Trabajo Práctico 1: Especificación y WP

Fondo Monetario Común

19 de mayo de 2024 — Algoritmos y Estructuras de Datos

Grupo Debuggers

Integrante	LU	Correo electrónico
Zegers, Santiago	1433/21	zegerssantiagob@gmail.com
Azcurra, Mariano	1321/21	mariano.azcurra@hotmail.es
Gonzalez Villagra, Nicolás Andrés	1545/21	nicofcen86@gmail.com
Basualdo, Camilo	225/19	camilobasualdo@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. Especificación

1.1. redistribuciónDeLosFrutos:

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

`requiere` $\{|cooperan| > 0 \land |recursos| = |cooperan| \land todosPositivos(recursos)\}$

`asegura` $\{|result| = |recursos| \land recursosLuegoDeDistribución(result, recursos, cooperan)\}$

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

`pred recursosLuegoDeDistribución` ($r_f : seq\langle\mathbb{R}\rangle, r_i : seq\langle\mathbb{R}\rangle, b : seq\langle \mathsf{Bool}\rangle$){
$(\forall i : \mathbb{Z})\ (0 \leq i < |r_i| \land_L aporta(i, b) \longrightarrow_L r_f[i] = redistribución(r_i, b)) \land$
$(\forall j : \mathbb{Z})\ (0 \leq j < |r_i| \land_L \neg aporta(j, b) \longrightarrow_L r_f[j] = r_i[j] + redistribución(r_i, b))$
}

`pred aporta` (i: $\mathbb{Z}$, b: $seq\langle \mathsf{Bool}\rangle$) {
$b[i] = true$
}

`aux redistribución` (s: $seq\langle\mathbb{R}\rangle$, b: $seq\langle \mathsf{Bool}\rangle$) : $\mathbb{R} = (\sum_{i=0}^{|b|-1} \text{if } b[i] = true \text{ then } s[i] \text{ else } 0 \text{ fi})/|b|$;

1.2. trayectoriaDeLosFrutosIndividualesALargoPlazo

`proc` `trayectoriaDeLosFrutosIndividualesALargoPlazo` (inout trayectorias: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, in cooperan: $seq\langle \mathsf{Bool}\rangle$, 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` $\{trayectorias = trayectorias_0 \land mismaLongitud(trayectorias, cooperan, apuestas, pagos, eventos)$
$\land |cooperan| > 0 \land mismasApuestasQuePagos(apuestas, pagos) \land sonPositivos(pagos)$
$\land eventosValidos(eventos, apuestas) \land comienzaSoloConRecursoInicial(trayectorias) \land sonApuestasValidas(apuestas)\}$

`asegura` $\{|trayectorias| = |trayectorias_0| \land contieneALosIniciales(trayectorias, trayectorias0) \land$
$tieneLosEventos(trayectorias, eventos) \land trayectoriasIndividuales(trayectorias, cooperan, apuestas, pagos, eventos)\}$

`pred mismaLongitud` (t, c, a, p, e: $seq\langle T\rangle$) {
$|t| = |c| \land |c| = |a| \land$
$|a| = |p| \land |p| = |e|$
}

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

`pred sonPositivos` (s1: $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |s1| \longrightarrow_L todosPositivos(s1[i]))$
}

`pred eventosValidos` (e: $seq\langle seq\langle\mathbb{N}\rangle\rangle$, p: $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |e|) \longrightarrow_L (\forall j : \mathbb{Z})\ (0 \leq j < |e[i]| \longrightarrow_L 0 \leq e[i][j] < |p[i]|)$
}

`pred comienzaSoloConRecursoInicial` (t: $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |t| \land_L sonPositivos(t) \longrightarrow_L |t[i]| = 1)$
}

`pred contieneALosIniciales` (t: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, t0: $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |t| \longrightarrow_L t[i][0] = t0[i][0])$

}

`pred tieneLosEventos` (t: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, e:$seq\langle seq\langle \mathbb{N}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |t| \longrightarrow_L |t[i]| - 1 = |e[i]|)$
}

`pred trayectoriasIndividuales` (t: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, c: $seq\langle \mathsf{Bool}\rangle$, a: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, p: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, e: $seq\langle seq\langle \mathbb{N}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |t| \longrightarrow trayectoria(i, t[i], t, c, a, p, e))$
}

`pred trayectoria` (i:$\mathbb{Z}$, r:$seq\langle \mathbb{R}\rangle$, t: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, c: $seq\langle \mathsf{Bool}\rangle$, a: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, p: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, e: $seq\langle seq\langle \mathbb{N}\rangle\rangle$) {
$(\forall j : \mathbb{Z})\ (1 \leq j < |r| \longrightarrow (\neg aporta(i, c) \longrightarrow_L r[j] = r[j-1] * pagoEvento(i, j, a, p, e) + redistribucionEnJ(j, t, c)) \vee$
$(aporta(i, c) \longrightarrow_L r[j] = redistribucionEnJ(j, t, c)))$
}

`pred sonApuestasValidas` (apuestas: $seq\langle seq\langle \mathbb{R}\rangle\rangle$) {
$(\forall j : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq j < |\text{apuestas}| \wedge 0 \leq k < |\text{apuestas}[j]| \longrightarrow_L 0 \leq \text{apuestas}[j][k] \leq 1)$
}
`aux pagoEvento` (i,j: $\mathbb{Z}$, a,p: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, e: $seq\langle seq\langle \mathbb{N}\rangle\rangle$) : $\mathbb{R}$ $= apuestas[i][evento[i][j-1]] * pagos[i][evento[i][j-1]]$;

`aux redistribucionEnJ` (j: $\mathbb{Z}$, t: $seq\langle seq\langle \mathbb{R}\rangle\rangle$, c: $seq\langle \mathsf{Bool}\rangle$) : $\mathbb{R}$ $= (\sum_{i=0}^{|b|-1} \text{if } c[i] = true \text{ then } t[i][j] \text{ else } 0 \text{ fi})/|c|$;

1.3. trayectoriaExtrañaEscalera

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

`requiere` $\{|trayectoria| > 1\}$

`asegura` $\{result = true \iff (|trayectoria| > 2 \wedge hayUnMaximoLocal(trayectoria)) \vee (|trayectoria| = 2 \wedge$
$trayectoria[0] \neq trayectoria[1])\}$

`pred hayUnMaximoLocal` (t: $seq\langle \mathbb{R}\rangle$) {
$(\exists i : \mathbb{Z})\ (1 \leq i < |t| \wedge_L (s[i] > s[i-1] \wedge s[i] > s[i+1])) \wedge \neg(\exists j : \mathbb{Z})\ (1 \leq j < |t| \wedge i \neq j \wedge_L (s[j] > s[j-1] \wedge s[j] > s[j+1]))$
}

1.4. individuoDecideSiCooperarONo

`proc individuoDecideSiCooperarONo` (in individuo: $\mathbb{N}$, in recursos: $seq\langle \mathbb{R}\rangle$, inout cooperan: $seq\langle \mathsf{Bool}\rangle$, 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` $\{0 \leq individuo < |recursos| \wedge cooperan = cooperan_0 \wedge$
$|cooperan| > 0 \wedge mismaLongitud(recursos, cooperan, apuestas, pagos, eventos) \wedge$
$\wedge mismasApuestasQuePagos(apuestas, pagos) \wedge sonPositivos(pagos)$
$\wedge eventosValidos(eventos, apuestas) \wedge sonApuestasValidas(apuestas)\}$

`asegura` $\{|cooperan| = |cooperan_0| \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |cooperan_0| \wedge i \neq individuo \longrightarrow_L cooperan[i] = cooperan_0[i]) \wedge$
$ganancias(individuo, apuestas[individuo], eventos[individuo], pagos[individuo], cooperan, recursos) \geq$
$ganancias(individuo, apuestas[individuo], eventos[individuo], pagos[individuo], cooperan_0, recursos))\}$

1.5. individuoActualizaApuesta

`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` $\{apuestas = A_0 \wedge sonApuestasValidas(A_0) \wedge |cooperan| > 0$
$sonPositivos(pagos) \wedge eventosValidos(eventos, apuestas) \wedge$
$0 \leq individuo < |recursos| \wedge mismaLongitud(recursos, cooperan, apuestas, eventos)\}$

`asegura` $\{|apuestas| = |A_0| \wedge$
$sonApuestasValidas(apuestas) \wedge$
$(\forall j : \mathbb{Z})\ (0 \leq j < |apuestas[individuo]| \wedge j \neq individuo \longrightarrow_L apuestas[j] = A_0[j])$
$\wedge \neg(\exists apuestaTeorica : seq\langle \mathbb{R}\rangle)\ ($

$esApuestaValida(apuestaTeorica)$
$\wedge_L\ ganancias(individuo, apuestaTeorica, eventos[individuo], pagos[individuo], cooperan, recursos) >$
$ganancias(individuo, apuestas[individuo], eventos[individuo], pagos[individuo], cooperan, recursos)$
)}

`aux ganancias` (individuo: $\mathbb{N}$, apuesta: $seq\langle\mathbb{R}\rangle$, eventos: $seq\langle\mathbb{N}\rangle$, pagos: $seq\langle\mathbb{R}\rangle$, cooperan: $seq\langle Bool\rangle$, recursos: $seq\langle\mathbb{R}\rangle$) : $\mathbb{R}$ =
if $cooperan[individuo]$ then
$redistribución(recursos, cooperan)$ else
$performanceIndividual(apuesta, pagos, individuo, eventos, recursos[individuo]) +$
$redistribución(recursos, cooperan)$ fi ;

`aux performanceIndividual` (apuestas:$seq\langle\mathbb{R}\rangle$, pagos: $seq\langle\mathbb{R}\rangle$, Individuo: $\mathbb{N}$, eventos[individuo]: $seq\langle\mathbb{R}\rangle$, recursos: $\mathbb{R}$) : $\mathbb{R}$ =
$recursos * \prod_{j=0}^{|apuestas|-1} pagos[j] * apuestas[j]^{apariciones(eventos, j+1)}$;

`pred esApuestaValida` (apuesta: $seq\langle\mathbb{R}\rangle$) {
$(\forall j:\mathbb{Z})\ (0 \leq j < |apuesta| \longrightarrow_L (-apuestas[j] \leq 0 \wedge \sum_{j=0}^{|apuesta|-1} apuestas[j] = 1))$
}

2. Demostración de correctitud

Tenemos la tripla de Hoare como dato, ya que nos dan el *requiere*, el *asegura* y el código que implementa en smallang. Si llamamos al *requiere* P, al *asegura* Q y al código S, tenemos que demostrar que

{P} S {Q}

es correcta respecto de S. Para eso, aplicaremos la siguiente fórmula:

$$\{P\}S\{Q\} \leftrightarrow \{P\} \implies WP(S,Q)$$

Empezamos por calcular entonces la WP(S,Q), la cual podemos reescribir de la siguiente forma.

WP(S,Q)= WP(res := recursos; i:= 0, **while**, Q)

Por el Axioma 1, tenemos lo siguiente

WP(S,Q)= WP(res := recursos; i:= 0, WP(**while**, Q))

Para demostrar que el ciclo es parcialmente correcto, aplicamos el Teorema del Invariante ya que es un ciclo, debemos probar lo siguiente

- $P_c \implies I$
- $\{I \wedge B\}S1\{I\}$
- $\{I \wedge \neg B\} \implies Q_c$

Donde $P_c \equiv \{i = 0 \wedge res = recursos \wedge apuesta_c + apuesta_s = 1 pago_c > 0 \wedge pago_s > 0 \wedge apuesta_c > 0 \wedge apuesta_s > 0 \wedge recurso > 0\}$, $B \equiv \{i < |eventos|\}$, $Q_c \equiv \{res = recursos * (apuesta.c * pago.c)^{cantApariciones(eventos,T)} * (apuesta.s * pago.s)^{cantApariciones(eventos,F)}\}$, S1 el código del ciclo

```
    if eventos[i] then
        res = (res x apuesta.c) x pago.c //lo llamaremos S2
    else
        res = (res x apuesta.s) x pago.s //lo llamaremos S3
    endif
    i = i+1
```

Código 1: Lo llamaremos S1 en los siguientes pasos.

e I es el invariante que proponemos:

$$I \equiv \{0 \leq i \leq |eventos| \wedge_L res = recursos * \prod_{j=0}^{i-1} \text{if } eventos[j] \text{ then } apuesta.c * pago.c \text{ else } apuesta.s * pago.s \text{ fi}\}$$

Ahora, podemos comenzar a demostrar los tres puntos del Teorema del Invariante.

$\underline{P_c \implies I}$:

Asumiendo P_c tenemos luego en I lo siguiente:

$I \equiv \{0 \leq \mathbf{0} \leq |eventos| \wedge_L res = recursos * \prod_{j=0}^{\mathbf{-1}} if... = recursos\} \equiv \{res = recursos\}$

Por lo que, se demuestra que la precondición del ciclo implica el Invariante, o lo que es lo mismo, el Invariante es válido antes de ingresar al ciclo.

$\underline{\{I \wedge B\}S1\{I\}}$:

Validar esta tripla, implica demostrar que

$$\{I \wedge B\} \implies WP(S1, I):$$

Por el Axioma 3, tenemos que

$$WP(S1, I) \equiv WP(\text{if } B \text{ then } S2 \text{ else } S3 \text{ fi}; i := i + 1, I) \equiv WP(\text{if } B \text{ then } S2 \text{ else } S3 \text{ fi}, WP(i := i + 1, I))$$

Calculamos $WP(i := i + 1, I)$:

Por Axioma 1, tenemos que

$$WP(i := i + 1, I) \equiv I^i_{i+1}$$

$$I^i_{i+1} \equiv \{0 \leq \mathbf{i+1} \leq |eventos| \wedge_L res = recursos * \prod_{j=0}^{\mathbf{i+1-1}} \text{if } eventos[j] \text{ then } apuesta.c * pago.c \text{ else } apuesta.s * pago.s \text{ fi}\}$$

Simplificando en la productoria tenemos el resultado de $WP(i := i + 1, I)$:

$$I^i_{i+1} \equiv \{0 \leq \mathbf{i+1} \leq |eventos| \wedge_L res = recursos * \prod_{j=0}^{\mathbf{i}} \text{if } eventos[j] \text{ then } apuesta.c * pago.c \text{ else } apuesta.s * pago.s \text{ fi}\}$$

Luego, por Axioma 4,

$WP(\text{if } B \text{ then } S2 \text{ else } S3 \text{ fi}, I^i_{i+1}) \equiv (B \wedge WP(S2, I^i_{i+1})) \vee (\neg B \wedge WP(S3, I^i_{i+1}))$

Calculamos $(B \wedge WP(S2, I^i_{i+1}))$

$\equiv \{eventos[i] \wedge (I^i_{i+1})^{res}_{res*apuesta.c*pago.c}\}$

$\equiv \{eventos[i] \wedge 0 \leq i + 1 \leq |eventos| \wedge_L$

res * apuesta.c * pago.c $= recursos * \prod_{j=0}^{\mathbf{i}} \text{if } eventos[j] \text{ then } apuesta.c * pago.c \text{ else } apuesta.s * pago.s \text{ fi}\}$

Como $eventos[i] = true$ podemos simplificar de productoria este valor, quedando lo siguiente:

$(B \wedge WP(S2, I^i_{i+1})$

$\equiv \{eventos[i] \wedge (0 \leq i+1 \leq |eventos|) \wedge_L$
$\mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

Análogamente, para el calculo de $\neg B \wedge WP(S3, I_{i+1}^{i})$, obtenemos:

$(\neg B \wedge WP(S3, I_{i+1}^{i}))$

$\equiv \{\neg eventos[i] \wedge (0 \leq i+1 \leq |eventos|) \wedge_L$
$\mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

Por lo que,

$WP(\textsf{if } B \textsf{ then } S2 \textsf{ else } S3 \textsf{ fi}, I_{i+1}^{i})$

$\equiv def(B) \wedge_L (B \wedge WP(S2, I_{i+1}^{i})) \vee (\neg B \wedge WP(S2, I_{i+1}^{i}))$

$\equiv 0 \leq i < |eventos| \wedge_L (eventos[i] \vee \neg eventos[i]) \wedge 0 \leq i+1 \leq |eventos| \wedge_L$
$\mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}$

$\equiv 0 \leq i < |eventos| \wedge_L 0 \leq i+1 \leq |eventos| \wedge_L$
$\mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}$

$\equiv 0 \leq i+1 \leq |eventos| \wedge_L$
$\mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}$

Asi que, tenemos lo siguiente:

$WP(S1, I) \equiv WP(\textsf{if } B \textsf{ then } S2 \textsf{ else } S3 \textsf{ fi}; i := i+1, I) \equiv$

$\{0 \leq i+1 \leq |eventos| \wedge_L$
$\mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

Debemos ahora, con los calculos hechos, volver al principio, e intentar demostrar la siguiente formula:

$$\{I \wedge B\} \implies WP(S1, I):$$

Donde

$\{I \wedge B\} \equiv \{0 \leq i < |eventos| \wedge_L res = recursos * \prod_{j=0}^{i-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

Y WP(S1,I) es el resultado que obtuvimos recien, es decir,

$WP(S1, I) \equiv \{0 \leq i+1 \leq |eventos| \wedge_L \mathbf{res} = recursos * \prod_{j=0}^{\mathbf{i-1}} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

$$0 \leq i < |eventos| \implies 0 \leq i+1 \leq |eventos|$$

Y como lo que esta luego del es lo mismo en ambos predicados, damos por terminada la demostracion.

<u>$\{I \wedge \neg B\} \implies Q_c$:</u>

$\{I \wedge \neg B\} \equiv \{0 \leq i \leq |eventos| \wedge_L$

$res = recursos * \prod_{j=0}^{i-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi} \wedge i >= |eventos|\}$

$\equiv \{i = |eventos| \wedge_L res = recursos * \prod_{j=0}^{i-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

$\equiv \{i = |eventos| \wedge_L res = recursos * \prod_{j=0}^{|eventos|-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\}$

$\equiv \{res = recursos * (apuesta.c * pago.c)^{cantApariciones(eventos,T)} * (apuesta.s * pago.s)^{cantApariciones(eventos,F)}\}$

$\equiv Q_c.$

Por lo que queda demostrada la tercera implicación.

Hemos demostrado que el ciclo es parcialmente correcto respecto de su especificación. Para ahora demostrar que el ciclo termina, usaremos una funcion variante f_v y probaremos lo siguiente:

- $\{I \wedge B \wedge f_v = V_0\}\ S\ \{f_v < V_0\}$
- $\{I \wedge f_v \leq 0\} \implies \{\neg B\}$

Donde $f_v = |eventos| - i$, e $I, B\ y\ S$ los mismos que en el apartado anterior.

<u>$\{I \wedge B \wedge f_v = V_0\}\ S\ \{f_v < V_0\}$:</u>

Demostrar este punto, nuevamente es demostrar que $\{I \wedge B \wedge f_v = V_0\} \implies WP(S, f_v < V_0\}$.

Calculamos $WP(S, f_v < V_0\}$:

$WP(\textsf{if } B \textsf{ then } S2 \textsf{ else } S3 \textsf{ fi}; i := i+1, f_v < V_0) \equiv$

$WP(\textsf{if } B \textsf{ then } S2 \textsf{ else } S3 \textsf{ fi}, WP(i := i+1, f_v < V_0)) \equiv$

$WP(\textsf{if } B \textsf{ then } S2 \textsf{ else } S3 \textsf{ fi}, |eventos| - i - 1 < V_0) \equiv$

$(B \wedge WP(S2, |eventos| - i - 1 < V_0)) \vee (\neg B \wedge WP(S3, |eventos| - i - 1 < V_0)) \equiv$

$(B \wedge eventos| - i - 1 < V_0) \vee (\neg B \wedge eventos| - i - 1 < V_0) \equiv$

$(B \vee \neg B) \wedge |eventos| - i - 1 < V_0 \equiv |eventos| - i - 1 < V_0$.

Luego,

$\{I \wedge B \wedge f_v = V_0\} \equiv \{0 \leq i \leq |eventos| \wedge_L res = recursos * \prod_{j=0}^{i-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi} \wedge |eventos| - i = V_0\} \implies \{|eventos| - i - 1 < V_0\}$

Ya que, si $|eventos| - i = V_0$, se tiene que $|eventos| - i - 1 < V_0$

<u>$\{I \wedge f_v \leq 0\} \implies \{\neg B\}$:</u>

$\{I \wedge f_v \leq 0\} \equiv$

$\{0 \leq i \leq |eventos| \wedge_L res = recursos * \prod_{j=0}^{i-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi} \wedge |eventos| - i \leq 0\} \equiv$

$\{i = |eventos| \wedge_L$

$res = recursos * \prod_{j=0}^{|eventos|-1} \textsf{if } eventos[j] \textsf{ then } apuesta.c * pago.c \textsf{ else } apuesta.s * pago.s \textsf{ fi}\} \implies \neg\{i < |eventos|\} \equiv \{\neg B\}$.

Finalmente, el ciclo termina y es correcto respecto de su especificación.

Ahora bien, ¿podemos decir cual es la precondición mas debil del ciclo? ¿Qué tenemos que hacer para probar que

$\{Pre\} res := recursos; i := 0; \textbf{while} \{Post\}$ es válida?

1. $\{Pre\} \implies WP(res := recursos; i := 0, P_c)$
2. $P_c \implies WP(while, Q_c)$
3. $Q_c \implies \{Post\}$

El punto 1 se demuestra observando que

$\{Pre\} \equiv \{apuesta.c + apuesta.s = 1 \wedge pago.c > 0 \wedge pago.s > 0 \wedge apuesta.c > 0 \wedge apuesta.s > 0 \wedge recurso > 0\}$

implica

$WP(res := recursos; i := 0, P_c) \equiv \{i = 0 \wedge res = recursos\}$

Como los recursos iniciales son positivos, el punto 1 es evidentemente correcto.

Los puntos 2 y 3 son igualdades de terminos, asi que la implicación es valida en ambos casos.

Luego, por Monotonía:

$\{Pre\} \implies WP(res := recursos; i := 0; while, Post)$

Que era lo que queríamos demostrar.