obsérvese que la sentencia $y : -Impar$ satisface:

(i) $[\, y : -Impar.(\exists q : q \geq 0 : y = 2q+1) \,]$

(ii) $\forall n : n \geq 0 : [y : -Impar.(y < n) \equiv Falso]$

Para probar que el bucle termina basta probar

$$I \wedge x > 1 \wedge y \leq 2 \wedge t = t_0 \;\Rightarrow\; x := x-2; y : -Impar.(t < t_0)$$

(obsérvese que en este caso no es posible aplicar el Lema 6.43). Pero

$$\begin{array}{ll} & x := x-2; y : -Impar.(t < t_0) \\ = & \quad \because \text{semántica de } y : -Impar\text{; o sea, } (*) \\ & x := x-2.(\forall k : k \geq 0 : y := 2k+1.(t < t_0)) \\ = & \quad \because \text{def. de } t\text{, sustitución, CP} \\ & \forall k : k \geq 0 : (x-2, 2k+1) < t_0 \\ \Leftarrow & \\ & (x,y) = t_0 \end{array}$$

El nuevo programa termina sólo débilmente ya que para cualquier K, podemos encontrar una ejecución con más de K pasos; por ejemplo, si se ejecuta la segunda sentencia guardada al principio asignando a y el valor $2K+1$, se podrá ejecutar sucesivamente la primera sentencia guardada K veces.

8.56 [179] Basta probar que el predicado

$$I \doteq x\; par \wedge y\; impar \wedge x, y \geq 0$$

es un invariante y $t \doteq (x,y)$ un $\mathbb{Z}^2$–contador; el razonamiento es similar al del Ejercicio 8.55. Termina débilmente ya que la sentencia $Azar_z$ conlleva indeterminismo no acotado. Para que termine fuertemente basta cambiar la inicialización (por ejemplo) en la forma $z := 100$, ya que en ese caso la función $t \doteq 2x+y$ es un contador entero, como puede verse fácilmente:

$$(x, y := y-1, x+1.t) < t \;\equiv\; (2(y-1)+x+1 < 2x+y) \;\equiv\; (y \leq x)$$

de donde una cota del número de pasos es $2*(100)+2*(100)+1$.

8.57 [179] Según el teorema de invariantes, hay que buscar un invariante que asegure la terminación del bucle y verifique

$$\begin{array}{ll} & I \wedge \neg OB \;\Rightarrow\; x = 1 \wedge y = 1 \\ \equiv & \\ & I \wedge x \leq y \leq 1 \wedge x \leq 2 \;\Rightarrow\; x = 1 \wedge y = 1 \end{array}$$

Para ello basta tomar $I \doteq x, y \geq 1$, que verifica

$$\begin{array}{ll} (A) & x, y := 10, 10.I \\ = & \\ & 10, 10 \geq 0 \\ = & \\ & Cierto \end{array}$$

de lo cual $\{C\}x, y := 10, 10\{I\}$.

(B) I es invariante. En efecto, *ptle*

$$\begin{array}{llll} x,y := y,x.I & & = & I \\ y := y-1.I & \equiv\ x \geq 0 \wedge y \geq 1 & \Leftarrow & I \wedge y > 1 \\ x,y := x-2,x^y.I & \equiv\ x \geq 2 \wedge x^y \geq 0 & \Leftarrow & I \wedge x > 2 \end{array}$$

(C) El bucle termina. En efecto; tomemos el conjunto bien construido $\mathcal{C} = \mathbb{N}^2$, y el $\mathbb{Z}^2$–contador $t \doteq (x,y)$, que es contador ya que tenemos

$$\begin{array}{ll} [\, I \wedge OB \Rightarrow t \in \mathcal{C}\,] & \text{— trivial} \\ [\, I \wedge OB \wedge t = k \Rightarrow SI.t < k\,] & \end{array}$$

puesto que

$$\begin{array}{llllll} (x,y := y,x.t) < t & \equiv & (y,x) < (x,y) & \Leftarrow & I \wedge x > y \\ (y := y-2.t) < t & \equiv & (x,y-2) < (x,y) & \equiv & Cierto \\ (x,y := x-2,x^y.t) < t & \equiv & (x-2,x^y) < (x,y) & \equiv & Cierto \end{array}$$

8.58 [180] El predicado

$$I \doteq y\ par\ \geq 0 \wedge x > 0$$

es un invariante (se prueba igual que para el Ejercicio 8.55). Busquemos un contador de la forma $t \doteq \alpha x^2 + \beta y$, $\alpha, \beta > 0$; debemos verificar, *ptle*

$$\begin{array}{llll} (C_1) & I \wedge OB & \Rightarrow & t > 0 \quad \text{— trivial} \\ (C_2) & I \wedge y > 2 & \Rightarrow & wdec(y := y-2, t) \\ & I \wedge x \neq 1 \wedge y \leq 2 & \Rightarrow & wdec(x, y := x-1, 2*x \,|\, t) \end{array}$$

En efecto

$$\begin{array}{ll} & wdec(y := y-2, t) \\ = & \\ & y := y-2.t < t \\ = & \\ & \alpha x^2 + \beta(y-2) < \alpha x^2 + \beta y \\ = & \quad \because \beta > 0 \\ & Cierto \end{array} \qquad \begin{array}{ll} & wdec(x, y := x-1, 2x \,|\, t) \\ = & \\ & \alpha(x-1)^2 + \beta 2x < \alpha x^2 + \beta \\ = & \\ & 2x(\beta - \alpha) + \alpha < \beta y \end{array}$$

Para $x = 1$ e $y = 0$, la última desigualdad de la derecha obliga a tomar $2\beta < \alpha$. Al ser enteros, los menores valores son $\beta = 1$ y $\alpha = 3$. O sea, finalmente, tomaremos como contador $t \doteq 3x^2 + y$, para el cual se tiene

$$wdec(x, y := x-1, 2x \,|\, t) \equiv -4x + 3 < y \Leftarrow x > 0 \wedge y \geq 0 \Leftarrow I$$

El valor inicial del contador es 3001000, y será una cota del número de pasos.

8.59 [180] (A).— Consideremos como invariante el predicado $Cierto$. Probaremos

$$x > 0 \Rightarrow wdec(x := x-1, t) \qquad x < 0 \Rightarrow wdec(x := x+1, t)$$

$$\begin{array}{ll} & wdec(x := x-1, t) \\ = & \quad \because \text{Lema 6.43, def. de } t \\ & (x := x-1.|x|) < |x| \\ = & \quad \because \text{asignación} \\ & |x-1| < |x| \\ \Leftarrow & \\ & x > 0 \end{array} \qquad \begin{array}{ll} & wdec(x := x+1, t) \\ = & \quad \because \text{Lema 6.43, def. de } t \\ & (x := x+1.|x|) < |x| \\ = & \quad \because \text{asignación} \\ & |x+1| < |x| \\ \Leftarrow & \quad \because x < 0 \Rightarrow |x+1| = -(x+1) \wedge \ldots \\ & x < 0 \end{array}$$

Finalmente basta probar $[b_i \Rightarrow t > 0]$, lo cual es trivial.

(B).— El bucle termina fuertemente al admitir un contador entero.

(C).— Procedemos por inducción sobre k; el caso base es trivial. El paso inductivo sería (pongamos $H^k.C == H^k$ para simplificar):

$$\begin{array}{ll}
 & H^{k+1} \\
= & \quad \because \text{definición} \\
 & H^0 \vee SI.H^k \\
= & \quad \because \text{HI; semántica selectiva} \\
\wedge & \begin{array}{l} x = 0 \vee x \neq 0 \wedge (x > 0 \Rightarrow x := x - 1.|x| < k) \\ (x < 0 \Rightarrow x := x + 1.|x| < k) \end{array} \\
= & \quad \because \text{cálculo, sustitución} \\
 & x = 0 \vee (x > 0 \Rightarrow |x-1| < k) \wedge (x < 0 \Rightarrow |x+1| < k) \\
= & \quad \because \text{oro} \\
\wedge & \begin{array}{l} x = 0 \vee (x > 0 \Rightarrow x > 0 \wedge |x-1| < k) \\ (x < 0 \Rightarrow x < 0 \wedge |x+1| < k) \end{array} \\
= & \quad \because \text{definición } |\cdot|, \text{CP} \\
 & x = 0 \vee (x > 0 \Rightarrow x - 1 < k) \wedge (x < 0 \Rightarrow -(x+1) < k) \\
= & \quad \because \text{cálculo} \\
 & x = 0 \vee (x > 0 \Rightarrow x < k+1) \wedge (x < 0 \Rightarrow -x < k+1) \\
= & \quad \because \text{definición } |\cdot|, \text{CP, oro} \\
 & x = 0 \vee (x > 0 \Rightarrow |x| < k+1) \wedge (x < 0 \Rightarrow |x| < k+1) \\
= & \quad \because \text{CP} \\
 & x = 0 \vee (x > 0 \vee x < 0 \Rightarrow |x| < k+1) \\
= & \quad \because \text{CP} \\
 & x = 0 \vee (x \neq 0 \Rightarrow |x| < k+1) \\
= & \quad \because \text{CP} \\
 & |x| < k+1
\end{array}$$

(D).— $\mathcal{R}.C \equiv (\exists k : k \geq 0 : |x| \leq k) \equiv Cierto$.

(E).— Sea ahora $\mathcal{R}$ el bucle

$$\begin{array}{ll}
*[\![& x > 0 \rightarrow x := x - 1; Azar_y \\
\square & x < 0 \rightarrow x := x + 1; Azar_y \\
\square & y > 0 \rightarrow y := y - 1 \,]\!]
\end{array}$$

donde todas las variables son enteras. Probaremos el triplete

$$\{C\}y := 100; \mathcal{R}\{y = 0 \wedge x = 0\}$$

con terminación sólo débil. Se considera el invariante $I \doteq y \geq 0$, el conjunto bien construido $\mathbb{N}^2$ y la función $t \doteq (|x|, y)$; bastará demostrar que tal función es un $\mathbb{N}^2$–contador. Ya que trivialmente $[I \wedge \neg OB \Rightarrow y = 0 \wedge x = 0]$, aplicando el teorema de invariantes, es necesario (1) $\{C\}y := 100\{I\}$ (trivial) y (2) el bucle termina. Para ello probaremos las condiciones

(A)	I es invariante (trivial)
(B)	$I \wedge OB \Rightarrow t \in \mathbb{N}^2$ (trivial)
(C_1)	$I \wedge x > 0 \wedge t = t_0 \Rightarrow x := x - 1; Azar_y.(t < t_0)$
(C_2)	$I \wedge x < 0 \wedge t = t_0 \Rightarrow x := x + 1; Azar_y.(t < t_0)$
(C_3)	$I \wedge y > 0 \wedge t = t_0 \Rightarrow y := y - 1.(t < t_0)$

La última es muy fácil. Veamos (C_1). Sabemos – Ejemplo 8.6:162 – que, *ptle*

$$Azar_x.Z \doteq \forall k : k \in \mathbb{N} : x := k.Z$$

Entonces,

$$\begin{array}{ll} & x := x-1; Azar_y.(t < t_0) \\ = & \quad \because \text{semántica de } Azar_y\text{, definición de } t \\ & x := x-1.\forall k : k \geq 0 : y := k.((|x|, y) < t_0) \\ = & \quad \because \text{sustitución} \\ & \forall k : k \geq 0 : (|x-1|, k) < t_0 \\ \Leftarrow & \quad \because \text{orden lexicográfico} \\ & I \wedge x > 0 \wedge (|x|, y) = t_0 \end{array}$$

La terminación es débil ya que dado K, si por ejemplo el valor inicial de x es positivo, existe una ejecución con más de K pasos: elegir en el primer ciclo la primera sentencia guardada, asignar a y el valor $K+1$, y después, en sucesivos ciclos, elegir la última sentencia guardada (realizará más de $K+2$ pasos).

8.61 [180] (A).— $\{C\}inc_b\{C\}$ significa: inc_b siempre termina, mientras que el triplete $\{b = k\}inc_b\{(b-k) \text{ par } \geq 0\}$ significa: inc_b incrementa b es un valor par no negativo. Por definición $[inc_b.C \equiv C]$, de donde obtenemos el primer triplete. Para probar el segundo:

$$\begin{array}{ll} & inc_b.(b-k \text{ par } \geq 0) \\ = & \\ & \forall i : i \geq 0 : b := b+2i.(b-k \text{ par } \geq 0) \\ = & \\ & \forall i : i \geq 0 : (b+2i-k) \text{ par } \geq 0 \\ \Leftarrow & \\ & b = k \end{array}$$

(B).— Tenemos $\forall k : k \geq 0 : [F \equiv inc_b.(b \leq k)]$, además de $[C \equiv inc_b.C]$.

(C).—

$$\begin{array}{lllll} & b, r :\in \mathbb{Z}; b, r := 3, 3; & & & \\ & * [\![& r > 0 \wedge b > 0 & \to & r := r-1; inc_b \\ & & r > 1 & \to & r := r-2 \\ & & b > 1 & \to & b := b-2]\!] \end{array}$$

(D).— Consideremos el predicado $I \doteq b$ 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 invariabilidad y el decremento de t veamos únicamente el efecto de la primera sentencia del bucle:

$$\begin{array}{ll} & r := r-1; inc_b.((r, b) < t_0 \wedge b \text{ impar} \wedge b \geq 0 \wedge r \geq 0) \\ = & \quad \because \text{semántica de composición y definición de } inc_b \\ & r := r-1. \\ & \forall i : i \geq 0 : b := b+2i.((r, b) < t_0 \wedge b \text{ impar} \wedge b \geq 0 \wedge r \geq 0) \\ = & \quad \because \text{sustitución} \\ & r := r-1. \\ & \forall i : i \geq 0 : (r, b+2i) < t_0 \wedge b+2i \text{ impar} \wedge b+2i \geq 0 \wedge r \geq 0 \\ = & \quad \because \text{sustitución} \\ & \forall i : i \geq 0 : (r-1, b+2i) < t_0 \wedge (b+2i) \text{ impar} \wedge b+2i \geq 0 \wedge r-1 \geq 0 \end{array}$$

$\Leftarrow$ $\quad\because$ 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

$$
\begin{aligned}
& I \wedge \neg OB \\
\Rightarrow \quad & \\
& b \text{ impar} \wedge 0 \leq b \leq 1 \wedge 0 \leq r \leq 1 \wedge (r \leq 0 \vee b \leq 0) \\
\Rightarrow \quad & \\
& r = 0 \wedge b = 1
\end{aligned}
$$

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

8.62 [181] Aplicaremos el Teorema de los Contadores Generalizados (TCG) tomando $t \doteq (x, y)$ y el invariante $I \doteq x, y \geq 0$. La invariancia es trivial. $\mathcal{C} \doteq \mathbb{N}^2$ es bien construido, y se verifican las condiciones del TCG. Falta probar:

$$
\begin{array}{ll}
(a) & I \wedge x > 0 \wedge t = t_0 \;\Rightarrow\; Azar_{x012}; y := y^x.(t < t_0) \\
(b) & I \wedge y > 0 \wedge t = t_0 \;\Rightarrow\; Azar_{x012}; y := y - 1.(t < t_0)
\end{array}
$$

Ambas se prueban en forma parecida. Antes se prueba

$$[\, x = a > 0 \;\Rightarrow\; Azar_{x012}.(0 \leq x < a)\,] \qquad (*)$$

que es muy fácil (véase Ejercicio 9.35). Además,

$$
\begin{aligned}
& Azar_{x012}; y := y^x.((x, y) < (x_0, y_0)) \\
= \quad & \because \text{sustitución} \\
& Azar_{x012}.((x, y^x) < (x_0, y_0)) \\
\Leftarrow \quad & \because \text{orden lexicográfico, monotonía de Azar} \\
& Azar_{x012}.(x < x_0) \\
= \quad & \because (*) \\
& x = x_0 > 0 \\
\Leftarrow \quad & \\
& I \wedge x > 0 \wedge t = t_0.
\end{aligned}
$$

Luego el bucle termina, y lo hace satisfaciendo $I \wedge x, y \leq 0 \;\Rightarrow\; x = y = 0$.

8.63 [181] Imposible, ya que el lenguaje de Dijkstra es continuo (Teorema 8.1).

8.64 [181] La corrección se obtiene del invariante $I \doteq x\ impar \geq 0 \wedge y\ impar\ \geq 0$, ya que, si terminara y fuera invariante tendríamos al final del bucle

$$
\begin{aligned}
& I \wedge \neg OB \\
= \quad & \\
& 0 \leq x \leq 1 \wedge 0 \leq y \leq 2 \wedge x, y \text{ impares} \\
\Rightarrow \quad & \\
& x = 1 \wedge y = 1.
\end{aligned}
$$

Para demostrar que termina probaremos que la función

$$t(x, y) \;\doteq\; \begin{cases} (|x| + 1, y) & \text{si} \quad x < 0 \\ (x, y) & \text{si} \quad x \geq 0 \end{cases}$$

es un $\mathbb{Z}^2$–contador asociado al invariante I para el conjunto bien construido $\mathbb{N}^2$ (con el orden lexicográfico). En definitiva hay que probar:

$\underline{(A)}$.— I es invariante. Veamos solamente un caso

$$
\begin{array}{ll}
 & [I \wedge x > 1 \wedge y \leq 2 \ \Rightarrow \ x, y := x-2, y+2.I] \\
= & \quad \because \text{semántica} \\
= & [x\ impar, y\ impar \geq 0 \wedge x > 1 \wedge y \leq 2 \ \Rightarrow \ x-2\ impar, y+2\ impar \geq 0] \\
 & Cierto
\end{array}
$$

$\underline{(B)}$.— $[I \wedge OB \ \Rightarrow \ t \in \mathbb{N}^2]$. Esta es fácil ya que $t \in \mathbb{N}^2$.

$\underline{(C)}$.— $\forall i : 1 \leq i \leq 3 : [I \wedge B_i \ \Rightarrow \ (S_i.t) < t]$. En efecto, veamos una de ellas

$$
\begin{array}{ll}
 & x := -x.t < t \\
= & \quad \because \text{sustitución} \\
 & t(-x) < t(x) \\
= & \quad \because \text{si } x < 0\text{, definición de } t \\
 & (x, y) < (|x|+1, y) \\
= & \quad \because \text{orden lexicográfico} \\
 & Cierto
\end{array}
$$

El programa termina solo débilmente ya que dado K podemos encontrar una ejecución con más de K pasos; basta observar que si la primera sentencia asigna a x el valor $-K$, y seleccionamos al principio la primera guarda y después sucesivamente la segunda, ejecutaríamos más de K pasos.

8.65 [181] $\underline{(A)}$.— Un programa termina débilmente si termina pero no es posible encontrar una cota del número de sentencias elementales que realiza como función del estado inicial. Como ejemplo vale el del apartado (C).

$\underline{(B)}$.— No, ya que continuidad y terminación débil implica terminación fuerte (véase Teorema 8.49).

$\underline{(C)}$.— El siguiente programa simula el juego, siendo la sentencia Inc_x una sentencia que incrementa x con un número natural con indeterminismo no acotado (véase Ejemplo 8.6:162):

$$
\begin{array}{llll}
b, v, r :\in \mathbb{Z} & & & \text{— tres variables con las frecuencias de cada color} \\
b, v, r := 20, 20, 20; & & & \\
\quad *[\![& b > 0 \rightarrow & b := b-1; Inc_r; Inc_v & \\
\quad \Box & r > 0 \rightarrow & r := r-1; Inc_v & \\
\quad \Box & v > 0 \rightarrow & v := v-1]\!] &
\end{array}
$$

Obsérvese que cada guarda determina si es posible extraer una bola de un color determinado. El bucle termina débilmente ya que $\mathcal{C} \doteq \mathbb{N}^3 (\subseteq \mathbb{Z}^3)$ es bien construido para la relación de orden lexicográfica, y la función $t : \mathcal{E} \rightarrow \mathbb{Z}^3$ definida por $t \doteq (b, r, v)$, es un contador generalizado relativo al predicado invariante $I \doteq (b, r, v) \in \mathcal{C}$, ya que, *ptle*

$$
\begin{array}{ll}
(a) & I \ \Rightarrow \ t \in \mathcal{C} \text{ (trivial)}, \\
(b_1) & I \wedge b > 0 \wedge t = t_0 \ \Rightarrow \ b := b-1; Inc_r; Inc_v.(t < t_0), \\
(b_2) & I \wedge r > 0 \wedge t = t_0 \ \Rightarrow \ r := r-1; Inc_v.(t < t_0), \\
(b_3) & I \wedge v > 0 \wedge t = t_0 \ \Rightarrow \ v := v-1.(t < t_0), \\
(c) & I \text{ es un invariante (trivial).}
\end{array}
$$

Recordemos que la sentencia $Inc\, x$ tiene como transformador de predicados:

$$Inc\, x\,.\,Z \doteq \forall k : k \geq 0 : x := x + k.Z$$

Con esta definición, veamos por ejemplo (b_2):

$$\begin{array}{ll}
& r := r - 1; Inc_v.(t < t_0) \\
= & \quad \because \text{definición de } Inc \text{ y de } t \\
& r := r - 1.\forall k : k \geq 0 : v := v + k.((b, r, v) < (b_0, r_0, v_0)) \\
= & \quad \text{sustitución} \\
& \forall k : k \geq 0 : (b, r - 1, v + k) < (b_0, r_0, v_0) \\
\Leftarrow & \quad \because \text{relación lexicográfica} \\
& (b, r, v) = (b_0, r_0, v_0)
\end{array}$$

Las otras implicaciones se prueban igual. El programa no termina fuertemente ya que dado K, podemos encontrar una ejecución con $K + 1$ asignaciones; por ejemplo, seleccionar en el primer paso la segunda guarda asignando a la variable v el valor K; después ejecutar la tercera guarda K veces, con lo que habremos ejecutado $K + 1$ sentencias elementales. Finalmente, no existe ninguna contradicción con el apartado (B) ya que el programa no es continuo.

8.66 [181] (A).— FALSO: la sentencia $desastre$ – Ejemplo 8.2 – es sana y no es continua.

(B).— FALSO: $desastre$ introduce indeterminismo no acotado.

(C).— FALSO: el transformador $[S.X \doteq x := 0.X \vee x := 1.X]$ es estricto, pero no es conjuntivo ya que, para $A \doteq (x = 0)$ y $B \doteq (x = 1)$, se verifica $[S.(A \wedge B) \equiv F]$, pero $[S.A \wedge S.B \equiv C]$.

(D).— CIERTO. Véase Ejercicio 3.18.

(E).— CIERTO. Por ejemplo, para $\mathcal{S} \doteq [\![\, C \rightarrow y := 1 \,\Box\, C \rightarrow y := 0 \,]\!]\, ; x := 1$,

$$\begin{array}{lclcl}
\mathcal{S}.(x = 1) & \equiv & [\![\, C \rightarrow y := 1 \,\Box\, C \rightarrow y := 0 \,]\!].Cierto & \equiv & Cierto \\
\mathcal{S}.(y = 1) & \equiv & y := 1.y = 1 \wedge y := 0.y = 1 & \equiv & Falso
\end{array}$$

e igualmente, $[\mathcal{S}.(y = 0) \equiv Falso]$, pero $[\mathcal{S}.(y = 1 \vee y = 0) \equiv Cierto]$, de donde $\mathcal{S}$ no es disyuntiva.

8.68 [182] El programa $Azar_x; *[\![\, x > 0 \rightarrow x := x - 1 \,]\!]$ termina solo débilmente ya que el número de pasos del bucle es el valor inicial de x, que es indeterminista no acotado. Esto no está en contradicción con *terminación* $\not\Rightarrow$ *terminación fuerte*, ya que es un ejemplo de lo anterior.

8.69 [182] (A).— Para la sentencia $S.X \doteq \neg X$, tenemos, *ptle*

$$\begin{array}{lclcl}
S.(x \geq 2) \wedge S.(x \leq 2) & \equiv & x < 2 \wedge x > 2 & \equiv & F \\
S.(x \geq 2 \wedge x \leq 2) & \equiv & S.(x = 2) & \equiv & x \neq 2
\end{array}$$

de donde $[S.x \geq 2 \wedge S.x \leq 2 \not\equiv S.(x \geq 2 \wedge x \leq 2)]$, y S no es conjuntiva.

(B).— Por ejemplo, $S \doteq [\![\, C \rightarrow x := 1 \,\Box\, C \rightarrow x := 2 \,]\!]$, que verifica *ptle*

$$S.Q \equiv C \wedge (C \Rightarrow x := 1.Q) \wedge (C \Rightarrow x := 2.Q) \equiv x := 1.Q \wedge x := 2.Q$$

y de aquí es fácil ver que es indeterminista, ya que, *ptle*

$$Cierto \equiv S.(x = 2 \vee x = 1) \not\equiv S.x = 2 \vee S.x = 1 \equiv F$$

y además, $[S.Cierto = Cierto]$.

(C).— Definimos la sentencia $\mathcal{A}.Z \doteq \forall n : n \in \mathbb{N} : x := 2n.Z$, que verifica:

(a) $[\ \mathcal{A}.(par\_pos\ x)\ ]$,
(b) $\forall n : n \geq 0 : [\mathcal{A}.(0 \leq x \leq n) \equiv Falso]$.

Si consideramos la sucesión de predicados $\{0 \leq x \leq k\}$, ésta es creciente y, *ptle*

$$
\begin{array}{ll}
 & \mathcal{A}.(\exists k : 0 \leq x \leq k : 0 \leq x \leq k \wedge par\_pos\ x) \\
= & \quad \because (a) \\
 & Cierto \\
\neq & \\
 & Falso \\
= & \quad \because (b) \\
 & \exists k : 0 \leq x \leq k : \mathcal{A}.(0 \leq x \leq k \wedge par\_pos\ x)
\end{array}
$$

y por tanto $\mathcal{A}$ no es continua.

8.71 [182] (A).— Véase el Ejemplo 8.19.

(B).— *ptle*

$$
\begin{array}{ll}
 & [\![\, p \rightarrow S \,\square\, q \rightarrow T \,]\!] .X \\
= & \quad \because \text{semántica selectiva} \\
 & (p \vee q) \wedge (p \Rightarrow S.X) \wedge (q \Rightarrow T.X) \\
= & \quad \because \text{regla de oro} \\
 & (p \vee q) \wedge (p \equiv p \wedge S.X) \wedge (q \equiv q \wedge T.X) \\
= & \quad \because S =_p S' \wedge T =_q T' \\
 & (p \vee q) \wedge (p \equiv p \wedge S'.X) \wedge (q \equiv q \wedge T'.X) \\
= & \quad \because \text{regla de oro y semántica selectiva} \\
 & [\![\, p \rightarrow S' \,\square\, q \rightarrow T' \,]\!] .X
\end{array}
$$

(C).—

$$
\begin{array}{ll}
 & [\![\ \square\ : 1 \leq i \leq n : b_i \rightarrow S_i \,]\!]\ .Z \\
= & \quad \because \text{semántica de la selectiva} \\
 & OB \wedge \forall i : 1 \leq i \leq n : b_i \Rightarrow S_i.Z \\
= & \quad \because \text{CP} \\
 & OB \wedge \forall i : 1 \leq i \leq n : b_i \Rightarrow b_i \wedge S_i.Z \\
= & \quad \because \text{hipótesis: } \forall Z, i : 1 \leq i \leq n : [b_i \wedge S_i.Z \equiv b_i \wedge T_i.Z] \\
 & OB \wedge \forall i : 1 \leq i \leq n : b_i \Rightarrow b_i \wedge T_i.Z \\
= & \quad \because \text{CP} \\
 & OB \wedge \forall i : 1 \leq i \leq n : b_i \Rightarrow T_i.Z \\
= & \quad \because \text{semántica de la selectiva} \\
 & [\![\ \square\ : 1 \leq i \leq n : b_i \rightarrow T_i \,]\!]\ .Z
\end{array}
$$

(D).—

$$
\begin{array}{ll}
 & *[\![\, p \rightarrow S \,\square\, q \rightarrow T \,]\!] = *[\![\, p \rightarrow S' \,\square\, q \rightarrow T' \,]\!] \\
= & \quad \because \text{equivalencia con bucles con una sola guarda}
\end{array}
$$

$*[\![p \vee q \to [\![p \to S \,\square\, q \to T]\!]]\!] = *[\![p \vee q \to [\![p \to S' \,\square\, q \to T']\!]]\!]$
$\Leftarrow$ $\because$ apartado (A)
$[\![p \to S \,\square\, q \to T]\!] = [\![p \to S' \,\square\, q \to T']\!]$
$\Leftarrow$ $\because$ apartado (B)
$S =_p S' \wedge T =_q T'$

(E).— *ptle*

$x > 0 \wedge [\![x > 0 \to x := x + 1 \,\square\, x < -3 \to x := x - 1]\!] \,.\, Z$
$=$ $\because$ semántica de la selectiva
$x > 0 \wedge (x > 0 \vee x < -3)$
$\wedge\, (x > 0 \;\Rightarrow\; x := x + 1.Z) \wedge (x < -3 \;\Rightarrow\; x := x - 1.Z)$
$=$ $\because$ CP
$x > 0 \wedge (x > 0 \;\Rightarrow\; x := x + 1.Z) \wedge (x < -3 \;\Rightarrow\; \ldots)$
$=$ $\because$ CP
$x > 0 \wedge x := x + 1.Z$

(F).— Sea $S \doteq [\![x > 0 \to x := x - 1 \,\square\, x < 0 \to x := x + 1]\!]$. Entonces,

$[\![x > 0 \to x := x + 1 \,\square\, x \leq 0 \to x := x - 1]\!] \,;\, S$
$=$ $\because$ Ejercicio 6.28(D)
$[\![x > 0 \to x := x + 1; S \,\square\, x \leq 0 \to x := x - 1; S]\!]$
$=$ $\because \{x > 0\} x := x + 1 \{x > 0\}$, además $S =_{x>0} x := x - 1$
$[\![x > 0 \to x := x + 1; x := x - 1 \,\square\, x \leq 0 \to x := x - 1; S]\!]$
$=$ $\because \{x \leq 0\} x := x - 1 \{x < 0\}$, además $S =_{x<0} x := x + 1$
$[\![x > 0 \to x := x + 1; x := x - 1 \,\square\, x \leq 0 \to x := x - 1; x := x + 1]\!]$
$=$ $\because$ Lema 4.7(i) (de sustitución)
$[\![x > 0 \to nada \,\square\, x \leq 0 \to nada]\!]$
$=$ $\because$ semántica
$nada$

8.72 [183] (A).— $Y : [Y \equiv i \geq N \vee i < N \wedge i := i + 2.Y]$

(B).—

$\forall k : k \geq 0 : [N - 2k \leq i \;\Rightarrow\; Y_1]$
$=$ $\because$ inducción:
–CASO BASE:$[N \leq i \;\Rightarrow\; Y_1]$
trivial, ya que si Y_1 es punto fijo, $Y_1 \equiv i \geq N \vee \ldots$

– PASO INDUCTIVO: *ptle*
Y_1
$=$ $\because$ si fuera un punto fijo
$i \geq N \vee i < N \wedge i := i + 2.Y_1$
$\Leftarrow$ $\because$ HI:$[N - 2k \leq i \;\Rightarrow\; Y_1]$; $i := i + 2$ es monótona
$i \geq N \vee i < N \wedge i := i + 2.N - 2k \leq i$
$=$ $\because$ semántica asignación
$i \geq N \vee i < N \wedge N - 2k \leq i + 2$
$=$ $\because$ cálculo
$N - 2(k + 1) \leq i$

(C).— Sea Y_1 un punto fijo; entonces, *ptle*

$Cierto$

$=\quad \because$ por el apartado (B)
$\quad \forall k : k \geq 0 : [N - 2k \leq i \;\Rightarrow\; Y_1]$
$=\quad \because [\,]$ es conjuntivo
$\quad [\forall k : k \geq 0 : (N - 2k \leq i \;\Rightarrow\; Y_1)]$
$=\quad \because$ cálculo
$\quad [(\exists k : k \geq 0 : N - 2k \leq i) \;\Rightarrow\; Y_1]$
$=\quad \because$ cálculo
$\quad [Cierto \;\Rightarrow\; Y_1]$
$=\quad \because$ cálculo
$\quad [Y_1]$

de donde cualquier punto fijo debe ser $Cierto$ *ptle*, y en particular $[\mathcal{R}.C \equiv C]$.

(D).— La nueva ecuación que debe verificar $\mathcal{R}'.C$ es $Y : [Y \equiv g.Y]$, donde $g.Y \doteq i \geq N \vee i < N \wedge S'.Y$. Pero, *ptle*

$\quad S'.(i \geq N)$
$=\quad \because$ semántica selección
$\quad i < N \wedge i + 2 \geq N \wedge i - 1 \geq N$
$=\quad \because$ cálculo
$\quad Falso$

de donde $[g.(i \geq N) \equiv i \geq N]$, y $i \geq N$ es un punto fijo; pero $[i \geq N \;\Rightarrow\; g.Y]$, luego $i \geq N$ es el menor punto fijo. La interpretación es que para asegurar la terminación no debe ejecutarse ninguna vez el cuerpo del bucle, ya que podría ejecutarse indefinidamente la segunda sentencia guardada.

8.73 [183] (Véase también Ejercicio 8.50) (A) y (C).— Calculemos $H^n.C$ pero tomando la sentencia $x := x + N$ en lugar de $x := x + 1$. Por definición $[H^0.C \equiv \neg b]$, mientras que (pongamos $H^n.C == H^n$ para simplificar), *ptle*

$\quad H^1$
$=\quad \because$ definición y semántica selectiva
$\quad H^0 \vee b \wedge x := x + N.b := x < 10.H^0 \wedge x := x - 1.b := x > 0.H^0$
$=\quad \because [H^0 \equiv \neg b]$
$\quad \neg b \vee b \wedge x := x + N.b := x < 10.\neg b \wedge x := x - 1.b := x > 0.\neg b$
$=\quad \because$ semántica asignación
$\quad \neg b \vee b \wedge x := x + N.x \geq 10 \wedge x := x - 1.x \leq 0$
$=\quad \because$ semántica asignación
$\quad \neg b \vee b \wedge x + N \geq 10 \wedge x \leq 1$

Luego, para $N = 1$, $[H^1 \equiv \neg b]$, y por inducción, $[H^n \equiv \neg b]$, de donde, ya que $[\mathcal{R}.C \equiv \exists n : n \geq 0 : H^n]$, $[\mathcal{R}.C \equiv \neg b]$. Lo mismo puede decirse para $N \leq 8$.

(B).— La interpretación es simple: si el bucle comienza (necesariamente con b) entonces se pueden ejecutar en forma alternativa ambas secuencias guardadas, y el bucle no termina. Pero esto no es posible si por ejemplo $N = 9$, ya que dejaría de verificarse la alternancia puesto que necesariamente una de las secuencias guardadas cambiará el valor de b.

(D).— La ecuación que determina la semántica en TPF de $\mathcal{R}.C$ es

$$Y : [Y \equiv \neg b \vee b \wedge x := x + N.b := x < 10.Y \wedge x := x - 1.b := x > 0.Y]$$

que admite la solución $\neg b$, y por la Nota 8.12, el menor punto fijo es $\neg b$, que sería la semántica de $\mathcal{R}.C$.

8.74 [183] (A).— Definimos $Extrae \doteq [\![\, C \rightarrow x := 1 \,\square\, C \rightarrow x := 3 \,\square\, C \rightarrow x := 5 \,]\!]$, cuyo transformador de predicados es

$$Extrae.Z \equiv x := 1.Z \wedge x := 3.Z \wedge x := 5.Z$$

Fácilmente vemos que $Extrae$ no es disyuntivo; así, tomando $Z_1 \doteq x = 1$, y $Z_2 \doteq x \neq 1$, entonces $[Extrae.Z_i \equiv Falso]$, mientras que $Extrae.(Z_1 \vee Z_2) = Cierto$, luego $Extrae$ no es disyuntivo. Además $Extrae.(x = 1 \vee x = 2 \vee x = 3) \equiv Cierto$; de aquí obtenemos el triplete $\{C\}Extrae\{x = 1 \vee x = 3 \vee x = 5\}$.

(B).— Consideremos el programa $\mathcal{P}$

$$\begin{array}{lll}
r, b := 3, 3; & & \\
\ast[\![\quad r > 1 & \rightarrow & r := r - 2 \\
\square \quad b > 1 & \rightarrow & b := b - 2 \\
\square \quad r > 0 \wedge b > 0 & \rightarrow & r, b := r - 1, b - 1; Extrae; b := b + x \,]\!]
\end{array}$$

Es fácil demostrar que $I \doteq r, b \geq 1 \wedge impar\ b$ es un invariante:

$$(r := r - 2.I) \equiv (r - 2, b \geq 1 \wedge impar\ b) \Leftarrow (I \wedge r > 1$$

$$\begin{array}{ll}
 & r, b := r - 1, b - 1.Extrae.b := b + x.I \\
= & \\
 & r, b := r - 1, b - 1.Extrae.b := b + x.(r, b \geq 1 \wedge impar\ b)) \\
= & \\
 & r, b := r - 1, b - 1.Extrae.(r, b + x \geq 1 \wedge impar\ (b + x) \\
= & \quad \because \text{definición de } Extrae \\
 & r, b := r - 1, b - 1.(r, b + 1 \geq 1 \wedge impar\ (b + 1) \\
\wedge & \\
 & r, b + 3 \geq 1 \wedge impar\ (b + 3) \wedge r, b + 5 \geq 1 \wedge impar\ (b + 5) \ ) \\
\Leftarrow & \quad \because \text{monotonía} \\
 & r, b := r - 1, b - 1.(r \geq 1 \wedge b \geq 1 \wedge par\ b) \\
= & \\
 & r - 1 \geq 1 \wedge b - 1 \geq 1 \wedge par\ (b - 1) \\
\Leftarrow & \\
 & I \wedge r, b > 0
\end{array}$$

(C).— Si el programa $\mathcal{P}$ termina siempre, entonces por el teorema de invariantes $\{C\}\mathcal{P}\{\neg OB \wedge I\}$, pero $[\neg OB \wedge I \Rightarrow r = 0 \wedge b = 1]$, y al final del juego la urna contiene exactamente una única bola blanca.

(D).— Un contador entero puede ser $t \doteq Kr + b$, donde K se tomará de forma que la tercera sentencia guardada S_3 decremente el contador. Ya que S_3 incrementa b a lo sumo en 5 unidades, bastará tomar $K > 5$ (*demuéstrese esto último*).

(E).— Si utilizamos conjuntos bien construidos, tomaremos $\mathcal{C} \equiv \mathbb{N}^2$ con el orden lexicográfico y el contador $t(r, b) = (r, b)$; entonces, solamente tenemos dificultad en la sentencia S_3; pero $[(S_3.t) < t]$ (demuéstrese).

8.75 [184] (A).— La ecuación es $Y : [Y \equiv g.Y]$, donde $g.Y \doteq x = y \vee SI.Y$.

(B).— Por el teorema de Tarski–Knaster (Teorema 2.13) bastará probar que $[g.Z \Rightarrow Z]$, siendo $Z \doteq (x - y)\ par$. Pero, *ptle*,

$$
\begin{array}{ll}
 & g.Z \\
= & \\
 & x = y \vee SI.Z \\
= & \quad \because \text{semántica selectiva} \\
 & x = y \vee x \neq y \wedge (x > y \Rightarrow x, y := x - 1, y + 1.Z) \\
\wedge & (x < y \Rightarrow x, y := x + 1, y - 1.Z) \\
= & \quad \because \text{definición de } Z \text{, ya que } [x, y := x - 1, y + 1.Z \equiv Z], \ldots \\
 & x = y \vee x \neq y \wedge (x > y \Rightarrow Z) \wedge (x < y \Rightarrow Z) \\
= & \quad \because \text{CP} \\
 & x = y \vee x \neq y \wedge (x \neq y \Rightarrow Z) \\
= & \quad \because \text{CP} \\
 & x = y \vee x \neq y \wedge Z \\
= & \quad \because x = y \Rightarrow Z \text{, regla de oro, tercio excluido} \\
 & Z
\end{array}
$$

Luego hemos demostrado que $[g.Z \equiv Z]$, y en particular $[g.Z \Rightarrow Z]$.

(C).— Por definición de triplete, basta probar $[A \Rightarrow \mathcal{R}.C] \Rightarrow [A \Rightarrow Z]$, que es consecuencia de $[\mathcal{R}.C \Rightarrow Z]$ y de la transitividad de $\Rightarrow$.

(D).— Ya sabemos que $\forall i :: [Z \equiv S_i.Z]$.

(E).— Hay que probar, $\forall i$ y *ptle*: (1) $b_i \wedge Z \Rightarrow t > 0$ (trivial), (2) $b_i \wedge Z \Rightarrow wdec(S_i, t)$. De nuevo por simetría, basta probar una de las implicaciones de (2). Tenemos, *ptle*,

$$
\begin{array}{ll}
 & wdec(x, y := x - 1, y + 1 \mid t) \\
= & \quad \because \text{Lema 6.43, definición de } t \\
 & |x - y - 2| < |x - y| \\
\Leftarrow & \quad \because \text{CP} \\
 & x > y \wedge (x - y)\ par
\end{array}
$$

(F).— Del apartado (E) y del (D), aplicando el Teorema de los Contadores (Teorema 6.38) y el Teorema de Invariantes, concluimos $[Z \Rightarrow \mathcal{R}.C]$; la otra implicación es consecuencia del apartado (B).

(G).— La interpretación es que, si comienza el bucle con $x - y\ impar$, entonces, llegará un momento en que los valores de x e y oscilen entre los valores $m - 1$ y $m + 1$, siendo m la media; por ejemplo, para $(x, y) = (2, 7)$, la secuencia de valores sucesivos es $(2, 7), (3, 6), (4, 5), (5, 4), (4, 5), \ldots$.

9.12 [196] Es fácil demostrar, *ptle*,

$$m.(i > 100) = i > 100 \vee i := i + 1.m.(m.i > 100)$$

La propiedad

$$[i = k \wedge m.(X \wedge i > 100) \equiv i = k \wedge m.X] \qquad (*)$$

es trivialmente cierta para $k > 100$. Para $k \leq 100$:

$$
\begin{array}{ll}
 & i = k \wedge m.(X \wedge i > 100) \\
= & \quad \because k \leq 100,\ (in) \\
 & i = k \wedge i := i + 101 - k.(X \wedge i > 100) \\
= & \\
 & i = k \wedge i := i + 101 - k.X \wedge i > k - 1 \\
= & \quad \because (in) \text{, regla de oro}
\end{array}
$$

$i = k \wedge m.X$

De aquí obtenemos, $m; m = m$, ya que $m.m.X$

$=$
$m.(m.X)$
$= \quad \because (*)$
$m.(m.X \wedge i > 100)$
$= \quad \because$ PF
$m.(X \wedge i > 100)$
$= \quad \because (*)$
$m.X$

9.15 [201] (A).— Tenemos, *ptle*

$SI.X$
$= \quad \because$ semántica
$(Cierto \Rightarrow U.X) \wedge (Cierto \Rightarrow V.X)$
$= \quad \because [(Cierto \Rightarrow A) \equiv A]$
$U.X \wedge V.X$

(B).— También, *ptle*

$[\![a \to U \,\square\, b \to V \,\square\, b \to W]\!] .X$
$\equiv$
$[\![a \to U \,\square\, b \to [\![C \to V \,\square\, C \to W]\!]]\!] .X$
$= \quad \because$ semántica de SI, (A)
$(a \vee b) \wedge (a \Rightarrow U.X) \wedge (b \Rightarrow V.X) \wedge (b \Rightarrow W.X)$
$\equiv$
$(a \vee b) \wedge (a \Rightarrow U.X) \wedge (b \Rightarrow V.X \wedge W.X)$
$= \quad \because [(b \Rightarrow V.X) \wedge (b \Rightarrow W.X) \equiv b \Rightarrow V.X \wedge W.X]$
$Cierto$

(C).— De nuevo, *ptle*

$m.X$
$= \quad \because (B)$
$[\![i > 10 \to nada \,\square\, i \leq 10 \to$
$\quad [\![C \to i := i + 2; m; m \,\square\, C \to i := i + 2; m]\!]]\!] .X$
$= \quad \because$ semántica selección binaria y (A)
$i > 10 \wedge nada.X \vee i \leq 10 \wedge i := i + 2; m; m.X \wedge i := i + 2; m.X$
$= \quad \because$ semántica nada, conjuntividad de $i := i + 2; m$
$i > 10 \wedge X \vee i \leq 10 \wedge i := i + 2; m.(m.X \wedge X)$

(D).—

$\{i = 10\} m \{X\} \equiv \{i = 10\} i := i + 2 \{X\}$
$= \quad \because$ def. triplete
$[i = 10 \Rightarrow m.X] \equiv [i = 10 \Rightarrow i := i + 2.X]$
$= \quad \because$ regla de oro
$[i = 10 \wedge m.X \equiv i = 10] \equiv [i = 10 \wedge i := i + 2.X \equiv i = 10]$
$\Leftarrow \quad \because$ regla de Leibniz
$[(i = 10 \wedge m.X) \equiv (i = 10 \wedge i := i + 2.X)]$
$= \quad \because$ por (C) y conjuntividad de asignación
$[i = 10 \wedge i := i + 2.m.(X \wedge m.X) \equiv i := i + 2.(i = 12 \wedge X)]$

$=\qquad \because$ semántica asignación, conjuntividad

$\Leftarrow \begin{array}{l}[i := i+2.(i=12 \wedge m.(X \wedge m.X)) \equiv i := i+2.(i=12 \wedge X)] \\ [i=12 \wedge m.(X \wedge m.X) \equiv i=12 \wedge X]\end{array}$

$=\qquad \because (C)$

$[i=12 \wedge X \wedge m.X \equiv i=12 \wedge X]$

$=\qquad \because (C)$

$= \begin{array}{l}[i=12 \wedge X \wedge X \equiv i=12 \wedge X] \\ Cierto\end{array}$

9.24 [206] Sea Z un predicado arbitrario. Primero probaremos por inducción,

$$\forall N : N \in \mathbb{N} : [xfact(N,u).Z \equiv u := N!.Z] \qquad (*)$$

El caso base corresponde a $N = 0$, y tendremos,

$xfact(0,u).Z$

$=\qquad \because$ semántica por nombre

$0, u \in \mathbb{N} \wedge [\![\, 0 = 0 \rightarrow u := 1 \,\Box\, 0 > 0 \rightarrow xfact(0-1,u); u := u * 0 \,]\!].Z$

$=\qquad \because$ semántica selectiva

$0, u \in \mathbb{N} \wedge u := 1.Z$

$=\qquad \because$ por la declaración de u, además de $0! = 1$

$u := 0!.Z$

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

$xfact(N,u).Z$

$=\qquad \because$ semántica por nombre

$N, u \in \mathbb{N} \wedge [\![\, N = 0 \rightarrow u := 1 \,\Box\, N > 0 \rightarrow xfact(N-1,u); u := u * N \,]\!].Z$

$=\qquad \because$ semántica selectiva, $N > 0$, además de $N, u \in \mathbb{N}$

$xfact(N-1,u).(u := u * N.Z)$

$=\qquad \because$ HI

$u := (N-1)!.(u := u * N.Z)$

$=\qquad \because$ lema de sustitución – Lema 4.7(i)

$u := (N-1)! * N.Z$

$=\qquad \because$ definición de factorial

$u := N!.Z$

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

$xfact(N,u).(u = N!)$

$=\qquad \because$ por $(*)$, tomando $Z \doteq (u = N!)$

$u := N!.(u = N!)$

$=\qquad \because$ sustitución

$= \begin{array}{l}N! = N! \\ Cierto\end{array}$

9.26 [207] (A).— $T.X \;\doteq\; \exists k : k \geq 0 : T^k.X$, donde

$$T^0 \;\doteq\; aborta, \qquad\qquad T^{k+1} \;\doteq\; S; [\![\, b \rightarrow T^k \,\Box\, \neg b \rightarrow nada \,]\!].$$

(B).— Basta probar que $S.\mathcal{R}.X$ es solución de la ecuación característica de T

$$Y : [\, Y \equiv S.((b \;\Rightarrow\; Y) \wedge (\neg b \;\Rightarrow\; X)) \,]$$

$$\begin{array}{ll} & S.((b \Rightarrow S.\mathcal{R}.X) \wedge (\neg b \Rightarrow X)) \\ = & \\ & S.[\![\, b \to S; \mathcal{R} \,\square\, \neg b \to nada \,]\!].X \\ = & \quad \because \text{semántica de } \mathcal{R} \text{ según puntos fijos} \\ & S.\mathcal{R}.X \end{array}$$

$\underline{(C)}$.— Tenemos

$$\begin{array}{ll} & [S.\mathcal{R}.X \Rightarrow T.X] \\ = & \quad \because \text{semánticas inductivas de } \mathcal{R} \text{ y } T;\, T^0 \doteq aborta \\ & [S.(\exists k : k \geq 0 : H^k.X) \Rightarrow (\exists k : k \geq 0 : T^{k+1}.X)] \\ \Leftarrow & \quad \because S \text{ es continuo} \\ & \forall k : k \geq 0 : [S.H^k.X \Rightarrow T^{k+1}.X] \end{array}$$

y lo último se prueba por inducción

— Caso Base:

$$\begin{array}{ll} & T^1.X \\ = & \quad \because T^{k+1} = S; [\![\, b \to T^k \,\square\, \neg b \to nada \,]\!] \\ & S; [\![\, b \to aborta \,\square\, \neg b \to nada \,]\!].X \\ = & \quad \because \text{semántica} \\ & S.(\neg b \wedge X) \\ = & \\ & S.H^0.X \end{array}$$

– Paso Inductivo:

$$\begin{array}{ll} & [S.H^{k+1}.X \Rightarrow T^{k+2}.X] \\ = & \\ & [S.H^{k+1}.X \Rightarrow S; [\![\, b \to T^{k+1} \,\square\, \neg b \to nada \,]\!].X] \\ = & \\ & [S.H^{k+1}.X \Rightarrow S.(\neg b \wedge X \vee b \wedge T^{k+1}.X)] \\ \Leftarrow & \quad \because S \text{ es monótona} \\ & [H^{k+1}.X \Rightarrow \neg b \wedge X \vee b \wedge T^{k+1}.X] \\ = & \quad \because \text{def. de } H^i \\ & [H^0.X \vee b \wedge S.H^k.X \Rightarrow \neg b \wedge X \vee b \wedge T^{k+1}.X] \\ \Leftarrow & \quad \because \text{CP} \\ & [S.H^k.X \Rightarrow T^{k+1}.X] \end{array}$$

$\underline{(D)}$.— Trivial. La interpretación es la posibilidad de implementar un bucle *repeat* a través de un bucle *while*.

<u>9.28</u> [207] La semántica del procedimiento T en términos de puntos fijos viene dada como el menor punto fijo de cierta ecuación, que resulta ser, por el teorema de Kleene, el límite de la sucesión de transformadores

$$T^0 \doteq aborta, \qquad T^{k+1} \doteq [\![\, x > 0 \to x := x - 1; T^k \,\square\, x \leq 0 \to T^k \,]\!]$$

de donde se obtiene

$$
\begin{array}{ll}
 & T^1 \\
= & \\
 & [\![\, x > 0 \rightarrow x := x - 1; aborta \,\Box\, x \leq 0 \rightarrow aborta \,]\!] \\
= & \quad \because \text{semántica selectiva} \\
 & aborta
\end{array}
$$

y es fácil demostrar por inducción que $\forall k : k \geq 0 : T^k = aborta$. Otra prueba directa es usando los siguientes hechos: (1) $aborta$ es solución de la ecuación característica de T (ya ha sido probado), y (2) es la menor solución (trivial, ya que $aborta$ es el menor transformador de predicados).

9.29 [207] $\underline{(A)}$.— Calculemos las dos semánticas:

$$
\begin{array}{ll}
 & asig(x+1).x = y \\
= & \quad \because \text{semántica por nombre} \\
 & [i := x+1]'i :\in \mathbb{Z}' \\
\wedge & \\
 & [i := x+1][\![\, x \neq i \rightarrow x := y \,\Box\, x = i \rightarrow y := i \,]\!] .(x = y) \\
= & \quad \because \text{definición de sustitución} \\
 & x + 1 \in \mathbb{Z} \wedge [\![\, x \neq x+1 \rightarrow x := y \,\Box\, x = x+1 \rightarrow y := x+1 \,]\!] .(x = y) \\
= & \quad \because \text{semántica selectiva} \\
 & x + 1 \in \mathbb{Z} \wedge C \wedge (x \neq x+1 \;\Rightarrow\; x := y.x = y) \\
\wedge & \\
 & (x = x+1 \;\Rightarrow\; y := x+1.x = y) \\
= & \quad \because \text{CP} \\
 & x + 1 \in \mathbb{Z} \wedge C \wedge (C \;\Rightarrow\; y = y) \wedge (F \;\Rightarrow\; \ldots) \\
= & \quad \because \text{CP} \\
 & x + 1 \in \mathbb{Z}
\end{array}
$$

$$
\begin{array}{ll}
 & asig(x+1).x = y \\
= & \quad \because \text{semántica por valor – \textit{observe los paréntesis}} \\
 & [i := x+1]'i :\in \mathbb{Z}' \\
\wedge & \\
 & [i := x+1]([\![\, x \neq i \rightarrow x := y \,\Box\, x = i \rightarrow y := i \,]\!] .(x = y)) \\
= & \quad \because \text{semántica selectiva} \\
 & x + 1 \in \mathbb{Z} \\
\wedge & \\
 & [i := x+1](C \wedge (x \neq i \;\Rightarrow\; x := y.(x = y)) \wedge (x = i \;\Rightarrow\; y := i.(x = y)) \\
= & \quad \because \text{definición de sustitución} \\
 & x + 1 \in \mathbb{Z} \wedge [i := x+1]((x \neq i \;\Rightarrow\; y = y) \wedge (x = i \;\Rightarrow\; x = i)) \\
= & \quad \because \text{CP} \\
 & x + 1 \in \mathbb{Z} \wedge [i := x+1]((x \neq i \;\Rightarrow\; C) \wedge C) \\
= & \quad \because \text{CP} \\
 & x + 1 \in \mathbb{Z} \wedge [i := x+1]C \\
= & \\
 & x + 1 \in \mathbb{Z}
\end{array}
$$

Luego, si x es entera, con ambas semánticas: $\{Cierto\}asig(x+1)\{x = y\}$.

$\underline{(B)}$.— Para obtener a través de la *semántica por necesidad* alguna diferencia basta tomar expresiones con algún error, como por ejemplo $asig(1/0)$, ya que la semántica por necesidad es no estricta y obtenemos, *ptle*

$$asig(1/0).(x = y) \overset{\text{s.p.necesidad}}{\equiv} Cierto, \qquad asig(1/0).(x = y) \overset{\text{s.p.valor}}{\equiv} Falso.$$

9.30 [207] Ver Ejercicio 9.25.

9.31 [207] Véase Ejemplo 9.11.

9.32 [208] (A).— En primer lugar, para cualquier predicado Z, la semántica del procedimiento para una llamada (estricta) por nombre es, *ptle*

$$f(y,a,u).Z \equiv y,a,u \in \mathbb{N} \wedge (y > 0 \wedge f(y-1, xa, u).Z \vee y \leq 0 \wedge u := a.Z) \quad (*)$$

Probaremos por inducción sobre y que se tiene $\forall y : y \in \mathbb{N} : \mathcal{V}(y)$, donde

$$\mathcal{V}(y) \doteq \forall a, x : a, x \in \mathbb{N} : [f(y,a,u).(u = ax^y)]$$

— CASO BASE; para $y = 0$,

$$\begin{array}{ll} & [f(0,a,u).(u = a)] \\ = & \quad \because (*) \\ & [u := a.(u = a)] \\ = & \quad \because \text{semántica asignación} \\ & Cierto \end{array}$$

— PASO INDUCTIVO; supongamos $y > 0$,

$$\begin{array}{ll} & [f(y,a,u).(u = ax^y)] \\ = & \quad \because y > 0, (*) \\ & [f(y-1, xa, u).(u = ax^y)] \\ = & \quad \because \text{tomando } xa = x' \\ & [f(y-1, x', u).(u = ax'x^{y-1})] \\ = & \quad \because \text{HI} \\ & Cierto \end{array}$$

(B).— Bastará probar, $\{a = 1\} f(p,a,u) \{u = x^p\}$. Pero,

$$\begin{array}{ll} & a = 1 \wedge f(p,a,u).(u = x^p) \\ = & \quad \because \text{Ver siguiente ecuación } (**) \\ & a = 1 \wedge f(p,a,u).(a = 1 \wedge u = x^p) \\ = & \quad \because \text{por } (*) \\ & Cierto \end{array}$$

y bastará demostrar que una llamada al procedimiento no cambia el valor de la variable a; es decir, que se tiene

$$\forall y : y \in \mathbb{N} : (\ \forall a, x : a, x \in \mathbb{N} : [a = a_0 \ \Rightarrow \ f(y,a,u).(a = a_0)]\ ) \qquad (**)$$

que se demuestra por inducción sobre y. La demostración es parecida. Por la regla de oro, bastará demostrar el siguiente predicado equivalente:

$$[a = a_0 \wedge f(y,a,u).(a = a_0) \ \equiv \ a = a_0]$$

— CASO BASE; para $y = 0$, y *ptle*

$$\begin{array}{ll} & a = a_0 \wedge f(0,a,u).(a = a_0) \\ = & \quad \because (*) \\ & a = a_0 \wedge u := a.(a = a_0) \\ = & \quad \because u \not\equiv a \\ & a = a_0 \end{array}$$

— PASO INDUCTIVO; si $y > 0$, *ptle*

$$\begin{array}{ll} & a = a_0 \wedge f(y,a,u).(a = a_0) \\ = & \quad \because y > 0, (*) \\ & a = a_0 \wedge f(y-1, xa, u).(a = a_0) \\ = & \quad \because \text{HI} \\ & a = a_0 \end{array}$$

9.34 [208] Estudiando el comportamiento de m para los valores $0, 1, \ldots$ intuimos que realiza las asignaciones $i := -1, i := -2, \ldots$. Probaremos pues, por inducción sobre a,

$$\forall a : a \geq 0 : [\ (i = a \wedge m.Z) \equiv (i = a \wedge i := -a - 1.Z)\ ] \qquad (*)$$

El caso base sería, *ptle*

$i = 0 \wedge m.Z$
$=$ $\because$ semántica en términos de PF
$i = 0 \wedge i := i - 1.m.i := i - 1.Z$
$=$
$i := i - 1.(i = -1 \wedge m.i := i - 1.Z)$
$=$ $\because$ semántica PF
$i := i - 1.(i = -1 \wedge i := i + 1.i := i - 1.Z)$
$=$ $\because$ lema de sustitución – Lema 4.7(i)
$i = 0 \wedge i := i - 1.Z$

El paso inductivo es parecido. Tenemos, *ptle*, si $a > 0$,

$i = a \wedge m.Z$
$=$ $\because a > 0$, semántica en términos de PF
$i = a \wedge i := i - 1.m.i := i - 1.Z$
$=$ $\because$ sustitución
$i := i - 1.(i = a - 1 \wedge m.i := i - 1.Z)$
$=$ $\because$ HI
$i := i - 1.(i = a - 1 \wedge i := -(a - 1).i := i - 1.Z)$
$=$ $\because$ lema de sustitución – Lema 4.7(i)
$i = a \wedge i := -a - 1.Z$

Por tanto,

$\{i = 100\}m\{i = -101\}$
$=$ $\because$ definición de triplete
$[i = 100 \;\Rightarrow\; m.(i = -101)]$
$=$ $\because$ regla de oro
$[i = 100 \equiv i = 100 \wedge m.(i = -101)]$
$=$ $\because$ por $(*)$, tomando $Z == (i = -101)$
$[i = 100 \equiv i = 100 \wedge i := -i - 1.(i = -101)]$
$=$ $\because$ CP
$[i = 100 \equiv i = 100 \wedge \; -i - 1 = -101]$
$=$ $\because$ CP
$Cierto$

9.35 [208] (A).— Para calcular el primer triplete calcularemos, *ptle*:

$x = a > 0 \wedge Azar_{x012}.(0 \leq x < a)$
$=$ $\because$ semántica selectiva, y asignaciones
$x = a > 0 \wedge x > 0 \wedge (x > 0 \;\Rightarrow\; 0 < a) \wedge (x > 1 \;\Rightarrow\; 1 < a)$
$\wedge$
$(x > 2 \;\Rightarrow\; 2 < a)$
$=$ $\because$ CP, sustitutividad de $x = a$
$x = a > 0 \wedge x > 0 \wedge (a > 0 \;\Rightarrow\; 0 < a) \wedge (a > 1 \;\Rightarrow\; 1 < a)$
$\wedge$
$(a > 2 \;\Rightarrow\; 2 < a)$
$=$ $\because$ CP
$x = a > 0$

De aquí obtenemos $[x = a > 0 \;\Rightarrow\; Azar_{x012}.(x < a)]$, y el primer triplete es Cierto. Para el segundo calcularemos antes:

$x > 1 \wedge Azar_{x012}.(x = q)$
$=$ $\because$ semántica selectiva, y asignaciones

$\quad x > 1 \wedge x > 0 \wedge (x > 0 \;\Rightarrow\; 0 = q) \wedge (x > 1 \;\Rightarrow\; 1 = q)$
$\wedge\; (x > 2 \;\Rightarrow\; 2 = q)$
$=\qquad \because$ CP
$\quad x > 1 \wedge x > 0 \wedge 0 = q \wedge 1 = q \wedge \ldots$
$=\qquad \because$ CP
$\quad Falso$

y obtenemos que el segundo triplete es Falso, ya que

$\quad \{x > 1\} Azar_{x012} \{x = q\}$
$=\qquad \because$ definición de triplete
$\quad [x > 1 \;\Rightarrow\; Azar_{x012}.(x = q)]$
$=\qquad \because$ regla de oro
$\quad [x > 1 \wedge Azar_{x012}.(x = q) \equiv x > 1]$
$=\qquad \because$ por lo anterior
$\quad [Falso \equiv x > 1]$
$=\qquad \because$ CP
$\quad [x \leq 1]$
$=\qquad \because x$ es entera
$\quad Falso$

(B).— Es fácil obtener $[Azar_{x012}.(x \leq 0) \equiv Falso]$, y de aquí que el predicado $x \leq 0$ sea la menor solución de la ecuación:

$$Y : [\, Y \equiv x \leq 0 \vee x > 0 \wedge Azar_{x012}.Y \,]$$

que caracteriza a la semántica de $\mathcal{R}.Cierto$ en términos de puntos fijos (TPF). Por tanto, $[\mathcal{R}.C \equiv x \leq 0]$. Es decir, no podemos garantizar la terminación del bucle si el estado inicial es $x > 0$; sin embargo garantizamos la terminación en los restantes casos. Esto no es sorprendente y es válido para cualquier bucle $*[\![\, b \rightarrow S \,]\!]$ con $[S.\neg b \equiv Falso]$ (véase el Ejercicio 8.14).

(C).— Calculemos el comportamiento de m para $3 < x \leq 5$:

$\quad 3 < x \leq 5 \wedge m.Q$
$=\qquad \because$ semántica en TPF
$\quad 3 < x \leq 5 \wedge x := x - 2.m.x := x + 2.Q$
$=\qquad \because$ sustitución
$\quad x := x - 2.(1 < x \leq 3 \wedge m.x := x + 2.Q)$
$=\qquad \because$ semántica en TPF
$\quad x := x - 2.(1 < x \leq 3 \wedge Azar_{x012}.x := x + 2.Q)$
$=\qquad \because$ CP
$\quad 3 < x \leq 5 \wedge [\![\, x > 2 \rightarrow x := 2 \,\square\, x > 3 \rightarrow x := 3 \,\square\, x > 4 \rightarrow x := 4 \,]\!] .Q$

Veamos ahora el comportamiento para $5 < x \leq 7$:

$\quad 5 < x \leq 7 \wedge m.Q$
$=\qquad \because$ semántica en TPF
$\quad 5 < x \leq 7 \wedge x := x - 2.m.x := x + 2.Q$
$=\qquad \because$ sustitución
$\quad x := x - 2.(3 < x \leq 5 \wedge m.x := x + 2.Q)$
$=\qquad \because$ por lo anterior

$$
\begin{array}{ll}
& x := x - 2.(3 < x \leq 5 \wedge \\
& [\![\, x > 2 \rightarrow x := 2 \,\square\, x > 3 \rightarrow x := 3 \,\square\, x > 4 \rightarrow x := 4 \,]\!] . \\
& x := x + 2.Q) \\
= & \quad \because \text{CP} \\
& 5 < x \leq 7 \wedge [\![\, x > 4 \rightarrow x := 4 \,\square\, x > 5 \rightarrow x := 5 \,\square\, x > 6 \rightarrow x := 6 \,]\!] .Q
\end{array}
$$

Es fácil entonces probar por inducción sobre k, que

$$\forall k : k \leq 0 : [\, 2k+1 < x \leq 2k+3 \wedge m.Q \equiv \; 2k+1 < x \leq 2k+3 \wedge Azar_k.Q \,]$$

donde

$$
\begin{array}{rcllll}
Azar_k & \doteq & [\![& x > 2k & \rightarrow x := 2k \\
& & \square & x > 2k+1 & \rightarrow x := 2k+1 \\
& & \square & x > 2k+2 & \rightarrow x := 2k+2 \,]\!]
\end{array}
$$

10.12 [218] Recordemos la definición de equivalencia:

$$U =_{\mathcal{N}} V \qquad \doteq \qquad \forall \rho, \rho' :: (\rho, U) \twoheadrightarrow_{\mathcal{N}} \rho' \Longleftrightarrow (\rho, V) \twoheadrightarrow_{\mathcal{N}} \rho' \qquad (*)$$

Ya que la relación $=_{\mathcal{N}}$ es de equivalencia, es transitiva, y (A) sigue de

$$
\begin{array}{ll}
(A_1) & nada; S =_{\mathcal{N}} S \\
(A_2) & S =_{\mathcal{N}} S; nada
\end{array}
$$

y tendremos directamente también (B). Veamos (A_1); tenemos

$$
\begin{array}{ll}
& (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
= & \quad \because \text{regla } (nada) \\
& (\rho, nada) \twoheadrightarrow_{\mathcal{N}} \rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{regla } (;) \\
& (\rho, nada; S) \twoheadrightarrow_{\mathcal{N}} \rho'
\end{array}
$$

que es la primera implicación de $(*)$. Probemos la segunda implicación,

$$
\begin{array}{ll}
& (\rho, nada; S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{ya que } (;) \text{ es la única regla aplicable, para cierto } \rho'' \\
& (\rho, nada) \twoheadrightarrow_{\mathcal{N}} \rho'' \wedge (\rho'', S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \twoheadrightarrow_{\mathcal{N}} \text{ es determinista y } (\rho, nada) \twoheadrightarrow_{\mathcal{N}} \rho, \text{ de donde } \rho = \rho'' \\
& (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'
\end{array}
$$

(A_2) se demuestra de la misma forma.

10.13 [218] Sean $\mathcal{R} \doteq * [\![\, b \rightarrow S \,]\!]$ y $SI \doteq [\![\, b \rightarrow S; \mathcal{R} \,\square\, nada \,]\!]$. Hay que demostrar, $\forall \rho, \rho'$, la doble implicación siguiente

$$(\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \Longleftrightarrow (\rho, SI) \twoheadrightarrow_{\mathcal{N}} \rho'$$

Demostremos la implicación $\Rightarrow$ por inducción estructural sobre la derivación $(\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho'$; las únicas reglas aplicables son las que tienen como antecedentes

$$
\begin{array}{ll}
& \vee \begin{array}{l} b.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'' \wedge (\rho'', \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \\ \neg b.\rho \wedge (\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho \wedge \rho' \equiv \rho \end{array} \\
\Rightarrow & \quad \because \text{reglas } (;) \text{ y } (si) \\
& b.\rho \wedge (\rho, S; \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \vee \neg b.\rho \wedge (\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{regla } (si)
\end{array}
$$

$(\rho, SI) \twoheadrightarrow_{\mathcal{N}} \rho'$

La otra implicación se prueba de forma similar.

10.14 [218] Basta probar que es imposible una derivación de la forma

$(\rho, aborta; S) \twoheadrightarrow_{\mathcal{N}} \rho'$
$\Rightarrow$ $\because$ ya que $(;)$ es la única regla aplicable, para cierto ρ''
$(\rho, aborta) \twoheadrightarrow_{\mathcal{N}} \rho'' \wedge (\rho'', S) \twoheadrightarrow_{\mathcal{N}} \rho'$
$\Rightarrow$
absurdo: no existe ninguna regla con consecuente $(\rho, aborta) \twoheadrightarrow_{\mathcal{N}} \rho''$

10.15 [218] Podemos definirla directamente

$$repite\ S\ hasta\ b \doteq S; *[\![\neg b \rightarrow S]\!]$$

o alternativamente a través de las dos reglas:

$$\frac{(\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' \qquad b.\rho'}{(\rho, repite\ S\ hasta\ b) \twoheadrightarrow_{\mathcal{N}} \rho'}$$

$$\frac{(\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' \qquad \neg b.\rho' \qquad (\rho', repite\ S\ hasta\ b) \twoheadrightarrow_{\mathcal{N}} \rho''}{(\rho, repite\ S\ hasta\ b) \twoheadrightarrow_{\mathcal{N}} \rho''}$$

Ya que la aplicación de las reglas anteriores son excluyentes, el lenguaje resultante sigue siendo determinista. Otra alternativa vía una única regla es:

$$\frac{(\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'' \qquad (\rho'', *[\![\neg b \rightarrow S]\!]) \twoheadrightarrow_{\mathcal{N}} \rho'}{(\rho, repite\ S\ hasta\ b) \twoheadrightarrow_{\mathcal{N}} \rho'}$$

y para demostrar que el lenguaje obtenido es determinista basta razonar por inducción estructural sobre la sentencia.

10.16 [218] Hay que probar

$$\forall \rho, \rho' :: (\rho, S; (T; U)) \twoheadrightarrow_{\mathcal{N}} \rho' \Longleftrightarrow (\rho, (S; T); U) \twoheadrightarrow_{\mathcal{N}} \rho'$$

Cada implicación sigue por inducción estructural sobre la derivación. Por ejemplo, para la implicación $\Rightarrow$ razonamos en la forma siguiente

$(\rho, S; (T; U)) \twoheadrightarrow_{\mathcal{N}} \rho'$
$=$ $\because$ la única regla aplicable es $(;)$, para cierto ρ''
$(\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'' \wedge (\rho'', T; U) \twoheadrightarrow_{\mathcal{N}} \rho'$
$=$ $\because$ la única regla aplicable es $(;)$, para cierto ρ'''
$(\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'' \wedge (\rho'', T) \twoheadrightarrow_{\mathcal{N}} \rho''' \wedge (\rho''', U) \twoheadrightarrow_{\mathcal{N}} \rho'$
$=$ $\because$ regla $(;)$
$(\rho, S; T) \twoheadrightarrow_{\mathcal{N}} \rho''' \wedge (\rho''', U) \twoheadrightarrow_{\mathcal{N}} \rho'$
$=$ $\because$ regla $(;)$
$(\rho, (S; T); U) \twoheadrightarrow_{\mathcal{N}} \rho'$

10.17 [218] Tomemos $S == x := 0$ y $T == y := x$; entonces desde el entorno $\rho_{1,1}$ las únicas transiciones posibles son:

$$(\rho_{1,1}, x := 0; y := x) \twoheadrightarrow_{\mathcal{N}} \rho_{0,1} \qquad (\rho_{1,1}, y := x; x := 0) \twoheadrightarrow_{\mathcal{N}} \rho_{0,0}$$

Ya que los entornos finales son distintos, $S; T \neq_{\mathcal{N}} T; S$.

<u>10.22</u> [221]

$$
\begin{array}{ll}
& b.\rho \wedge (\forall i : i \geq 0 : f^i.\rho) \;\Rightarrow\; b.\rho \wedge wlp.\mathcal{R}.Q.\rho \\
= & \\
& b.\rho \wedge (\forall i : i \geq 0 : f^i.\rho) \;\Rightarrow\; b.\rho \wedge (\forall \rho' : (\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho') \\
= & \\
& \forall \rho' : b.\rho \wedge (\forall i : i \geq 0 : f^i.\rho) \wedge (\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho' \\
= & \\
& \ldots
\end{array}
$$

En definitiva tenemos $[(\forall i : i \geq 0 : f^i.\rho) \equiv wlp.\mathcal{R}.Q.\rho]$, de donde $\mathcal{R}$ es definible.

<u>10.28</u> [226] Veamos la segunda

$$
\begin{array}{ll}
& \vdash_{\mathcal{O}} \{P\}S\{Q\} \\
= & \quad \because \text{definición} \\
& \forall \rho, \rho' : P.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho' \\
= & \quad \because \text{CP} \\
& \forall \rho' : (\exists \rho : P.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho') : Q.\rho' \\
= & \quad \because \text{definición} \\
& \forall \rho' : sp.S.P.\rho' : Q.\rho' \\
= & \\
& [sp.S.P \;\Rightarrow\; Q]
\end{array}
$$

Tenemos, por ejemplo,

$$
\begin{array}{ll}
& sp.nada.P.\rho' \\
= & \quad \because \text{definición} \\
& \exists \rho : (\rho, nada) \twoheadrightarrow_{\mathcal{N}} \rho' : P.\rho \\
= & \\
& P.\rho'
\end{array}
$$

<u>10.29</u> [226] Véase Ejercicio 10.34.

<u>10.30</u> [226] <u>(A)</u>.— Si consideremos las reglas de la Figura 5.0 eliminado las reglas de la selectiva y sustituyéndolas por la regla

$$
\frac{\{b \wedge X\}S\{Y\} \qquad \{b' \wedge X\}S'\{Y\}}{\{X\}[\![\, b \to S \,\square\, b' \to S' \,]\!]\,\{Y\}}\,(si)
$$

podemos tomar como reglas de la semántica operacional para la selectiva:

$$
\frac{b.\rho \qquad (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'}{(\rho, [\![\, b \to S \,\square\, b' \to S' \,]\!]\,) \twoheadrightarrow_{\mathcal{N}} \rho'}\,(si_1) \qquad \frac{b'.\rho \qquad (\rho, S') \twoheadrightarrow_{\mathcal{N}} \rho'}{(\rho, [\![\, b \to S \,\square\, b' \to S' \,]\!]\,) \twoheadrightarrow_{\mathcal{N}} \rho'}\,(si_2)
$$

NOTA 12.1 *Si en la regla de la selectiva añadimos el predicado* $[X \;\Rightarrow\; b \vee b']$

$$
\frac{[X \;\Rightarrow\; b \vee b'] \qquad \{b \wedge X\}S\{Y\} \qquad \{b' \wedge X\}S'\{Y\}}{\{X\}[\![\, b \to S \,\square\, b' \to S' \,]\!]\,\{Y\}}\,(si') \qquad (*)
$$

entonces el sistema es correcto para la semántica de Dijkstra y captura corrección total *(véase Ejercicio 5.24), pero entonces el cálculo de Hoare no será completo para la semántica operacional. Así, después veremos que para la selectiva*

$$
SI \;\doteq\; [\![\, x > 2 \to x := x + 1 \,\square\, x > 2 \to x := x + 1 \,]\!]
$$

se verifica $[wlp.SI.(x > 0) \equiv Cierto]$, *de donde se cumple también* $\vdash_{\mathcal{O}} \{P\}SI\{x > 0\}$, *para cualquier* P. *Sin embargo, con la nueva regla* $(*)$ *no es posible inferir, para* *cualquier P, el triplete $\vdash_{\mathcal{H}} \{P\}SI\{x > 0\}$. En efecto, por el Ejercicio 5.36, sabemos que, con la nueva regla se verifica:*

$$\vdash_{\mathcal{H}} \{P\}SI\{Q\} \quad \Rightarrow \quad [P \Rightarrow b \vee b']$$

pero es obvio que $[P \Rightarrow b \vee b']$ en nuestro caso es $[P \Rightarrow x > 0]$, y puede fallar.

$\underline{(B)}$.— Si el álgebra es expresiva, todas las sentencias son definibles y tenemos $\vdash_{\mathcal{O}} \{P\}S\{Q\} \equiv [P \Rightarrow wlp.S.Q]$, donde $wlpS.Q.\rho \equiv \forall\rho' : (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho'$. La prueba de esto último es similar a la prueba del Lema 10.21 salvo el caso de la selectiva. Calculemos pues $wlp.[\![\, b \to S \,\square\, b' \to S' \,]\!] .Q$, para las nuevas reglas indeterministas:

$$
\begin{array}{ll}
 & wlp.[\![\, b \to S \,\square\, b' \to S' \,]\!] .Q.\rho \\
= & \quad \because \text{definición} \\
 & \forall\rho' : (\rho, [\![\, b \to S \,\square\, b' \to S' \,]\!]\,) \twoheadrightarrow_{\mathcal{N}} t : Q.\rho' \\
= & \quad \because \text{reglas de la selectiva} \\
 & (b \vee b').\rho \wedge \forall\rho' : b.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' \vee b'.\rho \wedge (\rho, S') \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho' \\
= & \quad \because \text{CP} \\
 & (b \vee b').\rho \wedge (b.\rho \Rightarrow \forall\rho' : (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho') \\
 & \wedge\ (b'.\rho \Rightarrow \forall\rho' : (\rho, S') \twoheadrightarrow_{\mathcal{N}} \rho' : Q.\rho') \\
= & \quad \because \text{definición de } wlp \\
 & (b \Rightarrow wlp.S.Q).\rho \wedge (b' \Rightarrow wlp.S'.Q).\rho
\end{array}
$$

de donde, finalmente:

$$wlp.[\![\, b \to S \,\square\, b' \to S' \,]\!]\,).Q \equiv (b \Rightarrow wlp.S.Q) \wedge (b' \Rightarrow wlp.S'.Q)$$

Para probar que el cálculo de Hoare con la regla nueva es completo tenemos que demostrar

$$\vdash_{\mathcal{O}} \{P\}S\{Q\} \qquad \Rightarrow \qquad \vdash_{\mathcal{H}} \{P\}S\{Q\}$$

Utilizando la regla de refinamiento, basta demostrar, por inducción sobre la sentencia: $\forall S, Q :: \vdash_{\mathcal{H}} \{wlpS.Q\}S\{Q\}$; todos los pasos se prueban como en la prueba del Teorema 10.26, salvo el paso inductivo para la nueva selectiva; por HI tenemos, siendo $Z \doteq wlp[\![\, b \to S \,\square\, b' \to S' \,]\!] .Q$:

$$
\begin{array}{ll}
 & \vdash_{\mathcal{H}} \{wlpS.Q\}S\{Q\} \wedge \{wlp.S'.Q\}S'\{Q\} \\
\Rightarrow & \quad \because \text{refinamiento, } [b \wedge Z \Rightarrow b \wedge wlp.S.Q], [b' \wedge Z \Rightarrow b' \wedge wlp.S'.Q] \\
 & \vdash_{\mathcal{H}} \{b \wedge Z\}S\{Q\} \wedge \vdash_{\mathcal{H}} \{b' \wedge Z\}S'\{Q\} \\
\Rightarrow & \quad \because \text{regla de la selectiva} \\
 & \vdash_{\mathcal{H}} \{Z\}[\![\, b \to S \,\square\, b' \to S' \,]\!]\, \{Q\}
\end{array}
$$

$\underline{(C)}$.— Ya que $aborta; S =_{\mathcal{N}} aborta$ equivale a

$$\forall\rho, \rho' : (\rho, aborta; S) \twoheadrightarrow_{\mathcal{N}} \rho' \Longleftrightarrow (\rho, aborta) \twoheadrightarrow_{\mathcal{N}} \rho'$$

bastará probar que es imposible cualquiera de las transiciones; la segunda no puede darse, ya que $(\rho, [\![\, F \to S \,\square\, F \to S \,]\!]\,) \twoheadrightarrow_{\mathcal{N}} \rho'$ no puede derivarse al no poderse aplicar ninguna regla de la selectiva; la primera tampoco puede darse, porque ello exige, según la regla de la composición, que $(\rho, aborta) \twoheadrightarrow_{\mathcal{N}} \rho''$.

<u>10.31</u> [227] $\underline{(A)}$.— Véase la prueba del Teorema 10.8.

$\underline{(B)}$.— Podemos ampliar la relación $\twoheadrightarrow_{\mathcal{N}}$ con las reglas

$$\frac{b.\rho \qquad (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho'}{(\rho, [\![\, b \rightarrow S \,\Box\, b' \rightarrow S' \,]\!]) \twoheadrightarrow_{\mathcal{N}} \rho'} (si_1) \qquad \frac{b'.\rho \qquad (\rho, S') \twoheadrightarrow_{\mathcal{N}} \rho'}{(\rho, [\![\, b \rightarrow S \,\Box\, b' \rightarrow S' \,]\!]) \twoheadrightarrow_{\mathcal{N}} \rho'} (si_2)$$

$\underline{(C_1)}$.— es cierta; demostremos solamente una de las implicaciones

$$\begin{array}{ll}
& (\rho, [\![\, a \rightarrow A \,\Box\, b \rightarrow B \,]\!]\,; S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{regla para } (;), \text{ para cierto } \alpha \\
& (\rho, [\![\, a \rightarrow A \,\Box\, b \rightarrow B \,]\!]) \twoheadrightarrow_{\mathcal{N}} \alpha \wedge (\alpha, S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{distinguimos los dos casos, por las reglas de } (SI) \\
\vee & a.\rho \wedge (\rho, A) \twoheadrightarrow_{\mathcal{N}} \alpha \wedge (\alpha, S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
& b.\rho \wedge (\rho, B) \twoheadrightarrow_{\mathcal{N}} \alpha \wedge (\alpha, S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{reglas de } (;) \\
& a.\rho \wedge (\rho, A; S) \twoheadrightarrow_{\mathcal{N}} \rho' \vee b.\rho \wedge (\rho, B; S) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{regla de } (SI) \\
& (\rho, [\![\, a \rightarrow A; S \,\Box\, b \rightarrow B; S \,]\!]) \twoheadrightarrow_{\mathcal{N}} \rho'
\end{array}$$

$\underline{(C_2)}$.— es falsa y basta encontrar un contraejemplo; tenemos ($F == Falso$),

$$\begin{array}{ll}
& a := F; [\![\, a \rightarrow x := x \,\Box\, a \rightarrow x := x \,]\!] \\
\not\models_{\mathcal{N}} & \\
& [\![\, a \rightarrow a := F; x := x \,\Box\, a \rightarrow a := F; x := x \,]\!]
\end{array}$$

ya que para el entorno $\rho == \{a \rightarrow Cierto\}$ tenemos

$$(\rho, [\![\, a \rightarrow a := F; x := x \,\Box\, a \rightarrow a := F; x := x \,]\!]) \twoheadrightarrow_{\mathcal{N}} \rho\{a := Falso\}$$

pero al ser las dos guardas falsas después de $a := F$, es imposible

$$(\rho, a := F; [\![\, a \rightarrow x := x \,\Box\, a \rightarrow x := x \,]\!]) \twoheadrightarrow_{\mathcal{N}} \rho'$$

10.32 [227] $\underline{(A)}$.— Véase la Figura 10.4.

$\underline{(B)}$.— Probaremos que para todo bucle $\mathcal{R} \doteq * [\![\, b \rightarrow S \,]\!]$ se verifica

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

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

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

Si hubiera sido obtenida por la segunda es trivial ya que $\rho \equiv \rho'$. Si hubiera sido obtenida de la primera regla, tendríamos, para cierto τ:

$$\begin{array}{ll}
& b.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \tau \wedge (\tau, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \\
& I.\tau \wedge (\tau, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \\
\Rightarrow & \quad \because \text{HI}
\end{array}$$

$(\neg b.\rho'$

La equivalencia $*[\![\, Cierto \to x := x+1 \,]\!] =_{\mathcal{N}} aborta$ es trivial ya que es imposible ninguna transición $(\rho, *[\![\, Cierto \to x := x+1 \,]\!]\,) \twoheadrightarrow_{\mathcal{N}} \rho'$, ya que ésta verificaría $C.\rho' \equiv Falso$.

10.33 [227] $\underline{(A)}$.— Véase Ejercicio 10.32.

$\underline{(B)}$.— Se define

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

y aplicando el apartado (A) llegamos trivialmente a $\vdash_{\mathcal{O}} \{X\}\mathcal{R}\{\neg b\}$.

10.34 [227] $\underline{(A)}$.— $\vdash_{\mathcal{O}} \{X\}S\{Y\} \doteq \forall \rho, \rho' : X.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \rho' : Y.\rho'$.

$\underline{(B)}$.— Un predicado I es un invariante del bucle $\mathcal{R}$ si verifica $\vdash_{\mathcal{O}} \{I \wedge b\}S\{I\}$.

$\underline{(C)}$.— 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

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

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

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

Si hubiera sido obtenida por la segunda, tendríamos:

$$I.\rho \wedge \neg b.\rho \wedge \rho \equiv \rho' \;\Rightarrow\; (I \wedge \neg b).\rho$$

que es lo buscado. Si hubiera sido obtenida de la primera regla, tendríamos:

$$\begin{array}{ll} & I.\rho \wedge b.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \tau \wedge (\tau, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \\ \Rightarrow & \quad \because \text{por ser } I \text{ invariante, } (I.\rho \wedge b.\rho \wedge (\rho, S) \twoheadrightarrow_{\mathcal{N}} \tau) \;\Rightarrow\; I.\tau \\ & I.\tau \wedge (\tau, \mathcal{R}) \twoheadrightarrow_{\mathcal{N}} \rho' \\ \Rightarrow & \quad \because \text{HI} \\ & (I \wedge \neg b).\rho' \end{array}$$

10.43 [232] $\underline{(A)}$.— $nada; S =_{\mathcal{P}} S \;\doteq\; \forall \rho, \rho' : (\rho, nada; S) \twoheadrightarrow_{\mathcal{P}} \rho' \Longleftrightarrow (\rho, S) \twoheadrightarrow_{\mathcal{P}} \rho'$, y probamos una de las dos implicaciones:

$$\begin{array}{ll} & (\rho, nada; S) \twoheadrightarrow_{\mathcal{P}} \rho' \\ = & \quad \because \text{definición de } \twoheadrightarrow_{\mathcal{P}} \\ & \exists k : k \geq 1 : (\rho, nada; S) \to_{\mathcal{P}}^{k} \rho' \\ \Rightarrow & \quad \because \text{Lema 10.39, para cierto } p \text{ y cierto } \rho'' \\ & (\rho, nada) \to_{\mathcal{P}}^{p} \rho'' \wedge (\rho'', S) \to_{\mathcal{P}}^{k-p} \rho' \\ \Rightarrow & \quad \because \text{por la regla } (nada)\text{, debe tenerse } p = 1 \text{ y } \rho \equiv \rho'' \\ & (\rho, S) \to_{\mathcal{P}}^{k-p} \rho' \\ \Rightarrow & \quad \because \text{definición de } \twoheadrightarrow_{\mathcal{P}} \\ & (\rho, S) \twoheadrightarrow_{\mathcal{P}} \rho'. \end{array}$$

$\underline{(D)}$.— Pongamos $\mathcal{R} \doteq * [\![b \to S]\!]$ y $SI \doteq [\![b \to S; \mathcal{R} \,\Box\, nada]\!]$. Hay que probar, $\forall \rho, \rho'$, la doble implicación $(\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{P}} \rho' \Longleftrightarrow (\rho, SI) \twoheadrightarrow_{\mathcal{P}} \rho'$. Veamos $\Rightarrow$. Si $(\rho, \mathcal{R}) \twoheadrightarrow_{\mathcal{P}} \rho'$, para cierto k $(\rho, \mathcal{R}) \to^{k}_{\mathcal{P}} \rho'$; pero ya que existe una sola regla aplicable al bucle, tendremos $(\rho, \mathcal{R}) \to_{\mathcal{P}} (\rho, SI) \to^{k-1}_{\mathcal{P}} \rho'$.

<u>11.6</u> [254] [1]. $\mathcal{S}[\![* \langle\!\langle\, Cierto \to S \,\rangle\!\rangle]\!]$ es el mínimo punto fijo de la funcional BUC

$$\lambda F \to \lambda \rho \to \langle \mathcal{V}[\![Cierto \to S]\!]\,\rho \to (F \oplus \mathcal{S}[\![Cierto \to S]\!])\rho \,\Box\, \{\rho\} \rangle$$

y $aborta$ es la menor función del espacio $[\mathcal{E} \to \mathcal{R}]$; basta probar que $aborta$ es un punto fijo de la funcional anterior.

$$\begin{array}{ll}
 & BUC\ aborta \\
= & \\
 & \lambda \rho \to \langle \mathcal{V}[\![Cierto \to S]\!]\,\rho \to (aborta \oplus \mathcal{S}[\![Cierto \to S]\!])\rho \,\Box\, \{\rho\} \rangle \\
= & \quad \because \text{definición } \langle\rangle \\
 & \lambda \rho \to (aborta \oplus \mathcal{S}[\![Cierto \to S]\!])\rho \\
= & \quad \because (aborta \oplus g)\rho = (aborta_{\{\bot\}})^{+}(g.\rho) = \{\bot\} \\
 & \lambda \rho \to \{\bot\} \\
= & \quad \because \text{definición de } aborta \\
 & aborta.
\end{array}$$

[1] Hemos cambiado de nuevo los corchetes usuales de la selectiva por los paréntesis angulares para que no exista confusión con los utilizados para denotar la semántica denotacional.

Bibliografía

[Alagic y Arbib, 1978] Alagic, S. y Arbib, M. (1978). *The Design of Well-Structured and Correct Programs*. Springer-Verlag, New-York.

[ANSI-83, 1983] ANSI-83 (1983). Reference Manual for the Ada Programming Language. U.S. Government (Ada Joint Program Office). Reimpreso en [Horowitz, 1983].

[Apt, 1988] Apt, K. R. (1988). Proving Correctness of Concurrent Programs: A Quick Introduction. En Börger, E. (ed.), *Trends in Theoretical Computer Science*, pp. 305–345. Computer Science Press.

[Arsac, 1985] Arsac, J. (1985). Teaching Programming. En Griffiths, M. y Tagg, E. (eds.), *The role of programming in teaching Informatics. Proc. IFIP, TC3, Working Conference on Teaching Programming, París, 7–9 mayo'84*, pp. 3–6. Elsevier Science Pbl., Amsterdam.

[Babbage, 1864] Babbage, C. (1864). De la Máquina Analítica. En *Perspectives on Computer Revolution*. Prentice-Hall, New Jersey. Traducción al castellano, Alianza, Madrid (1975) de la del inglés (1970).

[Barendregt, 1984] Barendregt, H. P. (1984). *The Lambda Calculus, Its Syntax and Semantics*, volumen 103 de *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam. Edición revisada de la primera (1981).

[Berg y o., 1982] Berg, H. y o. (1982). *Formal Methods of Program Verification and Specification*. Prentice-Hall, New Jersey.

[Bird y Wadler, 1988] Bird, R. y Wadler, P. (1988). *Introduction to Functional Programming*. Pretice–Hall.

[Cauchy, 1821] Cauchy, A. L. (1821). Cours d'analyse. En *Oeuvres Complétes (II^e Série)*, volumen 3. École Royale Polytechnique. Reeditado en forma facsimilar por SAEM Thales (1999).

[Dijkstra, 1981] Dijkstra, E. (1981). Why correctness must be a mathematical concern. En Boyer, R. y Moore, J. S. (eds.), *The correctness problem in computer science*. Academic Press, London.

[Dijkstra, 1982] Dijkstra, E. (1982). The equivalence of bounded nondeterminacy and continuity. En Dijkstra, E. (ed.), *Selected Writings on Computing: A personal Perspective*, pp. 358–359. Springer-Verlag.

[Dijkstra, 1990] Dijkstra, E. (ed.) (1990). *Formal Development of Programs and Proofs*. Addison-Wesley. The Year of Programming.

[Dijkstra y Feijen, 1984] Dijkstra, E. y Feijen, W. (1984). *Een methode van programmeren*. The Hague: Academic Service. traducido al inglés en [Dijkstra y Feijen, 1988].

[Dijkstra, 1976] Dijkstra, E. W. (1976). *A Discipline of Programming*. Prentice-Hall.

[Dijkstra y Feijen, 1988] Dijkstra, E. W. y Feijen, W. (1988). *A Method of Programming*. Addison-Wesley, Massachusetts.

[Dijkstra y Scholten, 1990] Dijkstra, E. W. y Scholten, C. S. (1990). *Predicate Calculus and Program Semantics*. Springer-Verlag, New York.

[Field y Harrison, 1988] Field, A. y Harrison, P. (1988). *Functional Programming*. Addison-Wesley.

[Floyd, 1967] Floyd, R. W. (1967). Assigning Meanings to Programs. En Schwartz, J. T. (ed.), *Mathematical Aspects of Computer Science*, volumen 19 de *Symposia in Applied Mathematics*, pp. 19–32. American Mathematical Society, Providence, RI.

[Gehani y McGettrick, 1988] Gehani, N. y McGettrick, A. (1988). *Concurrent Programming*. Addison-Wesley.

[Gries, 1981] Gries, D. (1981). *The Science of Programming*. Springer-Verlag, New-York.

[Hebenstreit, 1985] Hebenstreit, J. (1985). Teaching programming to everybody, why? to whom? what? En Griffiths, M. y Tagg, E. (eds.), *The role of programming in teaching Informatics, Proceed. IFIP, TC3, Working Conference on Teaching Programming, París, 7–9 mayo, 1984*, pp. 17–21. Elsevier Science Pbl., Amsterdam.

[Hehner, 1984] Hehner, E. (1984). *The Logic of Programming*. Prentice-Hall, New Jersey.

[Hennessy, 1990] Hennessy, M. (1990). *The Semantics of Programming Languajes; An Elementary Introduction using Structural Operational Semantics*. Wiley.

[Hoare, 1969] Hoare, C. (1969). An Axiomatic Basis for Computer Programming. *Communications of the ACM*, 12(10):576–580. Reimpreso en *C.ACM*, 26(1):53-56, 1983, y también en [Hoare y Jones, 1989]:45-58.

[Hoare, 1971] Hoare, C. (1971). Computer Science. *New Lectures Series*, 62. reimpreso en [Hoare y Jones, 1989]:89–101.

[Hoare, 1978] Hoare, C. (1978). Communicating Sequential Processes. *Communications of the ACM*, 21(8). Reimpreso en [Gehani y McGettrick, 1988]:278-308, y también en [Horowitz, 1983]:311-322.

[Hoare, 1985] Hoare, C. (1985). *Communicating Sequential Processes*. Prentice–Hall, New Jersey.

[Hoare y Jones, 1989] Hoare, C. y Jones, C. (1989). *Essays in Computing Science*. Prentice-Hall.

[Horowitz, 1983] Horowitz, E. (1983). *Programming Languages. A grand Tour*. Computer Science Press.

[Horowitz y Sahni, 1978] Horowitz, E. y Sahni, S. (1978). *Fundamentals of Computer Algorithms*. Comp. Science Press.

[Huet, 1990] Huet, G. P. (1990). A Uniform approach to Type Theory. En Huet, G. (ed.), *Logical Foundations of Functional Programming*, pp. 337–397. Addison-Wesley.

[Knuth, 1968] Knuth, D. E. (1968). *The Art of Computer Programming. Vol. 1: Fundamental Algorithms*. Addison-Wesley, Massachusetts. Segunda edición (1973). Traducido al castellano en Ed. Reverté, Barcelona.

[Kowalski, 1979] Kowalski, R. (1979). *Logic for Problem Solving*. Elsevier Sc. Publ. Co. Traducción al castellano en Díaz de Santos, Madrid (1986), con el título *Lógica, Programación e Inteligencia Artificial*.

[Liskov y Zilles, 1974] Liskov, B. y Zilles, S. (1974). Programming with abstract data types. En *Proc. ACM SIGPLAN Conference on Very High Level Languages*, volumen 9, 4, pp. 50–59.

[Manna, 1974] Manna, Z. (1974). *Mathematical Theory of Computation*. McGraw-Hill.

[Meyer, 1988] Meyer, B. (1988). *Object-Oriented Software Construction*. Prentice–Hall.

[Morris, 1990] Morris, J. (1990). Programs from Specifications. En Dijkstra, E. (ed.), *Formal Development of Programs and Proofs*, pp. 81–115. Addison-Wesley. The Year of Programming.

[Nielson y Nielson, 1992] Nielson, H. y Nielson, F. (1992). *Semantics with Applications*. Wiley.

[Popek y Horning, 1977] Popek, G. y Horning, J. (1977). Notes on the Design of Euclid. *ACM SIGPLAN Notices*, 12(3):11–19.

[Ruiz Jiménez et al., 2000] Ruiz Jiménez, B. C., Gutiérrez López, F., Guerrero García, P., y Gallardo Ruiz, J. E. (2000). *Razonando con Haskell. Una Introducción a la Programación Funcional*. José E. Gallardo Ruiz (editor).

[Schmidt, 1988] Schmidt, D. (1988). *Denotational Semantics*. Allyn and Bacon.

[Shapiro, 1987] Shapiro, E. (1987). *Concurrent Prolog. Collected Papers*. MIT Press, Cambridge. Dos volúmenes.

[Sperschneider y Antoniou, 1991] Sperschneider, V. y Antoniou, G. (1991). *LOGIC. A Foundation for Computer Science*. Addison Wesley.

[Ueda, 1985] Ueda, K. (1985). Guarded Horn Clauses. Informe Técnico núm. 103, ICOT, Tokyo. También en [Shapiro, 1987]:(Vol.1,140-156).

[van Gasteren, 1990] van Gasteren, A. (1990). On the Formal Derivation of a Proof of the Invariance Theorem. En Dijkstra, E. (ed.), *Formal Development of Programs and Proofs*, pp. 49–54. Addison-Wesley. The Year of Programming.

[Wegner, 1984] Wegner, P. (1984). Capital-intensive software technology. *IEEE Software*, pp. 7–45.

[Wirth, 1973] Wirth, N. (1973). *Systematic Programming*. Prentice-Hall, New Jersey. traducción al castellano en Ed. El Ateneo, Buenos Aires (1982).

[Wirth, 1976] Wirth, N. (1976). *Algorithms + Data Structures = Programs*. Prentice-Hall, New York. traducción al castellano en Ed. del Castillo, Madrid, 1980.

[Wirth, 1983] Wirth, N. (1983). On the Design of Programming Languages. En *IFIP, 1974*, pp. 386–393. North-Holland Pub. Comp. reimpreso en [Horowitz, 1983]:23–30.

[Wirth y Hoare, 1973] Wirth, N. y Hoare, C. (1973). An Axiomatic Definition of the Programming Language PASCAL. *Acta Informatica*, 2(4):335–355. Reimpreso en [Hoare y Jones, 1989]:153–169.