DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 1: Especificación y WP

Fondo Monetario Común

19 de abril de 2024 — Algoritmos y Estructuras de Datos

Integrante	LU	Correo electrónico
Roda Baez, Santiago Ariel	1021/23	santiroda04@gmail.com
Sigal Aguirre, Mario	157/22	mariosigalaguirre@gmail.com
Astudillo, Marcos Ariel	841/22	astudillomarcos15@gmail.com
Moreira Siri, Juan Manuel	592/20	drakenn96@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

1. Predicados y funciones auxiliares usados en más de un ejercicio

`pred todosPositivos` (in s :$seq\langle\mathbb{R}\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |s| \longrightarrow_L s[i] > 0)$
}

`pred todasPositivas` (s : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall l : seq\langle\mathbb{R}\rangle)\ (l \in s \longrightarrow_L (\forall i : \mathbb{Z})\ (0 \leq i < |l| \longrightarrow_L l[i] > 0))$
}

`pred todasSumanUno` (s : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall l : seq\langle\mathbb{R}\rangle)\ (l \in s \longrightarrow_L \sum_{i=0}^{|l|-1} l[i] = 1)$
}

`pred todasMismaLongitud` (s : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i, j : \mathbb{Z})\ (0 \leq i, j < |s| \longrightarrow_L |s[i]| = |s[j]|)$
}

`pred todasPositivasOCero` (s : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall l : seq\langle\mathbb{R}\rangle)\ (l \in s \longrightarrow_L (\forall i : \mathbb{Z})\ (0 \leq i < |l| \longrightarrow_L l[i] \geq 0))$
}

`pred contienenListasDeIgualLongitud` (s, l : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i, j : \mathbb{Z})\ (0 \leq i, j < |s| \longrightarrow_L |s[i]| = |l[j]|)$
}

`pred todasNoVacias` (s : $seq\langle seq\langle T\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |s| \longrightarrow_L |s[i]| > 0)$
}

`pred eventosCorrectos` (s : $seq\langle seq\langle\mathbb{N}\rangle\rangle$, a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall l : seq\langle\mathbb{N}\rangle)\ (l \in s \longrightarrow_L (\forall i : \mathbb{N})\ (i \in l \longrightarrow_L 0 \leq i < |a[0]|))$
}

`pred trayectoriasDeLongitudAdecuada` (trayectorias : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$(\forall l : seq\langle\mathbb{R}\rangle)\ (l \in trayectorias \longrightarrow_L |l| = |eventos[0]| + 1)$
}

`aux parteDelFondo` (j : $\mathbb{Z}$, trayectorias, apuestas, pagos : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$, cooperan : $seq\langle\mathsf{Bool}\rangle$) : $\mathbb{R}$ = $\frac{\sum_{i=0}^{|cooperan|-1} \text{if } cooperan[i] \text{ then } recursosTrasApostar(i,j,trayectorias,apuestas,pagos,eventos) \text{ else } 0 \text{ fi}}{|cooperan|}$;

`aux recursosTrasApostar` (i, j : $\mathbb{Z}$, trayectorias, apuestas, pagos : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) : $\mathbb{R}$ = $trayectorias[i][j] * apuestas[i][eventos[i][j]] * pagos[i][eventos[i][j]]$;

`pred trayectoriasCorrectas` (trayectorias : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, recursos : $seq\langle\mathbb{R}\rangle$, cooperan : $seq\langle\mathsf{Bool}\rangle$,apuestas : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, pagos : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$|trayectorias| = |pagos| \ \wedge$
$trayectoriasDeLongitudAdecuada(trayectorias, eventos) \ \wedge \ recursosInicialesAdecuados(trayectorias, recursos)$
$\wedge \ pasosCorrectos(trayectorias, apuestas, pagos, cooperan, eventos)$
}

`pred recursosInicialesAdecuados` (trayectorias : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, recursos : $seq\langle\mathbb{R}\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \ \longrightarrow_L \ trayectorias[i][0] = recursos[i])$
}

`pred pasosCorrectos` (trayectorias, apuestas, pagos : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, cooperan : $seq\langle\mathsf{Bool}\rangle$, eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \wedge_L cooperan[i] = true \longrightarrow_L (\forall j : \mathbb{Z})\ (1 \leq j < |trayectorias[i]| \longrightarrow_L trayectorias[i][j] = parteDelFondo(j-1, trayectorias, apuestas, pagos, eventos, cooperan))) \ \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \wedge_L \neg cooperan[i] = true \longrightarrow_L (\forall j : \mathbb{Z})\ (1 \leq j < |trayectorias[i]| \longrightarrow_L trayectorias[i][j] = parteDelFondo(j-1, trayectorias, apuestas, pagos, eventos, cooperan) \ +$
$recursosTrasApostar(i, j-1, trayectorias, apuestas, pagos, eventos)))$
}

`aux ultimoRecurso` (trayectorias : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, individuo : $\mathbb{N}$) : $\mathbb{R}$ =
$trayectorias[individuo][|trayectorias[individuo]| - 1]$;

2. Especificación

1. **redistribucionDeLosFrutos**: Calcula los recursos que obtiene cada uno de los individuos luego de que se redistribuyen los recursos del fondo monetario común en partes iguales. El fondo monetario común se compone de la suma de *recursos* iniciales aportados por todas las personas que *cooperan.* La salida es la lista de recursos que tendrá cada jugador.

`proc redistribucionDeLosFrutos` (in recursos : $seq\langle\mathbb{R}\rangle$, in cooperan : $seq\langle\text{Bool}\rangle$) : $seq\langle\mathbb{R}\rangle$

`requiere` $\{todosPositivos(recursos) \ \wedge \ |recursos| = |cooperan|\}$

`asegura` $\{|res| = |recursos| \ \wedge_L$
$(\forall i : \mathbb{Z})\ (0 \leq i < |res| \wedge cooperan[i] = true \longrightarrow_L res[i] = parteDelFondoInicio(recursos, cooperan)) \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |res| \wedge \neg cooperan[i] = true \longrightarrow_L res[i] = recursos[i] +$
$parteDelFondoInicio(recursos, cooperan))\}$

`aux parteDelFondoInicio` (recursos : $seq\langle\mathbb{R}\rangle$, cooperan : $seq\langle\text{Bool}\rangle$) : $\mathbb{R} = \dfrac{\sum_{i=0}^{|recursos|-1} \text{if } cooperan[i] \text{ then } recursos[i] \text{ else } 0 \text{ fi}}{|recursos|}$;

2. **trayectoriaDeLosFrutosIndividualesALargoPlazo**: Actualiza (In/Out) la lista de *trayectorias* de los los recursos de cada uno de los individuos. Inicialmente, cada una de las trayectorias (listas de recursos) contiene un único elemento que representa los recursos iniciales del individuo. El procedimiento agrega a las *trayectorias* los recursos que los individuos van obteniendo a medida que se van produciendo los resultados de los *eventos* en función de la lista de *pagos* que le ofrece la naturaleza (o casa de apuestas) a cada uno de los individuos, las *apuestas* (o inversiones) que realizan los individuos en cada paso temporal, y la lista de individuos que *cooperan* aportando al fondo monetario común.

`proc trayectoriaDeLosFrutosIndividualesALargoPlazo` (inout trayectorias : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in cooperan : $seq\langle\text{Bool}\rangle$, in apuestas : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in pagos : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, In eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$)

`requiere` $\{trayectorias = A_0 \ \wedge \ todasLongitudUno(A_0) \ \wedge \ todasPositivas(A_0) \ \wedge$
$(|A_0| = |cooperan| = |apuestas| = |pagos| = |eventos|) \ \wedge \ todasSumanUno(apuestas) \ \wedge$
$todasMismaLongitud(apuestas) \ \wedge \ todasMismaLongitud(pagos) \ \wedge \ todasMismaLongitud(eventos) \ \wedge$
$todasPositivas(pagos) \ \wedge \ todasPositivasOCero(apuestas) \ \wedge$
$contienenListasDeIgualLongitud(apuestas, pagos) \wedge todasNoVacias(apuestas) \wedge todasNoVacias(pagos) \wedge$
$todasNoVacias(eventos) \ \wedge \ eventosCorrectos(eventos, apuestas)\}$

`asegura` $\{igualesRecursosIniciales(trayectorias, A_0) \ \wedge \ |trayectorias| = |A_0| \ \wedge$
$trayectoriasDeLongitudAdecuada(trayectorias, eventos) \ \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \wedge_L cooperan[i] = true \longrightarrow_L (\forall j : \mathbb{Z})\ (1 \leq j < |trayectorias[i]| \longrightarrow_L$
$trayectorias[i][j] = parteDelFondo(j-1, trayectorias, apuestas, pagos, eventos, cooperan)\,)) \ \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \wedge_L \neg cooperan[i] = true \longrightarrow_L (\forall j : \mathbb{Z})\ (1 \leq j < |trayectorias[i]| \longrightarrow_L$
$trayectorias[i][j] = recursosTrasApostar(i, j-1, trayectorias, apuestas, pagos, eventos) \ +$
$parteDelFondo(j-1, trayectorias, apuestas, pagos, eventos, cooperan)\,))\}$

`pred todasLongitudUno` (s : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {

$(\forall i : \mathbb{Z})\ (0 \leq i < |s| \longrightarrow_L |s[i]| = 1)$

}

`pred igualesRecursosIniciales` (s, l : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {

$(\forall i : \mathbb{Z})\ (0 \leq i < |s| \longrightarrow_L s[i][0] = l[i][0])$

}

3. **trayectoriaExtrañaEscalera**: Esta función devuelve *True* sii en la trayectoria de un individuo existe un único punto mayor a sus vecinos (llamado máximo local). Un elemento es máximo local si es mayor estricto que sus vecinos inmediatos. (Aclaramos que tomamos como posibles máximos locales a los extremos y que una lista con un único elemento tiene un máximo local)

`proc trayectoriaExtrañaEscalera` (in trayectoria : $seq\langle\mathbb{R}\rangle$) : Bool

`requiere` $\{True\}$

`asegura` $\{res = True \iff |trayectoria| = 1 \lor existeUnicoMaximoLocalIntermedio(trayectoria) \lor elMaximoLocalEsElPrimero(trayectoria) \lor elMaximoLocalEsElUltimo(trayectoria)\}$

`pred existeUnicoMaximoLocalIntermedio` (trayectoria : $seq\langle\mathbb{R}\rangle$) {

$(\exists i : \mathbb{Z})\ (0 < i < |trayectoria| - 1 \land_L trayectoria[i] > trayectoria[i+1] \land trayectoria[i] > trayectoria[i-1] \land \neg(trayectoria[0] > trayectoria[1]) \land \neg(trayectoria[|trayectoria| - 1] > trayectoria[|trayectoria| - 2]) \land \neg(\exists j : \mathbb{Z})\ (0 < j < |trayectoria| - 1 \land_L i \neq j \land trayectoria[j] > trayectoria[j+1] \land trayectoria[j] > trayectoria[j-1]))$

}

`pred elMaximoLocalEsElPrimero` (trayectoria : $seq\langle\mathbb{R}\rangle$) {

$|trayectoria| > 1 \land_L trayectoria[0] > trayectoria[1] \land \neg(trayectoria[|trayectoria| - 1] > trayectoria[|trayectoria| - 2]) \land \neg(\exists i : \mathbb{Z})\ (0 < i < |trayectoria| - 1 \land_L trayectoria[i] > trayectoria[i+1] \land trayectoria[i] > trayectoria[i-1])$

}

`pred elMaximoLocalEsElUltimo` (trayectoria : $seq\langle\mathbb{R}\rangle$) {

$|trayectoria| > 1 \land_L\ (trayectoria[|trayectoria| - 1] > trayectoria[|trayectoria| - 2]) \land \neg(trayectoria[0] > trayectoria[1]) \land \neg(\exists i : \mathbb{Z})\ (0 < i < |trayectoria| - 1 \land_L trayectoria[i] > trayectoria[i+1] \land trayectoria[i] > trayectoria[i-1])$

}

4. **individuoDecideSiCooperarONo**: Un *individuo* actualiza su comportamiento cooperativo / no-cooperativo (*cooperan*[*individuo*]) en función de los *recursos* iniciales, de quienes *cooperan*, de los *pagos* que se le ofrecen a cada individuo, de las inversiones o *apuestas* de cada individuo, y del resultado los *eventos* que recibe cada individuo, eligiendo el comportamiento que maximiza sus recursos individuales a largo plazo.

`proc individuoDecideSiCooperarONo` (in individuo: $\mathbb{N}$, in recursos: $seq\langle\mathbb{R}\rangle$, inout cooperan: $seq\langle$Bool$\rangle$, in apuestas: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in pagos: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in eventos: $seq\langle seq\langle\mathbb{N}\rangle\rangle$)

`requiere` $\{cooperan = C_0 \land 0 \leq individuo < |recursos| \land todosPositivos(recursos) \land (|recursos| = |cooperan| = |apuestas| = |pagos| = |eventos|) \land todasSumanUno(apuestas) \land todasMismaLongitud(apuestas) \land todasMismaLongitud(pagos) \land todasMismaLongitud(eventos) \land todasPositivas(pagos) \land todasPositivasOCero(apuestas) \land contienenListasDeIgualLongitud(apuestas, pagos) \land todasNoVacias(apuestas) \land todasNoVacias(pagos) \land todasNoVacias(eventos) \land eventosCorrectos(eventos, apuestas)\}$

`asegura` $\{cooperan = setAt(C_0, individuo, true) \iff (\exists trayectoriasCooperando, trayectoriasSinCooperar : seq\langle seq\langle\mathbb{R}\rangle\rangle)\ ($
$trayectoriasCorrectas(trayectoriasCooperando, recursos, setAt(C_0, individuo, true), apuestas, pagos, eventos) \land$
$trayectoriasCorrectas(trayectoriasSinCooperar, recursos, setAt(C_0, individuo, false), apuestas, pagos, eventos) \land$
$ultimoRecurso(trayectoriasCooperando, individuo) > ultimoRecurso(trayectoriasSinCooperar, individuo)$
$) \land$
$cooperan = setAt(C_0, individuo, false) \iff (\exists trayectoriasCooperando, trayectoriasSinCooperar : seq\langle seq\langle\mathbb{R}\rangle\rangle)\ ($
$trayectoriasCorrectas(trayectoriasCooperando, recursos, setAt(C_0, individuo, true), apuestas, pagos, eventos) \land$
$trayectoriasCorrectas(trayectoriasSinCooperar, recursos, setAt(C_0, individo, false), apuestas, pagos, eventos) \land$
$ultimoRecurso(trayectoriasCooperando, individuo) \leq ultimoRecurso(trayectoriasSinCooperar, individuo)$
$)\}$

5. **individuoActualizaApuesta**: Un *individuo* actualiza su apuesta ($apuestas[individuo]$) en función de los *recursos* iniciales, de la lista de individuos que *cooperan*, de los *pagos* que se le ofrecen a cada individuo, de las inversiones o *apuestas* de cada individuo y del resultado los *eventos* que recibe cada individuo, eligiendo la apuesta que maximiza sus recursos individuales a largo plazo.

`proc individuoActualizaApuesta` (in individuo : $\mathbb{N}$, in recursos : $seq\langle\mathbb{R}\rangle$, in cooperan : $seq\langle\mathsf{Bool}\rangle$, inout apuestas : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in pagos : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$)

`requiere` $\{apuestas = A_0 \ \wedge \ 0 \leq individuo < |recursos| \ \wedge$
$(|recursos| = |cooperan| = |apuestas| = |pagos| = |eventos|) \ \wedge \ todosPositivos(recursos) \ \wedge$
$todasSumanUno(apuestas) \ \wedge \ todasMismaLongitud(apuestas) \ \wedge \ todasMismaLongitud(pagos) \ \wedge$
$todasMismaLongitud(eventos) \ \wedge \ todasPositivas(pagos) \ \wedge \ todasPositivasOCero(apuestas) \ \wedge$
$contienenListasDeIgualLongitud(apuestas, pagos) \wedge todasNoVacias(apuestas) \wedge todasNoVacias(pagos) \wedge$
$todasNoVacias(eventos) \ \wedge \ eventosCorrectos(eventos, apuestas)\}$

`asegura` $\{|apuestas| = |A_0| \ \wedge_L \ soloCambiaElIndividuo(individuo, apuestas, A_0) \ \wedge$
$todasMismaLongitud(apuestas) \wedge todosPositivosOCero(apuestas[individuo]) \wedge sumanUno(apuestas[individuo])$
$\wedge$
$(\exists mejorTrayectorias : seq\langle seq\langle\mathbb{R}\rangle\rangle)$ (
$trayectoriasCorrectas(mejorTrayectorias, recursos, cooperan, setAt(A_0, individuo, apuestas[individuo]), pagos,$
$eventos) \ \wedge \ (\forall apuesta : seq\langle\mathbb{R}\rangle)\ (|apuesta| = |apuestas[individuo]| \wedge sumanUno(apuesta)$
$\wedge todosPositivosOCero(apuesta) \longrightarrow_L$
$(\exists trayectoriasApuesta : seq\langle seq\langle\mathbb{R}\rangle\rangle)$ (
$trayectoriasCorrectas(trayectoriasApuesta, recursos, cooperan, setAt(A_0, individuo, apuesta), pagos, eventos) \wedge$

$ultimoRecurso(mejorTrayectorias, individuo) \geq ultimoRecurso(trayectoriaApuesta, individuo)$
))
)\}

`pred soloCambiaElIndividuo` (individuo : $\mathbb{N}$, apuestasModificadas : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, apuestasOriginales : $seq\langle seq\langle\mathbb{R}\rangle\rangle$)
{
$(\forall i : \mathbb{Z})\ (0 \leq i < |apuestasModificadas| \wedge i \neq individuo \ \longrightarrow_L \ apuestasModificadas[i] = apuestasOriginales[i])$
}

`pred sumanUno` (apuesta : $seq\langle\mathbb{R}\rangle$) {
$\sum_{i=0}^{|apuesta|-1} apuesta[i] = 1$
}

`pred todosPositivosOCero` (s : $seq\langle\mathbb{R}\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |s| \longrightarrow_L s[i] \geq 0)$
}

3. Demostracion de correctitud

3.1. Introducción:

```
1  res = recursos
2  i = 0
3  while ( i < |eventos |) do
4      if eventos [ i ] then
5          res = (res * apuesta.c) * pago.c
6      else
7          res = (res * apuesta.s) * pago.s
8      endif
9      i = i + 1
10 endwhile
```

Código 1: demostraremos la correctitud de este codigo respecto de la siguiente especificacion

proc frutoDelTrabajoPuramenteIndividual (in recursos: $\mathbb{R}$, in apuestas $\langle$ s : $\mathbb{R}$, c : $\mathbb{R}\rangle$, in pago:$\langle$ s : $\mathbb{R}$, c : $\mathbb{R}\rangle$, in eventos: $seq\langle$Bool$\rangle$,out res:$\mathbb{R}$)

requiere $\{apuesta_c + apuestas_s = 1 \land pago_c > 0 \land pago_s > 0 \land apuesta_c > 0 \land apuesta_s > 0 \land recurso > 0\}$

asegura $\{res = recursos(apuestas_c, pago_c)^{\#apariciones(eventos,T)}(apuestas_s, pago_s)^{\#apariciones(eventos,F)}\}$

3.2. Resolución:

Supodremos:

$P \equiv requiere; Q \equiv asegura$

Queremos demostrar la siguiente tripla de Hoare:

$$\{P\}Código\ 1\{Q\} \tag{1}$$

Queremos ver que:

$$P \to wp(Código\ 1, Q) \tag{2}$$

Vemos que *Código* 1 se encuentra subdividido en sub-instrucciones de codigo $s1; s2; s3$. Siendo:

- s1:

```
res = recursos
```

- s2:

```
i = 0
```

- s3:

```
while ( i < |eventos |) do
    if eventos [ i ] then
        res = (res * apuesta.c) * pago.c
    else
        res = (res * apuesta.s) * pago.s
    endif
    i = i + 1
endwhile
```

Por lo tanto ver (2) es lo mismo que ver:

$$P \to wp(s1; s2; s3, Q) \tag{3}$$

A su vez, por el colorario de la monotonia, esto es equivalente a probar que:

$$\begin{aligned} P &\to wp(s1; s2, P_c) \\ P_c &\to wp(s3, Q) \end{aligned} \tag{4}$$

Como s3 es un ciclo, ver $P_c \to wp(s3, Q)$ es lo mismo que ver la correccion de su tripla de Hoare:

$$\{P_c\}s3\{Q_c\}\ con : Q_c \equiv Q \tag{5}$$

Para ello, enunciamos y demostramos que vale en este caso el teorema de corrección de un ciclo:

Teorema: Sean un predicado I y una función $fv : \mathbb{V} \to \mathbb{Z}$ (donde V es el producto cartesiano de los dominios de las variables del programa), y supongamos que $I \to def(B).Si$:

1. $P_c \to I$
2. $\{I \land B\}S\{I\}$
3. $I \land \neg B \to Q_c$
4. $\{I \land B \land v_0 = fv\}S\{fv < v_0\}$
5. $I \land fv \leq 0 \to \neg B$

Entonces, la siguiente tripla de Hoare es válida:

$$\{P_c\} while\ B\ do\ S\ endwhile \{Q_c\} \tag{6}$$

Definimos:

$I \equiv 0 \leq i \leq |eventos| \wedge_L res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

$P_c \equiv res = recurso \wedge i = 0 \wedge pago_c > 0 \wedge pago_s > 0 \wedge apuestas_c > 0 \wedge apuestas_s > 0 \wedge recurso > 0$

$Q_c \equiv Q \equiv res = recurso * (apuestas_c * pago_c)^{\#(eventos,T)} * (apuestas_s * pago_s)^{\#(eventos,F)}$

$B \equiv i < |eventos|$

Probaremos primero 1. $P_c \longrightarrow I$:

$i = 0 \longrightarrow 0 \leq i \leq |eventos|$

Y tambien:

$res = recurso \longrightarrow res = recurso * 1 \equiv res = recurso * (apuestas_c * pago_c)^0 * (apuestas_s * pago_s)^0$

Y como $i = 0$ esta última expresión implica:

$res = recurso * (apuestas_c * pago_c)^{\#(subseq(eventos,0,0),T)} * (apuestas_s * pago_s)^{\#(subseq(eventos,0,0),F)} \equiv$
$res = recurso * (apuestas_c * pago_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pago_s)^{\#(subseq(eventos,0,i),F)} \equiv I_\square$

Probaremos ahora 3. $I \wedge \neg B \longrightarrow Q_c$

$0 \leq i \leq |eventos| \wedge \neg(i < |eventos|) \longrightarrow i = |eventos|$

Luego:

$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)} \wedge i = |eventos| \longrightarrow$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,|eventos|),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,|eventos|),F)} \equiv$
$res = recurso * (apuestas_c * pagos_c)^{\#(eventos,T)} * (apuestas_s * pagos_s)^{\#(eventos,F)} \equiv Q_c\ \square$

Probaremos ahora 2. $\{I \wedge B\}\, S\, \{I\}$:

Probar esto es equivalente a probar que $I \wedge B \longrightarrow wp(S, I)$, siendo S:

$$S = S_1; S_2 = if(eventos[i]) then(res := res * apuestas_c * pago_c) else(res := res * apuestas_s * pago_s) endif; i := i + 1 \tag{7}$$

Entonces tenemos que:

$wp(S, I) \equiv wp(S_1, wp(S_2, I)) \equiv wp(S_1, wp(i := i + 1, I)) \equiv wp(S_1, I^i_{i+1}) \equiv def(eventos[i]) \wedge_L ((eventos[i] = true \wedge$
$wp(res := res * apuestas_c * pago_c, I^i_{i+1})) \vee (eventos[i] = false \wedge wp(res := res * apuestas_s * pago_s, I^i_{i+1}))) \equiv$

$0 \leq i < |eventos| \wedge_L ((eventos[i] = true \wedge (I^i_{i+1})^{res}_{res * apuestas_c * pago_c}) \vee (eventos[i] = false \wedge (I^i_{i+1})^{res}_{res * apuestas_s * pago_s}))$

Para probar que esto es verdadero ($I \wedge B \longrightarrow wp(S, I)$) separaremos en 2 casos: eventos[i] = true y eventos[i] = false.

Si eventos[i] = true podemos simplificar el predicado:

$0 \leq i < |eventos| \wedge_L (eventos[i] = true \wedge (I^i_{i+1})^{res}_{res * apuestas_c * pago_c}) \vee (eventos[i] = false \wedge (I^i_{i+1})^{res}_{res * apuestas_s * pago_s})$

$\equiv 0 \leq i < |eventos| \wedge_L (eventos[i] = true \wedge (I^i_{i+1})^{res}_{res * apuestas_c * pago_c}) \equiv 0 \leq i < |eventos| \wedge_L (I^i_{i+1})^{res}_{res * apuestas_c * pago_c}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i + 1 \leq |eventos| \wedge_L$
$res * apuestas_c * pago_c = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i + 1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i + 1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)-1} * (apuestas_s * pagos_s)^{\#(concat(subseq(eventos,0,i),<eventos[i]>),F)}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i + 1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)+if eventos[i]=false then 1 else 0}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i + 1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

Por hipótesis tenemos que $0 \leq i \leq |eventos| \wedge i < |eventos| \longrightarrow 0 \leq i < |eventos| \longrightarrow 0 \leq i+1 \leq |eventos|$

También tenemos que $res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)+1-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)+(if(true)then1else0fi)-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

Y como asumimos $eventos[i] = true$:

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)+(if(eventos[i])then1else0fi)-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)-1} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

Finalmente podemos concluir que $I \wedge B \longrightarrow wp(S, I)$ para el caso en que $eventos[i] = true$

Veamos ahora el caso en el que $eventos[i] = false$ y podemos simplificar el predicado:

$0 \leq i < |eventos| \wedge_L (eventos[i] = true \wedge (I^i_{i+1})^{res}_{res*apuestas_c*pago_c}) \vee (eventos[i] = false \wedge (I^i_{i+1})^{res}_{res*apuestas_s*pago_s})$

$\equiv 0 \leq i < |eventos| \wedge_L (eventos[i] = false \wedge (I^i_{i+1})^{res}_{res*apuestas_s*pago_s}) \equiv 0 \leq i < |eventos| \wedge_L (I^i_{i+1})^{res}_{res*apuestas_s*pago_s}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i+1 \leq |eventos| \wedge_L$
$res * apuestas_s * pago_s = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i+1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i+1),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)-1}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i+1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(concat(subseq(eventos,0,i)),<eventos[i]>),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)-1}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i+1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)+ifeventos[i]=truethen1else0} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)-1}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i+1 \leq |eventos| \wedge_L$
$res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)-1}$

Nuevamente por hipótesis tenemos que $0 \leq i \leq |eventos| \wedge i < |eventos| \longrightarrow 0 \leq i < |eventos| \longrightarrow 0 \leq i+1 \leq |eventos|$

Y $res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)}$

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)+1-1}$

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)+(if(true)then0else1)-1}$

Y como estamos asumiendo que $eventos[i] = false$:

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i),F)+(if(eventos[i])then0else1)-1}$

$\equiv res = recurso * (apuestas_c * pagos_c)^{\#(subseq(eventos,0,i),T)} * (apuestas_s * pagos_s)^{\#(subseq(eventos,0,i+1),F)-1}$

Por lo tanto concluimos que $I \wedge B \longrightarrow wp(S, I)$ también para el caso en que $eventos[i] = false$

Con lo cual hemos demostrado que la tripla de Hoare $\{I \wedge B\}S\{I\}$ es correcta. □

Para demostrar las dos condiciones del Teorema de terminación definiremos primero a la función:

$$fv = |eventos| - i \tag{8}$$

Demostraremos entonces 4. $\{I \wedge B \wedge v_0 = fv\}S\{fv < v_0\}$

Para ello probaremos que $I \wedge B \wedge v_0 = fv \longrightarrow wp(S, fv < v_0)$ Siendo S la misma que en la ecuación (7).

Entonces tenemos que:

$wp(S, fv < v_0) \equiv wp(S_1, wp(S_2, fv < v_0)) \equiv wp(S_1, wp(i := i + 1, |eventos| - i < v_0)) \equiv wp(S_1, |eventos| - (i + 1) < v_0) \equiv def(eventos[i]) \wedge_L ((eventos[i] = true \wedge wp(res := res * apuestas_c * pago_c, |eventos| - i - 1 < v_0)) \vee (eventos[i] = false \wedge wp(res := res * apuestas_s * pago_s, |eventos| - i - 1 < v_0))) \equiv$

$0 \leq i < |eventos| \wedge_L ((eventos[i] = true \wedge (|eventos| - i - 1 < v_0)) \vee (eventos[i] = false \wedge (|eventos| - i - 1 < v_0)) \equiv$

$0 \leq i < |eventos| \wedge_L (|eventos| - i - 1 < v_0)$

Veamos entonces que $I \wedge B \wedge v_0 = fv \longrightarrow 0 \leq i < |eventos| \wedge_L (|eventos| - i - 1 < v_0)$

Por hipótesis tenemos que $0 \leq i \leq |eventos| \wedge i < |eventos| \longrightarrow 0 \leq i < |eventos|$

Y también tenemos que $v_0 = fv \longrightarrow |eventos| - i - 1 < |eventos| - i$

Lo cual es trivialmente cierto. □

Finalmente probaremos 5. $I \wedge fv \leq 0 \longrightarrow \neg B$

Pero $|eventos| - i \leq 0 \equiv |eventos| \leq i \equiv \neg B$ □

De esta manera, como probamos los 5 puntos queda demostrado por el teorema de corrección de ciclos que:

$$P_c \rightarrow wp(s3, Q) \tag{9}$$

Ahora solo nos queda probar que $P \rightarrow wp(s1; s2, P_c)$. Para eso primero calculamos $wp(s1; s2, P_c)$:

$wp(s1; s2, P_c) \equiv$ wp(s1,wp(s2,P_c)) $\equiv$ wp(res := recurso,wp(i := 0, res = recurso $\wedge$ $i = 0 \wedge pago_c > 0 \wedge pago_s > 0 \wedge apuestas_c > 0 \wedge apuestas_s > 0 \wedge recurso > 0$)) $\equiv$ wp(res := recurso,(res = recurso $\wedge$ $0 = 0 \wedge pago_c > 0 \wedge pago_s > 0 \wedge apuestas_c > 0 \wedge apuestas_s > 0 \wedge recurso > 0$)) $\equiv$ recurso = recurso $\wedge pago_c > 0 \wedge pago_s > 0 \wedge apuestas_c > 0 \wedge apuestas_s > 0 \wedge recurso > 0$ $\equiv$ pago$_c$ $> 0 \wedge pago_s > 0 \wedge apuestas_c > 0 \wedge apuestas_s > 0 \wedge recurso > 0$

Luego, es trivialmente cierto que:
$P \equiv$ apuesta$_c$ + $apuesta_s = 1 \wedge$ pago$_c$ $> 0 \wedge$pago$_s$ $> 0 \wedge$apuesta$_c$ $> 0 \wedge$apuesta$_s$ $> 0 \wedge recurso > 0 \rightarrow$
pago$_c$ $> 0 \wedge pago_s > 0 \wedge apuesta_c > 0 \wedge apuesta_s > 0 \wedge recurso > 0 \equiv$ wp(s1;s2,P_c) □

Finalmente hemos demostrado que:

$$\begin{aligned} P &\rightarrow wp(s1; s2, P_c) \\ P_c &\rightarrow wp(s3, Q) \end{aligned} \tag{10}$$

y por lo tanto podemos concluir que la tripla $\{P\}s1; s2; s3\{Q\}$ es válida.