DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo prático 1: Especificación y WP

21 de abril de 2024 | Algoritmos y Estructuras de Datos

Grupo JDDBVCNLUCVDVTZLNSIH

Integrante	LU	Correo electrónico
Labastié, Gaspar	660/23	gaspilabastie@gmail.com
Rugo, Julian	1414/23	julianrugo22@gmail.com
Torres, Emiliano	80/23	emilianomtorres1@gmail.com
Vanotti, Franco	464/23	fvanotti15@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

0. Aclaraciones generales

- Los índices de las listas recursos, cooperan, trayectorias, apuestas, pagos, eventos representa el identificador de los individuos.
- recursos: seq⟨ℝ⟩ es la lista con el recurso de cada individuo.
- cooperan: seq⟨Bool⟩ es la lista que indica T rue si el individuo en dicha posición coopera.
- trayectorias: seq⟨seq⟨ℝ⟩⟩ indica para cada individuo, en cada paso de tiempos, cuántos recursos (ℝ) cuenta.
- eventos: seq⟨seq⟨ℕ⟩⟩ indica para cada individuo, en cada paso temporal, qué evento le ha tocado.
- apuestas: seq⟨seq⟨ℝ⟩⟩ indica para cada individuo, para cada evento posible (numerados desde 0), cuánto apostará.
- pagos: seq⟨seq⟨ℝ⟩⟩ indica para cada individuo, para cada evento, cuánto se pagará. Notar que a diferencia del ejemplo, estams resolviendo un caso más general donde el pago de cada evento puede diferir por individuo.
- Las personas que no *cooperan* no aportan nada al fondo monetario común.
- Los *recursos* iniciales son positivos.
- Todos los *pagos* son positivos.
- Las *apuestas* de los individuos representan la proporción de los recursos que los individuos invierten a cada una de los eventos posibles. Notar nuevamente que a diferencia del ejemplo, en este caso más general, podríamos tener apuestas distintas para cada evento por cada individuo.
- Cada individuo apuesta siempre el mismo porcentaje por cada evento posible (es decir, el mismo número en cada paso temporal). Por ejemplo, si tenemos dos eventos; cara y ceca y apuesta 0, 4 por cara y 0,6 por seca, en cada paso temporal apostará esas proporciones.
- Se considera al número 0 como parte de ℕ.
- Debido a la ambigüedad presente en el ejercico sobre especificación en cuanto a si un jugador puede o no puede apostar todo sus recursos a un unico evento, y por ende que la apuesta de dicho jugador a un evento sea igual a 0, nosotros tomamos bajo nuestro criterio personal que eso si es posible, y se llevo a cabo el ejercicio considerando dicha posibilidad.

1. 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` $recursos : \text{seq}\langle\mathbb{R}\rangle$, `in` $cooperan : seq\langle Bool\rangle$) : $\text{seq}\langle\mathbb{R}\rangle$

`requiere` $\{|recursos| > 0 \land |recursos| = |cooperan| \land$
$(\forall i : \mathbb{Z})\ (0 \leq i < |recursos| \longrightarrow_L recursos[i] > 0)\}$

`asegura` $\{|res| = |recursos| \land_L nuevosRecursosCooperan(recursos, cooperan, res) \land$
$nuevosRecursosNoCooperan(recursos, cooperan, res)\}$

`pred` `nuevosRecursosCooperan` ($recursos : \text{seq}\langle\mathbb{R}\rangle,\ cooperan : seq\langle Bool\rangle,\ res : \text{seq}\langle\mathbb{R}\rangle$) {

$(\forall i : \mathbb{Z})\ (0 \leq i < |recursos| \land_L cooperan[i] = \text{true} \longrightarrow_L res[i] = distribuciónFondoComún(recursos, cooperan))$

}

`pred` `nuevosRecursosNoCooperan` ($recursos : \text{seq}\langle\mathbb{R}\rangle,\ cooperan : seq\langle Bool\rangle,\ res : \text{seq}\langle\mathbb{R}\rangle$) {

$(\forall i : \mathbb{Z})\ (0 \leq i < |recursos| \land_L cooperan[i] = \text{false} \longrightarrow_L res[i] = distribuciónFondoComún(recursos, cooperan) +$
$recursos[i])$

}

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

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⟨seq⟨$\mathbb{R}$⟩⟩, in $cooperan : seq\langle Bool\rangle$, in $apuestas$: seq⟨seq⟨$\mathbb{R}$⟩⟩, in $pagos$: seq⟨seq⟨$\mathbb{R}$⟩⟩, in $eventos$: seq⟨seq⟨$\mathbb{N}$⟩⟩)

   `requiere` $\{|trayectorias| = |cooperan| = |apuestas| = |pagos| = |eventos| \wedge$
   $trayectorias = Trayectorias_0 \wedge_L$
   $(\forall i : \mathbb{Z})(0 \leq i < |trayectorias| \longrightarrow_L (|trayectorias[i]| = 1 \wedge trayectorias[i][0] > 0)) \wedge |pagos| > 0 \wedge$
   $(\forall k, l : \mathbb{Z})(0 \leq k, l < |apuestas| \longrightarrow_L |apuestas[k]| = |apuestas[l]|) \wedge$
   $(\forall i : \mathbb{Z})((0 \leq i < |apuestas| \longrightarrow_L sumarApuestasIndividuo(apuestas[i]) = 1) \wedge_L$
   $(\forall j : \mathbb{Z})(0 \leq j < |apuestas[i]| \longrightarrow_L 0 \leq apuestas[i][j] \leq 1)) \wedge$
   $(\forall k, l : \mathbb{Z})(0 \leq k, l < |pagos| \longrightarrow_L |pagos[k]| = |pagos[l]|) \wedge$
   $(\forall i : \mathbb{Z})(0 \leq i < |pagos| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |pagos[i]| \longrightarrow_L 0 < pagos[i][j])) \wedge$
   $(\forall i : \mathbb{Z})(0 \leq i < |pagos| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |apuestas| \longrightarrow_L |pagos[i]| = |apuestas[j]|)) \wedge$
   $(\forall i : \mathbb{Z})(0 \leq i < |eventos| \longrightarrow_L |eventos[i]| > 0) \wedge$
   $(\forall i : \mathbb{Z})(0 \leq i < |eventos| \longrightarrow_L |eventos[0]| = |eventos[i]|) \wedge$
   $(\forall i : \mathbb{Z})(0 \leq i < |eventos| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |eventos[i]| \longrightarrow_L 0 \leq eventos[i][j] < |pagos[i]|))\}$

   `asegura` $\{|trayectorias| = |eventos| \wedge_L (\forall i : \mathbb{Z})(0 \leq i < |trayectorias| \longrightarrow_L trayectorias[i][0] = Trayectorias_0[i][0]) \wedge$

   $(\forall i : \mathbb{Z})(0 \leq i < |trayectorias| \longrightarrow_L |trayectorias[i]| = |eventos[i]| + 1) \wedge$
   $(\forall i : \mathbb{Z})(0 \leq i < |trayectorias| \longrightarrow_L (\forall j : \mathbb{Z})(0 < j < |trayectorias[i]| \longrightarrow_L$
   $(trayectoriasCooperan(trayectorias, cooperan, apuestas, pagos, eventos) \wedge$
   $trayectoriasNoCooperan(trayectorias, cooperan, apuestas, pagos, eventos))))\}$

   `pred trayectoriasCooperan` ($trayectorias$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $cooperan$: seq⟨Bool⟩, $apuestas$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $pagos$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $eventos$: seq⟨seq⟨$\mathbb{Z}$⟩⟩) {

   $cooperan[i] = \text{true} \longrightarrow_L trayectorias[i][j] = distribuciónFondoComúnTrayectoria(trayectorias, cooperan, apuestas, pagos, eventos, j)$

   }

   `pred trayectoriasNoCooperan` ($trayectorias$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $cooperan$: seq⟨Bool⟩, $apuestas$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $pagos$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $eventos$: seq⟨seq⟨$\mathbb{Z}$⟩⟩) {

   $cooperan[i] = \text{false} \longrightarrow_L trayectorias[i][j] = distribuciónFondoComúnTrayectoria(trayectorias, cooperan, apuestas, pagos, eventos, j) + trayectoria[i][j-1] * gananciaIndividuo(apuestas[i], pagos[i], eventos[i][j-1])$

   }

   `aux sumarApuestasIndividuo` ($apuestasIndividuo$: seq⟨$\mathbb{R}$⟩) : $\mathbb{R}$ = $(\sum_{n=0}^{|apuestasIndividuo|-1})(apuestasIndividuo[n])$ **;**

   `aux gananciaIndividuo` ($apuestaIndividuo$: seq⟨$\mathbb{R}$⟩, $pagosIndividuo$: seq⟨$\mathbb{R}$⟩, $resultadoEventoIndividuo$: $\mathbb{R}$) : $\mathbb{R}$ = $apuestaIndividuo[resultadoEventoIndividuo] * pagosIndividuo[resultadoEventoIndividuo]$ **;**

   `aux recolecciónFondoComún` ($trayectorias$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $cooperan : seq\langle Bool\rangle$, $apuestas$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $pagos$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $eventos$: seq⟨seq⟨$\mathbb{N}$⟩⟩, j : $\mathbb{Z}$) : $\mathbb{R}$ = $(\sum_{i=0}^{j-1})(if\ cooperan[i] = \text{true}\ then\ trayectorias[i][j-1] * gananciaIndividuo(apuestas[i], pagos[i], eventos[i][j-1])\ else\ 0\ fi)$

   `aux distribuciónFondoComúnTrayectoria` ($trayectorias$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $cooperan : seq\langle Bool\rangle$, $apuestas$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $pagos$: seq⟨seq⟨$\mathbb{R}$⟩⟩, $eventos$: seq⟨seq⟨$\mathbb{N}$⟩⟩, j : $\mathbb{Z}$) : $\mathbb{R}$ = $\frac{(recolecciónFondoComún(trayectorias, cooperan, apuestas, pagos, eventos, j))}{|trayectorias|}$ **;**

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.

   `proc trayectoriaExtrañaEscalera` (in *trayectoria*: seq⟨ℝ⟩) : Bool

   `requiere` $\{|trayectoria| > 0 \land (\forall i : \mathbb{Z})\ (0 \leq i < |trayectoria| \longrightarrow_L trayectoria[i] \geq 0)\}$

   `asegura` $\{res = \text{true} \longleftrightarrow$
   $(\exists m : \mathbb{Z})((\forall i : \mathbb{Z})((0 \leq i, m < |trayectoria| \land i \neq m) \longrightarrow_L trayectoria[m] > trayectoria[i]) \land_L$
   $(\forall n : \mathbb{Z})(0 \leq n \leq m \longrightarrow_L trayectoria[n] > trayectoria[n-1]) \land$
   $(\forall n : \mathbb{Z})(m \leq n < |trayectoria| - 1 \longrightarrow_L trayectoria[n] > trayectoria[n+1]))\}$

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 de los *eventos* que recibe cada individuo, eligiendo el comportamiento que maximiza sus recursos individuales luego de que ocurren todos los eventos.

   `proc individuoDecideSiCooperarONo` (in *individuo*:ℕ, in *recursos*: seq⟨ℝ⟩, inout *cooperan*: seq⟨Bool⟩, in *apuestas*: seq⟨seq⟨ℝ⟩⟩, in *pagos*: seq⟨seq⟨ℝ⟩⟩, in *eventos*: seq⟨seq⟨ℕ⟩⟩)

   `requiere` $\{|recursos| > 0 \land |recursos| = |cooperan| = |apuestas| = |pagos| = |eventos| \land$
   $cooperan = Cooperan_0 \land$
   $0 \leq individuo < |recursos| \land_L$
   $(\forall i : \mathbb{Z})(0 \leq i < |recursos| \longrightarrow_L recursos[i] > 0) \land$
   $(\forall i : \mathbb{Z})(0 \leq i < |eventos| \longrightarrow_L |eventos[i]| > 0) \land$
   $(\forall i : \mathbb{Z})(0 \leq i < |eventos| \longrightarrow_L |eventos[i]| = |eventos[0]|) \land$
   $(\forall i : \mathbb{Z})(0 \leq i < |eventos| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |eventos[i]| \longrightarrow_L 0 \leq eventos[i][j] < |pagos[i]|)) \land$
   $(\forall k, l : \mathbb{Z})(0 \leq k, l < |apuestas| \longrightarrow_L |apuestas[k]| = |apuestas[l]|) \land$
   $(\forall i : \mathbb{Z})((0 \leq i < |apuestas| \longrightarrow_L sumarApuestasIndividuo(apuestas[i]) = 1) \land_L$
   $(\forall j : \mathbb{Z})(0 \leq j < |apuestas[i]| \longrightarrow_L 0 \leq apuestas[i][j] \leq 1)) \land$
   $(\forall k, l : \mathbb{Z})(0 \leq k, l < |pagos| \longrightarrow_L |pagos[k]| = |pagos[l]|) \land$
   $(\forall i : \mathbb{Z})(0 \leq i < |pagos| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |pagos[i]| \longrightarrow_L 0 < pagos[i][j])) \land$
   $(\forall i : \mathbb{Z})(0 \leq i < |pagos| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < |apuestas| \longrightarrow_L |pagos[i]| = |apuestas[j]|))\}$

   `asegura` $\{|cooperan| = |Cooperan_0| \land_L$
   $(\forall i : \mathbb{Z})(0 \leq i < |Cooperan_0| \land i \neq individuo \longrightarrow_L cooperan[i] = Cooperan_0[i]) \land$
   $(\exists cooperanAlt : seq{<}Bool{>})((|cooperanAlt| = |Cooperan_0| \land_L$
   $(\forall i : \mathbb{Z})(0 \leq i < |cooperanAlt| \land i \neq individuo \longrightarrow_L cooperanAlt[i] = Cooperan_0[i]) \land$
   $(cooperanAlt[individuo] = \neg Cooperan_0[individuo])) \land$
   $(\exists trayectoria : seq\langle seq\langle \mathbb{R}\rangle\rangle)(|trayectoria| = |eventos| \land_L primeroTieneARecursos(recursos, trayectoria) \land$
   $moduloEventosMasUno(eventos, trayectoria) \land elementosDeT(apuestas, pagos, eventos, Cooperan_0, trayectoria) \land$
   $(\exists trayectoriaAlt : seq\langle seq\langle \mathbb{R}\rangle\rangle)(|trayectoriaAlt| = |eventos| \land_L primeroTieneARecursos(recursos, trayectoriaAlt) \land$
   $moduloEventosMasUno(eventos, trayectoriaAlt) \land$
   $elementosDeT(apuestas, pagos, eventos, cooperanAlt, trayectoriaAlt) \land_L$
   $cooperan[individuo] = mejorEleccion(trayectoria, trayectoriaAlt, Individuo))))\}$

   `pred primeroTieneARecursos` (*recursos*:seq⟨ℝ⟩, *trayectoria*:seq⟨seq⟨ℝ⟩⟩) {

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

   }

   `pred moduloEventosMasUno` (*eventos*:seq⟨seq⟨ℝ⟩⟩, *trayectoria*:seq⟨seq⟨ℝ⟩⟩) {

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

   }

   `pred elementosDeT` (*apuestas*:seq⟨seq⟨ℝ⟩⟩,*pagos*:seq⟨seq⟨ℝ⟩⟩, *eventos*:seq⟨seq⟨ℝ⟩⟩, *cooperan*:seq⟨Bool⟩, *trayectoria*:seq⟨seq⟨ℝ⟩⟩) {

   $(\forall i : \mathbb{Z})(0 \leq i < |trayectoria| \longrightarrow_L (\forall j : \mathbb{Z})(0 \leq j < ||trayectoria[i]| \longrightarrow_L$
   $trayectoriasCooperan(trayectorias, cooperan, apuestas, pagos, eventos) \land$
   $trayectoriasNoCooperan(trayectorias, cooperan, apuestas, pagos, eventos)))$

   }

   `aux mejorEleccion` (*trayectoria*:seq⟨seq⟨ℝ⟩⟩,*trayectoriaAlt*:seq⟨seq⟨ℝ⟩⟩,*Individuo*) : Bool =
   $(if\ \ trayectoria[individuo][|trayectoria[Individuo]| - 1] \geq trayectoriaAlt[individuo][|trayectoriaAlt[Individuo]| - 1]\ \ then$
   $Cooperan_0[individuo]\ \ else\ \ CooperanAlt[individuo]\ \ fi)$;

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 de los eventos que recibe cada individuo, eligiendo la apuesta que maximiza sus recursos individuales luego de que ocurren todos los eventos.

proc `individuoActualizaApuesta` (in $individuo$: $\mathbb{N}$, in $recursos$: seq$\langle\mathbb{R}\rangle$, in $cooperan$: seq$\langle$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 $\{|recursos| > 0 \land |recursos| = |cooperan| = |apuestas| = |pagos| = |eventos| \land_L$
$(\forall i : \mathbb{Z})(0 \leq i < |recursos| \longrightarrow_L recursos[i] > 0) \land$
$apuestas = Apuestas_0 \land$
$(\forall i, j : \mathbb{Z})(0 \leq i, j < |apuestas| \longrightarrow_L |apuestas[i]| = |apuestas[j]|) \land$
$(\forall i : \mathbb{Z})(0 \leq i < |apuestas| \longrightarrow_L sumarApuestasIndividuo(apuestas[i] = 1)) \land$
$(\forall i, j : \mathbb{Z})(0 \leq i < |apuestas| \longrightarrow_L 0 \leq apuestas[i][j] \geq 1) \land$
$(\forall i, j : \mathbb{Z})(0 \leq i < |pagos| \land 0 \leq j < |pagos[i]| \longrightarrow_L pagos[i][j] > 0) \land$
$(\forall i, j : \mathbb{Z})(0 \leq i, j < |eventos| \longrightarrow_L |eventos[i]| = |eventos[j]|) \land$
$(\forall i, j : \mathbb{Z})(0 \leq i < |eventos| \land 0 \leq j < |eventos[i]| \longrightarrow_L 0 \leq eventos[i][j] \geq |pagos[i]|)\}$

asegura $\{(\exists m : seq\langle seq\langle\mathbb{R}\rangle\rangle)(esApuestaVariante(m, individuo) \land_L (\exists trayectoriam : seq\langle seq\langle\mathbb{R}\rangle\rangle)$
$(esTrayectoria(trayectoriam, recursos, eventos, pagos, cooperan, m) \land_L$
$(\forall A : seq\langle seq\langle\mathbb{R}\rangle\rangle)(esApuestaVariante(A, individuo) \longrightarrow_L$
$(\forall trayectoria : seq\langle seq\langle\mathbb{R}\rangle\rangle)(esTrayectoria(trayectoria, recursos, eventos, pagos, cooperan, A) \longrightarrow_L$
$trayectoriam[individuo][|trayectoriam[individuo]| - 1] \geq trayectoria[individuo][|trayectoria[individuo]| - 1])))))\}$

pred `esApuestaVariante` (A : seq$\langle$seq$\langle\mathbb{R}\rangle\rangle$, $individuo$: $\mathbb{N}$) {

$|A| = |Apuestas_0| \land (\forall i : \mathbb{Z})(0 \leq i < |Apuestas_0| \land i \neq individuo \longrightarrow_L A[i] = Apuestas_0[i]) \land$
$|A[individuo]| = |Apuestas_0[0]| \land sumarApuestasIndividuo(A[individuo]) = 1 \land$
$(\forall j : \mathbb{Z})(0 \leq j < |A[individuo]| \longrightarrow_L 0 \leq A[individuo][j] \leq 1)$

}

pred `esTrayectoria` ($trayectoria$: seq$\langle$seq$\langle\mathbb{R}\rangle\rangle$,$recursos$: seq$\langle\mathbb{R}\rangle$,$eventos$: seq$\langle$seq$\langle\mathbb{Z}\rangle\rangle$,$pagos$: seq$\langle$seq$\langle\mathbb{R}\rangle\rangle$, $cooperan$: seq$\langle$Bool$\rangle$, $apuestas$: seq$\langle$seq$\langle\mathbb{R}\rangle\rangle$) {

$primeroTieneARecursos(recursos, trayectoria) \land moduloEventosMasUno(eventos, trayectoria) \land$
$elementosDeT(apuestas, pagos, eventos, cooperan, trayectoria)$

}

2. Demostraciones de correctitud

Demostrar que la siguiente especificación es correcta respecto de su implementación. La función **frutoDelTrabajoPuramenteIndividual** calcula, para el ejemplo de apuestas al juego de cara o sello, cuánto se ganaría si se juega completamente solo. Se contempla que el evento *True* es cuando sale cara

`proc frutoDelTrabajoPuramenteIndividual` (in *recursos*:seq⟨$\mathbb{R}$⟩, in *apuestas*:⟨s: $\mathbb{R}$, c:$\mathbb{R}$⟩,in *pago*:⟨s: $\mathbb{R}$, c:$\mathbb{R}$⟩,in *eventos*:seq⟨Bool⟩, out res: $\mathbb{R}$)

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

`asegura` $\{res = recurso(apuesta_c pago_c)^{\#apariciones(eventos,T)}(apuesta_s pago_s)^{\#apariciones(eventos,F)}\}$

Donde $\#apariciones(eventos,\ T)$ es el auxiliar utilizado en la téorica, y #(eventos, T) es su abreviación.

res = *recursos*
i = 0
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

Para probar la correctitud de este código usamos el teorema de correción de un ciclo, para lo cual se propone el siguiente invariante:

$I \equiv 0 \leq i \leq |eventos| \land$
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$

Y la siguiente funcion decreciente:
$\mathsf{f_v} \equiv |eventos| - i$

Entonces hay que probar:

1. $\mathsf{P_c} \longrightarrow I$
2. $\{I \land B\} \quad S \quad \{I\}$
3. $I \land \neg B \longrightarrow \mathsf{Q_c}$
4. $\{I \land B \land \mathsf{v_0} = \mathsf{f_v}\} \quad S \quad \{\mathsf{f_v} < \mathsf{v_0}\}$
5. $I \land \mathsf{f_v} \leq 0 \longrightarrow \neg B$

1. Veamos que se cumple 1 ($\mathsf{P_c} \longrightarrow I$):

   $\mathsf{P_c} \equiv res = recursos \land i = 0$
   $I \equiv 0 \leq i \leq |eventos| \land$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$

   Podemos remplazar $\mathsf{P_c}$ en I para ver que es tautologico.

   $I \equiv 0 \leq 0 \leq |eventos| \land$
   $recurso = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{0-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{0-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$
   $\equiv \text{true} \land res = recurso(apuesta_c pago_c)^0(apuesta_s pago_s)^0$
   $\equiv \text{true} \land recurso = recurso \equiv \text{true}$

   Entonces se puede observar que $\mathsf{P_c} \longrightarrow I$ se cumple.

2. Veamos que se cumple 2 ($\{I \land B\} \quad S \quad \{I\}$):
$I \equiv 0 \leq i \leq |eventos| \land$
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$
$B : i < |eventos|$
Primero vemos si $I \land B \longrightarrow wp(if..., i := i + 1, I)$
$wp(i := i + 1, I) \equiv def(i + 1) \land_L \mathsf{I}^{\mathsf{i}}_{\mathsf{i+1}} \equiv (-1 \leq i \leq |eventos| - 1) \land$
$(res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)})$
$\equiv E1$

Entonces:
$wp(if..., E1) \equiv def(eventos[i]) \land ((eventos[i] \land wp(res := res\mathsf{apuesta_c pago_c}, E1)) \lor$
$(\neg eventos[i] \land wp(res := res\mathsf{apuesta_s} pagos, E1)))$
$\equiv (0 \leq i \leq |eventos|) \land$
$((eventos[i] \land$
$res\mathsf{apuesta_c pago_c} = recurso(\mathsf{apuesta_c pago_c})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}(\mathsf{apuesta_s pago_s})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)})$
$\lor$
$(\neg eventos[i] \land$
$res\mathsf{apuesta_s pago_s} = recurso(\mathsf{apuesta_c pago_c})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}(\mathsf{apuesta_s pago_s})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)})$
$)$
Luego, en la ecuacion:
$res\mathsf{apuesta_c pago_c} = recurso(\mathsf{apuesta_c pago_c})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}(\mathsf{apuesta_s pago_s})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)}$
se puede pasar dividiendo el término $\mathsf{apuesta_c pago_c}$ dividiendo, ya que tanto $apuesta_c$ como $pago_c$ son mayores a 0 por lo pedido en el requiere.
Lo mismo ocurre en la ecuacion:
$res\mathsf{apuesta_s pago_s} = recurso(\mathsf{apuesta_c pago_c})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}(\mathsf{apuesta_s pago_s})^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)}$
donde se puede pasar dividiendo el término $\mathsf{apuesta_s pago_s}$ dividiendo por la misma razón.

De esta forma, se obtiene la siguiente expresión:
$wp(if..., E1) \equiv (0 \leq i \leq |eventos|) \land$
$((eventos[i] \land$
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)}) \lor$
$(\neg eventos[i] \land$
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)}))$

Por otro lado, tambien cabe destacar que en las ecuaciones:
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)}$ y
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)}$
se pueden reemplazar
$(apuesta_s pago_s)^{(\sum_{j=0}^{i})(ifeventos[j]=\text{false}then1else0fi)}$ por $(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)}$ y
$(apuesta_c pago_c)^{(\sum_{j=0}^{i})(ifeventos[j]=\text{true}then1else0fi)}$ por $(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}$
respectivamente, ya que en que ambos casos, el último elemento es igual a 0 y por ende no afecta al resultado de la sumatoria.

De ahí que se obtiene la siguiente expresión:
$wp(if..., E1) \equiv (0 \leq i \leq |eventos|) \land$
$((eventos[i] \land$
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)}) \lor$
$(\neg eventos[i] \land$
$res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)}))$
$\equiv (0 \leq i \leq |eventos|) \land ((eventos[i] \lor \neg eventos[i]) \land$
$(res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)}))$
$\equiv (0 \leq i \leq |eventos|) \land$
$(res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{true}then1else0fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(ifeventos[j]=\text{false}then1else0fi)})$
$\equiv I$
Entonces se puede observar que $\{I \land B\} \quad S \quad \{I\}$ se cumple.

3. Veamos que se cumple 3 ($I \wedge \neg B \longrightarrow \mathsf{Q_c}$):

   $\mathsf{Q_c}$: $res = recurso(apuesta_c pago_c)^{\#apariciones(eventos, T)}(apuesta_s pago_s)^{\#apariciones(eventos, F)}$

   $\neg B : i \geq |eventos|$

   $I \wedge \neg B \longrightarrow \mathsf{Q_c}$

   $I \wedge \neg B \equiv 0 \leq i \leq |eventos| \wedge i \geq |eventos|$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$

   $I \wedge \neg B \equiv i = |eventos| \wedge$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{|eventos|-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{|eventos|-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$
   $I \wedge \neg B \equiv i = |eventos| \wedge res = recurso(apuesta_c pago_c)^{\#apariciones(eventos, T)}(apuesta_s pago_s)^{\#apariciones(eventos, F)}$

   Entonces se puede observar que $I \wedge \neg B \longrightarrow \mathsf{Q_c}$ se cumple.

4. Veamos que se cumple 4 ($\{I \wedge B \wedge \mathsf{v_0} = \mathsf{f_v}\}\ \ S\ \ \{\mathsf{f_v} < \mathsf{v_0}\}$):

   $I \equiv 0 \leq i \leq |eventos| \wedge$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$
   $B \equiv i < |eventos|$
   $\mathsf{f_v} = |evento| - i = \mathsf{v_0}$
   $I \wedge B \wedge \mathsf{v_0} = \mathsf{f_v}$
   $\equiv 0 \leq i \leq |eventos| \wedge$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)} \wedge$
   $i \leq |eventos| \wedge |evento| - i = \mathsf{v_0}$
   $\equiv 0 \leq i < |eventos| \wedge |evento| - i = \mathsf{v_0} \wedge$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)}$

   Primero hay que buscar la precondición más débil del ciclo:
   $wp(i := i+1, \mathsf{f_v} < \mathsf{v_0}) \equiv def(i+1) \wedge Q^i_{i+1} \equiv def(i) \wedge |evento| - (i+1) < \mathsf{v_0} \equiv def(i) \wedge |evento| - i \leq \mathsf{v_0}$

   Luego tenemos la siguiente expresión:
   $wp((if\ eventos[i]\ then\ res = (res * apuesta_c) pago_c\ else\ res = (res * apuesta_s) pago_s\ fi), Q)$
   $\equiv def(eventos[i]) \wedge_L ((eventos[i] \wedge wp(res := res(apuesta_c pago_c), Q)) \vee (\neg eventos[i] \wedge wp(res := res(apuesta_s pago_s), Q)))$
   $\equiv 0 \leq i < |evento| \wedge_L ((eventos[i] \wedge def(res(apuesta_c pago_c)) \wedge (def(i) \wedge |evento| - i \leq \mathsf{v_0})) \vee$
   $(\neg eventos[i] \wedge def(res(apuesta_s pago_s)) \wedge (def(i) \wedge |evento| - i \leq \mathsf{v_0})))$
   $\equiv 0 \leq i < |evento| \wedge_L ((eventos[i] \wedge def(res) \wedge def(apuesta_c) \wedge def(pago_c) \wedge def(i) \wedge |evento| - i \leq \mathsf{v_0}) \vee$
   $(\neg eventos[i] \wedge def(res) \wedge def(apuesta_s) \wedge def(pago_s) \wedge def(i) \wedge |evento| - i \leq \mathsf{v_0}))$
   $\equiv 0 \leq i < |evento| \wedge_L ((eventos[i] \wedge |evento| - i \leq \mathsf{v_0}) \vee (\neg eventos[i] \wedge |evento| - i \leq \mathsf{v_0}))$
   $\equiv 0 \leq i < |evento| \wedge_L ((eventos[i] \vee \neg eventos[i]) \wedge |evento| - i \leq \mathsf{v_0})$
   $\equiv 0 \leq i < |evento| \wedge |evento| - i \leq \mathsf{v_0}$

   Finalmente, se puede observar:
   $(0 \leq i < |eventos| \wedge |evento| - i = \mathsf{v_0} \wedge$
   $res = recurso(apuesta_c pago_c)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{true}\ then\ 1\ else\ 0\ fi)}(apuesta_s pago_s)^{(\sum_{j=0}^{i-1})(if\ eventos[j]=\text{false}\ then\ 1\ else\ 0 fi)})$
   $\longrightarrow (0 \leq i < |eventos| \wedge |evento| - i = \mathsf{v_0}) \longrightarrow (0 \leq i < |evento| \wedge |evento| - i \leq \mathsf{v_0})$
   y por ende, $\{I \wedge B \wedge \mathsf{v_0} = \mathsf{f_v}\}\ \ S\ \ \{\mathsf{f_v} < \mathsf{v_0}\}$ se cumple.

5. Veamos que se cumple 5 ($I \wedge \mathsf{f_v} \leq 0 \longrightarrow \neg B$):

   $\mathsf{f_v} \equiv |eventos| - i$

   $\neg B \equiv i \geq |eventos|$

   $I \wedge \mathsf{f_v} \leq 0 \equiv I \wedge |eventos| - i \leq 0 \equiv I \wedge |eventos| \leq i \equiv I \wedge \neg B$

   Luego, $I \wedge \neg B \longrightarrow \neg B$

   Entonces se puede observar que $I \wedge \mathsf{f_v} \leq 0 \longrightarrow \neg B$ se cumple.