DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 1: Especificación y WP

Trabajo práctico grupal sobre especificación y precondición más débil

19 de mayo de 2024 — Algoritmo y Estructura de Datos

Grupo supercalifragilisticexpialidocious

Integrante	LU	Correo electrónico
Harari, Lazaro	982/23	lazaort@gmail.com
Mazzanti Santana, Maria Fernanda	970/23	mfernandamazzanti@gmail.com
Perel, Tobias	1087/23	pereltobias@gmail.com
Sosa, Alejandro	806/23	alesezes@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. Ejercicio 1

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

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

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

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

1.2. Ejercicio 2

`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` $\{longitudesIguales(trayectorias, cooperan, apuestas, pagos, eventos) \wedge numerosBien(apuestas, pagos) \wedge_L$ todasLasTrayectoriasTienenUnElemento(trayectorias) $\wedge\ apuestasPositivas(apuestas) \wedge\ pagosPositivos(pagos) \wedge apuestasBien(apuestas) \wedge\ eventosEnRango(eventos, apuestas)\}$

`asegura` $\{logitudDeLasTrayectorias(trayectorias, eventos) \wedge_L$
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \wedge_L cooperan[i] = true \longrightarrow_L (\forall j : \mathbb{Z})\ (0 \leq j < |eventos[i]| \longrightarrow_L$
$trayectorias[i][j+1] = (fondoMonetarioComun(j, trayectorias, apuestas, pagos, cooperan, eventos) \div |eventos[i]|))) \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \wedge_L cooperan[i] \neq true \longrightarrow_L (\forall j : \mathbb{Z})\ (0 \leq j < |eventos[i]| \longrightarrow_L$
$trayectorias[i][j+1] = resultadoApuesta(i, trayectorias[i][j], eventos[i][j], apuestas, pagos) +$
$(fondoMonetarioComun(j, trayectorias, apuestas, pagos, cooperan, eventos) \div |eventos[i]|))))\}$

`pred longitudesIguales` (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 : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$(|t| = |c|) \wedge (|c| = |a|) \wedge (|a| = |p|) \wedge (|p| = |e|)$
}

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

`pred longitudDeLasTrayectorias` (trayectorias : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, eventos : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |trayectorias| \longrightarrow_L |trayectorias[i]| = |eventos[i] + 1|)$
}

`aux resultadoApuesta` (i : $\mathbb{Z}$, recursosantes : $\mathbb{R}$, evento : $\mathbb{N}$, a: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, p : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) : $\mathbb{R}$ $= recursosantes \times a[i][evento] \times p[i][evento]$;

`aux fondoMonetarioComun` (j : $\mathbb{Z}$, t : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, p : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, c : $seq\langle \mathsf{Bool}\rangle$, e : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) : $\mathbb{R}$ $= (\sum_{i=0}^{|c|-1})(if\ c[i] = true\ then\ resultadoApuesta(i, t[i][j], e[i][j], a, p)\ else\ 0\ fi)$;

1.3. Ejercicio 3

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

`requiere` $\{True\}$

`asegura` $\{res = true \longleftrightarrow ((\exists i : \mathbb{Z})\ (0 \leq i < |trayectoria| \wedge esUnMaximoLocal(i, trayectoria) \wedge_L \neg(\exists j : \mathbb{Z})\ (0 \leq j < |trayectoria| \wedge i \neq j \wedge esUnMaximoLocal(j, trayectoria)))\}$

`pred esUnMaximoLocal` (indice : $\mathbb{Z}$, s: $seq\langle\mathbb{R}\rangle$) {
$(|s| = 1) \vee (0 < indice < |s| - 1 \wedge_L (s[indice] > s[indice-1]) \wedge (s[indice] > s[indice+1])) \vee (indice = 0 \wedge_L s[indice] > s[indice+1]) \vee (indice = |s| - 1 \wedge_L s[indice] > s[indice-1])$
}

1.4. Ejercicio 4

`proc individuoDecideSiCooperaONo` (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` $\{personasBien(recursos, cooperan, apuestas, pagos, eventos) \wedge numerosBien(apuestas, pagos) \wedge_L apuestasBien(apuestas) \wedge personaExiste(individuo, |cooperan|) \wedge recursosPositivos(recursos) \wedge apuestasPositivas(apuestas) \wedge pagosPositivos(pagos \wedge eventosEnRango(eventos, apuestas) \wedge cooperan = Cooperan_0\}$

asegura $\{(rendInd(individuo, recursos, setAt(cooperan, individuo, false), pagos, apuestas, eventos)$
$> rendFondo(recursos, setAt(cooperan, individuo, false), pagos, apuestas, eventos) \longleftrightarrow cooperan[individuo] = true) \wedge$
$(rendInd(individuo, recursos, setAt(cooperan, individuo, false), pagos, apuestas, eventos)$
$\leq rendFondo(recursos, setAt(cooperan, individuo, false), pagos, apuestas, eventos) \longleftrightarrow cooperan[individuo] = false) \wedge$
$(\forall i : \mathbb{Z})\ (0 \leq i < |cooperan| \wedge i \neq individuo \longrightarrow_L cooperan[i] = Cooperan_0[\mathrm{i}]\ )\ \}$

1.5. Ejercicio 5

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 $\{personasBien(recursos, cooperan, apuestas, pagos, eventos) \wedge numerosBien(apuestas, pagos) \wedge_L apuestasBien(apuestas) \wedge personaExiste(individuo, |cooperan|) \wedge recursosPositivos(recursos) \wedge apuestasPositivas(apuestas) \wedge pagosPositivos(pagos) \wedge eventosEnRango(eventos, apuestas) \wedge apuestas = Apuestas_0\}$

asegura $\{(\forall i : \mathbb{Z})\ (0 \leq i < |apuestas| \wedge i = individuo \longrightarrow_L rendInd(i, recursos, cooperan, pagos, apuestas, eventos) \geq rendInd(i, recursos, cooperan, pagos, Apuestas_0, eventos))\ \wedge\ (\forall i : \mathbb{Z})\ (0 \leq i < |apuestas| \wedge i \neq individuo \longrightarrow_L apuestas[i] = Apuestas_0[\mathrm{i}]\ )\ \wedge noExisteApuestaMejor(individuo, recursos, cooperan, pagos, apuestas, eventos)\}$

pred noExisteApuestaMejor (ind : $\mathbb{N}$, rec : $seq\langle\mathbb{R}\rangle$, coop : $seq\langle\mathsf{Bool}\rangle$, pa : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ap : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ev : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$\neg(\exists s : seq\langle seq\langle\mathbb{R}\rangle\rangle)\ (longitudesIguales(ap, s) \wedge apuestasBien(s) \wedge_L rendInd(ind, rec, coop, pa, s, ev) >$ rendInd(ind, rec, coop, pa, ap, ev)) }

1.6. Predicados y funciones auxiliares globales

pred personasBien (s : $seq\langle\mathbb{R}\rangle$, r : $seq\langle\mathsf{Bool}\rangle$, t : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, u : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, v : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) {
$(|s| = |r|) \wedge (|r| = |t|) \wedge (|t| = |u|) \wedge (|u| = |v|)$
}
pred apuestasPositivas (a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |a| \longrightarrow_L ((\forall k : \mathbb{Z})\ (0 \leq k < |a[i]| \longrightarrow_L a[i][k] > 0)))$
}
pred pagosPositivos (p : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |p| \longrightarrow_L ((\forall k : \mathbb{Z})\ (0 \leq k < |p[i]| \longrightarrow_L p[i][k] > 0)))$
}
pred apuestasBien (a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$((\forall i : \mathbb{Z})\ ((0 \leq i < |a|) \longrightarrow_L suman(1, a[i]) \wedge enRango(0, 1, a[i])))$
}
pred longitudesIguales (a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, s : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$|a| = |s| \wedge_L (\forall i : \mathbb{Z})\ (0 \leq i < |a| \longrightarrow_L |a[i]| = |s[i]|)$
}
pred suman (num : $\mathbb{Z}$, l : $seq\langle\mathbb{R}\rangle$) {
$\sum_{i=0}^{|l|-1} l[i] = num$
}
pred enRango (piso : $\mathbb{Z}$, techo : $\mathbb{Z}$, l : $seq\langle\mathbb{R}\rangle$) {
$((\forall i : \mathbb{Z})\ ((0 \leq i < |l|) \longrightarrow_L (piso \leq l[i] \leq techo))$
}
pred numerosBien (a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, p : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$((\forall i : \mathbb{Z})\ ((0 \leq i < |a| - 1) \longrightarrow_L (|a[i]| = |a[i+1]|))) \wedge_L ((\forall i : \mathbb{Z})\ ((0 \leq i < |a|) \longrightarrow_L |a[i]| = |p[i]|))$
}
pred personaExiste (individuo : $\mathbb{N}$, rango : $\mathbb{N}$) {
(if $0 \leq individuo < rango$ then $true$ else $false$ fi)
}
pred recursosPositivos (r : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ ((0 \leq i < |r|) \longrightarrow_L r[i] > 0)$
}
pred eventosEnRango (e : $seq\langle seq\langle\mathbb{N}\rangle\rangle$, a : $seq\langle seq\langle\mathbb{R}\rangle\rangle$) {
$(\forall i : \mathbb{Z})\ (0 \leq i < |e| \longrightarrow_L enRango(0, |a[i]|, e[i]))$
}

aux rendFondo (rec: $seq\langle\mathbb{R}\rangle$, coop: $seq\langle\mathsf{Bool}\rangle$, pa: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, apu: $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ev: $seq\langle seq\langle\mathbb{N}\rangle\rangle$) : $\mathbb{R}$ = if $cantCooperan(coop) = 0 \vee |ev| = 0$ then 0 else (if $|ev| = 1$ then $calcularInicial(rec, coop, pa, apu, ev)$ else $(calcularInicial(rec, coop, pa, apu, ev) \cdot (\prod_{i=0}^{|ev|-1} calcularTasas(pa, apu, coop, cv)))$ fi) fi ;

`aux rendInd` (ind : $\mathbb{N}$, rec : $seq\langle\mathbb{R}\rangle$, coop : $seq\langle\mathsf{Bool}\rangle$, pa : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ap : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ev : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) : $\mathbb{R}$ $= (rec[ind] \cdot intAcum(0, ap[ind], pa[ind], ev[ind])) + (\sum_{i=0}^{|ev[ind]|-1}(fondoPaga(rec, coop, pa, ap, ev, i) \cdot intAcum(i+1, ind, ap, pa, ev)))$;

`aux cantCooperan` (coop : $seq\langle\mathsf{Bool}\rangle$) : $\mathbb{Z}$ $= \sum_{i=0}^{|coop|-1}(\mathsf{if}\ cooperan[i]\ \mathsf{then}\ 1\ \mathsf{else}\ 0\ \mathsf{fi})$;

`aux calcularInicial` (rec : $seq\langle\mathbb{Z}\rangle$, coop : $seq\langle\mathsf{Bool}\rangle$, pa : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, apu : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ev : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) : $\mathbb{R}$ $= ((1/|coop|) \cdot (\sum_{i=0}^{|coop|-1}(\mathsf{if}\ coop[i]\ \mathsf{then}\ apu[i][ev[i][0]] \cdot pa[i][ev[i][0]] \cdot rec[i]\ \mathsf{else}\ 0\ \mathsf{fi}))$;

`aux calcularTasas` (pa : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, apu : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, coop : $seq\langle\mathsf{Bool}\rangle$, t : $\mathbb{Z}$, ev : $seq\langle seq\langle\mathbb{N}\rangle\rangle$) : $\mathbb{R}$ $= ((1/|coop|) \cdot \sum_{i=0}^{|coop|-1}(\mathsf{if}\ coop[i]\ \mathsf{then}\ apu[i][ev[i][t]] \cdot pa[i][ev[i][t]]\ \mathsf{else}\ 0\ \mathsf{fi}))$;

`aux intAcum` (ronda : $\mathbb{Z}$, ind : $\mathbb{Z}$, apu : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, pa : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, ev : $\mathbb{N}$) : $\mathbb{R}$ $= if\ ronda \geq |ev|\ then\ 1\ else\ \prod_{i=\text{ronda}}^{|ev|-1}(pa[ind][ev[ronda]]\ \cdot\ apu[ind][ev[ronda]])$;

`aux fondoPaga` (rec : $seq\langle\mathbb{R}\rangle$, coop : $seq\langle\mathsf{Bool}\rangle$, pa : $seq\langle seq\langle\mathbb{R}\rangle\rangle$, apu : $seq\langle seq\langle\mathbb{N}\rangle\rangle$, ev : $seq\langle seq\langle\mathbb{Z}\rangle\rangle$, ronda : $\mathbb{Z}$) : $\mathbb{R}$ $= rendFondo(rec, coop, pa, apu, \mathsf{subseq}(ev, 0, ronda+1))$;

2. Demostraciones de correctitud

Para demostrar la correctitud de programas que contienen ciclos necesitamos hacer dos cosas: demostrar que la ejecución del programa es correcta y demostrar que el programa termina. Empezaremos demostrando la correctitud del ciclo con el Teorema del Invariante. Primero definimos la precondición y la postcondición del ciclo:

$\mathrm{P}_c \equiv i = 0 \wedge res = recursos \wedge |eventos| \geq 0$

$\mathrm{Q}_c \equiv res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(eventos,true)} \cdot (apuesta_s pago_s)^{\#apariciones(eventos,false)}$

Ahora busquemos el invariante I del ciclo. Notemos que a cada iteración el valor de res (que inicialmente es igual a *recursos*) se multiplica por el valor apostado a cara y su respectivo pago si eventos[i]=*true* o por el valor apostado a sello y su respectivo pago si eventos[i]=*false*. Además, a cada iteración el valor de i se incrementa en 1. Entonces proponemos:

$I \equiv 0 \leq i \leq |eventos| \wedge_L res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s pago_s)^{\#apariciones(subseq(eventos,0,i),false)}$

Como ya tenemos el invariante, empezaremos la demostración de correctitud. Lo primero que vamos a demostrar es que $\mathrm{P}_c \longrightarrow I$:

$\mathrm{P}_c \equiv i = 0 \wedge res = recursos \wedge |eventos| \geq 0$

$\longrightarrow 0 \leq i \leq |eventos| \wedge res = recursos$

$\longrightarrow 0 \leq i \leq |eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^0 \cdot (apuesta_s \cdot pago_s)^0$

$\longrightarrow 0 \leq i \leq |eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,0),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,0),false)}$

$\longrightarrow 0 \leq i \leq |eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)}$

$\equiv I$

Ahora tenemos que demostrar $\{I \wedge B\}\ S\ \{I\}$:

Para demostrar $\{I \wedge B\}\ S\ \{I\}$ *tenemos que probar que* $I \wedge B \longrightarrow wp(S, I)$. *Y sabemos que* $B \equiv i < |eventos|$.
Entonces empecemos calculando la wp:

wp(if . . . endif ; i := i+1 , I)

$\equiv wp(if...endif, wp(i := i+1, I))$

$\equiv wp(if...endif, I^i_{i+1})$

$\equiv (eventos[i] = true \wedge wp(res := res \cdot apuesta_c \cdot pago_c\ , I^i_{i+1})) \vee (eventos[i] = false \wedge wp(res := res \cdot apuesta_s \cdot pago_s\ , I^i_{i+1}))$

$\equiv (eventos[i] = true \wedge ((I^i_{i+1})^{res}_{res \cdot apuesta_c \cdot pago_c})) \vee (eventos[i] = false \wedge ((I^i_{i+1})^{res}_{res \cdot apuesta_s \cdot pago_s}))$

Ahora que ya tenemos la wp, para probar que $I \wedge B \longrightarrow wp(S, I)$ *es verdadero separemos en dos casos* : $eventos[i] = true$ *y* $eventos[i] = false$

Si eventos[i]=*true*, entonces podemos simplificar la wp

$\equiv eventos[i] = true\ \wedge\ ((I^i_{i+1})^{res}_{res \cdot apuesta_c \cdot pago_c})$

$\equiv 0 \leq i+1 \leq |eventos|\ \wedge\ res \cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i+1),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i+1),false)}$

y la implicación quedaría:

$0 \leq i \leq |eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)} \wedge i < |eventos| \longrightarrow_L 0 \leq i+1 \leq |eventos| \ \wedge \ res \cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i+1),true)} \cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i+1),false)}$

Ahora probemos que eso es verdadero:

Por hipótesis, $0 \leq i \leq |eventos|$ $y\ i < |eventos|. Por\ lo\ tanto:$

$0 \leq i < |eventos| \longrightarrow 0 \leq i+1 \leq |eventos| \qquad (1)$

Además, por hipótesis

res = recursos $\cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)} \cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)}$

Por lo tanto,

res $\cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)} \cdot$
(apuesta$_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)} \cdot apuesta_c \cdot pago_c$

Nos damos cuenta de que, al multiplicar apuesta$_c \cdot pago_c$, *la cantidad de apariciones true se incrementa en* 1 *y la cantidad* de apariciones *false* se incrementa en 0:

res $\cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)+1}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)+0}$

res $\cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)+(\text{if } eventos[i]=true \text{ then } 1 \text{ else } 0 \text{ fi})}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)+(\text{if } eventos[i]=false \text{ then } 1 \text{ else } 0 \text{ fi})}$

res $\cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i+1),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i+1),false)} \qquad (2)$

Por (1) y (2) demostramos que $I \wedge B \longrightarrow wp(S,I)$ *se cumple cuando* $eventos[i] = true$. *Ahora lo demostraremos para* eventos[i]=*false*.

Si eventos[i]=*false*, entonces podemos simplificar la wp

$\equiv eventos[i] = false \ \wedge \ ((I^{i}_{i+1})^{res}_{res \cdot apuesta_s \cdot pago_s})$

$\equiv 0 \leq i+1 \leq |eventos| \ \wedge \ res \cdot apuesta_s \cdot pago_s = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i+1),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i+1),false)}$

y la implicación quedaría:

$0 \leq i \leq |eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)} \wedge i < |eventos| \longrightarrow_L 0 \leq i+1 \leq |eventos| \ \wedge \ res \cdot apuesta_s \cdot pago_s = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i+1),true)} \cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i+1),false)}$

Ahora probemos que eso es verdadero:

Por hipótesis, así como en el caso eventos[i]=*true*, $0 \leq i \leq |eventos|$ $y\ i < |eventos|. Por\ lo\ tanto:$

$0 \leq i < |eventos| \longrightarrow 0 \leq i+1 \leq |eventos| \qquad (3)$

Además, por hipótesis

res = recursos $\cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)} \cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)}$

Por lo tanto,
res $\cdot apuesta_s \cdot pago_s = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)} \cdot apuesta_c \cdot pago_c$

Nos damos cuenta de que, al multiplicar apuesta$_s \cdot pago_s$, *la cantidad de apariciones false se incrementa en* 1 *y la cantidad* de apariciones *true* se incrementa en 0:

res $\cdot apuesta_s \cdot pago_s = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)+0}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)+1}$

res $\cdot apuesta_s \cdot pago_s = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)+(\text{if } eventos[i]=true \text{ then } 1 \text{ else } 0 \text{ fi})}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i),false)+(\text{if } eventos[i]=false \text{ then } 1 \text{ else } 0 \text{ fi})}$

res $\cdot apuesta_c \cdot pago_c = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i+1),true)}$
$\cdot (apuesta_s \cdot pago_s)^{\#apariciones(subseq(eventos,0,i+1),false)} \qquad (4)$

Por (3) y (4) demostramos que $I \wedge B \longrightarrow wp(S,I)$ *se cumple cuando* $eventos[i] = false$ *y como ya probamos lo mismo para* eventos[i]=$true$ concluimos que:

$I \wedge B \longrightarrow wp(S, I)$

Finalmente, tenemos que demostrar que $I \wedge \neg B \longrightarrow Q_c$:

I $\wedge \neg B \equiv 0 \leq i \leq |eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s pago_s)^{\#apariciones(subseq(eventos,0,i),false)} \wedge \neg(i < |eventos|)$

$\longrightarrow$ i=$|eventos| \wedge res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,i),true)}$
$\cdot (apuesta_s pago_s)^{\#apariciones(subseq(eventos,0,i),false)}$

$\longrightarrow$ res=recursos $\cdot (apuesta_c \cdot pago_c)^{\#apariciones(subseq(eventos,0,|eventos|),true)}$
$\cdot (apuesta_s pago_s)^{\#apariciones(subseq(eventos,0,eventos),false)}$

$\longrightarrow$ res=recursos $\cdot (apuesta_c \cdot pago_c)^{\#apariciones(eventos,true)} \cdot (apuesta_s \cdot pago_s)^{\#apariciones(eventos,false)}$

$\equiv Q_c$

Entonces, por el Teorema del Invariante concluimos que el ciclo es parcialmente correcto. Ahora nos queda probar que la ejecución del ciclo termina. Eso lo hacemos a través del Teorema de Terminación:

Como B $\equiv i < |eventos|,\ propongo\ la\ función\ variante\ f_v = |eventos| - i.$
Con esta f_v $veamos\ si\ se\ cumplen\ las\ dos\ condiciones\ del\ Teorema\ de\ Terminación.$
Para demostrar que $\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\}\ tenemos\ que\ probar\ que\ (I \wedge B \wedge f_v = v_0) \longrightarrow_L wp(S, f_v < v_0)$
Empecemos calculando la wp:
wp(if . . . endif ; i := i+1 , $|eventos|$ - i < v_0)

$\equiv wp(if...endif, wp(i := i+1, |eventos| - i < v_0))$

$\equiv wp(if...endif, (|eventos| - i < v_0)^i_{i+1})$

$\equiv (eventos[i] = true \wedge wp(res := res \cdot apuesta_c \cdot pago_c\ , (|eventos| - i < v_0)^i_{i+1})) \vee (eventos[i] = false \wedge wp(res := res \cdot apuesta_s \cdot pago_s\ , (|eventos| - i < v_0)^i_{i+1}))$

$\equiv (eventos[i] = true \wedge (((|eventos| - i < v_0)^i_{i+1})^{res}_{res \cdot apuesta_c \cdot pago_c})) \vee (eventos[i] = false \wedge$
$(((|eventos|$-i < $v_0)^i_{i+1})^{res}_{res \cdot apuesta_s \cdot pago_s}))$

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

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

$\equiv |eventos| - (i+1) < v_0$

Como $f_v = |eventos| - i,\ reemplazamos\ a\ v_0\ por\ |eventos| - i$:

$\equiv |eventos| - (i+1) < |eventos| - i$

$\equiv -(i+1) < -i$

$\equiv (i+1) > i$

lo cual es siempre verdadero. Entonces queda demostrado que $(I \wedge B \wedge f_v = v_0) \longrightarrow_L wp(S, f_v < v_0).\ O\ sea,\ se\ cumple\ que\ \{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\}$

Lo último que nos queda demostrar es que (I $\wedge f_v \leq 0) \longrightarrow \neg B$:

$f_v \leq 0 \equiv |eventos| - i \leq 0$

$\equiv |eventos| \leq i$

$\longrightarrow \neg(i < |eventos|)$

$\equiv \neg B$

Entonces queda probado que (I $\wedge f_v \leq 0) \longrightarrow \neg B$.

Hasta ahora, probamos que :

- $P_c \longrightarrow I$
- $\{I \wedge B\}\ S\ \{I\}$
- $I \wedge \neg B \longrightarrow Q_c$
- $\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\}$
- (I $\wedge f_v \leq 0) \longrightarrow \neg B$

Ahora nos queda demostrar que el programa es correcto respecto a la especificación. Para eso, primero debemos demostrar que Pre $\longrightarrow_L wp(S1, P_c)$.

Pre se refiere a la precondición de la especificación (el requiere) y S1 es el código que viene antes del ciclo en el programa, o sea, las asignaciones de las variables res=recursos e i=0.

Pre $\equiv apuesta_c + apuesta_s = 1 \wedge pago_c > 0 \wedge pagp_s > 0 \wedge apuesta_c > 0 \wedge apuesta_s > 0 \wedge recursos > 0$

$P_c \equiv i = 0 \wedge res = recursos \wedge |eventos| \geq 0$

wp(res=recursos ; i=0 , P_c) $\equiv wp(res = recursos, wp(i = 0, P_c))$

wp(i=0, P_c) $\equiv wp(i = 0, i = 0 \wedge res = recursos \wedge |eventos| \geq 0)$

$\equiv def(0) \wedge_L (i = 0 \wedge res = recursos \wedge |eventos| \geq 0)^i_0$

$\equiv 0 = 0 \wedge res = recursos \wedge |eventos| \geq 0$

$\equiv res = recursos \wedge |eventos| \geq 0$

Y ahora miramos:

wp(res=recursos, wp(i=0, P_c)) $\equiv wp(res = recursos, res = recursos \wedge |eventos| \geq 0)$

$\equiv def(recursos) \wedge_L (res = recursos \wedge |eventos| \geq 0)^{res}_{recursos}$

$\equiv recursos = recursos \wedge |eventos| \geq 0$

$\equiv |eventos| \geq 0$

Nos queda probar que:

(apuesta$_c$ $+ apuesta_s = 1 \wedge pago_c > 0 \wedge pagp_s > 0 \wedge apuesta_c > 0 \wedge apuesta_s > 0 \wedge recursos > 0) \longrightarrow_L |eventos| \geq 0$

Como siempre se cumple que $|eventos| \geq 0$ (*pues el largo de una lista no puede ser menor que cero*), *entonces la implicación* es siempre verdadera, como se quería demostrar.

Por último, para terminar de demostrar que el programa es correcto respecto a la especificación debemos probar que $Q_c \longrightarrow_L wp(S3, Post)$.

Post se refiere a la postcondición de la especificación (el asegura) y S3 sería el código que viene después del ciclo en el programa. Como no hay nada después del ciclo en el programa, nos queda probar que $Q_c \longrightarrow_L Post$.

$Q_c \equiv res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(eventos,true)} \cdot (apuesta_s pago_s)^{\#apariciones(eventos,false)}$

Post $\equiv res = recursos \cdot (apuesta_c \cdot pago_c)^{\#apariciones(eventos,true)} \cdot (apuesta_s pago_s)^{\#apariciones(eventos,false)}$

O sea:

(res=recursos $\cdot(apuesta_c \cdot pago_c)^{\#apariciones(eventos,true)} \cdot (apuesta_s pago_s)^{\#apariciones(eventos,false)}) \longrightarrow_L$
(res=recursos $\cdot(apuesta_c \cdot pago_c)^{\#apariciones(eventos,true)} \cdot (apuesta_s pago_s)^{\#apariciones(eventos,false)})$

Esa implicación es verdadera, como se quería demostrar.

En conclusión, queda demostrado por el Teorema del Invariante y el Teorema de Terminación que dada P_c *el ciclo siempre* termina y vale Q_c. *Y además, queda demostrado que ese ciclo es correcto respecto a la especificación propuesta.*